Delta University Scientific Journal
Journal home page: https://dusj.journals.ekb.eg

Open Issues for Intelligent Connectivity Wireless Sensor Networks (WSNs) and IoT: State of the Art

Ahmed A. Abdullah[1]*, Hesham A. Ali[2, 3], Tarek M. Hassan[4], Hanaa Salem Marie[5]

[1]*Faculty of Engineering, Delta University for Science and Technology, Gamasa 35712, Egypt Email: Ahmed.abdelaleem@deltauniv.edu.eg*
[2]*Department of Computer Engineering and Control Systems, Faculty of Engineering, Mansoura University, Egypt, Email: H_arafat_ali@mans.edu.eg*
[3]*Faculty Artificial Intelligence, Delta University for Science and Technology, Gamasa 35712, Egypt.*
[4]*Faculty of Engineering, Delta University for Science and Technology, Gamasa 35712, Egypt, Email: tarek.hassan@deltauniv.edu.eg*
[5]*Faculty of Engineering, Delta University for Science and Technology, Gamasa 35712, Egypt Hana.salem@deltauniv.edu.eg*

*** Correspondence:** Department of Mechatronics, Faculty of Engineering, Delta University for Science and Technology, International Coastal Road, Gamasa City35712, Egypt, Deltauniv.edu.eg Mobile: +20- 01004536910; Email: Ahmed.abdelaleem@deltauniv.edu.eg (Ahmed A. Abdullah).

ABSTRACT

To effortlessly gather knowledge and data from wireless devices, Wireless Sensor Networks (WSNs) are now used as one of the successful distributed applications. The unique architecture of WSNs made it possible to employ them in a wide range of contemporary industrial applications, including automated control systems and systems for surveillance and monitoring that can help bridge the gap between user needs and available technology. The control of topology, QoS, robustness, placement, power consumption, scalability, reliability, resource utilization, data availability, and security are additional problems faced by WSNs. WSNs are planned to be merged into the internet of things (IoT) in the future when sensor nodes automatically join the internet and use it to cooperate and complete their functions. This survey paper proposes a taxonomy for wireless sensor networks (WSN), highlights some of the essential technologies, and profiles some applications that have the potential to make a striking difference in human life, especially for the differently abled and the elderly. Compared to similar survey papers in the area, this paper is far more comprehensive in its range and exhaustively covers the most significant technologies, from sensors to applications. Highlights some of the most powerful technology and describes several applications that have the potential to significantly improve human life, particularly for the elderly and those with disabilities. Compared to a different area, this one is much more thorough and covers all essential critical technologies, from sensors to applications. This paper aims to provide a better understanding of such limitations.

Keywords: WSNs; automated control systems; routing; security; attacks.

1. Introduction

Today the Internet has become ubiquitous, has touched almost every corner of the globe, and is affecting human life unimaginable. We are now entering an era of even more pervasive connectivity where various appliances will be connected to the web [1]. Let us look at two of the most popular definitions. (1) Define the Internet of Things as simply an interaction between the physical and digital worlds. The digital world interacts with the physical world using many sensors and actuators. Another definition [2]. (2) Defines the IoT as a paradigm in which computing and networking capabilities are embedded in any conceivable object [3]. Most of the authors have used various definitions of this phrase. Let's examine the two most widely used reports. (1) Simply put, the

Internet of Things is the meeting point of the physical and digital worlds. Numerous sensors and actuators communicate between the physical and digital worlds. [2] Another definition. (2) The Internet of Things (IoT) is defined by two as a paradigm in which networking and computational capabilities are built into any imaginable device [3].

We use these capabilities to query the object's state and change its shape if possible. In common parlance, the IoT refers to a new world where almost all the devices and appliances we use are connected to a network. For this intelligence and interconnection, IoT devices are equipped with embedded sensors, actuators, processors, and transceivers. IoT is not a single technology instead, an accumulation of various technologies that work together in tandem [4]. IoT devices have interconnected sensors, actuators, CPUs, and transceivers for this intelligence and connectivity. IoT is a collection of different technologies operating in concert instead of being a single technology [4].

Sensors and actuators are devices that help interact with the physical environment. The data collected by the sensors must be stored and processed intelligently in order to derive valuable inferences from it [5]. Note that we broadly define the term sensor; a mobile phone or even a microwave oven can be a sensor if it provides inputs about its current state (internal state + environment). An actuator is a device used to effect a change in the background, such as the temperature controller of an air conditioner [6].

Devices that aid in interacting with the physical world include sensors and actuators. It must be intelligently stored and processed to draw insightful conclusions from the sensor data [5]. Keep in mind that we define the term "sensor" generally; a cell phone or even a microwave can qualify if it sends information about its current state (internal state plus environment). A device called an actuator is one that alters the background, like the air conditioner's temperature controller [6].

The storage and processing capabilities of an IoT object are also restricted by the resources available, which are often very constrained due to size, energy, power, and computational capability limitations. As a result, the main research challenge is to ensure that we get the right kind of data at the desired level of accuracy [7].

WSNs are a particular class of wireless networks that include a large number of specialized sensors but have little in the way of infrastructure. These tiny sensors are less expensive than conventional and have limited power [8]. These sensors are small devices that cooperate in gathering environmental data. The base station serves as an interface between the user and the internet after the sensors have processed and transmitted the collected data. The design of WSNs often depends on the application, where numerous aspects must be considered, including cost, the environment, hardware, the design objectives of the application, and the system restrictions [8], [9].

WSNs are deployed in numerous applications [10], [11], which closes the technological and user needs gap. Area monitoring, military applications [12], where sensors are used to detect enemy intrusion, environmental, earth tracking, and monitoring are among the most popular WSN applications. There are numerous sub-applications of monitoring, including A) Monitoring of air pollution [13], which many cities have implemented to track the concentration of hazardous gases. B) Forest fire detection, in which sensor nodes are positioned throughout the forest to detect the start of a fire and are outfitted with sensors to gauge the fire's temperature, humidity, and gas emissions. C) Monitoring water quality can be done using numerous wireless sensors.

WSNs are also employed in industrial monitoring applications [10], [14] because sensors can be incorporated into machinery and require minimal infrastructure. WSNs could be used in a variety of applications in this area, including monitoring the health of machines where sensors have been installed for machine maintenance, monitoring water waste where water levels and water quality can be checked, and watching the health of structures where WSNs can have control over civil infrastructure [15]. The radio transceiver, microcontroller, power source, and external memory make up the sensor nodes.

This paper is organized as follows: Section 2 describes the 'WSNs' basics and concepts. Section 3 presents an overview of routing in WSNs, its classification, challenges, and some of the routing techniques. Section 4 shows security in WSNs, goals, network layer attacks, and countermeasures. While section 5 presents routing issues in WSNs, the section explains, in brief, the future research directions, and Finlay section 6 introduces the conclusion.

2. Wireless Sensor Network

In this paper, the term sensor network refers to a heterogeneous system joining tiny sensors and actuators with general-purpose computing devices. It may consist of hundreds or thousands of low-power, low-cost nodes, perhaps mobile, but more likely at fixed locations, deployed in masse to monitor and affect the environment. There are fundamental differences between any traditional wireless network and a wireless sensor network [16]. The term "sensor network" is used in this research to describe a heterogeneous system that combines small sensors and actuators with general-purpose computing hardware. It might consist of hundreds or thousands of low-cost, low-power nodes deployed in large numbers to monitor and influence the environment. These nodes could be movable, but it's more likely that they would be fixed. A wireless sensor network differs fundamentally from any conventional wireless network in several ways [16]. Structured and unstructured WSNs are the categories into which WSNs are classified [17]. The network in the unstructured WSN is unattended to perform reporting and monitoring functions, making it challenging to perform network maintenance, such as detecting a failure and managing connectivity. The unstructured WSN comprises a sizable number of tiny randomly placed nodes throughout the area. On the other hand, structured WSNs have low maintenance and management costs because all the sensors are installed using a pre-planned technique with fixed nodes, resulting in full coverage.

Because sensor nodes have unique properties, unlike wired networks [16], routing in WSNs faces various difficulties [18]. The difficult deployment conditions may expose WSNs to failure [19]. In the network region, sensor nodes should be autonomous [20], [21], as this enables all nodes to communicate wirelessly and alters the topology. As a result, various attacks present a chance for numerous security issues [22], [23]. For instance, the attacker might be able to impersonate a sensor node, track data transmission, send bogus alerts, and use up network resources. A network like this must be secured to transmit data from its source to its destination [24]. Taking everything into account, there are numerous restrictions.

2.1. Wireless sensor network architecture

Wireless sensor system Architecture is designed according to an IoT system's layered architecture, outlined in Figure 1 [25]. The first layer represents **the environment layer** with the monitored signals such as temperature and humidity. The second is **the perception layer**, where the WSN is located with three sensor nodes, the encrypted data travels to the receiver using the suitable characteristics protocol in **the transport layer**. Like scalability, secure message sending and receiving, minimum bandwidth, energy consumption and processing, and its publisher/subscriber architecture.

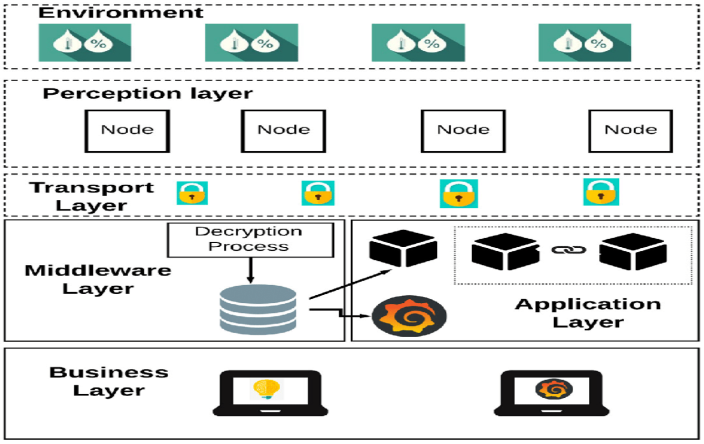

Figure١ : Architecture system scheme of WSN

The middleware layer is essential not only for the proposed methodology but also for the MQTT protocol and the publish/subscribe architecture based on topics. For the development of the IoT system of WSNs. This layer has the function of being an intermediary of messages in the wireless sensor network. In parallel, it decrypts messages and moves the records to the database. The application layer is where the visual display system is located.

Include publisher/subscriber architecture, scalability, secure message sending and receiving, minimal bandwidth, energy usage, and processing. In addition to the proposed technique, the MQTT protocol and the topic-based publish/subscribe architecture rely on the middleware layer. For the creation of the WSNs IoT system. In a wireless sensor network, this layer is an intermediate for messages. It simultaneously moves the records to the database and decrypts communications. The visual display system is positioned at the application layer.

The business layer manages the IoT system, including applications, business and profit models, and 'users' privacy. The business layer is out of the scope of this paper. Hence, we do not discuss it further

2.2. WSN Types and Topologies

Topologies of WSNs are categorized according to the number of nodes or the power and transmission [26], [27], whereas types can be classified according to their structure or intended application [28]. Terrestrial, Underground, Underwater, Multimedia, and Mobile WSNs are some of the different categories. The many types and topologies of wireless sensor networks are described in Figure 2.

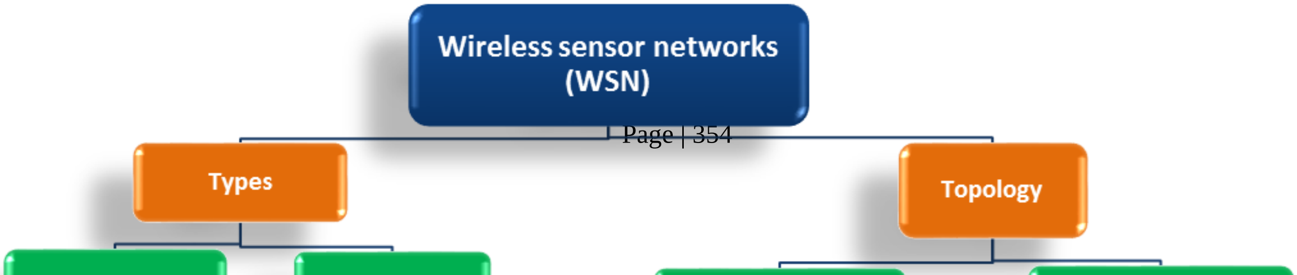

Figure 2 : WSN Types and Topology

3. Open Issues and Research Area in WSN

Although WSNs are given a lot of attention, they are also subject to several limitations and difficulties, including topology control, scalability, robustness, placement, power consumption, routing, security, and data availability. Due to the power, storage, and processing capacity restrictions placed on sensor nodes, wireless sensor networks are subject to several constraints that necessitate careful resource management. Due to a lack of infrastructure, wireless communication is also insecure. The vulnerability of sensor nodes and their varied makeup pose a problem. The frequent topology changes brought on by node failures, joining, or mobility are a drawback. The absence of a global addressing scheme also makes traditional IP-based protocols ineffective. For WSNs to become widely used and reliable, a variety of obstacles and widely used. These difficulties can be summed up as depicted in Figure 3 and Figure 4 [18], [22], [29], [30]; problems must be resolved. Table 1 concludes the most important research directions of WSN challenges in brief.

Table 1

Recent research directions for WSN

Challenges	Approaches	Objectives	Future directions
Topology control	A game theoretic for nodes in WSNs [31]	Change node transmission power to extend network lifetime.	Enhance the approach so that it is more general.
	A new link interference model [32]	Measures a link's interference by calculating the number of links covered in order to reduce link interference.	Creating interference-optimal topologies by designing efficient distributed algorithms
	Adaptive Cooperative Topology Control (CTCA)) [33]	Adapt the transmission powers of nodes to lengthen network longevity using an adaptive technique so that nodes do not end up with the same power level throughout their lifetime.	Creating and explaining a more generic version of this technique
Scalability	Broadcast session key "BROCK" protocol [28]	Reducing the number of transmissions can save energy.	Enhance sensor network security protocols while keeping data

			integrity and authentication in consideration.
	Multi-hop routing (HYMN) [34]	Enhance the Scalability of Wireless Sensor Networks by analyzing and comparing the scalability constraints of conventional routing methods to Hybrid Multi-hop routing (HYMN)	Increasing the efficiency of this approach
Robustness	Gene Regulatory Networks (GRNs) [35]	Face the difficulty of maximizing efficiency, in which sensor nodes must be energetic and adaptable to any faults.	Improve the algorithm to be more efficient
	A novel solution to obtain robust WSNs [36]	Enhancing the robustness of communications in WSNs by utilizing biological robustness concepts at the Nano scale	Investigate the use of GRNs in different network contexts, such as the Internet.
Placement	New relay placement approach [26]	Have the capacity to improve network connectivity in a wireless multi-hop network.	Develop a novel intelligent routing protocol that it takes advantage of two connected relay nodes.
	Sink Node Placement Strategies for WSNs [37]	Choose the optimal location in single-hop and multi-hop WSNs regarding network longevity.	Enhance the strategy to maximize network lifetime.
	Weighted relay node placement for WSN connectivity [38]	Minimize the total weight of the points on which the relay nodes are deployed	Investigate the problem of weighted relay node placement for robust and survivable WSN.
Power consuming	Topology control algorithm called A tree-based heuristic [27]	Increase the network's lifetime based on full network connectivity, high coverage of the sensing area and reduced power consumption.	Utilize minimal global information to enhance the technique.
	An energy-efficient, mobile sink-based data collection protocol for large-scale WSNs [38]	Reduces the total energy consumption based on (i) overhead updating routing information and (ii) increased operating time due to aperiodic query.	Refine the proposed method to reduce data collection time by using parallel transmissions, and extend this proposed method to cope with node failure
Routing	A polynomial time heuristic algorithm [18]	The network's performance can be enhanced by considering dynamic channel assignments while routing, which allows for more transmissions while simultaneously efficiently decreasing computational complexity and solving linear programming formulas.	Decrease the number of equations to reduce the computation time and increase network performance.
	Based on a genetic algorithm, an energy-efficient and trustworthy routing protocol (E2TRP) for wireless sensor networks has been developed[39]	Dynamic generation of CH and clusters depending on node distance from CH (of the sensor nodes) utilizing a genetic algorithm and sensor node trust	Creating and describing a more generic version of this method

	Enhanced clustering algorithm in wireless sensor networks based on energy consumption [40]	Protect the nodes with low energy and a long distance to prevent energy failure in the cluster heads.	How to handle the initial energy when it is not there in the same period
Security	New data-gathering strategies for a broad sensor network region when integrating one or more M-investors [22]	Provide security both for incoming data memory and network messages.	Enhancing mechanisms to boost security over a large area.
	Position Responsive Routing Protocol (PRRP) [41]	minimize energy consumed in each node based on (١)reducing the amount of time in which a sensor node is in an idle listening state and (2) reducing the average communication the distance over the network.	Improve the protocol to deal with mobile ad-hoc network

Now, we will focus on the most recent challenges and currently open issues in the environment that have effects on the performance of WSN.

1. **Interoperability and scalability [42]:** The significant challenges in interoperability are technical, semantic, and pragmatic. In addition, sensing nodes are becoming prominent and unbounded, so current WSN architectures need to be updated to cope with the rapid growth of sensing node numbers. The current security protocol also doesn't handle this growth, so it needs to be modified.
2. **Energy Efficiency [41]:** sensors are limited due to energy, storage and lifetime, so optimized, secure and efficient protocols need to be devised for WSN. A set of tasks need to be created to determine each charge which sensor is required; for executing this task, a sensor will be turned on the sensor for a particular time interval, and after completion of the study, the sensor will go to an idle state.
3. **Mobility Management [43]:** current mobility protocols can't deal with mobile nodes efficiently due to energy and processing constraints, so mobility management is critical in WSN.
4. **Deployment and Localization [44]:** Deployment means positioning and organizing an active sensor network in a real-world environment. Nodes can be deployed by placing one after another in a sensor field or dropping it from a plane. Deployment of the sensor networks is an intensive and cumbersome activity as we do not influence wireless communication quality. The real world also limits and strains sensor nodes by interfering during communications. Several deployment issues that need to be taken care of our power consumption and node death, Low data yield, Network Congestion & Self-configuration [45], [46].

For **Localization**: Sensor networks have been used in many fields like object tracking, forecasting and distant control of dangerous regions, surveillance, and routing. In such applications, sensor data need to be merged with location details. The location information of the sensor can further help route in calculating the coverage quality and attaining load balancing. Since sensor networks may be organized in unreachable environments or disaster assistance operations, the location of sensor nodes may not be scheduled, so localization is one of the fundamental problems for many applications. It contains the identification and association of collected data, query, and managing nodes localized in a determined area, node addressing, coverage and nodes density evaluation, generation of energy map, topographical routing, object tracking, and other algorithms. The significance of localization data ascends from numerous factors, some of which are correlated only to WSNs. Hence, localization turns out to be a crucial research topic in WSNs. Figure 3 summaries most of localization open issues [47], [48].

4. Deployment and Localization and Coverage

Coverage[17] is one of the measurements of WSN quality of service (QoS) that is affected by the sensing range (r_s) of the sensor node. The target area is fully covered if every point of the area is within the sensing range of at least one sensor node. Each node can detect events and objects within its sensing range and share this information with its neighbors, located in its communication range to guarantee connectivity between nodes. In most cases, many sensor nodes are required to achieve maximum coverage. Coverage may be area coverage, point coverage and barrier coverage [19], determined according to application. This paper concentrated mainly on area coverage. The primary coverage challenge is maximizing network coverage with the minimum number of sensor nodes which is the subject of this paper using genetic optimization algorithm (GA) [20]. This is considered a Non-deterministic Polynomial-time hard (NP-hard) problem [49].

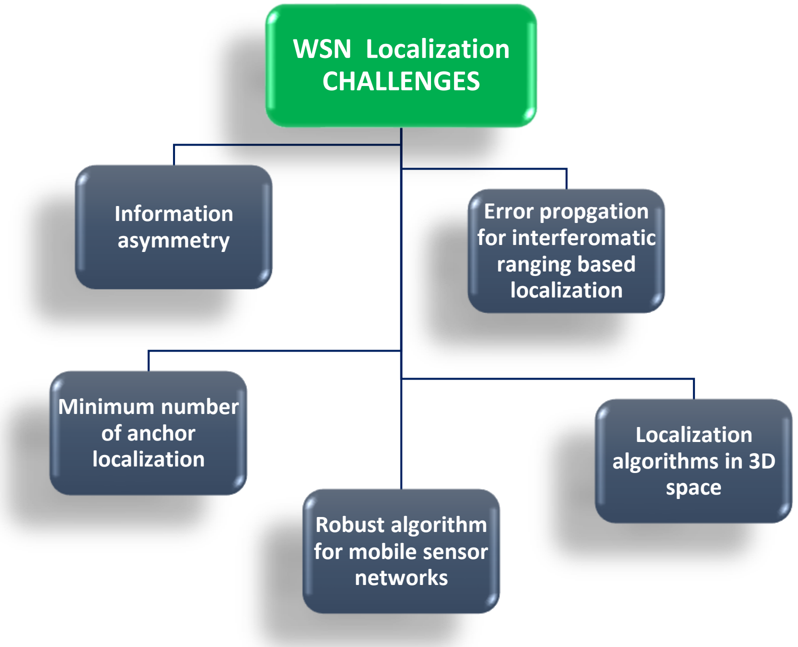
WSN Localization CHALLENGES
Information asymmetry
Error propgation for interferomatic ranging based localization
Minimum number of anchor localization
Localization algorithms in 3D space
Robust algorithm for mobile sensor networks

Figure 3: Taxonomy of Localization Open Issues

Nodes deployed in WSNs could be static, mobile, homogenous and/or heterogeneous[50]. Static nodes are initially deployed and keep their position fixed inside the region. They can be deployed deterministically or randomly according to environment and application requirements. The main advantages of static nodes are energy saving and cost reduction, as there is no mobility, which consumes the leading energy of nodes. However, the main drawback is that there is no mobility in the network and thus, coverage holes will arise. Accordingly, mobile nodes are used to fill up the coverage holes by moving to areas not covered by static nodes. Mobile nodes are deployed after the initial deployment of static nodes.

Nodes used in WSN deployments may be stationary, moving, homogeneous, or heterogeneous [50][12]. Initial deployments consist of static nodes, which maintain a fixed position within the region. Depending on the needs of the environment and the application, they can be distributed deterministically or randomly. As there is no motion, which is what uses most of a node's energy, static nodes have several benefits. The biggest disadvantage, however, is that coverage gaps will develop because the network is immobile. Mobile nodes are therefore employed to remedy the coverage gaps by dispersing to the regions that static nodes do not cover. After the initial deployment of static nodes, mobile nodes are deployed. Then, these sensors are deployed randomly but they increase the hardware costs and consume more energy [16] due to mobility feature. . Whether there are mobile nodes or static nodes, this paper classifies coverage strategies in WSN into three main parts: coverage based on deployment strategies, coverage based on meta-heuristic methods and range based on self-scheduling strategies. **Error! Reference source not found.**4 illustrates the classification of coverage strategies in WSN. Then, because of their mobility feature, these sensors are placed arbitrarily, but they raise hardware prices and use more energy [16][13]. This study divides coverage tactics in WSN into three primary categories: coverage based on deployment strategies, coverage based on meta-heuristic techniques, and coverage based on self-scheduling strategy, regardless of whether there are mobile nodes or static nodes. Figure 4 shows how coverage strategies in WSN are categorized.

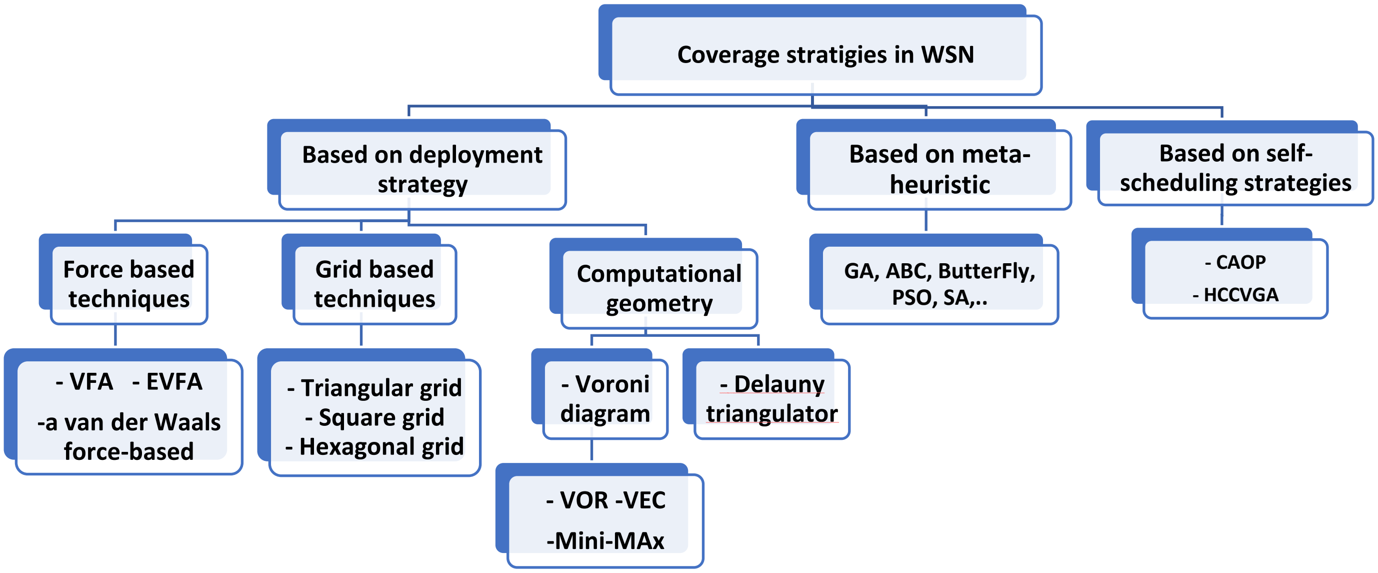

Figure 4: Coverage strategies taxonomy for WSNs

5. Routing Issues in WSNs

Routing is processed to find the best path to deliver the data from the source sensor node to the destination sensor node. It is more vital in WSN than any other network due to its many characteristics of an IP-based schema which is a routing protocol in which the traffic is routed from nodes to the base station. In WSNs, nodes are resource constrained regarding energy [30], storage, and computational capacity, so they must be used efficiently. Routing protocols are organized into three categories: (a) The first one is based on a mode of functioning classified into proactive, reactive and hybrid routing [51]. (b) The second one relies on the participation style of nodes classified into flat, direct, and clustering routing protocols [45]. Moreover, (c) the third one is based on the network structure divided into Hierarchical [46], Data-Centric [47], and Location-Based [48]. Many factors affect routing protocols that must be taken into consideration when designing routing protocols [52], [53]. Some of these factors are Node Deployment, Fault-Tolerance, Scalability, Data Aggregation, Routing Looping Problem, Energy Constraints, and Security, which consider the most critical factor in achieving secure routing.

This section discusses some routing techniques, showing their characteristics, types, advantages, and disadvantages. As shown in **Error! Reference source not found.**.

Table 2

Routing protocols summary

Approaches	Protocols	Characteristics	Advantage / Disadvantage
Re-active Routing Technique	Ad-hoc On-Demand Distance Vector (AODV) [54]	It is an incorporation of on-demand and distance-vector, not only that but a method of routing a message, whereby the message could be passed by exploring routes	**Advantages:** • Flat routing protocol where there is no need for the central administrative system that handles routing process, avoid loops and counting to infinity problem. • It keeps a small message overhead. • The connection setup delay is lower. • It establishes the shortest path with the lowest power consumption. • It is used in solving the black hole problem.

			Disadvantage • Takes a lot of time to build the routing table. • Consumes more share bandwidth. • Higher processing demand
	Dynamic Source Routing (DSR) [52]	An On-Demand routing protocol in which it calculates route only when it is necessary. Node discovers the route by sending the route request to all neighbors with a unique id, nodes list, source address, and destination address.	**Advantage** • It uses no periodic routing. It reduces bandwidth overhead. • Protect battery power. • Reduce route maintenance overhead. • The route caching also decreases the overhead gained from route discovery.
			Disadvantage • Packet header becomes larger with a route length • The problem of Route replay storm.
Pro-Active Routing Technique	Destination-Sequenced Distance-Vector (DSDV) [55]	It is a table-driven algorithm which depends on the Bellman-ford algorithm [39], where every node maintains a routing table arranged in the sequence that verifies the next hop, cost and the cost metric of each destination	**Advantage** • The simple routing protocol is designed for initiating an ad-hoc network with fewer sensor nodes. • It does not include format loops because it uses destination sequence numbers • No latency is caused by route discovery.
			Disadvantage • There are bandwidth and power consumed by sleeping nodes even if the network is idle • Most route information is never used. • Not the right choice for a highly dynamic network
Hierarchical Routing Technique	Low-Energy Adaptive Clustering Hierarchy (LEACH) [56]	Works on dividing data into clusters to decrease the consumption of energy. This operation consists of several rounds divided into two phases: Step up phase, and steady phase.	**Advantage** • It gives the sensor node a longer lifetime. • It reduces network traffic as it aggregates all data at the cluster head • It does not need the location information of nodes to create the cluster • It saves energy.
			Disadvantage • It does not give information about the cluster head in the network. • Clusters are randomly divided, which causes uneven cluster distribution and increases power consumption. • It is not suitable for applications with extensive place coverage.

6. Security Issues in WSNs

Security is a broadly used term to include the characteristics of authentication, privacy, integrity, non-repudiation, and anti-playback, as depicted in **Error! Reference source not found.**5. The greater the dependency o n the information supplied by the networks may be increased, the more the risk of secure information transmission in the networks has increased. To secure the communication of massive kinds of information over networks, several cryptographic, steganography and other techniques are utilized that happen to be used widely [52]. The following are the initial security requirements that every WSN application should adhere to [55]: Confidently, Authentication, Lack of Integrity, Protection against Message Reply attacks, Lightweight Encryption Mechanisms & Secure Management and Key Distribution Techniques.

Figure 6 depicts security as a critical issue, especially in WSNs, for many reasons; some of these reasons are that all wireless nodes are usually found in a hazardous environment, and the broadcast nature of WSNs makes it easy to be affected by any attack. Many security goals must be achieved; these security goals [57] can be classified as primary and secondary goals. The primary goals are common security goals, such as data confidentiality, authentication, integrity, and availability. The secondary goals [57] like data freshness, self-organization, time synchronization, and secure localization.

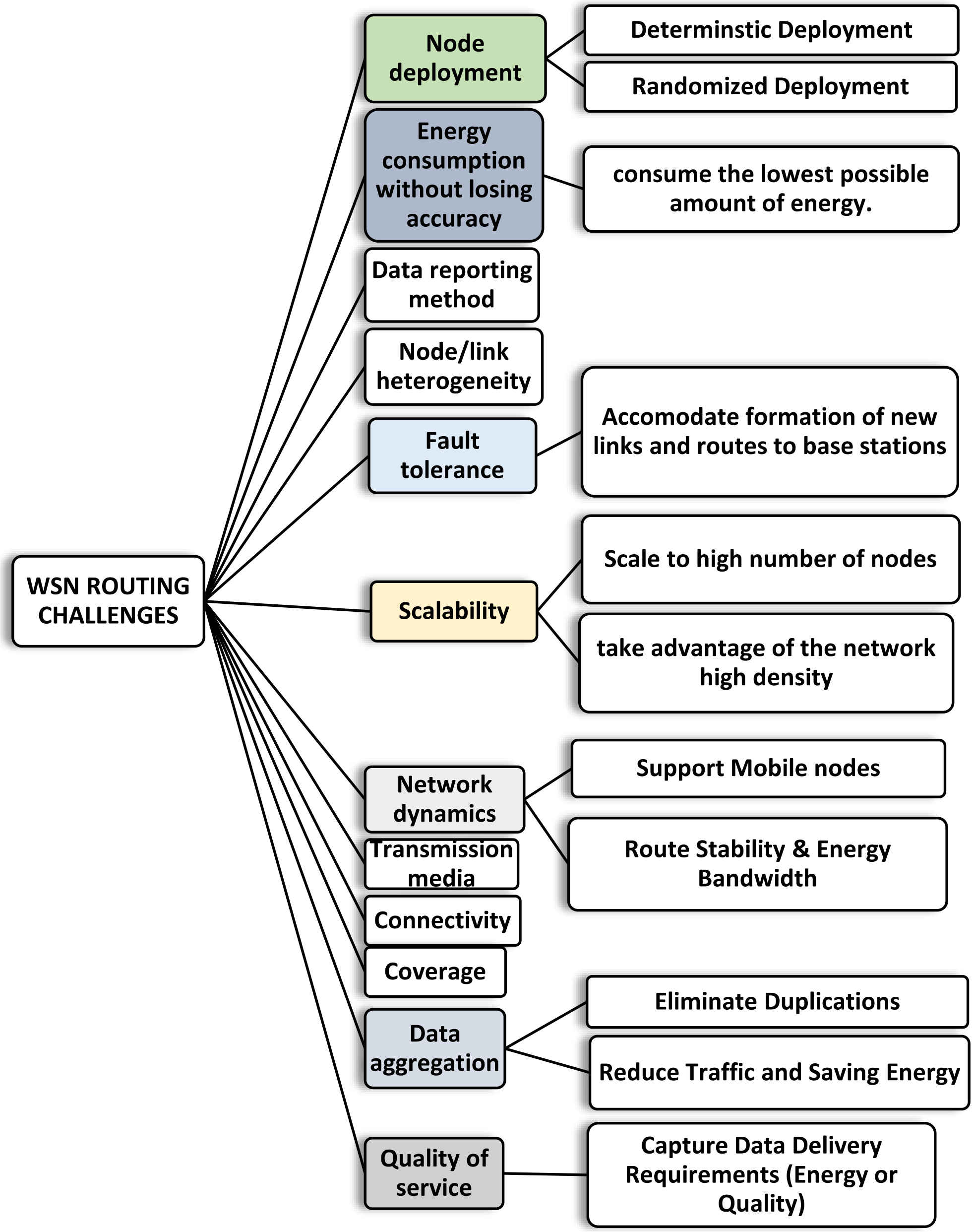
WSN ROUTING CHALLENGES
Node deployment
Determinstic Deployment
Randomized Deployment
Energy consumption without losing accuracy
consume the lowest possible amount of energy.
Data reporting method
Node/link heterogeneity
Fault tolerance
Accomodate formation of new links and routes to base stations
Scalability
Scale to high number of nodes
take advantage of the network high density
Network dynamics
Support Mobile nodes
Route Stability & Energy Bandwidth
Transmission media
Connectivity
Coverage
Data aggregation
Eliminate Duplications
Reduce Traffic and Saving Energy
Quality of service
Capture Data Delivery Requirements (Energy or Quality)

Figure 5: Coverage strategies taxonomy for WSNs

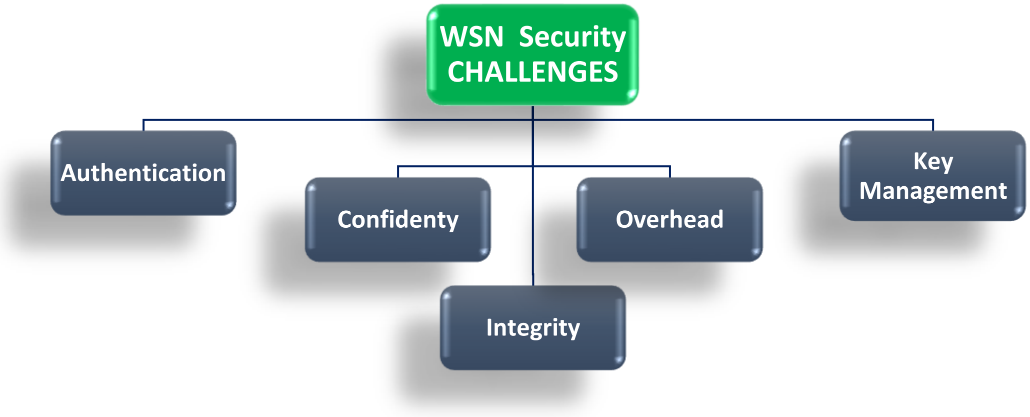

Figure 6: Taxonomy of Security Open Issues

7. Future Research Directions

Despite numerous works on WSN security, there are numerous unresolved issues. WSN security research is currently scattered, with each organization focusing on specific concerns or characteristics. It is critical to have an integrated strategy for diverse areas of WSN security. Several areas must be investigated in terms of secure routing, as there needs to be faster coverage because the scale of WSN operation is enormous, with thousands or millions of sensor nodes. WSNs have dynamic topology, and routing tables are subject to immediate modifications, so the routing protocols must have fast coverage. There must also be energy-optimized routing protocols to improve efficiency while providing security against possible attacks. As shown in Figure 7: future directions of research on routing protocols in WSNs. The future directions of research on routing protocols in WSNs have to concentrate on the following:

- Adding node mobility and multi-sink capabilities to the new routing protocols while meeting security and QoS standards will assist in securing networks and increasing their lifetimes.
- Because many learning algorithms rely on partial data and feedback, the discovering techniques of the route update are used to book all convenient routes from the source to the desired destination. The packets are separated and sent through different routes. Feedback is obtained to evaluate path performance, ensuring optimal efficiency through dynamic data allocation. Such a method will promote appropriate routing unpredictability. Furthermore, the data is arbitrarily separated into several pathways. These features provide excellent protection against various forms of attacks.
- Most traditional routing techniques are intended to communicate by utilizing optimal paths. WSNs are based on resources; such a system quickly depletes the resources along the best routes. Furthermore, it can improve system predictability. It is worth noting that all packets are sent via a single path, making routing methods more vulnerable to assaults. The energy-aware algorithm has been improved to assess these issues.
- Numerous protocols aid in resolving WSN security threats, but no one protocol or technique can address all security concerns and meet all need domains. As in [58], the author provides RADS, a rule-based anomaly detection system that can observe and detect timely Sybil attacks in various WSNs. This protocol doesn't require encryption methods or third-party trusted party authority; it reduces the overhead imposed by sensor node connection, and it is cost-effective in that each node may detect more than one Sybil assault without needing additional hardware enforcement. However, this approach is unable to detect indirect Sybil attacks. The author should improve the system's detection of threats like wormholes, floods, and sinkhole assaults. To make the system handle direct Sybil attacks, the author should also use a stochastic environment and genuine attack patterns. Finally, they must ensure that the RADS approach does not consume electricity.

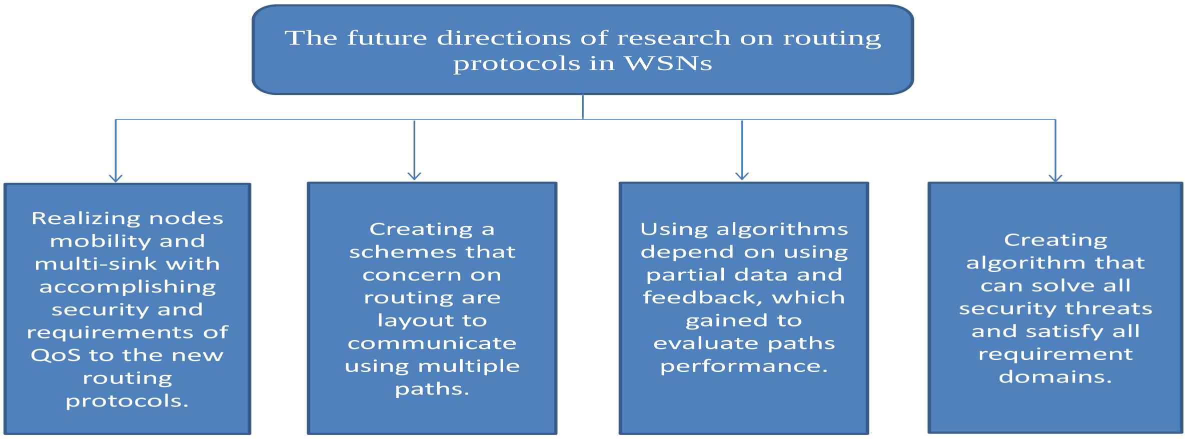
The future directions of research on routing protocols in WSNs
Realizing nodes mobility and multi-sink with accomplishing security and requirements of QoS to the new routing protocols.
Creating a schemes that concern on routing are layout to communicate using multiple paths.
Using algorithms depend on using partial data and feedback, which gained to evaluate paths performance.
Creating algorithm that can solve all security threats and satisfy all requirement domains.

Figure 7: Future research directions

8. Conclusion

The importance of WSNs cannot be overstated as the computing world is becoming more compact and portable. Because of their traditional wireless media, complex heterogeneous resources, and unpredictable topology, WSNs confront various security concerns. While routing in WSNs is the act of finding the optimum way between nodes, data on this route is vulnerable to several sorts of attacks, such as Sybil, Hello Flood, Wormhole, Sinkhole, and Selective Forwarding, in which the adversary is concerned with inserting misleading data into the network or sabotaging it. As a result, a robust defence system against such attacks is required. However, building a sensor network routing protocol that meets state-of-the-art sensor routing protocols' security and energy savings goals is still a work in progress. Such protocols rely on self-regulation, nodes, and BS that only hold local information.

Furthermore, the system must be globally known to establish security, which is an expensive process for sensor networks. Moreover, security is a multi-layered issue. If data is injected into any layer, it cannot be transmitted to the following layers, necessitating multi-security solutions that ensure comprehensive security across all protocol stacks.

Acknowledgments

……
…………………………………………………………………………….

Disclosure

This research did not receive any specific grant from funding agencies in the public, commercial or not-for-profit sectors. There is no Conflict of Interest

References

[1] S. Agrawal and D. Vieira, ""A survey on Internet of Things"," Abakós, vol. 1, no. 2, pp. 78–95, 2013.
[2] P. Sethi and S. R. Sarangi, ""Internet of things: architectures, protocols, and applications"," J. Electr. Comput. Eng., vol. 2017, 2017.
[3] A. Singh, A. Payal, and S. Bharti, ""A walkthrough of the emerging IoT paradigm: Visualizing inside functionalities, key features, and open issues"," J. Netw. Comput. Appl., vol. 143, pp. 111–151, 2019.
[4] S. Korade, V. Kotak, and A. Durafe, ""A review paper on internet of things (IoT) and its applications"," Int. Res. J. Eng. Technol., vol. 6, no. 6, pp. 1623–1630, 2019.
[5] Z. Mohamadian and S. H. HosseiniNazhad, ""Investigating the structure and challenges of the Internet of Things"," J. Artif. Intell. Electr. Eng., vol. 8, no. 31, pp. 34–42, 2019.
[6] V. Naresh and N. Lee, ""A review on biosensors and recent development of nanostructured materials-enabled biosensors"," Sensors, vol. 21, no. 4, p. 1109, 2021.
[7] H. F. Atlam, A. Alenezi, A. Alharthi, R. J. Walters, and G. B. Wills, ""Integration of cloud computing with internet of things: challenges and open issues"," in 2017 IEEE international conference on internet of things

(iThings) and IEEE green computing and communications (GreenCom) and IEEE cyber, physical and social computing (CPSCom) and IEEE smart data (SmartData), 2017, pp. 670–675.
[8] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, ""Wireless sensor networks: a survey"," Comput. Netw., vol. 38, no. 4, pp. 393–422, 2002.
[9] S. Hasan, Z. Hussain, and R. K. Singh, ""A survey of wireless sensor network"," Int J Emerg Technol Adv Engin, vol. 3, no. 3, pp. 487–492, 2013.
[10] D. Puccinelli and M. Haenggi, ""Wireless sensor networks: applications and challenges of ubiquitous sensing"," IEEE Circuits Syst. Mag., vol. 5, no. 3, pp. 19–31, 2005.
[11] M. F. Othman and K. Shazali, ""Wireless sensor network applications: A study in environment monitoring system"," Procedia Eng., vol. 41, pp. 1204–1210, 2012.
[12] M. A. Matin and M. M. Islam, ""Overview of wireless sensor network"," Wirel. Sens. Netw.-Technol. Protoc., vol. 1, no. 3, 2012.
[13] P. Völgyesi, A. Nádas, X. Koutsoukos, and Á. Lédeczi, ""Air quality monitoring with sensormap"," in 2008 International Conference on Information Processing in Sensor Networks (ipsn 2008), 2008, pp. 529–530.
[14] H. Chawla, ""Some issues and challenges of Wireless Sensor Networks"," Int. J. Adv. Res. Comput. Sci. Softw. Eng., vol. 4, no. 7, pp. 236–239, 2014.
[15] S. Mirshahi, A. Akbari, and S. Uysal, ""Implementation of structural health monitoring based on RFID and WSN"," in 2015 IEEE 28th Canadian Conference on Electrical and Computer Engineering (CCECE), 2015, pp. 1318–1323.
[16] K. Maraiya, K. Kant, and N. Gupta, ""Application based study on wireless sensor network"," Int. J. Comput. Appl., vol. 21, no. 8, pp. 9–15, 2011.
[17] S. Sharma, D. Sethi, and P. P. Bhattacharya, ""Wireless sensor network structural design and protocols: A survey"," Commun. Appl. Electron. CAE–ISSN, pp. 2394–4714, 2015.
[18] J. Li, X. Guo, L. Guo, S. Ji, M. Han, and Z. Cai, ""Optimal routing with scheduling and channel assignment in multi-power multi-radio wireless sensor networks"," Ad Hoc Netw., vol. 31, pp. 45–62, 2015.
[19] J. Chen, R. Du, Q. Wang, and S. Yao, ""Secure routing based on network coding in wireless sensor networks"," in 2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, 2013, pp. 58–64.
[20] K. Lin, C.-F. Lai, X. Liu, and X. Guan, ""Energy efficiency routing with node compromised resistance in wireless sensor networks"," Mob. Netw. Appl., vol. 17, no. 1, pp. 75–89, 2012.
[21] S. A. Abdel-Razek, H. S. Marie, A. Alshehri, and O. M. Elzeki, ""Energy Efficiency through the Implementation of an AI Model to Predict Room Occupancy Based on Thermal Comfort Parameters"," Sustainability, vol. 14, no. 13, p. 7734, 2022.
[22] S. S. Mariammal and J. Gayathri, ""Ensuring higher security for gathering and economically distributing the data in social wireless sensor networks"," Procedia Comput. Sci., vol. 47, pp. 408–416, 2015.
[23] E. Ashraf, N. F. Areed, H. Salem, E. H. Abdelhay, and A. Farouk, ""FIDChain: Federated Intrusion Detection System for Blockchain-Enabled IoT Healthcare Applications"," in Healthcare, 2022, vol. 10, no. 6, p. 1110.
[24] N. Abdel-hamid, L. M. Labib, and H. A. Ali, ""Wireless Sensor Networks (WSNs): New trends in Secure Routing Techniques"," Int. J. Comput. Appl., vol. 975, p. 8887.
[25] A. E. Guerrero-Sanchez, E. A. Rivas-Araiza, J. L. Gonzalez-Cordoba, M. Toledano-Ayala, and A. Takacs, ""Blockchain mechanism and symmetric encryption in a wireless sensor network"," Sensors, vol. 20, no. 10, p. 2798, 2020.
[26] R. Magán-Carrión, R. A. Rodríguez-Gómez, J. Camacho, and P. García-Teodoro, ""Optimal relay placement in multi-hop wireless networks"," Ad Hoc Netw., vol. 46, pp. 23–36, 2016.
[27] H. Wang, H. E. Roman, L. Yuan, Y. Huang, and R. Wang, ""Connectivity, coverage and power consumption in large-scale wireless sensor networks"," Comput. Netw., vol. 75, pp. 212–225, 2014.
[28] M. Sajwan, A. K. Sharma, and K. Verma, ""Analysis of scalability for hierarchical routing protocols in wireless sensor networks"," in Proceedings of ICETIT 2019, Springer, 2020, pp. 107–116.
[29] S. F. Ochoa and R. Santos, ""Human-centric wireless sensor networks to improve information availability during urban search and rescue activities"," Inf. Fusion, vol. 22, pp. 71–84, 2015.
[30] M. Bendjima and M. Feham, ""Multi-agent system for a reliable routing in WSN"," in 2015 Science and Information Conference (SAI), 2015, pp. 1412–1419.
[31] S. Sengupta, M. Chatterjee, and K. Kwiat, ""A game theoretic framework for power control in wireless sensor networks"," IEEE Trans. Comput., vol. 59, no. 2, pp. 231–242, 2009.
[32] G. Sun, L. Zhao, Z. Chen, and G. Qiao, ""Effective link interference model in topology control of wireless Ad hoc and sensor networks"," J. Netw. Comput. Appl., vol. 52, pp. 69–78, 2015.

[33] X. Chu and H. Sethu, ""Cooperative topology control with adaptation for improved lifetime in wireless ad hoc networks"," in 2012 Proceedings IEEE INFOCOM, 2012, pp. 262–270.

[34] A. E. Abdulla, H. Nishiyama, N. Ansari, and N. Kato, ""HYMN to improve the scalability of Wireless Sensor Networks"," in 2011 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), 2011, pp. 519–524.

[35] A. Nazi, M. Raj, M. D. Francesco, P. Ghosh, and S. K. Das, ""Robust deployment of wireless sensor networks using gene regulatory networks"," in International Conference on Distributed Computing and Networking, 2013, pp. 192–207.

[36] A. Nazi, M. Raj, M. Di Francesco, P. Ghosh, and S. K. Das, ""Efficient communications in wireless sensor networks based on biological robustness"," in 2016 International Conference on Distributed Computing in Sensor Systems (DCOSS), 2016, pp. 161–168.

[37] F. Chen and R. Li, ""Sink node placement strategies for wireless sensor networks"," Wirel. Pers. Commun., vol. 68, no. 2, pp. 303–319, 2013.

[38] M. Iwata, S. Tang, and S. Obana, ""Sink-based centralized transmission scheduling by using asymmetric communication and wake-up radio"," in 2017 IEEE Wireless Communications and Networking Conference (WCNC), 2017, pp. 1–6.

[39] S. Das, S. Barani, S. Wagh, and S. S. Sonavane, ""Energy efficient and trustable routing protocol for wireless sensor networks based on genetic algorithm (E2TRP")," in 2016 International Conference on Automatic Control and Dynamic Optimization Techniques (ICACDOT), 2016, pp. 154–159.

[40] W. Wu, N. Xiong, and C. Wu, ""Improved clustering algorithm based on energy consumption in wireless sensor networks"," Iet Netw., vol. 6, no. 3, pp. 47–53, 2017.

[41] N. Zaman, L. Tang Jung, and M. M. Yasin, ""Enhancing energy efficiency of wireless sensor network through the design of energy efficient routing protocol"," J. Sens., vol. 2016, 2016.

[42] J. Higuera and J. Polo, ""Interoperability in wireless sensor networks based on IEEE 1451 standard"," in Wireless Sensor Networks and Energy Efficiency: Protocols, Routing and Management, IGI Global, 2012, pp. 47–69.

[43] Y. Gu, F. Ren, Y. Ji, and J. Li, ""The evolution of sink mobility management in wireless sensor networks: A survey"," IEEE Commun. Surv. Tutor., vol. 18, no. 1, pp. 507–524, 2015.

[44] G. Tuna and V. C. Gungor, ""A survey on deployment techniques, localization algorithms, and research challenges for underwater acoustic sensor networks"," Int. J. Commun. Syst., vol. 30, no. 17, p. e3350, 2017.

[45] S. P. Singh and S. C. Sharma, ""A survey on cluster based routing protocols in wireless sensor networks"," Procedia Comput. Sci., vol. 45, pp. 687–695, 2015.

[46] Z. Manap, B. M. Ali, C. K. Ng, N. K. Noordin, and A. Sali, ""A review on hierarchical routing protocols for wireless sensor networks"," Wirel. Pers. Commun., vol. 72, no. 2, pp. 1077–1104, 2013.

[47] A. G. Kumar, R. Thiyagarajan, and N. Sripriya, ""Data centric based routing protocols for wireless sensor networks: A survey"," Int J Sci Res Publ, vol. 4, pp. 1–5, 2014.

[48] A. H. Iche and M. R. Dhage, ""Location-based routing protocols: A survey"," Int J Comput Appl, vol. 975, p. 8887, 2015.

[49] M. Brandl, K. H. Kellner, T. Posnicek, A. Kos, C. Mayerhofer, and C. Fabian, ""An efficient source initiated on-demand data forwarding scheme for wireless sensor networks"," in 2009 7th International Conference on Information, Communications and Signal Processing (ICICS), 2009, pp. 1–7.

[50] A. Abduvaliyev, A.-S. K. Pathan, J. Zhou, R. Roman, and W.-C. Wong, ""On the vital areas of intrusion detection systems in wireless sensor networks"," IEEE Commun. Surv. Tutor., vol. 15, no. 3, pp. 1223–1237, 2013.

[51] F. Rabeb, N. Nejah, K. Abdennaceur, and S. Mounir, ""An Extensive Comparison among DSDV, DSR and AODV Protocols in wireless sensor network"," in International Conference on Education and e-Learning Innovations, 2012, pp. 1–4.

[52] R. V. Biradar, V. C. Patil, S. R. Sawant, and R. R. Mudholkar, ""Classification and comparison of routing protocols in wireless sensor networks"," Spec. Issue Ubiquitous Comput. Secur. Syst., vol. 4, no. 2, pp. 704–711, 2009.

[53] K. Gupta and V. Sikka, ""Design issues and challenges in wireless sensor networks"," Int. J. Comput. Appl., vol. 112, no. 4, pp. 0975–8887, 2015.

[54] P. Samundiswary and P. Dananjayan, ""Performance analysis of trust based AODV for wireless sensor networks"," Int. J. Comput. Appl., vol. 4, no. 12, pp. 6–13, 2010.

[55] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, ""A survey on sensor networks"," IEEE Commun. Mag., vol. 40, no. 8, pp. 102–114, 2002.

[56] R. P. Mahapatra and R. K. Yadav, ""Descendant of LEACH based routing protocols in wireless sensor networks"," Procedia Comput. Sci., vol. 57, pp. 1005–1014, 2015.
[57] Y. Wang, G. Attebury, and B. Ramamurthy, ""A survey of security issues in wireless sensor networks"," 2006.
[58] P. Sarigiannidis, E. Karapistoli, and A. A. Economides, ""Detecting Sybil attacks in wireless sensor networks using UWB ranging-based information"," Expert Syst. Appl., vol. 42, no. 21, pp. 7560–7572, 2015.