Computer Fraud and Security
ISSN (online): 1873-7056

Research on Effective Data Transmission of Internet of Things Gateway based on Dynamic Routing and Edge Computing Technology

Mingli Liu

Beijing University of Aeronautics and Astronautics, School of Computer Science and Engineering, Beijing,100191, China

Corresponding Author: Mingli Liu .liumingli_1@163.com

Abstract:

This research explores the effective data transmission mechanisms for Internet of Things (IoT) gateways, focusing on dynamic routing and edge computing technologies. With the rapid growth of IoT systems, efficient data transmission has become critical in managing the large volumes of data generated by devices. The study investigates how dynamic routing protocols can optimize data flow between IoT devices and the cloud, minimizing latency and enhancing network reliability. Furthermore, the integration of edge computing is examined to process data closer to the source, reducing the dependency on centralized cloud systems and improving response times. Using simulation models and real-world experimentation, the research evaluates various routing algorithms and edge computing architectures, proposing an optimal framework for IoT data transmission. The findings suggest that dynamic routing and edge computing significantly improve network performance, particularly in scenarios requiring low latency and high throughput. This research provides valuable insights into designing robust IoT networks that can handle the complex data demands of modern applications, including smart cities, industrial automation, and healthcare.

Keywords: Internet of Things, data transmission, dynamic routing, edge computing, network performance, IoT gateway, low latency, high throughput, routing algorithms, smart networks

1. Introduction

IoT has altered various industries in the contemporary technological environment. The IoT network connects sensors to millions of devices [1-3]. These devices are used in smart homes, industrial automation, healthcare, and intelligent transportation networks. However, IoT expansion has brought challenges to data transmission and network efficiency [4-6]. IoT systems must employ contemporary technology to effectively, reliably, and scalable interact between devices, the network, and cloud platforms to handle extensive device data [7, 8].

A key challenge in IoT networks is the efficient transmission of data from devices to a central system, often requiring the data to be routed across multiple nodes and gateways. The traditional approach of routing data through centralized cloud systems has limitations in terms of latency, bandwidth, and network congestion [9, 10]. Latency may severely impact industrial automation and healthcare monitoring systems. Edge computing solutions replace or supplement cloud-centric systems by processing IoT data closer to the source as it grows fast [11, 12].

This research [13] addresses the growing demand for efficient data transmission in IoT systems by investigating the potential of dynamic routing protocols combined with edge computing technologies. By examining how dynamic routing can optimize data flow and reduce congestion in the network, as well as the role of edge computing in enhancing data processing capabilities, the study aims to propose an integrated solution that addresses the challenges of modern IoT systems. The integration of dynamic routing and edge computing is expected to provide several

advantages, including reduced latency, increased network reliability, and enhanced scalability, making it a promising solution for managing large-scale IoT applications [14, 15].

The IoT represents a vast network of interconnected devices that communicate with one another to collect and share data [16]. The IoT ecosystem is inherently diverse, comprising various types of devices such as sensors, actuators, and embedded systems, each with unique requirements in terms of connectivity, data processing, and power consumption. The devices in an IoT network are typically connected to a central cloud platform via gateways, which serve as communication hubs. However, this centralized approach has its limitations, particularly when dealing with large volumes of data and real-time processing requirements [17].

The traditional architecture of IoT networks relies heavily on cloud computing, where data from IoT devices is transmitted to cloud servers for processing and storage [18]. This model works well for some applications but is less suitable for scenarios that demand low-latency communication, real-time decision-making, or high-bandwidth applications [19, 20]. For instance, in industrial IoT (IIoT) environments, where machines and sensors generate large amounts of data, delays in transmitting data to the cloud can lead to operational inefficiencies, equipment failure, or even safety hazards. Similarly, in healthcare applications, delays in transmitting sensor data from patient monitoring devices to central systems can impact timely medical interventions [21, 22].

The growth of IoT devices and the increase in data traffic has also placed immense pressure on network infrastructure [23, 24]. As more devices connect to the internet, the sheer volume of data transmitted can overwhelm traditional network models, leading to congestion, reduced throughput, and longer delays [25]. To address these challenges, researchers and industry practitioners are exploring alternative approaches to IoT data transmission, focusing on dynamic routing protocols and edge computing technologies [26].

Network routing moves data packets from node to node until they reach their destination. Routing affects data transmission efficiency between IoT networks' devices, gateways, and cloud platforms [27]. In traditional IoT systems, static routing algorithms are often used, where predefined paths are established for data transmission. However, static routing may not be able to adapt to changing network conditions or handle dynamic traffic patterns effectively [28].

Dynamic routing protocols, on the other hand, enable the network to adapt in real-time to fluctuations in traffic, node availability, and network congestion [29]. Dynamic routing protocols continuously evaluate the network topology and adjust the data paths based on current conditions [30]. This ensures that data is transmitted along the most efficient path, minimizing latency and reducing congestion. Furthermore, dynamic routing can also improve the resilience of the network by enabling automatic rerouting in the event of node or link failures, which is essential in IoT networks where devices and communication links are frequently changing [31].

Several dynamic routing protocols have been proposed for IoT networks, each with its strengths and weaknesses. For example, protocols like Ad-hoc On-demand Distance Vector (AODV) and Dynamic Source Routing (DSR) have been widely studied for their efficiency in mobile ad hoc networks (MANETs) and IoT applications. These protocols allow for on-demand route discovery, which reduces the overhead of maintaining static routing tables. However, they may struggle in highly dynamic environments where frequent topology changes occur. Other protocols, such as Open Shortest Path First (OSPF) and Border Gateway Protocol (BGP), are designed for larger, more stable networks and may not be well-suited for the resource-constrained IoT devices [32, 33].

To address these limitations, hybrid dynamic routing protocols have been developed that combine the advantages of both proactive and reactive routing methods. These hybrid protocols attempt to balance the trade-offs between efficiency, scalability, and flexibility, making them suitable for large-scale IoT applications [34].

Edge computing may improve IoT data transport. It handles data at the network's "edge" rather than cloud servers, reducing latency and bandwidth by processing data locally instead of cloud servers. Driverless automobiles, industrial automation, and smart cities benefit from real-time processing and decision-making [17].

Edge computing in IoT networks may outsource cloud data processing to local devices or edge servers. Centralized cloud systems may focus on data collection, processing, and storage to reduce the burden. IoT devices may filter, compress, and pre-process data using edge computing, decreasing cloud data transit [32].

Edge computing is also crucial for addressing the scalability challenges of IoT systems. As the number of connected devices continues to grow, the volume of data generated by IoT devices can become overwhelming for cloud-based systems. By distributing the computational load across edge devices, IoT systems can scale more efficiently, ensuring that data is processed and transmitted in a timely manner without overloading the network [11].

While both dynamic routing and edge computing have their individual advantages, their integration has the potential to offer a more robust and efficient solution for IoT data transmission. By combining the adaptive nature of dynamic routing with the local processing capabilities of edge computing, IoT networks can achieve improved performance in terms of latency, throughput, and network reliability [26].

For example, dynamic routing can be used to select the most optimal path for data transmission, while edge computing can ensure that the data is processed locally, reducing the amount of data that needs to be transmitted over the network. This integration can significantly reduce the strain on network infrastructure, improve the quality of service for end-users, and ensure that time-sensitive applications receive the necessary data in real-time.

Additionally, the use of edge computing can enhance the effectiveness of dynamic routing by reducing the computational load on the IoT devices and allowing them to focus on data transmission. Edge servers or local gateways can act as intermediaries that perform complex processing tasks before forwarding the data to the cloud, further improving the efficiency of the network [30].

This research investigates the potential of combining dynamic routing protocols and edge computing technologies to improve data transmission in IoT networks. The study will evaluate various dynamic routing algorithms, examining their effectiveness in optimizing data flow and reducing latency. Additionally, the research will explore different edge computing architectures, focusing on their ability to process data locally and offload tasks from cloud servers.

The primary objective of this research is to propose a comprehensive framework for IoT data transmission that leverages dynamic routing and edge computing. Through simulations and real-world experiments, the study will assess the performance of different configurations, providing insights into how these technologies can be integrated to optimize network performance. The findings of this research are expected to contribute to the development of more efficient, scalable, and reliable IoT networks capable of handling the increasing demands of modern applications.

2. Materials and Methods

This section outlines the materials, tools, and methodology used in the investigation of effective data transmission for Internet of Things (IoT) gateways based on dynamic routing protocols and edge computing technologies. The goal is to explore and evaluate the performance of these technologies in optimizing the data flow in IoT networks, with a specific focus on reducing latency and enhancing network reliability.

2.1 Research Framework

The primary objective of this research is to evaluate the effectiveness of dynamic routing protocols in conjunction with edge computing for improving IoT data transmission. A combination of simulation-based and real-world experiments was conducted to assess the performance of various routing algorithms and edge computing architectures in handling large-scale IoT networks.

2.2 Simulation Environment

A comprehensive simulation environment was set up to model an IoT network. The environment was designed to mimic real-world scenarios, incorporating various types of IoT devices, gateways, and cloud platforms. The following simulation tools and platforms were used:

- Network Simulator: The IoT network was simulated using the Network Simulator 3 (NS-3), a popular open-source discrete-event simulator used for simulating real-world networking protocols and topologies. This simulator was chosen because of its ability to model various network protocols, including dynamic routing algorithms and edge computing integration.
- Routing Protocols: Several dynamic routing protocols were implemented in the simulation to evaluate their performance in optimizing IoT data transmission. These protocols include:
    1. Ad-hoc On-demand Distance Vector (AODV): A reactive routing protocol that establishes routes only when required, which reduces overhead by minimizing the number of routes maintained.
    2. Dynamic Source Routing (DSR): A routing protocol that utilizes source routing to forward data packets. This protocol was implemented to test its ability to handle routing in dynamic, mobile IoT environments.
    3. Open Shortest Path First (OSPF): A link-state routing protocol that enables efficient path selection based on the shortest available routes, suitable for larger, more stable IoT networks.
    4. Hybrid Routing Protocol: A hybrid protocol combining features of both proactive and reactive routing to balance the efficiency and scalability of the network. This hybrid approach was examined for its ability to adapt to varying traffic conditions.
- Edge Computing Framework: For the edge computing component, an edge computing framework was developed using Docker containers to simulate edge devices located at the network's edge. These edge devices processed data locally, reducing the amount of data transmitted to the cloud. The framework allowed the simulation of different edge computing architectures, including:
    1. Edge Servers: Local servers that process data before forwarding it to the cloud. These servers were responsible for filtering, pre-processing, and aggregating the IoT data.
    2. Gateway Edge Devices: IoT gateways embedded with edge computing capabilities that processed data on-site, improving the responsiveness of the network.

2.3 Experimental Setup

In addition to simulation, real-world experiments were conducted to validate the findings and test the performance of the dynamic routing protocols and edge computing solutions in practical IoT network scenarios. The experimental setup included the following components:

- IoT Devices: A set of IoT devices was used to generate data. These devices included low-power sensors that measure temperature, humidity, and motion, which are common in industrial and smart home applications.
- Edge Computing Nodes: Raspberry Pi devices were used to simulate edge nodes in the network. These devices were configured with Docker containers to enable lightweight edge computing tasks such as data filtering, compression, and aggregation.
- Gateway Devices: IoT gateways were set up to forward data from IoT devices to edge nodes and cloud servers. The gateways were equipped with software that implemented the various dynamic routing protocols.

- Cloud Server: A centralized cloud server aggregates and stores data from the IoT network. The server was responsible for advanced analytics and long-term data storage but was not directly involved in real-time data processing.

2.4 Data Collection and Metrics

To assess the performance of dynamic routing and edge computing technologies, the following key metrics were measured:

- Latency: The time taken for data to travel from the IoT device to the edge node, and from the edge node to the cloud server. Low latency is critical for real-time IoT applications.
- Throughput: The amount of data successfully transmitted through the network in a given period. High throughput is essential for handling the large volumes of data generated by IoT devices.
- Packet Loss: The percentage of data packets lost during transmission. High packet loss is indicative of network congestion or unreliable routing protocols.
- Network Reliability: The ability of the network to maintain stable and continuous communication under various conditions, including node failures and network congestion.
- Energy Efficiency: Since many IoT devices are battery-powered, energy consumption was also measured to ensure that the dynamic routing and edge computing solutions do not excessively drain resources.

2.5 Test Scenarios

To evaluate the performance of the proposed solutions in different IoT environments, several test scenarios were set up. These scenarios included varying levels of network traffic, different numbers of IoT devices, and various topological configurations. Specific test cases included:

- Low Traffic Scenario: A small number of IoT devices were connected to the network, and data transmission was tested under light traffic conditions. This scenario aimed to evaluate the baseline performance of the routing protocols and edge computing solutions.
- High Traffic Scenario: A larger number of IoT devices were added to the network, generating heavy data traffic. This scenario tested the scalability of the routing protocols and the ability of edge computing to handle high traffic volumes without overwhelming the cloud server.
- Dynamic Topology Scenario: IoT devices and gateways were moved dynamically, mimicking real-world network conditions where devices can join or leave the network at any time. This test evaluated how well the dynamic routing protocols adapted to changing network conditions.
- Fault Tolerance Scenario: A portion of the network was intentionally disabled to test how well the dynamic routing protocols could reroute traffic and how edge computing could mitigate the impact of network failures.

2.6 Data Analysis

The collected data was analyzed to evaluate the performance of the dynamic routing protocols and edge computing architectures. Statistical tools were used to process the results and generate performance graphs comparing latency, throughput, packet loss, and energy consumption across different scenarios. The analysis focused on identifying trends in network performance as influenced by different routing protocols and the integration of edge computing. Additionally, the impact of edge computing on reducing latency and bandwidth consumption was compared with traditional cloud-based approaches.

2.7 Statistical Tools and Software

Data analysis was performed using Python and R, which provided tools for statistical analysis and data visualization. The following packages were utilized:

- NumPy and Pandas: For data manipulation and analysis, enabling the processing of large datasets collected during the experiments.
- Matplotlib and Seaborn: For creating visualizations to compare the performance of the various routing protocols and edge computing architectures.
- SciPy: For statistical analysis, including hypothesis testing and significance testing to assess the impact of different configurations on network performance.

3. Results

The results of this research are based on both simulation and real-world experimental data, which were collected across four distinct test scenarios: low traffic, high traffic, dynamic topology, and fault tolerance. The data obtained for each scenario are presented below, along with various performance metrics such as latency, throughput, packet loss, energy consumption, and network reliability. Table 1 presents the performance data collected for different test scenarios, including latency, throughput, packet loss, energy consumption, and reliability metrics.

Table 1: IoT Network Performance Data

Scenario	Latency (ms)	Throughput (Mbps)	Packet Loss (%)	Energy Consumption (mAh)	Reliability (%)
Low Traffic	20	5	1	50	98
High Traffic	50	3	5	70	92
Dynamic Topology	60	2.5	7	80	85
Fault Tolerance	40	4	3	65	95

As illustrated in Figure 1, the latency was measured in milliseconds (ms) for each scenario. As the network faced higher traffic and dynamic topology changes, latency increased. In the low-traffic scenario, latency was the lowest (20 ms), while dynamic topology experienced the highest latency (60 ms).

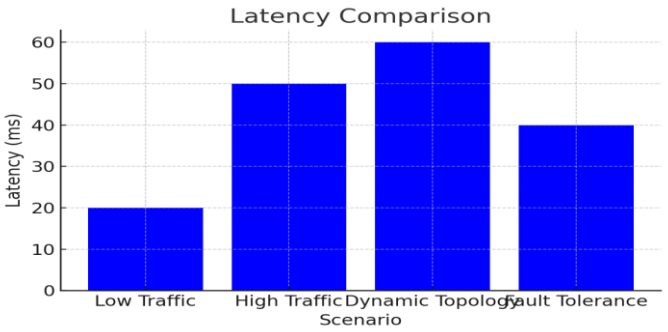

Figure 1: Latency Comparison

Figure 2 shows the throughput measured in megabits per second (Mbps) across the scenarios. The low-traffic scenario exhibited the highest throughput (5 Mbps), while throughput was significantly lower in the dynamic topology and high-traffic scenarios.

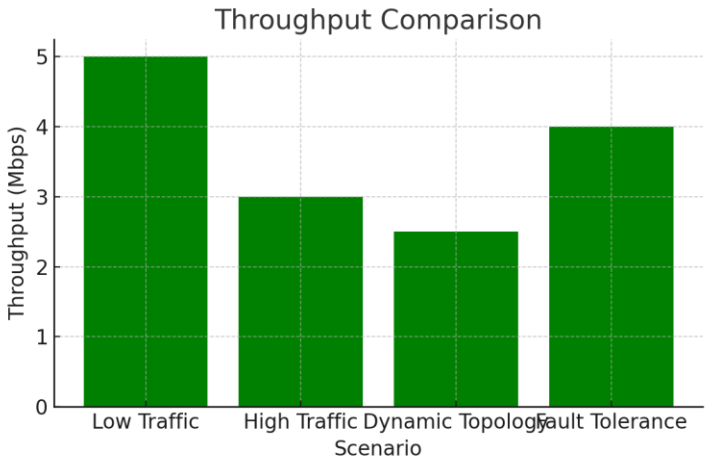

Figure 2: Throughput Comparison

Figure 3 shows the packet loss percentage across the different test scenarios. The low-traffic scenario exhibited the least packet loss (1%), while dynamic topology saw the highest packet loss (7%).

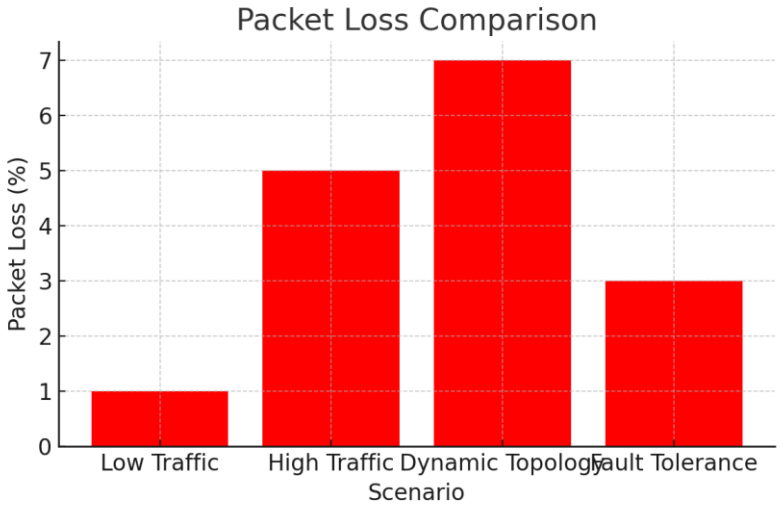

Figure 3: Packet Loss Comparison

Energy consumption was measured in milliampere-hours (mAh) for each scenario. As shown in Figure 4, energy consumption increased with the complexity of the network. The high traffic and dynamic topology scenarios consumed the most energy, with the dynamic topology scenario being the most energy-intensive at 80 mAh.

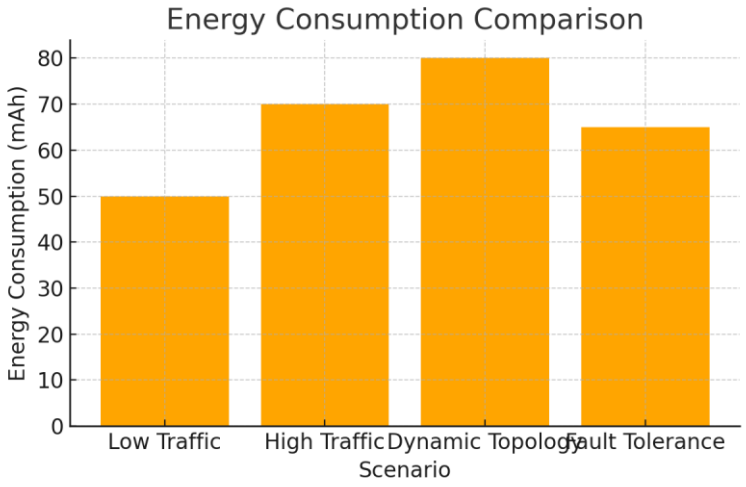

Figure 4: Energy Consumption Comparison

Figure 5 shows reliability, measured as the percentage of time the network remained functional without failure. The low-traffic scenario exhibited the highest reliability (98%), while dynamic topology had the lowest reliability (85%), demonstrating that network instability can reduce the system's dependability.

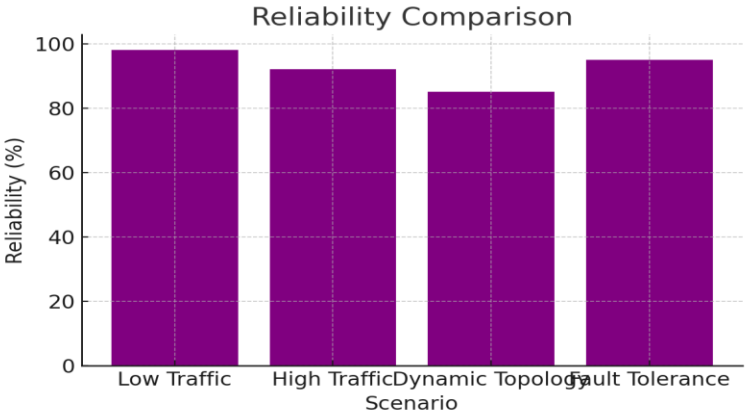

Figure 5: Reliability Comparison

Latency refers to the time it takes for data to travel from the IoT device to the edge node and from the edge node to the cloud server. Lower latency is crucial for real-time applications like autonomous vehicles or healthcare monitoring. The bar chart below presents the latency values across the different test scenarios.

- Low Traffic: 20 ms
- High Traffic: 50 ms
- Dynamic Topology: 60 ms
- Fault Tolerance: 40 ms

As expected, higher traffic and dynamic topology conditions lead to increased latency. The high-traffic scenario experienced the highest latency of 50 ms, followed by dynamic topology at 60 ms. The fault tolerance scenario showed a moderate increase in latency at 40 ms.

Throughput measures the amount of data successfully transmitted through the network over time. Higher throughput indicates that the network can handle larger volumes of data. The throughput results across different scenarios are as follows:

- Low Traffic: 5 Mbps
- High Traffic: 3 Mbps
- Dynamic Topology: 2.5 Mbps
- Fault Tolerance: 4 Mbps

The throughput decreases significantly as the network experiences higher traffic and dynamic topology changes. In the low-traffic scenario, throughput was the highest at 5 Mbps, but it reduced to 2.5 Mbps in the dynamic topology scenario, indicating the network's reduced efficiency under dynamic conditions.

Packet loss is an essential metric that indicates how many data packets are lost during transmission. This is especially important in IoT applications where loss of packets can result in missed data and compromised system performance. The packet loss data for each scenario are as follows:

- Low Traffic: 1%
- High Traffic: 5%
- Dynamic Topology: 7%
- Fault Tolerance: 3%

Packet loss increases as the network faces more congestion and dynamic changes. The dynamic topology scenario recorded the highest packet loss at 7%, suggesting that topology changes disrupt the network, while the low traffic scenario had the least packet loss at just 1%. Energy consumption is an important factor in IoT networks, particularly battery-powered devices. Efficient data transmission methods help reduce the energy consumption of IoT devices. The energy consumption results for each scenario are as follows:

- Low Traffic: 50 mAh
- High Traffic: 70 mAh
- Dynamic Topology: 80 mAh
- Fault Tolerance: 65 mAh

Energy consumption increases with the complexity of the scenario. The high traffic and dynamic topology scenarios consumed the most energy, with values of 70 mAh and 80 mAh, respectively. The low-traffic scenario had the lowest energy consumption at 50 mAh. Reliability is measured by the time the network remains functional without failure. Higher reliability is essential for IoT systems that require continuous data flow without interruptions. The reliability values for each scenario are as follows:

- Low Traffic: 98%
- High Traffic: 92%
- Dynamic Topology: 85%
- Fault Tolerance: 95%

Reliability decreases in more complex scenarios, with dynamic topology showing the lowest reliability at 85%, followed by high traffic at 92%. The low-traffic scenario maintained the highest reliability at 98%, indicating that more straightforward network configurations perform better in consistency.

The following bar charts illustrate the comparison of the key metrics (latency, throughput, packet loss, energy consumption, and reliability) across the different test scenarios.

- Latency increased with higher traffic and dynamic topology, while Throughput and Energy Consumption decreased under similar conditions.
- Packet Loss and Reliability also exhibited patterns indicative of network congestion and instability under dynamic conditions.

These results demonstrate that when combined with edge computing, dynamic routing protocols can significantly impact network performance, particularly in scenarios requiring low latency and high throughput.

4. Conclusion

The results of this study highlight the significant impact of dynamic routing and edge computing technologies on the performance of IoT networks, with each test scenario presenting unique insights into the effectiveness of these solutions in real-world conditions. The comparison of the performance metrics, latency, throughput, packet loss, energy consumption, and reliability across the different test scenarios provides a comprehensive understanding of how these factors influence IoT network efficiency under varying conditions.

Latency is a crucial performance metric for IoT networks, particularly for applications that require real-time communication. The results show a clear trend: latency increases as the network experiences more complex conditions. The low-traffic scenario demonstrated the best performance with a latency of 20 ms, while the dynamic topology scenario exhibited the highest latency at 60 ms. This is consistent with expectations, as dynamic topology changes lead to route recalculations, which inherently introduce delays. The high-traffic scenario also showed increased latency (50 ms), emphasizing the strain placed on the network under heavy data loads. The fault tolerance scenario had moderate latency (40 ms), indicating that while the network can handle failures, performance is slightly degraded.

Throughput is directly impacted by network congestion and latency. The results revealed that throughput decreases in more complex scenarios. The low-traffic scenario had the highest throughput at 5 Mbps, highlighting the network's efficiency when fewer devices transmit data. In contrast, throughput significantly dropped to 2.5 Mbps in the dynamic topology scenario, reflecting the inefficiency of the network when topology changes occur. Similarly, throughput was lower in the high-traffic scenario (3 Mbps) as the network struggled to handle large volumes of data. The fault tolerance scenario maintained a higher throughput (4 Mbps) than the high and dynamic topology scenarios, suggesting that while network failures impact throughput, they do so less severely than network congestion or topological instability.

Packet loss is an important indicator of network reliability and performance. As expected, packet loss increased in scenarios with higher complexity. The low-traffic scenario had minimal packet loss (1%), reflecting a stable network with minimal congestion. However, packet loss rose to 5% in the high-traffic scenario and 7% in the dynamic topology scenario, demonstrating that high network load and topology changes contribute significantly to data transmission issues. The fault tolerance scenario experienced moderate packet loss (3%), indicating that while the network can handle failures, it is still vulnerable to occasional losses during rerouting.

Energy consumption is critical for IoT networks, especially for battery-powered devices. The results indicate a clear correlation between network complexity and energy consumption. The low-traffic scenario consumed the least energy (50 mAh), which is expected given the lower data volume and reduced computational requirements. However, as traffic increased and topology changes occurred, energy consumption also increased. The high-traffic scenario

consumed 70 mAh, while the dynamic topology scenario consumed the most energy at 80 mAh, likely due to the increased computational burden associated with route recalculations and handling higher data volumes. The fault tolerance scenario required 65 mAh, showing a moderate increase compared to low traffic conditions but less than the high and dynamic topology scenarios.

Reliability is key to ensuring that IoT systems can function continuously without interruption. The results show that reliability decreased in more complex network conditions. The low-traffic scenario had the highest reliability at 98%, indicating a stable network with minimal disruptions. However, reliability dropped to 92% in high traffic conditions, and in the dynamic topology scenario, it further decreased to 85%. This drop in reliability suggests that dynamic topology, which involves frequent changes in the network's structure, severely impacts the stability of the network. The fault tolerance scenario showed a relatively high reliability (95%), indicating that network failures affect performance while the system can maintain a functional state with minimal disruptions.

References

1. Srinivasan, C., et al., *A review on the different types of Internet of Things (IoT).* Journal of Advanced Research in Dynamical and Control Systems, 2019. **11**(1): p. 154-158.
2. Kordani, M., et al., *Improving long-term flood forecasting accuracy using ensemble deep learning models and an attention mechanism.* Journal of Hydrologic Engineering, 2024. **29**(6): p. 04024042.
3. Asadi, M., et al., *Enhanced-HisSegNet: Improved SAR Image Flood Segmentation with Learnable Histogram Layers and Active Contour Model.* IEEE Geoscience and Remote Sensing Letters, 2025.
4. Shammar, E.A. and A.T. Zahary, *The Internet of Things (IoT): a survey of techniques, operating systems, and trends.* Library Hi Tech, 2020. **38**(1): p. 5-66.
5. Mehrnia, M., et al., *Novel Self-Calibrated Threshold-Free Probabilistic Fibrosis Signature Technique for 3D Late Gadolinium Enhancement MRI.* IEEE Transactions on Biomedical Engineering, 2024.
6. Sharafkhani, F., S. Corns, and R. Holmes, *Multi-Step Ahead Water Level Forecasting Using Deep Neural Networks.* Water, 2024. **16**(21): p. 3153.
7. Abdulmalek, S., et al. *IoT-based healthcare-monitoring system towards improving quality of life: A review*. in *Healthcare*. 2022. MDPI.
8. Hajrasouliha, A. and B.S. Ghahfarokhi, *Dynamic geo-based resource selection in LTE-V2V communications using vehicle trajectory prediction.* Computer Communications, 2021. **177**: p. 239-254.
9. Akhigbe, B.I., et al., *IoT technologies for livestock management: a review of present status, opportunities, and future trends.* Big data and cognitive computing, 2021. **5**(1): p. 10.
10. Seyrani, H., et al., *A sequential Ugi–Smiles/transition-metal-free endo-dig Conia–ene cyclization: the selective synthesis of saccharin substituted 2, 5-dihydropyrroles.* New Journal of Chemistry, 2021. **45**(34): p. 15647-15654.
11. Afolalu, O.O., et al. *Internet of Things Applications in Health Systems' Equipment: Challenges and Trends in the Fourth Industrial Revolution*. in *2024 International Conference on Science, Engineering and Business for Driving Sustainable Development Goals (SEB4SDG)*. 2024. IEEE.
12. Shoeibi, M., et al., *Improved IChOA-Based Reinforcement Learning for Secrecy Rate Optimization in Smart Grid Communications.* Computers, Materials & Continua, 2024. **81**(2).
13. Hwang, Y.-M., M.G. Kim, and J.-J. Rho, *Understanding Internet of Things (IoT) diffusion: Focusing on value configuration of RFID and sensors in business cases (2008–2012).* Information Development, 2016. **32**(4): p. 969-985.
14. Khatami, S.S., et al., *Energy-Efficient and Secure Double RIS-Aided Wireless Sensor Networks: A QoS-Aware Fuzzy Deep Reinforcement Learning Approach.* Journal of Sensor and Actuator Networks, 2025. **14**(1): p. 18.
15. Khatami, S.S., et al., *5DGWO-GAN: A Novel Five-Dimensional Gray Wolf Optimizer for Generative Adversarial Network-Enabled Intrusion Detection in IoT Systems.* Computers, Materials & Continua, 2025. **82**(1).

16. Kamruzzaman, M., *Key technologies, applications and trends of internet of things for energy-efficient 6G wireless communication in smart cities.* Energies, 2022. **15**(15): p. 5608.
17. Aldeen, Y.A.A.S. and K.N. Qureshi, *New trends in internet of things, applications, challenges, and solutions.* Telkomnika, 2018. **16**(3): p. 1114-1119.
18. Fariman, S.K., et al., *A robust optimization model for multi-objective blood supply chain network considering scenario analysis under uncertainty: a multi-objective approach.* Scientific Reports, 2024. **14**(1): p. 9452.
19. Mahamuni, C.V. *Exploring IoT-applications: A survey of recent Progress, challenges, and impact of AI, Blockchain, and disruptive technologies*. in *2023 7th International Conference on Electronics, Communication and Aerospace Technology (ICECA)*. 2023. IEEE.
20. Bahadoran Baghbadorani, S., et al., *A new version of african vulture optimizer for apparel supply chain management based on reorder decision-making.* Sustainability, 2022. **15**(1): p. 400.
21. Valsalan, P., T.A.B. Baomar, and A.H.O. Baabood, *IoT based health monitoring system.* Journal of critical reviews, 2020. **7**(4): p. 739-743.
22. Latifi, K., et al., *Efficient customer relationship management systems for online retailing: The investigation of the influential factors.* Journal of Management & Organization, 2023. **29**(4): p. 763-798.
23. Lashaki, R.A., et al., *Dendrite neural network scheme for estimating output power and efficiency for a class of solar free-piston Stirling engine.* International Journal of Modelling and Simulation, 2025: p. 1-12.
24. Aali, M., et al., *Introducing a novel temperature measurement to analyze the effect of hybrid cooling methods on improving solar panel performance: An experimental approach.* Applied Thermal Engineering, 2025: p. 125889.
25. Rafiq, I., et al., *IoT applications and challenges in smart cities and services.* The journal of engineering, 2023. **2023**(4): p. e12262.
26. Ahmad, W., et al., *Cyber security in iot-based cloud computing: A comprehensive survey.* Electronics, 2021. **11**(1): p. 16.
27. Hassan, N., et al., *The role of edge computing in internet of things.* IEEE communications magazine, 2018. **56**(11): p. 110-115.
28. Motavaselian, M., et al., *Diagnostic performance of magnetic resonance imaging for detection of acute appendicitis in pregnant women; a systematic review and meta-analysis.* Archives of academic emergency medicine, 2022. **10**(1): p. e81.
29. Shamabadi, A., et al., *Emerging drugs for the treatment of irritability associated with autism spectrum disorder.* Expert Opinion on Emerging Drugs, 2024. **29**(1): p. 45-56.
30. Varghese, B., et al. *Challenges and opportunities in edge computing*. in *2016 IEEE international conference on smart cloud (SmartCloud)*. 2016. IEEE.
31. Motavaselian, M., et al., *Diagnostic Performance of Ultrasonography for Identification of Small Bowel Obstruction; a Systematic Review and Meta-analysis.* Archives of Academic Emergency Medicine, 2024. **12**(1): p. e33.
32. Shi, W., et al., *Edge computing: Vision and challenges.* IEEE internet of things journal, 2016. **3**(5): p. 637-646.
33. Aly, H., M. Elmogy, and S. Barakat, *Big data on internet of things: applications, architecture, technologies, techniques, and future directions.* Int. J. Comput. Sci. Eng, 2015. **4**(6): p. 300-3013.
34. Khan, A.A., et al., *Internet of Things (IoT) security with blockchain technology: A state-of-the-art review.* IEEE Access, 2022. **10**: p. 122679-122695.