Idea: Future Research
Volume 1, Issue 2, July 2023
ISSN 2987-1565 (Online) | ISSN 2987-2715 (Print)
Published by:
Ideas for Future Research and Technology

Performance Analysis of Routing Protocols in IoT-Based Computer Networks

Firta Panjaitan[1], Roma Sinta[2], Juliana Batubara[3]
[1,2,3] Institute of Computer Science (IOCS), Indonesia

Introduction

The Internet of Things (IoT) represents a transformative shift in how devices and systems interact with each other and the environment. In essence, IoT refers to a network of physical objects embedded with sensors, software, and other technologies that allow them to connect to and exchange data over the internet. These devices, or "smart" objects, can range from everyday household items like refrigerators and thermostats to industrial machinery, healthcare equipment, and agricultural systems. The ultimate goal of IoT is to create an interconnected world where data flows seamlessly between devices, enabling them to perform tasks autonomously, improve decision-making, and enhance human experiences(Gubbi et al., 2013).

At the heart of IoT lies the idea of connectivity. Unlike traditional computing devices that require direct human interaction, IoT devices communicate with one another, often without human intervention(Poslad, 2011). This is made possible by the sensors and actuators embedded in the objects, which collect and process data from their surroundings. This data is then transmitted through networks to central systems or cloud platforms for analysis, decision-making, and, in many cases, automation of specific tasks. This capability to gather, process, and act on real-time information makes IoT a powerful tool in a wide array of applications.

One of the most significant applications of IoT is in smart homes, where IoT-enabled devices such as thermostats, lighting systems, security cameras, and appliances are interconnected to create an automated living environment(Abdulraheem et al., 2020). These devices can be controlled remotely via smartphones or other smart devices, providing users with greater convenience, energy efficiency, and security. For example, a smart thermostat can learn a household's temperature preferences and adjust settings automatically to save energy while maintaining comfort.

In healthcare, IoT has revolutionized patient monitoring and medical data management. Devices such as wearable fitness trackers, smartwatches, and connected medical instruments can continuously monitor vital signs like heart rate, blood pressure, and glucose levels(Dias & Paulo Silva Cunha, 2018). This data is sent to healthcare providers in real-time, enabling more proactive and personalized care.

Corresponding Author: Firta Panjaitan (firtapanjaita@gmai.com)

Additionally, IoT technologies support the development of telemedicine systems, where remote consultations and treatments can be provided, reducing the need for in-person visits and improving access to healthcare, particularly in underserved areas.

IoT is also having a profound impact on industrial automation and smart cities. In industrial settings, IoT devices help monitor and manage manufacturing processes, reducing downtime and improving efficiency. Sensors embedded in machinery can detect issues before they lead to failures, allowing for predictive maintenance and reducing operational costs. In smart cities, IoT is used to optimize urban infrastructure and services such as traffic management, waste collection, water supply, and public safety. Smart traffic lights, for example, can adjust their signals in real-time based on traffic flow data, reducing congestion and improving overall transportation efficiency(Aleko & Djahel, 2020).

The success of IoT relies heavily on computer networks, as they form the backbone that enables communication between devices. The architecture of IoT-based computer networks is distinct from traditional computer networks due to the sheer number of devices involved and the unique characteristics of IoT systems. These networks must be highly scalable, capable of handling the large volume of data generated by IoT devices while maintaining reliability and low latency(Gupta et al., 2017). Additionally, energy efficiency is crucial, as many IoT devices are battery-powered and must minimize power consumption.

In IoT networks, communication protocols play a critical role in ensuring that devices can discover one another, transmit data, and perform tasks efficiently. These protocols must be tailored to the specific needs of IoT devices, considering factors such as limited computational resources, variable network topologies, and high levels of data traffic. Specialized IoT protocols, such as MQTT (Message Queuing Telemetry Transport) for lightweight messaging and CoAP (Constrained Application Protocol) for low-power devices, are widely used to address these challenges(Katsikeas et al., 2017).

As IoT networks often consist of a large number of low-power, resource-constrained devices, traditional routing protocols designed for conventional computer networks are not suitable for IoT environments. IoT-based networks have unique characteristics, such as dynamic topologies, varying node mobility, limited battery power, and low computational capabilities(Arshad et al., 2018). These challenges necessitate the development of specialized routing protocols that can efficiently handle data transmission while optimizing resources like energy consumption and bandwidth.

Routing protocols are at the heart of any network, ensuring that data packets are forwarded from the source node to the destination node through optimal paths(Medhi & Ramasamy, 2017). In IoT networks, where nodes can frequently join or leave the network, maintaining an efficient routing protocol is crucial for reliable communication. Routing protocols for IoT must not only consider factors like packet delivery and network throughput but also address critical aspects such as energy efficiency, scalability, and robustness to network changes.

Several routing protocols have been proposed specifically for IoT networks, each with its advantages and limitations. These protocols, such as AODV (Ad hoc On-demand Distance Vector), LEACH (Low Energy Adaptive Clustering Hierarchy), RPL (Routing Protocol for Low-Power and Lossy Networks), and others, aim to address the unique challenges of IoT environments, especially focusing on energy-efficient data transmission. Despite the numerous options available, the choice of an optimal routing protocol depends on various factors, including network size, node density, mobility, and application requirements(Bhushan & Sahoo, 2019).

Given the importance of IoT in various sectors and its growing adoption, evaluating the performance of different routing protocols is critical to improving the efficiency and sustainability of IoT networks. By analyzing performance metrics such as packet delivery ratio, end-to-end delay, energy consumption, and network lifetime, this research aims to provide insights into the effectiveness of different IoT routing protocols and their suitability for specific applications. This evaluation is particularly important as IoT systems expand, requiring scalable, efficient, and secure communication methods to meet the demands of diverse real-world use cases(Asghari et al., 2019). Through a comprehensive performance analysis of IoT routing protocols, this research will contribute to the identification of optimal routing strategies that can enhance the reliability, efficiency, and longevity of IoT networks.

Research Problem Statement

The rapid expansion of the Internet of Things (IoT) has revolutionized the way devices communicate and interact, fostering a new era of smart applications in various sectors, including healthcare, transportation, agriculture, and urban development(Vermesan & Friess, 2014). However, the increasing number of interconnected devices and the dynamic nature of IoT networks present several challenges, particularly in the area of data routing. In IoT systems, routing protocols play a crucial role in ensuring efficient data transmission between devices. The performance of these protocols directly affects the reliability, scalability, energy efficiency, and overall effectiveness of IoT networks(Guleria & Verma, 2019).

One of the core challenges in IoT-based networks is the large scale of devices. As the number of connected devices continues to grow exponentially, traditional routing protocols, designed for stable and low-density networks, struggle to cope with the scale and complexity of modern IoT systems. The increase in the number of devices leads to network congestion, higher energy consumption, increased latency, and potential packet loss, all of which degrade network performance(Haas & Warkhedi, 2001). These issues are particularly critical for IoT applications that require real-time data transfer and low-latency communication, such as in healthcare monitoring, industrial automation, and autonomous vehicles.

Additionally, IoT networks often exhibit dynamic topologies, where devices frequently join or leave the network, and mobility is common, especially in mobile IoT applications like vehicular networks and smart cities. This dynamic behavior complicates the routing process, as the network topology can change unexpectedly, making it difficult to establish and maintain stable routes for data transmission(Paxson, 2006). Traditional routing protocols, such as those used in conventional computer networks, are not well-suited to handle such frequent topology changes, leading to inefficiencies in data delivery and increased overhead in the network.

Furthermore, many IoT devices are resource-constrained, meaning they have limited power, memory, and processing capabilities. Most IoT devices are powered by batteries and must operate under strict energy constraints to ensure long-term functionality. This imposes a significant challenge for routing protocols, as they must minimize energy consumption while maintaining reliable communication. Energy-efficient routing is vital in ensuring that devices do not run out of power prematurely, which could lead to network failures or disruptions in service(Zeadally et al., 2012).

Moreover, the heterogeneity of IoT devices and communication technologies adds an additional layer of complexity. IoT networks often consist of devices with diverse capabilities and different communication standards, such as Wi-Fi, Bluetooth, Zigbee, and cellular networks(Nikoukar et al., 2018). Efficient routing protocols must accommodate this variety, ensuring seamless interoperability across various technologies while maintaining the network's performance. Achieving efficient routing across such a heterogeneous network requires protocols that are flexible and capable of adapting to different communication environments and device capabilities.

The security of IoT networks is another critical concern that directly impacts the routing process. As IoT networks become more pervasive, they become attractive targets for cyber-attacks, such as data interception, unauthorized access, and denial-of-service attacks(Abomhara & Køien, 2015). Routing protocols in IoT networks must, therefore,

incorporate robust security mechanisms to protect the integrity of the data being transmitted, prevent unauthorized access, and ensure the overall security of the network. Failure to address these security issues can lead to severe vulnerabilities and compromise the entire network.

Given these challenges, there is a significant need to develop and evaluate efficient routing protocols specifically designed for IoT networks. These protocols must not only address issues of scalability, energy efficiency, dynamic topologies, and security but also ensure high levels of performance, reliability, and adaptability to meet the diverse requirements of IoT applications. The performance of routing protocols must be assessed across various parameters, including packet delivery ratio, network lifetime, end-to-end delay, energy consumption, and scalability, to determine the most suitable protocols for different IoT use cases.

Therefore, the research problem centers around the question: How can routing protocols be optimized to efficiently handle the large-scale, dynamic, and resource-constrained nature of IoT networks, ensuring reliable communication while minimizing energy consumption and maintaining security? This research aims to explore the performance of different IoT-specific routing protocols, identify their strengths and weaknesses, and propose solutions to improve the routing efficiency in IoT networks, ultimately contributing to the growth and success of IoT applications in various fields.

Novelty of Research

The rapid advancement of the Internet of Things (IoT) has introduced unprecedented opportunities for innovation across various sectors, from healthcare and agriculture to transportation and urban infrastructure. As IoT systems continue to scale, the challenges associated with efficiently managing communication between an ever-increasing number of interconnected devices become more pressing. Despite the significant progress made in IoT technologies, the existing routing protocols designed for such networks remain inadequate in fully addressing the unique complexities of modern IoT environments(Hammoudi et al., 2018). This research aims to contribute novel insights into optimizing routing protocols specifically tailored to the dynamic, large-scale, and resource-constrained nature of IoT networks.

The novelty of this research lies in its focus on evaluating and enhancing routing protocols in IoT networks by taking into account several critical aspects that are often overlooked in traditional network design. The first key contribution is its emphasis on dynamic and scalable routing solutions for IoT networks. While much of the current research has focused on optimizing protocols for small or relatively stable IoT environments, there is limited exploration into how routing protocols can adapt and

scale as networks grow to incorporate millions of devices with fluctuating topologies. This research seeks to develop protocols that not only maintain high performance but can dynamically adapt to the evolving network conditions as devices join, leave, or change positions.

Furthermore, this study introduces the concept of energy-efficient routing with a focus on the energy constraints of IoT devices. Most IoT devices, such as sensors, wearables, and smart home devices, rely on battery power and thus need to minimize energy consumption to ensure long-term operation(Nižetić et al., 2020). Many existing routing protocols, though effective in conventional networks, do not prioritize energy conservation in IoT networks. By integrating energy-efficient mechanisms into the routing protocol design, this research aims to reduce the overall energy consumption of the network, thereby prolonging the lifespan of IoT devices and improving the sustainability of large-scale IoT deployments.

Another novel aspect of this research is its security-driven routing approach. The IoT landscape is increasingly susceptible to security threats, including data breaches, unauthorized access, and denial-of-service attacks(Anisetti et al., 2020). While security is an acknowledged concern in IoT networks, few routing protocols provide robust security measures without compromising performance. This research proposes an innovative approach to embedding security features directly into the routing protocols, ensuring that data integrity, confidentiality, and network resilience are maintained even as devices communicate across potentially insecure channels(Ficco & Palmieri, 2017). The integration of security and routing optimization is crucial in safeguarding the IoT ecosystem from emerging threats while maintaining reliable and efficient communication.

In addition, the heterogeneity of IoT devices presents a significant challenge for routing protocols, as devices may operate using various communication standards and technologies, such as Wi-Fi, Bluetooth, Zigbee, and cellular networks. The novelty of this research lies in its focus on developing adaptable routing protocols that can seamlessly integrate and manage communication between diverse devices and technologies. By considering the multi-technology nature of IoT networks, the study aims to design protocols that ensure interoperability without introducing unnecessary complexity or inefficiencies.

The research also introduces a comprehensive evaluation framework that not only focuses on traditional performance metrics such as packet delivery ratio and network throughput but also emphasizes other critical factors like latency, network lifetime, and scalability in the context of real-world IoT applications. By conducting a multi-

dimensional analysis of routing protocols, this research will provide a more holistic view of the trade-offs involved in routing decisions and offer practical recommendations for optimizing routing strategies tailored to different IoT use cases.

Finally, the research is novel in its holistic approach to IoT network performance, combining the analysis of dynamic topology management, energy efficiency, security, and scalability in one cohesive study. While individual aspects of IoT network performance have been explored in isolation, the interplay between these factors has received limited attention(Atzori et al., 2012). By addressing the challenges of large-scale IoT networks in a unified manner, this research aims to provide valuable insights into the optimal design of routing protocols that balance multiple performance metrics, making it a significant contribution to the field.

Plan for the results and discussion of this research

The results and discussion section of this research will serve as the core analysis of the effectiveness of the proposed IoT-specific routing protocols, focusing on how well they address the challenges posed by large-scale deployments, dynamic topologies, energy constraints, security concerns, and device heterogeneity. This section will provide a comprehensive evaluation of the performance of these protocols, comparing them against existing solutions and discussing the implications of the findings in the context of real-world IoT applications.

To ensure the validity and reliability of the results, the research will begin with a detailed description of the experimental setup, including the simulation environment, tools, and metrics used for evaluation. A variety of IoT scenarios will be created, ranging from small-scale to large-scale networks, with devices representing different types of IoT devices such as sensors, actuators, and smart devices. The experimental conditions will simulate dynamic topologies (e.g., devices frequently joining or leaving the network) and will include different network densities to reflect the real-world complexities of IoT environments.

Performance metrics such as packet delivery ratio, network latency, energy consumption, end-to-end delay, scalability, and packet loss will be collected for each routing protocol evaluated. Additionally, security performance will be assessed by measuring the ability of the protocols to maintain data integrity and prevent unauthorized access or attacks within the IoT network(Frustaci et al., 2017). The results will be presented using graphs, tables, and charts for a clear comparison of performance across the different scenarios and protocols.

One of the key objectives of the research is to compare the newly proposed IoT routing protocols with existing protocols used in IoT networks, such as AODV (Ad hoc On-demand Distance Vector), DSR (Dynamic Source Routing), and LEACH (Low-Energy Adaptive Clustering Hierarchy). The discussion will center around the strengths and weaknesses of each protocol based on the performance data collected.

For instance, the analysis will examine how scalability is handled by the different protocols, particularly as the network size increases. IoT networks often have hundreds or even thousands of devices, so it is essential to assess how well each protocol scales in terms of network overhead, control message exchange, and its ability to maintain low latency and high throughput as the number of devices grows. The energy consumption will also be compared, especially in resource-constrained devices, to determine which protocol optimally reduces power consumption while ensuring reliable communication.

The dynamic nature of IoT networks is another critical factor that will be examined. As devices move or change network statuses (e.g., joining or leaving the network), the routing protocol's ability to adapt will be assessed. The discussion will include a detailed analysis of how each protocol responds to these topology changes, focusing on the routing stability and reaction time to topology fluctuations. Protocols that can quickly adapt to these changes without introducing excessive delays or communication overhead will be highlighted.

Energy efficiency is a major concern for IoT networks, especially for devices operating on limited battery power. The research will explore how different protocols optimize energy consumption during data transmission. Energy-saving mechanisms like sleep modes, data aggregation, and efficient route discovery will be compared. Protocols that incorporate these features will be discussed in terms of their effectiveness in prolonging network lifetime and minimizing energy expenditure for both end devices and intermediary nodes. The results will offer insights into the trade-offs between energy efficiency and network performance, such as latency and throughput, and suggest the most suitable protocols for energy-constrained IoT applications.

As security is paramount in IoT networks, particularly when sensitive data is transmitted, the research will assess the security features integrated into the proposed routing protocols. The discussion will address vulnerabilities in traditional IoT routing protocols and evaluate the effectiveness of the proposed mechanisms in preventing threats such as man-in-the-middle attacks, data interception, and denial-of-service attacks. The ability of the protocols to secure routing paths and prevent unauthorized access to the network will be critically analyzed.

The trade-off between security and performance will also be explored, as security measures can introduce additional overhead that may impact network performance. The discussion will weigh the benefits of robust security against the potential performance losses and provide recommendations for balancing these two aspects in IoT networks.

Another key aspect to be discussed is the scalability of the routing protocols in handling heterogeneous devices operating under different communication technologies (e.g., Wi-Fi, Bluetooth, Zigbee, cellular). The research will examine the ability of each protocol to support multi-technology communication and ensure seamless interoperability among diverse devices. The performance of the routing protocols when applied to heterogeneous networks will be compared, with particular focus on their ability to efficiently route data across different communication mediums without sacrificing performance.

Finally, the discussion will contextualize the findings within the scope of real-world IoT applications. The results will be linked to practical scenarios such as smart cities, healthcare systems, and industrial automation, where the optimal routing of data is critical for ensuring reliable service delivery. The research will provide recommendations for protocol selection based on the specific requirements of these applications, such as low latency in autonomous vehicles, high throughput in industrial automation, or energy efficiency in environmental monitoring systems.

The discussion will conclude with a comprehensive summary of the research findings, emphasizing the contributions of the study in advancing the understanding of IoT routing protocols. Potential future directions for further optimization of routing protocols, especially in light of emerging IoT technologies such as 5G, edge computing, and machine learning, will also be suggested.

References

Abdulraheem, A. S., Salih, A. A., Abdulla, A. I., Sadeeq, M. A., Salim, N. O., Abdullah, H., Khalifa, F. M., & Saeed, R. A. (2020). Home automation system based on IoT. *Technology Reports of Kansai University*, *62*(5), 2453.

Abomhara, M., & Køien, G. M. (2015). Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks. *Journal of Cyber Security and Mobility*, 65–88.

Aleko, D. R., & Djahel, S. (2020). An efficient adaptive traffic light control system for urban road traffic congestion reduction in smart cities. *Information*, *11*(2), 119.

Anisetti, M., Ardagna, C., Cremonini, M., Damiani, E., Sessa, J., & Costa, L. (2020).

Security threat landscape. *White Paper Security Threats*.

Arshad, S., Azam, M. A., Rehmani, M. H., & Loo, J. (2018). Recent advances in information-centric networking-based Internet of Things (ICN-IoT). *IEEE Internet of Things Journal*, *6*(2), 2128–2158.

Asghari, P., Rahmani, A. M., & Javadi, H. H. S. (2019). Internet of Things applications: A systematic review. *Computer Networks*, *148*, 241–261.

Atzori, L., Iera, A., Morabito, G., & Nitti, M. (2012). The social internet of things (siot)–when social networks meet the internet of things: Concept, architecture and network characterization. *Computer Networks*, *56*(16), 3594–3608.

Bhushan, B., & Sahoo, G. (2019). Routing protocols in wireless sensor networks. *Computational Intelligence in Sensor Networks*, 215–248.

Dias, D., & Paulo Silva Cunha, J. (2018). Wearable health devices—vital sign monitoring, systems and technologies. *Sensors*, *18*(8), 2414.

Ficco, M., & Palmieri, F. (2017). *Security and resilience in intelligent data-centric systems and communication networks*. Academic Press.

Frustaci, M., Pace, P., Aloi, G., & Fortino, G. (2017). Evaluating critical security issues of the IoT world: Present and future challenges. *IEEE Internet of Things Journal*, *5*(4), 2483–2495.

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, *29*(7), 1645–1660.

Guleria, K., & Verma, A. K. (2019). Comprehensive review for energy efficient hierarchical routing protocols on wireless sensor networks. *Wireless Networks*, *25*, 1159–1183.

Gupta, A., Christie, R., & Manjula, R. (2017). Scalability in internet of things: features, techniques and research challenges. *Int. J. Comput. Intell. Res*, *13*(7), 1617–1627.

Haas, Z. J., & Warkhedi, A. (2001). The design and performance of Mobile TCP for wireless networks. *Journal of High Speed Networks*, *10*(3), 187–207.

Hammoudi, S., Aliouat, Z., & Harous, S. (2018). Challenges and research directions for Internet of Things. *Telecommunication Systems*, *67*, 367–385.

Katsikeas, S., Fysarakis, K., Miaoudakis, A., Van Bemten, A., Askoxylakis, I., Papaefstathiou, I., & Plemenos, A. (2017). Lightweight & secure industrial IoT communications via the MQ telemetry transport protocol. *2017 IEEE Symposium on Computers and Communications (ISCC)*, 1193–1200.

Medhi, D., & Ramasamy, K. (2017). *Network routing: algorithms, protocols, and architectures*. Morgan kaufmann.

Nikoukar, A., Raza, S., Poole, A., Güneş, M., & Dezfouli, B. (2018). Low-power wireless for the internet of things: Standards and applications. *IEEE Access*, *6*, 67893–67926.

Nižetić, S., Šolić, P., Gonzalez-De, D. L.-I., & Patrono, L. (2020). Internet of Things (IoT):

Opportunities, issues and challenges towards a smart and sustainable future. *Journal of Cleaner Production*, *274*, 122877.

Paxson, V. (2006). End-to-end routing behavior in the internet. *ACM SIGCOMM Computer Communication Review*, *36*(5), 41–56.

Poslad, S. (2011). *Ubiquitous computing: smart devices, environments and interactions*. John Wiley & Sons.

Vermesan, O., & Friess, P. (2014). *Internet of things applications-from research and innovation to market deployment*. Taylor & Francis.

Zeadally, S., Khan, S. U., & Chilamkurti, N. (2012). Energy-efficient networking: past, present, and future. *The Journal of Supercomputing*, *62*, 1093–1118.