

WIRELESS SENSING AND COMMUNICATION DESIGN FOR THE INTERNET OF THINGS: AN ANALYSIS

S.Devipriya¹, M.Jestin Joseph², S.Karthick³

^{1,2,3}Assistant professor, Department of ECE, Annapoorana Engineering College, Salem

Abstract

The Internet is evolving from a network that is centred on people to one that is centred on objects. By 2020, it is predicted that 50 billion things will be connected to the Internet. However, maintaining compatibility across diverse Internet things, such as handheld mobile devices, wireless connectivity, and Radio Frequency Authentication, becomes incredibly challenging as a result of this shift. Numerous little devices are now being used in various facets of daily life thanks to advancements in wireless information and electronic equipment. These devices are capable of sensing, computing, and communicating. Common parts include integrated CPUs, several intelligent systems, and low-power antennas. A WSN, which is necessary for sensing and monitoring environmental factors, is built using these sensors. In addition to WSNs, the idea of the Internet of Things (IoT) is gaining popularity. According to this definition, the IoT is the connection of identifiable objects to the internet for the purpose of detection and monitoring.

Keywords: wireless sensor network, Internet of things, identification, radio frequency, technology, devices, interoperability

1. INTRODUCTION

WSNs are small-scale sensor collecting nodes that are used to observe, sense, capture, and analyse data in the vicinity of an implementation— i.e., events of focus. As a consequence, these nodes are resource-hungry while also being highly reliant on battery management, storage, processing, data size, and available connectivity. Normally, these networks are fixed in a specific method and left as a single point in a residing in remote location to perform information tracking and gathering. The term "wireless" has evolved into a broad and vague term for telecommunications in which electromagnetic radiation are employed to transfer data over a portion or the entire communication line.

The term "Internet of Things" refers to a wide range of research and innovation that allows Internet people to login with the physical world. However, there are two primary understandings of what the Internet of Things entails and, as a result, what kind of technological breakthroughs should be evaluated. [1]Alternatively, techniques such as RFID,

low-range communication technology, real-time localization, and network sensing are frequently used in IoT. [2] From this perspective, the key feature of IoT is the use of wireless detector communications, which enables device functionality. However, one line of research suggests that the meaning of the term "thing" must not be confined to a physical object, but should also include conceptual and virtual parts, particularly those related to service. [3]

WSNs have piqued academics' interest due to fast technological advancements in wireless communication and integrated electronics. A typical WSN is made up of nodes, which are small devices. Embedded CPUs, limited processing capability, and sensor technologies are all present in these nodes. Endpoints are used to detect the environmental parameters like moisture, pressure, temperature, and vibration using these sensors. [4] Sensor interface, computation unit, transceiver unit, and power unit are typical components of a WSN node. These devices serve critical functions by allowing nodes to connect with one another in order to relay data collected by their sensors. To establish a centralised system, connectivity between the components is required.

[11-13] For a number of applications, such as monitoring systems, smart homes, social work, and public safety, WSNs offer indisputable advantages over traditional approaches. WSNs are a part of the IP that helps to create the Internet of Things by linking common things to the Internet. On the basis of detecting scope development, the mainstream has increased greatly, while WSN devices became more cost-effective. This, on the other hand, has shown a plan for a massive increasing tracking expansion of sensor-equipped system status, structures, automobiles, and equipment. [14-17] Wireless networks' core components concentrate around current breakthroughs in networking technology innovation, such as wireless technology and portable ad-hoc connectivity in conjunction with device-coordinating techniques. [18-19] As a result, WSNs are positioned to be used in monitoring transportation infrastructures such as mass transportation, bed tracking, gear monitoring, and bridges, and also vehicle location and safety, particularly wheels, waggons, divots, and frames. [20] Condition-monitoring eliminates the requirement for human examinations by automating monitoring, minimizes repairs by detecting problems in advance, and increases general wellbeing and dependability.

2. SYSTEM ARCHITECTURE

The suggested system for incorporating WSNs into IoT is made up of several key components, including: 1. Wireless Sensor Network (WSN)

3. Middleware 2. Portal Server

4. Client for mobile devices

The WSN's communication channel is Zigbee, and the core network is IPv6. The connection between the gateway node, gateway, and portable client, on the other hand, is built on IPv4 over Wi-Fi. This architecture allows every device in the system to interact with other device,

regardless of the multimedia technologies or network protocol utilised . The system structure is shown in Fig 1.

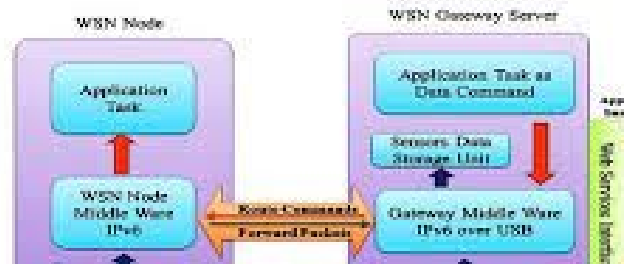


Fig. 1. System Architecture in General

It shows the system's four primary components, as well as the essential subcomponents. The information flow between the system's many components is also depicted in this diagram. The operational sequence diagram, shown in Figure 2, displays the many elements of the system and also the links that exist between them.

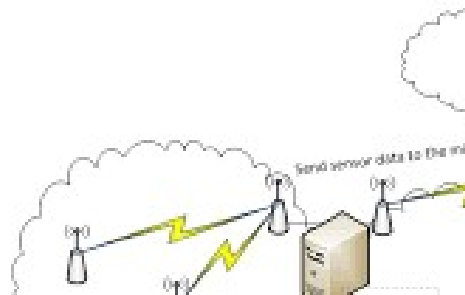


Fig. 2. Network Diagram

2.1.WSN

The WSNs test-bed is made up of seven Crossbow MPR2600 motes. The WSN was a multi-hop wireless service that connects the AODV routing technology from a network topology standpoint. It's an ad-hoc network in which motes can be deployed anywhere with no predetermined topology as much as there's at least one wireless transmission link.

2.2. WSNs Communication Architecture

A radio consists of two parts: a broadcaster and a reception. These two components must be provided for any node in order for it to communicate with other nodes fully. The radio collects information from the brain and distributes it to other sensor network during data transfer. The radio collects information from some other node's antenna and transfers it to the brain throughout data reception. The parent node receives all of the data received by the

sensor node. This parent network is linked to a multi-functional desktop, allowing users to access data from other nodes via the computing device. If the user provides instructions, the instructions will be transferred to the multi-functional computer via the Internet.

2.3.Sensor Node

One of the most important elements of any WSN is the sensory - motor. A sensor node was a compact, low-power gadget. It features concurrent processing capabilities and a reasonable cost, despite its restricted energy supplies. The elements of a sensor node are indicated in Figure 3. A sensor node's specialised units are in charge of data gathering and data transport.

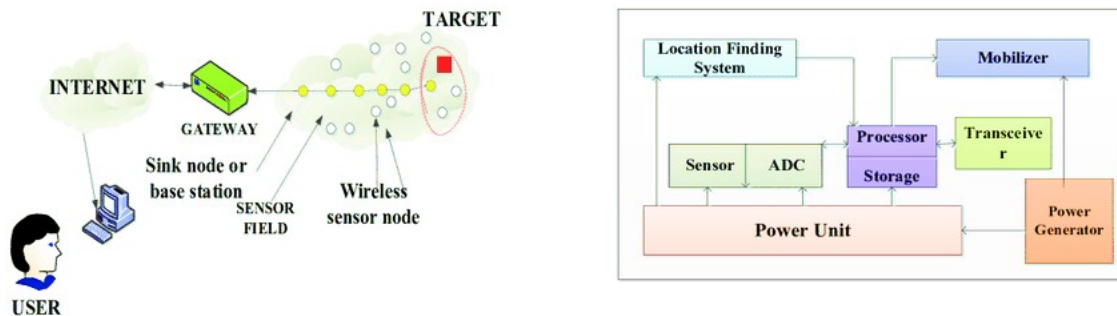


Fig. 3. WSN Components

2.4.IPv4/IPv6 Gateway

This is the most important part of the system. It deals with the issue of gatewaying between IPv4 and IPv4 networks, such as the Web and the WSN. While the WSN system only allows IPv6, other elements like middleware and the smartphone client do not require an IPv6 address, we still want those parts to be able to connect regardless of the IP technology utilised.

2.5.Power Source

The sensor node's base is connected to the power source. It provides power to various sensor node components such as sensing units (sensors), CPUs, and radios. Energy is required to continue performing sensing, processing, and communication operations. As a result, strategies for gathering ambient energy are employed to operate sensing element nodes. Rechargeable batteries, watch battery packs, solar cells, and smart systems are all examples of power sources.

2.6. Gateway Server

The gateway server was an important part of the overall system. It gathers and inhales Wi-Fi frames before converting them to Zigbee frames and forwarding them to the sink by substituting the relevant frames headers. The gateway server, on the other hand, receives Zigbee frames carrying IP packets. These are encased in a USB framework, which is subsequently removed at the Gateway server - side to fit into a Wi-Fi frame. The gateway server was also in charge of receiving IPv4 messages and converting them to IPv6, as well as the other way around. It also has other features, such as collecting sensor information from the WSN and sending it to the middleware. In the event that the connection between the gateway node and the software is lost, the host computer saves the data.

A Zigbee frame wraps an IPv6 packet, which is transmitted to the mote sink, which extracts the IPV6 packet, wraps it in a USB frame, and then passes it to the gateway, where the TCP data packet is retrieved. The sensory information is transmitted to the middleware once it arrives at the gateway. The sensory input is temporarily saved in a database if the connection is down (Fig. 3). The mobile client providing On/Off commands to the gateway is depicted in this data flow diagram. Once the connection is established, all stored data is transmitted to the middleware and the dataset is cleared.

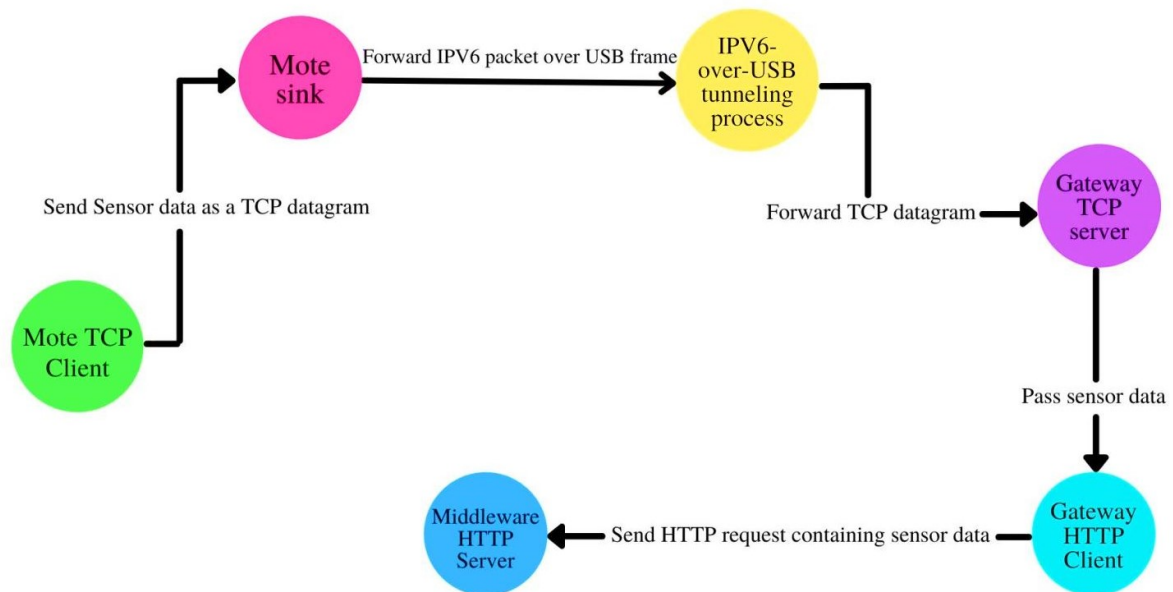


Fig. 4.The sending of sensory data is depicted in this data flow diagram.

2.7. Microcontroller

A sensor's CPU was typically made up of a microcontroller and flash storage. Connectors are included in most sensor nodes so that external units and sensors can be simply added to the

main unit. Making decisions and dealing with data collected are two instances of the CPU's critical functions. Until more data has been acquired, the CPU stores it in flash memory. Once the system has gathered enough data, the microcontroller part of the CPU places the data in envelopes, which are very efficient in data transfer. These packets are then delivered to the radio station for broadcast.

2.8.Sensor Transducer

The sensors are the most important component of a WSN. Environmental variables such as light, pollution, temperature, and sound, among others, are converted into electrical impulses via sensors. Multiple sensing methods have improved rapidly in the last two decades, making it easier for sensors to operate..

3. RESULTSANDDISCUSSIONS

Simulations were used to test the suggested cluster creation methodology. Furthermore, studies were carried out with varied numbers of nodes, starting with 100 nodes and testing up to 500 nodes. These nodes were spread out over a (100x100) m² space. Table 1 lists the model parameters that were employed in this study.

Table1 Parameters for Network Simulation

Parameters	Simulation Area	No. of Sensor Nodes	Initial energy of nodes	Eelec	ϵ_{fs}	ϵ_{mp}	Packet size
Values	100x100 m ²	100	2 J	50 nJ/bit	10 pJ/bit/m ²	0.0013pJ/bit/m ⁴	4096 bits

We tracked the system's ability to run reliably and provide an acceptable degree of efficiency in order to evaluate it. To assess the study's validity, two experiments were carried out.

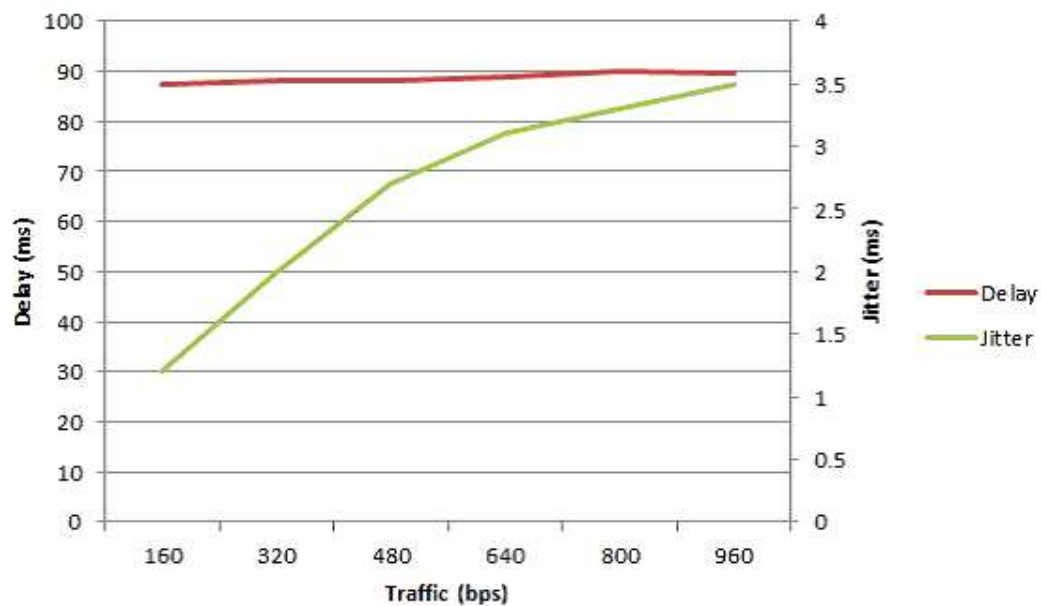


Fig. 5. Delay and Jitter variation with increasing traffic

The overall communication delay is caused by the Gateway Packet Transformation procedure. To put it another way, how much delay would the packet translation procedure add? The waiting time and jitter calculated over the time elapsed from packet sniffer in the Gateway Network Transition process to modification and transmission to the receiver are presented in the results. This was carried in 200 packets, each of which was sniffed and changed by the procedure. The elapsed time of the conversion system is determined in microseconds.

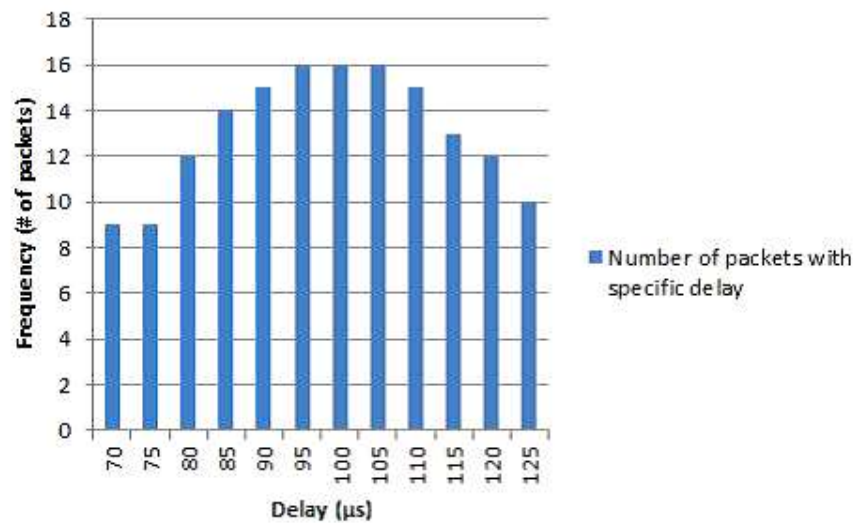


Fig. 6.Histogram of Delay Frequency

In addition, the variation of the delay rate is illustrated in the histogram portrayed in figure 6 based on the devices load. It is clear from this diagram that the latency is distributed normally. Furthermore, this experiment demonstrates that the Gateway Protocol Transformation procedure has a negligible impact on the overall delay..

3.1.Reliability:

The ability of a sensor node to sustain its network operations without disruption is referred to as reliability (or fault tolerance). Sensor node breakdown is a type of interruption that can happen due to a lack of energy, significant injury, or interference from the environment.

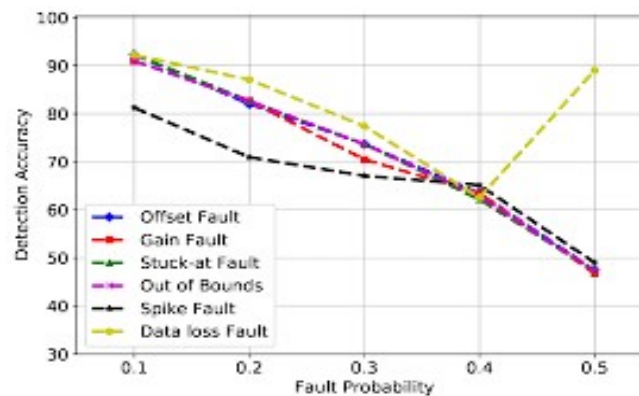


Figure 7 Reliability

3.2.Density and Network Dimension:

The user can deploy an unlimited number of sensor nodes to investigate a phenomenon under investigation. As a result, the density of these networks rises substantially, affecting the coverage area of study, as well as accuracy and reliability..

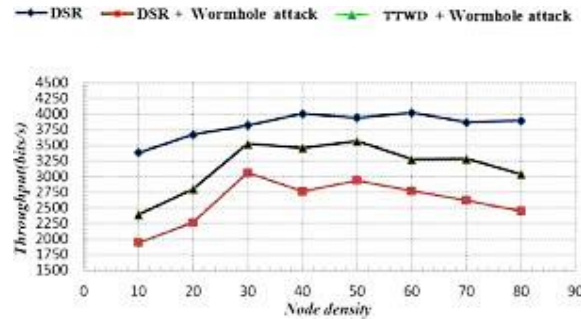


Figure 8 Density and Network Dimension

3.3. Topology of Sensor Network

Network topology has an impact on network speed, increasing network, and network resiliency. Moreover, network architecture influences the difficulty of data forwarding.

3.4. Energy Consumption:

Because sensor nodes are powered by batteries, their lifespan is likely to be influenced by battery life.

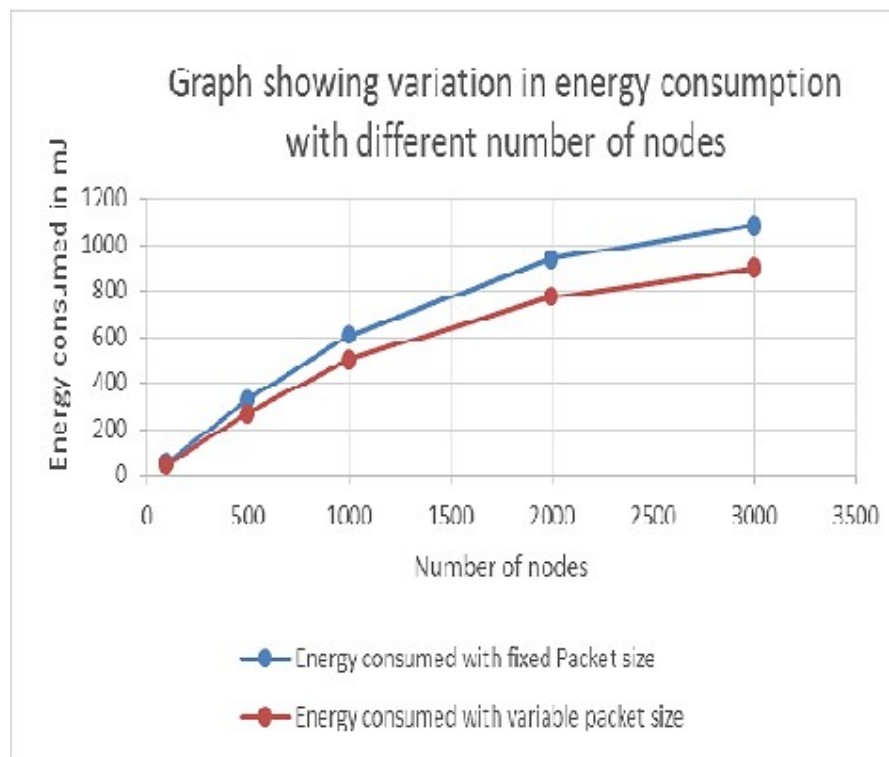


Figure 9 Energy consumption

4. Conclusion

We discussed the nuances of connecting wireless sensor networks with the Internet to regulate electrical items in this study. The architecture for installing a real-world testbed was defined. The given architecture is straightforward and adaptable to comparable deployments. We focused on essential issues, such as IPv4 to IPv6 gatewaying. We plan to continue researching the middleware subsystem in the future in order to support mobile wireless sensor motes and not limit distribution to specific specks. A few standards have previously been established in this area, such as IPv6, 6LoWPAN, and M2M. The incorporation of wsns into the Internet of Things is the topic of this article.

References:

1. Gardašević, Gordana, et al. "Emerging wireless sensor networks and Internet of Things technologies—Foundations of smart healthcare." *Sensors* 20.13 (2020): 3619.
2. Pundir, Sumit, et al. "Intrusion detection protocols in wireless sensor networks integrated to Internet of Things deployment: Survey and future challenges." *IEEE Access* 8 (2019): 3343-3363.
3. Reddy, Vandana, and P. Gayathri. "Integration of internet of things with wireless sensor network." *International Journal of Electrical and Computer Engineering* 9.1 (2019): 439.

4. Graessley, Scott, et al. "Industrial big data analytics for cognitive internet of things: wireless sensor networks, smart computing algorithms, and machine learning techniques." *Analysis and Metaphysics* 18 (2019): 23-29.
5. Misra, Sudip, et al. "MEGAN: multipurpose energy-efficient, adaptable, and low-cost wireless sensor node for the internet of things." *IEEE Systems Journal* 14.1 (2019): 144-151.
6. Martínez, William Ruíz, et al. "Application of the Internet of Things through a Network of Wireless Sensors in a Coffee Crop for Monitoring and Control its Environmental Variables." *TecnoLógicas* 22.46 (2019): 155-170.
7. Haseeb, Khalid, et al. "Intrusion prevention framework for secure routing in WSN-based mobile Internet of Things." *Ieee Access* 7 (2019): 185496-185505.
8. Al-Kashoash, Hayder AA, et al. "Congestion control in wireless sensor and 6LoWPAN networks: toward the Internet of Things." *Wireless Networks* 25.8 (2019): 4493-4522.
9. Rajput, Anagha, and VinothBabuKumaravelu. "Scalable and sustainable wireless sensor networks for agricultural application of Internet of things using fuzzy c-means algorithm." *Sustainable Computing: Informatics and Systems* 22 (2019): 62-74.
10. Alarifi, Abdulaziz, and AmrTolba. "Optimizing the network energy of cloud assisted internet of things by using the adaptive neural learning approach in wireless sensor networks." *Computers in Industry* 106 (2019): 133-141.
11. Lyu, Chen, et al. "Selective authentication based geographic opportunistic routing in wireless sensor networks for Internet of Things against DoS attacks." *IEEE Access* 7 (2019): 31068-31082.
12. Gulati, Kamal, et al. "A review paper on wireless sensor network techniques in Internet of Things (IoT)." *Materials Today: Proceedings* (2021).
13. Worlu, Chijioke, AzrulAmri Jamal, and Nor Aida Mahiddin. "Wireless sensor networks, internet of things, and their challenges." *International Journal of Innovative Technology and Exploring Engineering* 8.12S2 (2019): 556-566.
14. Majid, Mamoon, et al. "Applications of wireless sensor networks and internet of things frameworks in the industry revolution 4.0: A systematic literature review." *Sensors* 22.6 (2022): 2087.
15. Ali, A., and S. Alshmrany. "Health monitoring and management system by using wireless sensor network and Internet of Things (IoT)." *Int. J. Comput. Netw. Inf. Secur.* 19.12 (2019): 179-184.
16. Mahbub, Mobasshir. "A smart farming concept based on smart embedded electronics, internet of things and wireless sensor network." *Internet of Things* 9 (2020): 100161.
17. Feng, Xiang, Fang Yan, and Xiaoyu Liu. "Study of wireless communication technologies on Internet of Things for precision agriculture." *Wireless Personal Communications* 108.3 (2019): 1785-1802.