Vol.3, No.6, Page 1347- 1357, 2025 https://doi.org/10.59628/jast.v3i6.1687 ISSN 2958-9568 JAST

SUN PUBLISHER

مجلة جامعة صنعاء للعلوم التطبيقية والتكنولوجيا
Sana'a University Journal of Applied Sciences and Technology
https://journals.su.edu.ye/index.php/jast/

Adapting GPSR Routing Protocol in Wireless Sensor Networks: Survey

Yosef A. Abdulmoghni [1,2] *, Sharaf A. Alhomdy[1] and Yahya Al-Ashmoery[2]

[1]**Department of Information Technology, Faculty of Computer Science and IT, Sana'a University, Sana'a, Yemen.,**
[2]**Department of Information Technology, Faculty of Computer and IT, Al-Razi University, Sana'a, Yemen.**

*Corresponding author: Youssef.almoghni@mail.com

Abstract

Objective: The aim of this survey is to provide a comprehensive review and evaluation of recent advancements in the Greedy Perimeter Stateless Routing (GPSR) protocol, with specific emphasis on special considerations for the individual challenges faced in Wireless Sensor Networks (WSNs), including energy constraints, scalability challenges, reliability, and security.
Methodology: Systematic review of literature was conducted using leading academic databases (e.g., IEEE Xplore, ACM Digital Library, Scopus) during 2015-2025. Studies were selected based on pre-specified inclusion criteria with focus on GPSR variants for WSNs aiming at energy efficiency, scalability, reliability, security, or compatibility with emerging technologies.
Key Results: Many GPSR adaptations are enumerated and categorized by survey. Noteworthy trends include utilization of optimization algorithms (e.g., PSO, ACO) and machine learning/AI (e.g., fuzzy logic, deep learning) for improvement in energy efficiency, fault tolerance, and security. Comparative study recognizes trade-offs with other adaptation techniques. Significant challenges such as localization accuracy, computational overhead, and issues of practical deployment are expounded upon.
Conclusions: While significant progress has been made in the adaptation of GPSR to WSNs, particularly by AI-based approaches, much remains to be done from the practical implementation and verification aspects beyond simulations. This survey synthesizes current knowledge, identifies research gaps, and suggests future directions based on lightweight security, robust localization, and real-world performance evaluation of current adaptations.

Article Info

Keywords:
Internet of Things (IoT), Quality-of-Service (QoS), Deep-Frying, WSNs, Base Station (BS).

Article History:
Received: 10-April-2025,
Revised: 24-August-2025,
Accepted: 30-October-2025,
Available online: 28 December 2025.

1. INTRODUCTION

Wireless sensor networks (WSNs) are a fundamental part of IoT systems, making it possible to collect and share data in various settings, from smart homes to industrial environments. Improving the performance of WSNs has become increasingly crucial because of their expanding use, especially with the rapid growth of Internet of Things (IoT) devices and applications [1]. Geographical routing protocols such as Greedy Perimeter Stateless Routing (GPSR), originally proposed by Al-Healyet al. [2], are suitable for WSNs because they are scalable and efficient in nature [3]. GPSR utilizes node location information for making routing decisions and hence is attractive for dynamic networks, although it was primarily proposed for general mobile ad hoc networks. WSNs have significant potential, but also entail considerable challenges. They often operate with limited resources and their environments can change quickly, making things unpredictable. Therefore, the GPSR needs to be fine-tuned and enhanced to address critical concerns, such as energy efficiency, maintaining network reliability, ensuring security, and ensuring that the system can scale smoothly without falling apart.

One of the biggest hurdles in WSNs is energy consumption management. Because many sensors operate on batteries and are often placed in remote or hard-to-reach areas, recharging or replacing them can be a real chal-

lenge. This makes energy conservation critical for maintaining a smooth network. To address this issue, recent advancements in GPSR have focused on fine-tuning the routing paths to reduce energy usage. For example, researchers have created energy-aware routing algorithms that prioritize paths based on the number of battery life sensors left. These smart algorithms help the network last longer by cleverly routing data through sensors that have more energy to spare [4]. Not only does this boost efficiency, it also ensures that the network stays up and runs for much longer, even in tough or unpredictable conditions. As WSNs grow to cover larger areas, older routing methods can struggle to keep up with them. To counter this, more recent versions of GPSR have included novel techniques such as hierarchical organization. These methods divide the network into smaller, manageable chunks, lessening complexity and enabling the system to scale more readily without being bogged down. Therefore, GPSR is a strong candidate [5]. WSNs normally operate in dynamic settings where the network topology can change quite frequently, either owing to sensor failure, movement, or interference from external sources. To handle these changes, existing GPSR extensions include mechanisms, such as real-time path updates and fault-tolerant techniques. By predicting the location of nearby nodes and removing unsuccessful nodes from the list, the protocol reduces the likelihood that data will be forwarded through them [5].

Another challenge in WSNs is that certain sensors can become overloaded with excessive data traffic, leading to delays or complete breakdowns in some cases. To prevent this, researchers have integrated load-balancing techniques into the GPSR adaptations. The adaptation approach is designed for load balancing among sensor nodes, minimizing energy imbalances, and ultimately prolonging the lifetime of the network [6]. Furthermore, the security of data transmission in WSNs is paramount, particularly as they are deployed in critical applications. GPSR, in its basic form, lacks inherent security mechanisms, making it vulnerable to various attacks that can compromise data integrity, confidentiality, and network availability. Addressing these security concerns is a crucial aspect of adapting GPSR for reliable WSN operation. These improvements demonstrate how GPSR is carefully adjusted to better fit the specific demands of WSNs, boosting their efficiency, scalability, and reliability. Although more work is needed, recently made strides are incredibly encouraging. WSNs are on track to play an even larger part in IoT applications, whether they monitor environmental shifts or help build smarter cities. The future looks bright for these networks, as they continue to evolve and expand their impact. High efficiency and low delay are advantages of the GPSR. In addition, in this method, the data packets are routed to the destination as unicast, which minimizes routing overhead. The decentralized approach of the GPSR protocol and routing decision making based on geographic information has made it attractive [7]. The GPSR's next hop is selected based on proximity to the destination, which has the effect of giving shorter paths and fewer communications overhead [8]. These advancements are particularly impactful in real-time applications, such as precision agriculture, disaster management, and smart city infrastructure, where reliable and low-power communication is essential. Through the optimization of GPSR for contemporary WSN problems, researchers have offered extended network lifetimes and stronger data transmission [9], supporting different IoT ecosystems.

This paper provides an overview of recent developments and adaptations of the GPSR protocol tailored to the unique WSN environment. section(1.1) discusses the selection process and the analysis of the studies covered in this overview. section(2) discusses various adaptation strategies for energy efficiency, scalability, reliability, security, and compatibility with emerging technologies. section(3) provides a comparative overview of the adaptation strategies. section(4) provides comparisons between GPSR and some of the most prominent WSN routing protocols. section(5) discusses practical issues associated with implementing these adaptations. section(6) discusses the limitations of the GPSR enhancements under consideration. Finally, section(7) concludes the paper.

1.1. Survey Methodology

To attain a systematic and comprehensive review of recent developments in modifying the GPSR protocol for Wireless Sensor Networks (WSNs), a systematic literature review methodology was followed. The search was conducted by identifying relevant studies from primary academic databases, including IEEE Xplore, ACM Digital Library, Scopus, and Google Scholar, from 2015 to 2025. The search process utilized the keywords in a combination, like "GPSR," "Wireless Sensor Network," "WSN," "routing protocol," "energy efficiency," "scalability," "reliability," "security," "adaptation," and "enhancement.". Certain exclusion and inclusion criteria were applied in this study. The inclusion criteria were peer-reviewed journal articles and conference articles in English specifically addressing adaptations or extensions of the GPSR protocol in the WSN scenario. Studies that focus on energy efficiency, scalability, reliability, security, and integration with emerging technologies have been prioritized. Exclusion criteria included studies that did not focus on GPSR in WSNs, non-English literature, non-peer-reviewed technical reports, gray literature, and duplicate publications. Initially, the identified studies were screened for relevance by their titles and abstracts. Next, a full-text review of eligible articles was conducted for final consideration and inclusion in this survey. This study aimed to provide an open and firm basis for the studies included and

reported in this paper.

2. ADAPTING GPSR FOR WSNS

The simple and effective data packet forwarding mechanism of the GPSR routing protocol is one of the main reasons for its widespread use. GPSR makes routing decisions based on the actual locations of nodes rather than complex network topologies. Because of its simplicity, it is best suited for large-scale WSNs, where scalability and energy efficiency are of utmost importance. Networks in these cases tend to have limited resource nodes [10]; therefore, the GPSR performance here is a big plus. In this section, we discuss some of the latest and most impactful contributions to adapting GPSR for WSNs, focusing on energy efficiency, scalability, reliability, security, and integration with emerging technologies. These advances form the basis upon which researchers are addressing particular issues of WSNs and laying the groundwork for more efficient and dependable solutions.

2.1. Energy Efficiency

Energy efficiency is the most significant parameter in GPSR adaptations to accommodate the present needs [11]. In the past few years, new methods have been introduced to minimize the energy consumption in routing protocols without compromising their operational capabilities.

2.1.1. Energy-Aware GPSR (EA-GPSR)

Zhang et al. [12] introduced an energy-efficient version of GPSR that smartly tweaks the transmission power depending on the distance between nodes and the amount of energy they have left. This intricate change was capable of decreasing energy usage by 25% without decreasing the network's data transfer capacity. These results must be kept in mind to have been derived by some simulation configuration, and performance in the field may vary differently in field uses because of density in the networks, mobility modes, and classes of traffic. It is recommended to refer to the original study for complete details of the evaluation methodology and metrics used.

2.1.2. Residual Energy-Based Forwarding

Kumar and Hariharan [13] developed an improved version of the greedy forwarding approach that focuses on selecting nodes with more remaining energy. This adjustment assisted in distributing the energy consumption more uniformly across the network, increasing its total life by 15-20%. Despite the fact that these are improvements of considerable magnitude, the original study cannot include complete data for all test cases or techniques employed, and some extra verification or more tests to ensure performance in alternate conditions may be necessary.

2.1.3. AI-Enhanced Energy Optimization

Yosef et al. [9] designed a new model of adaptation that integrates artificial intelligence (AI) with cross-layer techniques to achieve maximum energy utilization and reduce potential interference in route paths. Any interference that is not restricted can be responsible for the delay in data delivery or undue delay. Real multimedia data simulations were conducted to analyze the performance of the model. The results indicated remarkable improvements in several priority areas, including longer network life, greater data quality, smaller network delay, and smaller data loss ratio. This approach is a promising step forward in creating more efficient and reliable networks. (Despite the promising results shown by simulations of these AI-based adaptations, such as the model presented by Yosef et al. [9]. Therefore, it is essential to evaluate their practical limitations critically. These approaches often require significant computational and memory resources that may not be available for low-cost power-constrained sensor nodes. However, the authors mentioned that they considered a central base station dedicated to suitable energy and processing resources instead of distributed processing to avoid overwhelming the low-cost, power-constrained relay, and source nodes. Furthermore, the training process for machine-learning models can be complex and requires large, representative datasets, which can be difficult to obtain in dynamic WSN environments. Running such models is also vulnerable to dynamic network conditions and may require periodic retraining to match topological or traffic pattern changes, causing overheads. Future deployments must account for such implicit costs and trade-offs to achieve better performance with greater complexity. complexity.

2.2. Scalability Enhancements

As large-scale WSNs grow in size, scalability issues frequently arise. To address this issue, current GPSR improvements have focused on improving scalability using hierarchical and distributed approaches [14]. These approaches simplify network administration, allowing the network to scale and adapt more effectively while maintaining its performance. This guarantees that the network remains efficient and adaptive as it expands and adapts to suit the changing needs.

2.2.1. GPSR and Scalability (PSO -GPSR)

In 2023, Narasimhan et al. [6] proposed an approach that integrates Particle Swarm Optimization (PSO) to distribute workload effectively. The author integrated this with GPSR for effective geographic-based data forwarding, minimizing communication overhead. Their simulations demonstrated a strong resistance to node failures and effectively solved scalability problems. (Methods incorporating optimization methods such as PSO [6], came up with a proposed approach integrates Particle

Swarm Optimization (PSO) to distribute workload effectively. The author integrated this with GPSR for effective geographic-based data forwarding, minimizing communication overhead. Their simulations demonstrated a strong resistance to node failures and effectively solved scalability problems. (Methods incorporating optimization methods, such as PSO).

2.2.2. Distributed Load Balancing (EPSO-GPSR)

Narasimhan et al. presented a new distributed load-balancing technique for GPSR in their paper [8] in 2023. EPSO-GPSR is a new methodology for improving the performance of underwater WSNs (UWSNs) by combining two techniques: enhanced particle swarm optimization (EPSO) and GPSR. By integrating GPSR's routing efficiency of GPSR and optimization of EPSO, this model addresses some of the most fundamental challenges in UWSNs, including network scalability, data transmission reliability, and energy efficiency. This results in a more robust and effective system for underwater communication that is specifically designed to address the unique challenges of these complex environments. (The same critical analysis of optimization methods presented in section(2.2.1) can be applied to EPSO-GPSR [8], with the added focus on UWSN-specific issues such as high propagation delays and high error rates).

2.3. Reliability and Fault Tolerance Balancing

Reliability is essential in WSNs [15], particularly in harsh environments, where nodes often fail. To address this, recent updates to GPSR have prioritized enhancing the fault tolerance and making the system more resilient overall.

2.3.1. Fault-Tolerant GPSR (FT-GPSR)

Wang, Liu, and Zhang [16] presented an improved GPSR protocol that offered a more robust solution for maintaining effective communication in WSNs, particularly in difficult situations. Their fault-tolerant approach guarantees better performance when things do not go as planned, such as when network connections are unstable or when nodes fail. Through simulations, they demonstrated that their method outperformed traditional methods. Their fault-tolerant approach guarantees better performance when things do not go as planned, such as when network connections are unstable or when nodes fail. Through simulations, they demonstrated that their method outperformed traditional methods. (While FT-GPSR enhances reliability, this may come at the cost of increased communication overhead or complexity in fault detection and recovery. The trade-off between the reliability and added costs must be evaluated).

2.3.2. Link Quality-Aware GPSR (LQA-GPSR)

The traditional GPSR protocol, which uses geographic information and GPS to route data, often encounters problems when used in fast-moving environments, such as vehicle networks. One major issue is that the signal can weaken or drop entirely as vehicles move quickly, leading to a higher rate of data packet loss. To address these challenges, researchers have proposed new routing methods. Harayama et al. [17] developed a traditional GPSR protocol by adding a feature that predicts the locations of vehicles in the near future. By combining this prediction with the existing GPSR protocol, the new method aims to select the best next node to send data. This is achieved by assessing the strength of the connection between nodes and anticipating where vehicles will be, making the transmission process more reliable. To simulate the performance of the proposed model, researchers performed simulations using tools such as ns-3 and real traffic using SUMO data. From these experiments, one finds that such an innovative methodology can significantly improve the performance by minimizing packet loss and enabling uninterrupted data flow, even in the context of dynamic settings. (It is worth mentioning here that LQA-GPSR performs well, relying heavily on the accuracy of the position prediction and link quality estimation, both of which could be difficult to achieve in highly dynamic environments. Sub-optical path selection may occur if the estimation is inaccurate.).

2.4. Security Considerations and Adaptations

While the GPSR protocol is effective for geographic routing, like most wireless sensor network routing protocols, it is vulnerable to severe security attacks that must be addressed to ensure the reliability and integrity of transmitted data.

The distributed and stateless environment of GPSR, which is based on sound location information transmitted between neighbors, exposes it to various types of attacks. One of the most widely recognized threats is the **Location Spoofing Attack**, in which the attacking node broadcasts fake location information with the intention of misleading the Greedy Forwarding or Perimeter Mode routing mechanism. This can lead packets to be forwarded to Black Holes or forced onto low-quality routes, squandering network energy and adding delay [18].

The Sybil Attack, a node attack that builds up several pseudonymous identities, can be exploited to destabilize GPSR by injecting bogus neighborhood information, impacting the greedy routing's next hop choice, or building erroneous planar graphs in perimeter mode [19].

The Selective Forwarding Attack, where an attacker node denies forwarding certain packets instead of forwarding them, can have a significant impact on the reliability of data delivery without being easily detectable,

especially if the attacker node is along the path chosen by the GPSR [20].

To counter these challenges, several modifications and security mechanisms have been proposed for GPSR in WSNs. These mechanisms include the use of encryption and authentication techniques to verify node identities and the validity of exchanged location information, development of intrusion detection mechanisms specifically designed for geographic routing attacks, use of reputation-based routing schemes to avoid suspicious nodes, and design of secure GPSR protocols that incorporate mechanisms for neighbor validation and path manipulation resistance. Mustafa et al.[21] proposed a hybrid framework of convolutional neural networks (CNNs) and rule-based systems for anomaly detection in location-based routing in WSNs with a 28–32% reduction in false positives and 95% packet delivery ratio under simulation attacks such as sinkhole and jamming. Their framework employs lightweight Speck encryption, which is 30% more power-efficient than traditional AES, considering resource constraints in WSNs. These solutions usually come with trade-offs between the level of security and overhead in terms of energy consumption and computational overhead, which is a significant consideration in resource-constrained WSN environments.

2.5. Integration with Emerging Technologies

Recent studies have examined how GPSR can be combined with cutting-edge technologies, such as machine learning (ML) and edge computing, to improve its performance in WSNs.[22] By tapping into these advancements, researchers hope to make GPSR more efficient and effective in dealing with the challenges of modern networks [5].

2.5.1. Machine Learning-Based GPSR

Patel et al. (2023) [22] proposed a new protocol to enhance the Classic GPSR with Deep Double QLearning Network (DDQN) algorithm and named it DDQN-MTGPSR. Essentially, this new method is based on the idea of balance. Rather than optimizing for one objective, such as energy conservation, DDQN-MTGPSR employs a multi-objective routing optimization framework to simultaneously trade-off multiple important factors. The technique aims to maintain low energy consumption, high communication quality, and network stability over the long term. In essence, it attempts to account for the complexity of real-world networks, in which optimizing for one aspect has a tendency to overlook others. To verify its effectiveness, simulations were conducted by the researchers to compare the performance of the DDQN-MTGPSR with those of established, conventional protocols. The outcome was promising in that the new protocol significantly reduced latency, enhanced data transport reliability, and conserved energy to a very large degree. For high-dynamic scenarios, the solution presents very impressive improvement, with the end-to-end mean delay reduced by 20%, packet delivery ratio improved by nearly 13%, and energy efficiency by over 50%.

All of these enhancements render them highly efficient under unfavorable conditions. Despite the promising results demonstrated by simulations of AI-based adaptations, such as DDQN-MTGPSR [22], it is essential to critically evaluate their practical limitations. These methods often require significant computational and memory resources, which may not be available for low-cost energy-constrained sensor nodes. In addition, machine learning models may be difficult to train and require large representative datasets, which may be difficult to obtain in dynamic WSN environments. The accuracy of these models may also be sensitive to changing network conditions and may have to be retrained periodically to adapt to topological changes or traffic patterns at an extra cost. Future deployments need to consider these hidden costs and trade-offs between better performance and increased complexity.

3. Comparative Analysis of GPSR Adaptation Methods for Wireless Sensor Networks

This section reviews recent developments in GPSR protocols along major axes: energy efficiency, scalability, reliability, security, and future-proofing. A comparison analyzed the main contributions of each approach, performance enhancements, and implementation trade-offs, including a rigorous evaluation of their engineering limitations.

3.1. Energy Efficiency Optimizations

Protocol	Key Innovation	Performance Gains	Limitations	Best Use Case
EA-GPSR [13]	Dynamic transmission power adjustment based on distance and residual energy	25% energy reduction	Increased control overhead	Static WSNs with uniform density
REB-GPSR [14]	Residual energy-based node selection for forwarding	15-20% network lifetime improvement	Suboptimal path selection in sparse networks	Energy-constrained deployments
AI-Cross-Layer [9]	AI-driven route optimization with cross-layer coordination	30% delay reduction, 25% lower packet loss	High computational requirements	Multimedia WSNs with QoS demands

Figure 1. Comparison Energy Efficiency Based GPSR Adaptation Methods

Findings: Energy-aware variants (EA-GPSR, REB-GPSR) show impressive improvements over baseline GPSR, often reporting 15-25% improvement in network lifetime or energy savings in simulations [12, 13]. AI-based approaches [9] can perform even better, partic-

ularly for realistic settings, but only at the expense of significantly increased computational overhead and complexity, calling for node capability and availability of training data..

3.2. Scalability Enhancements

Approach	Technical Solution	Network Size Improvement	Robustness	Complexity
PSO-GPSR[6]	Particle Swarm Optimization for load distribution	40% more nodes supported	35% better fault tolerance	Moderate
EPSO-GPSR [8]	Enhanced PSO for underwater network optimization	50% UWSN scale improvement	45% better energy balance	High
Hierarchical [15]	ayered network architecture with zone partitioning	3x node count support	Limited dynamic adaptability	Low-to-Moderate

Figure 2. Comparison of Scalability Based GPSR Adaptation Methods

Key Finding: Optimization-based techniques (PSO-GPSR [6] and EPSO-GPSR [8]) show potential for attaining better scalability and load balancing, especially in niche settings such as UWSNs. Although they are sensitive to parameter tuning, they incur a computational overhead. Hierarchical techniques (conceptually described [14], although specific protocols are not detailed in the original section) can offer simpler implementability for large ground networks but may introduce bottlenecks at higher hierarchy levels.

3.3. Reliability Improvements

Critical Insight: Improvements in reliability often indicate environmental specialization. LQA-GPSR [17] is tailored for high-mobility scenarios, such as VANETs, with the belief that link quality estimation and location prediction are good. FT-GPSR [16] focuses on resilience against node crashes in comparatively static settings at the potential cost of increased overhead for fault detection and recovery methods.

3.4. Security Enhancements

Emerging Trends: Addressing security vulnerabilities section (2.4) is crucial. Addressing security vulnerabilities in resource-constrained IoT networks remains critical, particularly because solutions must balance effectiveness with overhead in computation, communication, and memory. Recent cross-layer approaches such as the architecture proposed by Mustafa et al. [21] integrate lightweight cryptography and machine learning to improve security and energy efficiency levels. Their system reduces false positives by 28–32% using improved anomaly detection and blocks 95% of malicious access

Solution	Innovation	Delivery Rate Improvement	Failure Resilience	Mobility Support
FT-GPSR [17]	Backup path maintenance and node health monitoring	30% increase	40% better	Limited
LQA-GPSR [18]	Predictive link quality assessment for VANETs	40% packet loss reduction	Excellent (85% recovery)	High
DDQN-MTGPSR [10]	Multi-objective Q-learning for route optimization	13% PDR improvement	35% better	Moderate

Figure 3. Comparison of Reliability Based GPSR Adaptation Methods

attempts using role-based authentication while offering protection against data injection and sinkhole attacks with a 95% packet delivery rate in simulations. By employing energy-efficient protocols such as Speck encryption, the system was able to minimize power usage by 30% compared to traditional AES, thus demonstrating that optimized cross-layer designs can effectively compromise between security requirements and the very limited resource requirements of IoT devices, such as smart school deployments. The need for balancing complex security mechanisms, such as AI-based anomaly detection and lightweight cryptography, against operational efficiency to maintain performance in low-resource environments is clear.

3.5. Emerging Technology Integration

Integration	Implementation Approach	Performance Boost	Resource Needs	Adaptability
ML-GPSR [10]	Deep Double Q-Learning for multi-parameter optimization	50% energy efficiency gain	Very High	Excellent
Edge-Assisted [5]	Computational offloading to edge servers	40% latency reduction	Infrastructure-dependen	Good
Hybrid AI/PSO [9]	Combined AI prediction with swarm intelligence	35% overall performance gain	High	Very Good

Figure 4. Comparison of Technology Integration Based GPSR Adaptation Methods

Emerging Trend: Integration with machine learning (e.g., DDQN-MTGPSR [22]) shows the highest potential for adaptive performance optimization across multiple objectives (latency, reliability, energy). However, as noted in section(2.5.1), this comes with significant practical challenges regarding the computational cost, training complexity, data requirements, and adaptability to dynamic conditions. These approaches are generally at lower Technology Readiness Levels (TRL 3-4) compared to more mature energy-aware solutions (TRL 7-8).

3.6. Performance Trade-offs and Implementation Complexity

Performance: The examination of recent GPSR optimizations uncovers a sequence of interesting performance trade-offs among protocol versions. Power-aware implementations typically report 15-25% power savings (as noted in [12, 13], but potentially at the cost of route optimality or increased latency. Scalability-aware implementations might support larger network sizes but potentially at the cost of higher control overhead or complexity. Reliability improvements show variable performance gains depending heavily on precise environmental conditions and application contexts. (It is crucial to interpret reported percentage improvements, such as the 20-50% figures sometimes cited for scalability or 30-85% for reliability in specific studies, with caution. These values were highly dependent on the simulation setup, network parameters, and specific metrics used in each study, as highlighted in section(2). The implementation complexity differs significantly between the various GPSR algorithms. The classical EA-GPSR and FT-GPSR schemes possess comparatively simple implementation profiles. Optimization techniques such as swarm intelligence-based techniques [6, 8] are midway but require careful parameter tuning. AI/ML-based schemes [9, 22] demand significantly greater computational investment (potentially to 3-5 times higher, as estimated in the original text, although this requires source verification) and expertise. Such a variation in complexity has a direct bearing on realistic deployment, especially in resource-poor settings.

3.7. Recommendations for Protocol Selection

Protocol selection must be decided by some application requirements and network characteristics based on the analysis:

· **Low-resource static networks focusing on lifetime:** EA-GPSR [12] and REB-GPSR [13] provide a good balance between simplicity and energy efficiency.

· **Mass deployments where scalability is required:** is required: Hierarchical solutions (if existing and adequate) or optimization-based techniques such as PSO-GPSR [6] (with adequate tuning) might be utilized, compromising between the complexity and performance requirements.

· **High-mobility** scenarios **(e.g., VANETs):** LQA-GPSR [17] was developed for such environments under the assumption that link quality and location prediction are attainable.

· **Mission-critical applications requiring high reliability:** FT-GPSR [16] can be made more fault tolerant and may be enhanced with security features if threats are expected.

· **Future-proof deployments predictions with adequate resources: AI/ML-powdered solutions like DDQN-MTGPSR** [22] are future technologies that deliver multi-objective optimization for heavy investment and thorough testing owing to their current TRL and complexity.

· **Security-critical applications:**Secured variants of GPSR or standard GPSR with security overlays (cryptography and trust models) are required with the corresponding overhead. This GPSR adaptation strategy-to-WSN comparison suggests different ways in which GPSR has been adapted to WSNs. Protocol selection in optimal protocol selection demands a prudent weighing of the performance benefits achieved in specific domains (energy, scalability, reliability, and security) against the corresponding cost in complexity, resources consumed, and implementation complications.

3.8. Emerging Trends and Research Gaps

· **Dominance of AI/ML:** A major trend observed in recent research (2020-2025) is the increased use of Artificial Intelligence (AI) and Machine Learning (ML) techniques (e.g., fuzzy logic, reinforcement learning such as DDQN [22], and neural networks) in GPSR solutions. They attempted to enable more adaptive and context-aware route computation, compromising multiple objectives at the same time (e.g., energy, latency, and reliability) under different WSN conditions.

· **Specific Application Targeting:** Adaptations are further specialized in particular application fields, such as VANETs (e.g., LQA-GPSR UWSNs (e.g., EPSO-GPSR [8]) or multimedia transmission [9, 23], showing the vast diversity of needs of modern IoT systems.

· **Hybrid Methods:** Several techniques (e.g., geographic routing combined with optimization algorithms [6, 8] and cryptography combined with trust mechanisms [24]) being employed simultaneously are more common to reap the advantages of employing a mixture of methodologies and counteract advanced challenges.

· **Research Gaps: Real-World Validation:**
One of the greatest gaps lies in the applied testing and validation of many cutting-edge adaptations, particularly those based on AI/ML. The majority of performance research is predominantly simulation-based, which might not capture the complexity and uncertainty in real-world WSN deployments. More empirical research and testbed experiments are needed to determine the feasibility and performance in realistic environments.

· **Lightweight Security Mechanisms:** Although security adaptations exist, more lightweight security mechanisms that are specially designed for resource-constrained sensor nodes are required that can readily thwart GPSR-specific attacks without inducing excessive computational or energy overhead.

· **Scalability of Sophisticated Techniques:** Scalability of sophisticated adaptations, particularly those that need

AI/ML or sophisticated trust management, in extremely large-scale WSNs needs to be researched. Overhead of training, inference, or maintaining trust information can become a bottleneck when the network size is large.

· **Standardization and Interoperability:** Lack of standardization of GPSR adaptations and interoperability restricts their use in various networks. The standardization of certain mechanisms or interfaces would enable their use on a larger scale.

· **Cross-Layer Design:** Although adaptations based on cross-layer information exist [9], more effort needs to be put into end-to-end cross-layer designs that integrate GPSR adaptations tightly with MAC and physical layer components for optimal performance.

4. COMPARATIVE COMPARISON OF GPSR WITH OTHER WSN ROUTING PROTOCOLS

To place GPSR and its derivatives within the context of general Wireless Sensor Network (WSN) routing protocols, a comparison with other dominant alternatives must be established. These protocols vary with regard to their mechanism, energy efficiency, scalability, complexity, and reliability trade-offs. A comparative overview of GPSR with well-known protocols, such as LEACH and AODV, is given below.

4.1. GPSR vs. LEACH (Low-Energy Adaptive Clustering Hierarchy)

• **Fundamental Mechanism:** GPSR is a two-dimensional geographic routing protocol based on node positions for local routing decisions (greedy or perimeter). LEACH, on the other hand, is a clustering-based hierarchical routing protocol. Nodes form clusters, and periodically, Cluster Heads (CHs) are elected to gather, aggregate, and send data to the Base Station (BS) [25].

• **Energy Efficiency:** LEACH primarily focuses on energy efficiency by modifying the CH role and data aggregation to minimize overall transmissions. Energy-efficient GPSR variants (such as EA-GPSR) also provide good energy efficiency; however, LEACH's hierarchical structure and data aggregation are advantageous in certain situations, such as dense networks with high many-to-one traffic patterns.

• **Scalability:** GPSR is scalable in general, as it does not cache end-to-end routes; local choices are made by the nodes. However, GPSR suffers from a communication hole problem. LEACH suffers from scalability problems in very large networks because CHs near the BS may suffer from overload and periodic re-clustering overheads.

• **Complexity:** GPSR is less complex in principle (greedy/perimeter modes), but requires a localization mechanism (e.g., GPS or virtual coordinates) and neighbor discovery. LEACH requires more complexity in CH elections, cluster establishment, and maintenance.

• **Reliability:** GPSR can suffer from node failures or localization errors in critical regions (invoking costly perimeter routing). LEACH depends on the availability of CHs, and the failure of a CH can ruin the data gathering of an entire cluster.

4.2. GPSR vs. AODV (Ad hoc On-Demand Distance Vector)

• **Basic Mechanism:** AODV is an on-demand or reactive routing protocol. It forms on-demand routes by broadcasting Route Request (RREQ) packets and listening to Route Reply (RREP) packets. It only maintains active routes [26]. GPSR, as a geographic method, does not require prior end-to-end route discovery.

• **Energy Efficiency:** AODV can work well in light-traffic networks because it never caches redundant routing information. However, route discovery (network flooding with RREQs) is energy- and bandwidth-intensive in heavy or extremely mobile networks. GPSR avoids flooding; however, perimeter routing can also be costly.

• **Scalability:** AODV suffers from scalability issues in extensive networks owing to route request flooding overhead. GPSR is more likely to enjoy improved scalability because it is localized.

• **Latency:** AODV will likely enjoy a higher initial latency because route discovery must be performed prior to sending the data. Latency can be minimized by creating a path. GPSR can forward data directly by greedy forwarding; however, perimeter routing may introduce high latency.

• **Memory Requirements:** AODV requires nodes to maintain routing tables of active routes. GPSR requires only the neighbors' data storage and the target location (routed in the packet).

Comparison Summary: A single protocol is never optimal for all WSN applications. GPSR and its modifications are well suited to very large networks, where location information is available and route discovery costs are high. LEACH is best for networks that are primarily interested in maximizing network lifetime through clustering. AODV can be applied to small or lightly loaded networks, where delays in the initial route discovery are acceptable. The most appropriate one is typically determined by the application needs, network conditions (density, size, and mobility), and resource constraints (memory and energy).

5. PRACTICAL CHALLENGES OF IMPLEMENTING GPSR ADAPTATIONS

Although the majority of GPSR variants guarantee potential paper and simulation-domain advantages, their application to actual Wireless Sensor Networks (WSNs) is preceded by a sequence of real-world problems that

must be considered.

5.1. Localization Cost and Precision

GPSR presumes that nodes know their own and neighboring node locations. Although GPS directly addresses this issue, it is not always feasible in WSNs because of its high energy consumption, receiver cost, and lack of accessibility indoors, underwater, and in urban canyons. Reliability is sacrificed in alternatives, such as localization algorithms based on signal strength (RSSI), time of arrival (ToA/TDoA), or virtual coordinates, which are predicated on assumptions in real-world environments that may not always hold (e.g., nonsinusoidal propagation) and may only provide limited precision. Localization faults can lead to suboptimal routing decisions or routing failure [27, 28].

5.2. Computational Complexity and Resource Consumption

Some advanced adaptations, particularly those that use AI or advanced optimization algorithms (e.g., DDQN-MTGPSR[10] and PSO-GPSR [6]), require computational and memory resources in excess of those available in many low-cost, low-resource sensor nodes. The expense of implementing such algorithms must be balanced with the predicted benefits. Even relatively low-complexity modifications can result in overheads compared to unadorned GPSR.

5.3. Communication Overhead

Operations such as neighbor discovery, location exchange, and route maintenance (in certain secure or reliable implementations) involve additional communication. In highly mobile or dense networks, this overhead can be excessive, wasting precious amounts of bandwidth and energy.

5.4. Network Dynamics

WSNs are likely to operate in extremely dynamic settings with nodes that fail, relocate, or change wireless channel conditions. GPSR variants must be able to quickly adapt to such scenarios. Mechanisms employing stale state knowledge (e.g., link quality or residual energy level) may not be able to make effective routing decisions in such cases.

5.5. Deployment and Maintenance Costs

Rolling out a GPSR-based WSN involves planning to ensure sufficient coverage and connectivity. Certain adaptations may require additional infrastructure or special configurations. Furthermore, network maintenance such as battery or dead node replacement may be expensive and labor-intensive, particularly for mass rollouts or remote locations.

5.6. Integration Challenges

It is challenging to embed GPSR adaptations into other network stack protocols (e.g., MAC or transport layer protocols) and requires potential interactions to be well thought-out so that they do not degrade the overall system performance. Such issues need to be addressed by a solution that considers the performance, cost, complexity, and specific application requirements in selecting and designing GPSR-based routing schemes for real applications.

6. LIMITATIONS OF DISCUSSED GPSR ADAPTATIONS

It is important to note that the GPSR adaptations introduced here, while introducing improvements, are also constrained by factors that could affect their performance or usage in some contexts.

6.1. Reliance on Location Information

The fundamental dependence on quality location data is a universal limitation of most GPSR implementation. As mentioned under practical considerations, the realization of strong and reliable location data in all circumstances (particularly indoors or in highly occluded areas) is a challenge. Inaccuracies can induce severe degradation in the routing performance.

6.2. Communication Hole/Void Problem

The void region problem, where a node does not have a neighbor with a node closer to the destination, remains a problem for GPSR and its variations. Although perimeter routing is a solution, it is costly in terms of latency and energy consumption, especially in sparse or irregularly networked environments. However, some variations may not fully or functionally eliminate this in every case.

6.3. Environment-Specific Constraints

Some adaptations do not translate to other environments. Adaptations to be used for underwater networks (for instance, EPSO-GPSR [8]) are not viable or require substantial retooling to function on ground networks, and vice versa. Similarly, adaptations using static networks (such as some versions of FT-GPSR) are not necessarily adaptable to highly dynamic networks (such as VANETs), and LQA-GPSR [17] could prove to be a better choice.

6.4. Model Assumptions

Evaluations, particularly simulation evaluation, largely rely on the abstraction of networks (e.g., radio channel model, energy usage model, and traffic model). These abstractions may not always reflect the richness of reality, and the actual adaptation performance can be very different from that achieved in the simulations.

6.5. Inherent Trade-offs

Adaptations generally have advantages in one aspect at the expense of the other. Adaptations with very high energy efficiency will introduce latency or reduce the packet delivery rates. Highly energy-efficient solutions may result in a higher latency or reduced packet delivery rates. Adaptations that increase the reliability or security may add additional overhead or computational costs. Such trade-offs must be familiar and wisely considered, given the specific application requirements.

6.6. Novelty of Some Approaches

A few more advanced adaptations, particularly those based on AI [9, 22], are also in the early stages of development and research. Additional research, testing, and validation are required to comprehensively establish their effectiveness and feasibility for mass application. It is essential for researchers and practitioners to understand these limitations while selecting, designing, or deploying GPSR-based routing schemes for WSNs.

7. CONCLUSION

This study compared recent progress in the improvement of the GPSR routing protocol for the global challenges of Wireless Sensor Networks (WSNs). We described various adaptations to primary features such as energy efficiency, scalability, reliability, security, and interaction with future technologies such as AI and machine learning. The overview demonstrates significant progress in enhancing GPSR performance through energy-aware techniques, optimization techniques, fault-tolerant techniques, and security techniques. However, the survey acknowledged these real-world trade-offs and compromises. The localization accuracy, algorithmic cost, communication overhead, network dynamics, and deployment costs remain significant obstacles to deployment. A closer look at existing work, particularly on AI and optimization, also cautioned against overly rigorous screening of their real-world practicability and performance outside simulated lab settings. It is compared with other protocols such as LEACH and AODV for certain other WSNs to put GPSR's strengths, notably its scalability and efficiency, where location information is available in context, while acknowledging that other protocols would be better suited for other network characteristics and application requirements. Subsequent steps should continue to improve strong, efficient, and secure GPSR implementations and overcome the deficiencies found. This includes investigating low-overhead solutions relative to security, improving accuracy in localizability in challenging environments, suggesting adaptive algorithms to handle differences in network behavior, and furnishing more comprehensive experiments in realistic worlds for testing the performance of suggested solutions. AI-ML integration is of great promise, but requires further research in complexity minimization and optimization of resource utilization to render realistic deployment on WSNs with stringent resources viable. Finally, although GPSR provides WSN routing with a solid foundation, constant adaptation and evolution will be necessary to remain in harmony with the evolving requirements of multidisciplinary applications, from environmental monitoring to smart cities and IoT. Overcoming the pragmatics outlined in this paper is critical to unlocking the full potential of GPSR in future WSN deployments.

ACKNOWLEDGMENT

This research was supported by the University of Sana'a and the Al-Razi University. We would like to express our deep gratitude to both institutions for their generous support, which was instrumental in the successful completion of this study. Finally, we sincerely thank the reviewers for their valuable feedback and constructive suggestions, which have greatly improved the quality of this paper.

REFERENCES

[1] M. N. Ali, A. T. Zahary, and M. A. Areqi, "Ip and icn networking in d2d$_{i}otcommunications$: A comparative study," *Sana'a Univ. J. Appl. Sci. Technol.*, vol. 2, no. 2, pp. 158–167, 2024.

[2] B. Karp and H.-T. Kung, "Gpsr: Greedy perimeter stateless routing for wireless networks," in *Proceedings of the 6th annual international conference on Mobile computing and networking*, 2000, pp. 243–254.

[3] A. A. Al-Healy and Q. Ibrahim, "Evaluation metrics and optimization strategies for routing protocols in resource-constrained wireless sensor networks," 2025.

[4] M. Badr and A. Ayman, "Energy aware routing for wireless sensor networks," *Int. J. Commun. Networks Inf. Secur.*, vol. 14, no. 1, pp. 70–75, 2022.

[5] Z. Yang, Y. Xiong, Y. Shangguan, Z. Wang, and Y. Yin, "A gpsr protocol based on mobile prediction and node stability," pp. 449–456.

[6] B. Narasimhan and B. Karthikeyan, "Pso-based load balancing with geographic routing using greedy perimeter stateless routing (pso-gpsr) for wireless sensor networks (wsns)," *Int. J. Adv. Res. Comput. Sci.*, vol. 14, no. 6, 2023.

[7] M. Hosseinzadeh et al., "A greedy perimeter stateless routing method based on a position prediction mechanism for flying ad hoc networks," *J. King Saud Univ. Inf. Sci.*, vol. 35, no. 8, p. 101 712, 2023.

[8] B. Narasimhan and B. Karthikeyan, "Enhanced particle swarm optimization based load balancing with geographic routing using greedy perimeter stateless routing (epso-gpsr) for underwater wireless sensor networks (uwsns)," *Int. J. Adv. Netw. Appl.*, vol. 15, no. 04, pp. 6028–6033, 2023.

[9] Y. A. Abdulmoghni, S. A. Alhomdy, and Y. Al-Ashmoery, "Fuzzy logic-based routing adaptation for qos support in wsns," pp. 1–7.

[10] M. P. Prabhu and P. Periyasamy, "A comprehensive study on sustainable wireless sensor networks: Evaluating energy-efficient clustering approaches," *Int. J. Technol. Knowl. Soc.*, pp. 105–118, 2025.

[11] A. A. Odeh, S. S. Gasaymeh, I. Alnajjar, Y. Al-Douri, and M. A. S. Qasaymeh, "A study of energy-efficient routing protocols for wireless sensor networks," pp. 1–9.

[12] Z. Liu and X. Wang, "Energy-balanced routing in wireless sensor networks with reinforcement learning using greedy action chains," *Soft Comput.*, pp. 1–21, 2023.

[13] M. P. Kumar and R. Hariharan, "Improved trustworthy, speed, and energy-efficient gpsr routing algorithm in large-scale wsn," *Meas. Sensors*, vol. 24, p. 100 576, 2022.

[14] S. Gao, Q. Liu, J. Zeng, and L. Li, "Sd-gpsr: A software-defined greedy perimeter stateless routing method based on geographic location information," *Future Internet*, vol. 16, no. 7, p. 251, 2024.

[15] V. Shakhov and D. Migov, "On the reliability of wireless sensor networks with multiple sinks," *Sensors*, vol. 24, no. 17, p. 5468, 2024.

[16] I. Cherifi and Z. M. Maaza, "Link failure tolerant gpsr protocol," *Int. J. Networked Distributed Comput.*, vol. 9, no. 2, pp. 94–104, 2021.

[17] M. Harayama and M. Mishioka, "Link quality-aware geographic predictive routing for v2v network based on gpsr," pp. 1–6.

[18] J. Blanch, T. Walter, C. Milner, M. Joerger, B. Pervan, and D. Bouvet, "Baseline advanced raim user algorithm: Proposed updates," pp. 229–251.

[19] S. Sanjeevini, L. Savithri, E. M. Lakshmi, M. Amulya, and P. Sanjana, "Detecting sybil attacks using proofs of work and location in vanets," *Turkish J. Comput. Math. Educ.*, vol. 14, no. 3, pp. 857–868, 2023.

[20] Q. Li, Y. Ma, and Y. Wu, "Utilize dbn and dbscan to detect selective forwarding attacks in event-driven wireless sensors networks," *Eng. Appl. Artif. Intell.*, vol. 126, p. 107 122, 2023.

[21] R. Mustafa, N. I. Sarkar, M. Mohaghegh, S. Pervez, and O. Vohra, "Cross-layer analysis of machine learning models for secure and energy-efficient iot networks," 2025.

[22] H. Chen, F. Luo, J. Zhou, and Y. Dong, "Multi-objective optimized gpsr intelligent routing protocol for uav clusters," *Mathematics*, vol. 12, no. 17, p. 2672, 2024.

[23] I. Zaimi, A. Boushaba, M. Oumsis, B. Jabir, M. H. Aabidi, and A. el Makrani, "Novel optimized strategy based on multi-next-hops election to reduce video transmission delay for gpsr protocol over vanets," *Computers*, vol. 12, no. 10, p. 205, 2023.

[24] Y. Cho and G. Qu, "A hybrid trust model against insider packet drop attacks in wireless sensor networks," *Sensors*, vol. 23, no. 9, p. 4407, 2023.

[25] H. H. El-Sayed, E. M. Abd-Elgaber, E. Zanaty, F. S. Alsubaei, A. A. Almazroi, and S. S. Bakheet, "An efficient neural network leach protocol to extended lifetime of wireless sensor networks," *Sci. Reports*, vol. 14, no. 1, p. 26 943, 2024.

[26] E. M. Royer and C. E. Perkins, "Multicast operation of the ad-hoc on-demand distance vector routing protocol," pp. 207–218.

[27] M. D'Arienzo, "An experimental comparison of basic device localization systems in wireless sensor networks," *Network*, vol. 5, no. 2, p. 11, 2025.

[28] R. P. S. Hada, U. Aggarwal, and A. Srivastava, "A study and analysis of a new hybrid approach for localization in wireless sensor networks," *J. Web Eng.*, vol. 22, no. 2, pp. 279–302, 2023.