Wireless Sensor Networks Applications, Challenges, and Security Requirements

Ali Hadi Abdulwahid[1*], Muwaffaq Jameel Salih[2]
{dr.hajjiali@stu.edu.iq, muwaffaq.jameel@stu.edu.com[2]}

Southern Technical University/Engineering Technical College /Basra[1]
Southern Technical University/Faculty of Graduate studies/ Basra[2]

Abstract. Wireless sensor networks (WSNs) are a type of network that consists of connected sensor nodes that communicate wirelessly to gather data about the environment. WSNs have grown in popularity, but they have several major limits and security issues that must be carefully considered while building and implementing them. An overview of WSN and common communications standards are given in this paper, and as a result of the wide range of WSN applications, these applications are briefly discussed with focusing on Designing challenges and key security goals.

Keywords: Wireless, sensor node, network, mote, sink, ZigBee, LoRa.

1 Introduction

As a result of considerable advances in the fields of telecommunications, and computer technology, we currently have a new computing and networking architecture known as wireless sensor networks (WSNs). Traditionally, installing wired sensors in restricted appliance areas only yielded poor results. Meanwhile, compared to wired sensor nodes, the practice of adopting wireless technology created sensor nodes that formulated more viable solutions. Recently, there has been a measurable advantage associated with the considerable possibility of linking multiple devices and networks in an eloquent attempt to solve critical issues and challenges. The first wireless sensor network was a sound surveillance system created by the US navy in the 1950s to identify and monitor enemy submarines.[1]. Today, this servicing technology is used to detect undersea biodiversity and volcanic activity. With the rapid growth of the aforementioned WSN, this technology can now be easily applied around the world[2].

2 Overview on Wireless Sensor Networks

Small individual sensor nodes form up a wireless sensor network. When a node is linked to other nodes, this number will rise to hundreds of thousands of nodes, depending on the application scenario. Depending on the network deployment, every sensor node in a wireless sensor network observes its environment and transmits the collected data to a single or group of sink stations utilizing a wireless connection. Sensor nodes have three main functions: the first is to sense their surrounding environment, the second is to process the data that was initially detected, and the third is to communicate or interact with other sensor nodes or sink stations in the network. The most critical of the above specifications are sensing the environment. WSNs may be organized in a variety of ways, including centralized, distributed, and ad hoc. The general communication structure of a WSN is demonstrated in Fig 1 Sensor field, a sink node, and user or task management component are the main components. A sensor field is a collection of sensor nodes deployed in a certain area. Each sensor node in the sensor field can sense its phenomenon and send the data to the sink through a multi-hop link A sink is a type of sensor node that gathers data from the sensor field and either performs the necessary operations or simply transfers the data to the user or task monitor node. It also sends queries to the network's sensor nodes and retrieves the information required. Finally, each sensor node in

IMDC-IST 2021, September 07-09, Sakarya, Turkey

DOI 10.4108/eai.7-9-2021.2314823

the sensor field is assigned by the user or task manager node. Regardless, the sink node communicates with the user or task monitor node over the Internet or via satellite [1][2].

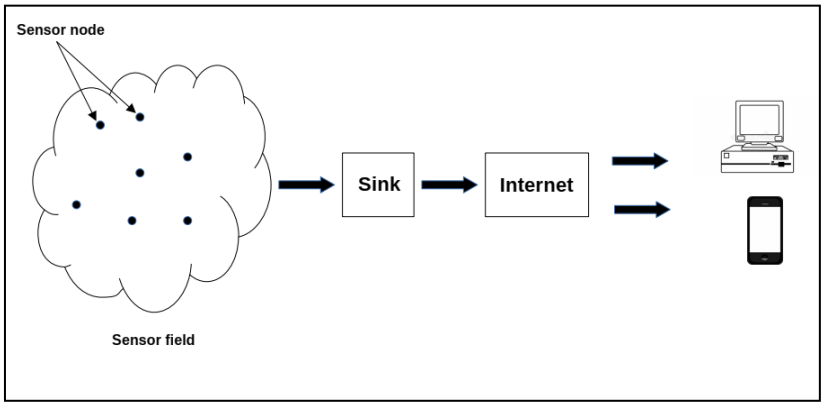

Fig.1. The communication architecture of wireless sensor network

3 Sensor Node Description

A sensor node can be defined as a small system with four main hardware components: sensing, processing, transceiver, and power generator. A global positioning system (GPS) and a mobilizer are both used by the sensor node for location purposes. Fig 2 depicts the basic architecture of a sensor node[3].

Sensing Unit: A sensing device collects information (such as temperature, pressure, light, and displacement) from its surroundings and produces an optical or electrical signal in response. The two fundamental components of a sensing network are a sensor and an analog to digital converter (ADC). One or more sensors generate analog signals in the sensor section, which are then converted to digital signals by the ADC and fed into a processing unit for supplementary operations. Sensor nodes are categorized as thermal, optical, acoustic, or mechanical sensors based on the phenomenon observed or gathered[3].

Processing Unit*:* A processing unit is made up of two components: storage and a processor. Sensed data is temporarily stored in a storage component that functions as nonvolatile memory for programming instructions. On occasion, it will also store processed data. The sensor node's processor enables it to collaborate with other network nodes to finish the task. The microcontroller of a sensor node conducts tasks, processes data, and manages the sensor node's other operations. Microcontrollers are used in sensor nodes because of their unique characteristics, such as low cost, ease of attachment to auxiliary apparatuses, ease of training, and squat power utilization. Because of their power-saving features, ATMEL, At super 128L, and MSP430 are the most widely used microcontrollers. The MSP 430 has six power modes, ranging from fully powered up to powered down. These kinds of power-saving techniques extend the system's lifetime and extend the sensor node's life[3].

Transceiver Unit: The transceiver connects the node to the rest of the network. It combines a transmitter and receiver into a single unit that operates on a particular radio frequency (RF). Modulation, filtering, multiplexing, band bass, and demodulation are all needed for the RF message, making it more complicated and costly. Sensor nodes depend on industrial science medical bands (ISM), which provide a free radio band with wide accessibility. Optical communication, infrared, and radio frequency are the three transmission systems available in wireless transmission. For starters, optical communication requires low power, sightlines, and

squatting in ambient conditions. Second, whereas infrared communication does not necessitate the use of antennae, it has a limited broadcasting range. Third, since it offers free bandwidth at 173, 433, 868, and 915 MHz and 2.4 GHz, radio frequency communications are the most appropriate medium best suited for wireless transmission. The IEEE 802.15.4 specification is used by the majority of sensor nodes to create low-rate wireless personal area networks. The transceiver is standard in that it has four operating modes: send, receive, idle, and sleep. The transceiver consumes the same amount of power in both receive and idle modes. When the transceiver is not actively running, it can go into sleep mode rather than being left in idle mode, as this wastes a lot of energy. It will simply transition from sleep to active broadcast or receive mode[3].

Power Unit: The sensor node is a small micro-electrical device that consumes very little power. The sensor node is kept alive by the power unit in a harsh and unforgiving world where changing batteries is costly and difficult. Sensor nodes primarily use energy for sensing, transmission, and data aggregation. The transmission of information uses the most energy of the aforementioned operations as compared to the others. The sensor node's lifespan, on the other hand, will be determined by the application scenario. Scientists monitoring the presence or age of ice (particularly in the form of glaciers) or ocean bed slides, for example, need sensors that can operate continuously. Finding the temperature in a specific area can take several hours or days when sensors are deployed on the battlefield. Previously, vanadium and molybdenum oxide were used to make the batteries for tiny sensor nodes. Since sensor nodes worked in a variety of locations, future energy exploration from the atmosphere is possible. Sensor node batteries should be as small as possible and as effective as possible. Electrochemical objects made of nickel-zinc, lithium-ion, and nickel-metal hydride are used as electrodes. Furthermore, since sensor nodes are typically installed in unconditional areas and must collaborate with other sensor nodes about their current location for data transmission, certain routing protocols and particular applications require the location of a sensor node, which is made possible by a location-finding device. A mobilizer is an optional part of a sensor node's definition that moves the sensor node from one location to another to complete the mission[3].

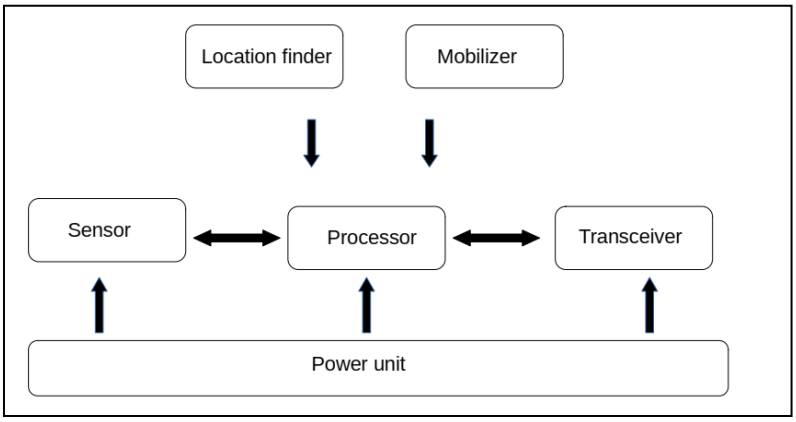

Fig.2. A sensor node's basic configuration

4 Applications of WSN

WSNs can be used for military, industrial, medical, and environmental monitoring, to name a few. Since these applications have different operational needs, they prefer to use different WSN architectures. High bandwidth, high security, and good coverage are the most critical criteria for military surveillance. WSN solutions that are stable, reliable, robust, and real-time

are required for industrial monitoring applications. In medical applications, security and network stability are generally valued, and environmental monitoring typically needs strong, energy-efficient, and independent sensor nodes[4]–[6]. Fig 3 shows some of the Wireless sensor network applications.

Environmental surveillance*:* The progress of humankind has had enormous environmental effects, and all efforts to promote environmental protection have been conducted with zeal. Environmental monitoring is an example of a large effort that allows for the monitoring of various physical characteristics to control or limit environmental pollution. Manual data collection was required in traditional environmental monitoring systems, which were eventually declared unsuccessful due to their need for human intervention and lack of early detection ability for pollution cases. Digital data loggers were introduced a few years ago to help improve the geographical and temporal quality of environmental monitoring, but they missed real-time data analyses. With the development of micro-electromechanical systems (MEMS), low-power WSN systems were introduced, and environmental surveillance could be done remotely as well as in real-time. Since then, this strategy has favored a proactive approach to environmental pollution. In the field of environmental monitoring, sensor nodes provide the following services [7], [8]:

A. Pollution Monitoring.
B. Forest Fire Detection.

Fig 4 shows a forest fire detection system by using WSN.

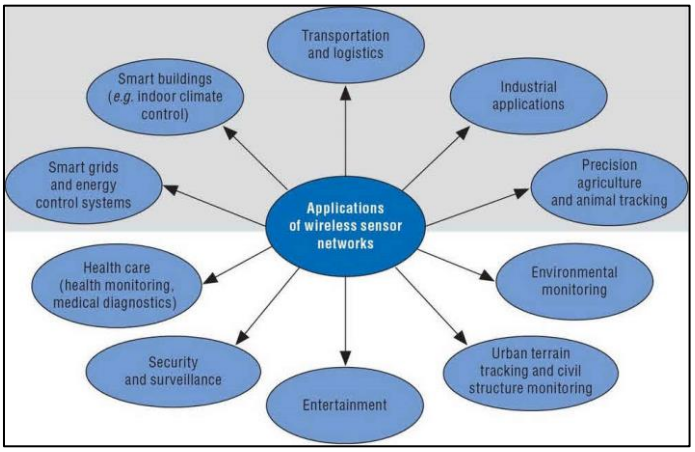

Fig.3. Wireless sensor network applications**.**

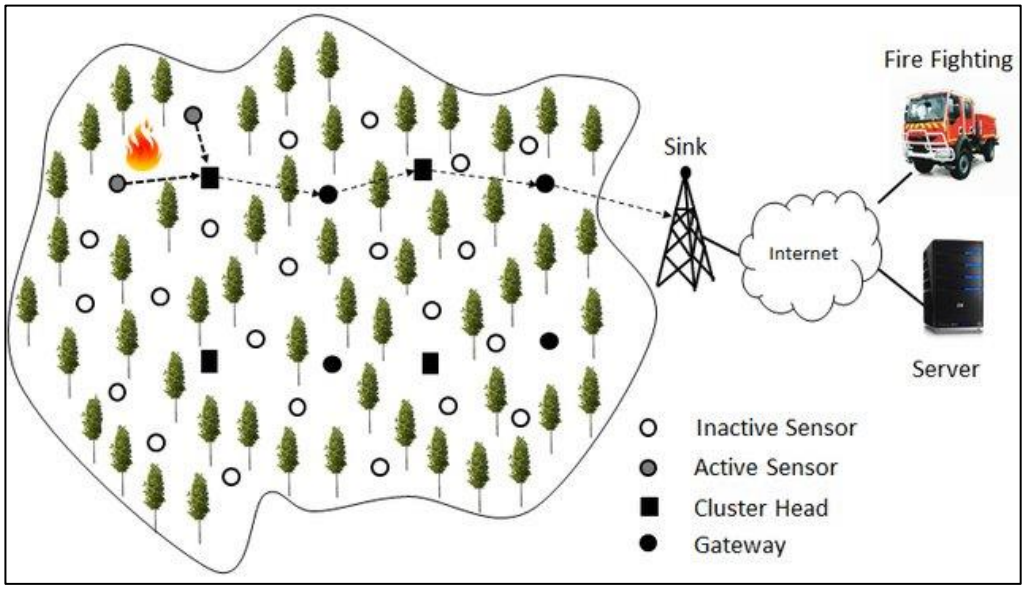

Fig.4. Wireless sensor Network applications in forest fire detection systems**.**

Military Applications: With the formation of The Defense Advanced Research Projects Agency (DARPA) and enemy monitoring, wireless sensor network development largely started with military applications. The destruction of specific sensor nodes by hostile activities has little consequence on or influence on military action because sensor nodes are extensively placed. As a result, sensor nodes are suitable for use on the battlefield. Identification of enemy forces, movement detection, analysis, and progress of their movement can all be accomplished using appropriate sensors in a particular network region. On the battlefield, sensor nodes have the following functions [9]:

A. Battlefield Surveillance.
B. Targeting.
C. Intrusion Detection.
D. Monitoring Forces.
E. Target Classification.
F. Battle Damage Evolution.

Industrial Monitoring: Wireless sensor networks are primarily used by industries to determine the degree of output quality in their operations as well as in cost-cutting procedures. Sensors are used to measure the water level in the tank and the temperature and pressure in refrigerators in nuclear power plants, for example. The monitoring of machine health is another important application of sensor networks. This application aims to find faulty equipment parts that need to be repaired or replaced. Inventory management is another major issue in large businesses. Larger industries' globalization makes it difficult to handle their equipment and goods, so these companies' management is accomplished by wireless sensor networks[10].

Agriculture Monitoring: In the agricultural research community, the use of wireless sensor networks is increasingly growing. Sensor nodes in agricultural production measure elements including temperature, wetness, moisture levels of soil, and sunlight, allowing stakeholders to take the necessary precautions to maximize harvest. In potato fields, the LOFAR-Agro project is used for crop monitoring. Wireless sensor networks are used to identify diseased potatoes in this experiment. The use of pesticides is reduced and limited to vulnerable areas by locating

those areas[10]. Fig 5 below demonstrate using Wireless sensor Network applications in Agriculture.

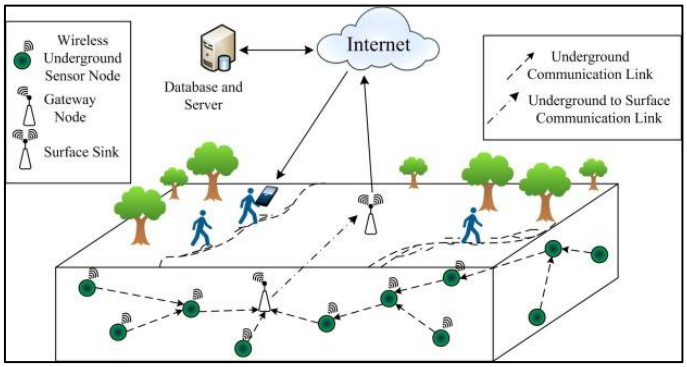

Fig.5. Wireless sensor Network applications in Agriculture**.**

Health Monitoring: Patients are fitted with collective sensors on specific points of their body in this application, which tracks patient measurements such as blood pressure, heart rate, and so on. Some of the applications that benefit from health monitoring include home-based wireless ECG monitoring systems that use Zigbee technology. Such techniques, in addition to occasional supervision by a general practitioner, can be useful for supervising patients in their homes. Electrocardiograms (ECG) are important for detecting abnormalities in heart disease. While clinical ECG equipment is useful for short-range inspection, it is impractical for home health care. Wireless ECG monitoring systems have recently been developed that are compliant with both Bluetooth and Zigbee protocols. A ZigBee device will support an unfailing multi-hop, self-organizing, and mesh network, which keeps the IEEE 802.15 plus ZigBee alliance's appliance software layers stable. ZigBee can provide low-energy networking and a low rate for equipment that requires a long battery life[10].

Smart Home: The use of certain integrated, specially built sensor nodes allows for remote control of home applications. Sensor nodes can be used in household appliances such as microwaves and washing machines, and they can be maintained without human intervention. In intelligent home projects, sensor nodes share resources such as water, heaters, and electricity.

Power Grids*:* Wireless sensor nodes used in power grid applications provide essential information about eclectic use, allowing them to operate more efficiently. Sensor nodes are used to control the entire surrounding environment by measuring and monitoring energy output and consumption. If any irregular positions are observed, the nodes will send diagnostic information to a central authority for resolution.

Automobiles: For a long time, sensor networks have been used to control and track vehicles. Video cameras that are mounted in a specific location to monitor traffic are a typical example. The videos are sent to a human operator, and small sensor nodes are used to track traffic as a low-cost alternative to video cameras. Sensor nodes capture images of traffic and send them to a human operator or automated controllers, as well as receiving control signals. Sensor nodes are placed in specific vehicles to track and control their movements.

5 WSN communication standards

WSNs often employ the Wireless Personal Area Network (WPAN) or Low Power Wide Area Network (LPWAN) standards to transport gathered data to the sink. These standards include IEEE 802.15.4, Sigfox, and low-power Bluetooth. There is no specific networking standard that is deemed perfect for all WSNs, and the standard that is adopted is based on the communication requirements and resource restrictions of a particular function. Table 1 shows some of the most important elements to think about when selecting a wireless communication solution[8]. The following are common communication standards for WSNs*:*

ZigBee: On the highest part of the IEEE 802.15.4 specification, ZigBee is a WPAN standard that covers the networking and device layers. With a maximum bandwidth of 250 kbps, ZigBee devices may transmit over several hundreds of meters and build mesh, a cluster tree, and star network architectures.[11], [12].

Bluetooth low energy (BLE): BLE is a low-energy edition of the Bluetooth protocol that can transmit data at up to 1 megabit per second over a distance of 30–80 meters. [11][12].

Long-range wide area network (LoRaWAN): LoRaWAN is a network protocol designed for applications that send limited quantities of data across great distances only a few times per 24 hours. Its low-power technology allows it to run for up to ten years without recharging[13].

SigFox: SigFox may be considered the first cellular network depend specialized to low-bandwidth Machine-to-Machine (M2M) and Internet-of-Things (IoT) applications. Its unique Ultra Limited Band (UNB) technology uses unlicensed frequency bands to transfer data over an extremely narrow spectrum. SigFox has a range of up to 40 kilometers in open space.[8].

Table 1. Considerations in the selection of a WSN connectivity standard.

Item	Description
Frequency	For low-cost deployment, WSNs frequently use unlicensed ISM frequency channels. Several of these bands are susceptible to channel blockage and interference of signals, making them unsuitable for mission-critical applications.
Range	Nodes are placed in remote locations in some WSN applications, necessitating connectivity technologies with long-range capability. good planning of network coverage needs is required when choosing the suitable solution.
Data Rate	The type and volume of data that will be delivered through a WSN will influence the connectivity mode used. In comparison to another type of data signal, multimedia signals necessitate high-speed data solutions.
Power	All WSNs have a finite amount of energy, but various applications need a various degree of autonomy, therefore the connectivity standard chosen should meet the related power needs.
Security	Different levels of protection are available in WSN connectivity specifications. Sensors that support mission-critical applications will have to take this into account.

6 Designing challenges for WSNs

The following are some design challenges for WSNs[2], [4], [14], [15]:

Fault Tolerance: Based on the application, the number of sensor nodes can reach thousands. A few sensor nodes can stop working or become blocked as a result of physical damage or environmental changes. The fault-tolerance problem's trustworthiness is determined by the failure nodes' ability to adjust the sensor network's entire task. Fault tolerance refers to the ability to extend the functionality of a sensor network, excluding any interruptions caused by sensor node failure. There are several fault tolerance and energy-efficient algorithms that can be used to extend the network's lifespan. As a result, losing one node has no impact on the network's results. Consider some sensor nodes installed in the office to monitor temperature and humidity; the toleration value must below.

Production Cost: Sensor network design aims to have the least expensive sensor nodes possible. WSNs have a large number of sensors to calculate or estimate network costs, but the outlay of each sensor node is more significant. We can purchase 10 Bluetooth devices for the price of one sensor node. Bluetooth devices are considered to be low-cost devices. Consider the sensor node in Fig 1, which includes additional units such as a sensing device, a processing unit, a position finding system, and a mobilizer, all of which add to the sensor node's cost. As a result, with all of the application criteria, the expense of the sensor node becomes a challenge.

Scalability: Sensor nodes may be monitoring thousands of operations at any given time. To complete the application, the number could reach tens of thousands. Adding more nodes to an established network does not affect the sensor network's continuous efficiency. The density of the nodes is calculated using how many nodes are in a specific region, with densities variable depending on the node function and where the sensor nodes are placed.

Network Topology*:* A sensor network's geographical configuration is known as network topology, and it must have a high-density value. *Pre-deployment*, *post-deployment*, and *re-deployment* are the three topologies that make up a wireless sensor network. Pre-deployment is the first step of sensor node deployment, which is accomplished by throwing or positioning each sensor node in the network field one after the other. This deployment method involves manually or mechanically placing nodes one by one (released from plane, rocket, missile, etc.). Even though these sensor nodes are distributed according to engineering measurements, the schemes used for initial deployment nodes in the network are inserted in the factory. Using the above methods comes at a high price tag: encouraging self-organization and avoiding fault tolerance, eliminating the need for any pre-deployment, and re-planning generally lowers the initialization cost. Post-deployment occurs after the initial deployment of sensor node topology, which can change due to substantial operations on the sensor network, such as jamming or sensor nodes moving from one location to another to complete the assigned task, resulting in changes in vacant energy, reachability, task specifics, and malfunctioning. Due to energy shortages or other causes, device failure is typical in any network design. As a result, the geometrical and spatial relationships of sensor networks are horizontal to the implementation challenges. If certain sensor nodes fail to function properly due to changes in the environment, re-deployment is used. As a result, certain auxiliary sensor nodes can be re-deployed in place of shattered nodes at any time, as well as necessary adjustments in assignment dynamics. The addition of new nodes could necessitate network reorganization.

Data Delivery Mode: Reactive, proactive, hybrid, query-driven, and event-driven data is the most typical type of wireless sensor network data; however, in the application of wireless sensor networks, only one data delivery model is required.

Global Identification: The setup of wireless sensor networks has many sensor nodes, yet this does not prevent global identification. A GPS provides location data to adjacent sensor nodes, but it relies on line-of-sight from many satellites. However, sensors installed within a building, underwater, or beneath deep foliage, or those jammed by eavesdroppers, make this impossible in some cases.

Storage and Retrieval: Sensor networks investigate environmental changes and generate a significant volume of raw data in a continuous time series. Traditional database management is not suitable for wireless sensor networks, even though data is continuous. In wireless sensor nodes, three forms of memory are used: flash memory, fuse bits, and electrically erasable programmable read-only memory (EEPROM).

Area Coverage*:* WSNs are made up of a few sensor nodes. With a few homogenous sensor nodes, area coverage tends to expand across the entire region. WSNs are traditionally made up of two processes: (1) area coverage and (2) computational complexity. The first is after discreetly organizing into pre-defined sections. Sensor nodes keep track of environmental data indefinitely. Furthermore, even though this type of sensor consumes a lot of energy, sensed substances are transferred to a base station via a communication component, either directly or through additional nodes.

In-Network Processing: In wired and wireless networks, transport protocols are used to ensure that data transmitted from senders to receivers is not modified by intermediary nodes until it reaches its destination or receiver. To eliminate information redundancy, wireless sensor network data can be changed or aggregated by intermediate nodes.

Latency: The time required for a packet to pass from the sender to the receiver and be correctly received is known as latency. Because the environment changes so quickly, sensor data is only valid for a limited time. As a result, receiving sensed data in a timely and latency-free way is critical.

Network Lifespan: Because the sensor node is a small electrical device with limited resources and energy, the network's lifespan is limited. When all of the nodes in a network are inactive, it is said to be effective. When networking is running well, it can monitor the entire region and gather data utilizing a variety of superior services. Appropriate practices aim to limit energy usage and increase the life of the network.

6 Basic Security Requirements

The goal of security in a sensor network is to safeguard specific sensor nodes as well as the entire network from malicious attacks from both within and outside the network. The most important security needs for protecting a network's integrity are listed below[16]:

Data confidentiality: This is usually the most important purpose, and it concentrates on preventing unauthorized individuals from accessing the sensor through activities like eavesdropping. This is especially critical for applications like WBANs that use several sensor streams. Correlating data streams allows attackers to deduce information about an individual. The most popular method for protecting data is to encrypt it with ciphers.

Data integrity*:* The focus is on ensuring that the data received has not been tampered with in any way throughout the transmission process, whether deliberately or accidentally.

Authentication: Authentication helps the sensor node to confirm the identity of the sensor node it is communicating with. Authentication can be done in many ways, including the interchange of authentication keys or the use of digital signatures. These tactics can be used by a party to validate its identity. They also protect against impersonation and forgeries.

Non-repudiation: The principle of non-repudiation ensures that a sensor node cannot reject sending a message it has already sent.

Authorization: Due to authorization, only permitted nodes will reach network services or certain destinations.

Freshness: The freshness of sensor data messages is examined to ensure that they are fresh, sorted, and unduplicated. This prevents an attack from replaying previous messages from a security point of view. Freshness is commonly implemented by using sequence numbers and timestamps in the data sent by the sensor.

7 Conclusion

Many applications can benefit from the use of wireless sensor networks. Their main advantage is their low cost and flexibility to take measurements remotely and in real-time. These networks, however, face resource constraints in terms of fault tolerance, production cost, scalability, and area coverage, among other issues. These restrictions, if not addressed appropriately, might reduce the efficacy and efficiency of using WSN applications.

References

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey," *Comput. networks*, vol. 38, no. 4, pp. 393–422, 2002.

[2] S. K. Gupta and P. Sinha, "Overview of wireless sensor network: a survey," *Telos*, vol. 3, no. 15µW, p. 38mW, 2014.

[3] H. T. T. Binh and N. Dey, *Soft computing in wireless sensor networks*. CRC Press, 2018.

[4] M. Bhende, S. J. Wagh, and A. Utpat, "A quick survey on wireless sensor networks," in *2014 fourth international conference on communication systems and network technologies*, 2014, pp. 160–167.

[5] C. Buratti, A. Conti, D. Dardari, and R. Verdone, "An overview on wireless sensor networks technology and evolution," *Sensors*, vol. 9, no. 9, pp. 6869–6896, 2009.

[6] G. Zhao, "Wireless Sensor Networks for Industrial Process Monitoring and Control: A Survey.," *Netw. Protoc. Algorithms*, vol. 3, no. 1, pp. 46–63, 2011.

[7] L. M. L. Oliveira and J. J. P. C. Rodrigues, "Wireless sensor networks: A survey on environmental monitoring," *J. Commun.*, vol. 6, no. 2, pp. 143–151, 2011, doi: 10.4304/jcm.6.2.143-151.

[8] M. Pule, A. Yahya, and J. Chuma, "Wireless sensor networks: A survey on monitoring water quality," *J. Appl. Res. Technol.*, vol. 15, no. 6, pp. 562–570, 2017.

[9] B. Shahi, S. Dahal, A. Mishra, S. B. V. Kumar, and C. P. Kumar, "A review over genetic algorithm and application of wireless network systems," *Procedia Comput. Sci.*, vol. 78, pp. 431–438, 2016.

[10] H. T. T. Binh, N. T. Hanh, and N. Dey, "Improved cuckoo search and chaotic flower pollination optimization algorithm for maximizing area coverage in wireless sensor networks," *Neural Comput. Appl.*, vol. 30, no. 7, pp. 2305–2317, 2018.

[11] V. C. Gungor and G. P. Hancke, "Industrial wireless sensor networks: Challenges, design principles, and technical approaches," *IEEE Trans. Ind. Electron.*, vol. 56, no. 10, pp. 4258–4265, 2009.

[12] J.-S. Lee, Y.-W. Su, and C.-C. Shen, "A comparative study of wireless protocols: Bluetooth, UWB, ZigBee, and Wi-Fi," in *IECON 2007-33rd Annual Conference of the IEEE Industrial Electronics Society*, 2007, pp. 46–51.

[13] A. Augustin, J. Yi, T. Clausen, and W. M. Townsley, "A study of LoRa: Long range & low power networks for the internet of things," *Sensors*, vol. 16, no. 9, p. 1466, 2016.

[14] P. Papageorgiou, “Literature survey on wireless sensor networks.” Citeseer, 2003.
[15] R. Soua and P. Minet, “A survey on energy efficient techniques in wireless sensor networks,” in *2011 4th Joint IFIP Wireless and Mobile Networking Conference (WMNC 2011)*, 2011, pp. 1–9.
[16] M. J. McGrath, C. Ni Scanaill, and D. Nafus, *Sensor technologies: healthcare, wellness, and environmental applications*. Springer Nature, 2013.