Wireless sensor networks protocols, applications, and network-on-chip communications

Ompal[1,2], Niraj Kumar[2], Vishnu Mohan Mishra[3], Adesh Kumar[4]
[1]Department of Electronics and Communication Engineering, Veer Madho Singh Bhandari, Uttarakhand Technical University, Dehradun, India
[2]Department of Electronics and Communication Engineering, Chhatrapati Shahu Ji Maharaj University, Kanpur, India
[3]Department of Electrical Engineering, Govind Ballabh Pant Institute of Engineering and Technology, Ghurdauri, Pauri Garhwal, Uttarakhand, India
[4]Department of Electrical and Electronics Engineering, School of Advanced Engineering, UPES, Dehradun, India

Article Info

Article history:

Received Mar 6, 2024
Revised Jun 29, 2024
Accepted Jul 7, 2024

Keywords:

Communication protocols
Network-on-chip
Performance parameters
Wireless communication
Wireless sensor network

ABSTRACT

A wireless sensor network (WSN) is a network consisting of self-governing sensors that are deployed in space and communicate with each other using wireless technology to monitor physical or environmental variables. These networks generally include compact, inexpensive sensor nodes equipped with sensing, processing, and communication functionalities. WSNs are specifically engineered to gather data from their immediate environment, do local data processing, and subsequently communicate pertinent information either to a central hub or to other interconnected nodes within the network. Continuous research in the domain of WSNs is devoted to advancing security concerns, developing novel sensing technologies, and optimizing communication protocols. The advancements in these domains enhance the ongoing development and efficiency of WSNs. The WSNs are very important for getting information from the real world in many situations. WSNs are flexible tools for keeping an eye on and controlling different environments because they have sensor nodes, wireless communication, and distributed processing. WSNs use network-on-chip (NoC) communication architecture to connect sensor nodes. The article explains the introduction to WSN, the background of wireless communication, motivation, ZigBee protocol, and WSN applications.

Corresponding Author:

Adesh Kumar
Department of Electrical and Electronics Engineering, UPES
Dehradun, India
Email: adeshmanav@gmail.com

1. INTRODUCTION

The latest developments in microelectromechanical systems, processor technologies, and low-power radio communication technologies have produced low-power, low-cost, multi-functional small sensor devices that can track alterations in the physical spectacles of their surroundings and respond accordingly [1]. These sensing capabilities of such devices can be combined to produce an overall result when connected via wireless media. An array of radio transceivers or transducers are features of wireless sensors that enable them to gather data about their environment. These sensors can spontaneously establish themselves into an ad-hoc multi-hop system to interact with one another and one or additional sink nodes when placed in a sensor field in large numbers. With the help of the sink, a remote operator can send instructions to the sensor-based communication network, giving the sensors the responsibility for data processing, collection, and transmission [2]. The user can also subsequently utilize the sink to access the network-based sensed data.

The sensors connect the physical and digital worlds by catching and disclosing phenomena that occur in the actual world and converting them into a format that can be managed, saved, and used for information [3]. Sensors are widely used in machines, settings, and gadgets, and have a significant positive social impact. They can reduce the likelihood of disastrous infrastructure failures, protect priceless natural possessions, boost throughput, improve safety, and make possible innovative requests like context-responsive systems and smart home automation technologies. The spectacular advancements in technologies like wireless communications, microelectromechanical systems (MEMS), and very large-scale integration (VLSI) have all contributed to the extensive adoption of disseminated sensor communication environments. For instance, the remarkable advancements in semiconductor technologies endure in producing microprocessors with smaller forms and higher processing rates [4]. Small, low-cost, and low-power sensors, actuators, and controllers may now be created because of the shrinking of computing and sensing technology. Additionally, embedded computer systems are often interfaced directly with the real-time world and are created to only accomplish a small set of specific operations that remain to find use in an expanding variety of fields. There is a growing emphasis on systems to monitor and safeguard pipeline infrastructure, the national power grid, and civil structures like tunnels, bridges roads even if defense and aerospace systems continue to dominate the market [5]. Multiple sensor nodes are already governed in networks to monitor the larger geographic location for exhibiting, forecasting, and modeling environment behavior and parameters in flooding, and pollution, gathering operational health care data, monitoring the bridges using vibration sensors, and handling pesticide, water, and fertilize amount to advance the crop quantity and health [6]. The growing number of sensors transmit the acquired data wirelessly to a centralized dispensation station, even while many sensors physically connect to controllers and other handling stations in the local area network (LAN). This is crucial since many complicated requests require thousands and hundreds of sensor nodes, many of which are placed in difficult-to-reach locations and remote locations. Consequently, a wireless sensor also includes a sensing module, data processing, communication, and parameter storage capabilities. With these developments, a sensor node is now frequently responsible for not just collecting data objectively but also for correlating, analyzing networks, and fusing data from both its sensors and those of other sensor nodes. A WSN is generated when several sensor nodes cooperate to cooperatively monitor a sizable physical environment [7].

The sensor nodes interact not only with one another but also with the base station (BS), enabling with the help of their wireless communication radios to transmit their sensor data to distant handling, analysis, visualization, and storage systems. Figure 1 depicts the data processing in WSN two sensor nodes used to monitor two different geographical areas and use their BS to access the Internet. The abilities of the sensor nodes in specific WSNs might vary greatly. For instance, simple sensor nodes might be used to track a single bodily event, whereas more complex devices could incorporate a variety of sensing modalities such as acoustic, optical, and magnetic. Additionally, they may have different ways of communicating, such as using ultrasonic, infrared, or radio frequency technologies, all of which have different data rates and latencies. Additional controlling devices, which are used with substantial data processing, storage capacity, and energy, may be used to conduct complex handling and aggregation functions, whereas simple sensors may merely gather and send statistics about their sensing environment. Such devices frequently take on extra roles in a WSN, such as forming communication backbones that other sensor devices with limited resources can utilize to connect to the base station. In addition, this is crucial, some devices may be connected to additional supporting technologies, including global positioning system (GPS) receivers, allowing them to pinpoint their location. Additionally, these systems usually consume too much energy to be useful for cheap, low-power sensor nodes [8].

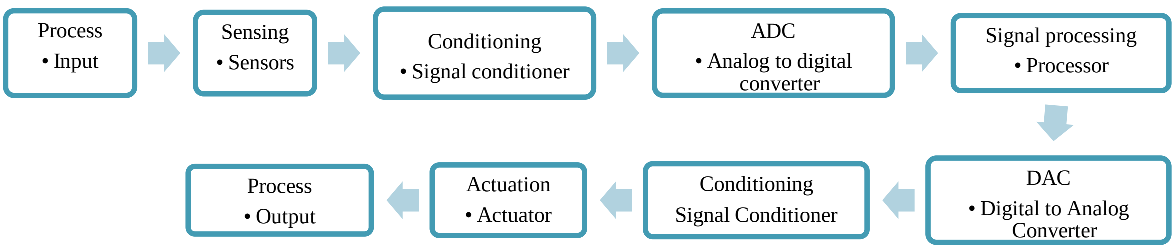

Figure 1. Data processing in WSN [9]

Simple point elements or multipoint detection arrays can be used as sensors. For the abstraction and preprocessing operation of physical surroundings data, nodes are often outfitted with one or additional application-specific sensors and on-node signal communication competencies. Embedded network sensing refers to the cooperative integration of micro-sensors in surroundings or structures; embedded sensing provides intensive monitoring of the system under study in both space and time (e.g., an environment, a building, or a battlefield). It may be that many sensors involve only a small amount of energy from the battery or line feed farther down the power consumption chain. Sensors can also be passive or self-powered. Some sensors might require extremely high-power feeds at the top of the power-consumption chain (e.g., for radars). Sensors make instrumenting and regulating buildings, cars, homes, offices, cities, and the environment easier, particularly as commercial off-the-shelf machinery develops more readily accessible [10]. Aircraft, ships, and buildings can self-detect physical defects utilizing particularly, embedded networked sensing based on sensor communication technology such as fatigue-induced cracks. Detecting airborne contaminants like poisons and tracking their source, if any, can be done in public gathering places. This is also possible in ground and underground conditions. Building sensors that are designed for earthquakes can help assess structural damage and locate potential survivors; tsunami-alerting sensors are helpful for countries with long coasts. In-depth applications of sensors for reconnaissance and surveillance are also found on the battlefield.

A sensor is a device that is used to capture data for the physical process and convert it into electrical signals that can be used to measure, process, assess, and record. Any real-world data, including those related to pressure, force, temperature, sound, light, motion, flow, position, radiation, and humidity could be a part of a physical process. A sensor-based system is a network made up of computing equipment, sensors, and communication apparatuses that can be used to monitor, record, and react to events and phenomena. Events may resemble the real-time communication and physical world, manufacturing setting, or a genetic system, while the body in charge of controlling or keeping watch may be a customer application, civil government agency, military force, or an industrial organization. These sensor-based communication networks can be applied for telemetry in medicine, remote sensing, data gathering, monitoring, and other purposes. Sensors, a controller, and a communication system make up a typical sensor network. When a wireless protocol is used to implement the communication system in a sensor network, the networks are referred to as WSNs [11]. The factors stated thus far can be considered when designing WSN nodes. Using a dynamic definition of the most cost-effective operating circumstances, a dynamic power management (DPM) method tries to reduce the system’s power consumption once the design time parameters have been fixed.

2. MOTIVATION

The motivation for the recent developments in the new domain relating to sensor design, communication-based information technology (IT), and wireless methods inventions are the consequence of current communication, engineering, and system-level networking developments. A bridge between the real and digital worlds can be built using such sophisticated sensors. Sensors are active in an extensive diversity of products, industries, and equipment to aid in avoiding setup failures, accidents, the conservation of wildlife and expected resources, the augmentation of production and the provision of security. The implementation of distributed sensor networks is a result of technological developments in VLSI, MEMS, and wireless communication. Modern semiconductor technology has made it possible to create powerful microprocessors that are more compact than those found in previous-generation goods. Due to the shrinking of computing, processing, and sensing technologies, low-cost sensors, small controllers, and actuators are now available. It is possible to separate a typical wireless sensor network into two components as follows: a sensor node in WSN is made up of four fundamental parts: processing unit, sensor, power supply, and communication system. An ADC converts the analog data that the sensor acquires from the outdoor environment into digital data. A microprocessor or a microcontroller serves as the primary processing unit that computes and processes data intelligently. All these components are based on low-power consumption and electronics. For example, a small battery is applied to power the complete system. The electronic transmission system comprises a radio receiver and a small-range radio communication system for data communication and reception. In addition to the sensing element, a sensor node also includes processing, communication, and storage components. A sensor node is in charge of gathering data from the physical world, analyzing networks, correlating data, and fusing that data with data from other sensors to all these characteristics, components, and improvements. Industrial automation and home automation have both made extensive use of ZigBee [12]. Figure 2 shows the diagram of ZigBee for communication and industrial automation-related applications. Proportional-integral-derivative (PID) and programmable logic controller (PLC)-based feedback [13], feedforward, and cascade control mechanisms are the foundation of industrial automation [14]. These controls are used to regulate various sensing devices, such as level sensors, pressure sensors, and temperature sensors. Sensor devices can also control these parameters thanks to a variety of actuators, servomotors, and valves. The full information is gathered for the supervisory control and data acquisition (SCADA) system deployment [15] during the monitoring at the human machine interface (HMI) level in the central room. Such automation requires a more complicated wired communication system. One wireless technology that can operate in such a setting is ZigBee. Two major factors that greatly impact the functioning of a wireless sensor network are the minimization of energy consumption and the assurance of safety. Additional security precautions are necessary for wireless sensor networks, such as encryption and key management.

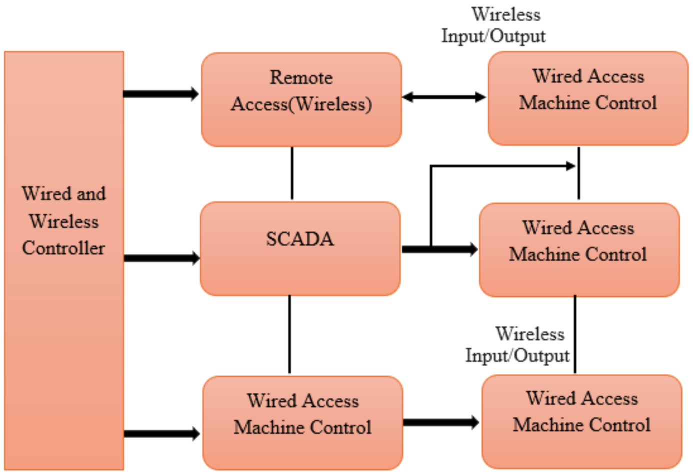

Figure 2. ZigBee for communication and industrial automation

3. METHOD

The wireless LAN connects multiple devices to utilize an access point to the larger internet and wireless distribution technology like spread-spectrum radio or orthogonal frequency division multiplexing (OFDM). Users now have the freedom to move within a limited-service area while outstanding associated with the communication network. Wi-Fi communication is used to identify most contemporary wireless LANs, which follow the IEEE 802.11 standards. Wi-Fi LANs have grown in popularity in households and commercial complexes that offer their clients wireless access often for free due to their ease of installation. Extensive wireless network deployments are being developed in several of the most important cities. A representation of successful Wi-Fi transmission with Ethernet, a Wi-Fi dish, a Wi-Fi router, and an internet service provider. Commonly adopting various radio frequency (RF) methods, widely used wireless communication devices typically operate in frequency ranges that are shared by numerous users. Bluetooth, Wi-Fi, and newer ZigBee are specific technology examples used for communication. All three of them work in the unrestricted working in 2.4 GHz band, also referred to as the ISM band, which has proved essential to the growth of a vibrant and cutting-edge industry for embedded wireless communication devices. However, the peaceful coexistence of various technologies is essential for each user of these bands to achieve its communication goals, just as it is with any shared resource. Communication technologies that transmit, for occurrence, at extremely different energy intensities may inhibit one another, despite efforts by standards bodies to assure peaceful coexistence. It has been explicitly observed that Wi-Fi traffic may theoretically interfere with ZigBee if both protocols interact on the matching channel, but Wi-Fi broadcasts frequently ensue at significantly advanced energy levels.

3.1. Peer to peer

Ad-hoc networks, often known as Wi-Fi direct networks, are ones where stations only speak to one another (P2P). No one grants permission to speak, and there is no basis. This works well when using the self-governing simple provision set. All other devices in the P2P Wi-Fi group are clients, while the cluster possessor [16] serves as the access point. The Wi-Fi direct group can have a group owner by using one of two major procedures. One method involves manually setting up a P2P cluster possessor. The name of this technique is independent cluster possessor. Two devices compete in the additional technique, also known as negotiation-based cluster conception, according to the cluster owner concentrating assessment. The group owner of the group is the device with the greater intent value, and the client is the second device. The outstanding battery life, whether it was previously a cluster possessor in the alternative collection, and/or the first wireless device's anticipated signal strength can all affect the group owner intent value if the wireless device establishes a cross-connection between a setup wireless LAN facility and a P2P cluster [17]. Wireless devices can communicate with one another directly through a peer-to-peer (P2P) network. Without using central access points, wireless devices that are close to one another can find and speak with one another directly. Usually, two computers will employ this technique to join forces to create a system. If the signal power meter is applicable in this scenario, it may not reliably deliver the intensity and may even be deceptive because it measures the intensity of the robust signal, which might be the definite signal from the nearest computer. Carrier sense multiple access/collision avoidance (CSMA/CA) is the foundation upon which IEEE 802.11 outlines the physical (PHY) layer and medium access control (MAC) layers. The 802.11 protocol incorporates measures intended to reduce collisions since two portable devices may be within range of the same admission point but not within reach of one another. Ad-hoc mode and infrastructure mode are the two fundamental modes of the 802.11 protocol. Mobile devices broadcast straight P2P when in an ad-hoc manner. When operating in infrastructure mode, mobile devices connect to wire network infrastructure via a contact point that acts as a channel for communication. The 802.11 communication researchers additionally added encryption methods based on shared-key mechanisms: Wi-Fi protected access (WPA), and wired equivalent privacy (WEP), to safeguard wireless processor systems because wireless communication uses a more open standard for transmission than wired LANs. Figure 3 presents an example of peer-to-peer topology.

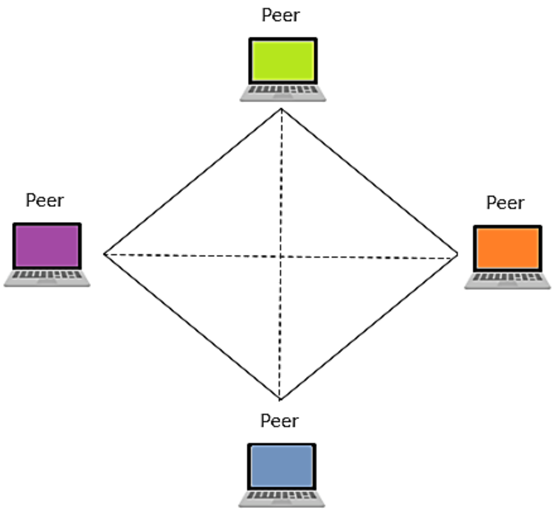

Figure 3. Peer-to-peer topology

3.2. Bridge

The bridge associates the different networks, usually of various sorts. The devices on a wired Ethernet communication system can join a wireless setup using a wireless Ethernet embedded bridge. The bridge assists as a wireless LAN accessing point. Figure 4 presents the bridge network used to communicate between two hub networks. A bridge receives every frame or packet from LAN segments. To determine which LAN or segment a packet is coming from and going to the bridge, create a table of addresses. All data chunks and packets from LAN are directed to computers on LAN that are delivered by the bridge, which then discards them all. Conversely, packets from one LAN are sent to a computer on another LAN that is read by the bridge and then retransmitted to the LAN. Bridges are used to divide large, demanding networks into several smaller, consistent networks to increase implementation. Bridges also allow the physical scope of a system to expand. Additionally, bridges are used to establish a disconnected relationship between two LAN segments using a synchronous modem component. WSN platforms have the feasibility that sensors are positioned in a number of different locations throughout the bridge in a typical wireless sensor network platform, which is used for the switching of bridges. In order to gather information about their surroundings, the sensors that have been deployed and are dispersed throughout the structure conduct data collection.

3.3. Distribution

The wireless linking of contact sockets in an IEEE 802.11 system is made possible by a wireless distribution system. Instead of a cable backbone connecting them, as is typically necessary, it enables a wireless communication system to be extended by utilizing many contact points. The MAC addresses of client packets are preserved by wireless distribution system (WDS) over other solutions across links between access points, which is a significant advantage. A contact point may be a foremost, relay, or distant base location. If WPA and WEP keys are fully employed, all base places in the wireless dissemination network should be aligned to use the identical radio channel or to be shared with them. The scheme could be set up with various service set identifiers. The individual base station must be set up to advance to other stations in the network for WDS to function. WDS is also frequently stated as a repeater approach since it performs bridge and receives wireless consumers simultaneously unlike the customary association of nodes. Moreover, the throughput in this technique is halved for all wirelessly associated users [18]. Figure 5 depicts the case of distributed topology when connecting a network's access points proving difficult repeaters can also be installed as access points. The following are some features and considerations that are associated with the implementation of a NoC for WSN.

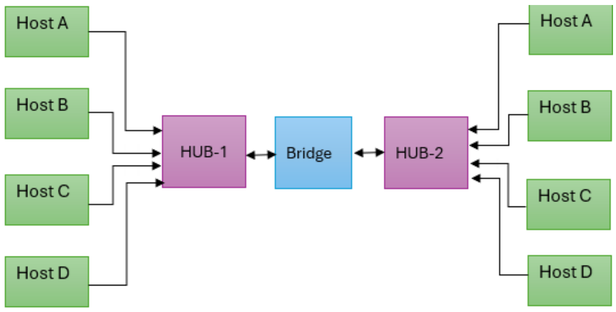

Figure 4. Bridge network

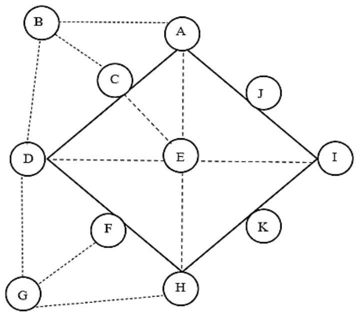

Figure 5. Example of distributed topology [19]

- Energy efficiency: Energy efficiency is important for WSN sensor nodes, which are generally battery powered. Communication energy usage should be minimized via the NoC. The use of energy-efficient routing algorithms and protocols is required to connect nodes without wasting energy.
- Topology: The configuration of NoC is of utmost importance. Various topologies, such as mesh, tree, or cluster-based topologies, may be appropriate depending on the specific application and deployment environment. The topology should be engineered to maximize communication efficiency [20] and minimize total energy usage.
- Scalability: WSNs can exhibit significant variations in terms of their physical dimensions. The NoC should possess the ability to scale and handle varying quantities of sensor nodes without experiencing notable declines in performance. Scalability considerations encompass routing algorithms that can adjust to variations in network size and effective techniques for addressing and managing nodes [21].
- Real-time communication: Certain applications of WSN necessitate instantaneous communication, as seen in industrial automation or healthcare monitoring. The NoC should be capable of accommodating the demands of real-time communication. It is required to create communication protocols that can ensure predictable and consistent performance in terms of both speed and dependability for applications that require precise timing [22].
- Reliability: Sensor nodes are susceptible to failures or may have limited capabilities. The NoC should be engineered to effectively manage node failures and guarantee dependable connectivity. To improve the reliability of the communication infrastructure, it is possible to include redundancy and fault-tolerant technologies.
- Quality of service (QoS): Communication requirements for distinct sensor nodes may differ depending on the application. The capability of the NoC to deliver varying levels of QoS should be contingent upon the requirements of the nodes.
- Security: The deployment of WSNs in sensitive environments raises substantial security concerns incorporating authentication and encryption mechanisms to safeguard communications. Additionally, intrusion detection mechanisms and secure routing protocols may be incorporated into the design of the NoC [23].
- Resource management: WSNs rely heavily on effective resource administration. To maximize the utilization of resources, the NoC ought to contemplate mechanisms that govern power management, data aggregation, and dynamic resource allocation.
- Cross-layer optimization: The design of communication protocols may be influenced by cross-layer optimization strategies, which consider interactions across multiple protocol stack layers. As a result, WSN solutions may become more streamlined and individualized.

4. STANDARD ZIGBEE PROTOCOL

IEEE 802.15.4 standard includes the MAC and PHY layers and are the foundation for the ZigBee network layer stack. The RF and communication components used for interfacing with other devices are found in the MAC and PHY layers. An application support sub-layer, a networking layer, and a security service provider (SSP) make up the ZigBee stack [24]. ZigBee and IEEE 802.15.4 each have their pros and disadvantages. Low data rates or smaller bandwidths are both technologies' principal drawbacks. Therefore, only applications requiring modest data transmission rates can use these protocols. The system's power use, price, and complexity all rise when the data rate is increased. Power usage must be kept to a minimum because sensor nodes are spread out in the field. The favored method is typically battery powered. In addition, a large bandwidth is not necessary for sensor data. Figure 6 indicates that for a small sensor network, ZigBee is the best protocol. The three primary network topologies utilized in ZigBee wireless networking are the star, point-to-point, and mesh networks [25]. These topologies can be applied in various contexts and settings. Most often, a single communication line is replaced by a point-to-point system. A point-to-point network can work successfully when its two endpoints are close to one another. A wireless point-to-multipoint system is another name for star topology. IEEE 802.11 or Bluetooth is the system's primary foundation. There is just one primary base station in the system, and it regulates connectivity with all other end nodes. The caliber of the RF link between each end node and the base station determines how reliable this network is. The main issue with this system is that it can be challenging to locate a base station that is suited for industrial applications and can interact with each end node. Peer-to-peer networks are another name for mesh topology.

An ad hoc multi-hop system is what this one is. Each node in a ZigBee-based mesh network can send and receive data [26]. Data will thus safely get to its intended location via intermediate nodes, and reliably reach its destination. The network has numerous redundant communication channels. The mesh network has three crucial characteristics: self-configuration, self-healing, and scalability. ZigBee mesh networks automatically form; there is no need for manual configuration. New nodes are recognized by the network and are automatically added. Moreover, if a node stops working, the network reroutes communications through different channels to avoid it. The ZigBee specification states that a mesh network can have up to 65,536 network node clients.

An application could be made up of interconnected items that work together to do the required activities. The primary goal of ZigBee is to spread work across numerous router components that are housed and contained by distinct ZigBee nodes, which together form a network [27]. This work is often mostly indigenous to each end device, such as the controlling of individually distinct home machines. The group of items that make up the system interact via the APS conveniences, which are controlled through ZigBee device object (ZDO) interfaces. The request-confirm/indication-response pattern is used by the application-level data facility. A single device can support up to 240 application objects with numbers between 1 and 240. The range between 241 and 254 is not present in practice but maybe in the upcoming time, '0' is set aside for the ZDO interlink of data, and 255 is set aside for transmission. In ZigBee 1.0, application objects can access two services. Key-value pair (KVP) or key-value enabled pair facility, which is used for this arrangement. Through a straightforward interlink built on get/set and occurrence primitives, it allows for the depiction, application, and alteration of object properties, with some permitting an application for the reply. Compressed extensible markup language (XML) (the occupied XML may also be utilized) is used in configuration to offer a flexible and elegant approach. By providing a universal approach to information treatment, the message service is intended to obviate the need to modify application procedures and any impending overhead caused by KVP. It permits the transmission of any payload over application support sublayer (APS) frames. A component of the application layer is addressing. An 802.15.4-compliant radio transceiver plus one or more components descriptions ultimately, assortments of features that may be sampled, set, or watched through events that make up a network node [28]. The devices inside a node are identified by endpoint identifiers that fall within the range of 1-240, with the transceiver serving as the base for addressing.

WSNs employ diverse protocols to facilitate communication between the sensor nodes. These protocols specifically target the distinct obstacles encountered in WSNs, including constrained energy resources, fluctuating communication circumstances, and the requirement for optimal data transmission**.** Figure 7 presents several frequently utilized protocols in WSNs. An automated home management system's light switch is one such example in which most typical ZigBee network topologies are configured for effective communication in the nodes. In a star network, a single coordinator is responsible for starting up and overseeing several nodes. Only the coordinator can receive communications from end devices. ZigBee application layer architecture includes the application support layer, the ZigBee device object, and application objects defined by the manufacturer. The application layer is responsible for several tasks, including the maintenance of the binding database and the transmission of messages between bound devices.

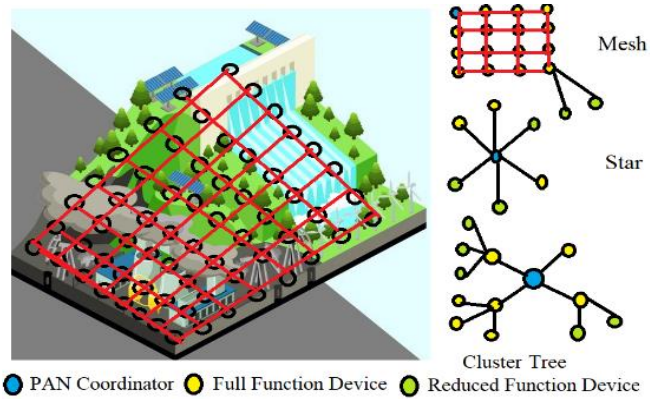

Figure. 6 Network topology associate for ZigBee [29]

IEEE 802.15.4

- This standard specifies the physical and MAC (Medium Access Control) layers for low-rate wireless personal area networks (LR-WPANs). Its low power consumption and appropriateness for short-range communication make it extensively utilized in WSNs.

(IPv6 over Low-Power Wireless Personal Area Networks)

- 6LoWPAN allows IPv6 on low-power wireless networks. It helps integrate WSNs with existing network infrastructure by connecting them to the internet.

Constrained Application Protocol (CoAP)

- CoAP is a simple application-layer protocol made for networks and devices that do not have a lot of space. It is often used in WSNs to let devices with limited resources talk to each other. CoAP and 6LoWPAN are often used together.

Zigbee

- Based on the IEEE 802.15.4 standard, Zigbee is a group of high-level chat systems. Low-cost, low-power, and low-data-rate apps are what it's made for. Zigbee is often used for WSNs, home automation, and industrial control.

Message Queuing Telemetry Transport (MQTT)

- A simple publish-subscribe messaging system called MQTT is often used for IoT applications, such as WSNs. It makes contact between sensor nodes and a main server or gateway quick and easy.

Routing Protocol for Low-Power and Lossy Networks (RPL)

- For WSNs that use low-power, lossy links, there is a routing protocol called RPL.It determines efficient paths between sensor nodes. Combining RPL with 6LoWPAN is a popular practice.

Low-Energy Adaptive Clustering Hierarchy (LEACH)

- LEACH protocol is used in WSNs that utilizes clustering to reduce energy consumption using the nodes into clusters led by a rotating cluster leader. This facilitates the distribution of energy demand and extends the lifespan of the network.

Mobile and Ad-hoc Networks for Tiny embedded Systems (MANTIS)

- The MANTIS communication architecture framework offers communication, routing, and localization protocols that effectively tackle the distinct obstacles presented by sensor nodes with limited resources.

Sensor Protocol for Information via Negotiation (SPIN)

- SPIN is a family of protocols utilized in WSNs to aggregate distributed data. By negotiating the transmission of solely pertinent information between nodes, it minimizes redundancy and preserves energy, thereby optimizing communication.

Transmission Energy Protocol (TEP)

- The TEP protocol considers the energy consumption of both communication and sensing activities in WSNs. It dynamically modulates the transmission power of nodes according to the distance to the destination, with the goal of conserving energy.

Figure 7. Major protocols of WSN

5. DISCUSSION

Numerous applications of WSNs are either already in mature use or are still in the infancy phases of research. Some of the major applications are highlighted here.

- Area monitoring: WSNs are frequently used for area monitoring. The nodes are deployed in WSN across a region during area monitoring to keep an eye on a certain phenomenon [30]. Geo-fencing of oil pipelines or gas is an example of a civilian application; using sensors to identify opponent entry is a military example. One of the base stations receives a signal from the sensors indicating the monitored event such as heat or pressure, which is then dealt with appropriately such as by directing a message to a satellite or through the internet. In the same way, WSN may use a range of sensors, from motorcycles to railway cars, to locate vehicles.
- Environmental/earth monitoring: WSNs have been widely used for environmental parameters such as pressure, humidity temperature, and pressure. for real-time monitoring of earth data. The concept of 'Environmental Sensor Networks' has grown to encompass an extensive variety of WSN submissions in earth science study and related research. This includes detecting glaciers, oceans, forests, and volcanoes. These are a few of the key areas.
- Forest fire detection: To determine whether a forest fire has started, a collection of sensor network nodes can be set up there. The nodes may have sensors that record temperature, humidity, and gases released by burning wood or other vegetation. The fire contingent will be capable of recognizing when a fire is happening and how it is increasing owing to WSN, which is essential for the firefighters' ability to act successfully.
- Air pollution monitoring: The concentration of dangerous substances is being monitored by WSN in several major cities, including Stockholm, London, and Brisbane, for the benefit of the local population. WSNs are used to monitor air pollution in India as well, in places like Delhi, Chennai, Bangalore, Kolkata, and Mumbai. Instead of using wired installations, these can proceed with the benefits of ad-hoc wireless communication networks, accessing them additionally transportable for challenging interpretations in various locations [31]. Many topologies and different kinds of data exploration and insertion can be employed for these applications.
- Landslide detection: The landslide exposure method makes use of WSN to detect minute soil activities and changes in a variety of limitations that may occur before or during a landslide. Additionally, utilizing the collected data, it may be possible to anticipate the likelihood of landslides far before they occur.
- Machine health monitoring: WSNs have been created for condition-based maintenance (CBM) of machinery because they offer substantial budget reductions and open the door to new functions. Often, installing enough sensors is impossible due to the value of wiring in wired systems. Wireless sensors can now access previously inaccessible regions, dangerous or limited areas, whirling machinery, and mobile resources.
- Data logging: WSNs are also used to collect data for the monitoring of environmental statistics. This might be as simple as keeping track of a refrigerator's temperature or a nuclear power plant's overflow tank's water level. After that, the statistical data can be used to demonstrate how well the systems have performed. The "live" data stream that is possible with WSNs gives them an edge over traditional loggers [32].
- Industrial sense and control applications: Numerous wireless sensor network communication protocols have been created in recent years of research. While earlier studies mostly concentrated on power cognizance, more research that is current has started to take an extensive range of factors into account, such as the dependability of wireless links, real-time competencies, and QoS. These new attributes are seen as key enablers for forthcoming wireless sense and controller applications in industrial settings as well as those that are related, and they have the potential to supplement or completely replace traditional wired networks.
- Water/wastewater monitoring: The water and wastewater sectors offer numerous prospects for the use of wireless sensor networks. It is feasible to monitor facilities that are not wired for power or data transmission using manufactured wireless I/O components and sensors powered by battery packs or solar panels, as well as being used in pollution control boards.
- Agriculture: A growing trend in the agricultural sector is the use of wireless sensor networks, which relieve farmers of the maintenance-intensive task of maintaining wiring in challenging conditions. Wireless I/O components can operate pumps, and water applications can be detected and wirelessly relayed back to the main controlling center for advertising. Pressure transmitters can be used to monitor water tank levels in gravity-feed water systems. Automation in irrigation provides more effective water usage and lowers waste.
- Greenhouse monitoring: WSNs also manage the humidity and temperature levels within viable greenhouses. The greenhouse administrator gets information and related data via email or textual

communication when the temperature and humidity fall below predetermined thresholds for host systems to avoid activating misting networks, opening vents, turning on fans, or controlling a range of other system reactions.

- Structural monitoring: WSN can be used to monitor movement inside of buildings and infrastructure, such as embankments, bridges, flyovers, and tunnels, sparing engineering practice from the expense of site visits and allowing it to take advantage of daily data, as opposed to the traditional method of collecting this data, which required physical site visits and, in some cases, required closing roads or rail lines. It is also far more accurate than a visual inspection. Figure 8 presents the applications of WSN.
- Passive localization and tracking: Utilizing the ubiquitous and affordable behavior of such technology as well as the characteristics of the wireless associations, which are recognized in mesh interconnected WSN nodes in communication infrastructure, the submission of WSN to the inactive localization and following of non-cooperative targets has been utilized in such applications as people who lack identification tags, mask, or any other identity [33].
- Smart home monitoring: Using wireless sensors included in common objects to build a WSN, monitoring actions carried out in a smart home is made possible. The wireless sensor network, which enables activity-support services, records state deviations to objects based on human operation.

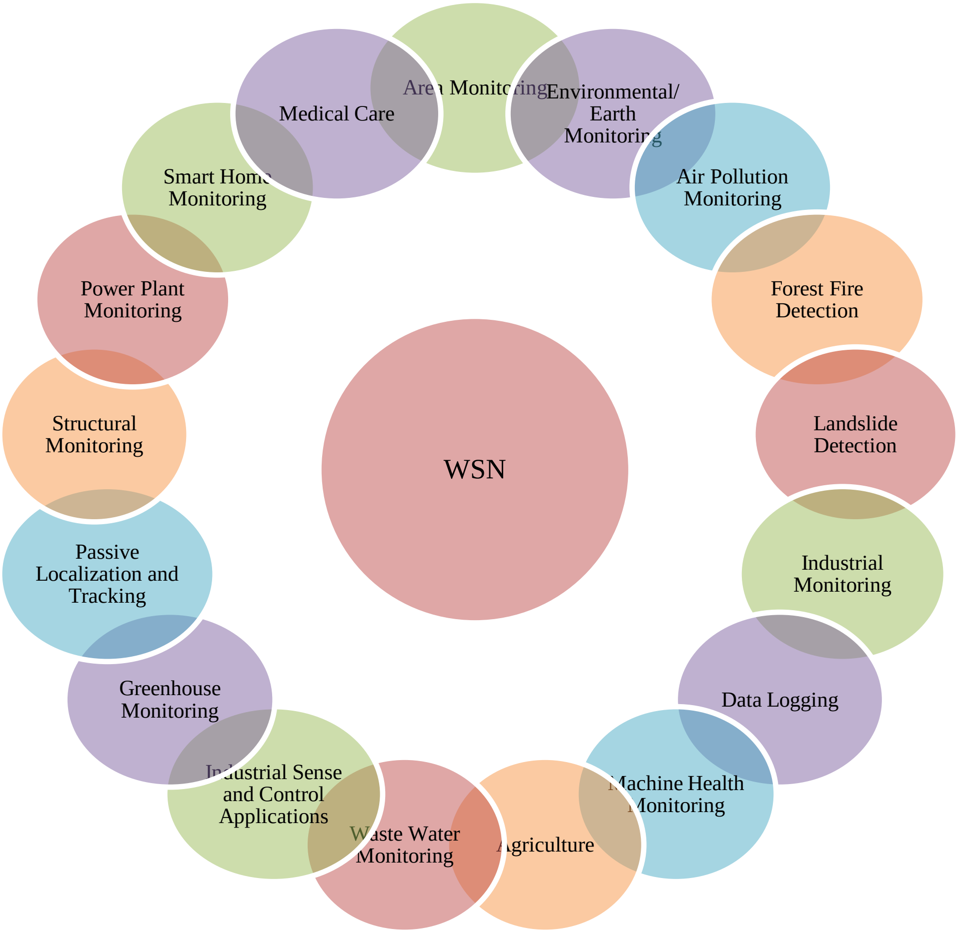

Figure 8. Applications of WSN [34]–[36]

The infrastructure is very impost for smart communication and a smart city, and the safety lifecycle for fully autonomous cars is all part of the recommended smart communication solution [37]. It is crucial to localize sensor nodes because without knowing where they came from, the data they collect may be worthless. Some of the sensor nodes may run out of battery life too soon and stop performing their intended purpose because of the network's unevenly loaded data and the limited battery life [38]. This could cause the network to become divided, with some parts of the network unable to transmit their sensed data to the sink node. In this case, we must deploy additional new nodes into the network [39], [40].

6. CONCLUSION

A multidisciplinary approach is required when designing a NoC for WSN considering hardware design, energy efficiency, communication protocols, and application-specific requirements. Before deploying a NoC into a real-world environment, simulation, and modeling tools may also be useful for assessing the efficacy of various NoC designs. The research can concentrate on augmenting the efficiency of NoC by enhancing data transfer speeds, minimizing latency, and optimizing power consumption by designing optimized routing algorithms and protocols to enhance communication efficiency among on-chip components. The integration of WSN IoT and edge computing enables advanced data processing and decision-making capabilities, enhancing research in the field of Integration with IoT and edge computing. Exploring the function of WSN facilitating applications such as smart cities, healthcare monitoring, and environmental sensing. Researchers in both NoC and WSN collaborate to investigate combined solutions that utilize the advantages of both technologies. This includes developing communication systems that are both energy-efficient and scalable, specifically designed for emerging applications.

ACKNOWLEDGEMENTS

Thanks to the UPES Communication System Lab for providing the platform for carrying out the work.

REFERENCES

[1] H. A. H. Alobaidy, J. S. Mandeep, R. Nordin, and N. F. Abdullah, "A review on ZigBee-based WSNs: concepts, infrastructure, applications, and challenges," *International Journal of Electrical and Electronic Engineering & Telecommunications*, pp. 189–198, 2020, doi: 10.18178/ijeetc.9.3.189-198.

[2] O. B. Akan and I. F. Akyildiz, "Event-to-sink reliable transport in wireless sensor networks," *IEEE/ACM Transactions on Networking*, vol. 13, no. 5, pp. 1003–1016, Oct. 2005, doi: 10.1109/TNET.2005.857076.

[3] I. F. Akyildiz, Weilian Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," *IEEE Communications Magazine*, vol. 40, no. 8, pp. 102–114, Aug. 2002, doi: 10.1109/MCOM.2002.1024422.

[4] N. Heydarishahreza, S. Ebadollahi, R. Vahidnia, and F. J. Dian, "Wireless sensor networks fundamentals: a review," in *2020 11th IEEE Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, Nov. 2020, pp. 1–7, doi: 10.1109/IEMCON51383.2020.9284873.

[5] N. Bulusu, J. Heidemann, and D. Estrin, "GPS-less low-cost outdoor localization for very small devices," *IEEE Personal Communications*, vol. 7, no. 5, pp. 28–34, 2000, doi: 10.1109/98.878533.

[6] P. Baronti, P. Pillai, V. W. C. Chook, S. Chessa, A. Gotta, and Y. F. Hu, "Wireless sensor networks: a survey on the state of the art and the 802.15.4 and ZigBee standards," *Computer Communications*, vol. 30, no. 7, pp. 1655–1695, May 2007, doi: 10.1016/j.comcom.2006.12.020.

[7] M. S. BenSaleh, R. Saida, Y. H. Kacem, and M. Abid, "Wireless sensor network design methodologies: a survey," *Journal of Sensors*, vol. 2020, pp. 1–13, Jan. 2020, doi: 10.1155/2020/9592836.

[8] R. Challoo, A. Oladeinde, N. Yilmazer, S. Ozcelik, and L. Challoo, "An overview and assessment of wireless technologies and co-existence of ZigBee, Bluetooth and Wi-Fi devices," *Procedia Computer Science*, vol. 12, pp. 386–391, 2012, doi: 10.1016/j.procs.2012.09.091.

[9] J. Yick, B. Mukherjee, and D. Ghosal, "Wireless sensor network survey," *Computer Networks*, vol. 52, no. 12, pp. 2292–2330, Aug. 2008, doi: 10.1016/j.comnet.2008.04.002.

[10] N. John and A. Jyotsna, "A survey on energy efficient tree-based data aggregation techniques in wireless sensor networks," in *2018 International Conference on Inventive Research in Computing Applications (ICIRCA)*, Jul. 2018, pp. 461–465, doi: 10.1109/ICIRCA.2018.8597222.

[11] M. Shafiq, H. Ashraf, A. Ullah, and S. Tahira, "Systematic literature review on energy efficient routing schemes in WSN-A survey," *Mobile Networks and Applications*, vol. 25, no. 3, pp. 882–895, Jun. 2020, doi: 10.1007/s11036-020-01523-5.

[12] M. A. Bin Karnain and Z. Bin Zakaria, "A review on ZigBee security enhancement in smart home environment," in *2015 2nd International Conference on Information Science and Security (ICISS)*, Dec. 2015, pp. 1–4, doi: 10.1109/ICISSEC.2015.7370969.

[13] N. Vamsi, A. Gupta, A. Dutta, and S. G. Singh, "Ultra low power on-chip hybrid start-up for wireless sensor networks," in *2015 Nordic Circuits and Systems Conference (NORCAS): NORCHIP & International Symposium on System-on-Chip (SoC)*, Oct. 2015, pp. 1–4, doi: 10.1109/NORCHIP.2015.7364415.

[14] H. Fitriawan, M. Susanto, A. S. Arifin, D. Mausa, and A. Trisanto, "ZigBee based wireless sensor networks and performance analysis in various environments," in *2017 15th International Conference on Quality in Research (QiR) : International Symposium on Electrical and Computer Engineering*, Jul. 2017, pp. 272–275, doi: 10.1109/QIR.2017.8168495.

[15] S. Katyara, M. A. Shah, B. S. Chowdhary, F. Akhtar, and G. A. Lashari, "Monitoring, control and energy management of smart grid system via WSN technology through SCADA applications," *Wireless Personal Communications*, vol. 106, no. 4, pp. 1951–1968, Jun. 2019, doi: 10.1007/s11277-018-5738-x.

[16] A. Shahraki, A. Taherkordi, O. Haugen, and F. Eliassen, "A survey and future directions on clustering: from WSNs to IoT and modern networking paradigms," *IEEE Transactions on Network and Service Management*, vol. 18, no. 2, pp. 2242–2274, Jun. 2021, doi: 10.1109/TNSM.2020.3035315.

[17] Y. Yu, B. Xue, Z. Chen, and Z. Qian, "Cluster tree topology construction method based on PSO algorithm to prolong the lifetime of ZigBee wireless sensor networks," *EURASIP Journal on Wireless Communications and Networking*, vol. 2019, no. 1, Dec. 2019, doi: 10.1186/s13638-019-1523-0.

[18] T. Kim, S. H. Kim, and D. Kim, "Distributed topology construction in ZigBee wireless networks," *Wireless Personal Communications*, vol. 103, no. 3, pp. 2213–2227, Dec. 2018, doi: 10.1007/s11277-018-5905-0.

[19] J. Kim and I. Lee, "802.11 WLAN: history and new enabling MIMO techniques for next generation standards," *IEEE Communications Magazine*, vol. 53, no. 3, pp. 134–140, Mar. 2015, doi: 10.1109/MCOM.2015.7060495.

[20] A. Jain, A. Kumar, and S. Sharma, "Comparative design and analysis of mesh, torus and ring NoC," *Procedia Computer Science*, vol. 48, pp. 330–337, 2015, doi: 10.1016/j.procs.2015.04.190.

[21] A. Kumar, P. Kuchhal, S. Singhal, and A. Kumar, "Network on chip for DTMF Decoder and TDM switching in telecommunication network with HDL environment," in *2013 3rd IEEE International Advance Computing Conference (IACC)*, Feb. 2013, pp. 1582–1588, doi: 10.1109/IAdCC.2013.6514464.

[22] A. Kumar, P. Sharma, M. K. Gupta, and R. Kumar, "Machine learning based resource utilization and pre-estimation for network on chip (NoC) communication," *Wireless Personal Communications*, vol. 102, no. 3, pp. 2211–2231, Oct. 2018, doi: 10.1007/s11277-018-5376-3.

[23] A. Kumar, G. Verma, M. K. Gupta, M. Salauddin, B. K. Rehman, and D. Kumar, "3D multilayer mesh NoC communication and FPGA synthesis," *Wireless Personal Communications*, vol. 106, no. 4, pp. 1855–1873, Jun. 2019, doi: 10.1007/s11277-018-5724-3.

[24] S. Crul, G. Ottoy, and L. De Strycker, "Location awareness enables autonomous commissioning in wireless sensor networks," in *2016 International Conference on Indoor Positioning and Indoor Navigation (IPIN)*, Oct. 2016, pp. 1–6, doi: 10.1109/IPIN.2016.7743604.

[25] V. K. Arora, V. Sharma, and M. Sachdeva, "On QoS evaluation for ZigBee incorporated wireless sensor network (IEEE 802.15.4) using mobile sensor nodes," *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 2, pp. 27–35, Feb. 2022, doi: 10.1016/j.jksuci.2018.10.013.

[26] T. Rajasekaran and S. Anandamurugan, "Challenges and applications of wireless sensor networks in smart farming—a survey," in *Advances in big data and cloud computing*, 2019, pp. 353–361.

[27] D. M. Adat, P. V Mane-Deshmukh, S. K. Tilekar, and B. P. Ladgaonkar, "Smart fusion-based cSoC for wireless sensor network for agricultural applications," *International Journal of Scientific Research in Science, Engineering and Technology*, vol. 3, no. 5, pp. 161–168, 2017.

[28] J. Liao, B. K. Singh, M. A. S. Khalid, and K. E. Tepe, "FPGA based wireless sensor node with customizable event-driven architecture," *EURASIP Journal on Embedded Systems*, vol. 2013, no. 1, Dec. 2013, doi: 10.1186/1687-3963-2013-5.

[29] Ompal, V. M. Mishra, and A. Kumar, "FPGA integrated IEEE 802.15.4 ZigBee wireless sensor nodes performance for industrial plant monitoring and automation," *Nuclear Engineering and Technology*, vol. 54, no. 7, pp. 2444–2452, Jul. 2022, doi: 10.1016/j.net.2022.01.011.

[30] P. Suresh, J. V. Daniel, V. Parthasarathy, and R. H. Aswathy, "A state of the art review on the internet of things (IoT) history, technology and fields of deployment," in *2014 International Conference on Science Engineering and Management Research (ICSEMR)*, Nov. 2014, pp. 1–8, doi: 10.1109/ICSEMR.2014.7043637.

[31] D. Kandris, C. Nakas, D. Vomvas, and G. Koulouras, "Applications of wireless sensor networks: an up-to-date survey," *Applied System Innovation*, vol. 3, no. 1, Feb. 2020, doi: 10.3390/asi3010014.

[32] S. M. Mohamed, H. S. Hamza, and I. A. Saroit, "Coverage in mobile wireless sensor networks (M-WSN): a survey," *Computer Communications*, vol. 110, pp. 133–150, Sep. 2017, doi: 10.1016/j.comcom.2017.06.010.

[33] B. Rashid and M. H. Rehmani, "Applications of wireless sensor networks for urban areas: a survey," *Journal of Network and Computer Applications*, vol. 60, pp. 192–219, Jan. 2016, doi: 10.1016/j.jnca.2015.09.008.

[34] S. M. Aziz, D. H. Hoskin, D. M. Pham, and J. Kamruzzaman, "Remote reconfiguration of FPGA-based wireless sensor nodes for flexible Internet of Things☆," *Computers and Electrical Engineering*, vol. 100, May 2022, doi: 10.1016/j.compeleceng.2022.107935.

[35] N. Gupta, A. Jain, K. S. Vaisla, A. Kumar, and R. Kumar, "Performance analysis of DSDV and OLSR wireless sensor network routing protocols using FPGA hardware and machine learning," *Multimedia Tools and Applications*, vol. 80, no. 14, pp. 22301–22319, Jun. 2021, doi: 10.1007/s11042-021-10820-4.

[36] S. Bhatnagar *et al.*, "Efficient logistics solutions for e-commerce using wireless sensor networks," *IEEE Transactions on Consumer Electronics*, p. 1, 2024, doi: 10.1109/TCE.2024.3375748.

[37] X. Shao and R. Zhang, "Target-mounted intelligent reflecting surface for secure wireless sensing," *IEEE Transactions on Wireless Communications*, p. 1, 2024, doi: 10.1109/TWC.2024.3365215.

[38] Y. Y. Ghadi *et al.*, "Machine learning solutions for the security of wireless sensor networks: a review," *IEEE Access*, vol. 12, pp. 12699–12719, 2024, doi: 10.1109/ACCESS.2024.3355312.

[39] M. Y. Arafat, S. Pan, and E. Bak, "Distributed energy-efficient clustering and routing for wearable IoT enabled wireless body area networks," *IEEE Access*, vol. 11, pp. 5047–5061, 2023, doi: 10.1109/ACCESS.2023.3236403.

[40] R. Priyadarshi, "Exploring machine learning solutions for overcoming challenges in IoT-based wireless sensor network routing: a comprehensive review," *Wireless Networks*, vol. 30, no. 4, pp. 2647–2673, May 2024, doi: 10.1007/s11276-024-03697-2.

BIOGRAPHIES OF AUTHORS

Ompal a research scholar in the Electronics and Communication Engineering Department, Veer Madho Singh Bhandari Uttarakhand Technical University, Dehradun India. He is M. Tech in Electronics & Communication Engineering from M.M.M Engineering College, Gorakhpur. He is also working as an assistant professor in the Department of Electronics & Communication Engineering, UIET, Chhatrapati Sahu Ji Maharaj University, Kanpur, India. His areas of interest are digital systems, wireless communication, and VLSI design. He can be contacted at op.ompal85@yahoo.co.in.

Niraj Kumar is working as an associate professor in Department of Electronics and Communication Engineering, UIET, Chhatrapati Sahu Ji Maharaj University, Kanpur, India. He is a Ph.D. in Electronics and Communication Engineering Department, Veer Madho Singh Bhandari Uttarakhand Technical University, Dehradun India His areas of interest are digital systems, smart grid communication, and VLSI design. He can be contacted at neeraj_mmmec@yahoo.com.

Vishnu Mohan Mishra is working as a professor and Head of the Department of Electrical Engineering at G. B Pant Engineering College, Pauri Garhwal India, and assistant professor at Madan Mohan Malviya Engineering College, Gorakhpur, India. He has a B.E. in Electrical Engineering from M.M.M Engineering College, Gorakhpur, an M.Tech. in Power Systems from NIT Kurukshetra, and a Ph.D. in Electrical Engineering from Uttar Pradesh Technical University, Lucknow, India. His areas of interest are an area of teaching and research are power electronics and drives, electrical machines, power systems, facts controllers TSR, TSC, SVC, STATCOM, UPFC, power quality, harmonics analysis, harmonics injection due to different sources, motor drives controls using artificial intelligence, genetic algorithms and fuzzy controllers. He can be contacted at vmm66@rediffmail.com.

Adesh Kumar has been working as a professor in the Department of Electrical and Electronics, Engineering, in the Department of Electrical and Electronics Engineering, School of Advanced Engineering, The University of Petroleum and Energy Studies (UPES), Dehradun, India since 2010. He has a B.Tech. in Electronics and Communication Engineering from UPTU, Lucknow India in 2006. MTech (Hons) in Embedded Systems Technology, from SRM University, Chennai in 2008. Ph.D. (Electronics Engineering) from UPES, Dehradun India in 2014. He has also worked as a Senior Engineer in TATA ELXSI LIMITED Bangalore and as a faculty member in ICFAI University, Dehradun. His areas of interest are VLSI design, embedded systems design, telecommunications, and signal processing. He has supervised 8 Ph.D. scholars, and 5 candidates are doing research under his supervision. He has worked on more than 10 editorial assignments for Edited books, Conference proceedings, and journals, having citations of more than 2000, H-index-25, i10-index-45. He has 16 years of experience in the teaching research industry, published more than 120 research papers in international peer-reviewed journals (SCI/Scopus) and conferences. He can be contacted at: adeshmanav@gmail.com; or adeshkumar@ddn.upes.ac.in.