Digital Innovations & Contemporary Research in SCIENCE, ENGINEERING & TECHNOLOGY
Vol. 12. No. 4, 2024 Series

Article Citation Format
Fagbote O.O., Adeosun O.O., Ogunbiyi T.O., Olaniran O., Adeniran J.O., Adoyi O.P. & Atiba T.J. (2024): Evaluation of a Fault Tolerant Packet Routing System for Enhanced Network Resilience and Performance. Journal of Digital Innovations & Contemporary Research in Science, Engineering & Technology. Vol. 12, No. 4. Pp 37-44. www.isteams.net/digitaljournal. dx.doi.org/10.22624/AIMS/DIGITAL/V12N4P4

Article Progress Time Stamps
Article Type: Research Article
Manuscript Received: 7th October, 2024
Review Type: Blind Peer
Final Acceptance:22nd December, 2024

Evaluation of a Fault-Tolerant Packet Routing System for Enhanced Network Resilience and Performance

Fagbote O.O*[1], Adeosun O.O[2], Ogunbiyi T.O[3], Olagoke O.V[4], Adeniran J.O[5], Adoyi O.P[6], Atiba T.J[7]
[1,4] Agric. Development & Management Department, Agriculture and Rural Management Training Institute (ARMTI). Ilorin, Kwara State. Nigeria.
[2,7] Department of Computer Science, Ladoke Akintola University of Technology, Oyo State. Nigeria.
[3] Department of Animal Nutrition, University of Ilorin, Ilorin, Kwara State Nigeria.
[5] Department of Computer Science, Osun State University, Osogbo, Osun State. Nigeria.

ABSTRACT

This study evaluates a fault-tolerant packet routing system aimed at enhancing network resilience and performance. As computer networks continue to expand, ensuring reliable and efficient packet delivery has become increasingly critical, particularly in the face of potential network failures. The research involved developing a simulation model and using the Cisco Network Simulator to test the system's ability to maintain network reliability and efficiency under various conditions. Key performance metrics such as packet delivery rate, failover time, and network throughput were evaluated to assess the system's effectiveness. The results demonstrated an average packet delivery rate of 96.4%, with an average failover time of 4 seconds, indicating swift and effective recovery from router failures. Additionally, the network throughput showed variability based on traffic conditions, with an average rate of 5.586 bps. These findings highlight the system's capabilities in handling diverse network scenarios, ensuring continuous data transmission with minimal downtime. This research contributes to the broader field of network engineering by providing valuable insights into the design and implementation of fault-tolerant routing systems, which are essential for maintaining high network performance and reliability.

Keywords: Fault-tolerant, Routing, Network, Performance Metric, Redundancy, Routing methods, data flow

1. INTRODUCTION

Globally, computer networks are the backbone of our digital world in an era where information flows ceaselessly. According to Mills (2017), computer networks are the collection of interconnected and simultaneously autonomous computer systems that share computer resources and communication. However, the importance of computer networks has led to their increase in use of today's communication system that is; it offers data, voice, and video communication, which are the expectations of its users at both ends of the network (Bertsekas and Gallager, 2021).

Beneath the surface of seamless connectivity lies a challenge in ensuring that data packets traverse this vast network landscape reliably and efficiently (Kabashkin, 2023). This challenge has given rise to packet routing. The network relies on routing systems to promptly ensure these packets reach their intended destinations (Hasan et al., 2017). Moreover, managing and evaluating network resources, such as bandwidth and processing power, becomes more intricate as data volumes surge (Bi et al., 2015). Routing systems must allocate these resources wisely to ensure smooth data flow and prioritise vital traffic, a task increasingly challenging with the data deluge. Additionally, ensuring a consistent quality of service for applications like video conferencing and online gaming, which rely on low-latency data delivery, becomes a concern when data volume surges (Elbamby et al., 2018). As data volume increases, the likelihood of packet loss and delays also rises, putting pressure on routing systems to efficiently handle data packets, especially for time-sensitive applications like voice and video communication. Moreover, with a fault-tolerant routing system, the network could swiftly and seamlessly reroute traffic through alternate paths, circumventing the troubled path and ensuring uninterrupted data flow.

According to Dhawan et al. (2022), fault tolerance involves designing routing systems that anticipate and pre-emptively prepare for potential failures. It is about building digital networks that are as resilient as they are efficient. In essence, fault-tolerant routing seeks to provide the best of both network reliability and efficiency. Meanwhile, the modern computer network landscape faces growing challenges such as network congestion, reliability and fault tolerance in maintaining and evaluating robust and efficient packet routing. The need for reliable and efficient packet routing systems remains an ongoing challenge which has led to suboptimal routing decisions, network inefficiencies, and performance bottlenecks.

In light of the increasing demands placed on computer networks, from the exponential growth in data traffic to the increasing number of connected devices, the need to improve routing systems' reliability and efficiency has become more pronounced. Hence, this research aimed to evaluate a fault-tolerant packet routing system using an automatic failover mechanism that optimises network reliability and efficiency in different network scenarios by providing dynamic adaptation to faults and ensuring seamless network performance during unforeseen disruptions, addressing scalability concerns and potential shortcomings in diverse network conditions.

2. LITERATURE REVIEW

The evaluation of a fault-tolerant packet routing system is a critical aspect of network performance, particularly in ensuring reliability and efficiency in the face of failures. This literature review delves into four key areas related to the evaluation of such models: fault-tolerant mechanisms, performance metrics, simulation tools, and network resilience strategies.

2.1 Fault-Tolerant Mechanisms in Packet Routing

Fault-tolerant mechanisms are designed to ensure the continuity of network services despite failures in components such as routers or links. These mechanisms often involve redundancy, where backup routes or routers take over when the primary ones fail. Dhawan et al. (2022) highlighted the importance of designing routing systems that anticipate and prepare for potential failures, emphasizing that fault tolerance is crucial for maintaining network reliability and efficiency. In fault-tolerant packet routing, the automatic failover mechanism plays a pivotal role, where the system quickly reroutes traffic through alternate paths, ensuring minimal disruption to data flow.

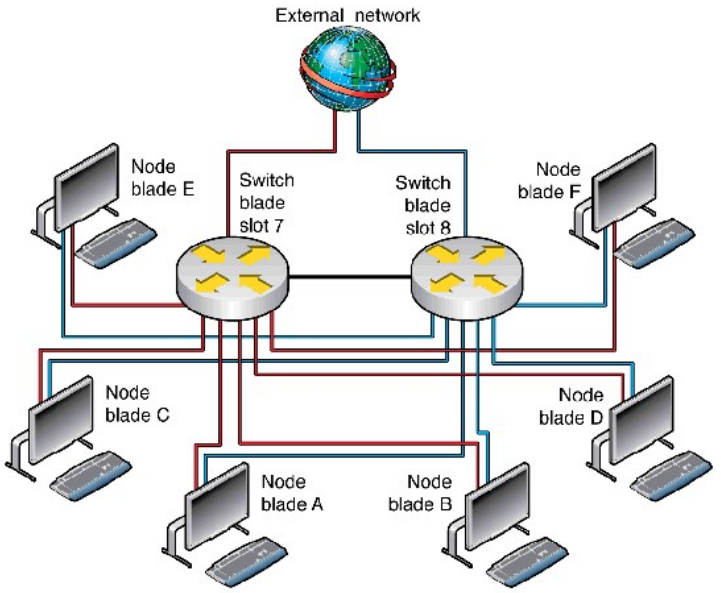

Fig 1: Designing a Fault-Tolerant Network
Source: https://docs.oracle.com/cd/E19217-01/820-7346/guide.html

2.2 Performance Metrics for Evaluating Fault-Tolerant Routing

Performance metrics are vital for assessing the effectiveness of fault-tolerant routing systems. The key metrics include packet delivery rate, failover time, and network throughput. Packet delivery rate measures the percentage of successfully delivered packets, providing insights into the reliability of the routing system. Failover time quantifies how quickly the system recovers from failures, while network throughput evaluates the efficiency of data transmission under varying conditions. These metrics collectively offer a comprehensive view of the system's performance.

2.2 Simulation Tools for Performance Evaluation

Simulation tools like the Cisco Network Simulator are instrumental in evaluating fault-tolerant routing systems. These tools allow researchers to model network scenarios and assess the system's behaviour under different conditions. By simulating router failures and measuring the system's response, researchers can determine the robustness and resilience of the routing mechanism. The Cisco Network Simulator, used in this study, provided a controlled environment to test the fault-tolerant system's ability to maintain network reliability and efficiency, highlighting its capability to handle diverse network scenarios.

2.3 Related Research

The evaluation of fault-tolerant packet routing systems is grounded in a rich body of research that explores various mechanisms and strategies for maintaining network reliability and performance in the face of failures. Dhawan et al. (2022) provide a comprehensive review of fault tolerance techniques in distributed and scalable systems, emphasizing the importance of designing routing mechanisms that can proactively anticipate and manage potential network disruptions. Their study highlights key strategies such as redundancy and dynamic rerouting, which are essential for sustaining network operations even when failures occur.

Similarly, Bertsekas and Gallager (2021) contribute foundational insights into the complexities of data networks, particularly focusing on the critical role of fault-tolerant routing in ensuring uninterrupted data flow. Their work underscores the necessity of robust routing systems that can minimize packet loss and reduce failover times, which are crucial for maintaining network stability. Further contributing to this area, Kabashkin (2023) explores the challenges associated with maintaining end-to-end service availability in heterogeneous multi-tier networks, such as those incorporating cloud, fog, and edge computing environments. This study is particularly relevant to modern network architectures, where efficient fault-tolerant routing is imperative to adapt to the dynamic and complex nature of these systems, ensuring high availability and minimal service interruption. In the context of wireless communications and big data, Bi et al. (2015) discuss the significant challenges posed by the need to manage network resources efficiently.

They highlight the role of fault tolerance in maintaining reliable communication within data-intensive environments, where the ability to handle failures without compromising performance is critical. Elbamby et al. (2018) address the stringent requirements of low-latency and ultra-reliable networks, particularly in the context of emerging technologies such as virtual reality. Their research underscores the necessity for routing systems that can guarantee high performance and reliability, even under conditions where latency and failure tolerance are paramount. The insights from these studies collectively inform the evaluation of fault-tolerant packet routing systems, providing a comprehensive framework for understanding the mechanisms that contribute to network resilience and efficiency.

3. METHODOLOGY

The model used for this research was set out to evaluate a fault-tolerant packet routing system that is resilient to failures and supports different types of traffic as shown in Figure 1. A systematic approach involving the development of a simulation model and rigorous testing using the Cisco Network Simulator was adopted. The performance evaluation was carried out using packet delivery rate, failover time and Network Throughput as metrics to measure the performance of the fault tolerant packet routing scheme:

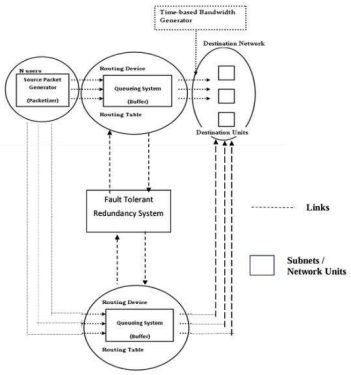

Figure 1: Schematic Diagram of the Fault-Tolerant Packet Routing Model

3.1 Performance Evaluation

Performance metrics shows the system's ability to maintain network reliability, handle failovers

effectively, and ensure efficient data transmission. Evaluating the system based on these metrics has helped gauge its overall performance.

3.2 Packet Delivery Rate

The packet delivery rate represents the percentage of data packets that successfully reach their intended destinations without being lost or dropped. The packet delivery rate can be measured by dividing the number of successfully delivered packets by the total number of packets sent and expressing the result as a percentage.

Packet Delivery Rate (%) = (Delivered Packets / Total Packets Sent) * 100 .....(1)

3.1 Failover Time

Failover time quantifies the time it takes for the system to detect a router failure, activate the failover mechanism, and reroute traffic through the backup router. Measure the time interval from the detection of a router failure to the successful completion of failover. Typically, this is expressed in seconds.

Failover Time (seconds) = Time of Failover Activation - Time of Router Failure Detection .....(2)

3.4 Network Throughput

Network throughput represents the rate at which data can be transmitted successfully. It assesses the system's ability to handle and transmit data efficiently. Network throughput is calculated by measuring the total data transferred (in bits or bytes) within a specific period, typically one second.
Network Throughput (bps or Bps) = Total Data Transferred / Time Interval

4. RESULTS

4.1 The Packet Delivery Rate

This was measured by sending 100 packets (4 sets of 25 pings each) and recording the number of packets successfully delivered versus the number lost. The analysis of the packet delivery rate (PDR) involves evaluating how many packets successfully reach their destination out of a given number sent. This measure is crucial for assessing network reliability and efficiency. The number of loss packets was determined by subtracting the number of packets delivered from the total packets sent, resulting in a range of 0 to 12 lost packets. The packet delivery rate (PDR) was calculated as (Packets Delivered / Total Packets Sent) * 100, yielding rates of 98%, 96%, 100%, 88%, and 100% across the five trials. As shown in Figure 2, the average PDR was computed by summing the individual PDRs (98 + 96 + 100 + 88 + 100 = 482) and dividing by the number of trials (5), resulting in an average PDR of 96.4%.

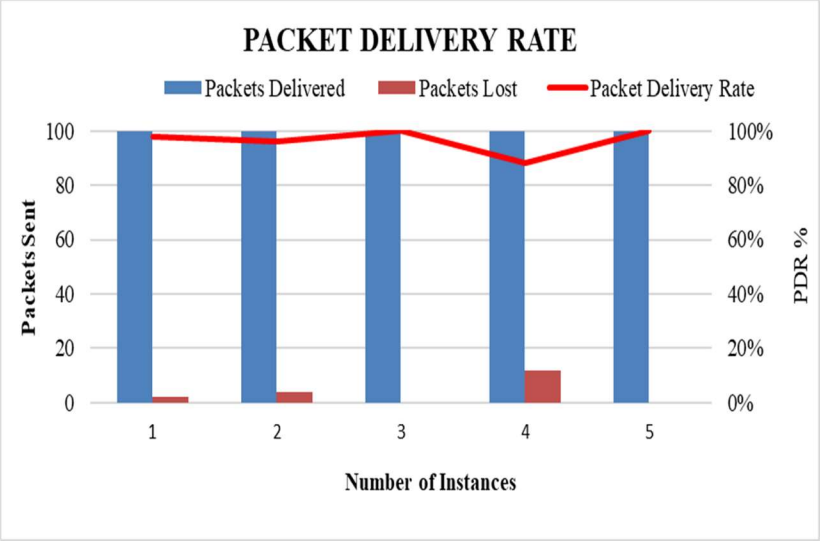

Figure 2: Packet delivery rate across different instances

4.2 Failure time

The times recorded are 3, 4, 5, 3, and 5 seconds, representing the delay between the activation of the failover mechanism and the detection of the router failure. The average failure time is calculated as the mean of the recorded failure times. The sum of the failure times is 3 + 4 + 5 + 3 + 5 = 20 seconds, and with five observations, the average failure time is 20 / 5 = 4 seconds. In Figure 3, the result analysis indicates that the backup router's failover mechanism is effective, with an average detection and switchover time of 4 seconds. This performance metric is crucial for ensuring minimal downtime and maintaining network reliability.

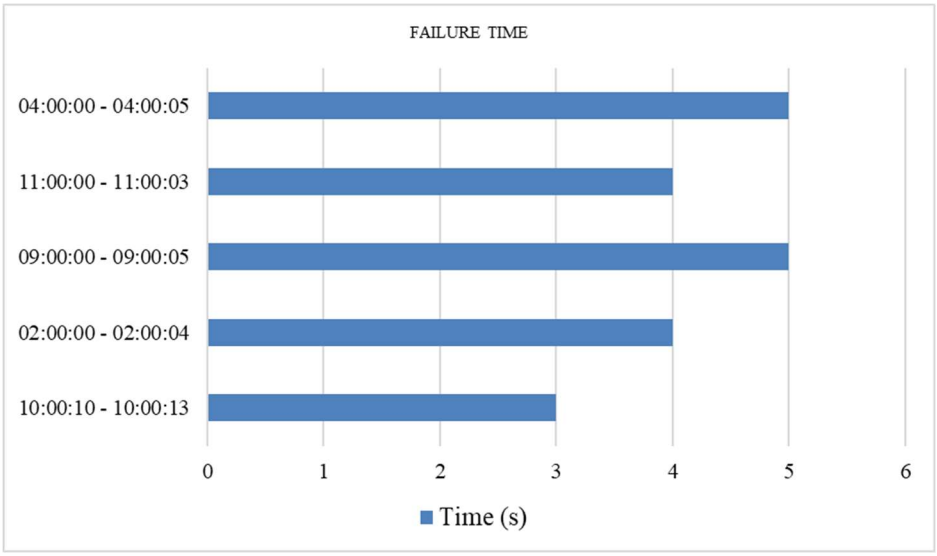

Figure 3: Failover time for router failure detection and recovery

4.3 Network Throughput

The analysis of network throughput involves evaluating how efficiently data packets are transmitted across the network within a specified time interval. The network throughput is measured by the total number of packets successfully transferred divided by the time interval. The recorded throughput values for the trials are 5.16, 6.00, 5.00, 6.77, and 5.00 bps respectively. There was variability in throughput, indicating fluctuations in network performance. The highest throughput recorded was 6.77bps (Test 4), and the lowest throughput is 5.00bps (Test 3 and 5). A shorter time interval generally results in higher throughput, as observed in test 4 where the interval is 13ms, leading to the highest throughput. To find the average network throughput, the sum of the throughput values is

5.16 + 6.00 + 5.00 + 6.77 + 5.00 = 27.93bps .....(3)

With five tests, the average throughput is 27.93 / 5 = 5.586bps .....(4)

The average network throughput was 5.586bps, indicating the network's general performance in transferring packets efficiently within the specified time intervals. Perusing Figures 4 and 5 shows that most tests have high numbers of packets transferred, close to 100, indicating efficient packet delivery. The time interval plays a crucial role in determining network throughput. This metric is crucial for understanding the network's capacity and identifying areas for potential improvement in data transmission efficiency.

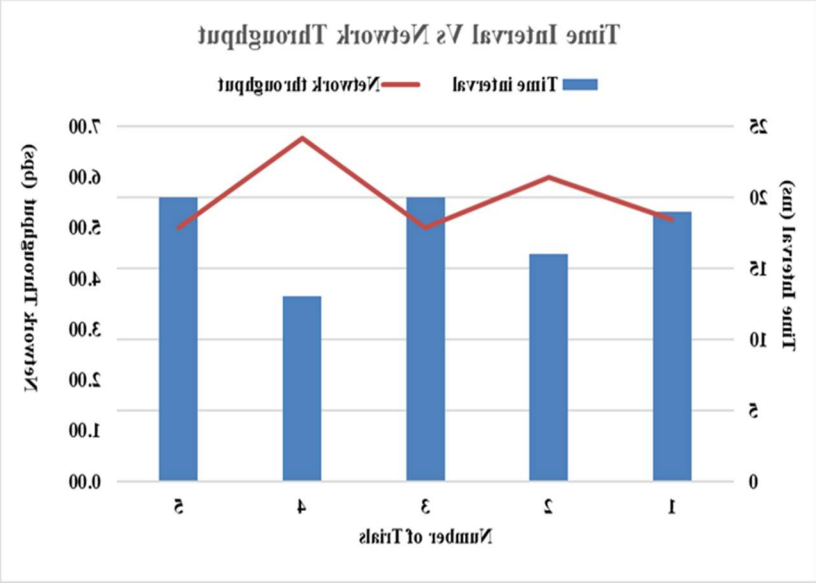

Figure 4: A graph showing the comparison of Time interval and Network Throughput

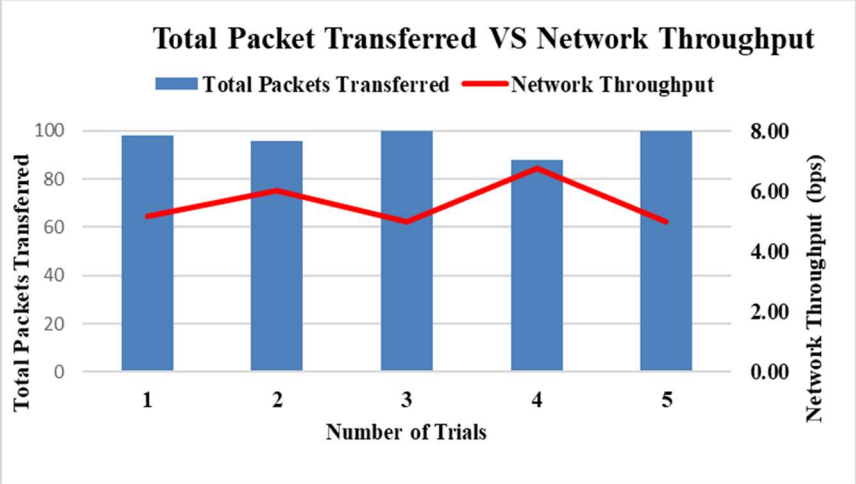

Figure 5: A graph showing the comparison of total packets transferred and network throughput

5. DISCUSSION AND CONCLUSION

5.1 Discussion

The fault-tolerant packet routing system was simulated on a Cisco network simulation platform. Two routers were configured with different priorities to ensure redundancy: the main router had a higher priority of 150, while the backup router had a priority of 100. Hosts were set up to send packets through these routers, with the system designed to automatically switch to the backup router in case of a primary router failure. Testing involved sending 100 packets and measuring key performance metrics such as packet delivery rate, failover time, and network throughput.

The packet delivery rate averaged 96.4%, demonstrating high reliability under normal operating conditions and indicating an uptime of 96%. Failover time averaged 4 seconds, well within the acceptable threshold of 10 seconds, indicating the system's ability to maintain network continuity. Network throughput varied based on the number of packets transferred and the time interval, showcasing the system's efficiency in handling packet transmission, albeit with occasional variations due to packet loss or delays.

The findings from the implementation and testing phases highlight the system's effectiveness and reliability. The high packet delivery rate aligns with the research objective of designing a system that supports different types of traffic and maintains high performance. The low average failover time demonstrates the effectiveness of the failover mechanism, ensuring minimal downtime and quick recovery from router failures. The low average failover time is crucial for network resilience, directly supporting the objective of creating a failure-resilient routing system. Ensuring consistent high throughput is essential for maintaining network efficiency, especially under varying traffic loads and conditions. The ability to handle packet transmission efficiently confirms the system's capability to manage dynamic network conditions, fulfilling the objective of evaluating the system's performance in diverse scenarios.

6. CONCLUSION

This research provides valuable contributions to the broader field of computer networking. It offers a practical implementation and evaluation of a fault-tolerant routing system, emphasizing the importance of integrating robust failover mechanisms and efficient routing methods. The research findings effectively showcased the system's capabilities and limitations, providing valuable insights into its performance and real-world usability.

REFERENCE

[1] Bertsekas, D., and Gallager, R. (2021). Data networks. Athena Scientific.
[2] Bi, S., Zhang, R., Ding, Z., & Cui, S. (2015). Wireless communications in the era of big data. IEEE Communications Magazine, 53(10), 190–199.
[3] Dhawan, D., Ahmad, F., & Tripathi, M. M. (2022). A System Model of Fault Tolerance Technique in the Distributed and Scalable System: A Review.
[4] Elbamby, M. S., Perfecto, C., Bennis, M., & Doppler, K. (2018). Toward low-latency and ultra-reliable virtual reality. IEEE Network, 32(2), 78–84.
[5] Hasan, M. Z., Al-Rizzo, H., & Al-Turjman, F. (2017). A survey on multipath routing protocols for QoS assurances in real-time wireless multimedia sensor networks. IEEE Communications Surveys and Tutorials, 19(3), 1424–1456.
[6] Kabashkin, I. (2023). End-to-End Service Availability in Heterogeneous Multi-Tier Cloud–Fog–Edge Networks. Future Internet, 15(10), 329.
[7] Mills, D. L. (2017). Computer network time synchronisation: the network time protocol on earth and in space. CRC press.
[8] Osunade, O. (2012). A Packet Routing Model for Computer Networks. In International Journal of Computer Network and Information Security, pp. 4, 13-20
[9] Roy, A., and Deb, T. (2018). Performance comparison of routing protocols in mobile ad hoc networks. In Proceedings of the International Conference on Computing and Communication Systems: I3CS 2016, NEHU, Shillong, India (pp. 33–48). Springer Singapore.
[10] Sathyasri, B., Ganesh, E. N., Kumar, P. S., Rathna, S., Bai, R. J., and Nalini, G. (2017). Performance Evaluation of Efficient and Reliable Routing Protocol Algorithm. International Journal on Smart Sensing and Intelligent Systems, 10(5), 358.
[11] Zahid, S., Ullah, K., Waheed, A., Basar, S., Zareei, M., and Biswal, R. R. (2022). Fault-tolerant DHT-based routing in MANET. Sensors, 22(11), 4280.
[12] Zhang, Y., Fan, W., Han, Z., Song, Y., and Wang, R. (2021). Fault-tolerant routing algorithm based on disjoint paths in 3-ary n-cube networks with structure faults. The Journal of Supercomputing, p. 77, 13090–13114.