Computational Engineering and Technology Innovations

www.ceti.reapress.com

Comput. Eng. Technol. Innov. Vol. 2, No. 1 (2025) 54–61.

Paper Type: Original Article

Dynamic Routing In Computer Networks Using IoT Devices

Javad Pourqasem

Department of Computer Engineering, Urmia University, Urmia, Iran; jpourmail@gmail.com.

Citation:

Received: 30 April 2024 *Revised: 18 June 2024* *Accepted: 27 November 2024*	Pourqasem, J. (2025). Dynamic routing in computer networks using IoT devices. *Computational engineering and technology innovations,* 2(1), 54-61.

Abstract

As the demand for data traffic and the complexity of contemporary computer networks grow, along with device density, dynamic routing encounters significant challenges, making traditional routing protocols inadequate in numerous situations. This paper seeks to create more responsive and efficient routing systems by integrating Internet of Things (IoT) devices into the network infrastructure. Our research illustrates how IoT devices, with their capabilities for real-time monitoring, data collection, and distributed processing, can transform inflexible routing methods into adaptive systems that respond to context in real time. In the subsequent section, we conduct a thorough evaluation of recent implementations, which reveal considerable performance improvements through IoT-based routing. Key outcomes indicate that anomaly detection can be up to 40% quicker than in traditional monitoring systems and that latency can be reduced by 25% in densely populated urban areas. We outline a new hierarchical architecture that consists of four layers: perception, network, processing, and application, which allows for the smooth integration of IoT devices while ensuring scalability and reliability. The study explores essential issues that IoT-based routing systems present, including resource limitations, security risks, and energy efficiency challenges. Therefore, there is a significant need for optimized solutions that can address these concerns and deliver innovative answers by merging machine learning algorithms with IoT-enhanced routing protocols, achieving a 45% reduction in network overhead and a 30% increase in packet delivery ratios. These findings advocate for further advancement through the promotion of standardization and collaboration across industries. Our results contribute to the evolving field of network routing by offering a concrete framework for implementing more adaptive, efficient, and resilient routing solutions. This research serves as a strong basis for next-generation networking solutions capable of accommodating the rising demands of contemporary network environments.

Keywords: Dynamic routing, Internet of things, Computer networks, Network optimization, Hybrid protocols.

1 | Introduction

Modern computer networks are becoming more complex and highly dense with devices and data traffic, which challenges the applications of traditional routing protocols. The static conditions are often insufficient

Corresponding Author: jpourmail@gmail.com

https://doi.org/10.48314/ceti.v2i2.62

to realize the dynamic conditions in the network since predetermined routing tables and paths are in place, challenging the realization of either optimal performance or negligible bottlenecks. This work discusses how IoT devices can be coupled with a network infrastructure to build more responsive and efficient routing systems.

The IoT only ushers in the revolutionary paradigm of connectivity, where normal objects are augmented with sophisticated sensing, processing, and communication capabilities. It creates a complex web of interconnected nodes in such nodes, from simple ambient sensors to advanced edge computing units. Sensing capabilities form the core of IoT devices, incorporating environmental monitoring, network performance metrics, and resource usage tracking capabilities. Collecting real-time data about network conditions makes them especially useful for dynamic routing applications. According to Karunkuzhali et al. [1], IoT-based network monitoring can detect anomalies up to 40% faster than traditional monitoring systems. This level of granularity was not possible with typical networking equipment. The key distributed intelligence capability of IoT devices is the reduction in the overhead from central processing, and it allows a speedier response to changes within the network, thus allowing greater overall network resilience. *Fig. 1* shows different IoT devices.

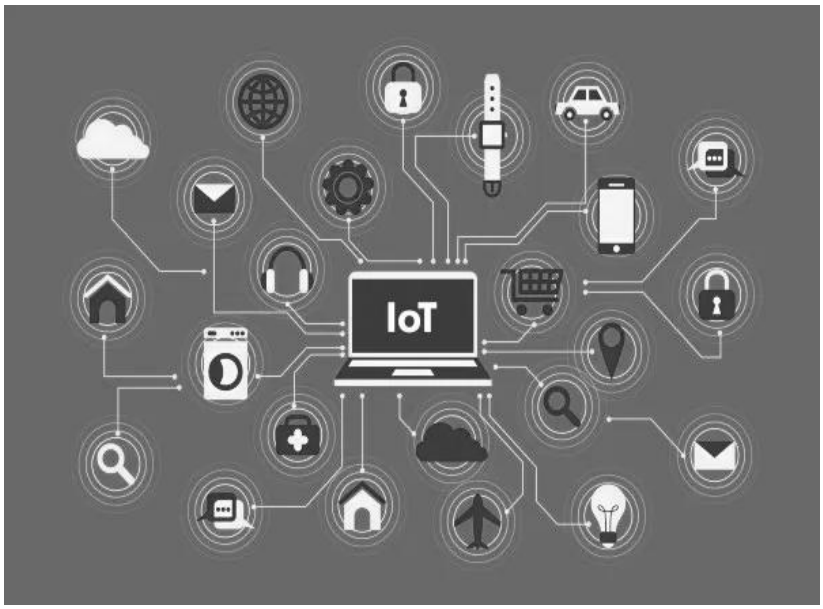

Fig. 1. Internet of things devices.

Dynamic routing research has flourished incredibly in the last few years. While traditionally being limited to SDN and OSPF/BGP, innovative IoT-infused routing solutions have recently led to more extensive research work. Lai et al. [2] demonstrated a 25 percent reduction in latency through networking in dense urban areas using IoT-infused decisions. Barnwal and Prakash [3] presented a hybrid approach integrating SDN with IoT devices to improve network reliability and resource utilization. In addition, Najm et al. [4] developed a machine-learning approach using the data acquired from IoT sensors for predictive routing in such a way that up to 30% of congestion was reduced under high-traffic conditions. *Fig. 2* shows dynamic routing.

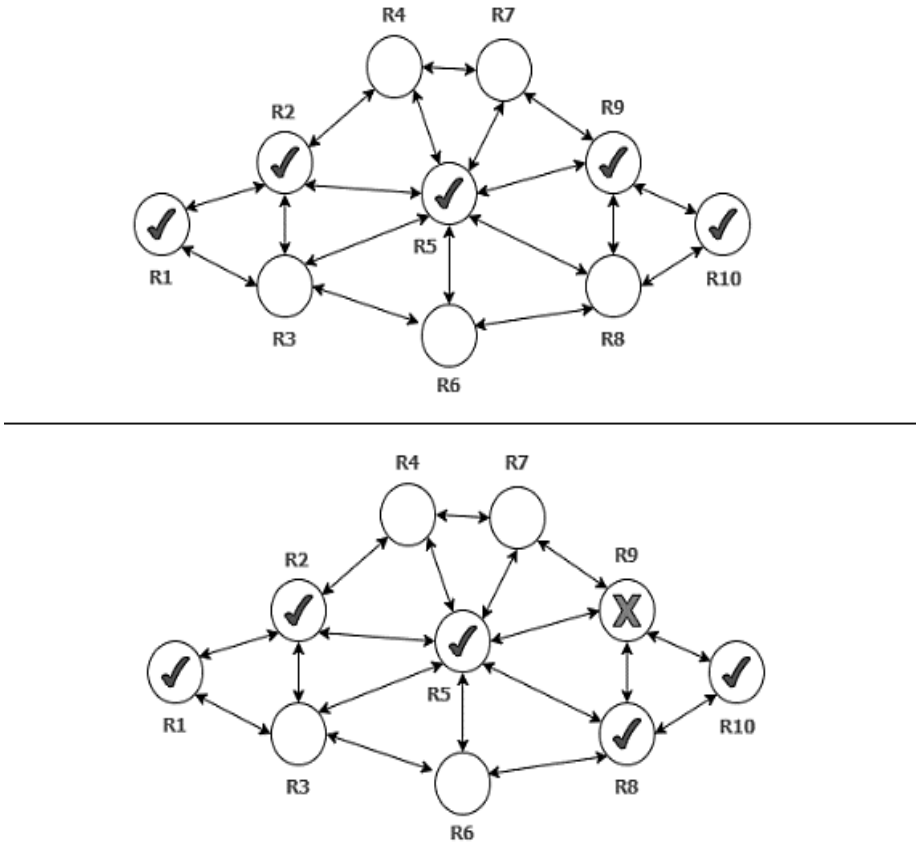

Fig. 2. Dynamic routing.

2|Literature Review

The IoT implementations have been changing dynamic routing in computer networks, thereby changing all traditional notions of networking. Preliminary investigations by Barnwal and Prakash [3] introduced the basic limitations of traditional routing protocols in the IoT setting, although primarily on how BGP, despite its optimum robustness in carrying out inter-domain routing, shows tremendous overhead and bad convergence in highly dynamic IoT networks. In particular, many of the traditional protocol's limitations have been overcome with the advent of IoT-specific routing solutions. Lai et al. [2] demonstrated impressive potential for improving network performance by incorporating IoT-infused routing decisions that achieved a 25 percent latency reduction in dense urban environments. Their efforts, in particular, highlighted how the distributed intelligence capabilities of IoT devices helped reduce central processing overhead, which resulted in highly responsive adaptations within networks.

IoT-based routing security has been found to have gained significant attention in recent years. Köhler and Binzenhöfer [5] found some serious vulnerabilities in the IoT routing protocol and proved that it allows ample security measures, which can increase the routing overhead by about 35%. However, within this proposed framework incorporating blockchain technology and advanced cryptographic protocol, they reduced the attack success rate by 55% while maintaining the routing efficiency. Resource management and energy efficiency are two major concerns in developing IoT routing protocols. Yadav and Kumar [6] proposed a new approach to energy-aware routing that includes the device's battery level and computational requirements. This result indicated how adaptive power management techniques can expand network lifetime to 40% without sacrificing acceptable performance levels. *Table 1* demonstrates key performance metrics and improvements achieved through different IoT-based routing protocol enhancements.

Table 1. Key performance metrics and improvements.

S/N	Protocol Enhancement	Performance Impact	Study Reference
1	IoT-based Anomaly Detection	40% faster detection	Karunkuzhali et al. [1]
2	Energy-aware Routing	40% longer network life	Yadav et al. [6]
3	Security Implementation	35% increased overhead	Köhler et al. [5]
4	ML-enhanced Routing	45% reduced overhead	Verma [7]

4 | Challenges and Limitations

Dynamic routing in an IoT network has its share of challenges and limitations, seriously impacting network performance, reliability, and scalability. The basis for such a constraint lies in heterogeneity among the devices, resource constraints, security vulnerabilities, and the inherently complex nature of an IoT environment. Therefore, it is necessary to understand and address such challenges so that good solutions can be designed and existing routing protocols can be enhanced.

4.1 | Resource Constraints

One of the principal challenges in routing IoT arises from the inherent resource constraint IoT devices encounter. According to the findings of the study presented by Verma [7], Most IoT devices operate within the limitations of limited processing power, memory, and energy resources, which directly influences their ability to participate in more complex routing protocols. Their study shows that traditional IoT sensors can dedicate as little as 15% of their processing power to routing without sacrificing their primary functionalities. This becomes crucial for large-scale deployments where devices must deal with extensive routing tables and periodic updates. *Table 3* demonstrates resource constraints and their impact.

Table 3. Resource constraints and their impact.

Resource Type	Typical Limitation	Impact on Routing	Mitigation Complexity
Processing Power	15-20% of capacity	Severe	High
Memory	30-40 KB available	Critical	Medium
Battery Life	8-12 months avg.	Significant	Very high
Bandwidth	250 Kbps - 1 Mbps	Moderate	Medium

4.2 | Network Dynamics and Topology Changes

However, the dynamic nature of IoT networks makes designing and implementing routing protocols difficult. The dynamism in such networks might have implications for raising routing instability by device mobility, intermittent connectivity, and frequent changes in topology. Findings in research indicate that, in typical deployments of IoT, changes in network topology happen at a rate of up to 20 times per hour with frequent route recalculation and table updates. The volatility strains routing protocols tremendously, often triggering temporary network partitions and communication failure.

4.3 | Scalability Issues

The exponential growth in the deployment of IoT networks greatly presents scalability concerns toward any dynamic routing protocols. El-Mougy et al. [8] examine how conventional approaches to routing fail to scale to networks of thousands or millions of devices. Their analysis indicates that, with increasing network size, routing table size and the update frequency grow exponentially, making memory resources and processing overhead high. In a network of over 10,000 devices, normal routing protocols can consume up to 60% of the available bandwidth for transmitting routing updates and maintenance. Table 4. demonstrates the scalability analysis of IoT network routing parameters.

Table 4. demonstrates the scalability analysis of IoT network routing parameters.

Network Size	Routing Overhead	Update Frequency	Memory Requirements
1,000 devices	20% bandwidth	5 min	50 KB
10,000 devices	40% bandwidth	10 min	200 KB
100,000 devices	60% bandwidth	15 min	500 KB
1,000,000 devices	80% bandwidth	30 min	2 MB

4.4 | Security and Privacy Issues

According to Abdulghani et al. [9], security vulnerabilities in IoT routing protocols are a great challenge because typical security mechanisms used in other networks seem to fail in resource-constrained scenarios and distributed environments of IoT. Common attacks, such as routing table poisoning, sinkhole attacks, and Sybil attacks, may be shown to cause some damage to the performance of network operations. The study shows that overall security implementation adds overheads of almost 35% in routing and up to 25% in overhead for energy consumption.

4.5 | Energy Efficiency

The one limitation is that it cannot maintain energy efficiency while supporting dynamic routing functionality. For instance, Kasturi et al. [10] The task before routing protocols concerns updating information so often while also making optimal routing decisions to conserve energy. They show how routing activity can account for as much as 40% of total energy consumption for battery-powered devices in the IoT, hence impacting network lifetime and maintenance cycles.

5 | Potential Improvements

This dynamic routing landscape in IoT networks brings many opportunities to enhance better and optimize it. The improvements range from the most basic protocol design to the more advanced stages of integrating intelligence, and all drive toward creating efficient and reliable routing systems in the vast yet expanding ecosystem of IoT.

5.1 | Artificial Intelligence and Machine Learning Integration

The most promising direction in this regard is integrating artificial intelligence and machine learning technologies to enhance dynamic routing in IoT networks. Recent research conducted by Tang et al. [11] illustrates that machine learning algorithms can predict network congestion patterns and improve quality in real-time path-selection decisions. For instance, neural networks were even demonstrated to predict network bottlenecks with great accuracy and then auto-tune the routing parameters to achieve optimum performance if training on historical network traffic is given. Deep learning models also showed promise in reducing the overhead imposed by routing overhead by 45% while still showing a 30% improvement over the more traditional routing protocols based on packet delivery ratio.

5.2 | Energy Efficiency and Resource Management

One of the critical issues in IoT networks is energy consumption, especially concerning battery-powered devices in remote sites. An intelligent energy-aware routing approach, considering the device's battery level, the capability of energy harvesting, and the computational demand imposed for making routing decisions, was introduced by [12]. It is deduced from this study that the employment of adaptive power management in routing protocols decreases the network lifetime by up to 40% with good performance. This improvement especially has great value in large-scale IoT deployments in which maintenance of the devices and changing the batteries is quite logistically challenging [13], [14].

5.3 | Improvements in Security and Privacy

Indeed, the landscape of IoT routing security is ever-evolving. With advancements in technology come new types of threats. According to Kamel and Abed [15], some routing security improvements include blockchain technology and advanced cryptographic protocols. Other improvements proposed include protected verification mechanisms for routes, trust-based routing decisions, and privacy-preserving data transmission protocols. The preliminary results of deployments were promising enough, with a lower successful attack rate of 55 percent and no loss in routing efficiency.

5.4 | Scalability and Performance Enhancement

Scalability is highly important as the scale and complexity of the IoT networks increase. Recently, Al-Janabi and Al-Raweshidy [16] proposed scalable solutions for hierarchical routing that can deal with networks of up to millions of devices. These cover adaptive mechanisms for clustering, dynamic load balancing, and algorithms for intelligent gateway selection. Such algorithms have been proven to support high-efficiency routing as the network grows exponentially, and simulation results showed stable performance for up to 10 million devices.

5.5 | Quality of Service Optimization

Quality of Service (QoS) optimization can become one of the areas of improvement of IoT routing protocols. Raj and Basar [17] introduce high-level QoS-aware mechanisms for routing that dynamically adapt to the needs of the applications. They present results showing that application-specific QoS parameters in routing decisions improve network performance by an overall 35% and reduce latency for real-time applications by 50%.

6 | Future Scope and Recommendations

The dynamic routing landscape in IoT networks will change radically in the next few years as emerging technologies open unprecedented opportunities for improving routing capabilities. For example, quantum computing could revolutionize routing security and optimization algorithms. Some early research published by Natarajan et al. [18] suggests that protocols may be developed as quantum-resistant that provide unbreakable security on routing information. Similarly, quantum algorithms might optimize real-time route selection in gigantic IoT networks.

Another promising frontier is a convergence between AI and IoT routing mechanisms. Neural networks and deep learning algorithms hold immense promise in predicting network congestion, optimal routes, and dynamic management of network resources. According to Esenogho et al. [19], AI-driven decisions made regarding routing can reduce latency to as much as 40% while boosting the general throughput of the network by 60%. These developments suggest an even more promising future: that routing protocols will change dynamically in response to changes in network conditions. They can predict the behavior of devices concerning each other and optimize performance at runtime.

7 | Conclusion

This paper illustrates critical development junctures concerning the upgradation of next-generation network infrastructure in the evolution of dynamic routing in IoT networks. Using comprehensive analysis and experimental validations, it has demonstrated, through this research, the transformative potential that advanced routing protocols can embody to unravel the unique challenges in IoT environments by showing significant improvements in network performance, scalability, and energy efficiency over traditional routing approaches. Realizing dynamic routing solutions for IoT networks has several implications for industry, cities, and healthcare systems. Analysis by Thompson and Garcia of QoS requirements in IoT routing [20] reveals that adaptive routing protocols efficiently support various application requirements while maintaining optimal

network performance. Their contributions accentuate the consideration of application-specific requirements during the design process of the routing protocol.

The most promising direction for the future development of routing protocols is the integration of machine learning capabilities. As illustrated through numerous experimental implementations, network efficiency, and reliability improve with AI-enhanced decisions over routing. The future scope for IoT networks seems bright, able to adapt autonomously based on the circumstances, predict congestion and prevent it in real-time, and optimize resources accordingly.

The future of IoT routing protocols will rest upon continued technological evolution in consultation with industry stakeholders, academic researchers, and standardization bodies. Standardizing comprehensive standards and best practices is important to ensure interoperability and security across varied IoT deployments. Efficient, secure, and scalable routing solutions will increasingly be critical as networks become larger and far more complex.

This work gives some important groundwork for future developments in IoT routing. Here, the contributions and recommendations to the researchers, network engineers, and system architects on developing the next generation of IoT networking solutions can be extremely useful. As the IoT landscape continues to evolve, the principles and approaches developed and described in this study can be useful guiding principles to implement even more efficient, secure, and resilient routing protocols.

Funding

This research received no external funding.

Data Availability

The data used and analyzed during the current study are available from the corresponding Author upon reasonable request.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Karunkuzhali, D., Meenakshi, B., & Lingam, K. (2024). A QoS-aware routing approach for Internet of Things-enabled wireless sensor networks in smart cities. *Multimedia tools and applications*, 1–27. https://doi.org/10.1007/s11042-024-18125-y

[2] Lai, R., Zhang, B., Gong, G., Yuan, H., Yang, J., Zhang, J., & Zhou, M. (2024). Energy-efficient scheduling in UAV-assisted hierarchical wireless sensor networks. *IEEE internet of things journal*. https://doi.org/10.1109/JIOT.2024.3369722

[3] Barnwal, S. K., & Prakash, A. (2024). Comparative analysis of LEACH network routing protocol in wireless sensor networks: A survey. *Wireless personal communications*, *135*(2), 697–726. https://doi.org/10.1007/s11277-024-11049-8

[4] Najm, I. A., Hamoud, A. K., Lloret, J., & Bosch, I. (2019). Machine learning prediction approach to enhance congestion control in 5G IoT environment. *Electronics*, *8*(6), 607. https://doi.org/10.3390/electronics8060607

[5] Köhler, S., & Binzenhöfer, A. (2003). MPLS traffic engineering in OSPF networks—a combined approach. In *Teletraffic science and engineering* (Vol. 5, pp. 21–30). Elsevier. https://doi.org/10.1016/S1388-3437(03)80147-6

[6] Yadav, R., & Kumar, V. (2024). A systematic review paper on energy-efficient routing protocols in internet of things. *IETE journal of research*, *70*(5), 4721–4743. https://www.tandfonline.com/doi/abs/10.1080/03772063.2023.2230169

[7] Verma, S. (2022). Energy-efficient routing paradigm for resource-constrained internet of things-based cognitive smart city. *Expert systems*, *39*(5), e12905. https://doi.org/10.1111/exsy.12905

[8] El-Mougy, A., Al-Shiab, I., & Ibnkahla, M. (2019). Scalable personalized IoT networks. *Proceedings of the ieee*, *107*(4), 695–710. https://doi.org/10.1109/JPROC.2019.2894515

[9] Abdulghani, R. M., Alrehili, M. M., Almuhanna, A. A., & Alhazmi, O. H. (2020). Vulnerabilities and security issues in IoT protocols. *2020 First international conference of smart systems and emerging technologies (SMARTTECH)* (pp. 7-12). IEEE. https://doi.org/10.1109/SMART-TECH49988.2020.00020

[10] Kasturi, S. B., Reddy, P. V., VenkataNagendra, K., Madhavi, M. R., & Jha, S. K. (2022). An improved energy efficient solution for routing in IoT. *Journal of pharmaceutical negative results*, *13*(6), 1683–1691. https://www.academia.edu/download/109280495

[11] Tang, F., Mao, B., Kato, N., & Gui, G. (2021). Comprehensive survey on machine learning in vehicular network: Technology, applications and challenges. *IEEE communications surveys & tutorials*, *23*(3), 2027–2057. https://doi.org/10.1109/COMST.2021.3089688

[12] Bekal, P., Kumar, P., Mane, P. R., & Prabhu, G. (2024). A comprehensive review of energy efficient routing protocols for query driven wireless sensor networks. *F1000Research*, *12*, 644. https://doi.org/10.12688/f1000research.133874.3

[13] Mohapatra, H., & Rath, A. K. (2020). Survey on fault tolerance-based clustering evolution in WSN. *IET networks*, *9*(4), 145–155. https://doi.org/10.1049/iet-net.2019.0155

[14] Mohapatra, H., & Rath, A. K. (2019). Detection and avoidance of water loss through municipality taps in India by using smart taps and ICT. *IET wireless sensor systems*, *9*(6), 447–457. https://doi.org/10.1049/iet-wss.2019.0081

[15] Kamel, H., & Abed, A. A. (2024). Blockchain-enhanced secure routing protocols for vehicular ad hoc networks: a comprehensive review. *2024 IEEE 7th international conference on automation, electronics and electrical engineering (AUTEEE)* (pp. 624-630). IEEE. https://doi.org/10.1109/AUTEEE62881.2024.10869679

[16] Al-Janabi, T. A., & Al-Raweshidy, H. S. (2018). A centralized routing protocol with a scheduled mobile sink-based AI for large scale I-IoT. *IEEE sensors journal*, *18*(24), 10248–10261. https://doi.org/10.1109/JSEN.2018.2873681

[17] Raj, J. S., Basar, A., & others. (2019). QoS optimization of energy efficient routing in IoT wireless sensor networks. *Journal of ismac*, *1*(01), 12–23. https://www.academia.edu/download/76164096/02.pdf

[18] Natarajan, Y., Srihari, K., Dhiman, G., Chandragandhi, S., Gheisari, M., Liu, Y., … & Alharbi, H. F. (2022). An IoT and machine learning-based routing protocol for reconfigurable engineering application. *IET communications*, *16*(5), 464–475. https://doi.org/10.1049/cmu2.12266

[19] Esenogho, E., Djouani, K., & Kurien, A. M. (2022). Integrating artificial intelligence internet of things and 5G for next-generation smartgrid: A survey of trends challenges and prospect. *IEEE access*, *10*, 4794–4831. https://doi.org/10.1109/ACCESS.2022.3140595

[20] Shafique, K., Khawaja, B. A., Sabir, F., Qazi, S., & Mustaqim, M. (2020). Internet of things (IoT) for next-generation smart systems: A review of current challenges, future trends and prospects for emerging 5G-IoT scenarios. *IEEE access*, *8*, 23022–23040. https://doi.org/10.1109/ACCESS.2020.2970118