A Systematic Literature Review of Routing Protocols in Wireless Sensor Networks: Current Trends and Future Directions

Peter Maina Mwangi

Abstract—Wireless Sensor Networks (WSNs) have emerged as a key technology in various applications, ranging from environmental monitoring to healthcare and industrial automation. Efficient data communication among sensor nodes is essential for the success of WSNs, and routing protocols play a critical role in determining the overall network performance. This review aims to comprehensively analyze and synthesize the existing literature on routing protocols in WSNs, highlighting their strengths, weaknesses, and applications. The review also aims to highlight various performance indicators (metrics) used by researchers to evaluate the performance of routing protocols in WSN, emerging trends that may influence the future design of routing protocols in WSN, and security concerns in WSN routing protocols. To attain this goal, a systematic literature review process was employed based on Barbara Kitchenham's original guidelines (2007). Relevant papers were retrieved from major academic databases such as Elsevier, Springer, Wiley, IEEE, and the ACM Digital Library, as well as preprints posted on arXiv. The findings demonstrate that various existing routing protocols have been created throughout time and are classified as data-centric, location-based, mobility-based, multi-path-based, heterogeneity-based, and hierarchical routing protocols. The routing protocols in WSNs vary depending on the application and network architecture. The paper also focuses on the performance criteria used to evaluate them, their pros, limitations, areas of applications, emerging trends in WSN, and security challenges. The future of WSN routing protocols is moving toward intelligent, adaptive, and robust protocols that can serve larger, more complex networks.

Index Terms--Artificial intelligence (AI), Machine Learning (ML), performance Indicators, Routing Protocols, Security Wireless Sensor Network (WSN)

I. Introduction

Wireless Sensor Networks (WSNs) are one of the paradigm-changing technological advancements with applications ranging from environmental monitoring, and industrial automation to healthcare and smart cities [1] . These networks feature a large number of sensor nodes, most of which are deployed in the field and operate unattended to sense various phenomena, then wirelessly collect and report the data. WSNs can function with the help of reliable and efficient routing protocols, which are known to be sole for broadcasting data in WSN [2].

With the advancement of Wireless Sensor Networks (WSNs) and as they face a variety of issues, routing protocols is one area that we must have deep coverage. These protocols are used to ensure the proper and reliable transmission of data from source nodes, or other endpoints, to sink node(s), influencing important key performance indicators like energy consumption, latency, and packet delivery fractions. Wireless Sensor Networks (WSNs), characterized by both constrained sensor nodes and dynamic environmental dynamics, require routing protocols resilient to such challenges [1], [3].

Several researchers have proposed and designed different routing protocols for WSN addressing distinct challenges to meet the desired network performance. Protocol types (commonly flat, hierarchical, or location-based routing with their strengths and limitations). The WSN routing landscape is evolving rapidly as a result of technological progress, new application scenarios and the growing fusion with other technologies like IoT or 5G [4], [5].

Due to the various kinds of routing protocols and ever-changing nature of WSNs, it is important for researchers, practitioners as well as policymakers to know where things currently stand [6]. A systematic review of the literature, not only confirm us about what we know from existing protocols but also highlight knowledge gap which gives direction for further research. Further, with the adoption of WSN in an increasingly broader range of applications where security and privacy have become a high-priority concern (e.g., military, healthcare application), it is important to review existing security solutions for routing protocols as well as suggest some directions that could be explored further on.

The purpose of this systematic review is to bring into a single forum and investigate all the available studies related to routing protocols in WSNs. In synthesizing the existing research, it is hoped that a mechanism for which this large body of work can be built upon will have been provided to researchers in the field and mitigating insights at optimizing WSN deployments could offered to practitioners along with

Manuscript revised on November 11, 2024 and published on December 04, 2024

Peter Maina Mwangi*, School of Computing and Information Technology, Murang'a University of Technology, Kenya.*
Email: pmwangi@mut.ac.ke

doi: 10.32622/ijrat.124202401

informing policymakers as per the advancements made on these challenges within wireless sensor networks. By providing an exhaustive review based on current trends and needs for possible directions of the field, this work contributes to ways that would make WSNs more efficient reliable [9] secure thus aiding in further future progress it can have spanning its diversified application sections.

II. Related Work

This paper provides a detailed discussion of the most existing routing protocols in WSN - and highlights their deficiencies, ongoing approach, and future perspectives with a list of other reviews conducted by different researchers. In this work, we classify WSN routing based on how they function. There are several routing protocols available for wireless sensor networks. However, many of them can be divided into several broad categories [1].

Multiple reviews have been conducted over the years on existing routing protocols in WSN. Some reviews include:

Rashmi Sonkar and Shish Ahmad [6] did a comprehensive review of routing protocols in wireless sensor networks. They examined routing protocols in-depth with an emphasis on extending network lifespan. The review recommended several categories for routing protocols, including single-path and multiple-path routing protocols. The weakness of this review is that the researchers only reviewed two categories of routing protocols but there are other categories such as location-based routing protocols, data-centric routing protocols, hierarchical routing protocols, mobility-based routing protocols, and heterogeneity-based Routing Protocols. Another drawback is that it is a typical literature review, which means there is no methodology and the author may be biased.

Another review was done Abhay Gaidhani and Amol Potgantwar [4] where they carried out a review of machine learning -Based Routing Protocols for Wireless Sensor Network Lifetime together with their benefits, limitations, and parameters that affect network longevity. The study's main flaws are the lack of statistical data on the discussed protocols and the absence of a statistical chart for the risk analysis. The paper additionally lacks a research methodology.

Swati Jaryal, Devendra Prasad and Amit Verma [7] performed a review Routing Protocol in the Wireless Sensor Network. The paper mostly focuses on energy-efficient routing protocols in Wireless Sensor Networks. The weakness of this paper is that it is very brief and there is no methodology hence the author may be biased.

Nagesh Kumar and Yashwant Singh [8] reviewed with the aim of classification and analysis of routing protocols for WSN and concluded with open research issues in routing strategies in WSN. The researchers determined that numerous routing strategies in Wireless Sensor Networks have been created over time to preserve energy and other resources such as memory for WSN. The routing protocols are primarily dependent on the applications and architecture of WSN. The challenge with this review is that it is very brief and it lacks the methodology the researcher used to arrive at the conclusions.

III. Research Method

This research was carried out as a systematic literature review based on Barbara Kitchenham's original guidelines (2007) to systematically review existing and current routing protocols for Wireless Sensor Networks. The review also focuses on the features, advantages, disadvantages and. current trends in routing protocols in WSNs. The researcher used these standards because they are specifically designed for software engineers and computer scientists. They offer domain-specific guidance when dealing with technical papers, software development studies, programming approaches, and IT initiatives. A scientific literature review identifies, evaluates, and interprets relevant research for a certain question, topic area, or phenomenon of interest. This study is classified as a tertiary literature review since it focuses on systematic literature reviews, which are considered secondary studies. The approach is broken down into three steps.

A. Review planning

Planning a systematic literature review (SLR) is an important step in ensuring that the review is thorough, objective, and adheres to a planned approach. The planning phase involves identifying the need for a review, defining subjects for study, and developing a review technique.

B. Objectives of the Systematic Literature Review

The purpose of this literature study is to compile and assess the extensive body of knowledge about routing protocols in WSNs. By integrating existing research, we hope to lay a platform for future research, give insights for practitioners to optimize WSN deployments, and enlighten policymakers about the challenges and advances in this crucial component of wireless sensor networks. This work contributes to ongoing efforts to improve the efficiency, energy, reliability, and security of WSNs, opening the way for their sustained growth and innovation in a wide range of application domains. The study asks many research questions to stimulate discussion.

doi: 10.32622/ijrat.124202401

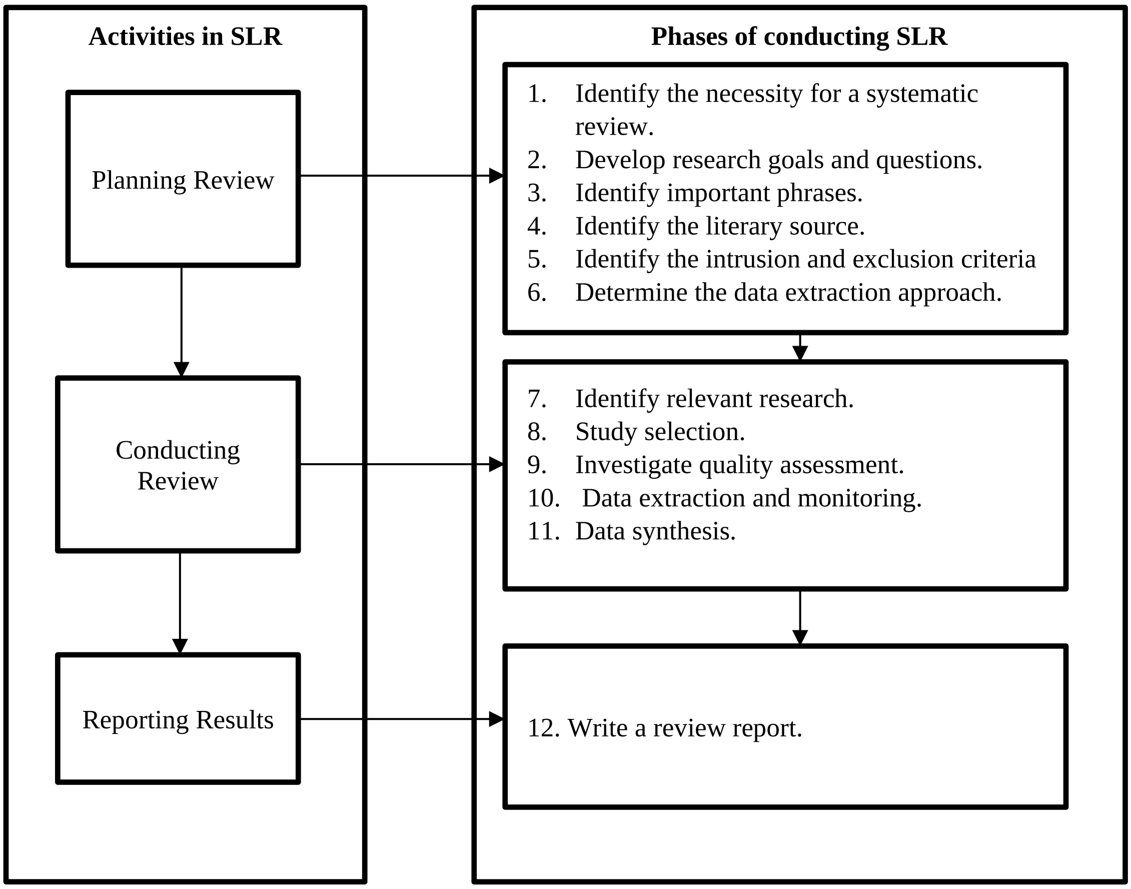
Activities in SLR
Planning Review
Conducting Review
Reporting Results
Phases of conducting SLR
1. Identify the necessity for a systematic review.
2. Develop research goals and questions.
3. Identify important phrases.
4. Identify the literary source.
5. Identify the intrusion and exclusion criteria
6. Determine the data extraction approach.
7. Identify relevant research.
8. Study selection.
9. Investigate quality assessment.
10. Data extraction and monitoring.
11. Data synthesis.
12. Write a review report.

Fig. 1: Phrases of Conducting Systematic Literature Review Based on Barbara Kitchenham's original guidelines (2007)

C. *Research questions*

To reach the goal of the research, several research questions were used.

i. What are the primary categories of routing protocols used in wireless sensor networks (WSNs)?
ii. What are the crucial performance indicators for evaluating routing protocols in WSNs?
iii. What are the advantages, limitations, and application areas of existing routing protocols in WSNs?
iv. What emerging technologies or techniques may influence the future design of routing protocols in WSNs?
v. What are the most significant security concerns in WSN routing protocols, and how have existing protocols addressed these concerns?

D. *Conducting the Review*

Conducting a systematic literature review (SLR) involves carefully following the protocol designed during the planning phase and systematically analyzing the collected studies. To conduct this review the researcher took the following steps: Search the Literature, Eligibility Criteria, data extraction and synthesis, and reporting and Interpretation.

E. *Search Literature*

This process deals with defining the search strategy, searching a variety of academic databases to ensure comprehensive coverage of the literature, and how to document the search. The search strategy reflected the scope of the review, covering key concepts related to routing protocols, Wireless Sensor Networks (WSNs), Energy-Aware Routing, performance metrics used to evaluate routing protocols in WSN and other relevant terms., select relevant databases, and document your entire process. The researcher reviewed relevant papers from the following major academic databases, including Elsevier, Springer, Wiley, IEEE, ACM Digital Library, Citeseer Library, and arXiv preprints. The investigation was restricted to works published between 2015 and September 2024 since the researcher was especially interested in recent advances in this field of study. The papers were analyzed to identify relevant publications for further research using titles, abstracts, and keywords. To find more publications, a backward and forward snowballing strategy was applied. This involved using the reference lists of selected research and citations to identify further papers.

F. *Eligibility Criteria*

This document outlines the criteria for conducting a literature review and grouping research for synthesis. This establishes the parameters of the review. This ensures only relevant studies are included in the data analysis. Articles for the Systematic Literature Review were chosen in three stages: first by title, then by abstract, and finally by paper. This study utilized the following criteria to determine inclusion and exclusion:

i. Articles about existing routing protocols for wireless sensor networks should be included.
ii. Include comparative studies of routing protocols for Wireless Sensor Networks (WSN).
iii. Use the most recent version of each article (if any).
iv. Consider the publications published between 2015 and June 2024.
v. Articles must be peer-reviewed or published in conference proceedings.
vi. Non-peer-reviewed journal or conference papers are excluded.

G. Data Extraction and Synthesis

A table has been generated for the years 2015-2024, displaying the academic databases from which papers were reviewed, as well as the quantity of journal papers studied. Table 1 displays papers picked from each academic database.

TABLE 1: LIST OF JOURNAL PAPERS COLLECTED FROM MAJOR ACADEMIC DATABASES

Academic Databases	No of Journal Papers Reviewed
Elsevier	60
IEEE	55
ACM Digital library	24
SPRINGER	21
Wiley	20
arXiv.	20
Total	200

The data extraction tool captured pertinent bibliographic information (e.g., title, author, database, and page numbers) for each article and provided a hyperlink for further reading. The article abstract was a key component of the initial analysis for each article.

To answer questions, the researcher examined the abstract, introduction, literature review, and results parts of all selected studies. The choice to include an article in the final review occurred in two stages. The first step was to read each abstract and determine whether the paper was relevant to the review. The relevance of the abstract was determined by comparing it to the aforementioned search terms. The review considered the authors, publication date, article type (e.g., journal, conference proceedings), technique-based taxonomy, and datasets. These details must be discovered before the research questions can be addressed. Figure 2 shows a flow chart for selecting articles and papers.

IV. REPORTING AND INTERPRETATION

This section discusses the responses to the research questions found in the reviewed publications. The study investigates routing protocols in wireless sensor networks, including their performance metrics, limitations, problems, upcoming technologies, and security issues. The research findings are structured according to the study questions:

RQ 1: What are the primary categories of routing protocols used in wireless sensor networks (WSNs)?

Wireless sensor networks (WSNs) are made up of small nodes that can sense, compute, and communicate wirelessly [12]. Many routing, power management, and data dissemination protocols have been developed expressly for WSNs, where energy awareness, limited computing power, limited resources, unreliable communication, memory limitation, unattended operations, and limited bandwidth are some of the important design considerations. The study identified that various routing protocols in WSN have been proposed by different developers [1], [9], [10]. These routing protocols in WSN vary according to application and network architecture and they have been classified according to Table 2 below [2], [11]- [13]:

TABLE 2: CLASSIFICATIONS OF ROUTING PROTOCOLS FOR WSNS

Classifications	Protocols
Data-centric Protocols	EAD, Directed Diffusion
Location-based Protocols	GEAR, MECN, GAF
Mobility-based Protocols	Tree-Based Dynamic Proxy, TTDD, SEAD
Multipath-based Protocols	CHR, IDSQ
Heterogeneity-based Protocols	Energy-aware routing, SAR
Hierarchical Protocols	HEED, PEGASIS, LEACH, VGA, TEEN, APTEEN, GAF, SOP, SEP

Data-centric routing protocols in WSNs are intended to improve data transfer primarily focusing on the data rather than individual node addresses [9]. These protocols treat the network as a distributed database, allowing data to be requested based on properties (such as temperature and pressure) rather than node IDs. These protocols' major properties include data aggregation, in-network processing, and reducing duplicated transmissions. SPIN, Directed Diffusion, Gradient-Based Routing (GBR), COUGAR, and Rumor Routing are some examples. The general limitation of data-centric protocols is that they frequently impose delays since data must be collected at intermediary nodes before being delivered to the sink. This renders them unsuitable for time-sensitive applications [9]. Also, because nodes aggregate and analyze data in the network, they are susceptible to attacks like as data tampering, false data injection, and node compromise. Secure routing mechanisms are frequently required to ensure the integrity of the data. Lastly, data-centric protocols often presume a static network topology. In circumstances where sensor nodes or sinks are mobile, these protocols may struggle to maintain effective routing [4].

doi: 10.32622/ijrat.124202401

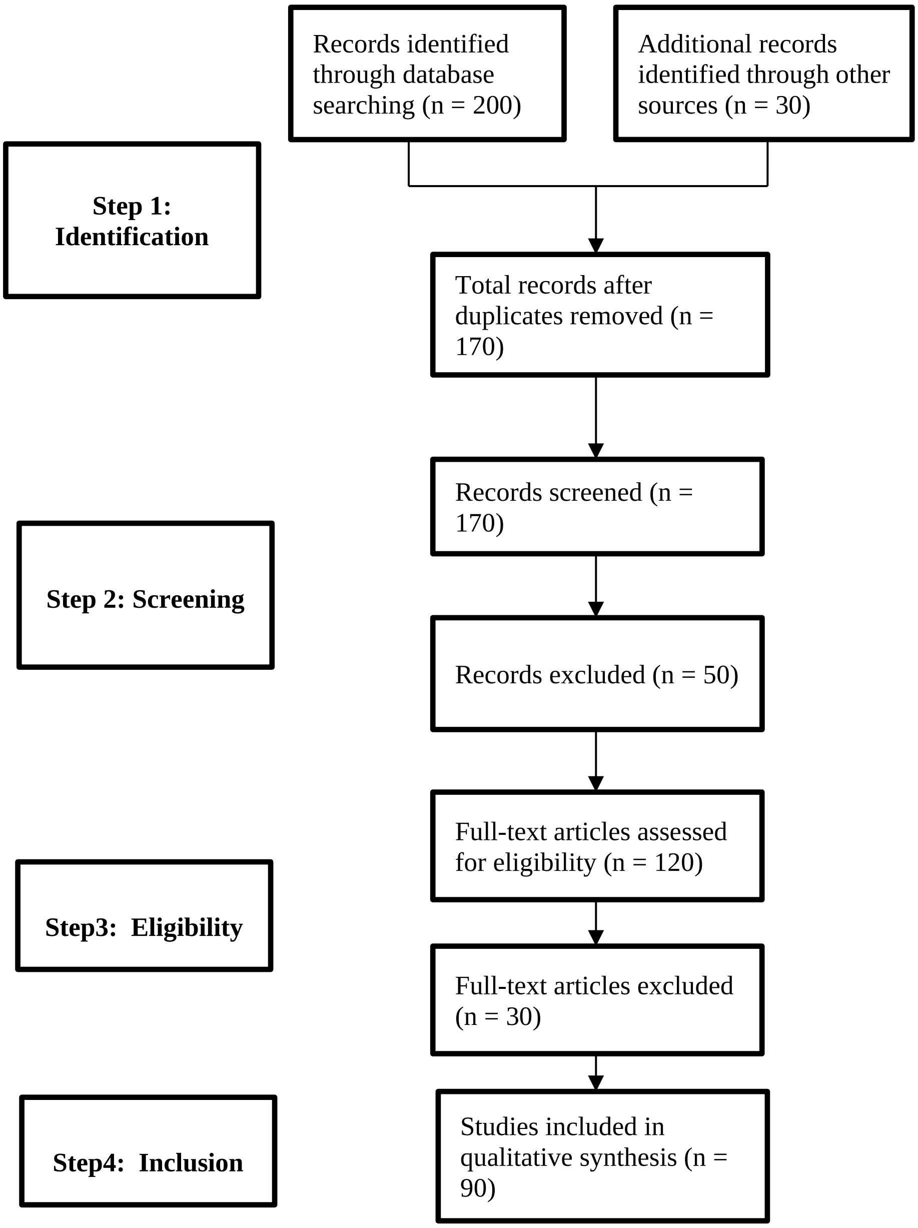
Records identified through database searching (n = 200)
Additional records identified through other sources (n = 30)
Step 1: Identification
Total records after duplicates removed (n = 170)
Records screened (n = 170)
Step 2: Screening
Records excluded (n = 50)
Full-text articles assessed for eligibility (n = 120)
Step3: Eligibility
Full-text articles excluded (n = 30)
Step4: Inclusion
Studies included in qualitative synthesis (n = 90)

Fig. 2: Flow chart for selecting the articles

V. Reporting and interpretation

This section discusses the responses to the research questions found in the reviewed publications. The study investigates routing protocols in wireless sensor networks, including their performance metrics, limitations, problems, upcoming technologies, and security issues. The research findings are structured according to the study questions:

RQ 1: What are the primary categories of routing protocols used in wireless sensor networks (WSNs)?

Wireless sensor networks (WSNs) are made up of small nodes that can sense, compute, and communicate wirelessly [12]. Many routing, power management, and data dissemination protocols have been developed expressly for WSNs, where energy awareness, limited computing power, limited resources, unreliable communication, memory limitation, unattended operations, and limited bandwidth are some of the important design considerations. The study identified that various routing protocols in WSN have been proposed by different developers [1], [9], [10]. These routing protocols in WSN vary according to application and network architecture and they have been classified according to Table 2 below [2], [11]- [13]:

Table 2: Classifications of Routing Protocols for WSNs

Classifications	Protocols
Data-centric Protocols	EAD, Directed Diffusion
Location-based Protocols	GEAR, MECN, GAF

doi: 10.32622/ijrat.124202401

Mobility-based Protocols	Tree-Based Dynamic Proxy, TTDD, SEAD
Multipath-based Protocols	CHR, IDSQ
Heterogeneity-based Protocols	Energy-aware routing, SAR
Hierarchical Protocols	HEED, PEGASIS, LEACH, VGA, TEEN, APTEEN, GAF, SOP, SEP

Data-centric routing protocols in WSNs are intended to improve data transfer primarily focusing on the data rather than individual node addresses [9]. These protocols treat the network as a distributed database, allowing data to be requested based on properties (such as temperature and pressure) rather than node IDs. These protocols' major properties include data aggregation, in-network processing, and reducing duplicated transmissions. SPIN, Directed Diffusion, Gradient-Based Routing (GBR), COUGAR, and Rumor Routing are some examples. The general limitation of data-centric protocols is that they frequently impose delays since data must be collected at intermediary nodes before being delivered to the sink. This renders them unsuitable for time-sensitive applications [9]. Also, because nodes aggregate and analyze data in the network, they are susceptible to attacks like as data tampering, false data injection, and node compromise. Secure routing mechanisms are frequently required to ensure the integrity of the data. Lastly, data-centric protocols often presume a static network topology. In circumstances where sensor nodes or sinks are mobile, these protocols may struggle to maintain effective routing [4].

Location-based routing protocols in WSNs make routing decisions based on the geographical position of sensor nodes. These protocols presume sensor nodes are aware of their position (by GPS or other localization techniques) and use that knowledge to efficiently route data. The goal is to save energy, reduce latency, and increase scalability by using node position information to send data to the base station or sink. [5]. An optimal route can be created using location information by calculating the distance between two nodes. Geographic Adaptive Fidelity (GAF), GPSR (Greedy Perimeter Stateless Routing), Geographic and Energy-Aware Routing (GEAR), Minimum Energy Communication Network (MECN), and SPAN are some examples of location-based routing protocols. One of these protocols' shortcomings is that obtaining and keeping node position information (by GPS or other means) incurs expense, and the accuracy of localization can influence routing decisions. Another challenge is that in heavily populated networks, location-based routing may experience congestion or excessive routing overhead as multiple nodes attempt to route data to the same place at the same time. Lastly, location-based routing is vulnerable to attacks such as spoofing, in which a rogue node advertises a bogus location to disrupt routing.

Mobility-based routing protocols are intended specifically for Wireless Sensor Networks (WSNs) in which either the sensor nodes, the sink (data collecting point), or both are mobile. Traditional WSN protocols assume a static network architecture, however, mobility is critical in many real-world applications (for example, automobile networks, disaster response, and healthcare systems). Mobility presents issues such as frequent topological changes, increased energy consumption, and route maintenance, which these protocols seek to address [14]. Scalable Energy-Efficient Asynchronous Dissemination (SEAD), Dynamic Proxy Tree-Based Data Dissemination, Two-Tier Data Dissemination (TTDD), Low Energy Adaptive Clustering Hierarchy for Mobile Nodes (LEACH-M) and Mobility-Based Clustering (MBC)are examples of these categories. The drawback is that the mobility of nodes or sinks might cause frequent route failures, necessitating the protocols to constantly update routing information, which can raise overhead. Additionally, managing mobility necessitates regular monitoring and updating of routes, which might increase energy usage when compared to static protocols. Finally, mobility frequently causes delays in data delivery due to the time required to re-establish routes or wait for mobile nodes to come into range.

Heterogeneity-based routing algorithms are intended for Wireless Sensor Networks (WSNs) in which nodes differ in terms of energy levels, computational capabilities, and communication range. Unlike homogeneous networks, which have comparable nodes, heterogeneous WSNs use the diversity of node capabilities to improve performance, energy efficiency, and network lifetime. In such protocols, high-powered nodes (also known as super nodes) are frequently assigned more resource-intensive responsibilities like as data aggregation, routing, or serving as cluster chiefs. Meanwhile, lower-powered nodes are responsible for sensing and forwarding data. This tiered topology optimizes energy usage and extends network life by intelligently dividing jobs based on node capabilities [15]. Examples of this routing protocol are Stable Election Protocol (SEP), Distributed Energy-Efficient Clustering (DEEC), Energy-Efficient Cluster Head Election Protocol (EECHE), SAR, and energy-aware routing. One is burdened with the difficulty of managing a network composed of any-sized nodes, requiring complex algorithms for load distribution and communication cost balancing. Another challenge is that if the network were to rely too much on resource-rich nodes, they could become bottlenecked or lint faster than naturally leading to uneven expenditure of energy. Thirdly, security problems may be exacerbated in a heterogeneous network because high-capacity nodes attract more attacks with the potential to disturb the communication of an entire network.

The Hierarchical routing protocols are one of the most used in Wireless Sensor Networks (WSNs). The entire network is divided into clusters or layers with sensor nodes grouped together and within each group there is an elected leader referred to as cluster head. Ultimately, the main goal is to reduce energy consumption and enhance scalability by reducing communication overhead to prolong the network lifetime. In hierarchical routing, sensor nodes do not communicate directly with the base station. Instead, they send their data to the cluster head, which collects and sends it

doi: 10.32622/ijrat.124202401

to the base station. This two-tier technique minimizes the number of transmissions to the base station, resulting in decreased energy consumption [16]. Examples of these protocols include LEACH (Low-Energy Adaptive Clustering Hierarchy), TEEN (Threshold-sensitive Energy Efficient sensor Network protocol), PEGASIS (Power-Efficient Gathering in Sensor Information Systems) and HEED (Hybrid Energy-Efficient Distributed Clustering). One of the limitations of these protocols is that the cluster head is in charge of data gathering and transmission to the base station, which can rapidly exhaust its energy. If cluster heads are not adequately controlled, they might create bottlenecks or fail early in the network's operation. Another concern is that forming and sustaining clusters can result in increased communication and computation overhead, particularly in large networks or when the network topology changes often. Although cluster heads can rotate, poor cluster head selection might cause some nodes to consume much more energy than others, resulting in premature failure. Finally, hierarchical protocols may cause delays since data must be forwarded to the cluster head before reaching the base station, which is not ideal for applications that require real-time data transmission.

RQ 2: What are the crucial performance indicators for evaluating routing protocols in WSNs?

The study identified that there are various performance indicators for evaluating routing protocols in WSN. These can provide key performance indicators (KPIs) or metrics to evaluate the efficiency, scalability & efficacy of the protocol. Dynamic and resource-constrained environments like WSNs are benchmarked by these KPIs for evaluating the efficiency of routing protocol. The following are some of the most important performance indicators identified in the study [17]-[20].

Since the battery life of sensor nodes is very limited, energy consumption plays a key role in estimating routing protocol efficiency in WSNs. This smart routing system greatly decreases energy on your network improving network longevity. It uses energy per packet, residual energy, and network lifetime which depicts the number of live as well as the number of dead nodes at the end simulation.

Scalability: It is one of the metrics to determine how efficient routing protocols are in WSN. We are particularly interested in the endurance of a routing protocol; i.e., how many sensors can it sustain while still maintaining reasonable performance. The protocol also needs to allow the network to scale up and down in size, managing larger numbers of nodes without a huge drop-in performance.

Throughput is also a performance metric for routing protocols in WSNs. Throughput—The combined volume of data that has been transferred successfully across a network over time. A higher throughput means, data is reached successfully to the sink or base station and results in good protocol routing performance.

Another criterion to be evaluated in WSN with other routing systems is Latency or End-to-End Delay. These metrics measure the distribution delay of the package from source to destination (sink). Real-time or time-sensitive applications need rapid data delivery, hence low latency is crucial

.

Another metric to evaluate the performances of routing protocols in WSN is Packet Delivery Ratio (PDR). This is a ratio of the packets that reach this destination node divided by the total number of generated source nodes. A high packet delivery ratio (PDR) being high means that communication and routing work. Packets received by the destination node (R2) / Packets sent from source to R1, such transmissions are done either from nodes to cluster heads or from the latter ones towards a base station.

This potentially gives an idea of more traditional routing system performance via routing overhead. It is the extra control packets or messages needed to build and maintain network paths. The lower the routing overhead, the lesser would-be network congestion and better bandwidth utilization that increases overall efficiency. This includes control messages as such routing updates, acknowledgments, and routing table maintenance.

Well, Congestion Control is another metric that might evaluate the performance of routing protocols in WSN. The solution to this question revolves around the effectiveness of routing protocol concerning network traffic congestion, especially in cases high-density areas or data flow is higher than expected… This mitigates packet loss and better communication. Another indication to evaluate the performance of routing approaches in WSNs is network topology adaptability. It has to do with the routing protocol's ability to respond and adjust when a network changes (i.e. nodes on the move, fail, or if new nodes are entering into YOUR space). With that level of performance, we can keep up with the worst-case scenarios very well in a dynamic environment.

Lastly, route stability is another indicator that may be used to evaluate the performance of the routing protocol in WSN. Stability assesses the durability of established routes over time. Frequent route changes owing to node failures or network topology changes can result in increased overhead, packet losses, and delays. A routing protocol with stable routes provides consistent performance.

RQ 3: What are the Advantages, limitations, and application areas of existing routing protocols in WSNs?

The study reviewed the numerous routing protocols for WSN that have been developed over the years, as discussed in RQ1, and classified them as Data-Centric Protocols, Location-Based Routing Protocols, Mobility-Based Routing Protocols, Heterogeneity-Based Routing Protocols, and

doi: 10.32622/ijrat.124202401

Hierarchical Routing Protocols. These routing techniques have not completely addressed the issue of energy consumption and other concerns in WSN. This section discusses the advantages, limitations, and application areas of some of the routing protocols listed in Tables 3-7 below, according to their classification [21]-[26].

TABLE 3: COMPARISON OF DATA-CENTRIC PROTOCOLS

Protocol	Advantages	Disadvantages	Applications
Directed Diffusion	Energy-efficient, adaptive to event detection	High delay for real-time applications	Event-based monitoring (e.g., fire detection)
Rumor Routing	Reduces energy by limiting flooding	May miss events, not suitable for dense networks	Event-driven WSNs (e.g., intrusion detection)
SPIN	Reduces redundant transmissions	No guaranteed data delivery	Environmental monitoring
COUGAR	Supports complex queries and processing	High computational overhead at nodes	Wildlife monitoring, pollution tracking
GBR	Load balancing, fault tolerance	Higher delay, gradient maintenance overhead	Disaster recovery, fault-tolerant systems

TABLE 4: COMPARISON OF LOCATION-BASED ROUTING PROTOCOLS

Protocol	Advantages	Disadvantages	Applications
GAF	Reduces energy consumption via node sleeping	Delays due to nodes turning off and on	Environmental monitoring, military surveillance
GEAR	Balances energy consumption and geographical distance	Higher overhead due to energy monitoring	Geographic data dissemination, precision agriculture
GPSR	Simple, stateless routing using greedy forwarding	Local minimum problems, accuracy-dependent	Mobile sensor networks, VANETs, urban monitoring
MECN	Minimizes energy consumption	Overhead from maintaining relay regions	Long-term environmental monitoring, smart agriculture
SPAN	Energy-efficient through adaptive coordination	Coordinator selection may be suboptimal	Large-scale WSNs, smart buildings, habitat monitoring

TABLE 5: COMPARISON OF MOBILITY-BASED ROUTING PROTOCOLS

Protocol	Advantages	Disadvantages	Applications
SEAD	Scalable, energy-efficient, no global routing	Delays due to sink mobility	Wildlife monitoring, mobile environmental monitoring
TTDD	Supports large networks, balances energy usage	Grid-based structure introduces complexity	VANETs, military surveillance, disaster response
MobiRoute	Predicts mobility, reduces route breaks	Complex prediction models required	Mobile healthcare, emergency services, mobile robotics
LEACH-M	Supports mobility with energy-efficient clustering	Frequent re-clustering leads to overhead	Mobile healthcare systems, patient monitoring
MBC	Adaptable clustering reduces transmissions	Frequent re-clustering introduces delays	Urban surveillance, smart city applications

TABLE 6: COMPARISON OF HETEROGENEITY-BASED ROUTING PROTOCOLS

Protocol	Advantages	Disadvantages	Applications
SEP	Increases network lifetime, simple implementation	Depends heavily on high-energy nodes	Environmental monitoring, healthcare
DEEC	Adaptive to changing energy levels, balanced energy usage	High computation and communication overhead	Industrial automation, military applications
HEED	Efficient cluster head selection reduces energy holes	Communication overhead due to periodic updates	Smart grids, remote monitoring
EECHE	Balances energy usage, considers multiple factors	Complex decision-making process, high overhead	Harsh environments, disaster recovery
M-LEACH	Better energy efficiency than LEACH, scalable	Requires initial energy resource distribution	Long-term monitoring, smart agriculture, healthcare

TABLE 7: COMPARISON OF HIERARCHICAL ROUTING PROTOCOLS

Protocol	Advantages	Disadvantages	Applications
LEACH	Simple, energy-efficient, rotates cluster heads	Random cluster head selection may lead to an imbalance	Environmental monitoring, healthcare systems
TEEN	Suitable for time-sensitive applications, energy-efficient	Threshold setting can lead to missed data	Time-critical applications like disaster monitoring
PEGASIS	Reduces direct transmissions to the base station	High latency due to chain-based communication	Data gathering in large sensor fields
HEED	More balanced energy consumption considers proximity	More complex cluster head selection process	Smart cities, environmental and industrial monitoring
H-PEGASIS	Further reduces energy usage, improves scalability	Increased latency, complex implementation	Industrial monitoring, smart grid, agricultural monitoring

RQ 4: What emerging technologies or techniques may influence the future design of routing protocols in WSNs?

The study discovered that the design of routing protocols in Wireless Sensor Networks (WSNs) is fast evolving as a result of numerous emerging technologies and novel methodologies. These developments are pushing the limits of energy efficiency, data processing, and security in WSNs. The important emerging themes listed below may have a substantial impact on the future design of routing protocols [27]- [31] .

Some of the current emerging areas to design routing protocols in WSN include Machine Learning and Artificial Intelligence. In routing protocols, AI/ML techniques are applied for intelligent dynamic route selection, dynamic cluster head selection, energy management, and traffic handling. For example, reinforcement learning can help nodes learn the optimal routing patterns based on their previous experiences. In this way, the techniques of clustering can be maximized towards node grouping and data aggregation; thus, leading to efficiency in terms of energy use. Predictive models enable the ability to predict potential node failures or trends in network traffic, and upon prediction, change the routes accordingly. AI-based protocols respond well to dynamic changes in network conditions like node mobility, energy levels, and topologies.

Another emerging trend that can be applied in the routing protocol construction in WSN is blockchain technology. Blockchain supplies decentralized, secure, and tamper-proof data management important for WSN applications that require intensive trust, such as financial, military, or medical applications. The technology of blockchain may thus be used for routing protocols to perform secure and transparent route discovery and node verification. More importantly, blockchain enables incentive-based processes within cooperative routing protocols, for instance, rewarding nodes for their data forwarding, and therefore, higher collaboration and energy efficiency by the nodes become encouraged.

Energy harvesting mechanisms are another newly developed technology that can be exploited for the elaboration of the routing protocols for WSNs. Energy harvesting technology allows sensor nodes to collect energy from their environment, such as solar, thermal, or RF energy, reducing dependence on batteries. Routing protocols will need to adapt their behavior dynamically depending on the energy-harvesting capability of the node. While nodes with high energy-harvesting potential may assume more network responsibilities, energy-limited nodes could conserve their resources by restricting their involvement in routing tasks. In leveraging this technology, energy-adaptive protocols will play a determining role in the lifetime related to WSNs.

These future technologies and methodologies will pave the way for the future of WSN routing protocols in the direction of energy efficiency, security, scalability, and adaptability in dynamic and heterogeneous contexts. Unfortunately, it would appear that for now, all these different advances need to be brought together to develop more intelligent, secure, and robust WSNs that could meet such ever-growing demands from so many contemporary applications.

RQ 5: What are the most significant security concerns in WSN routing protocols, and how have existing protocols addressed these concerns?

According to the findings of the study, Wireless Sensor Networks (WSNs) face several significant routing security concerns due to inherent vulnerabilities in their architecture, such as limited computational resources, energy constraints, and the often hostile or unattended environments in which they operate. The security concerns in WSN routing protocols can be broadly classified as risks to data integrity, confidentiality, availability, and authentication. The following are the most important security concerns in WSN routing protocols identified in this study, as well as how current protocols have solved them [32]- [34], [3] :

Arguments reported compromise nodes as one of the security concerns in the WSN routing protocols. The sensor nodes may be deployed in an open or hostile area where they are easily physically captured and tampered with. An attacked node would allow an attacker to take full control of the node by modifying its routing behavior to introduce fabricated data into the network, eventually resulting in false routing decisions. To handle this issue, some protocols like LEACH (Low-Energy Adaptive Clustering Hierarchy) and SPINS (Security Protocols for Sensor Networks) incorporate authentication aspects in their architecture so that hacked nodes cannot deliver misleading data. Cryptographic techniques such as symmetric key encryption are used to ensure that only authorized nodes connect to the network. IDS has also been proposed in various protocols, which detect intrusion by observing anomaly node behavior in case of node compromise.

Sinkhole attacks are another risk with the WSN routing system. A sinkhole attack occurs when a malicious node advertises a high-quality route (for example, claiming to have a shorter path to the base station), attracts local traffic, and then misroutes or drops packets. This undermines both data integrity and network performance. To address this concern, protocols such as TinySec and Ariadne include route validation algorithms and authenticated broadcasting to ensure that nodes do not promote bogus routes. Furthermore, multi-path routing schemes, such as those used in the Multipath Ring Routing Protocol (MRRP), aid in transmitting data across numerous channels, making it more difficult for a single compromised node to disrupt the entire network.

Another problem in WSN is a wormhole attack. In a wormhole attack, two or more collaborating malicious nodes form a tunnel (wormhole) between them and relay packets at high speeds to disrupt the usual routing mechanism, leading

doi: 10.32622/ijrat.124202401

the network to assume that the wormhole is the shortest path. Solutions to combat wormhole attacks include the use of Geographical routing techniques, such as Geographic and Energy-Aware Routing (GEAR), use of node location to detect suspect routing activity. Other protocols use hop-count monitoring to reduce wormhole assaults by ensuring that routing pathways have a proper hop count, which can aid in detecting unnatural shortcuts caused by wormholes.

The HELLO Flood Attack is also a security problem for WSN. In this attack, a malicious node floods the network with HELLO packets (broadcast messages), posing as a legitimate node with a strong connection and misleading other nodes into routing traffic via it. This can result in network congestion or energy depletion. To address the concern, protocols such as LEACH and SPINS use bidirectional link verification to verify that nodes only react to HELLO messages if they can also receive responses from the broadcaster. Furthermore, signal strength-based and distance-based validation procedures can keep malevolent nodes from claiming to be nearby when they aren't.

Blackhole attacks are a risk in WSN. A blackhole attack occurs when a rogue node pretends to have the quickest path to the base station and then drops all packets it receives rather than forwarding them. Addressing the Concern, existing protocols employ watchdog techniques to monitor neighboring nodes' forwarding activity. If a node repeatedly fails to forward packets, it is classified as malevolent. Multi-path routing, as done in SEEM (Secure and Energy-Efficient Multipath Routing), can also help to lessen the impact of blackhole nodes by providing alternate paths.

Other security threats include jamming attacks in wireless sensor networks. The jamming attacks shut down the communication channels by continuously issuing signals of interference that cause network congestion or refuse services. Frequency hopping and spread spectrum techniques are employed in enhancing resilience in communication against jamming. Moreover, the adaptive power control makes it possible for nodes to dynamically adjust the transmission power by accommodating the jamming signal. Safe hierarchical routing protocols, such as LEAP (Localized Encryption and Authentication Protocol), can also use mechanisms of key management that make routing safe against jamming.

Replay Attack is another security concern in routing protocols for WSNs. This is a security hazard associated with WSN. Concern: In a replay attack, the malicious nodes intercept the valid packets and send them repeatedly after a while to disturb the usual activities of the network. Against the replay attacks, time-stamped messages and sequence numbers are sent intended by like SPINS protocols to ensure that the packet old is not repeated. With symmetric key encryption techniques, replayed communications might not be accepted - only when secure time synchronization is employed with them.

Eavesdropping and data confidentiality are security concerns in WSNs. Because WSNs usually send sensitive data (such as environmental data, health monitoring, and military information), eavesdropping on data packets can reveal confidential information. Protocols such as TinySec and SPINS use end-to-end encryption to maintain data secrecy, making it difficult for attackers to read even if they capture it. Key management systems play an important role in delivering secure and scalable encryption algorithms that reduce computational overhead on resource-constrained sensor nodes.

Another security problem with WSNs is the disclosure of routing information. If an attacker learns about the network's routing pathways, they can target crucial nodes or links, creating interruptions or launching more complex assaults such as sinkholes, selective forwarding, or black holes. Protocols like SERP (Secure and Efficient Routing Protocol) use encrypted routing updates and secure neighbor findings to prevent unauthorized nodes from accessing routing information. By encrypting route discovery packets and employing authenticated broadcasting, these protocols prevent attackers from discovering the network topology.

VI. Discussions

The study aims to review existing work on routing protocols in WSN. Kitchenham and Charters' systematic literature technique and suggestions were used in the study (2007). From 2015 to 2024, data were obtained from primary studies published in journal articles, conference proceedings, and selected arXiv preprints. After applying our selection criteria, the study identified 90 acceptable papers. The study's discussions are summarized below:

RQ1. The first research question addressed the basic categories of routing protocols. The research revealed that there are numerous types of routing protocols in wireless sensor networks. These routing protocols are classed as data-centric protocols, location-based protocols, mobility-based protocols, multi-path protocols, heterogeneity protocols, and hierarchical protocols. The study also provided examples for each category of routing protocols, as seen in Table 2 above.

RQ2. The study's second objective was aimed at identifying the key performance metrics for evaluating routing methods in WSNs. The study discovered that numerous performance indicators or metrics are utilized to assess the performance of routing protocols in WSNs. The identified performance parameters include energy consumption, scalability, latency, packet delivery ratio (PDR), routing overheads, congestion, and route stability.

RQ3. The study's third goal was to assess the benefits, limits, and potential applications of existing routing methods in WSNs. The investigation discovered that several routing protocols have been established over the years, as stated in RQ 1. The study concluded that routing protocols offer some advantages, but they have not fully addressed all design difficulties. The study identified several advantages, limits, and application areas, as given in Table 3-7 in the preceding section.

RQ4. The study's fourth focus was to determine how emerging technologies or methodologies might influence the future design of routing protocols in WSNs. The study discovered that numerous developing technologies or methodologies could influence the future design of routing protocols in WSNs. Machine learning and artificial intelligence, blockchain technology, and energy harvesting techniques are among the developing technologies highlighted as potentially influencing the future design of routing protocols in WSNs.

RQ5. The study's fifth research topic examined key security vulnerabilities in WSN routing methods and how existing protocols addressed these concerns. The study uncovered multiple security vulnerabilities with routing protocols, and researchers developed various techniques to counter these threats. This study discovered several types of attacks, including node compromise, sinkhole, wormhole, hello flooding, blackhole, jamming, replay, and eavesdropping.

VII. Conclusion

Wireless sensor networks (WSNs) have gained popularity in recent years and can be utilized for various applications. Wireless Sensor Networks' most important study areas include routing protocols, new trends, and security. Over the last few years, much effort has gone into developing effective, efficient, and secure routing algorithms for wireless sensor networks. Designing an effective, durable, scalable, and secure routing protocol in WSNs is a challenging undertaking. This paper reviewed, classified, and described many types of routing protocols, with a special emphasis on the performance criteria used to evaluate them, their benefits, limits, and application areas, developing trends in WSN, and security issues.

The future of WSN routing protocols is evolving toward intelligent, adaptive, and robust systems capable of supporting larger, more complicated networks. This evolution will rely heavily on AI and machine learning, as well as integration with edge and fog computing, increased security measures, energy-harvesting capabilities, and context-aware routing. With these advancements, WSNs will be able to handle a wide range of applications, including urban IoT networks, environmental monitoring, industrial automation, and healthcare. Future work could explore adaptive or hybrid routing protocols that react to dynamic network conditions more efficiently, also focus on creating robust, lightweight security routing protocols tailored to WSNs with constrained resources, and explore how WSN routing protocols can integrate with emerging technologies like 5G, edge computing, AI, and machine learning.

Conflict of Interest

The authors declare no conflict of interest.

References

[1] S. Anjali and M. Sharma, "Wireless sensor networks: Routing protocols and security issues," in Fifth International Conference on Computing, Communications and Networking Technologies (ICCCNT), Hefei, China, 2014.

[2] Manimekala, "Wireless Sensor Networks: Routing Protocols," International Journal of Research in Advent Technology, , , vol. 7, no. 55, pp. 136-141, May 2019.

[3] K. M. A. Hassan, M. A. Madkour and S. A. Nouh, "A REVIEW OF SECURITY CHALLENGES AND SOLUTIONS IN WIRELESS SENSOR NETWORKS," Journal of Al-Azhar University Engineering Sector, pp. 914 - 938, 2023.

[4] G. R. Abhay and P. D. Amol, "A Review of Machine Learning-Based Routing Protocols for Wireless Sensor Network Lifetime," in International Conference on Recent Advances in Science and Engineering, 2023.

[5] R. S. Battula and O. S. Khanna, "Geographic Routing Protocols for Wireless Sensor Networks: A Review.," International Journal of Engineering and Innovative Technology (IJEIT), , vol. 2, no. 12, pp. 39-42, 2013.

[6] S. Rashmi and A. Shish, "A comprehensive review on routing protocols in wireless sensor networks," NeuroQuantology, vol. 20, no. 16, pp. 1785-1816, 2022.

[7] J. Swati, P. Devendra and A. Verma, "Routing Protocol in Wireless Sensor Network: A Review," International Journal of Computer Applications, pp. 16-18, 2017.

[8] K. Nagesh and S. Yashwant, "Routing Protocols in Wireless Sensor Networks : A Brief Review," Computer Science, Engineering, 2018.

[9] S. K. Sing, M. P. S. and ". D K Singh, "Routing protocols in Wireless Sensor Networks-A Survey,," International Journal of Computer Science and Engineering Survey, vol. 1, no. 2, pp. 63-83, 2010.

[10] H. Mohapatra, S. Debnath and A. K. Rath, "Energy Management in Wireless Sensor Network Through EB-LEACH," International Journal of Research and Analytical Reviews, pp. 56-60, 2019.

[11] A. Chandel, V. Chouhan and S. Sharma, "A Survey on Routing Protocols for Wireless Sensor Networks," Advances in Information Communication Technology and Computing, vol. 135, p. 143–164, 2021.

[12] A. Sarkar and T. S. Murugan, "Routing protocols for wireless sensor networks: What the literature says?," Alexandria Engineering Journal, vol. 55, no. 4, pp. 3173-3183, 2016.

[13] M. K. Khan, M. Shiraz, Q. Shaheen, S. A. Butt, R. Akhtar, M. A. Khan and W. Changda, "Hierarchical Routing Protocols for Wireless Sensor Networks: Functional and Performance Analysis," Hindawi Journal of Sensors, pp. 1-18, 2021.

[14] S. K. Singh, M. P. Singh and ". D K Singh, "Routing protocols in Wireless Sensor Networks-A Survey," International Journal of Computer Science and Engineering Survey, vol. 1, no. 2, pp. 63-83, 2010.

[15] J. Balen, D. Zagar and G. Martinovic, "Quality of Service in Wireless Sensor Networks-A Survey and Related Patents," Recent Patents on Computer Science,, vol. 4, no. 3, pp. :188-202, 2011.

[16] X. Yang, D. Deng and Meifeng Liu, " "An overview of routing protocols on Wireless Sensor Network," 2015 4th International Conference on Computer Science and Network Technology (ICCSNT) , no. doi: 10.1109/ICCSNT.2015.7, pp. 1000-1003,, 2015.

[17] R. Saxena, V. Rishiwal and O. Singh, "Performance Evaluation of Routing Protocols in Wireless Sensor Networks," in 3rd International Conference On Internet of Things: Smart Innovation and Usages (IoT-SIU), 2018, 2028.

[18] K. K. Kumar, J. Bhanu, G. U. Rani and A. S. Rao, "Performance Evaluation of Routing Protocols in Wireless Sensor Networks," in National Conference on Contemporary Advancements in Computers,

doi: 10.32622/ijrat.124202401

Networks in Machine Learning (NCACNM), 2017.

[19] R. Zaghal, F. Alyounis and S. Salah, "Performance Evaluation of Routing Protocols in Wireless Sensor Networks: A Comparative Study," in Proceedings of the Fifth International Conference on Informatics and Applications, Takamatsu, Japan, 2016.

[20] T. Rahman, I. Ahmad, A. Zeb, I. Khan, G. Ali and M. ElAffendi, "Performance Evaluation of Routing Protocols for Underwater Wireless Sensor Networks," Journal of Marine Science and Enineering , vol. 11, no. 1, 2023.

[21] R. Azizi, "Consumption of Energy and Routing Protocols in Wireless Sensor Network," Network Protocols and Algorithms , pp. 76-87, 2016.

[22] N. Shabbir and S. R. Hassan, "Routing Protocols for Wireless Sensor Networks (WSNs)',," Wireless Sensor Networks - Insights and Innovations. InTech,, Oct. 04, 2017.

[23] A. Kumar, H. Y. Shwe, K. J. Wong and P. H. J. Chong, "Location-Based Routing Protocols for Wireless Sensor Networks: A Survey," Wireless Sensor Network, vol. 9, no. 1, pp. 25-72, 2017.

[24] T. K. Pandey, I. Singh and M. Kumar, "A Review on the Performance of Different Routing Protocols in WSN- A Comparative Survey," International Journal of Current Microbiology and Applied Sciences, vol. 8, no. 10, pp. 1476-1485, 2019.

[25] M. Shwetha and S. Krishnaveni, "A Systematic Analysis, Outstanding Challenges, and Future Prospects for Routing Protocols and Machine Learning Algorithms in Underwater Wireless Acoustic Sensor Networks," Journal of Interconnection Networks, 202.

[26] P. C and D. Suresha, "Existing Routing Protocols for Wireless Sensor Network – A Study," International Journal of Computational Engineering Research (IJCER), vol. 4, no. 7, p. 2250 – 3005, 2014.

[27] B. Saoud, I. Shayea, M. H. Azmi and A. A. El-Saleh, "New scheme of WSN routing to ensure data communication between sensor nodes based on energy warning," Alexandria Engineering Journal, vol. 80, no. 1, pp. 397-407, 2023.

[28] J. X, S. A and C. M-Y., "Energy-efficient routing sensing technology of wireless sensor networks based on Internet of Things.," Journal of High Speed Networks., pp. 225-235, 2021.

[29] A. Umar, Z. Khalid, M. Ali, M. Abazeed, A. Alqahtani, R. Ullah and H. Safdar, "A Review on Congestion Mitigation Techniques in Ultra-Dense Wireless Sensor Networks: State-of-the-Art Future Emerging Artificial Intelligence-Based Solutions," Applied Sciences, vol. 13, no. 22, 2023.

[30] S. Shah, Z. Sun, K. Zaman, A. Hussain, I. Ullah, Y. Ghadi and M. Khan, "Advancements in Neighboring-Based Energy-Efficient Routing Protocol (NBEER) for Underwater Wireless Sensor Networks," Sensors , vol. 23, 2023.

[31] D. R, R. S, S. J. Kavita, K. S and I. MF., "Enhanced Smart Energy Efficient Routing Protocol for Internet of Things in Wireless Sensor Nodes," Sensors (Basel), vol. 22, no. 16, 2022.

[32] F. M, M. MN, S. MFM and A. A., "Wireless sensor network security: A recent review based on state-of-the-art works.," International Journal of Engineering Business Management, vol. 15, 2023.

[33] R. Jadhav and V. Vatsala, "Security Issues and Solutions in Wireless Sensor Networks," International Journal of Computer Applications, vol. 162, no. 2, 2017.

[34] K. S. Adu-Manu, F. Engmann, G. Sarfo-Kantanka, G. E. Baiden and B. A. Dulemordzi, "WSN Protocols and Security Challenges for Environmental Monitoring Applications: A Survey," HindawiJournal of Sensors, vol. 2022, no. 1, pp. 1-20, 2022.

AUTHORS PROFILE

Peter Maina Mwangi is a Tutorial Fellow at the Department of Computer Science, Murang'a University of Technology, Kenya. He received his BSc. in Computer Science from Busoga University, Uganda in 2010, his MSc in Data Communication and Networks from KCA University, Kenya in 2018 and PhD in Computer Science from Murang'a University of Technology, Kenya in 2024. His Research interest is in Computer Network, Security, artificial Intelligence. He is a Professional Member of Institute of Electrical and Electronics Engineers (IEEE), the International Association of Engineers (IAENG) and Scientific & Technical Research Association (STRA)

doi: 10.32622/ijrat.124202401

APPENDIX I

TABLE 8: COMPARATIVE TABLE OF WSN ROUTING PROTOCOLS

Protocol Type	**Examples**	**Description**	**Authors**	**Future Directions and Recommendations**
Data-Centric Protocols	Directed Diffusion, SPIN (Sensor Protocols for Information via Negotiation), Rumor Routing	Protocols that focus on querying and aggregating data based on attributes, reducing redundant transmissions.	Intanagonwiwat et al. (Directed Diffusion), Heinzelman et al. (SPIN)	- Enhance data aggregation methods to improve energy efficiency. - Integration with machine learning for dynamic query optimization. - Address challenges of scalability and continuous data generation.
Location-Based Routing Protocols	GAF (Geographic Adaptive Fidelity), GPSR (Greedy Perimeter Stateless Routing), GeRaF (Geographic Random Forwarding)	Utilize node geographical positions for routing decisions to minimize route state information.	Xu et al. (GAF), Karp and Kung (GPSR)	- Develop more accurate localization techniques with reduced overhead. - Integrate energy-efficient localization to handle dense and dynamic networks. - Address limitations posed by complex terrains and obstacles.
Mobility-Based Routing Protocols	MobiHoc, CBR-Mobile (Cluster-Based Routing for Mobile Nodes), MSWSN (Mobile Sensor Wireless Sensor Networks)	Designed for WSNs with mobile nodes; adapt dynamically to changes in topology.	Kumar et al. (CBR-Mobile), Basagni et al. (MobiHoc)	- Create adaptive protocols with minimal energy consumption during mobility. - Address potential data loss with predictive mobility models. - Leverage AI for predictive routing and seamless handovers.
Heterogeneity-Based Routing Protocols	HEED (Hybrid Energy-Efficient Distributed Clustering), SEP (Stable Election Protocol), DEEC (Distributed Energy Efficient Clustering)	Exploit node heterogeneity by leveraging differences in energy, computation power, etc., for optimized performance.	Younis and Fahmy (HEED), Smaragdakis et al. (SEP)	- Develop load-balancing mechanisms to handle node diversity effectively. - Explore heterogeneous data processing and cooperative energy-sharing strategies. - Integration with multi-tiered IoT systems.
Hierarchical Routing Protocols	LEACH (Low-Energy Adaptive Clustering Hierarchy), TEEN (Threshold-sensitive Energy Efficient Network Protocol), PEGASIS (Power-Efficient GAthering in Sensor Information Systems)	Employ a layered structure with cluster heads to aggregate data and reduce communication overhead.	Heinzelman et al. (LEACH), Manjeshwar and Agrawal (TEEN)	- Reduce cluster head overhead through distributed clustering mechanisms. - Employ AI-driven algorithms for dynamic cluster formation. - Focus on minimizing intra-cluster energy dissipation.

doi: 10.32622/ijrat.124202401