Original Research

Routing Optimization and Challenges in Wireless Sensor Networks under IoT Framework

Hamidreza Farahani[1], Gholam-Reza Mohammad-Khani[2*], Amir Hossein Miremadi[3]

Received: 7 July 2025 / Accepted: 17 January 2026 / Published online: 30 January 2026

*** Corresponding Author Email, mohammadkhani@irost.ir**

1, 3 - Department of Electrical Engineering, WT.C., Islamic Azad University, Tehran, Iran
2- Department of Electrical Engineering and Information Technology, Iranian Research Organization for Science and Technology (IROST), Tehran, Iran

Abstract
Wireless Sensor Networks (WSNs) constitute a key enabling technology for the Internet of Things (IoT), providing large-scale, low-power sensing and monitoring capabilities in smart cities, industrial automation, environmental surveillance, healthcare, and agriculture. However, the integration of WSNs into the IoT framework exacerbates classical routing challenges such as energy scarcity, dynamic topology, data redundancy, link unreliability, and Quality of Service (QoS) constraints. At the same time, recent advances in optimization and artificial intelligence have introduced new opportunities for adaptive, context-aware, and cross-layer routing solutions. This paper presents a comprehensive review of routing optimization and challenges in WSNs under the IoT framework. First, we discuss the fundamental characteristics of WSNs in IoT scenarios and the design requirements of routing protocols. Then, we classify routing challenges into energy efficiency, scalability, reliability, latency, heterogeneity, mobility, and security-privacy issues. We examine state-of-the-art routing protocols and optimization approaches including Ant Colony Optimization (ACO), Particle Swarm Optimization (PSO), Genetic Algorithms (GA), Fuzzy Logic, mathematical programming, Reinforcement Learning (RL), and deep learning-based schemes. Special emphasis is placed on context-aware routing, Software-Defined Networking (SDN)-enabled IoT, edge/fog-assisted routing, and blockchain-based secure routing. We also summarize and compare representative protocols and recent solutions published from 2020 to 2025 in terms of their design goals, performance metrics, and application domains. Finally, we identify open research problems and future directions towards self-optimizing, sustainable, and trustworthy routing mechanisms for next-generation IoT-driven WSNs.

Keywords - Wireless Sensor Networks, Internet of Things, Routing Protocols, Energy Efficiency, Reinforcement Learning, Optimization, Edge Computing, Blockchain

INTRODUCTION

The Internet of Things (IoT) has evolved into a pervasive paradigm, interconnecting billions of physical objects equipped with sensing, computing, and communication capabilities. Wireless Sensor Networks (WSNs) are among the most critical building blocks of IoT, as they enable pervasive, fine-grained monitoring of the physical environment by deploying a large number of low-cost sensor nodes. These nodes collaborate to sense physical phenomena (e.g., temperature, humidity, vibration, pollution, physiological signals) and forward data to one or more sinks or gateways, which connect the WSN to edge servers or cloud platforms.

When WSNs operate as part of an IoT system, routing becomes even more complex than in traditional standalone sensor networks. IoT-driven WSNs are often deployed in heterogeneous environments, may involve hierarchical or multi-tier architectures, and must satisfy application-specific QoS constraints such as bounded latency, reliability, and security. Moreover, IoT applications may dynamically adjust sampling rates and control actions based on analytics, which in turn changes the traffic patterns within the WSN. These dynamics impose stringent requirements on routing protocols, which must simultaneously optimize energy consumption, load balancing, end-to-end delay, packet delivery ratio, and robustness under varying conditions.

Classical WSN routing protocols such as LEACH, PEGASIS, TEEN, and hierarchical clustering schemes have provided useful baselines for energy efficiency. Standard IoT routing solutions, for example the IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL), have become widely adopted in constrained IoT deployments. However, recent studies highlight that many of these protocols struggle to cope with the highly dynamic, context-rich, and large-scale scenarios of modern IoT-driven WSNs, particularly when mobility, context-awareness, and security are critical requirements [1,2].

Simultaneously, a large body of work has proposed optimization-based and intelligent routing strategies leveraging metaheuristics (e.g., ant colony optimization, particle swarm optimization), mathematical programming, and artificial intelligence (e.g., Q-learning, deep reinforcement learning, and context-aware reasoning) to produce near-optimal routes under complex constraints. For example, Han et al. [3] design an improved ant colony algorithm for IoT-oriented WSN routing to prolong network lifetime, whereas various recent works adopt RL-enhanced RPL variants, cluster optimization, or edge AI for adaptive decision-making.

Existing surveys often focus either on classical WSN routing or on broader IoT networking issues. There is still a need for an integrated review that explicitly targets routing optimization and challenges in WSNs under the IoT framework, covering both classical protocol families and emerging optimization and learning-based solutions from roughly 2020 onwards.

CONTRIBUTIONS

This paper makes the following contributions:

- Provides a structured overview of routing requirements and constraints for WSNs operating under IoT frameworks.
- Classifies routing challenges into energy, scalability, reliability, latency, heterogeneity, mobility, and security/privacy, with direct relevance to IoT scenarios.
- Reviews state-of-the-art optimization-based and intelligent routing techniques (ACO, PSO, GA, Fuzzy, LP/MILP, RL, DRL, SDN, edge, and Blockchain) with a focus on real works from 2020–2025.
- Compares representative routing protocols in terms of metrics, strengths, limitations, and IoT application domains.
- Highlights open research issues and suggests future directions such as federated learning-based routing, cross-layer RL, sustainable and green routing, and quantum-inspired optimization.

The rest of the paper is organized as follows. The first section briefly presents the background on WSNs and IoT architectures, as well as routing protocol families. The next section identifies and analyzes routing challenges under IoT frameworks. The third section reviews classical routing protocols and RPL-based solutions. The fourth section presents optimization and intelligent techniques for routing. The next section discusses emerging trends including context-aware, SDN, edge, and blockchain-enabled routing. The sixth section provides a comparative discussion. The final section concludes the paper and outlines future research directions.

BACKGROUND: WSNS IN THE IOT FRAMEWORK

I. Architecture of IoT-driven WSNs

A typical IoT-driven WSN architecture involves three or four logical layers:

- Perception (or sensing) layer: Composed of sensor nodes that sense, process, and transmit data wirelessly. Nodes are battery-powered, with limited CPU, memory, and bandwidth. Multiple communication technologies may coexist, such as IEEE 802.15.4 (ZigBee), BLE, LoRaWAN, and sub-GHz proprietary protocols.
- Network (or transport) layer: Responsible for multi-hop routing, addressing, and connectivity management among sensor nodes, sinks, and IoT gateways. In many IoT scenarios, IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN) is used, with RPL as a primary routing protocol. LoRaWAN and NB-IoT may act as backhaul technologies to send aggregated data to cloud servers.

• Edge/fog layer: Consists of intermediate nodes with higher computing capabilities (e.g., gateways, micro data centers) that can perform localized analytics, caching, and routing optimization. Edge/fog computing contributes to reduced latency and bandwidth consumption by avoiding sending all raw data to the cloud.
• Cloud/application layer: Hosts large-scale data processing platforms, machine learning models, and application logic that consume the data produced by WSNs and orchestrate control decisions.

In such architectures, WSN routing does not merely forward sensor data to a fixed sink but increasingly must consider multi-tier communication paths, edge-based processing, and application-aware routing criteria.

II. Routing Protocol Families

Routing protocols in WSNs and IoT-driven sensor networks can be broadly categorized into:
1. Flat (data-centric) routing: Nodes are mostly homogeneous and play symmetric roles. Protocols such as Directed Diffusion and rumor routing use data-centric communication and in-network aggregation, but are less adopted directly in IP-based IoT stacks.
2. Hierarchical (cluster-based) routing: Nodes are organized into clusters; cluster heads (CHs) collect and aggregate data from cluster members and forward it to sinks. Classical examples include LEACH, PEGASIS, TEEN, and their numerous variants.
3. Location-based routing: Node positions (obtained via GPS or localization algorithms) are used to guide forwarding decisions, e.g., GEAR or geographic greedy routing. These protocols reduce state and simplify path selection but require reliable location information.
4. QoS-aware and multipath routing: Protocols that explicitly consider metrics such as latency, jitter, throughput, or reliability and may use multiple paths to improve robustness and load balancing.
5. Standard IoT routing protocols: The IETF RPL protocol is the most prominent example, constructing a Destination-Oriented Directed Acyclic Graph (DODAG) rooted at the sink. RPL supports different objective functions (e.g., ETX, energy, hop count) and is widely used in 6LoWPAN-based IoT.
6. Software-defined and cognitive routing: SDN-based WSNs centralize control logic in a controller, enabling adaptive routing configurations. Cognitive routing uses learning and reasoning techniques to adapt to dynamic contexts.

III. Performance Metrics and Optimization Objectives

Key performance metrics for routing in IoT-driven WSNs include:
• Energy consumption and network lifetime: Sum of energy spent for sensing, processing, and communication; lifetime commonly defined as the time until first or last node dies.
• Packet delivery ratio (PDR): Ratio of successfully received packets to generated packets.
• End-to-end delay and latency distribution: Time required for a packet to reach the sink; often critical in industrial IoT and healthcare.
• Throughput and goodput: Amount of successfully delivered data per unit time.
• Control overhead: Number of control packets or routing updates required.
• Reliability and robustness: Ability to sustain connectivity under node failures, interference, or mobility.
• Scalability: Performance as network size and density increase.
• Security and privacy: Resilience to attacks such as sinkhole, spoofing, selective forwarding; validity of trust and authentication mechanisms.

Routing optimization often involves multi-objective formulations that trade off these metrics under constraints such as battery limits, bandwidth, and processing capacity.

ROUTING CHALLENGES IN WSNS UNDER IOT FRAMEWORK

Although many routing protocols have been introduced, IoT-driven WSNs face a combination of old and new routing challenges.

I. Energy Constraints and the Energy-Hole Problem

Sensor nodes are typically battery-powered and may be deployed in harsh environments where replacing or recharging batteries is difficult or impossible. Routing protocols must therefore minimize energy consumed by data transmission and reception, which are typically the dominant contributors to energy usage.

A particular challenge is the energy-hole problem, where nodes near the sink or gateways deplete their energy much faster than distant nodes due to relaying large amounts of traffic. This leads to network partitioning and reduces overall network lifetime. The Studies such as Haque and Baroudi [4] and Han et al. [3] address energy-efficient routing by balancing the load among nodes and selecting energy-aware paths [4, 5, 6].

II. Scalability and Topology Dynamics

IoT deployments may consist of hundreds or thousands of sensor nodes. As network size grows, maintaining up-to-date routing tables and control information becomes challenging. Classical cluster-based protocols may fail to scale efficiently due to frequent cluster reformation and control overhead.

In addition, many IoT applications involve topology dynamics, including node mobility (e.g., in vehicular sensing or wearable health monitoring), duty-cycling (nodes periodically sleep/wake), and dynamic sink placement (e.g., mobile sink or drone-assisted data mules). Routing must adapt quickly to such dynamics, which is non-trivial under strict energy constraints.

III. Reliability, Interference, and Link Quality Variation

Low-power wireless channels are prone to fading, interference from coexisting technologies (Wi-Fi, Bluetooth), and environmental obstructions. Link quality is thus highly variable and asymmetric. Protocols that rely on static link-cost metrics may suffer from high packet loss and frequent retransmissions.

Modern works increasingly incorporate link quality indicators (LQI), received signal strength (RSSI), and statistically learned metrics into routing decisions. Context-aware and RL-based protocols attempt to learn stable high-quality paths while avoiding links with poor reliability [1, 7].

IV. Latency and QoS Constraints

Many IoT applications require timely data delivery, especially in industrial automation, vehicular networks, and healthcare monitoring. Routing protocols need to meet bounded end-to-end delay and sometimes jitter requirements. Delay-constrained routing must prioritize shorter paths and reduce congestion, often at the cost of higher energy consumption.

Recent QoS-aware RPL variants and context-aware routing schemes explicitly trade off energy and latency by incorporating delay metrics into objective functions [1, 8].

V. Heterogeneity and Multi-Technology Integration

IoT-driven WSNs are heterogeneous along several dimensions: node capabilities (energy, CPU, storage), radio interfaces (e.g., ZigBee, BLE, LoRaWAN), and application-level requirements. In some deployments, high-end nodes act as cluster heads, relay nodes, or gateways, while low-end nodes primarily sense.

Routing protocols must exploit this heterogeneity to assign more complex responsibilities to powerful nodes and offload computation or aggregation tasks, while ensuring fairness and avoiding bottlenecks. Multi-hop routing over heterogeneous links and multi-radio configurations brings additional design complexity.

VI. Mobility and Mobile Sink Placement

Mobility is increasingly common in IoT scenarios: mobile robots, UAVs, vehicles, and human-carried devices interact with static or mobile sensors. Mobility breaks assumptions of static topology. Besides, employing a mobile sink can mitigate energy holes by changing the traffic pattern, but raises a joint problem of sink trajectory planning and routing.

Recent works use deep reinforcement learning (DRL) to jointly optimize mobile sink trajectories and routing decisions, reducing both energy consumption and delay as used in other applications [9].

VII. Security, Privacy, and Trust

Routing protocols in IoT-driven WSNs are exposed to various attacks, such as sinkhole, wormhole, blackhole, Sybil, and selective forwarding. Adversaries may compromise nodes and misroute traffic or inject bogus control messages. Traditional cryptographic security is necessary but not sufficient; routing must integrate trust management and anomaly detection mechanisms.

Blockchain and distributed ledger technologies have been proposed to provide tamper-proof records of routing and trust transactions in WSN-based IoT systems [10]. However, the overhead of blockchain must be carefully managed to maintain energy efficiency.

CLASSICAL ROUTING PROTOCOLS AND IOT EXTENSIONS

This section briefly revisits classical energy-aware routing and then focuses on IoT-oriented protocols, particularly RPL and its enhancements.

I. Cluster-Based and Chain-Based Protocols

LEACH (Low-Energy Adaptive Clustering Hierarchy), though older, remains a reference design. It randomly selects cluster heads in each round to balance energy consumption and uses single-hop communication between CHs and the sink. However, LEACH is unsuitable for large-scale or multi-hop IoT scenarios due to its assumptions and randomness.

PEGASIS arranges nodes in a chain, where each node communicates only with close neighbors and passes data along the chain to reach the sink. This reduces the number of transmissions but may increase delay. Recent works such as Chugh et al. [2] propose Advanced Energy-Efficient PEGASIS-based routing tailored for IoT applications, improving energy distribution and PDR.

Hierarchical cluster-tree protocols like CT-RPL [8] integrate clustering concepts with RPL, forming a cluster tree to maximize IoT network lifetime.

II. RPL and Its Variants

RPL (Routing Protocol for Low-Power and Lossy Networks) is the de facto standard for many IoT deployments using 6LoWPAN and IPv6. RPL organizes nodes into a Destination-Oriented Directed Acyclic Graph (DODAG), where each node selects a preferred parent based on an objective function (OF). Common metrics include Expected Transmission Count (ETX), hop count, and residual energy.

However, vanilla RPL has limitations in terms of:

- Handling mobility and frequent topology changes.
- Ensuring load balancing and avoiding parent overuse.
- Supporting QoS metrics beyond ETX/hop count.
- Mitigating routing attacks and ensuring trust.

To address these issues, various RPL enhancements have been proposed:

- Energy-aware RPL variants, e.g., integrating residual energy into the OF.
- Cluster-tree based RPL (CT-RPL) [8], which combines hierarchical clustering with RPL's DAG structure to prolong network lifetime.
- Context-aware RPL (CA-RPL) [1], which uses contextual information (mobility, link quality, energy, traffic type) to adapt parent and route selection dynamically.
- Secure and trust-enhanced RPL [10, 11], which incorporates trust scores and potentially blockchain support.

III. Data Aggregation and In-Network Processing

Since communication dominates energy consumption, routing protocols often integrate data aggregation to reduce redundant transmissions. Surveys on data aggregation and routing [7, 12] and recent Q-learning based aggregation schemes [12] show that intelligently combining routing and aggregation can significantly reduce energy consumption, especially in IoT scenarios with highly correlated data (e.g., environmental monitoring).

Aggregation-aware routing must ensure that data compression does not violate application requirements regarding accuracy or timeliness.

OPTIMIZATION AND INTELLIGENT ROUTING TECHNIQUES

Optimization and AI techniques have become central to routing design in IoT-driven WSNs. This section reviews major approaches and illustrates how they are used to address the challenges outlined earlier.

I. Ant Colony Optimization (ACO) and Its Variants

Ant Colony Optimization (ACO) is a bio-inspired metaheuristic that uses artificial pheromones to explore and exploit good paths. In routing, each ant corresponds to a candidate path from a source to the sink, and pheromone trails are updated based on path quality.

Han et al. [3] propose a wireless sensor network routing optimization based on an improved ant colony algorithm in the IoT. Their approach integrates energy and hop-count metrics into the pheromone updating rule. The objective function considers the trade-off between minimizing network energy consumption and maximizing throughput. According to their simulation results, the improved ACO significantly reduces the number of dead nodes and improves network throughput compared to baseline methods.

Other works integrate ACO with fuzzy logic or clustering to accelerate convergence and adapt to network dynamics, particularly under IoT workloads.

II. Particle Swarm Optimization (PSO) and Hybrid PSO-GA

Particle Swarm Optimization (PSO) treats candidate routing configurations as particles in a search space. Each particle updates its velocity and position based on individual and global best solutions.

In IoT routing, PSO can be used to optimize cluster head selection, relay node placement, or multi-hop paths. An interesting direction is adaptive PSO with genetic mutation for IoT-enabled software-defined WSNs, where PSO is combined with a genetic operator to escape local minima and adapt to dynamic conditions.

Hybrid PSO-GA methods use PSO for quick convergence and GA's crossover/mutation to maintain diversity, which is beneficial in highly dynamic IoT environments.

III. Fuzzy Logic-Based Routing

Fuzzy logic handles uncertainty and vagueness in metrics like residual energy, link quality, and traffic load. A fuzzy inference system maps linguistic inputs (e.g., "high energy", "medium quality", "low congestion") to a routing score.

In IoT-driven WSNs, fuzzy logic has been used to:

- Rank candidate cluster heads based on residual energy and connectivity.
- Select next-hop nodes considering RSSI, LQI, and queue length.
- Combine multiple QoS dimensions into a single routing decision.

For example, a fuzzy rule might be: IF residual energy is high AND link quality is good AND queue length is low THEN routing score is very high. Routing then chooses the neighbor with the highest fuzzy score.

Fuzzy systems have low computational complexity and are suitable for resource-constrained sensors, although tuning membership functions and rules remains a challenge.

IV. Mathematical Programming and MILP

Some works formulate routing as a mathematical programming problem, typically as Linear Programming (LP) or Mixed-Integer Linear Programming (MILP) as is used in other problems [13-15]. The objective may be to maximize network lifetime or minimize total energy consumption subject to connectivity and capacity constraints.

Deployment optimization for WSNs using deep neural networks (e.g., SAE-PNN models) also implicitly addresses routing by optimizing node placements and connectivity.

The drawback of MILP-based methods is their computational complexity, which limits their direct application to large-scale IoT networks. They are often used to derive upper bounds or offline designs, not real-time routing.

V. Reinforcement Learning (RL) and Q-Learning

Reinforcement learning formulates routing as a sequential decision-making problem. Each node (or controller) acts as an agent that learns a policy π(s)\pi(s)π(s) mapping states (e.g., residual energy, neighbor link qualities, queue length) to actions (e.g., next-hop selection) to maximize a long-term reward.

Q-learning is a model-free RL algorithm. At each step, the Q-value is updated by:

Recent works in WSN routing have used Q-learning for:

- Energy-aware cluster formation and cluster head selection.
- In-network data aggregation routing [12, 16].
- Adaptive parent selection in RPL variants (RL-RPL).

For example, a Q-learning based aggregation routing protocol can reward actions that reduce the number of transmitted packets while maintaining acceptable delay and loss rates, thus aligning with IoT application requirements.

VI. Deep Reinforcement Learning (DRL) and Edge AI

Deep reinforcement learning extends RL by using deep neural networks to approximate value functions or policies. This is particularly useful when the state space is large or high-dimensional (e.g., when considering multiple metrics, topological features, and temporal history).

In IoT-driven WSNs:

- DRL has been used for mobile sink trajectory optimization and joint routing.
- RL-enhanced RPL designs apply deep Q-networks (DQNs) or actor–critic architectures to learn dynamic objective functions that adapt to varying traffic loads and mobility.
- Edge AI architectures allow DRL models to be partially executed at gateways, reducing the burden on sensor nodes.

DRL improves adaptability and can outperform heuristic methods under diverse conditions. However, model training and inference cost must be carefully managed.

VII. Software-Defined Networking (SDN) and Centralized Optimization

Software-Defined Networking (SDN) decouples the control plane from the data plane. In SDN-based WSNs, sensor nodes act as simple forwarding devices, while a central controller maintains a global view of the network and computes optimized routes.

In an IoT framework, SDN-enabled WSNs can:

- Use global optimization algorithms (e.g., MILP, PSO, GA) at the controller to configure routing tables.
- Dynamically reconfigure routes based on traffic and energy states.
- Facilitate network slicing and QoS differentiation for different IoT applications.

A limitation is the potential overhead and single point of failure at the controller, which motivates hierarchical or distributed SDN approaches.

Emerging Trends: Context-Aware, Edge, Blockchain and Beyond

Recent literature (particularly 2020–2025) points to several emerging trends that significantly impact routing design in IoT-driven WSNs.

I. Context-Aware Routing

Context-aware routing exploits contextual information such as node mobility patterns, environmental conditions, application priorities, and user-defined policies to make more informed routing decisions. Instead of relying solely on static metrics like ETX, context-aware protocols adapt their behavior based on current conditions.

Khedr et al. [1] provide a detailed classification of context-aware routing protocols. Key insights include:

- Context-aware clustering can significantly reduce energy usage compared to classical LEACH; the Context-Aware Clustering Hierarchy (CACH) shows up to 58.8% energy savings.
- Context-aware RPL variants (CA-RPL) adapt to node mobility and dynamic traffic, achieving packet delivery ratios above 80–90% under varying mobility levels.
- Proactive context-aware routing methods dominate current research, while reactive and hybrid methods remain underexplored.

Context-aware routing is particularly attractive for IoT scenarios with heterogeneous devices and applications, as it can prioritize delay-sensitive traffic or critical sensor readings while saving energy on non-critical flows.

II. Edge and Fog-Assisted Routing

Edge and fog computing bring computation and storage closer to the data sources. Instead of performing all optimization in the cloud, intermediate edge nodes (e.g., gateways) can host:

- RL/DRL agents that learn and update routing policies.
- Aggregation and filtering functions to reduce data volume.
- Localized controllers for SDN-based WSNs.

Fog-assisted routing can significantly reduce control overhead and latency, as decisions are taken near the sensors rather than in distant clouds. This is crucial for applications like industrial IoT, smart grids, and autonomous systems.

Emerging designs use a hierarchical approach: sensor nodes perform simple forwarding based on rules provided by edge controllers, which themselves coordinate with cloud-level controllers for system-wide optimization.

III. Blockchain and Trust-Enhanced Routing

Blockchain or distributed ledger technologies can provide immutable logging of network events and support decentralized trust management in IoT-driven WSNs. In routing, blockchain can be used to:

- Record trust scores and reputation information for nodes.
- Validate control messages and prevent tampering.

- Support secure multipath routing with verifiable histories.

Biswas et al. [10] propose secure energy-efficient multipath routing for WSNs, and more recent work in 2024 discusses blockchain-enhanced routing for industrial IoT. The challenge is to integrate blockchain with minimal overhead; lightweight consensus algorithms and permissioned blockchains are commonly adopted to reduce energy consumption.

IV. 6G-Enabled and Internet of Robotic Things (IoRT)

The vision of 6G networks involves ultra-reliable low-latency communications (URLLC), massive machine-type communications (mMTC), and integrated sensing and communication. WSNs in such environments will interact with robotic agents (IoRT), drones, and autonomous vehicles.

Routing in this context must account for:

- High mobility.
- Strict latency and reliability constraints.
- Cross-domain orchestration between terrestrial and aerial WSNs.

Optimization techniques like DRL and graph neural networks (GNNs) are being explored to learn routing policies that exploit spatial-temporal patterns and to coordinate multiple agents.

V. Federated and Privacy-Preserving Learning for Routing

Federated learning (FL) allows multiple devices to collaboratively train models without sharing raw data. In IoT-driven WSNs, FL can be used to learn routing or traffic prediction models while preserving privacy.

Integrating FL with routing can lead to:

- Distributed training of link quality predictors.
- Collaborative learning of context-aware routing policies.
- Reduced communication overhead compared to sending raw logs to the cloud.

Challenges include handling non-IID data across nodes, limited bandwidth, and stragglers.

VI. Quantum-Inspired and Bio-Inspired Routing

Quantum-inspired optimization techniques such as Quantum Particle Swarm Optimization (QPSO) or quantum annealing are being investigated for complex combinatorial problems, including routing in large-scale networks [17-25]. Although practical deployment remains exploratory, such techniques may offer advantages in exploring very large solution spaces quickly.

Bio-inspired routing continues to evolve beyond classical ACO/PSO, drawing ideas from ecological systems, immune systems, and neural dynamics to design robust and self-healing protocols.

COMPARATIVE DISCUSSION

This section synthesizes insights from the reviewed literature and compares different categories of routing solutions.

I. Classical vs. Optimization-Based vs. Learning-Based Routing

- Classical cluster-based and RPL-based protocols:
  - Pros: Simplicity, standardization (especially RPL), relatively low overhead.
  - Cons: Limited adaptability to rapid topology changes, complex QoS requirements, and multi-metric optimization.
- Optimization-based (ACO, PSO, MILP, GA):
  - Pros: Provide near-optimal or optimal solutions for targeted objectives; often outperform classical heuristics in energy and lifetime.
  - Cons: May involve heavy computation and parameter tuning; not always suitable for real-time adaptation at node level.
- Learning-based (RL, DRL, context-aware, SDN with AI):
  - Pros: Capable of continuous adaptation to traffic patterns, mobility, and environmental context; can integrate multiple metrics into reward functions.
  - Cons: Require training data, convergence time, and additional computing resources; need careful deployment at edge/gateway level.

In practice, hybrid designs that combine RPL with RL (e.g., RL-RPL), or cluster-based routing with ACO/PSO for cluster head optimization, show promising trade-offs between performance and complexity.

II. Trade-offs and Design Guidelines

Based on the literature, several design guidelines can be drawn:

- For static or slowly changing WSNs with strong energy constraints and moderate QoS needs, cluster-based or ACO/PSO-enhanced routing is effective.
- For dynamic IoT environments with mobility, heterogeneous devices, and mixed QoS requirements, context-aware RPL variants and RL-based routing provide better adaptability.
- Edge/fog-assisted routing should be considered when low-latency decisions and rich analytics are needed; DRL models can be located at gateways.
- For security-critical IoT applications, secure multipath routing and trust-enhanced or blockchain-based schemes can provide robustness, though energy overhead must be managed.
- Future systems will likely require multi-objective optimization, considering energy, latency, reliability, security, and sustainability simultaneously.

Conclusion and Future Research Directions

This paper has presented a comprehensive review of routing optimization and challenges in wireless sensor networks under the IoT framework. We have discussed the key characteristics of IoT-driven WSNs, outlined routing requirements and constraints, and systematically analyzed routing challenges including energy constraints, scalability, reliability, latency, heterogeneity, mobility, and security/privacy.

We reviewed classical routing protocols such as cluster-based schemes and RPL, and examined their strengths and shortcomings in IoT contexts. We then focused on optimization-based techniques including ACO, PSO, GA, fuzzy logic, and mathematical programming, as well as intelligent approaches such as RL, DRL, and SDN-based routing. Special attention was given to emerging trends such as context-aware routing, edge/fog-assisted routing, blockchain and trust-enhanced routing, 6G-enabled IoRT, federated learning, and quantum-inspired optimization.

From the survey of literature between 2020 and 2025, several future research directions emerge:

1. Cross-layer and multi-objective RL routing: There is a need for joint optimization across MAC, network, and application layers, with RL/DRL-based policies that consider energy, delay, reliability, and security simultaneously.
2. Lightweight learning on constrained devices: While DRL and FL provide strong optimization capability, their resource demands are high. Techniques such as model compression, knowledge distillation, and on-device incremental learning should be further explored for sensor-level deployment.
3. Federated and privacy-aware routing intelligence: Integrating federated learning with routing protocols offers promising privacy and scalability benefits. Managing non-IID data, intermittent connectivity, and limited bandwidth in FL remains open.
4. Secure and trustworthy routing with minimal overhead: Blockchain and trust management schemes should be tailored for ultra-low-power sensor nodes, using lightweight consensus, off-chain storage, and hybrid on-chain/off-chain designs.
5. Sustainable and green routing: Future IoT-driven WSNs should consider environmental sustainability, aligning routing decisions with energy harvesting capabilities, carbon footprints, and long-term ecological impact.
6. 6G and IoRT-aware routing: As 6G and the Internet of Robotic Things become realities, routing protocols must address highly mobile, multi-domain environments involving terrestrial, aerial, and underwater sensors and actuators, potentially leveraging advanced AI and graph-based models.
7. Benchmarking and open datasets: The community would benefit from shared benchmarking platforms and publicly available datasets to fairly evaluate routing algorithms under comparable conditions, including realistic mobility, interference, and energy models.

By addressing these directions, future routing solutions in IoT-driven WSNs can move towards self-optimizing, context-aware, secure, and sustainable systems capable of meeting the demands of next-generation smart environments.

References

[1] A. M. Khedr *et al*., “Advancing IoT-driven wireless sensor networks with context-aware routing: A comprehensive review,” Computer Science Review, vol. 58, Art. no. 100803, Nov. 2025, doi: 10.1016/j.cosrev.2025.100803.

[2] P. Chugh *et al*., “Advanced energy-efficient PEGASIS-based routing protocol for Internet of Things applications,” Microprocessors and Microsystems, vol. 103, Art. no. 104727, 2023.

[3] H. Han, J. Tang, and Z. Jing, “Wireless sensor network routing optimization based on improved ant colony algorithm in the Internet of Things,” Heliyon, vol. 10, no. 1, Art. no. e23577, Jan. 2024, doi: 10.1016/j.heliyon.2023.e23577.

[4] M. E. Haque and U. Baroudi, “Dynamic energy-efficient routing protocol in wireless sensor networks,” Wireless Networks, vol. 26, no. 5, pp. 3715–3733, Jul. 2020.

[5] G. Farahani, “Improving network energy consumption using novel proposed geographic routing with mobile sink in wireless sensor networks,” Journal of Industrial Engineering International, vol. 20, no. 2, p. 23, 2024, doi: 10.82374/jiei.2025.1197138.
[6] G. Farahani and A. Farahani, “Optimization of mobile base station placement to reduce energy consumption in multi-hop wireless sensor networks,” Journal of Industrial Engineering International, vol. 19, no. 2, p. 1, 2023, doi: 10.1109/ICAC55051.2022.9911088.
[7] R. E. Mohamed *et al*., “Energy-efficient collaborative proactive routing protocol for wireless sensor networks,” Computer Networks, vol. 142, pp. 154–167, 2018.
[8] S. Sankar *et al*., “CT-RPL: Cluster-tree-based routing protocol to maximize the lifetime of the Internet of Things,” Sensors, vol. 20, no. 20, 2020.
[9] G. Farahani *et al*., “Identification of grape leaf diseases using proposed enhanced VGG16,” in Proceedings of the 27th International Conference on Automation and Computing (ICAC), Sep. 2022, pp. 1–6, IEEE, doi: 10.1109/ICAC55051.2022.9911074.
[10] P. Biswas *et al*., “A multipath routing protocol for secure and energy-efficient communication in wireless sensor networks,” Computer Networks, vol. 232, Art. no. 109842, 2023.
[11] D. B. D. and F. Al-Turjman, “A hybrid secure routing and monitoring mechanism in Internet of Things-based wireless sensor networks,” Ad Hoc Networks, vol. 97, Art. no. 102022, 2020.
[12] R. Maivizhi and P. Yogesh, “Q-learning-based routing for in-network aggregation in wireless sensor networks,” Wireless Networks, vol. 27, pp. 1–20, 2021.
[13] A. Farahani and M. L. Moghadam, “Workers scheduling in production logistics in a job shop production system,” Journal of Industrial Engineering International, vol. 21, no. 3, p. 18, 2025, doi: 10.82374/jiei.2025.1205831.
[14] A. Farahani *et al*., “Flexible personnel scheduling in large multi-product unpaced asynchronous assembly lines,” in Proceedings of the 27th International Conference on Automation and Computing (ICAC), Sep. 2022, pp. 1–6, IEEE, doi: 10.82374/jiei.2024.1039666.
[15] A. Farahani *et al*., “Partial flexible job shop scheduling considering preventive maintenance and priorities,” Working Papers on Operations Management, vol. 11, no. 2, pp. 27–48, 2020, doi: 10.4995/wpom.v11i2.14187.
[16] A. Feng *et al*., “In-network aggregation for data center networks: A survey,” Computer Communications, vol. 198, pp. 63–76, 2023.
[17] X. Li *et al*., “A distributed routing algorithm for data collection in low-duty-cycle wireless sensor networks,” IEEE Internet of Things Journal, vol. 4, no. 5, pp. 1420–1433, 2017.
[18] V. Kanakaris, D. Ndzi, and G. A. Papakostas, “Sensitivity analysis of the Ad hoc On-Demand Distance Vector routing protocol regarding forwarding probability,” Optik, vol. 127, no. 3, pp. 1016–1021, 2016.
[19] T. O. Kebeng, S. M. Sheikh, and M. Kgwadi, “Reducing routing overhead with a clustering protocol based on Ad Hoc Distance Vector and Dynamic Source Routing protocols,” in Proceedings of the International Conference on Artificial Intelligence, Big Data, Computing and Data Communication Systems (ICABCD), 2022.
[20] S. Roy *et al*., “Secure data aggregation in wireless sensor networks: Filtering out the attacker’s impact,” IEEE Transactions on Information Forensics and Security, vol. 9, no. 4, pp. 681–694, 2014.
[21] A. Poornima and B. Amberker, “SEEDA: Secure end-to-end data aggregation in wireless sensor networks,” in Proceedings of the World Congress on Nature and Biologically Inspired Computing (WOCN), 2010.
[22] M. Venkatanaresh *et al*., “Effective proactive routing protocol using smart nodes system,” Measurement: Sensors, vol. 24, Art. no. 100456, 2022.
[23] S. Pourroostaei Ardakani, J. Padget, and M. De Vos, “A mobile agent routing protocol for data aggregation in wireless sensor networks,” International Journal of Wireless Information Networks, vol. 24, pp. 27–41, 2017.
[24] S. Saginbekov and A. Jhumka, “Many-to-many data aggregation scheduling in wireless sensor networks with two sinks,” Computer Networks, vol. 123, pp. 184–199, 2017.
[25] M. Umar, N. Alrajeh, and A. Mehmood, “SALMA: An efficient state-based hybrid routing protocol for mobile nodes in wireless sensor networks,” International Journal of Distributed Sensor Networks, 2016.