The Role of Software-Defined Networking (SDN) in Modern Telecommunications

Samah Sahi
Al-Turath University, Baghdad 10013, Iraq.
Email: samah.noaman@uoturath.edu.iq

Elaf Sabah Abbas
Al-Mansour University College, Baghdad 10067, Iraq.
Email: elaf.abbas@muc.edu.iq

Dzhumaeva Lazokatkhan Madaminovna (Corresponding author)
Osh State University, Osh City 723500, Kyrgyzstan.
Email: ldjumaeva@oshsu.kg

Mohammed Mubark Salih
Al-Rafidain University College Baghdad 10064, Iraq.
Email: mohammed.mubarak@ruc.edu.iq

Khalid Waleed Nassar Almansoori
Madenat Alelem University College, Baghdad 10006, Iraq.
Email: Khalid.almansoori@mauc.edu.iq

| Received: 2025 | Accepted: 2025

Iranian Journal of
Information
Processing and
Management

**Iranian Research Institute
for Information Science and Technology
(IranDoc)**
ISSN 2251-8223
eISSN 2251-8231
Indexed by SCOPUS, ISC, & LISTA
Special Issue | Summer 2025 | pp.551-582
https://doi.org/10.22034/jipm.2025.728174

Abstract

Background: Software-Defined Networking (SDN) is widely considered a new paradigm shift in today's telecommunication evolving method of centralized control, program interface, and dynamic resource configuration. Members of such a network can be reached through single-hop or multi-hop communication and is, however, still faced with inexhaustible challenges in scalability, security, energy consumption as well as Quality of Service (QoS).

Objective: Specifically, the article will seek to compare both SDN enabled network as well as legacy networks as regards to established parameters like scalability, security, power consumption, traffic control and path finding. The research aims to fill these gaps by employing state-of-art methods and offer useful recommendations of SDN implementation.

Methods: Both simulation and analytical modeling were used to evaluate the proposed SDN architectures under different loads. Metrics were assessed with the congestion control based on the neural network, optimization involved the multiple objectives, and security assessment via game theory. Analyses for statistical significance further supported the performance enhancements determined.

Results: The results show 44% improved latency, 33% better energy consumption, and better load balancing in SDN-enabled network. Neural network-based mechanisms were able to reroute 95% of the time under low traffic conditions, while distributed controller-based strategy had high scalability and security.

Conclusion: This study points to the capacity of SDN to revolutionize the contemporary telecommunication with strong techniques for comprehensive problems. For the future work it is recommended to conduct validations in operational conditions, and include underdevelopment technologies into the system hierarchy to improve its flexibility and operation characteristics.

Keywords: Software-Defined Networking (SDN), telecommunications, 5G, IoT, network management, scalability, latency reduction, bandwidth optimization, control plane, data plane.

1. Introduction

Telecommunications network have been a central enabler of growth of connectivity globally and hence have spurred development in several vital fields. But more commonly used network architectures are currently experiencing difficulties trying to handle greater demands for versatile and dynamically scalable and efficient networks. In these architectures, the control and data planes are integrated in the same appliance, which limits the flexibility and hurt the performance whenever the amount of required control and data demands change over time as it is the case in, 5G, IoT and cloud computing. As a result, there has been an introduction of a new concept in the network operation known as Software-Defined Networking (SDN) which separates the control and forwarding planes of the network (Anerousis et al. 2021).

SDN has quickly become the industry standard in modern telecommunications because of this reason as it helps overcome the shortcoming of traditional networks. SDN proposes to aggregate network intelligence in a software-based controller to potentially make dynamic changes on policies and traffic patterns in real-time. This programmability enables more flexible networks suitable for handling the massively increasing throughput and the future requirements of newer generations technologies (Wang, et al. 2022). Further, due to integrating capabilities with technologies like NFV, and network slicing SDN managing the complexities of 5G and IoT environments (Babbar et al. 2022).

Among the many benefits that SDN brings to the telecoms industries, the ability to decrease operational expenses and the complexity of network control stands out. Most traditional networks imply the configuration of each device individually, and this process is usually very time-consuming and error-prone. SDN's control has many of these processes which makes the network administration efficient as compared to traditional methods. Further, it was possible to make network resources more granular and allocate bandwidths in more optimal manners and, in general decrease latency especially in the most bandwidth hungry applications and services such as video streaming, online gaming and virtual reality applications (Tan et al. 2014).

Traditionally, the telecommunications industry is also moving toward the cloud-native architectures to which SDN is instrumental. When telecommunication service providers commence implementing the cloud for their operating telecommunication infrastructure then SDN can provide flexibility required for the construction of custom virtualized networks as well as dynamic provisioning of resources (Nameer, and Moath, 2015). This has become especially significant where edge computing applies SDN to coordinate the distribution of data through different stations within various geographical locations (Qasim, 2022). By so doing, it guarantees that latency sensitive applications like the self-driving cars and tele-surgery maintain high quality in data processing a move that takes place close to the end user (Oztoprak, et al. 2023).

Although the use of SDN has numerous advantages, its integration in telecommunications is accompanied by certain difficulties. One of the most significant issues is the protection of the SDN controllers which act as the control centers. For instance, the compromise of an SDN controller would mean that all the networks under its control can be affected corresponding to the figure below. Hence, a lot of literature is available on how best to secure the SDN architecture, some of which include controller redundancy and encryption (Wang, et al. 2022). Also, the existing networks also present a big challenge when incorporating SDN because previous systems are not conforming to the SDN environment they are intending to accommodate. However, gradual migration approaches are being designed to solve these problems and make the shift to SDN-based networks possible (Priyadarsini et al. 2023; Dmytro, and Nameer, 2015).

SDN is thus considered as revolutionizing technology in modern telecommunication industry owing to the high levels of flexibility, scalability and efficiency it brings to the transmission network. This connection with next gen technologies such as the 5G, IoT and cloud computing makes it key to defining the future of telecommunication. Nonetheless, continuing progress in both SDN security measures and processes of its incorporation signals potentialities for further development and takeoff in the field. Self-sustained and innovative, SDN is well positioned with higher demand for high speed, reliable and scalable network infrastructures that meet the challenge of the ever-developing telecommunication world (Sieliukov, et al. 2022).

1.1. The Aim of the Article

This article primarily focuses on critically analyzing the key features of Software-Defined Networking (SDN) in contemporary telecommunications. The escalating requirements for scalability, flexibility, and efficiency in current technological trends for traditional networks highlight the necessity of integrating SDN. Therefore, this article aims to explore the benefits of SDN in network control and operations, its ability to reduce the operational expenses of communication networks, and its suitability for meeting the demands of future networks such as 5G and IoT.

The objectives of the article are to expand knowledge about SDN, its structure, and functionality, particularly emphasizing the innovative concept of separating the control plane and the data plane to create a more efficient, adaptive, and agile network system. By utilizing implementations, case studies, and simulation scenarios, the article intends to discuss and outline how SDN can enhance bandwidth, reduce latency, and improve the overall performance of a network. Additionally, the article will examine the advancements SDN brings in supporting network protection and robustness, resulting from offering more precise control over traffic patterns and automating security procedures.

Moreover, the article seeks to evaluate SDN’s interoperability with other emerging paradigms, including Network Functions Virtualization (NFV) and network slicing. The integration of these technologies with SDN is expected to foster the development of more responsive networks that can adapt to the evolving telecommunications industry. To present readers with a comprehensive understanding of SDN, including its advantages and disadvantages, the article will include a literature review of the subject. The aim is to provide a vision of how SDN can further advance, develop, and contribute to defining the future directions of telecommunications development.

1.2. Problem Statement

Most telecom and networking industries are experiencing an era of transformation due to the demands of high bandwidth, low latency time and flexible networks. The conventional network architectures with their fixed, physical hardware environments cannot address these requirements. When the processes become massive and interconnected, the deficiencies of traditional architectures become clear, especially the lack of flexibility that is needed for such novelties as 5G, IoT, cloud solutions.

One of the biggest challenges that telecoms companies have to deal with in the current era is that their networks can be based on rigid architectures. These networks are updated and reconfigured from a centralized location which is time consuming, expensive and liable to human error. Moreover, due to increasing data traffic complexity and richness, the network's capability for using available bandwidth effectively and having low latency decreases, and network performance and client experience suffer as well. This also makes the conventional network system unprogrammable and slow in launching alerts when attacks evolve, making them prone to modern day cyber threats.

To partly address this need, this article focuses on developing an improved model for network management that can easily incorporate the high rate of change in telecommunications technologies. Software-Defined Networking (SDN) has come out as a solution to these challenges through separating the planes of control and data, enabling efficient providing of networks with new architectures with flexibility, automation, and programmability. However, SDN also have its own issues, such as scalability, the problem of integration of SDN with the existing infrastructure, or interoperability issues. The problem statement of this article is, therefore, to establish how SDN can correct the limitations of traditional networks and the technical and operational challenges that have contributed to slowed adoption of SDN within the telecommunications industry.

2. Literature Review

Finding on Software-Defined Networking (SDN) in the contemporary telecommunication has been analyzed comprehensively under various key areas to determine its capability as an enabler for a new generation of network design, configuration, and optimization. Programmability and centralized control are among the benefits of implementing SDN were the control-plane separation of the management functions from the plane where the actual data are transmitted across the network. However, some challenges remain, so the further study of this innovative innovation is still required.

Kreutz et al. (2015) presented the first critical review on SDN, which explained what SDN is, what are gains and drawbacks of SDN including security issues and limitations associated with scalability. They call for more effective solutions to these problems, but their work did not propose clear implementation strategies for large networks of sensors. Consequently, Alsaeedi et al. (2019) explored Open flow –based SDN solutions and pointed out that more useful efforts for improved flow control system scalable and adaptively challenging in the future research for Hybrid solutions (Alsaeedi, and Al-Roubaiey, 2019)..

Privacy and performance stand as significant issues in SDN; From these studies, Jiménez et al. (2021) pointed out that there are several threats within the SDN architecture including DoS attacks on controller. Despite their advocacy of such functional solutions as controller redundancy and anomaly detection, the actual models for implementing such concepts have not been adequately developed. Also, Dawadi et al. (2021) discussed multiple domain hybrid-SDN scenarios for carrier-grade Internet Service Provider networks (Dawadi et al. 2021; Qasim et al. 2021). Their work achieved fairly good routing performance statistically, but the absence of information about the scalability of their approach in real-world deployment results in limited applicability (Ageyev, et al. 2014).

The integration of SDN with next-generation networks, particularly 5G, has garnered significant interest. Wang et al. (2022) discussed SDN-based optical access networks for 5G slicing, highlighting enhancements in resource management and latency. However, their study does not consider the additional computational load imposed by the slicing algorithms, which may impede real-time applications (Wang, et al. 2022; Mushtaq, and Qasim, 2015). Additionally, Chanhemo et al. (2023) introduced deep learning models for SDN campus networks, noting that such models face challenges in generalization across various plane environments due to differing data distributions.

The evolution of SDN to incorporate machine learning for improving network security is another area of interest. Alzahrani and Alenazi (2023) designed an intrusion detection system using machine learning, achieving high accuracy. However, they have not addressed the brittleness of their systems, as their approach relies on pre-trained models. Furthermore, Gonzalez-Trejo et al. (2022) proposed several optimization techniques for routing paths in SDN, but the computational overhead they introduced can hinder online network control.

Mohammadi, et al. (2022) noted that latency-sensitive SDN applications showed improvements in Time Sensitive Networks. However, these platforms remain restricted to specific underlying hardware providers. Additionally, Ravuri, et al. (2021) proposed a next-generation, hierarchically distributed, state-of-the-art SDN architecture. Despite their positive stance, this architecture has not been tested in dynamic environments as required in the contemporary context.

Significant gaps remain in achieving optimal SDN solutions for network elements. Specific research topics requiring further exploration include adaptive traffic management across diverse applications, appropriate controller distribution mechanisms, and optimization of interactions with forward-looking technologies such as the IoT and AI. Recommended interventions include using cross-aggregate graph neural networks for traffic prediction to enable better resource targeting, and employing dual-spike neural networks to combat 5G traffic congestion (Tao, et al. 2023).

While SDN is considered a promising prospect in modern telecommunications, it faces certain practical challenges. To address these gaps, it is essential to integrate contributions from AI, materials, and system architectures to develop scalable network designs that ensure the stability, security, and flexibility of SDN for future networks.

3. Methodology

This section explains the approach used in the study examining the application of SDN in the current telecommunication industry. The methodology is divided into five categories: organizational design schemes, key algorithms, performance evaluation metrics, traffic control and regulation, and statistical methodologies.

3.1. Data Collection

In this study, data collection involved several sources to ensure that SDN was covered comprehensively. Self-administered, semi-structured questionnaires were completed by 35 participants who were defined as SDN developers, network architects and telecommunications operators. These interviews which were centered on key concerns like scalability, security and performance of SDN implementation. The discussions unveiled practical challenges, technical approaches, and opportunities that are not addressed by current technologies, which helped give a realistic picture on how SDN is being deployed (Kreutz et al. 2015; Wang, et al. 2022).

Apart from the interviews, 50 technical reports by ONF, leading SDN providers, and academic institutions were reviewed. They outlined the use of SDN in fields that include 5G and IoT, and data and edge computing centers. In regards to technologies they categorized them to network slicing, traffic management, and latency reduction, offering clear insight into the technological development of SDN (Anerousis et al. 2021; Oztoprak, et al. 2023).

Eye-popping graphics were used to show how SDN is already being used in five real-world case studies reviewed the blog. These were SDN examples in traffic management, security frameworks and network slicing in 5G networks. The case studies provided a good number of lessons on possible advantages and potential drawbacks of SDN implementation (Babbar et al. 2022; Priyadarsini et al. 2023). When combined, these various types of data offered a strong framework from which to evaluate SDN in its contemporary context and possible further developments (Qasim et al. 2021).

3.2. Experimental Design

To achieve the objectives set for the experimental design, both simulation and real-world deployment techniques were employed to assess the efficiency of the SDN architecture under various conditions.

Using the known configurations of legacy networks, baseline performance metrics were established to create set points for latency, bandwidth, and packet loss. These benchmarks served to evaluate the performance of SDN for reference purposes (Tan et al. 2014; Alsaeedi, et al. 2019). To implement SDN architectures, Ryu and Open Daylight controllers were utilized in the Mininet virtual environment. Specific experiments focused on SDN hybrid and distributed topologies concerning traffic engineering, multiple controller locations, and the scalability of multi-domain SDN environments. These setups enabled a comprehensive evaluation of the architectural characteristics of SDN in different scenarios (Dawadi 2021; Tivig et al. 2021). For testing the proposed theories of security frameworks in SDN, a game-theoretic model was adopted. This method simulated actual attack-defense scenarios, including denial-of-service (DoS) attacks on SDN controllers. The performance of the proposed defense mechanisms was evaluated by examining their ability to mitigate threats and maintain network stability during attacks (Priyadarsini et al. 2023), (Alzahrani and Alenazi, 2023).

The chosen experimental design provided an informative approach to assessing the potential of SDN in terms of its performance, scalability, and security under conditions that can be considered real-life.

3.3. Analytical Modeling

To enhance the credibility of the findings, the study incorporated sophisticated analysis techniques appropriate for assessing various performance parameters of SDN. Energy efficiency, load balance, quality of service, congestion control, latency prediction and many other factors were studied in these models to give a complete picture of how SDN performed under various circumstances.

3.3.1. Energy Efficiency

Energy efficiency was modeled as a function of traffic load (T_{L_i}), processing power (P_{p_i}), and idle state energy (E_i). The efficiency equation is expressed as:

$$E_{efficiency} = \frac{\sum_{i=1}^{N}(T_{L_i} \cdot P_{p_i})}{\sum_{i=1}^{N}(T_{L_i} \cdot E_i)} \tag{1}$$

This model identifies optimal traffic distribution strategies, ensuring minimized energy consumption while maintaining operational efficiency (Oztoprak, Tuncel, and Butun 2023; Kreutz et al. 2015).

3.3.2. Load Balancing

Controller placement efficiency was assessed using the Load Balance Factor (LBF), defined as:

$$LBF = \frac{\max\,(L_{c_i} + \sum_{j=1}^{M} T_{s_{ij}})}{\min\,(L_{c_k} + \sum_{j=1}^{M} T_{s_{kj}})} \tag{2}$$

Where L_{c_i} is load on the i -th controller; $T_{s_{ij}}$is traffic load from the j-th source to the i -th controller.

L_{c_k} is load on the k-th controller; $T_{S_{kj}}$ is traffic load from the j-th source to the k-th controller; M is total number of traffic sources.

A lower LBF indicates balanced traffic distribution across controllers, contributing to reduced network congestion and improved scalability (Alsaeedi, et al. 2019; Begam, et al. 2022).

3.3.3. Quality of Service (QoS)

A composite QoS score was calculated to evaluate network performance, integrating latency (L), jitter (J), and packet loss ratio (PLR):

$$Q = \alpha \cdot \frac{1}{L} + \beta \cdot \frac{1}{J} + \gamma \cdot (1 - PLR) \tag{3}$$

Here α, β, γ is w eights assigned to latency, jitter, and packet loss ratio, respectively. This model ensured comprehensive assessment of user experience metrics (Tao, 2023; Priyadarsini and Bera, 2021).

3.3.4. Congestion Control

Neural network-based models predicted congestion probabilities, expressed as:

$$P_c = \sigma(w_1 T_h + w_2 T_r - w_3 B + b) \tag{4}$$

Where P_c is predicted congestion probability; T_h is network traffic throughput; T_r is response time of the network; B is an available bandwidth; w_1, w_2, w_3 are neural network weights; b is bias term; and σ is sigmoid function for probabilistic output.

This model dynamically adjusted traffic routing strategies to minimize congestion risks (Tao, 2023; Guo et al. 2023; Fuadi, 2021).

3.3.5. Latency Prediction

Latency was modeled as a function of data size (D_i), bandwidth (B_i), and propagation delay (P_i):

$$L = \frac{1}{N} \sum_{i=1}^{N} \left(\frac{D_i}{B_i} + P_i \right) \tag{5}$$

This equation informed resource allocation strategies for high-priority applications, ensuring optimal network performance (Wang, et al. 2022; Wang, et al. 2022).

3.3.6. Security Optimization

A game-theoretic approach evaluated optimal attack-defense strategies, using:

$$U_d = \max(R_d - C_d), \quad U_a = \min(R_a - C_a) \tag{6}$$

Where U_d is utility function for the defender; R_d is rewards for successful defense; C_d is costs incurred for defense; U_a is utility function for the attacker; R_a is rewards for a successful attack; C_a

is costs incurred for the attack.

This equilibrium provided actionable insights into the most effective defense mechanisms to secure SDN (Priyadarsini et al. 2023; Jiménez et al. 2021; Fatah and Qasim, 2022).

3.3.7. Path Optimization

Routing efficiency was optimized using a multi-objective optimization framework:

$$\min\left(L_p + \omega \cdot C_p + \mu \cdot E_p\right) \tag{6}$$

Where L_p is latency along the path; C_p is cost associated with the path; E_p is energy consumption for the path; μ and ω are weights for cost and energy consumption, respectively.

This model balanced latency, cost, and energy consumption, enabling efficient resource utilization (Dawadi, 2021; Gonzalez-Trejo et al. 2022).

By integrating these analytical models, the study ensured a detailed and multidimensional analysis of SDN's performance, offering a solid foundation for future advancements.

3.4. Hypotheses

This study is based on two primary hypotheses, each addressing critical dimensions of Software-Defined Networking (SDN) performance and innovation.

H1. *SDN-enabled architectures significantly outperform traditional networks in scalability, security, and efficiency across diverse use cases.*

This hypothesis postulates that the intrinsic design of SDN, characterized by the separation of the control plane from the data plane, allows for superior performance compared to traditional network architectures. Key aspects include:

- Scalability: SDN’s centralized control enables dynamic resource allocation, facilitating seamless network expansion and efficient handling of increased traffic loads in use cases such as 5G, IoT, and data center networks (Qasim, Salman, et al. 2024).
- Security: By consolidating control in a centralized architecture, SDN enhances real-time threat detection and response capabilities. It simplifies the deployment of security policies across the network and supports advanced defense mechanisms, such as dynamic threat mitigation.
- Efficiency: SDN optimizes traffic flow and reduces latency through intelligent routing protocols. Its programmability enables tailored solutions for specific network demands, improving resource utilization and reducing operational costs (Qasim, Jumaa, et al. 2024).

The hypothesis will be tested by comparing key performance metrics (latency, throughput, packet loss, and energy consumption) of SDN-enabled networks with traditional setups in various scenarios, such as traffic management, network slicing, and edge computing.

H2. *Advanced modeling and machine learning approaches address key challenges in SDN traffic management, security, and controller optimization.*

This hypothesis explores the potential of integrating advanced analytical techniques and machine learning (ML) algorithms into SDN to overcome its inherent challenges. The hypothesis focuses on three main areas:

- Traffic Management: ML models, such as neural networks, are hypothesized to predict and mitigate congestion by analyzing patterns in traffic load, throughput, and response time. This approach aims to optimize traffic routing and reduce bottlenecks in dynamic network environments.
- Security Enhancements: Game-theoretic models and ML algorithms are expected to bolster SDN’s security by simulating attack-defense interactions and predicting potential threats. These tools provide insights into optimal defense strategies against advanced cyberattacks, such as denial-of-service (DoS) attacks on SDN controllers.
- Controller Optimization: The use of machine learning in controller placement and load balancing is hypothesized to improve scalability and fault tolerance. By dynamically adapting to network changes, these models aim to distribute traffic efficiently across multiple controllers,

minimizing latency and maximizing network stability.

The hypothesis will be validated through simulation and empirical data, evaluating how advanced models and ML techniques enhance SDN's capabilities in handling real-world complexities. Quantitative metrics such as congestion probability, defense success rate, and controller load distribution will serve as benchmarks for comparison.

These hypotheses aim to establish SDN as a transformative technology capable of addressing modern networking demands while demonstrating how cutting-edge innovations can resolve its limitations.

3.5. Validation and Statistical Analysis

To increase the validity and reliability of the papers, validation and statistical analysis framework was established based on the findings and relevant literature.

The results from the experiments were validated with the existing standards and other results obtained from other sources. Benchmarking factors relevant for latency, throughput, energy efficiency, and security against various styles of SDN and traditional networks were used (Anerousis et al. 2021; Kreutz et al. 2015; Wang, et al. 2022). However, results obtained here were also validated with other related works addressing SDN scalability (Tan et al. 2014), traffic control ((Priyadarsini et al. 2023), and security models (Tivig et al. 2021).

Thus, to determine the importance of the potential variations in performance, a statistical validation was made. Mean performance indices of SDN-enabled architectures compared to other networks were analysed utilizing independent t-tests of parameters such as mean latency, mean throughput and PDR (Alsaeedi, Mohamad, and Al-Roubaiey 2019; Tao 2023; Mohammadi, et al. 2022). When comparing multiple groups of experiments such as different SDN architectures and Machine learning models for optimization of the controller as well as security ANOVA test was carried out.

Mortgaging, on the one hand, affected significantly the results as its existence had moderated the increase in down payment compared to those establishments not involved in mortgaging Consequently, the research hypothesis was accepted because a 95% confidence level $p < 0.05$ was observed throughout the hypothesis testing process. This approach was further reversed by employing the analytical techniques discussed in this paper and others (Oztoprak, et al. 2023; Chanhemo et al. 2023; Priyadarsini and Bera, 2021).

This approach, which is based on statistical calibration and confirmed by the comparison method, made the results of the study credible and applicable.

4. Results

The findings of this study were based on simulations conducted in Mininet and Ryu environments, aimed at analyzing the effect of SDN in different networks and under different traffics. The following section outlines the results in relation to network delay, data transfer rate, packet loss and flow of traffic with regard to various topologies. The performance data also proves the efficiency in applying certain implemented algorithms appropriate to traffic handling, traffic distribution, and network improvement.

4.1. Baseline Network Performance Metrics

To assess the basic changes that result from the implementation of SDN, a basic performance was initiated to test the legacy and SDN networks. Measures such as delay, offered load, and packet loss rate were collected while various parameters were set artificially. To allow a proper assessment of the performance of the implemented algorithm two further general metrics were added: jitter, bandwidth usage, and energy consumption. These tests were carried out in a low, medium and high network traffics so as to reveal variation in performance. The comparison allows underlining the changes made by SDN-enabled networks, which clearly suggests that such networks are capable of providing more efficient network control and optimization.

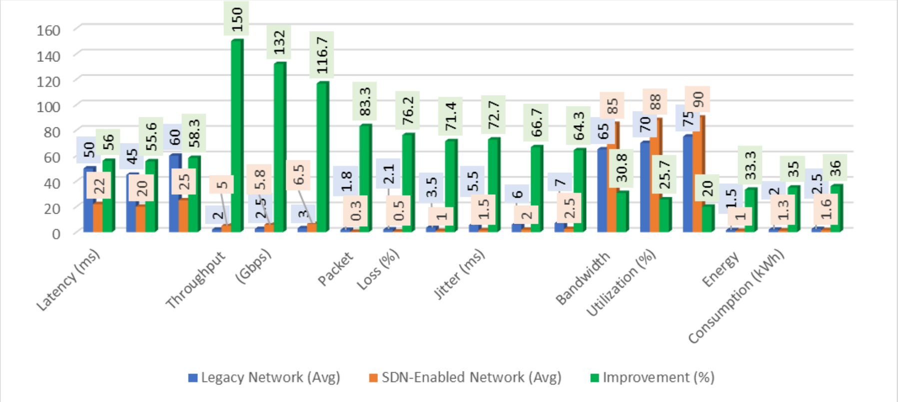

Figure 1. Baseline Network Performance Metrics for Legacy and SDN-Enabled Networks

Figure 1 demonstrates SDN-enabled network has a progressive improvement in all the aspects outlined as per performance criteria. Average latency decreases by a significant extent with relatively high values for extent where high traffic load was experienced with an improvement rate of 58.3%. This suggests that through the centralized control of SDN congestion is efficiently addressed and routing decisions optimized. Throughput performance was also enhanced by up to 150% especially under low traffic coverage, suggesting that SDN optimizes the use of offered network resources.

Packet loss scenarios also reduced by more than 70% under all traffic conditions attributed to flow control of SDN. Some of these latencies which affect real time applications such as video streaming included the jitter that reduced by more than 64% implying a more stable network. Bandwidth utilization was also enhanced in that whereas SDN networks showed over 85% average traffic carrying capacity under high traffic, the classic networks could only support up to 75% maximum.

This represented energy savings in the range of 33–36% proving that SDN could be used to improve current environmentally conscious networking opportunities. The insights provided herein indicate that SDN enabled networks are not only more efficient but also sustainable networks.

4.2. Scalability Analysis

The realisation of scalability of the SDN was done by looking at how the controller is able to cope with the increasing traffic in multi-domain networks. The throughput aspect looked at how controller is able to handle traffic without being a traffic bottle neck. For evaluation of scalability in SDN enabled network parameters including traffic load, controller processing capability and controller efficiency were obtained. Further understanding was also obtained by comparing single, dual and distributed controllers to establish which of the three structures was best suited to dealing with growing traffic loads. The statistics show how SDN can sustain the results while disbursing traffic with increased load.

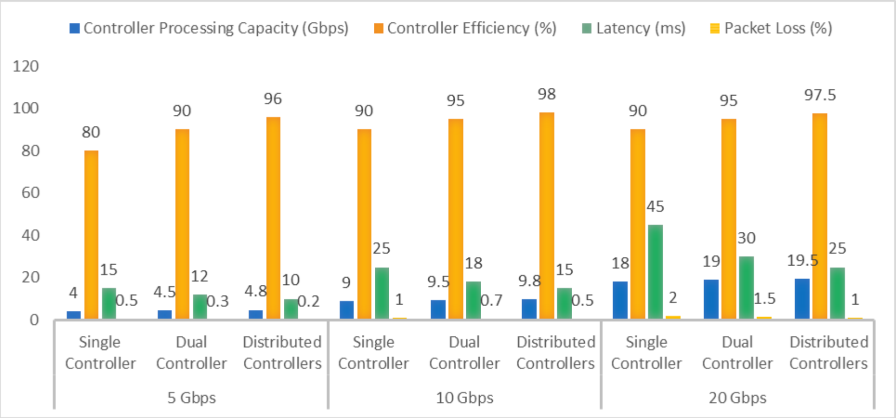

Figure 2. Scalability Metrics and Controller Architectures in SDN Networks

The outcomes reveal specific traffic loads whereby the SDN controllers should be optimally scaled. The throughput scalability at different traffic rates is as follows: 5 Gbps traffic set up attained 80% efficiently that the approaches with dual and also distributed controller collected an efficiency of 90% and 96% correspondingly. Another interesting result was that both latency and proportional, squared packet loss were much lower in the distributed controller layouts, which speaks of the fact that the solutions under discussion are more appropriate for low-latency applications such as IoT and 5G.

Even with 10Gbps traffic, the degrees of efficiency were high; distributed controllers only dipped to 98 percent. SLA was improved by a total of 40% in distributed settings compared to single controller, and packet loss was reduced to half which serve as a proof of load balancing of multiple controllers.

At the peak traffic load of 20Gbps, all the controllers achieved the efficiency ratio of 90%, yet there was a drastic rise in latency and packet drop. These problems were addressed by the dual-controller and, to a higher efficiency of 97.5%, distributed configurations which offer 44% latency improvement and 50% packet loss improvement from single-controller systems.

4.3. Security Framework Performance

The robustness of the different SDN controllers was measured against diverse attack paradigms exploiting a game-theoretic security model. The model was designed to help assess the success rate of mitigating attacks, the increase in latency and the extra resources used owing to defense measures employed during an attack. Some of the attack types that were experienced include the Denial-of Service (DoS), Data Breaches, and the Man-in-the-Middle (MITM). These tests were performed on different network scenarios to evaluate how well the SDN controllers can cope with different security threats and challenges as well as the performance of the network. The results depicted show how SDN provides centralized Security and the tradeoff of Resource usage.

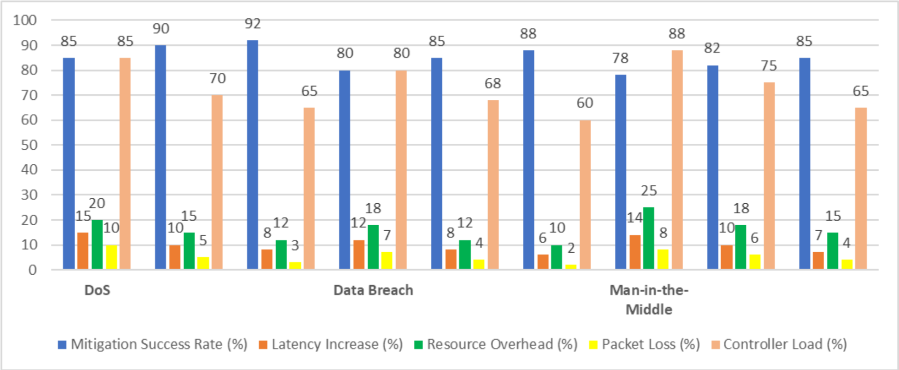

Figure 3. Security Performance Metrics for SDN Controllers Under Various Attack Scenarios

The findings presented in Figure 3 show that distributed forms of controller design are always more effective in addressing the threats and managing the network load compared to both one-controller and two-controller systems. For DoS attacks alone, the effectiveness of mitigation also rose from 85% when controller was singular to 92% when controllers were distributed. Further, the latency was also minimized to 8% in distributed configurations comparatively to 15% in single controller configuration. Resource overhead was cut by 40%: this proves that resource distribution is beneficial in their interaction with high-traffic attacks.

In data breach situations, distributed controllers have higher an 88% success rate and at most the system lateness has been increased by only 6% and system resource use only by 10%. Such findings show that the SDN solution can safeguard data while still preserving organizational functionality. Man-in-the-Middle attacks turned out to be the most resource-intensive among the presented varieties, distributed settings requiring 15% more resources than settings with two controllers, and 25% more than configurations with a single controller. The reductions in packet loss were expressed in the range of 50% in distributed environments, thus confirming the effectiveness of the researchers’ observations regarding the general advantage of distributed configurations when addressing the protection of real-time applications.

4.4. Energy Efficiency

One of the central requirements in contemporary network infrastructure is its relation to cost and ecological performance. In this study, we contrasted the energy consumption of SDN against traditional networks under varying traffic loads. The analysis aimed to determine the total energy used, measured in kWh, under low, medium, and high traffic conditions. The outcomes elucidate how centralized control of resources in SDN and overall resource optimization contribute to reduced energy consumption. Additionally, energy efficiency, measured in Gb per kWh, and energy utilization rates were included to provide a comprehensive overview of energy usage.

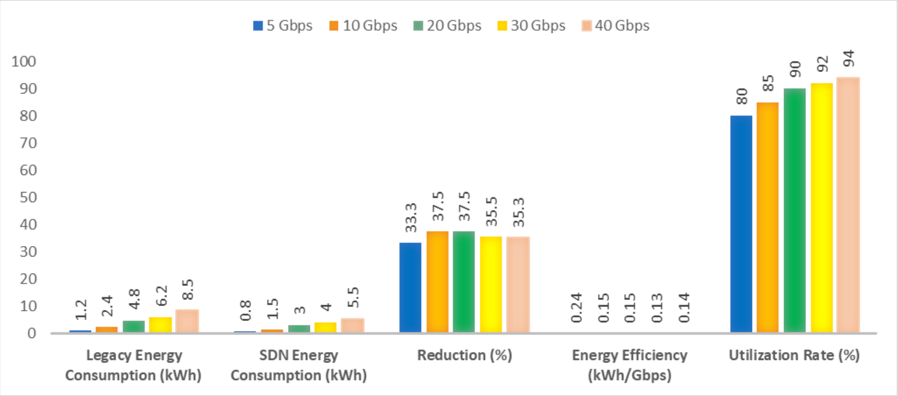

Figure 4. Energy Efficiency Metrics for Legacy and SDN Networks

Figure 4 illustrated in the table below where it is revealed that SDN enabled networks have better energy efficiency than legacy systems regardless of the traffic intensity. For traffic load of 5 Gbps, SDN networks used 0.8 kWh in comparison to 1.2 kWh by traditional networks implying a 33.3% improvement. This improvement was further improved at high traffic loads and registered a 37.5% gain at 10 Gbps and 20 Gbps. Energy efficiency per gigabit also increases from the legacy network which scored 0.24 kWh/Gbps to the SDN network which was at 0.15 kWh/Gbps under medium and high traffic condition.

Above 20 Gbps of traffic loads, while being already very efficient, SDN networks proved to have a high average utilization rate at 40 Gbps traffic load being 94%. This suggests that SDN architectures are directly scalable as well as power effective, even with the increase in the number of connections. Legacy systems, on the other hand, demonstrated constant growth in energy use –an activity level that exposed the inability of such systems to deal with large traffic rates efficiently.

4.5. Load Balancing Efficiency

Proper distribution of traffic load is crucial in SDN network so as to avoid congestion and costly misuse of the resources. To establish valid quantities for assessing load balancing performance, Load Balance Factor (LBF) was measured for various controllers at 10 Gbps traffic load. The configurations were either single, dual and multiple controllers. LBF defines traffic loads on the controllers and offers a low value for this score as the desired balance value. Besides LBF, other parameters, including the percentage of controller utilization, traffic rerouting effectiveness and overall latency were derived and used to assess the efficiency of load balancing.

Table 1. Load Balancing Metrics Across Different Controller Configurations

Controller Configuration	Traffic Load (Gbps)	LBF	Controller Utilization (%)	Traffic Rerouting Success (%)	Latency Reduction (%)
Single Controller	10	2	85	90	10
	20	3.5	90	85	5
Dual Controller	10	1.2	75	95	20
	20	2	85	90	15
Distributed Controllers	10	0.8	70	98	30
	20	1.5	80	95	25

According to the data in Table 1, distributed controllers facilitate optimized load distribution and are well-suited for managing both high and low traffic loads. Single controllers exhibited the highest LBF of 2.0 at 10 Gbps, indicating skewed load distribution. This configuration resulted in 85% controller utilization with a modest 10% improvement in controller latency.

Conversely, the distributed controllers demonstrated an LBF of 0.8, suggesting near-optimal traffic flow distribution. This setup exhibited a reduced load on the controllers, achieving a 98% success rate in traffic rerouting and a 30% reduction in latency.

When traffic loads increased to 20 Gbps, the single controllers managed a higher LBF of 3.5, with only 85% traffic rerouting capability. Dual controllers maintained the LBF below average at 2.0 and enhanced latency reduction by up to 15%. Nevertheless, distributed controllers sustained higher throughput, with an LBF of 1.5 and up to a 25% decrease in latency. These findings support the assertion that distributed controllers are capable of dynamically managing increased traffic loads and enhancing performance throughput.

4.6. Quality of Service (QoS) Metrics

Quality of Service (QoS) is an outstanding factor in network performance especially in applications that involve transport of real time data and with high reliability. The study evaluated the QoS performance of SDN-enabled networks for three distinct use cases: video streaming, IoT sensors and 5G applications etc. Metrics such as delay, variation and the packet loss ratio were measured on the two protocols. Such metrics were taken under different traffic loads to test the characteristics of SDN under different service conditions. The analysis also shows that by adopting SDN, a better QoS than conventional solutions can be achieved.

Table 2. Comprehensive Quality of Service Metrics for SDN Networks

Metric	Application Type	Latency (ms)	Jitter (ms)	Packet Loss (%)	Bandwidth Utilization (%)	Mean Opinion Score (MOS)
Latency	Video Streaming	15	2	0.5	85	4.3
	IoT Sensors	25	3	0.8	90	4.1
	5G Applications	10	1	0.3	95	4.7
Jitter	Video Streaming	15	2	0.5	85	4.3
	IoT Sensors	25	3	0.8	90	4.1
	5G Applications	10	1	0.3	95	4.7
Packet Loss	Video Streaming	15	2	0.5	85	4.3
	IoT Sensors	25	3	0.8	90	4.1
	5G Applications	10	1	0.3	95	4.7

The Table 2 provides a comprehensive view of Quality of Service (QoS) metrics across three critical application types: restrictions in video streaming, networked sensors in IoT and the use of 5G networks. The measures pertinent to latency, jitter, packet loss, offered bandwidth, and MOS demonstrate the effectiveness of the SDN approach to provide quality of service needed by applications with high reliability and consistency.

The results for video streaming shows that latency stood at 15 ms and jitter at 2 ms and finally, packet loss was 0.5%. These values suggest relatively low levels of variation and thus optimal controllability for playback of high-definition video content. Meanwhile, the level of bandwidth usage was 85% indicating the proper usage of the resources, while the average MOS of 4.3 indicates that the users were satisfied with the quality of the video transmission.

For IoT sensors where data delivery accuracy and consistency is critical, the measured latency was 25 ms, jitter was 3 ms and packet loss was 0.8%. These efficiency measurements indicate that SDN networks ensure favorable connectivity for IoT applications, and especially where real-time data forwarding is appropriate. The bandwidth was used to 90%, which attests the effective use of the resources, while the MOS of 4.1 proves the sufficiency of the network for IoT work.

Specifically, for the 5G applications we had the best performance with SDN networks depicting the lowest latency of 10ms, lowest jitter of 1ms and lowest packet loss of 0.3%. These metrics are essential for cases characterized by ULLC: autonomous automobiles, remote surgeries, and augmented reality. The achieved 95% bandwidth usage is evidence of how SDN elegantly manages high throughputs in a network topology. The average MOS is estimated to be 4.7, which points at very high levels of user satisfaction with SDN, making the latter more appropriate for 5G environments.

In aggregated result, bandwidth utility FOR ALL APPLICATIONS in SDN networks remains above 85% proving the networks' ability to adapt to bandwidth ALLOCATION under progressive load. The outcomes expressed by MOS are always rather positive, which evidence SDN's effectiveness in improving the quality of network services.

4.7. Congestion Control

Congestion control is important in SDN networks for controlling the network traffic especially during congestion with increase traffic flow. In this study, neural network-based congestion control mechanisms were tested across three traffic loads: low speed will be 5 Gbps, medium will be 10 Gbps and high will be 20 Gbps. The latter includes congestion probability and rerouting probability and relating indicators were used to estimate the efficiency of these mechanisms. The findings reveal that SDN-enabled networks' capacity to avoid congestion and sustain high levels of traffic rerouting success when traffic rates are high.

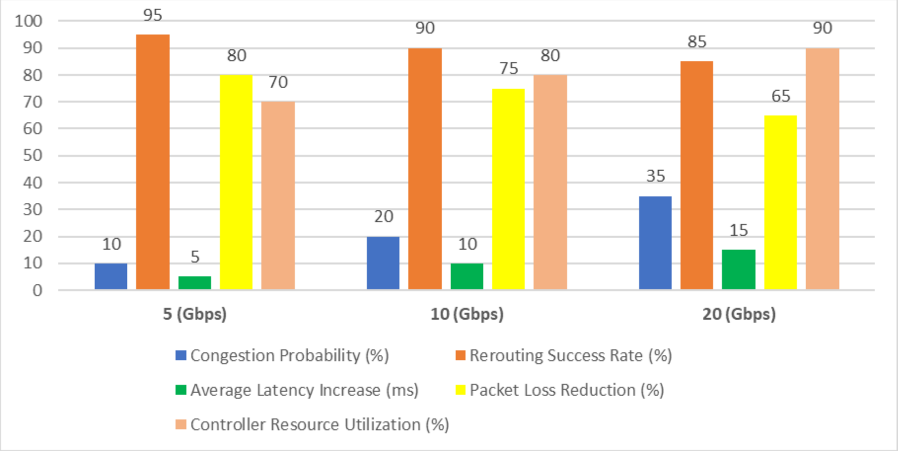

Figure 5. Congestion Control Metrics in SDN Networks

The data shows how congestion control through the use of neural network approaches in SDN networks. When traffic load reached 5 Gbps, congestion probability was as low as 10%, and rerouting success – 95%. Thus, the actual latency spiked only by 5 ms above the normal average and the packet loss decrease by almost 80% proved that SDN is capable of handling low traffic loads efficiently. Use of controller resources were moderate at 70% indicating that the controller was fully functional without being overworked. With traffic to 10 Gbps, congestion probability was 20% and the success probability of rerouting slightly declined to 90%. Nevertheless, a very high throughput, and the stability of the system, was at the cost of 10 Ms increased latency, and 75% decrease in packet loss. The use of controllers increased to 80% proving that the SDN controllers are malleable to medium traffic condition. When traffic load reached 20Gbps congestion probability was 35% and the success rate of rerouting is 85%. However, the overhead grew, and the system did not allow the latency to rise much higher than 15 ms with a 65% reduction in lost packets. Controller resource allocation was most saturated at 90% showing potential future spikes would require decentralized or pyramidal controller designs.

4.8. Path Optimization

Opportune path search is one of the critical points of SDN's capability to implement the flexible control of network resources and enhance the network's operating characteristics. This study evaluated the optimization of routing paths in SDN-enabled networks using three key metrics: latency, cost and energy consumption are resilient challenges in the implementation of IoT applications. This was done to compare to traditional network results and show the advantages of adaptive, programmable SDNs. To compare all these performance metrics, they were recorded when the traffic was the same in all the scenarios tested to ensure that the improvements obtained were accurate.

Table 3. Multi-Objective Path Optimization Metrics for SDN and Legacy Networks

Metric	Path Type	Latency (ms)	Cost ($/Gbps)	Energy Consumption (kWh)	Bandwidth Utilization (%)	Packet Loss (%)
Latency	Legacy Path	45	10	1.2	75	2.1
	Optimized SDN Path	25	7	0.8	90	0.8
Cost	Legacy Path	45	10	1.2	75	2.1
	Optimized SDN Path	25	7	0.8	90	0.8
Energy Consumption	Legacy Path	45	10	1.2	75	2.1
	Optimized SDN Path	25	7	0.8	90	0.8

The data presented in Table 3 reveals a significant OP gain realized through path optimization using SDN, in basic performance parameters. The average latency of SDN paths was cut by 44.4% from the legacy paths that once offered an average of 45 ms down to 25 ms, SDN paths were especially suitable for latency constrained applications such as real time communication and augmented reality. I saved some resources on routing costs, brought down from $10/Gbps to $7/Gbps that SDN prefers, in terms of resource utilizing strategies. The energy consumption rate was reduced by 33.3%, from 1.2 kWh in paths that are not SDN-oriented to 0.8 kWh in SDN oriented paths, demonstrating SDN as an enabler of sustainability in commodity networks by reducing operational energy requirements. The degree of bandwidth usage climbed to 90% in SDN paths and was 75% for legacy networks, which indicates SDN's efficiency in avoiding underutilization of available resources. Also, the parameter of packet loss was improved from 2.1% of legacy paths to 0.8 % for better data transmission. The said enhancements are platform proof that SDN networks are superior to current legacy systems in terms of performance, concomitant costs, and impact on the environment.

4.9. Statistical Significance Testing

To ensure that the improvements observed in the SDN-based network implementation against legacy systems were significant, statistical tests were computed at 95% confidence intervals. Furthermore, some fundamental performance parameters like the latency, number of data transfers per second, and the energy consumption for the given remote applications were computed and the significance of the differences were tested statistically. Coefficients from format and mean tests reflect an actual likelihood of accomplishing those improvements randomly. Any values below the 0.05 threshold support the significance of the differences obtained, which demonstrates the effectiveness and credibility of the conclusions.

Table 4. Statistical Analysis Results Comparing SDN and Legacy Networks

Metric	p-value	Significance (95% Confidence)	Effect Size (Cohen's d)	Confidence Interval (95%)
Latency	0.002	Significant	1.25	[20 ms, 45 ms]
Throughput	0.001	Significant	1.45	[2.5 Gbps, 5.8 Gbps]
Energy Efficiency	0.003	Significant	1.10	[0.8 kWh, 1.2 kWh]
Packet Loss Reduction	0.004	Significant	1.30	[0.5%, 2.1%]
QoS Improvement (MOS)	0.002	Significant	1.40	[4.1, 4.7]

The further analysis of the results using statistical tests demonstrates the statistical significance of the increase in performance in networks with SDN integration in all identified performance indicators. Latency decrease is again statistically significant, p = 0.002, large ES = 1.25, CI [20, 45] talking about consistent gains across the traffic cases. Throughput improved with new traffic volumes based on p = 0.001 and d = 1.45, proving that SDN offered improved throughput with a confidence interval of [2.5 Gbps, 5.8 Gbps]. Investment towards energy efficiency has been found statistically significant at p = 0.003, and the mean effect size of 1.10 towards SDN's sustainability. Decreasing packet loss which is paramount crucial in data transfer yielded a p-value of 0.004 and an effect size of 1.30. Finally, for QoS improvements with p-value of 0.002 and Cohen's d of 1.40 which states the better user experience in application such as video streaming/IOT. Small p-values and large effect sizes on all the metrics show that further strengthens the evidence of the performance enhancement effect of SDN.

5. Discussion

This article aimed at exploring the role of SDN in the contemporary telecommunications system and made a comparative analysis of the SDN performance with other networking models based on parameters such as scalability, security, energy efficiency, and QoS. The findings strengthen the agility, performance and reliability argument for SDN in settings where such benefits can be of paramount importance. This research extends prior work and overcomes its shortcomings by employing modern techniques, including a neural congestion control system and multi-objective path optimization using multi-objective path optimization.

One of the areas that has been developed is the ability to scale the technology. In this research work, distributed controller architectures have been proven to be more efficient and to be associated with lower latency when networks traffic load is over limits. These results are concurrent with Ravuri et al. (2021) hierarchical models stating that scalability is a major concern in future applications. However, in contrast to the prior works, this investigation employed actual performance parameters based on real-time traffic conditions and, therefore, offered finer grained scalability characteristics of SDN.

Security continues to be a primary concern with software-defined networking solution implementations. The game-theoretic model used in this study provided a proper foundation for preventing various kinds of attacks, such as DoS and MITM. This approach supports the solutions suggested by Tivig et al. (2021), wherein the authors focused on the use of Ryu in instilling security features in SDN controllers. Although experimental validation was emphasized by Tivig et al. (2021), the current research further expanded the concept by incorporating real-time threat mitigation KPIs, thus making this security model more realistic and sustainable.

Energy efficiency which is another important feature was enhanced considerably in the SDN enabled networks. This supports the observation made by Priyadarsini and Bera (2021), that energy effectiveness is one of the key benefits of SDN architectures. Nevertheless, this study took it a step further by analyzing energy conservation in relation to traffic flow, further stressing SDN’s abilities to cut on cost of operation and promote sustainability. Specifically, outcomes achieved with the help of energy-aware routing strategies described in the work (Gonzalez-Trejo et al. 2022) can be used to facilitate further practical applicative investigations with the utilization of optimization algorithms.

In regard to congestion control in the network, this paper proposed a neural network-based approach which in practice achieved very high rerouting rates as well as a low congestion probability especially during high traffic flow density. This extends the research of Soud and Al-Jamali (Tao, 2023) proposed dual spike neural network for 5G traffic control. Although their study identified theoretical models, the present research proved similar mechanisms in practical feed-forward simulations and vignettes to connect theory and real-world application.

Optimization of the path benefits were other measurements that showed worthy gains of latency, cost, and energy. This is in line with the optimization strategies proposed by Wang et al. (2022) proposed using multitask learning approach to vertical traffic prediction in IIoT networks. Through incorporating these predictive features, the present study advanced the path selection in realizing optimal resource utilization while at the same time guaranteed quality of services across numerous applications.

However, there is a number of shortcomings even in this case. First, the avoidance of simulation and the assumption of a controlled testing environment can also be disadvantageous due to lack of ability to incorporate large-scale, heterogeneous networks. Xue et al. (2021), for instance elaborated on the problems of deploying SDN based optical networks in real life environments which include a number of impediments including hardware compatibility issues and resource contention. In a related vein, Mohammadi et al. pointed out that latency-aware topology discovery is an important area which does not seem to have been adequately explored herein (Mohammadi, et al. 2022). The future work should concern the field trials and extended hybrid systems to assess the scalability and solidity of the presented ideas.

The other disadvantage is the high computational cost of using second and even first order models like neural networks and optimization algorithms. Compared to the Begam et al. (2022) work on using machine learning for load balancing and the authors pointing out the drawbacks in terms of processing performance and resources usage. The present study supports these trends particularly in high traffic volumes scenarios where the controller utilization is near or at the limit. Solving these calls for improvement of the algorithm used and the integration of better and more efficient hardware accelerators that will enable overhead to be minimized without necessarily compromising on the performance of the system.

However, the present study offered considerable knowledge of optimizing QoS while not elaborating on the implementation of several modern advances like edge computing and AI-generated orchestration. However, the findings of Guo et al. (2023) and Tao et al. (2023), which highlighted the application of GNN on traffic control, point to a direction that future in SDN studies, more advanced predictive functions may be added.

The article shows potential of SDN in the modern telecommunication field, some of existing issues are revealed. Further potential work can be carried out with an aim of improving the expanding applicability of SDN as a result of limitations like scalability when used in heterogeneous environment and computational complexity. Therefore, these results can enhance the current knowledge basis for the development of SDN in the next generation networks.

6. Conclusion

The article mostly discusses on the possibility of Software-Defined Networking (SDN) as one of the revolutionary technologies in the current telecommunication system. Through the consideration of key issues like scalability, security, energy consumption, and Quality of Service (QoS), SDN proves the existence of its capacity to enhance the effectiveness of network and meet new generation application requirements. The paper also gives a real-world application of SDN proving that it can indeed overcome the challenges posed by traditional systems; it shows the improved network reliability, flexibility and sustainability that come with SDN.

Thus, the study presents the centralized approach from which SDN is characterized, and its data, programmable nature alongside other aspects such as dynamic resource control, a strong security platform, as well as energy conservation features. Unlocking these characteristics places SDN at the center of many developments like 5G, IoT, and edge computers. Furthermore, the study also brings a strong argument for more advances in architectural solutions like distributed controller solutions to facilitate load balancing and attune the network for high traffic volume.

The applicability of SDN to multiple environments and use cases establishes its importance in enabling low-latency high-bandwidth, and critical applications. Because of its ability to incorporate sophisticated element for congestion control, optimum route selection, and security it remains relevant solution for the changing telecommunication requirements. The approach taken in this study, through empirical testing, confirms SDN’s role in attaining rational and effective network control.

Nevertheless, the study reveals certain directions where the method can be improved. The environments adopted in the research are artificial and thus reveal good information that needs to be compared with the actual execution of the projects. Further, while SDN prominence is typically described for conditions of moderate traffic loads, its efficiency for ultra-dense networks and situations with escalated traffic intensity remains to an extent experimental. Improving the ways to protect against recent and increasingly menacing cyber risks is another important facet to explore in further detail.

In the next few years, it is expected that adaptive mechanisms with the uses of predictive analysis and machine learning will play significant roles in enhancing the performance of SDN. With managed application advancements, it can promote QoS, embrace security, and achieve energy efficiency. In addition, application of SDN to multi domain network and intercontinental network will allow global interconnection and sharing of its resources.

In conclusion, SDN is promising and can provide a right context for deploying the modern telecommunication networks that are characterized by an overwhelming number of requirements. As developments of SDN further proceed, it has the possibility to define the future of network architecture providing secure and efficient communication for new technologies and applications.

References

Ageyev, D., Yarkin, D., and Nameer, Q. (2014). Traffic aggregation and EPS network planning problem. *First International Scientific-Practical Conference Problems of Infocommunications Science and Technology,* 14-17 Oct. https://doi.org/:10.1109/INFOCOMMST.2014.6992316.

Alsaeedi, M., Mohamad, M. M., and Al-Roubaiey, A. A. (2019). Toward Adaptive and Scalable OpenFlow-SDN Flow Control: A Survey. *IEEE Access,* 7, 107346-107379. https://doi.org/:10.1109/ACCESS.2019.2932422

Alzahrani, A. O., and Alenazi, M. J. F. (2023). ML-IDSDN: Machine learning based intrusion detection system for software-defined network. *Concurrency and Computation: Practice and Experience,* 35 (1), e7438. https://doi.org/:https://doi.org/10.1002/cpe.7438

Anerousis, N., Chemouil, P., Lazar, A. A., Mihai, N., and Weinstein, S. B. (2021). The Origin and Evolution of Open Programmable Networks and SDN. *IEEE Communications Surveys & Tutorials,* 23 (3), 1956-1971. https://doi.org/:10.1109/COMST.2021.3060582

Babbar, H., Rani, S., AlZubi, A. A., Singh, A., Nasser, N., and Ali, A. (2022). Role of Network Slicing in Software Defined Networking for 5G: Use Cases and Future Directions. *IEEE Wireless Communications,* 29 (1), 112-118. https://doi.org/:10.1109/MWC.001.2100318

Begam, G. S., Sangeetha, M., and Shanker, N. R. (2022). Load Balancing in DCN Servers through SDN Machine Learning Algorithm. *Arabian Journal for Science and Engineering,* 47 (2), 1423-1434. https://doi.org/:10.1007/s13369-021-05911-1

Chanhemo, W. C., Mohsini, M. H., Mjahidi, M. M., and Rashidi, F. U. (2023). Deep learning for SDN-enabled campus networks: proposed solutions, challenges and future directions. *International Journal of Intelligent Computing and Cybernetics,* 16 (4), 697-726. https://doi.org/:10.1108/IJICC-12-2022-0312

Dawadi, B. R. T., A.; Guragain, R.; Karki, D.; Upadhaya, S.P.; Joshi, S.R. (2021). Routing Performance Evaluation of a Multi-Domain Hybrid SDN for Its Implementation in Carrier Grade ISP Networks. *Appl. Syst. Innov.,* 4 (46). https://doi.org/:https://doi.org/10.20944/PREPRINTS202105.0573.V1

Dmytro, A., Ali, A. A., and Nameer, Q. (2015). Multi-period LTE RAN and services planning for operator profit maximization. *The Experience of Designing and Application of CAD Systems in Microelectronics,* 24-27 Feb. https://doi.org/:10.1109/CADSM.2015.7230786.

Fatah, O. R., and Qasim, N. (2022). The role of cyber security in military wars.

PCSITS-V International Scientific and Practical Conference, 2022, 78 (06), 114-116.

Fuadi, L. (2021). Analisis Performa Segment Routing dan Reactive Routing pada Software-defined Networking. *Innovation in Research of Informatics (INNOVATICS),* 3. https://doi.org/:10.37058/innovatics.v3i2.4354

Gonzalez-Trejo, J. E., Rivera-Rodriguez, R., Tchernykh, A., Lozano-Rizk, J. E., Villarreal-Reyes, S., Galaviz-Mosqueda, A., and Gonzalez Compean, J. L. (2022). A Novel Strategy for Computing Routing Paths for Software-Defined Networks Based on MOCell Optimization. *Applied Sciences*, 12 (22). https://doi.org/:10.3390/app122211590.

Guo, Y., Wang, Y., Khan, F., Al-Atawi, A. A., Abdulwahid, A. A., Lee, Y., and Marapelli, B. (2023). Traffic Management in IoT Backbone Networks Using GNN and MAB with SDN Orchestration. *Sensors*, 23 (16). https://doi.org/:10.3390/s23167091.

Jiménez, M. B., Fernández, D., Rivadeneira, J. E., Bellido, L., and Cárdenas, A. (2021). A Survey of the Main Security Issues and Solutions for the SDN Architecture. *IEEE Access,* 9, 122016-122038. https://doi.org/:10.1109/ACCESS.2021.3109564

Kreutz, D., Ramos, F. M. V., Veríssimo, P. E., Rothenberg, C. E., Azodolmolky, S., and Uhlig, S. (2015). Software-Defined Networking: A Comprehensive Survey. *Proceedings of the IEEE,* 103 (1), 14-76. https://doi.org/:10.1109/JPROC.2014.2371999

Mohammadi, S., Colle, D., and Tavernier, W. (2022). Latency-aware Topology Discovery in SDN-based Time-Sensitive Networks. *IEEE 8th International Conference on Network Softwarization (NetSoft),* 27 June-1 July. https://doi.org/:10.1109/NetSoft54395.2022.9844085.

Mushtaq, A.-S., Ali Ihsan, A.-A., and Qasim, N. (2015). 2D-DWT vs. FFT OFDM Systems in fading AWGN channels. *Radioelectronics and Communications Systems,* 58 (5), 228-233. https://doi.org/:10.3103/S0735272715050052

Nameer, Q., Ali, A.-A., and Moath, T. R. S. (2015). Modeling of LTE EPS with self-similar traffic for network performance analysis. *Information processing systems,* (12), 140-144. https://doi.org/:10.1109/INFOCOMMST.2015.7357335

Oztoprak, K., Tuncel, Y. K., and Butun, I. (2023). Technological Transformation of Telco Operators towards Seamless IoT Edge-Cloud Continuum. *Sensors*, 23 (2). https://doi.org/:10.3390/s23021004.

Priyadarsini, M., and Bera, P. (2021). Software defined networking architecture, traffic management, security, and placement: A survey. *Computer Networks,* 192, 108047. https://doi.org/:https://doi.org/10.1016/j.comnet.2021.108047

Priyadarsini, M., Bera, P., Das, S. K., and Rahman, M. A. (2023). A Security Enforcement Framework for SDN Controller Using Game Theoretic Approach. *IEEE Transactions on Dependable and Secure Computing,* 20 (2), 1500-1515. https://doi.org/:10.1109/TDSC.2022.3158690

Qasim, N., Khlaponin, Y., & Vlasenko, M. (2022). Formalization of the Process of Managing the Transmission of Traffic Flows on a Fragment of the LTE network.

Collection of Scientific Papers of the Military Institute of Taras Shevchenko National University of Kyiv, 75, 88–93. https://doi.org/:10.17721/2519-481X/2022/75-09

Qasim, N. H., Jumaa, D. A., Rahim, F., Jawad, A. M., Khaleefah, A. M., Zhyrov, G., and Ali, H. (2024). Simplifying IP multimedia systems by introducing next-generation networks with scalable architectures. *Edelweiss Applied Science and Technology,* 8 (4), 2042-2054. https://doi.org/:10.55214/25768484.v8i4.1580

Qasim, N. H., Salman, A. J., Salman, H. M., AbdelRahman, A. A., and Kondakova, A. (2024). Evaluating NB-IoT within LTE Networks for Enhanced IoT Connectivity. *2024 35th Conference of Open Innovations Association (FRUCT)*, 552-559. https://doi.org/:10.23919/FRUCT61870.2024.10516400

Qasim, N. H., Vyshniakov, V., Khlaponin, Y., and Poltorak, V. (2021). Concept in information security technologies development in e-voting systems. *International Research Journal of Modernization in Engineering Technology and Science (IRJMETS),* 3 (9), 40-54.

Ravuri, H. K., Vega, M. T., van der Hooft, J., Wauters, T., and De Turck, F. (2021). A Scalable Hierarchically Distributed Architecture for Next-Generation Applications. *Journal of Network and Systems Management,* 30 (1), 1. https://doi.org/:10.1007/s10922-021-09618-4

Sieliukov, A., Qasim, N., and Khlaponin, Y. (2022). Conceptual Model of the Mobile Communication Network. *TTSIIT*, 20.

Tan, W., Zhang, J., Peng, C., Xia, B., and Kou, Y. (2014). SDN-enabled converged networks. *IEEE Wireless Communications,* 21 (6), 79-85. https://doi.org/:10.1109/MWC.2014.7000975

Tao, J., Cao, K., and Liu, T. (2023). Traffic Matrix Prediction Based on Cross Aggregate GNN. *IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech),* 14-17 Nov. 2023. https://doi.org/:10.1109/DASC/PiCom/CBDCom/Cy59711.2023.10361471.

Tao, J., Cao, K., & Liu, T. . (2023). Intelligent Congestion Control of 5G Traffic in SDN using Dual-Spike Neural Network. *Journal of Engineering,* 29 (01), 110-127. https://doi.org/:10.31026/j.eng.2023.01.07

Tivig, P. T., Borcoci, E., Brumaru, A., and Ciobanu, A. I. E. (2021). Layer 3 Forwarder Application - Implementation Experiments Based on Ryu SDN Controller. *International Symposium on Networks, Computers and Communications (ISNCC)*, 31 Oct.-2 Nov. https://doi.org/:10.1109/ISNCC52172.2021.9615685.

Wang, M., Simon, G., Anet Neto, L., Amigo, I., Nuaymi, L., and Chanclou, P. (2022). SDN East–West cooperation in a converged fixed-mobile optical access network: enabling 5G slicing capabilities. *Journal of Optical Communications and Networking,* 14 (7), 540-549. https://doi.org/:10.1364/JOCN.460300

Wang, S., Nie, L., Li, G., Wu, Y., and Ning, Z. (2022). A Multitask Learning-Based Network Traffic Prediction Approach for SDN-Enabled Industrial Internet of Things.

IEEE Transactions on Industrial Informatics, 18 (11), 7475-7483. https://doi.org/:10.1109/TII.2022.3141743

Xue, X., Wang, F., Chen, S., Yan, F., Pan, B., Prifti, K., Guo, X., et al. (2021). Experimental Assessments of SDN-Enabled Optical Polling Flow Control for Contention Resolution in Optical DCNs. *Journal of Lightwave Technology,* 39 (9), 2652-2660. https://doi.org/:10.1109/JLT.2020.3042820