



Paper Type: Original Article

Multi-Hop Routing Techniques in IoT-Driven Wireless Sensor Networks

Kalpak Dhole^{1*}, Hitesh Mohapatra² 

¹ School of Computer Engineering, KIIT (Deemed to Be) University, Bhubaneswar-751024, Odisha, India; kalpak.dhole@gmail.com; hiteshmahapatra@gmail.com.

Citation:

Received: 13 August 2025

Revised: 25 October 2025

Accepted: 19 December 2025

Dhole, K., & Mohapatra, H. (2026). Multi-hop routing techniques in IoT-driven wireless sensor networks. *Smart Internet of Things*, 3(1), 19-24.

Abstract

With the rise of the Internet of Things (IoT), Wireless Sensor Networks (WSNs) have gained increasing attention for their ability to collect and process environmental data in applications such as healthcare, smart cities, and industrial automation. Multi-hop routing, where data packets traverse multiple nodes before reaching the final destination, is a fundamental concept in WSNs. Efficient multi-hop routing is crucial for enhancing energy efficiency, minimizing latency, and extending network longevity. This paper explores multi-hop routing techniques in IoT-driven WSNs, focusing on the design challenges, performance metrics, and prominent routing protocols. We also highlight future research directions and open challenges to improve multi-hop routing in IoT applications.

Keywords: Multi-hop routing, Wireless sensor networks, Internet of things, Energy efficiency, Machine learning in routing.

1 | Introduction

The proliferation of Internet of Things (IoT) applications has increased demand for robust, energy-efficient communication methods in WSNs. WSNs comprise many low-power sensor nodes deployed to monitor and report data on environmental parameters, physical movements, or specific events. Multi-hop routing, where data travels from node to node across multiple paths to a base station or sink, is critical in WSNs due to limited power, processing capabilities, and communication range of individual nodes. Given these constraints, multi-hop routing techniques aim to enhance network efficiency by balancing energy consumption, reducing delays, and maintaining high data accuracy.

This paper examines multi-hop routing techniques in IoT-driven WSNs, analyzes the challenges of implementing them, and evaluates some of the most commonly used multi-hop routing protocols.

 Corresponding Author: kalpak.dhole@gmail.com

 <https://doi.org/10.48313/siot.v3i1.274>



Licensee System Analytics. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0>).

2 | Background and Related Work

2.1 | Wireless Sensor Networks and IoT

Wireless Sensor Networks (WSNs) consist of sensor nodes distributed across specific areas to gather information from their surroundings. Each node contains sensors, a processor, and a communication module to transmit collected data to a sink node or gateway. In IoT, WSNs serve as data collection systems for diverse applications, such as smart cities, environmental monitoring, industrial automation, and healthcare. However, because sensor nodes typically operate on limited power, implementing efficient routing protocols is essential to maximize network lifetime and maintain data fidelity.

2.2 | Multi-Hop Routing in WSNs

Multi-hop routing allows data to traverse multiple nodes before reaching the final destination. Compared to single-hop routing, where nodes communicate directly with the sink, multi-hop routing is more energy-efficient for extensive networks as it reduces the need for long-range transmissions, which consume substantial energy [1]. Multi-hop routing is also more adaptable to various network topologies and environmental conditions, making it a preferred approach in large-scale WSNs.

2.3 | Existing Literature on Multi-Hop Routing

Several multi-hop routing protocols have been proposed in WSN literature, each with unique advantages and limitations [2], [3]. Notable examples include:

- I. Low-Energy Adaptive Clustering Hierarchy (LEACH): A hierarchical protocol that forms clusters to balance energy usage across nodes [4].
- II. Ad-Hoc On-Demand Distance Vector (AODV): A reactive protocol that finds paths based on demand [5].
- III. Routing Protocol for Low-Power and Lossy Networks (RPL): A distance vector protocol standardized for IPv6-based IoT applications [6].

3 | Design Challenges in Multi-Hop Routing for IoT-Driven WSNs

3.1 | Energy Efficiency

Due to limited battery resources, energy efficiency is a top priority in WSNs [7]. Multi-hop routing must balance the workload across nodes to avoid premature depletion of nodes near the sink, which could lead to network partitioning. Energy-efficient protocols often employ clustering and data aggregation to minimize redundant data transmission and conserve power [8], [9].

3.2 | Scalability

IoT-driven WSNs may involve many nodes, so protocols must adapt to different network sizes and densities. Scalability is critical, as network performance should not degrade significantly as the number of nodes increases.

3.3 | Latency and Reliability

Applications like healthcare monitoring or industrial automation may demand real-time or near-real-time data delivery, which can be challenging due to potential delays in multi-hop paths. Additionally, high packet delivery reliability is crucial for ensuring accurate data collection, especially in critical IoT applications.

3.4 | Mobility

In some IoT applications, nodes may be mobile, as in vehicular networks or wearable healthcare devices. Multi-hop routing protocols should be adaptable to dynamic topology changes to maintain connectivity.

4 | Prominent Multi-Hop Routing Protocols for IoT-Driven WSNs

4.1 | Low-Energy Adaptive Clustering Hierarchy

LEACH is a hierarchical routing protocol that organizes nodes into clusters, with each cluster led by a randomly selected cluster head. By distributing the cluster-head role, LEACH balances energy usage across nodes, extending network lifetime [7]. LEACH suits large-scale networks with periodic data transmission requirements, although it may struggle with scalability and adaptivity in highly dynamic environments.

4.2 | Ad-Hoc On-Demand Distance Vector

AODV is a reactive routing protocol that establishes paths between nodes only when needed [5], reducing the overhead of maintaining continuous routing tables. AODV is effective in highly dynamic environments but may experience delays due to route discovery time. It is less suitable for applications that require consistent data transmission.

4.3 | Routing Protocol for Low-Power and Lossy Networks

RPL is a distance vector protocol designed for low-power and lossy networks, making it suitable for IPv6-based IoT applications [6]. It uses a Destination-Oriented Directed Acyclic Graph (DODAG) structure to route data, which allows RPL to support multi-hop communication with a high degree of reliability. However, RPL may require optimization for applications with stringent latency requirements.

5 | Performance Metrics

5.1 | Energy Consumption

Energy consumption is a primary metric in WSNs, impacting the network lifetime and operational cost. Energy-efficient multi-hop routing protocols aim to minimize the energy usage per packet transmission by selecting optimal paths.

5.2 | Latency

Latency, the time taken for a data packet to reach the sink, is essential for time-sensitive applications. Low-latency multi-hop routing protocols prioritize shorter paths or paths with fewer nodes to reduce transmission time.

5.3 | Packet Delivery Ratio

Packet Delivery Ratio (PDR) measures the ratio of successfully delivered packets to the total sent packets. Multi-hop routing protocols aim to maintain a high PDR to ensure data integrity and accuracy.

5.4 | Network Lifetime

Network lifetime, defined as the duration until the first node depletes its battery, is a crucial metric in WSNs. Efficient multi-hop routing protocols aim to extend network lifetime by balancing energy usage across nodes.

6 | Future Directions and Open Challenges

6.1 | Integration of Machine Learning for Adaptive Routing

Machine learning algorithms could be integrated to enhance routing adaptability to dynamic conditions, such as changing traffic patterns or node mobility [10]. Reinforcement Learning (RL), for example, could allow protocols to learn optimal routing paths from experience.

6.2 | Security in Multi-Hop Routing

WSNs in IoT applications are vulnerable to attacks such as eavesdropping, data modification, and denial of service [11]. Developing secure multi-hop routing protocols to protect data privacy and integrity is an ongoing research challenge [12].

6.3 | Cross-Layer Optimization

Cross-layer design, which shares information across network layers, can improve routing efficiency. By allowing interaction between routing, data link, and physical layers, protocols could optimize path selection, reduce overhead, and improve latency.

6.4 | Energy Harvesting

Energy harvesting techniques, such as solar power, could supplement node energy in WSNs, enabling longer network operation and reducing energy constraints. Multi-hop routing protocols could be adapted to manage both harvested and stored energy to optimize network performance.

7 | Literature Review

In the domain of IoT-driven WSNs, multi-hop routing has become a crucial aspect of ensuring efficient data transmission across extensive sensor nodes. Many protocols have been proposed to address different challenges in these networks:

- I. LEACH: LEACH is a popular hierarchical protocol where nodes are divided into clusters, with one node acting as the cluster head. This method conserves energy by reducing the number of transmissions needed to communicate with the base station. LEACH has been widely studied for its simplicity and energy efficiency but is criticized for its scalability issues, especially in large networks with dynamic topologies.
- II. AODV: AODV is a reactive routing protocol that establishes routes on-demand. While it benefits mobile networks and networks with dynamic topologies, it incurs higher delays due to the route discovery process. It is suitable for scenarios where data is sporadically transmitted.
- III. RPL: RPL is a standard protocol developed specifically for low-power IoT devices. It uses a Directed Acyclic Graph (DAG) structure for routing, allowing multiple hops to reach the destination. RPL is more resilient to packet loss but may suffer from suboptimal routing decisions when network conditions change frequently.

These studies reveal that energy efficiency, scalability, and adaptability to network changes are among the primary concerns in multi-hop routing for WSNs in IoT.

8 | Proposed Work

The proposed work focuses on enhancing the efficiency of multi-hop routing protocols by integrating machine learning techniques to dynamically adapt routing decisions. In this approach:

- I. RL could be utilized to dynamically select the best routing paths based on factors like energy consumption, network congestion, and node mobility. The protocol would learn over time, optimizing routing decisions to balance energy usage and network longevity.
- II. Cross-layer optimization: Integrating data from different layers (application, network, and physical) could improve routing efficiency by considering factors like application requirements (e.g., latency) and physical conditions (e.g., signal strength). This optimization would help avoid congestion and improve packet delivery rates.

Combining these methods could yield a routing protocol that adapts to varying network conditions, offering better energy management, lower latency, and higher reliability in packet delivery.

9 | Results and Discussions

The proposed approach is tested against conventional multi-hop routing protocols such as LEACH, AODV, and RPL in a simulation environment. The evaluation metrics include energy consumption, latency, PDR, and network lifetime.

- I. Energy consumption: Integrating machine learning techniques and cross-layer optimization significantly reduces energy consumption compared to traditional protocols, particularly in large-scale networks.
- II. Latency: The proposed protocol outperforms other protocols in latency because it dynamically adjusts paths to avoid congested or distant nodes.
- III. PDR: The PDR of the proposed approach is higher than that of AODV, demonstrating its reliability in packet delivery. It also outperforms LEACH in larger networks where node energy and congestion are critical factors.
- IV. Network Lifetime: By efficiently balancing energy usage and optimizing path selection, the proposed protocol significantly extends network lifetime compared to LEACH and RPL.

These results suggest that integrating adaptive techniques into multi-hop routing protocols can significantly enhance the overall performance of WSNs in IoT applications.

10 | Future Work

The proposed work could be extended in the following directions:

Security enhancement: Because IoT devices are prone to attacks, it would be beneficial to incorporate secure routing mechanisms that prevent eavesdropping, data tampering, and denial-of-service attacks. Integrating cryptographic methods or intrusion detection systems into the routing protocol would enhance network security [13].

Energy harvesting: Future studies could explore integrating energy harvesting techniques, such as solar or thermal energy, into the routing protocol. This argument would reduce dependence on batteries and make WSNs more sustainable, especially for remote IoT applications.

Integration with 5G networks: Explore integrating IoT networks with 5G technology. Multi-hop routing protocols could be designed to work seamlessly with 5G's ultra-low latency and high-speed capabilities, further enhancing IoT performance.

Mobility support: Investigating the adaptation of multi-hop routing protocols to support high mobility scenarios, such as in vehicular networks, could expand the applicability of the work to newer IoT domains.

11 | Conclusion

Multi-hop routing is essential for the efficiency and reliability of IoT-driven WSNs. This paper reviewed various multi-hop routing protocols, including LEACH, AODV, and RPL, discussing their strengths, limitations, and applications in IoT. The paper highlighted challenges such as energy efficiency, scalability, and latency, as well as emerging areas like machine learning and energy harvesting. With continued research into adaptive and secure routing techniques, WSNs can play an even more significant role in supporting IoT applications across diverse fields.

Acknowledgments

The authors would like to express their sincere appreciation to all individuals whose valuable comments and support contributed to the successful completion of this study.

Funding

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Data Availability

The data supporting the findings of this study are available from the corresponding author upon reasonable request.

References

- [1] Al-Karaki, J. N., & Kamal, A. E. (2004). Routing techniques in wireless sensor networks: A survey. *IEEE Wireless Communications*, 11(6), 6–28. <https://doi.org/10.1109/MWC.2004.1368893>
- [2] Akkaya, K., & Younis, M. (2005). A survey on routing protocols for wireless sensor networks. *Ad Hoc Networks*, 3(3), 325–349. <https://doi.org/10.1016/j.adhoc.2003.09.010>
- [3] Radi, M., Dezfouli, B., Bakar, K. A., & Lee, M. (2012). Multipath routing in wireless sensor networks: Survey and research challenges. *Sensors*, 12(1), 650–685. <https://doi.org/10.3390/s120100650>
- [4] Heinzelman, W. R., Chandrakasan, A., & Balakrishnan, H. (2000). Energy-efficient communication protocol for wireless microsensor networks. *Proceedings of the 33rd Annual Hawaii International Conference on System Sciences* (pp. 10–pp). IEEE. <https://doi.org/10.1109/HICSS.2000.926982>
- [5] Perkins, C., Belding-Royer, E., & Das, S. (2003). *Ad hoc on-demand distance vector (AODV) routing*. <https://doi.org/10.17487/RFC3561>
- [6] Winter, T., Thubert, P., Brandt, A., Hui, J., Kelsey, R., Levis, P., ... & Alexander, R. (2012). *RPL: IPv6 routing protocol for low-power and lossy networks*. <https://doi.org/10.17487/RFC6550>
- [7] Kandris, D., Evangelakos, E. A., Rountos, D., Tselikis, G., & Anastasiadis, E. (2023). LEACH-based hierarchical energy efficient routing in wireless sensor networks. *AEU-International Journal of Electronics and Communications*, 169, 154758. <https://doi.org/10.1016/j.aeue.2023.154758>
- [8] Altowaijri, S. M. (2022). Efficient next-hop selection in multi-hop routing for IoT enabled wireless sensor networks. *Future Internet*, 14(2), 35. <https://doi.org/10.3390/fi14020035>
- [9] Alnawafa, E., & Marghescu, I. (2018). New energy efficient multi-hop routing techniques for wireless sensor networks: Static and dynamic techniques. *Sensors*, 18(6), 1863. <https://doi.org/10.3390/s18061863>
- [10] Nayak, P., Swetha, G. K., Gupta, S., & Madhavi, K. (2021). Routing in wireless sensor networks using machine learning techniques: Challenges and opportunities. *Measurement*, 178, 108974. <https://doi.org/10.1016/j.measurement.2021.108974>
- [11] Karlof, C., & Wagner, D. (2003). Secure routing in wireless sensor networks: Attacks and countermeasures. *Ad Hoc Networks*, 1((2-3)), 293–315. [https://doi.org/10.1016/S1570-8705\(03\)00008-8](https://doi.org/10.1016/S1570-8705(03)00008-8)
- [12] Alansari, Z., Anuar, N. B., Kamsin, A., & Belgaum, M. R. (2022). A systematic review of routing attacks detection in wireless sensor networks. *Peerj Computer Science*, 8, e1135. <https://doi.org/10.7717/peerj-cs.1135>
- [13] Ishmanov, F., & Bin Zikria, Y. (2017). Trust mechanisms to secure routing in wireless sensor networks: Current state of the research and open research issues. *Journal of Sensors*, 2017(1), 4724852. <https://doi.org/10.1155/2017/4724852>