Hindawi
Journal of Sensors
Volume 2022, Article ID 1628537, 21 pages
https://doi.org/10.1155/2022/1628537

Review Article

WSN Protocols and Security Challenges for Environmental Monitoring Applications: A Survey

Kofi Sarpong Adu-Manu,[1] **Felicia Engmann**,[2] **Godwin Sarfo-Kantanka**,[1] **Godwill Enchill Baiden**,[1] **and Bernice Akusika Dulemordzi**[1]

[1]*Department of Computer Science, University of Ghana, Legon, Accra, Ghana*
[2]*School of Technology, Ghana Institute of Management and Public Administration, Accra, Ghana*

Correspondence should be addressed to Kofi Sarpong Adu-Manu; ksadu-manu@ug.edu.gh

Received 25 March 2022; Revised 26 June 2022; Accepted 20 July 2022; Published 21 August 2022

Academic Editor: Zhenxing Zhang

In recent years, communication technology has improved exponentially, partly owing to the locations and nature of the deployment of sensor nodes. Wireless sensor networks (WSNs) comprise these sensor nodes and can provide real-time physical and environmental measurements. The sensor nodes have limited power, which reduces their lifespan, especially when placed in human-inaccessible locations. This paper reviews energy-efficient protocols for environmental monitoring applications and energy harvesting-wireless sensor networks. The dynamic deployment and communication challenges associated with environmental monitoring applications (EMAs) make this paper take into account the WSN protocol stack, focusing on the physical layer, network layer (routing), and medium access control (MAC). The paper will delve deeper into the security challenges of deploying sensor nodes for environmental monitoring applications (EMAs). The paper further describes scientific approaches that churn out innovative and engineering applications that must be followed to improve environmental monitoring applications.

1. Introduction

Environmental monitoring is aimed at identifying the status of a changing environment using data collection tools. Data collection tools employed for determining the status of the changing environment rely on data acquisition systems (DAS). DAS uses measurement devices that are designed to allow for gathering representative samples. The samples depend on the device's intrusiveness, sampling accuracy, and sample storage [1–3]. These measurement devices have varying degrees of impact depending on the application and the data gathering method. For example, the sensitivity of the measured physical value to external influences may vary depending on the type of application. The traditional way of collecting the status of the changing environment has proven ineffective, having data reliability, delays, and security challenges [4]. Hence, in recent times, the introduction of technological devices such as sensor nodes capable of forming a wireless sensor network (WSN) is used to sense the changes in the environment and wirelessly communicate the sensed data to a base station for processing.

WSNs are distributed systems comprised of several nodes and base stations (BS) to monitor physical environmental conditions [5]. Each sensor node contains a wireless radio transceiver to communicate with other nodes and the BS. Sensor nodes communicate via insecure radio channels prone to interference and fading [6].

WSNs are used in several applications and deployed on land (terrestrial), underground, and underwater. Recently, they have been used in multimedia applications and mobile applications such as animal tracking, air quality monitoring, forest fire warning, and flood detection, among the terrestrial applications of WSNs. WSNs monitor soil conditions underground, particularly for agricultural and mining purposes. Underwater applications include freshwater quality, climate change, ocean monitoring for aquatic life, and

assessing coral reef alterations underwater—WSNs track events such as video, audio, and imaging in multimedia applications. They are utilised in real-time monitoring of hazardous compounds, target tracking, and rescue and search applications in mobile applications [7, 8]. Despite the capabilities presented by WSNs, they are also associated with challenges in various application domains. Table 1 summarises some of these challenges and their associated recommended solutions when WSNs are utilised in the different application domains.

Researchers have studied the design of protocols that can address these challenges in a variety of application domains, taking into account the challenges of the application [9–13]. The protocols are intended to operate at the sensor network protocol stack (physical, link, network, and transport layers). Protocol design is aimed at helping with data collection, aggregation, processing, and communication to maximize network lifetime and uptime [14]. Protocols govern the operation of sensor nodes in a sensor network, specify the requirements and guidelines for operation, and ensure that the sensor network fulfils its intended use [8]. A wide range of protocols is designed in communication networks to overcome the challenges discussed in Table 1 and improve network performance. These protocols extend the operationality of the network to perform some intended function.

In WSNs, data packets are transmitted to the BS in two ways: single-hop or multihop. The node sends the generated packet directly to the base station in a single hop. In contrast, in multihop, source nodes send packets to the BS via a multipath, with each node in the path forwarding the received (or, in the case of the source node, generated) packet to another node until the packet reaches the BS [6]. WSNs face some challenges, which include energy consumption, sensor node deployment, routing algorithms, energy efficiency, cluster-head (CH) selection, resilience, etc. Researchers have developed several routing and medium access control (MAC) protocols to address these issues. Optimisation algorithms have also been designed to determine the best path between the transmitter and receiver nodes to save energy and extend the network lifetime.

Designing efficient communications and network protocols for WSNs for EMAs manages sensor node operation in their deployable environment and achieves successful sensor node objectives [15]. The variability of EMAs and their peculiar characteristics should be considered when designing efficient protocols suitable for gathering accurate and timely data from sensors in the field. A unique channel is frequently used to communicate between wireless sensor nodes. The channel has the property that only one node can send a message at any time. As a result, shared channel access necessitates the implementation of a MAC protocol among the sensor nodes [16]. The MAC protocol is aimed at managing access to the shared wireless medium to meet the underlying application's performance requirements.

On the other hand, routing protocols are essential during data transmission to create optimum paths from sensed data to be transmitted from source to destination [17]. Maintaining optimum paths in WSNs for EMAs is critical to maximizing the nodes' lifespan and data throughput. Another essential feature of the WSN is the maintenance of a secured network [18]. The different applications in EMAs require that their security solutions are provided with the objectives and application needs in mind.

The paper explores how WSNs for EMAs are affected by new security vulnerabilities at the physical, network, and data link layers. To appreciate the security challenges in EMAs, the paper discusses the WSN protocol stack, energy-efficient protocols, and energy harvesting protocols suitable for environmental monitoring applications. There are further discussions on the design requirements, simulation environments for EMA protocol designs, quality-of-service requirements, and network topology requirements. Finally, the paper presents the security issues in WSN for EMAs, detailing the threats at the nodal and network levels and their prevention and countermeasures.

2. WSN Protocol Stack

WSNs are distinguished by their adaptable network topology, which various networking protocols enable at multiple layers. Designing efficient and reliable communication protocols for WSNs for EMAs is difficult due to different constraints on the sensor platform and the different environments' lack of certainty and dynamics [19]. An analysis of the design requirements of protocols for WSNs for EMAs is provided in this section. Physical, data link, network, transport, and application are the five core layers of the WSN protocol stack, of which three (physical, data link, and network) will be explored in this section.

The physical, data link, network, transport, and application layers of the wireless sensor network protocol stack are similar to the classic open system interconnection (OSI) paradigm. In each of these layers, several activities are undertaken. The physical layer handles frequency selection, carrier frequency production, signal detection, modulation, and data encryption. The data link layer handles the multiplexing of data streams, data frame detection, medium access, and error correction. In a communication network, it enables reliable point-to-point and point-to-multipoint connections. The data given by the transport layer is routed by the network layer [8]. In WSNs, the network layer design must consider energy consumption, communication, aggregation, and other factors. The transport layer aids in data-flow maintenance and may be necessary if WSNs are accessed over the Internet or other external networks. Depending on the sensing duties, different forms of application software can be set up and employed at the application layer. The following section discusses the routing protocols for managing the increasing energy requirement of sensor nodes to monitor environmental applications such as photosynthesis, soil carbon flux, and soil salinity.

2.1. Routing Protocols. Routing protocols in EMAs determine optimum dynamic routes for exchanging information between sensor nodes depending on the application-specific requirements. These application-specific requirements of the routing protocols include throughput, capacity, coverage, network performance, end-to-end delay, real-time delay, and

Table 1: Challenges in WSN application domains.

Application domain	Challenges	Recommended solutions
Terrestrial	Limited power supply Data redundancy Data latency	Energy minimisation techniques Design of efficient routing protocols Use of energy harvesting Implement an effective node deployment strategy (e.g., multihop) Short transmission range
Underground	Difficulty in deployment High signal losses High levels of attenuation Higher energy cost Difficulty in battery replacement	Design of efficient data communication protocols
Underwater	Limited bandwidth of the acoustic channels Low link quality of acoustic channels Significant propagation delays due to the speed of sound Energy limitation with sensor nodes Creation of the Doppler effect due to the relative motion of the transmitter and the receiver Nodes are susceptible to corrosion	Design of efficient underwater data communication precools
Multimedia	High bandwidth demand High energy consumption Provisioning of quality of service due to variable delays and channel capacity High demand for data processing Challenges with cross-layer design Data compression	In-network processing Filtering Design of efficient compression techniques Design of cross-layer protocols
Mobile	Unreliable data transfer Uncontrolled mobility results in poor network performance Localization and coverage Unstable contact detection due to shorter contact durations	Design of efficient mobility-aware protocols for message exchanges Design of efficient mobility-aware power management protocols

collision. They are helpful, especially in mobile applications such as battlefields, disaster zones, animal tracking, water monitoring (freshwater/ocean), and air quality. Some EMAs are time-sensitive, while others have bandwidth constraints. The sensor nodes are either powered by fixed-energy batteries or rechargeable batteries. Battery-powered WSNs for EMAs are expected to operate for at least two (2) years without failure [20]. However, most applications of EMAs are deployed in areas where changing or recharging batteries is a difficult task. Generally, routing protocols are classified into route discovery protocols, network organization protocols, and protocol operations, as shown in Figure 1.

There are three route discovery protocols: reactive, proactive, and hybrid. There are four network organization protocols: flat-based, hierarchical-based, location-based, and data-centric. Based on their operation and how the protocols work in a deployable environment, routing protocols are classified as negotiation-based, multipath-based, query-based, quality-of-service-based, and coherent-based protocols [21, 22]. The following sections cover each category in detail, providing examples for each.

2.1.1. Discovery Protocols. Discovery routing protocols are discussed in this section. Developments of discovery routing protocols are presented in Figure 2.

(1) Proactive Protocols. Proactive protocols are table-driven protocols. Proactive routing techniques store the routes without any route matching. These protocols keep track of every sensor node's connectivity to other nodes in the sensor network at any given time. Proactive routing protocols enable every sensor node to send periodic updates and have a clear and consistent network topology view. Proactive routing keeps a fresh list of destinations and associated paths by frequently disseminating routing tables over the sensor network. Examples of proactive routing protocols include destination sequence vector (DSDV), optimised link state routing (OLSR), and wireless routing protocol (WRP). Other proactive protocols proposed in the literature include source tree adaptive routing (STAR); global state routing (GSR); cluster head gateway, switch routing (CGSR); and fisheye state routing (FSR) [23–25]. The popular examples discussed in this paper are DSDV and OLSR.

DSDV is a proactive table-driven protocol that uses the Bellman-Ford routing technique. Through sequence numbers, DSDV ensures loop-free operation. Every mobile node in the network keeps a routing table that lists all of the network's possible destinations and the number of hops required to reach each one. A sequence number is assigned to each entry by the destination node. The sequence

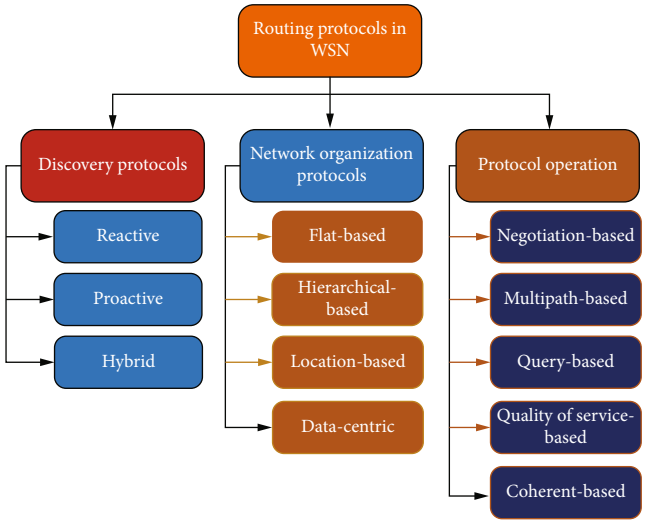

Figure 1: Classification of routing protocols.

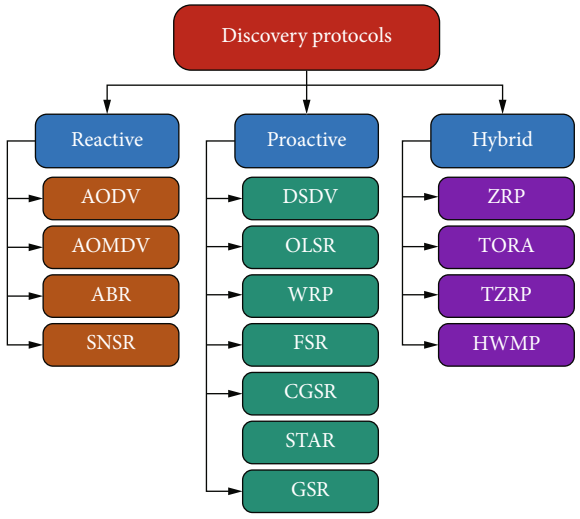

Figure 2: Discovery routing protocols.

numbers let the mobile nodes distinguish between old and new routes, preventing routing loops [26].

OLSR is a proactive protocol where frequent topology changes cause flooding of the network with erratic updates. The OLSR reduces the maximum time interval for updating control overhead messages to optimise the link-state information. The critical concept of OLSR is the multipoint relays (MPRs), which are selected nodes that forward broadcast packets during the flooding of the network. The MPR reduces the control overhead of flooding since only MPRs generate link-state information. Therefore, the flooding of the network with control overhead messages reduces when OLSR is employed [27]. OLSR only transmits partial link-state information between MPRs and their MPR selectors for route calculations. This approach reduces the computational cost of route calculations and hence minimal delay in establishing routes. This protocol is best for networks where larger subsets of the network communicate with other larger subsets of the same network. It is suitable for networks where the source/destination pair with time. It is also suitable for applications that do not allow for long delays and operate in dense networks. However, it is disadvantageous in mobile networks where the frequent change in topology increases the exchange of control overhead messages, increasing the cost of energy and memory use [27].

(2) Reactive Protocols. Reactive protocols are designed, so sensor nodes within the network initiate a route discovery process only when a route to a destination node is required. The routes are subjected to computation because the sensor node computes its route based on demand [20]. The routes that have been established are created and maintained in two stages: route discovery and route maintenance. The route discovery occurs on-demand by flooding the network with route request (RRQ) packets. When a route is discovered, the destination responds with a route reply (RREP) containing the route information traversed by the RREQ. Ad hoc on-demand distance vector (AODV), ad hoc on-demand multipath distance vector (AOMDV), associativity-based routing (ABR), sequence number-based secure routing (SNSR), signal stability routing (SSR), and dynamic source routing (DSR) are popular examples of reactive protocols [25, 26, 28]. More popular reactive protocols are discussed here. They are best suitable for applications where the sensors are mobile and have their routes changing frequently.

AODV reduces control traffic by generating path requests on-demand and constructs its routes without prior knowledge using an RREQ and RREP request loop between the source and destination nodes. RREQ packets are broadcast as part of the route-building process. When a node receives an RREQ packet, it checks its record to see if it has previously received an RREQ packet. If a packet is not logged when received, the node resends it [28]. Ad hoc on-demand multipath distance vector (AOMDV) is a modified version of the AODV routing protocol. AOMDV is a protocol with multiple routes, disjoint paths, and no loops from source to destination. AOMDV uses hop count during the advertisement. AOMDV is designed to keep multiple disjoint loop-free paths in route discovery. The AOMDV protocol reduces energy consumption and packet loss in WSNs. Compared to AODV, it performs better in applications with high traffic loads. The essence of the AOMDV protocol is guaranteeing that multiple pathways discovered are loop-free and discontinuous and identifying such paths fast utilising a flood-based route discovery method. AOMDV route update rules are critical for maintaining loop-freeness and applying disjointness properties locally at each node [29].

When a source node has packets to send to a destination node, dynamic source routing (DSR) checks its cache first to see if it has a route to that destination. A new packet header is constructed to include the destination's path if a route is available. Suppose no route is found in the cache. In that case, the node initiates the discovery process by sending an RREQ broadcast packet with the source and destination node identifiers of the route to be discovered and a unique identifier for the RREQ. Associativity-based routing (ABR)

is an on-demand routing protocol initiated by the source node. ABR employs both point-to-point and broadcast routing techniques. In ABR, the destination node decides on a route based on the property of "associativity." The chosen route is used, and all other routes are discarded because the decision is based on the property of "associativity," resulting in long-lived routes. ABR is divided into three stages (route discovery, route reconstruction, and route deletion).

(3) Hybrid Protocols. Hybrid routing methods combine the benefits of proactive and reactive routing strategies and their drawbacks. In some scenarios, hybrid routing is preferable. These hybrid protocols can achieve consistency across proactive and reactive protocols. Because nodes must keep high-level topological information, these protocols have a drawback in that they require more memory and power. Examples of hybrid routing protocols include zone routing protocol (ZRP), two-zone routing protocol (TZRP), temporarily ordered routing algorithm (TORA), and hybrid wireless mesh protocol (HWMP). A description of the most popular hybrid routing protocol is provided [25, 26]. ZRP was created to work in a zoned network. The node in ZRP maintains routes to all the routing zone's destinations. Intrazone routing protocol (IARP), interzone routing protocol (IERP), and bordercast resolution protocol are the three subprotocols of ZRP (BRP). When the route is within the zone, intrazone routing protocol (IZRP) is used, and when it is outside the zone, interzone routing protocol (IERP) is used [26].

2.1.2. Network Organization Protocols. Sensor nodes collaborate to complete the tasks of the app for which they were deployed. Sensor nodes with extreme energy constraints have limited computation, storage, and communication capabilities. Some network-level protocols are designed to address the limited computing, storage, and communication capabilities of WSNs. These include flat-based routing protocols, hierarchical protocols, data-centric protocols, and location-based protocols. In flat-based protocols, all nodes are treated as peers. Hierarchical protocols are a type of protocol that is based on clusters. Data-centric protocols are intended to disseminate information throughout the network, whereas location-based protocols are aimed at addressing sensor network concerns by utilising node position information. In each of these categories, several routing algorithms have been proposed. The following sections provide brief descriptions of the various network organization protocols, as illustrated in Figure 3.

(1) Hierarchical Protocols. Hierarchical routing protocols enable large-scale network deployment through self-organization capabilities. The primary goal of the hierarchical routing protocol is to keep sensor nodes' energy consumption as low as possible by performing data aggregation and fusion to reduce the amount of data transmitted to the base station [30]. In Figure 3, a list of hierarchical routing protocols is designed for use in WSNs. Details of these protocols are low energy adaptive clustering hierarchy (LEACH), power-efficient gathering in sensor information systems (PEGASIS), and hybrid energy-efficient distributed (HEED) clustering. Also, we have protocols such as the threshold-sensitive energy-efficient sensor network (TEEN), base station-controlled dynamic clustering protocol (BCDCP), concentric clustering scheme (CCS), and adaptive threshold sensitive energy-efficient protocol (APTEEN). Finally, hierarchical routing protocols also designed for large-scale networks include energy-efficient clustering scheme (EECS), self-organizing protocol (SOP), energy-balanced chain-cluster routing protocol (EBCRP), chain-based hierarchical routing protocol (CHIRON), energy-aware data aggregation tree (EADAT), balanced aggregation tree routing (BATR), power-efficient data gathering and aggregation protocol (PEDAP), and enhanced tree routing (ETR).

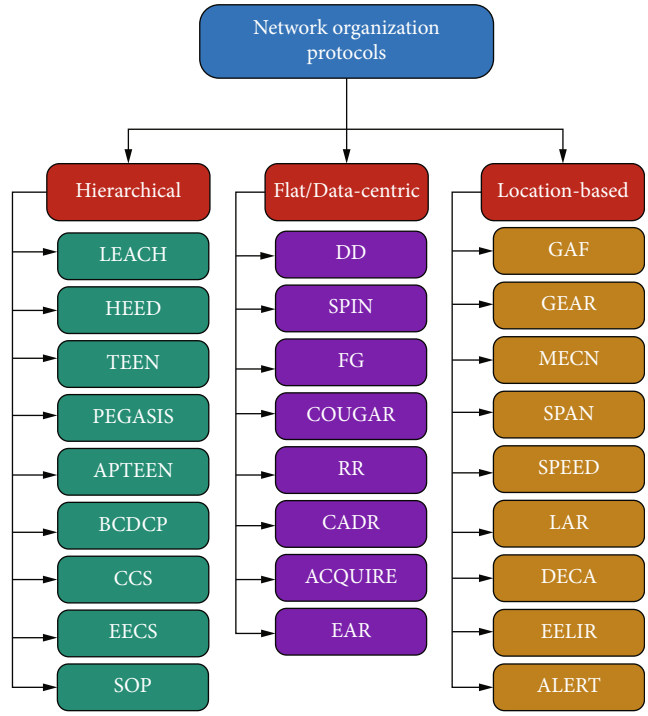

Figure 3: Network organization protocols.

Hierarchical routing protocols are divided into four types: cluster-based (LEACH, TEEN, HEED, APTEEN), chain-based (PEGASIS, CHIRON, EBCRP, CCS), tree-based (EADAT, BATR, ETR, PEDAP), and grid-based (SOP, BCDCP). Figures 4–7 illustrate the four hierarchical routing protocols employed for environmental monitoring applications depending on the requirements.

We describe two popular hierarchical protocols (LEACH and PEGASIS) suitable for environmental monitoring applications due to their flexibility in handling the routing information. LEACH (low-energy adaptive clustering hierarchy) is a routing algorithm that collects and delivers data to a sink node or base station. LEACH is the most widely used energy-efficient cluster-based hierarchical routing protocol for EMAs in WSNs. It employs localized coordination to enable scalability and robustness in dynamic networks.

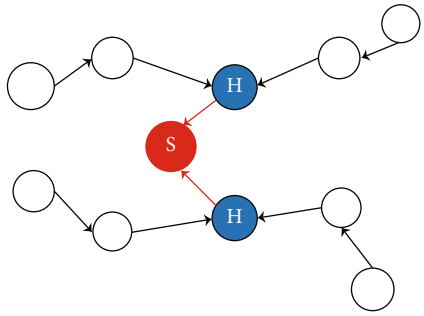

Figure 4: Chain-based.

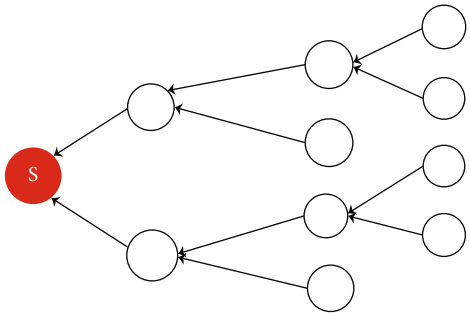

Figure 5: Tree-based.

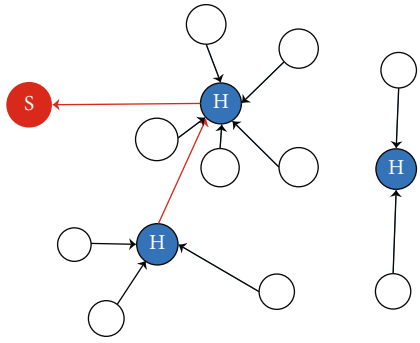

Figure 6: Grid-based.

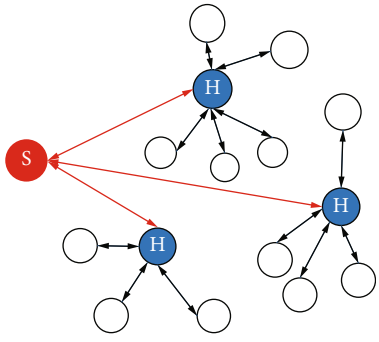

Figure 7: Cluster-based.

LEACH incorporates data fusion into the routing protocol to reduce the information transmitted to the base station and organizes the network into clusters using a hierarchical approach. A cluster head is responsible for each cluster. The cluster head carries out multifaceted tasks [10, 30, 31].

In PEGASIS, nodes are connected in a chain, with one node connected to the opposite and the last node connected to the base station. The advantage of PEGASIS is that it reduces the amount of data transferred between contiguous nodes by moving information obtained by detector nodes from one node to the next until the last node transmits the data to the final terminal and restricts the number of transmissions and receptions between nodes. Two main impediments challenge the use of PEGASIS in environmental monitoring applications. First, the base station acts as a single leader, which can cause bottlenecks. Secondly, PEGASIS generates excessive disruption for remote nodes in the chain. These two challenges can be solved by enabling concurrent transmission between neighbouring nodes, which reduces the latency incurred during connection with the base station. Other ideas include using signal coding or only permitting data to be transmitted simultaneously between far apart nodes [31].

(2) Flat/Data-Centric Protocols. It is not practical to issue global identifiers to each node in many sensor network applications. The lack of global identifiers and the random deployment of sensor nodes make selecting a set of sensor nodes to interrogate problematic. As a result, data is often transported to a deployment location with a high level of redundancy. The solution to these challenges led to developing a data-centric routing protocol [21]. Examples of flat/data-centric routing protocols include gradient-based routing (GBR), COUGAR, and constrained anisotropic diffusion routing (CADR). The others are directed diffusion (DD), flooding and gossiping (FG), energy-aware routing (EAR), active query forwarding in sensor networks (ACQUIRE), and rumor routing (RR). Two popular examples (SPIN and directed diffusion) of data-centric protocols discussed are provided in this paper.

SPIN stands for "sensor protocols for information via negotiation," a data-centric, negotiation-based family of WSN information dissemination protocols. The fundamental goal of these protocols is to efficiently distribute data collected by source nodes to the rest of the network's sensor nodes. Simple protocols such as flooding and gossiping are frequently recommended to achieve information distribution in WSNs. Each node in the network must send a copy of the data packet to its neighbours until the information reaches all nodes in the network [6, 9, 22]. Directed diffusion is a data-centric routing approach. There must be a list of attribute-value pairs (interval, name of objects, duration, and area). If a node is interested in specific data, the sink broadcasts the inquiry to its neighbours. The interest is cached by the nodes that get it to use later. The data is compared to the values in the cached interests. Within the interest, there are additional gradient fields. The gradient is a reply link to the neighbour who sent the interest [22, 32]. This data-centric strategy is used to acquire and deliver information because it is energy efficient, saving energy, and extending the network's lifespan. The directed diffusion routing protocol does not require addressing because all communication is node-to-node [22].

(3) Location-Based Protocols. A source node sends a packet to a destination node in a location-based routing (LBR) protocol, and the destination node appends to each packet by the source node. Packets received by intermediate nodes along the path to the destination node use the location information in the packet and deliver it to the next one-hop neighbours. They are geographically closest to the destination. The operation is repeated until the data packets arrive at the destination node. Because of the locality, location-based routing necessitates the minor state in each node. Because advertisements of routing tables, as in traditional routing protocols, are not required, it has a low communication overhead. As a result, route creation and maintenance are no longer needed with location-based routing. Location-based routing is used in more extensive networks where node positions change and the destination node's location is known to the source [33]. LBR makes use of node location information to improve efficiency and scalability. In LBR, each node in the network must be aware of its location information, obtained via GPS or other techniques. Also, each node must be informed of the position of its one-hop neighbour node, and the source must know where the destination node is located.

LBR generally requires accurate location information, which can be acquired through some sort of localization technique. Because location information is critical for many EMA WSNs, such as animal tracking and forest fire monitoring, it is expected that each wireless sensor node in the network will be equipped with some form of localization device. Location-based routing is categorised into GPS-based and non-GPS-based protocols. The sensor nodes may be deployed as mobile or static in each category. LBR employs greedy algorithms to forward packets from the source node to the destination node. It is critical in preserving the energy of the sensor nodes. Examples of location-based routing protocols are illustrated in Figure 3. Details of these protocols are geographic adaptive fidelity (GAF), geographical and energy-aware routing (GAER), minimum energy communication network (MECN), sensor protocols for information via negotiation (SPAN), SPEED (a real-time routing protocol for sensor networks), location-based energy-efficient intersection routing (EELIR), anonymous location-based efficient routing protocol (ALERT), energy-efficient geographic forwarding algorithm for wireless ad hoc and sensor network (DECA), improved hybrid location-based ad hoc routing protocol (IHLAR), location-based routing protocol (LBRP), selective bordercast in ZRP (SBZRP), and location-based selective bordercast in ZRP (LBZRP). In this paper, GAF and GEAR are described.

The geographic and energy-aware routing (GEAR) algorithm employs geographic information to route queries to the most relevant places. In many location-aware systems, notably sensor networks, disseminating information to a geographic region is valuable. GEAR uses an energy-aware and geographically informed neighbour selection algorithm to route a packet to the target region instead of flooding the query or packet across the whole network. On the contrary, interest is inundated throughout the entire network in directed diffusion. As a result, GEAR saves more energy than directed diffusion.

Geographical adaptive fidelity (GAF) is a location-based routing technology considering energy consumption. Sensor networks will find it informative and applicable. Algorithms control the network's nodes, turning them on and off to save energy while maintaining high fidelity. For the covered space, GAF develops a virtual grid. Each node receives its current location through GPS, associated with a virtual grid point. Regarding packet routing costs, nodes belonging to the same grid are regarded as the same.

2.1.3. Protocol Operation Routing. Protocol operation is another way to categorise routing protocols in WSNs. This category can be divided into five major sections based on protocol processes. Some subcategories include multipath, query, negotiation, quality-of-service, and coherent-based routing protocols. Examples of these protocols are presented in Figure 8.

In WSNs, data processing is critical, and several strategies are applied to lower processing costs to save energy. In this case, the obtained data can be handled logically. In coherent data processing-based protocols, the sensor nodes perform the bare minimum of processing locally [34]. Data is sent to sink nodes after minimal data processing in coherent routing. Tasks like time-stamping and duplicate elimination are often included in the minimum processing. Coherent processing is frequently used to produce energy-efficient routing [35]. Examples of protocols include the multiple winner algorithm (MWA) and single winner algorithm (SWA).

The protocol may use various methods to transmit data from source to destination in multipath routing. Multiple routes improve network fault tolerance while significantly increasing energy consumption and protocol overhead. An extension of the method evaluates only the path with the highest energy nodes. When a better path is found, the protocol changes to it. The network's reliability can be strengthened using the multipath routing protocol in severely unstable conditions. A large packet can be broken down into smaller chunks and sent via numerous channels. A message can still be produced even if one of the subpackets is lost owing to connection issues [16]. Some multipath routing protocols include energy-constrained multipath routing (ECMP) and multiconstrained quality-of-service multipath routing (MCMP).

A node initiates a query and propagates it across the network in query-based routing. The query is sent to each node; only the node with matching data receives responses. Rather than disseminating the queries throughout the network, the node could send them down a random path and wait for a response. If none of the other nodes responds, the node can broadcast it to the entire network [36]. Quality-of-service (QoS-based) routing ensures that a wireless network will deliver the expected results. Latency (delay), throughput, error rate, and energy consumption are a few quality-of-service parameters in WSNs, which differentiates traffic flows by treating packets differently based on their nature. The quality-of-service routing protocol is also in charge of

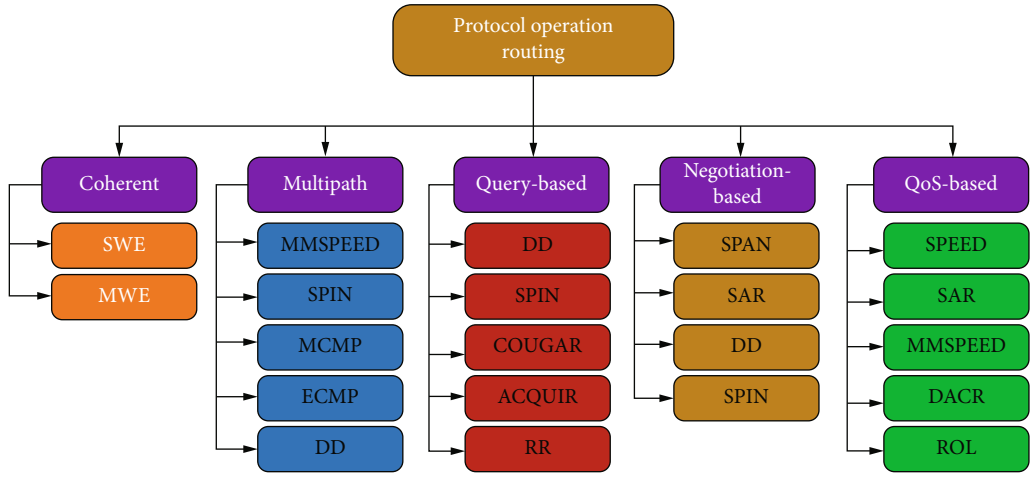

Figure 8: Protocol operation routing protocols.

prioritising data flows to maintain a predefined performance level. When delivering data in applications where parameters such as delay, resources, and bandwidth are critical, the routing protocol must maintain the quality and specifications of the required parameter. The quality-of-service routing protocol balances energy consumption and other metrics [37]. Sequential assignment routing (SAR) is a typical QoS-based routing protocol. Flooding and gossiping in WSNs can cause the network to implode; thus, a single node may get several copies of data. Negotiation-based protocols are intended to prevent duplicate packets from propagating. In wireless sensor networks (WSNs), sensor nodes exchange negotiation messages to send redundant data to the next node. It reduces network congestion and conserves energy.

Routing protocol categories (route discovery protocols, network organization protocols, and protocol operation) are beneficial in specific application areas. These protocols provide myriad challenges and energy requirements when used for specialised purposes. Table 2 highlights most of the application areas, challenges, and energy requirements for the various forms of routing protocols.

3. Energy-Efficient Protocols

Data communication is a critical challenge in many WSN applications. As a result, it is advantageous to construct and develop easily accessed resources to give data in WSNs. The number and position of nodes in WSNs make recharging or replacing batteries impossible. As a result, energy consumption is a universal design concern for WSNs. Researchers have concentrated on reducing energy dissipation at all stages of system design, from hardware to protocols to algorithms. As a result, it is critical for the network to carefully define the parameters of the protocols in the network stack to achieve the required energy efficiency and meet the quality-of-service requirements. The following is a discussion of some energy-efficient protocols used in the WSN architecture at the physical, link, and network layers.

3.1. Energy-Efficient Physical Layer Protocols. The Zigbee protocol suite is the preferred physical layer protocol for environmental monitoring. It is widely considered due to its low duty cycle for energy-efficient implementations. The communication range of Zigbee is within 100 m, with a reduced communication range of 30 m for indoor applications [38]. Using precision agriculture and farming applications, Zigbee enabled supervised irrigation, water quality management, pesticide and fertiliser control, and total field surveillance [39]. Other implementations of Zigbee include investigating signal propagation and strength distribution characteristics of wireless sensor networks in date palm orchards with application-efficient specific parameters such as signal strength on the spacing between nodes, the leaf density, and antenna height of the base station. Cattle grazing-field implementation [40, 41], greenhouse [42, 43], livestock monitoring [44], and smart beehives [45] are some current implementations using Zigbee.

3.1.1. LoRa (Long Range Radio). LoRa is a digital wireless data communication technology spread-spectrum radio modulation (EP2763321 from 2013 and US7791415 from 2008) derived from chirp spread spectrum (CSS) technology. It uses the unlicensed free radio frequency bands 169 MHz, 433 MHz, and 868 MHz in Europe and 915 MHz in the US.

LoRa is presented in two ways: the physical layer shown as LoRa on devices and the upper layers presented as the long range wide area network (LoRaWAN) [46]. LoRa provides a low-cost, secure bidirectional mobile communication for IoTs and other machine-to-machine (M2M) for high throughput systems. These systems typically run on 3G or Ethernet networks, WiFi, or cellular technologies. The LoRa has been implemented in smart bee monitoring farms to ensure communication of the colony activities [47]. Greenhouses measure air temperature, humidity, light intensity, and soil moisture [48]. LoRa's advantage is its scalability to several nodes and adaptability to interference and noise. Another implementation involves real-time monitoring using a multisensor combination module (MSCM) and LoRa. In the implementation, wetland parameters include

Table 2: Application areas, challenges, and energy requirements of routing protocols.

Categories of routing protocols		Application areas	Challenges	Energy requirements
Route discovery	Reactive	Animal tracking, habitat monitoring	Continuous energy source, size of sensor nodes, frequent change in node position, latency, security	Energy harvesting sources, rechargeable batteries
	Proactive	Infrastructure systems, hospice care, weather forecasting, military surveillance	Significant overhead for storing routing tables in sensor nodes, not suitable for mobile applications	Fixed energy batteries, capacitors, rechargeable batteries. Mobile energy transmitters
	Hybrid	Sewage and gully pot monitoring	Require more memory and power, mobility	Mobile energy transmitters, energy harvesting nodes
Network organization		Animal tracking, military surveillance, crop farming, forest fires, disasters. Habitat monitoring, disaster monitoring	Size of sensor nodes, energy source, number of nodes, modulation schemes	Fixed energy batteries, rechargeable batteries
Protocol operations		Smart farming, structural monitoring, earthquake monitoring, water quality monitoring, air quality monitoring, climate change monitoring	Energy consuming, topology control, maintaining energy-neutral operation (ENO), mobility of nodes, antenna sensitivity	Supercapacitors, rechargeable batteries, energy harvesting sources (primarily solar)

water temperature, pH, conductivity, turbidity, dissolved oxygen, and water level [11]. A recent work by authors considers the inability of the elderly and disabled farmers to monitor and oversee agricultural tasks on farms. In their implementation, LoRa radios were used to run several software applications from speech processing software, voice recognition, and other assistive artificial intelligence (AI) features. However, LoRA may only transmit data not exceeding a few kbps (not suitable for video capturing) over longer distances (not exceeding 3 km). The work by the authors included smartphones and tablets intercepting voice commands generated to be transmitted to a remote agent's device, usually at the farm's end. Applications on the agent's device are designed using raspberry pi and other programming facilities like the Arduino Uno unit with a WiFi radio module. Countries with existing implementations include smart gardens, vineyard crops in Spain, irrigation on kiwi and corn farms in Italy, and banana farming in Columbia.

3.1.2. Bluetooth. Bluetooth is another short-range communication protocol in environmental monitoring applications. It is usually implemented between movable portable devices such as laptops over 10 m distances. Due to its availability on most handheld devices, it can be used for multilevel agricultural applications. Agricultural implementations include weather information, soil moisture, temperature, and irrigation. Bluetooth is beneficial due to its low energy consumption, wide availability of devices, and ease of use. It has also been used in other monitoring environments, such as disaster prediction and monitoring [49], food storage systems [50], and environmental monitoring in small spaces [51].

3.1.3. Sigfox. Sigfox is the name of the company and the low power wireless area network (LPWAN) operator. It is one protocol gaining popularity in IoT and environmental monitoring applications in several countries, cooperating with various mobile network operators. Sigfox provides a software-based communication platform that allows the complexities of network computing to be carried out on the cloud instead of the devices. Their unique setup with mobile cellular networks provides an extensive network of global devices transmitting data without setting up or maintaining a connection [52]. Therefore, the Sigfox setup removes network bottlenecks such as signalling overheads, providing a robust and optimised network protocol. It uses the radio frequency channel on the 100 Hz band, with a data rate of 100 bps. It is based on the ultra narrow band (UNB). It uses a differential binary phase shift keying (DBPSK) modulation scheme, with scattered nodes accessing the network using random frequency time division multiple access (RFTDMA) [53].

Narrowband Internet of Things (NB-IoT) is developed by the 3rd Generation Partnership Project (3GPP) to scale up WSN applications and make them more dependable. NB-IoT uses an unlicensed frequency band in long-term evolution (LTE) and consumes more power than LoRaWAN due to its constant need for synchronisation. It implements orthogonal frequency-division multiplexing (OFDM) and frequency division multiple access (FDMA), increasing its power consumption. However, its applications require low latency and high data rates.

Other less implemented physical layer protocols in environmental monitoring include Bluetooth LE and mobile cellular technologies such as GPRS, 3G, and 4G. Due to their high energy consumption, mobile technologies are limited in IoTs and environmental monitoring applications. In contrast, the high data rate they provide may not be helpful in many applications [54–61]. Table 3 summarises the characteristics of energy-efficient physical layer protocols for environmental monitoring applications.

3.2. Energy-Efficient Routing Protocols. Energy-efficient routing is aimed at increasing the network lifetime by

Table 3: Characteristics of energy-efficient physical layer protocols.

Protocol	Standard	Power consumption	Security capability	Applications	Limitations	Range	Topology
Bluetooth	IEEE 802.15.1 (no more). The current standard is Bluetooth 5.3	Low (100 mW)	128-bit AES	Fire and disaster monitoring, food storage, greenhouse monitoring	Line of sight between communicating devices	1-10 m	Point-to-point
Zigbee	IEEE 802.15.4	Low (36.9 mW)	128-bit AES	Temperature and fire monitoring in underground mines, agriculture, cattle grazing, bee hives, and greenhouse monitoring	Line of sight between communicating devices	1-75 m and more	Mesh
LoRa	IEEE 802.15.4g	Low (100 mW)	AES CCm 128B	Greenhouse monitoring, voice detection techniques in farming, irrigation monitoring	Scalability, the maximum data rate of 250 kbps	2-5 km (urban) and 15 km (rural)	Star of stars
WiFi	IEEE 802.11a,b,g,n	High (835 MW)	128-bit AES	Air pollution, earthquake detection, temperature and humidity sensing, humiture and optical sensing	High power consumption, security, long access time (13.74 s)	100 m	Star
Sigfox	Sigfox	Low	Key generation, message encryption sequence	Water quality prediction, air quality monitoring, and optimum farming parameters	Mobility of nodes can only be deployed in a few countries, and communication is limited from the base station to the nodes	100 km	Star
NB-IoT	3GPP	Medium	NSA/AES 256	Water quality monitoring, air pollution, industrial environment	High power, high data rate		Star

considering the energy cost of the communication path. The routing protocols generally are categorised based on clustering, the mode of the protocol's functionality, the node's participation, and the network structure [20]. The general challenges for environmental monitoring include security, scalability, node deployment strategies, connectivity, and coverage. In mitigating these challenges, energy consumption is integral in implementing these solutions.

The challenges of WSN applications are diversified based on the application areas, which influences the routing protocols and quality-of-service parameters. For example, underwater communications in underwater wireless sensor networks (UWSN) use acoustic signals for propagation, unlike radio frequency (RF) signals that are used in terrestrial wireless sensor networks (TWSN). These acoustic signals are at lower magnitudes of 1500 m/s, five times lower than in TWSNs. Quality parameters such as delay are critical in acoustic mediums, which may be negligible for terrestrial environments. A centralised routing protocol, proposed by authors in [62], is based on a full-duplex communication that implements network management (gateway managers) and routing agents. These agents periodically probe the network for the statuses of the nodes to allow the gateways to determine a priori the optimum path between neighbouring nodes to avoid congestion for high traffic applications. Other protocols implemented in [63, 64] were based on water depth and temperature. Fire hazard monitoring applications require adaptive routing to ensure efficient real-time data delivery. The routing protocols for such emergency services include the real-time routing protocol with proposed load distribution [65] and improvement [66].

3.3. Energy-Efficient MAC Protocols. Using energy-efficient MAC protocols in WSN is aimed at meeting the challenges of general WSNs such as latency, throughput and fairness, channel utilisation, and scalability. Latency refers to the time it takes from a source node to reach the destination node. Its requirements in WSN are application dependent. The throughput is also a measure of successful data received by the destination node. Fairness here refers to the ability of the destination node to receive a fair amount of data from each sensor node in the network. Therefore, the MAC protocols ensure optimal results, with energy efficiency integral to its operations. To ensure energy efficiency, MAC protocols must overcome the challenges of multiple transmissions in the networks, such as energy losses due to control overheads, idle listening, collisions, and overhearing.

Environmental monitoring applications require MAC protocols that adapt to mission-critical applications. These applications require a quick response time. The applications may be deployed in inaccessible human environments. Hence, efficient energy management systems are needed to prolong the network lifetime. Examples include volcanic eruption-prone areas, surveillance applications,

environmental monitoring and control systems, and health care systems. The quality-of-service (QoS) parameters identified for MAC protocol implementation in any set of mission-critical system is similar and may be applied to other systems. ADMC-MAC is a mission-critical MAC protocol using regression techniques to decide the duty cycle of sensor nodes [67].

4. Energy Harvesting-Based Protocols

The slow development in battery technologies makes energy harvesting (EH) a viable solution to the energy challenge in environmental monitoring protocols. Using energy harvesting in environmental monitoring hampers the destruction of environmental pollution from the disposal of batteries. Energy harvesting is increasingly becoming important in IoT implementations due to the massive number of sensor nodes deployed for some applications, primarily working for long periods without human interferences.

Energy challenges like traditional WSN applications may not constrain energy harvesting due to energy availability. Some identified EH sources in environmental monitoring include sunlight, vibration, sound, wind, thermal, electromagnetic waves, and body heat and movement. Hence, some applications apply architectures such as mobile, stationary, or hybrid. They may also be classified as single-tier, multitier, or homogeneous [68]. Sources like solar energy, commonly used in many applications, use the photovoltaic energy harvesting approach. In photovoltaic energy harvesting, solar light energy is converted into electrical energy to recharge the batteries of WSN nodes. The highest energy conversion for outdoor solar energy harvesting was $15\,mW/cm^2$ and an efficiency of about 30%. It is the preferred renewable energy source. It is primarily available in the environment where sensor nodes are deployed and have the highest energy conversion efficiency. Solar energy harvesting does not pollute the environment but requires little preservation and may be stored for several years. Solar harvesters may be deployed in applications that include agriculture (farms), forest monitoring, greenhouse monitoring, and animal monitoring. Recently, commercial applications have been deployed by Crossbow Inc. USA, using Mote View 2.0 for measuring parameters such as temperature, humidity, pressure, acceleration, and light. The application uses the Zigbee protocol for communication with an expandable distance of 100 m to 1.5 km. An example of implementation was discussed in the survey by authors in [69] which reviewed the literature on solar energy harvesting WSN (SHE-WSN).

A smart agricultural application simulated by the authors in [70] is intended to extend the network lifetime using solar energy harvesting. Using similar tools described by Sharma et al., the lifetime of nodes deployed on a farm was extended from 5.75 days when energy harvesting was not implemented to 115.75 days. With an increase in throughput of 160 kbits/s from 100 kbits/s, the duty cycle of these sensor nodes could be adjusted upwards to more than 25% (which is a message transmitted every 4 s) since energy is no longer the main challenge of these networks. The network setup consists of MICAz WSN nodes deployed at fixed locations in a mapped-out area on a smart farm. Sensor nodes are connected to a gateway/base station powered by the main supply. Sensor nodes transmit their data to relays through multihop transmits for forwarding to the gateway. The network supports bidirectional communication from the gateway directly with the deployed sensor nodes.

For a comprehensive review of up-to-date energy harvesting WSNs (EH-WSN), the reader may refer to [14] for references. An energy harvesting–based clustering protocol is proposed by authors in [71] to improve network stability and efficiency. Their approach includes the selection of the cluster head for each cluster based on the node's energy level, the amount of energy harvested, and the number of its neighbours. The leach-based clustering protocol uses a lower threshold of 0.1 J and a higher threshold of 1 J to compete in the cluster head selection. Other protocols implementing prediction models that may be difficult in WSN are made possible due to energy harvesting. Weather forecasting-based applications include implementations in IproEnergy [72], autoregressive (AR) models [73], ARIMA models [74], and reinforcement learning applications using Q-learning [75].

Mechanical kinetic energy harvesting converts mechanical motions and vibration harnessed from the environment into electrical energy. This energy source is self-power sensing, convenient, energy-saving, sustainable, and eco-friendly. It is applied in aerospace, biomedical engineering, and military and environmental monitoring applications [76]. However, mechanical energy has few implementations in WSN due to low conversion efficiency, low power output, and conversion being time-dependent and may even cause damage to the device. It requires unique modulation of the energy source to harness the energy from the ambient environment. Applications depending on mechanical include structural condition monitoring, smart devices and cities, biomedical and wearable devices, and machine monitoring. Biomass, which converts organic materials from plants and animals, has seen applications in WSNs where devices deployed in unreachable locations harvest energy from organic ambient sources. Examples of sources include corn, soyabeans, woody plants, paper, cotton, food, wood wastes, and animal and human sewage. Authors in [77] harvested energy from switchgrass, while authors in [78] mentioned the extraction of Xenopus oocytes from female frogs to power capacitors in their application.

5. Environmental Monitoring Application Design Requirements

Environmental monitoring applications are different in many ways. Some of the applications are dynamically deployed, and others are statically deployed. In dynamic deployments, the nodes are primarily mobile, and in static deployments, the nodes are positioned at various points in the environment. In each of these deployments, the design requirements may differ. Also, environmental monitoring applications are characterised by energy efficiency, network

complexity, scalability, data transmission, bandwidth, and processing storage. These characteristics are critical design criteria considered in EMAs. Different topologies associated with the various applications determine the routing and MAC protocols employed for the energy-constrained sensor node. Efficient routing protocols schedule routes efficiently to minimise the amount of energy consumed by the nodes to prolong the lifetime of the sensor network. With efficient routing, gains are made in data communication. MAC layer protocol requirements such as duty cycling, slot scheduling, time synchronisation, node prioritisation, and efficient channel utilisation improve performance and increase network lifespan. MAC protocol implementation in WMAs achieves high reliability, effective scheduling, and efficient time synchronisation in EMAs [79].

5.1. Quality-of-Service Requirements. Quality of service (QoS) guarantees that the network provides the expected results. In WSNs for EMAs, there are essential parameters that the application may be designed to achieve. These QoS parameters include throughput, delay, packet delivery ratio, and energy consumption. For example, in forest fire monitoring, the nodes are deployed to access real-time data and remotely acquire data from forest zones for decision-makers to make decisions based on the data received from the sensor nodes. The sensor nodes report any unusual temperature, smoke, oxygen levels, and humidity that may be collected to mitigate forest fires. Collecting and studying event data from the forest employ sensors that may trigger alarms, calculate and track humidity levels and temperature variations, and detect smoke patterns. From such sensor networks, throughput and data reliability are essential. Also, measuring delay is crucial because the different sensors may collect the data in specified periods. This means that delays in sensor data reporting may cause forest fires. The sensor nodes' energy efficiency will optimise network performance and uptime. For example, in forest fires, sensor nodes must operate in the forest for a long time. Therefore, efficient energy consumption or low energy consumption of the sensor nodes' energy will make the node live longer. Energy-aware sensor network architecture (SNA) techniques are paramount in such networks [80]. Therefore, protocols designed at the various layers must be energy-aware to enhance the overall network lifetime.

5.2. Topology Requirements. WSN network topology is the physical or logical placement or arrangement of sensor nodes in an observed area of interest. It also includes how sensor nodes communicate within the network to collect data from the environment and transmit it to a base station via a sink node [81]. Topology requirements in WSN for EMAs vary depending on the environment and application. Network topologies are typically application-specific, and the structure serves as an essential foundation in EMAs [82]. Network topologies must be designed to balance the energy consumed by sensor nodes while the network lifetime is maximized. The topology of a network can directly impact its performance [83].

WSN topologies such as basic peer-to-peer, linear, star, tree, a cluster tree, or mesh are used in EMAs to monitor and set up the sensor network. Sensor nodes may be deployed remotely at an area of interest to acquire data wirelessly using one WSN topology to monitor agriculture, the environment, or water resources. Topologies can be built either statically or dynamically. Several sensor nodes can freely move in dynamic topologies in some application domains (for example, water quality monitoring and oceanography). The topology can self-organize when individual sensor nodes fail or deplete their energy. In dynamic topologies, when new nodes are added to the network after some nodes fail, the identity of the new node enters the network without changing the topology [81].

In WSNs for EMAs, the transmission power of the nodes determines the network topology, which directly impacts network performance [82]. The network topology in EMAs can be designed to accommodate mobile or static sensor nodes and a sink. Mobile nodes in a sensor network are typically designed to deal with the dynamic network topology required for node mobility. Because node mobility in WSNs makes the topology dynamic, the communication protocol becomes more complicated, necessitating more processing resources and energy. The network topology may generate minimal heavy traffic load depending on the network size and application domain (animal tracking, water quality, oceanography, fire monitoring). The sensor node in an EMA must be able to reconfigure itself for different network topologies (such as star and tree topology). All sensor nodes directly communicate with the sink node in the star topology. Most sensor nodes in a tree or mesh communicate with neighbours to maintain connectivity with the sink node [84].

EMAs' network topology requirements should consider the number of nodes and the distance between neighbour nodes to determine node placement density, network diameter, and coverage. The minimum number of data relays between sensor nodes is used when packets are transmitted between nodes in the network [85]. Researchers developing applications to monitor the environment must consider network topology requirements because network functionality and stability are critical to meeting application objectives. To determine the type of topology, it is also necessary to consider the traffic load density. Network topologies should be well-designed to be fault-tolerant, reconfigurable, energy-efficient, and scalable [86].

6. WSN Security Approaches for EMAs

WSN application security is a complex problem to solve. It requires finding the best method to maximize network performance while dealing with complex restrictions. The goal is to find a reasonable balance between efficiency, energy efficiency, and routing protocol design. Wireless sensor networks (WSNs) are being utilised for various applications, including environmental monitoring applications (EMAs), like a new computer and network infrastructure platform, and operational security is a significant problem. Security issues in WSN for EMAs are more concerned with the reliability of the network, positioning of the nodes

Table 4: Security attacks at the layer(s) on the OSI model.

Network layers	Security attacks	Effects of network/node	Defense mechanism
Application	Message corruption, DoS, disrupt or intercept confidential data	Increases packet reception time Reduces data reliability	Firewalls and the use of antiviruses
Transport	Session hijacking, DoS	Degradation of energy Fake packets are injected Data integrity, availability, and authenticity are affected	Provision of authentication Reducing packet response rate
Network	Wormhole, blackhole, sinkhole, Sybil, selective forwarding, spoofing, altered or replayed routing information, internet smurf	Continuous request to send packets floods the network Generation of false messages Creation of routing loops Causes selective forwarding	Encryption Authorisation Probing Monitoring firewalls
Data link	Traffic analysis, HELLO flood, monitoring, channel exhaustion, 802.11 disruptions (MAC)	Retransmission of data The decreased energy level of the sensor node Nodes may miss the transmission Degradation in network performance	Error correction Use of virtual private networks Reprogramming senor devices
Physical	Jamming, node malfunctioning, node destruction, tampering (direct node attack), DoS, radio interference, interception	Corrupts or sends a large number of packets Sensor node physically tampered Addition of other sensor nodes Network services get stopped (data collection) Network energy is exploited	Hiding Region mapping Spread-spectrum techniques such as DSSS and FHSS

(localization), and the topological characteristics that may affect data collection, data processing, and increased delay in the network [18, 87].

In WSNs, a security attack is defined as any attempt to expose, steal, manipulate, modify, or obtain unauthorised access to information in the sensor network [87]. A wireless sensor network is highly vulnerable to attacks because the sensor nodes are physically unprotected. In WSN, there are two types of attacks: active and passive. The attackers just monitor the communication channel in a passive attack, but they modify the data stream in an active attack. Passive attacks include eavesdropping, node dysfunction, node destruction, and traffic analysis. Active attacks occur when an adversary attempts to disrupt the operation of the network under attack. Active attacks include denial-of-service (DoS), sinkhole attacks, flooding, and Sybil. At various tiers of the network, many attacks exist. The attackers aim to exploit the nodes directly at the physical layer. Jamming is a denial-of-service attack in which the victim's computer's functions are disrupted. There are various attacks at various layers of the network. Table 4 presents security attacks at the layers on the OSI model. At the physical layer, attackers attempt to exploit the nodes physically. Physical layer threats put data availability, integrity, and confidentiality at risk. The data link layer is responsible for framing, addressing, error correction, and flow control. At this layer, a variety of attacks may occur. When two separate nodes send data on the same frequency, the packet's data varies by a small amount. As a result, the packet becomes unusable, and the data is deleted. An attacker may cause these collisions [5, 87].

For communication, many networks employ a two-way handshake. An attacker can make a constant request to send the packet. The network link may be flooded as a result. Interrogation is the term used to describe this type of attack. The network layer handles packet routing from one node to another. Several attacks at this layer in wireless sensor networks take advantage of the routing mechanism. In WSNs, the transport layer ensures that the entire message is delivered in the exact sequence. At this level, some attacks can be made. New connection requests are produced repeatedly in floating till the resources reach their maximum capacity.

To develop secure WSNs, application designers must consider security objectives (integrity, availability, authorisation, authentication, and confidentiality). Data integrity ensures that data is not tampered with by unauthorised parties. Data availability ensures that authorised system stakeholders have immediate and unrestricted access to the system's and network's resources. The most critical aspect of security is availability. The authority to access the data is primarily concerned with maintaining the confidentiality of the information. Authentication requires genuine access to sensor nodes and the network by application designers throughout implementation. The sensor nodes must provide authorised data to stakeholders while operating the network [5]. Encryption techniques are used to protect the privacy of system resources and operations. As a result, data confidentiality is conditional on a certain level of information [88].

6.1. Types of Security Threats in EMAs. Security targets in WSNs for EMAs apply to the wireless medium between sensor nodes, and the sensor devices are susceptible to attacks and vulnerabilities. The environmental monitoring applications are designed to achieve specific objectives. Some applications such as water quality, air quality, animal tracking, and forest fire are life-threatening, endangering the lives of humans and animals. They require essential security measures to ensure that the nodes remain operational 100% of the time. Security attacks of the sensor nodes may cause the nodes to malfunction, disrupt the network, and

Table 5: Description of various security threats.

Attack	Description
Denial of service (DoS)	This attack overflows the network with traffic, utilises more bandwidth, and causes services or resources to become unavailable to the user. This type of attack is most common in all WSN applications. It is aimed at interrupting the system, making it unavailable or unusable, which attacks its availability and efficiency.
Selective forwarding	In this situation, the attacker installs a malicious node which masquerades as a genuine node, which may refuse to forward or simply discard specific messages. This jeopardises the availability and integrity of system data.
Sinkhole	This exploits the network by adding a node that collects all data as though it were the base station. This threatens the confidentiality of the system where applicable.
Sybil attack	In this case, the compromised node assumes several identities (creating the illusion of being present in multiple locations) to connect with a large number of nodes. This poses a risk to the network's confidentiality.
Wormhole	The attack records the information to a different location before transmitting it or a portion of it. This is a threat to data integrity.
HELLO flood	The HELLO packet is transmitted to the nodes, and the attacked device may be misidentified as a neighbour seeking to communicate with it. Its objective is to use network resources. The availability of network resources is jeopardised as a result.
Spoofed, altered, or replayed routing information	This is a more direct attack whereby the attacker can wreak havoc on the network by sending falsified error messages or establishing routing loops. This compromises the network's integrity and availability.
Blackhole	With this attack, the targeted node is forced to transmit the reply to the malicious node by providing fake route information. This disrupts availability.
Node destruction	This attack seeks to either disable the node so that a compromised node with the same identifier may take its place or prohibit it from gathering data.
Monitor and eavesdropping	The goal of this exploit is to obtain network information. This jeopardises confidentiality.
Traffic analysis	The goal is to capture and analyse messages to derive information from communication patterns. Its threat stems from its capacity to function even when data are encrypted and compromised confidentiality.
Node replication	This attack duplicates nodes and uses them to set up multiple attacks.
Message corruption	This attack takes three significant steps: it accepts a message, alters it to make it incomprehensible, and finally sends it to its intended recipient—the integrity and availability of data are being compromised.
Jamming	Jamming disrupts the sensor nodes' RF signals, rendering them inoperable and compromising availability.
Node malfunctioning	Node malfunctioning creates erroneous data that might jeopardise the integrity of the cluster heads' data-aggregation process.

introduce delays in data communication, halting the monitoring process and degrading the overall quality of service. Table 5 illustrates the attacks and descriptions of the various security threats.

Also, when the sensor nodes and network are attacked, the attackers may reprogram the nodes to transmit false data readings, which may endanger the lives of humans and animals.

Attackers may also cause the sensor nodes to continuously send packets until they are exhausted, drain their energy, and die. Table 6 depicts some common types of attacks and the environmental monitoring application they affect, which an attacker may exploit to render the sensor network inefficient affecting its intended use.

6.2. Node and Network Security Approaches in Environmental Monitoring Applications. This paper has established that wireless sensor networks (WSNs) have minimal operational energy, limited memory capacity, and constrained computing abilities. These nodes can sense, record, and monitor environmental conditions. The sensor node and the sensor network have a lot of practical uses, but they are also challenged with several deployment problems of which security is paramount. The node is deployed in hostile environments, making them physically vulnerable to attacks (adversaries and natural disasters). When sensor nodes are deployed in hostile environments, the kind of topology formed because of the node depleting its energy or being damaged by animals is unclear. The section examines different security approaches suitable for specific operations in WSNs for EMAs. Some data gathered from sensor nodes in EMAs may be sensitive. Hence, there is a need to safeguard the node, network and sensed data to prevent any attack or tampering. The data obtained from the sensor nodes and transferred to a base station require levels of authorisation and authentication to access it. These security

Table 6: Threats in environmental applications.

Threat	Animal tracking	River/ocean monitoring	Forest fire detection	Air quality	Precision agriculture	Earth/ landslide	Active	Passive
Denial of service	×	×	×	×	×	×	×	
Selective forwarding		×	×	×	×	×		×
Sinkhole	×		×	×	×	×	×	
Sybil			×	×		×	×	
Wormhole		×	×	×	×	×	×	
HELLO flood	×	×	×	×	×	×		×
Spoofed, altered, or replayed routing information	×			×	×		×	
Blackhole	×		×		×	×	×	
Node destruction	×	×	×	×	×	×	×	
Monitor and eavesdropping	×	×		×	×			×
Traffic analysis	×				×		×	
Node replication	×		×	×	×	×	×	
Message corruption	×	×	×	×	×	×	×	
Jamming	×	×	×	×	×	×	×	
Node malfunction	×	×	×	×	×	×	×	

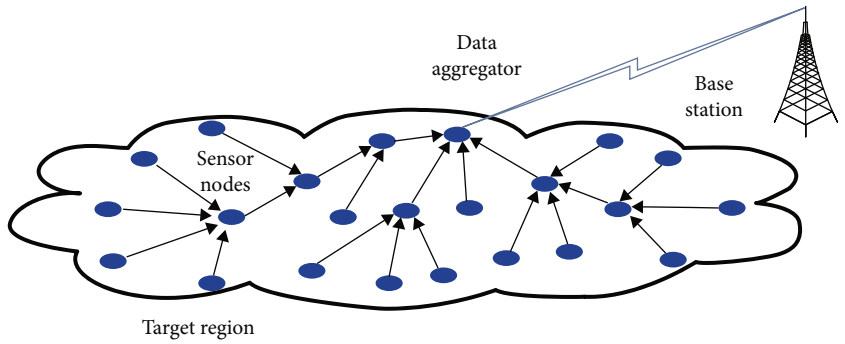

Figure 9: Data aggregation in a wireless sensor network (adapted from [92]).

levels will prevent unauthorised data from getting into the hands of the wrong users [89].

6.2.1. Secure Data Aggregation. The sensor nodes in EMAs collect enormous amounts of data. The sensed data must be aggregated to avoid overload at the base station. As illustrated in Figure 9, data aggregation is how sensed data is processed and combined en route by intermediary sensor nodes. In a typical WSN, many sensor nodes gather application-specific data from the environment and transfer it to a centralized base station for processing, analysing, and use by the application [90]. The basic strategy is to analyse data from multiple sensor nodes as transmitted collectively. The plain text sensed by the deployable environment's nodes may be encrypted before being transferred to the base station. For example, water quality data such as pH or dissolved oxygen sensed by nodes deployed in a river is encrypted after sensing and transmitted to the base station. Before data aggregation operations can be performed on the data, the encrypted water quality data is decrypted at the base station [91, 92]. In real-time applications, data aggregation occurs to prevent false alarms. Data can be aggregated within a node, across a network, at the sink, or the base station. All of these data collection points require some level of security. Where sensitive data is being collected, as in military deployments, encryption may be needed to prevent data from being read and compromised by adversaries [93].

6.2.2. Access Control. Access control is a security strategy that governs who has access to and uses resources in a computing environment. It is a fundamental security concept used to mitigate risk. The two types of access control are physical and logical access control. Physical access control is used to restrict access to physical IT assets. Logical access control governs all communication systems, files, and data connections. Nodes are fixed or mounted on endangered species (for example, turtles) in animal tracking applications to track their movements. Physical access to the nodes is impossible while the animals are in motion. Still, logically, the algorithms or protocols are accessible to researchers who track the position of the animals and all data residing on the node. This could be applied to the battlefield, forest

fire, and water resource monitoring. Farmers can have physical and logical control over agricultural monitoring and use the necessary security at each level to provide the restrictions required for the device and the data [94].

6.2.3. Secure Routing. Nodes in WSNs for environmental monitoring communicate to transfer data from one node to another. Data exchange between nodes necessitates a secure pathway to avoid data compromise. Because nodes in a WSN route packets over multiple paths, secure routing techniques must be used to secure the route. Secure routing is a set of transport and network security controls that apply to routing protocols and individual nodes. However, to establish the network architecture (reactive, proactive, or hybrid), nodes must communicate with their peers to use one of the routing protocols. Safe routing and secure data forwarding are two approaches to routing security used in EMAs. Secure routing necessitates node collaboration to share accurate routing information and keep the network connected. Secure data forwarding requires the protection of data packets from corruption, dropping, and manipulation by an untrusted source.

6.2.4. Secure Localization. The positional information of nodes mounted on animals and floating in water sources is critical in mobile-based sensor deployments such as animal tracking and water quality monitoring. For example, in the case of animal tracking, the location of endangered species such as turtles, elephants, and others will provide information. Localization computes the location or position of sensor nodes in WSNs. Because of the dynamic nature of the applications, WSN deployment has shifted from static to dynamic (mobile). Because such networks are dynamic, node localization is also variable, making the process critical in WSNs. Knowledge of a network entity's physical location is useful in various applications. The primary factor in location determination is a group of particular nodes known as anchor/beacon nodes, which are resource privileged and have more excellent storage and computing capacity. Other unknown nodes calculate their position in various ways based on the location of anchor/beacon nodes. As a result, malicious anchor/beacon nodes must be prevented from providing false location information, as unknown nodes rely entirely on them to compute their position [95].

6.2.5. Cryptographic Algorithms. The communication infrastructure (radios in the network) in WSNs for EMAs may also be compromised. If the radio is compromised, it will no longer be able to securely communicate the data obtained from the sensor nodes. Furthermore, the data obtained from the sensor nodes may necessitate additional security at the base station and backup systems if the base station is attacked. As a result, using cryptographic algorithms to provide the desired security is critical. Cryptographic algorithms are methods and procedures for securing a system linked with keys. The crypto security of an environmental monitoring application against attacks and malicious infiltration can be defined by two factors: (1) the strength of the keys and the efficiency of procedures and protocols associated with the keys and (2) the protection of the keys through key management (secure key generation, storage, distribution, use, and destruction). Poor algorithms embedded in a robust key management framework are just as likely as good algorithms embedded in a weak key management framework to fail. Data encryption, authentication, and digital signatures are tasks that require using cryptographic algorithms [96].

6.3. Challenges of WSNs for EMAs. Wireless sensor networks' intense constraints and demanding application environments make computer security for such systems more complicated than traditional networks. Some challenges, like most systems, have a negative impact on the system's operations and resources. WSNs are not immune to challenges, particularly in terms of security. Wireless communication is less secure due to its distributed nature, allowing easy interception. An adversary can easily intercept, change, or rerun any message. An attacker can easily intercept legal packets and inject malicious ones [97].

6.3.1. Constrained Resources. A constrained resource is one in which you have a finite supply. Sensor nodes in WSNs are subject to resource constraints such as limited power, restricted communication bandwidth, limited processing capability, and limited storage capacity due to their varying sizes and cost. Wireless channels in the network are typically unstable when sensor data is shared among nodes or transferred for data processing, resulting in unpredictable transmission delays and packet losses. Energy constraints, for example, require strategies to save energy to enable nodes to operate for a longer time since sensor nodes mainly rely on batteries. The deployment type also affects the communication and connectivity between nodes in the network. This challenge also requires optimal node deployment schemes to ensure effective communication among the nodes in the network in EMAs.

6.3.2. Node Failure. Sensor nodes are the main components of the wireless sensor network for environmental monitoring applications. They operate unattended and are capable of adapting to their deployable environment. Due to its size, it comes with stringent energy requirements because, on most occasions, the nodes are not inaccessible to humans. Hence, its battery and other hardware cannot fail to operate since monitoring will not be possible. Sensor nodes comprise sensing, energy, transceiver, and processing units. The node fails to operate if any of these components fail, affecting the overall network's operation. In EMAs, node failure means no sensing can occur, and there will be an optimal communication medium [93].

6.3.3. Network Converge and Fault Tolerance. Typically, sensor nodes fail because of a lack of power, physical harm, or environmental interferences, and such failures should not impact the WSN's intended mission. Fault tolerance refers to a WSN's capacity to maintain sensor functionality in the face of node failures. Fault-tolerance protocols and algorithms must be designed to handle their specified performance levels. For example, tolerance can be minimal in a

house, but tolerance levels must be quite high for environmental monitoring to maintain operation [98].

6.3.4. Data Privacy. Data privacy is the ability to control when, how, and to what extent data or information is shared or divulged to others. WSNs in EMAs, like most data systems, collect sensitive information, necessitating the need to protect its privacy, which in turn protects its confidentiality. However, the data collected by the sensors can be obtained by an attacker using a powerful receiver, resulting in a privacy breach [99]. Furthermore, a hacker can quickly introduce harmful messages into the network by using wireless communication, allowing easy eavesdropping and potentially breaching data privacy.

6.3.5. Location and Positioning of Nodes. Localization techniques are critical in applications such as animal tracking, where the location of the animals at a given time is required, particularly in the case of endangered species. Localization is a technique used in WSNs for EMAs to determine the location of sensor nodes. WSNs are thousands of tiny nodes, making GPS installation on each sensor node impractical. Furthermore, even when GPS is installed on sensor nodes, it does not provide ideal localization results. Establishing location references on each sensor node in a dense network is practically impossible [100]. It thus creates a problematic situation in which the sensor nodes must define their current position without the support of any special equipment such as a global positioning system.

6.3.6. Propagation Delay. The nodes in EMAs are strategically placed throughout the deployment area to achieve detection and identification probabilities close to 100% for specified parameters [101]. However, even when the nodes detect the required parameters, propagation delays affect their transmission during in-node or in-network communication and a node sink communication. The propagation delay is the time it takes packets to travel through the transmission medium and is limited by the speed of light. For example, if the source and destination are both in the same deployment area or region but are 100 meters apart, the propagation delay can be estimated to be 1 microsecond. If they are separated by 500 meters in a different deployment environment, the delay can be estimated to be 0.1 seconds [102]. Factors influencing node propagation with underwater nodes differ from those influencing node propagation with tracking animals on land in environmental monitoring applications. As a result, the number of packets transmitted between the source and destination nodes may vary depending on the environment and channel conditions. Delays in packet transmission have serious consequences for WSNs used in environmental monitoring applications that require a response time of fewer than 200 milliseconds. When the propagation delay exceeds the threshold in such applications as forest fire monitoring, battlefield, and freshwater quality, it may affect stakeholders' decisions to avoid the effects if no such delays occur.

7. Conclusion

The applications of WSN technology for environmental monitoring have been discussed in this paper. The paper reviewed vital protocols used in WSNs for EMAs, focusing on some protocols in the WSN protocol stack. Given the importance of security in environmental monitoring applications, this review discussed wireless sensor network routing protocols, security implementations, the types of security threats in environmental monitoring applications, node and network security practices, and some suggested WSN challenges for EMAs. Researchers interested in designing protocols at the physical, data link, and network layers should consider the type of applications and the associated peculiarities. The paper also examines some essential protocols researchers use to track animals, water quality, and forest health.

Data Availability

No data is available.

Conflicts of Interest

The authors declare that there is no conflict of interest regarding the publication of this paper.

Acknowledgments

This work was funded in part by the BANGA-AFRICA, University of Ghana, under the Seed Research Grant UG-BA/SRG-001/2022.

References

[1] K. S. Adu-Manu, C. Tapparello, W. Heinzelman, F. A. Katsriku, and J.-D. Abdulai, "Water quality monitoring using wireless sensor networks," *ACM Transactions on Sensor Networks*, vol. 13, no. 1, pp. 1–41, 2017.

[2] W. Honghui, T. Xianguo, L. Yan et al., "Research of the hardware architecture of the geohazards monitoring and early warning system based on the IoT," *Procedia Computer Science*, vol. 107, pp. 111–116, 2017.

[3] B. Jiang, G. Huang, T. Wang, J. Gui, and X. Zhu, "Trust based energy efficient data collection with unmanned aerial vehicle in edge network," *Transactions on Emerging Telecommunications Technologies*, vol. 33, no. 6, article 3942, 2020.

[4] S. Bader, *Enabling autonomous environmental measurement systems with low-power wireless sensor networks terms with low-power wireless sensor networks, [Ph.D. thesis]*, Mid Sweden University, Faculty of Science, Technology and Media, Department of Information Technology and Media, Sweden, 2011.

[5] M. Keerthika and D. Shanmugapriya, "Wireless sensor networks: active and passive attacks - vulnerabilities and countermeasures," *Global Transitions Proceedings*, vol. 2, no. 2, pp. 362–367, 2021.

[6] M. Almazaideh and J. Levendovszky, "Novel reliable and energy-efficient routing protocols for wireless sensor networks," *Journal of Sensor and Actuator Networks*, vol. 9, no. 1, 2020.

[7] F. Engmann, K. S. Adu-Manu, J.-D. Abdulai, and F. A. Katsriku, *Applications of prediction approaches in wireless sensor networks*, IntechOpen, London, 2021.

[8] H. M. A. Fahmy, "Energy harvesting projects for WSNs," in *Wireless Sensor Network*, Springer, Cham, 2020.

[9] M. Y. Arafat, M. A. Habib, and S. Moh, "Routing protocols for UAV-aided wireless sensor networks," *Applied Sciences*, vol. 10, no. 12, p. 4077, 2020.

[10] I. Daanoune, B. Abdennaceur, and A. Ballouk, "A comprehensive survey on LEACH-based clustering routing protocols in wireless sensor networks," *Ad Hoc Networks*, vol. 114, article 102409, 2021.

[11] Y. Jia, "LoRa-based WSNs construction and low-power data collection strategy for wetland environmental monitoring," *Wireless Personal Communications*, vol. 114, no. 2, pp. 1533–1555, 2020.

[12] O. I. Khalaf and G. M. Abdulsahib, "Energy efficient routing and reliable data transmission protocol in WSN," *International Journal of Advances in Soft Computing and Its Applications*, vol. 12, no. 3, pp. 45–53, 2020.

[13] V. Pandiyaraju, R. Logambigai, S. Ganapathy, and A. Kannan, "An energy efficient routing algorithm for WSNs using intelligent fuzzy rules in precision agriculture," *Wireless Personal Communications*, vol. 112, no. 1, pp. 243–259, 2020.

[14] K. S. Adu-Manu, N. Adam, C. Tapparello, H. Ayatollahi, and W. Heinzelman, "Energy-harvesting wireless sensor networks (EH-WSNs)," *ACM Transactions on Sensor Networks (TOSN)*, vol. 14, no. 2, pp. 1–50, 2018.

[15] F. Engmann, F. A. Katsriku, J.-D. Abdulai, and K. S. Adu-Manu, "Reducing the energy budget in WSN using time series models," *Wireless Communications and Mobile Computing*, vol. 2020, Article ID 8893064, 15 pages, 2020.

[16] A. Kochhar, P. Kaur, P. Singh, and S. Sharma, "Protocols for wireless sensor networks: a survey," *Journal of Telecommunications and Information Technology*, vol. 1, no. 2018, pp. 77–87, 2018.

[17] K. Sohraby, D. Minoli, and T. Znati, *Wireless sensor networks: technology, protocols, and applications*, John wiley & Sons, United States, 2007.

[18] M. Elhoseny, A. E. Hassanien, M. Elhoseny, and A. E. Hassanien, "Secure data transmission in WSN: an overview," *Studies in Systems, Decision and Control*, vol. 165, pp. 115–143, 2019.

[19] J. Yang, *Design and implementation of large-scale wireless sensor networks for environmental monitoring applications*, University of North Texas, United States, 2010.

[20] A. Sarkar and T. Senthil Murugan, "Routing protocols for wireless sensor networks: what the literature says?," *Alexandria Engineering Journal*, vol. 55, no. 4, pp. 3173–3183, 2016.

[21] B. Abidi, A. Jilbab, and M. E. Haziti, "Routing protocols for wireless sensor networks: a survey," in *Advances in Ubiquitous Computing*, pp. 3–15, Academic Press, United States, 2020.

[22] N. Shabbir and S. R. Hassan, "Routing protocols for wireless sensor networks (WSNs)," in *Wireless Sensor Networks - Insights and Innovations*, Intecopen Science, 2017.

[23] S. Arjunan and P. Sujatha, "Lifetime maximization of wireless sensor network using fuzzy based unequal clustering and ACO based routing hybrid protocol," *Applied Intelligence*, vol. 48, no. 8, pp. 2229–2246, 2018.

[24] U. Draz, A. Ali, M. Bilal et al., "Energy efficient proactive routing scheme for enabling reliable communication in underwater Internet of Things," *IEEE Transactions on Network Science and Engineering*, vol. 8, no. 4, pp. 2934–2945, 2021.

[25] D. Kothandaraman, S. Naik Korra, A. Balasundaram, and S. Magesh Kumar, "Sequence number based secure routing algorithm for IoT networks," *Materials Today: Proceedings*, 2021.

[26] F. Tabbana, "Performance analysis of AODVDSDV and ZRP routing protocols," *Wireless Sensor Networks using NS2 Tool*, vol. 10, pp. 279–297, 2020.

[27] K. S. Adu-Manu, F. Katsriku, J.-D. Abdulai, J. M. Gómez, and W. Heinzelmann, "Network lifetime maximization with adjustable node transmission range," in *Smart Cities/Smart Regions–Technische, wirtschaftliche und gesellschaftliche Innovationen*, pp. 693–707, Springer Vieweg, Wiesbaden, 2019.

[28] O. A. Osanaiye, O. O. Ogundile, and F. Aina, "Evaluating DoS jamming attack on reactive routing protocol in wireless sensor networks," *African Journal of Science, Technology, Innovation and Development*, pp. 1–8, 2021.

[29] P. Sarao, "Ad hoc on-demand multipath distance vector based routing in ad-hoc networks," *The Journal of Communication*, vol. 14, no. 4, pp. 2953–2953, 2019.

[30] L. Chan, K. Gomez Chavez, H. Rudolph, and A. Hourani, "Hierarchical routing protocols for wireless sensor network: a compressive survey," *Wireless Networks*, vol. 26, no. 5, pp. 3291–3314, 2020.

[31] A. K. Singh, A. Bhalla, P. Kumar, and M. Kaushik, "Hierarchical routing protocols in WSN: a brief survey," in *2017 3rd International Conference on Advances in Computing, Communication & Automation (ICACCA)(Fall)*, pp. 1–6, Dehradun, India, September 2017.

[32] K. Haseeb, N. Islam, A. Almogren, I. U. Din, H. N. Almajed, and N. Guizani, "Secret sharing-based energy-aware and multi-hop routing protocol for IoT based WSNs," *IEEE Access*, vol. 7, pp. 79980–79988, 2019.

[33] A. Ghaffari and H. R. Bannaeian, "QoS-based routing protocols for wireless sensor networks: a survey," *World Applied Sciences Journal*, vol. 14, no. 6, pp. 866–875, 2011.

[34] R. Zagrouba and A. Kardi, "Comparative study of energy efficient routing techniques in wireless sensor networks," *Information*, vol. 12, no. 1, p. 42, 2021.

[35] J. N. Al-Karaki and A. E. Kamal, "A taxonomy of routing techniques in wireless sensor networks," in *Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems*, pp. 116–139, CRC Press, 2004.

[36] F. Lakrami, N. Elkamoun, and M. E. Kamili, "Advances in ubiquitous networking," *Lecture Notes in Electrical Engineering*, vol. 366, pp. 287–300, 2016.

[37] B. Bhushan and G. Sahoo, "Routing protocols in wireless sensor networks," *Studies in Computational Intelligence*, vol. 776, 2019.

[38] J. J. Cancela, M. Fandiño, B. J. Rey, and E. M. Martínez, "Automatic irrigation system based on dual crop coefficient, soil and plant water status for *Vitis vinifera* (cv Godello and cv Mencía)," *Agricultural Water Management*, vol. 151, pp. 52–63, 2015.

[39] M. Usha Rani and S. Kamalesh, "Energy efficient fault tolerant topology scheme for precision agriculture using wireless

sensor network," in *2014 IEEE International Conference on Advanced Communications, Control and Computing Technologies*, pp. 1208–1211, Ramanathapuram, India, May 2014.

[40] M. Gameil and T. Gaber, "Wireless sensor networks-based solutions for cattle health monitoring: a survey," in *International Conference on Advanced Intelligent Systems and Informatics*, pp. 779–788, Springer, Cham, 2020.

[41] B. Sharma and D. Koundal, "Cattle health monitoring system using wireless sensor network: a survey from innovation perspective," *IET Wireless Sensor Systems*, vol. 8, no. 4, pp. 143–151, 2018.

[42] Y. Liu and C. Bi, "The design of greenhouse monitoring system based on ZigBee WSNs," in *2017 IEEE international conference on computational science and engineering (CSE) and IEEE international conference on embedded and ubiquitous computing (EUC)*, pp. 430–433, Guangzhou, China, 2017.

[43] Z. Yiming, Y. Xianglong, G. Xishan, Z. Mingang, and W. Liren, "A design of greenhouse monitoring & control system based on ZigBee wireless sensor network," in *2007 International Conference on wireless communications, networking and Mobile computing*, pp. 2563–2567, Shanghai, China, September 2007.

[44] T. Hidayat, R. Mahardiko, and S. T. D. Franky, "Method of systematic literature review for Internet of Things in ZigBee smart agriculture," *2020 8th International Conference on Information and Communication Technology, ICoICT*, 2020, pp. 20–23, Yogyakarta, Indonesia, 2020.

[45] S. Cecchi, S. Spinsante, A. Terenzi, and S. Orcioni, "A smart sensor-based measurement system for advanced bee hive monitoring," *Sensors*, vol. 20, no. 9, p. 2726, 2020.

[46] L. Joris, F. Dupont, P. Laurent, P. Bellier, S. Stoukatch, and J. M. Redoute, "An autonomous Sigfox wireless sensor node for environmental monitoring," *IEEE Sensors Letters*, vol. 3, no. 7, pp. 01–04, 2019.

[47] S. Gil-Lebrero, F. J. Quiles-Latorre, M. Ortiz-López, V. Sánchez-Ruiz, V. Gámiz-López, and J. J. Luna-Rodríguez, "Honey bee colonies remote monitoring system," *Sensors*, vol. 17, no. 1, 2016.

[48] S. S. Reka, B. K. Chezian, and S. S. Chandra, "A novel approach of IoT-based smart greenhouse farming system," in *Green Buildings and Sustainable Engineering*, Springer, 2019.

[49] M. Y. Cheng, K. C. Chiu, Y. M. Hsieh, I. T. Yang, J. S. Chou, and Y. W. Wu, "BIM integrated smart monitoring technique for building fire prevention and disaster relief," *Automation in Construction*, vol. 84, pp. 14–30, 2017.

[50] S. Kaushik and C. Singh, "Monitoring and controlling in food storage system using wireless sensor networks based on Zigbee & Bluetooth modules," *International Journal of Multidisciplinary in Cryptology and Information Security*, vol. 2, no. 3, pp. 7–10, 2013, http://warse.org/pdfs/ijmcis01232013.pdf.

[51] S. Aram, A. Troiano, F. Rugiano, and E. Pasero, "Low power and Bluetooth-based wireless sensor network for environmental sensing using smartphones," in *Artificial Intelligence Applications and Innovations*, pp. 332–340, Springer, 2012.

[52] P. Di Gennaro, D. Lofú, D. Vitanio, P. Tedeschi, and P. Boccadoro, "WaterS: a Sigfox-compliant prototype for water monitoring," *Internet Technology Letters*, vol. 2, no. 1, article e74, 2019.

[53] F. Pitu and N. C. Gaitan, "Surveillance of SigFox technology integrated with environmental monitoring," in *2020 15th International Conference on Development and Application Systems, DAS 2020 - Proceedings*, pp. 69–72, Suceava, Romania, 2020.

[54] A. Chehri and R. Saadane, "Zigbee-based remote environmental monitoring for smart industrial mining," in *SCA2019: The Fourth International Conference on Smart City Applications*, pp. 2–7, Casablanca Morocco, 2019.

[55] M. Dangana, S. Ansari, Q. H. Abbasi, S. Hussain, and M. A. Imran, "Suitability of NB-IoT for indoor industrial environment: a survey and insights," *Sensors*, vol. 21, no. 16, p. 5284, 2021.

[56] S. Duangsuwan, A. Takarn, R. Nujankaew, and P. Jamjareegulgarn, "A study of air pollution smart sensors LPWAN via NB-IoT for Thailand smart cities 4.0," *2018 10th International Conference on Knowledge and Smart Technology: Cybernetics in the Next Decades, KST*, 2018, pp. 206–209, Chiang Mai, Thailand, 2018.

[57] M. Ibrahim, A. Elgamri, S. Babiker, and A. Mohamed, "Internet of Things based smart environmental monitoring using the Raspberry-Pi computer," *2015 5th International Conference on Digital Information Processing and Communications, ICDIPC*, 2015, pp. 159–164, Sierre, Switzerland, 2015.

[58] Y. Liu, A. Liu, N. Zhang, X. Liu, M. Ma, and Y. Hu, "DDC: dynamic duty cycle for improving delay and energy efficiency in wireless sensor networks," *Journal of Network and Computer Applications*, vol. 131, pp. 16–27, 2019.

[59] K. Lokesh Krishna, J. Madhuri, and K. Anuradha, "A ZigBee based energy efficient environmental monitoring alerting and controlling system," *2016 international conference on information communication and embedded systems, ICICES*, 2016, Chennai, India, 2016, 2016.

[60] J. A. Lossio-Ventura and H. Alatrista-Salas, "Information management and big data: SIMBig overview," in *6th International Conference, SIMBig 2019*, Lima, Peru, 2016.

[61] S. Zafar, G. Miraj, R. Baloch, D. Murtaza, and K. Arshad, "An IoT based real-time environmental monitoring system using Arduino and cloud service," *Engineering, Technology & Applied Science Research*, vol. 8, no. 4, pp. 3238–3242, 2018.

[62] G. G. Xie and J. H. Gibson, "A network layer protocol for UANs to address propagation delay induced performance limitations," *Oceans Conference Record (IEEE)*, vol. 4, no. - November, pp. 2087–2094, 2001.

[63] H. Yan, Z. J. Shi, and J. H. Cui, "DBR: depth-based routing for underwater sensor networks," *Networking 2008 Ad Hoc and Sensor Networks, Wireless Networks, Next Generation Internet*, vol. 4982, pp. 72–86, 2008.

[64] M. Zorzi, P. Casari, N. Baldo, and A. F. Harris, "Energy-efficient routing schemes for underwater acoustic networks," *IEEE Journal on Selected Areas in Communications*, vol. 26, no. 9, pp. 1754–1766, 2008.

[65] A. A. Ahmed and N. Fisal, "A real-time routing protocol with load distribution in wireless sensor networks," *Computer Communications*, vol. 31, no. 14, pp. 3190–3203, 2008.

[66] A. Ali Ahmed, "An enhanced real-time routing protocol with load distribution for mobile wireless sensor networks," *Computer Networks*, vol. 57, no. 6, pp. 1459–1473, 2013.

[67] G. Sakya and V. Sharma, "ADMC-MAC: energy efficient adaptive MAC protocol for mission critical applications in WSN," *Sustainable Computing: Informatics and Systems*, vol. 23, pp. 21–28, 2019.

[68] D. K. Sah and T. Amgoth, "Renewable energy harvesting schemes in wireless sensor networks: a survey," *Information Fusion*, vol. 63, pp. 223–247, 2020.

[69] H. Sharma, A. Haque, and Z. A. Jaffery, "Solar energy harvesting wireless sensor network nodes: a survey," *Journal of Renewable and Sustainable Energy*, vol. 10, no. 2, 2018.

[70] H. Sharma, A. Haque, and Z. A. Jaffery, "Maximization of wireless sensor network lifetime using solar energy harvesting for smart agriculture monitoring," *Ad Hoc Networks*, vol. 94, article 101966, 2019.

[71] S. M. Bozorgi, A. Shokouhi Rostami, A. A. R. Hosseinabadi, and V. E. Balas, "A new clustering protocol for energy harvesting-wireless sensor networks," *Computers and Electrical Engineering*, vol. 64, pp. 233–247, 2017.

[72] H. K. Qureshi, U. Saleem, M. Saleem, A. Pitsillides, and M. Lestas, "Harvested energy prediction schemes for wireless sensor networks: performance evaluation and enhancements," *Wireless Communications and Mobile Computing*, vol. 2017, 14 pages, 2017.

[73] T. Xie, G. Zhang, H. Liu, F. Liu, and P. Du, "A hybrid forecasting method for solar output power based on variational mode decomposition, deep belief networks and autoregressive moving average," *Applied Sciences*, vol. 8, no. 10, p. 1901, 2018.

[74] A. G. Salman and B. Kanigoro, "Visibility forecasting using autoregressive integrated moving average (ARIMA) models," *Procedia Computer Science*, vol. 179, no. 2019, pp. 252–259, 2021.

[75] M. Prauzek, N. R. A. Mourcet, J. Hlavica, and P. Musilek, "Q-learning algorithm for energy management in solar powered embedded monitoring systems," in *2018 IEEE Congress on Evolutionary Computation, CEC 2018 - Proceedings*, Rio de Janeiro, Brazil, 2018.

[76] H. X. Zou, L. C. Zhao, Q. H. Gao et al., "Mechanical modulations for enhancing energy harvesting: principles, methods and applications," *Applied Energy*, vol. 255, article 113871, 2019.

[77] V. Larnaudie, M. D. Ferrari, and C. Lareo, "Switchgrass as an alternative biomass for ethanol production in a biorefinery: perspectives on technology, economics and environmental sustainability," *Renewable and Sustainable Energy Reviews*, vol. 158, article 112115, 2022.

[78] J. Singh, R. Kaur, and D. Singh, "Energy harvesting in wireless sensor networks: a taxonomic survey," *International Journal of Energy Research*, vol. 45, no. 1, pp. 118–140, 2021.

[79] B. Paharia and K. Bhushan, "A comprehensive review of distributed denial of service (DDoS) attacks in fog computing environment," in *Handbook of Computer Networks and Cyber Security: Principles and Paradigms*, Springer, 2019.

[80] K. S. Adu-manu, *A study into lifetime maximization of wireless sensor networks for water quality monitoring, [Ph.D. thesis]*, University of Ghana, 2020.

[81] W. Tiberti, F. Caruso, L. Pomante, M. Pugliese, M. Santic, and F. Santucci, "Development of an extended topology-based lightweight cryptographic scheme for IEEE 802.15.4 wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 16, no. 10, Article ID 155014772095167, 2020.

[82] C. Mallick and S. Satpathy, "Challenges and design goals of wireless sensor networks: a sate-of-the-art challenges and design goals of wireless sensor networks: a sate-of-the-art review," *International Journal of Computer Applications*, vol. 179, no. 28, pp. 42–47, 1970.

[83] J. Hou and Y. Zhang, "Mobile-service based approach for topology control of wireless sensor networks," *Wireless Personal Communications*, vol. 102, no. 2, pp. 1839–1851, 2018.

[84] G. M. E. Rahman and A. W. Khan, "LDAP: lightweight dynamic auto-reconfigurable protocol in an IoT-enabled WSN for wide-area remote monitoring," *Remote Sensing*, vol. 12, no. 19, p. 3131, 2020.

[85] A. Sobchuk, Y. Kravchenko, M. Tyshchenko, P. Gawliczek, and O. Afanasyeva, "Analytical aspects of providing a feature of the functional stability according to the choice of technology for construction of wireless sensor networks," in *2019 IEEE International Conference on Advanced Trends in Information Theory (ATIT)*, pp. 102–106, Kyiv, Ukraine, 2019.

[86] M. Dong, H. Li, Y. Li, Y. Deng, and R. Yin, "Fault-tolerant topology with lifetime optimization for underwater wireless sensor networks," *Sādhanā*, vol. 45, no. 1, 2020.

[87] R. Jadhav and V. Vatsala, "Security issues and solutions in wireless sensor networks," *International Journal of Computer Applications*, vol. 162, no. 2, pp. 14–19, 2017.

[88] V. Ekong and U. Ekong, "A survey of security vulnerabilities in wireless sensor networks," *Nigerian Journal of Technology*, vol. 35, no. 2, p. 392, 2016.

[89] J. Bhola, S. Soni, and G. K. Cheema, "Recent trends for security applications in wireless sensor networks - a technical review," in *Proceedings of the 2019 6th International Conference on Computing for Sustainable Global Development, INDIACom 2019*, pp. 707–712, New Delhi, India, 2019.

[90] S. Roy, M. Conti, S. Setia, and S. Jajodia, "Secure data aggregation in wireless sensor networks," *Networks*, vol. 7, no. 3, pp. 1040–1052, 2012.

[91] A. Aseeri and R. Zhang, "Secure data aggregation in wireless sensor networks: enumeration attack and countermeasure," in *ICC 2019 - 2019 IEEE International Conference on Communications (ICC)*, Shanghai, China, 2019.

[92] S. Ozdemir and Y. Xiao, "Secure data aggregation in wireless sensor networks: a comprehensive overview," *Computer Networks*, vol. 53, no. 12, pp. 2022–2037, 2009.

[93] A. J. Watt, M. R. Phillips, C. E. Campbell, I. Wells, and S. Hole, "Wireless sensor networks for monitoring underwater sediment transport," *Science of the Total Environment*, vol. 667, pp. 160–165, 2019.

[94] A. Razaque and S. S. Rizvi, "Secure data aggregation using access control and authentication for wireless sensor networks," *Computers & Security*, vol. 70, pp. 532–545, 2017.

[95] M. B. Shanthi and D. K. Anvekar, "Secure localization for underwater wireless sensor networks based on probabilistic approach," in *Proceedings of 2018 2nd International Conference on Advances in Electronics, Computers and Communications, ICAECC 2018*, pp. 1–6, Bangalore, India, 2018.

[96] E. Barker and Q. Dang, *Recommendation for key management – part 3: application-specific key management guidance*, vol. 800-57, NIST Special Publication, 2007.

[97] V. Kumar, A. Jain, and P. N. Barwal, "Wireless sensor networks: security issues, challenges and solutions," *International Journal of Information & Computation Technology*, vol. 4, no. 8, pp. 859–868, 2014, http://www.irphouse.com.

[98] C. S. Kingsly and J. G. C. Chandran, "Critical study on constraints in wireless sensor network applications,"

International Journal of Engineering Research & Technology, vol. 2, no. 7, pp. 1311–1316, 2013.

[99] N. Sharma and R. Bhatt, "Privacy preservation in WSN for healthcare application," *Procedia Computer Science*, vol. 132, pp. 1243–1252, 2018.

[100] J. Kuriakose, S. Joshi, R. Vikram Raju, and A. Kilaru, "A review on localization in wireless sensor networks," *Adv. Intell. Syst. Comput.*, vol. 264, pp. 599–610, 2014.

[101] A. J. Garcia-Sanchez, F. Garcia-Sanchez, F. Losilla et al., "Wireless sensor network deployment for monitoring wildlife passages," *Sensors*, vol. 10, no. 8, pp. 7236–7262, 2010.

[102] S. Khanvilkar, F. Bashir, D. Schonfeld, and A. Khokhar, "Multimedia networks and communication," in *The Electrical Engineering Handbook*, pp. 401–425, University of Illinois, Chicago, 2005.