Journal of Information Systems Engineering and Management
2025, 10(35s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Optimized and Secure Routing in Software-Defined Networking Using Reinforcement Learning and Cryptographic Techniques

Nagaraju Tumakuru Andanaiah[1,2*], Malode Vishwanatha Panduranga Rao[3]

[1]*Electronics Engineering, Faculty of Engineering & Technology, JAIN (Deemed-to-be University), Kanakapura Main Road, Bengaluru, 562112, Karnataka, India.*

[2]*Department of Electronics & Communication Engineering, Government Engineering College, Ramanagara, 562159, Karnataka, India.*

[3]*Computer Science & Engineering, Faculty of Engineering & Technology, JAIN (Deemed-to-be University), Kanakapura Main Road, Bengaluru, 562112, Karnataka, India.*

**Corresponding Author: nagarajuta76@gmail.com*

ARTICLE INFO

Received: 14 Dec 2024

Revised: 19 Feb 2025

Accepted: 28 Feb 2025

ABSTRACT

The increasing complexity of digital communication networks demands efficient, scalable, and secure network management solutions. Software-Defined Networking (SDN) has emerged as a transformative technology, enabling centralized control, real-time traffic management, and adaptive routing. However, existing routing mechanisms often struggle to balance key performance factors such as latency, energy efficiency, and security. To address these challenges, this study presents a comparative analysis of reinforcement learning-based cognitive routing and a security-enhanced, energy-efficient SDN framework. The proposed approach integrates Exponential Spline Regression Reinforcement Learning (ESR-RL) for optimized routing decisions and Genus Weierstrass Curve Cryptography (GWCC) for secure data transmission. The study evaluates various SDN routing techniques based on latency, throughput, energy consumption, and encryption/decryption efficiency. Comparisons with traditional SDN routing, reinforcement learning-based methods, genetic algorithm-based optimizations, and load-balanced approaches demonstrate that the proposed scheme significantly reduces end-to-end delay while maintaining strong security. Additionally, ESR-RL proves effective in minimizing network overhead, while GWCC ensures robust encryption without imposing excessive computational costs. Simulation results indicate that the proposed SDN optimization framework offers superior scalability and adaptability, making it highly suitable for dynamic network environments. The findings highlight that integrating advanced learning-based routing with lightweight cryptographic techniques can significantly enhance SDN performance, making it ideal for future networking applications such as 5G, IoT, and cloud-based infrastructures. This research contributes to the development of more resilient and intelligent SDN frameworks capable of meeting evolving network demands.

Keywords: Reinforcement Learning, Energy-Efficient Routing, Cryptographic Security, Latency Optimization, Weierstrass Curve Cryptography.

1. INTRODUCTION

The rapid growth of digital communication networks has led to a rising demand for network management solutions that are efficient, scalable, and secure. Software-Defined Networking (SDN) has emerged as a groundbreaking approach that separates the network control plane from the data forwarding plane, allowing for centralized control, dynamic traffic management, and greater adaptability [1,2]. This shift enhances network performance by enabling intelligent decision-making, real-time monitoring, and optimized routing [3]. However, as network infrastructures become increasingly complex, traditional routing methods face challenges in maintaining a balance between latency, throughput, energy efficiency, and security, making the development of advanced methodologies essential.

Optimizing routing is crucial for ensuring the efficient flow of data within SDN architectures. Traditional routing algorithms often prove ineffective in dynamic network environments due to their dependence on predefined rules [4]. To overcome these limitations, cognitive routing mechanisms leverage machine learning (ML) and reinforcement learning (RL) to dynamically identify optimal paths in real time [5,6]. By continuously learning from network

conditions and adjusting routing decisions accordingly, cognitive routing enhances overall network performance [7]. While these adaptive techniques significantly improve throughput and latency, they do not inherently address critical aspects such as energy efficiency and security, which remain vital in modern network infrastructures.

Energy efficiency has become a crucial aspect of SDN, especially with the growing adoption of energy-intensive technologies like the Internet of Things (IoT), 5G networks, and cloud computing. Traditional routing methods in SDN primarily focus on performance factors such as packet loss and delay, often overlooking the energy consumption of networking devices. To bridge this gap, energy-aware routing strategies have been integrated into SDN frameworks, leading to enhanced performance and optimized power usage [8]. Reinforcement learning-based models, such as Exponential Spline Regression RL (ESR-RL), offer a data-driven approach to balancing network performance with energy efficiency.

Security remains a significant challenge in SDN environments, as centralized controllers create potential vulnerabilities, making them prime targets for cyber threats [9]. Encryption methods, such as public-key cryptography [10] and lightweight cryptographic protocols [11], enhance data security by preventing unauthorized access and ensuring secure communication between network components. However, traditional encryption techniques often introduce computational overhead, leading to higher latency and reduced throughput. To mitigate these issues, advanced cryptographic solutions like Genus Weierstrass Curve Cryptography (GWCC) have been developed, offering strong security while minimizing processing delays.

This study presents a comparative analysis of existing research alongside peer methodologies that address various aspects of SDN optimization. The first investigation focuses on the application of RL models in SDN to enhance network performance by optimizing throughput and reducing latency through cognitive routing. The second study proposes a security-enhanced, energy-efficient SDN framework that incorporates GWCC for secure data transmission and ESR-RL for optimized routing. While both approaches demonstrate significant improvements in SDN performance, they differ in their optimization strategies and criteria. This paper aims to provide a comprehensive evaluation of these methods, highlighting their strengths, limitations, and practical implications.

The comparative analysis will assess the effectiveness of each method in optimizing routing, enhancing network performance, reducing energy consumption, and implementing security measures. Furthermore, this paper will contextualize these findings by comparing them with existing peer-reviewed methodologies to identify potential areas for further enhancement. The insights gained from this research will contribute to the development of more adaptable, scalable, and resilient SDN frameworks capable of meeting the evolving demands of modern network infrastructures.

2. RELATED WORKS

SDN has emerged as a critical technology for optimizing traffic engineering, security, and energy efficiency in modern networks. Several studies have explored SDN-driven routing mechanisms using RL, cryptographic security models, and heuristic optimization techniques. Chen et al. introduced RL-Routing, a deep reinforcement learning (DRL)-based algorithm that dynamically adapts to network conditions, outperforming traditional methods like OSPF and LL routing in throughput and latency optimization [12]. Similarly, Zhang et al. proposed TBPPO, a DRL-based multi-path routing algorithm integrating KL divergence for trust evaluation and enhanced security, reducing average delay and mitigating Distributed Denial of Service (DDoS) attacks [19]. Zabeehullah et al. developed DQQS, a DRL model for secure routing in SDN-IoT environments, effectively balancing Quality of Service (QoS) and Quality of Experience (QoE) [20]. RL has also been applied in security-driven approaches, such as QTSRA, introduced by Zhang et al., which employs Q-learning and Dempster-Shafer theory to assess node trustworthiness, improving security in SDN-enabled wireless sensor networks (WSNs) [21].

Beyond RL, cryptographic and blockchain-based mechanisms have been integrated into SDN routing frameworks to enhance security and reliability. Abbas et al. combined Genetic Algorithm (GA)-based routing with blockchain authentication to improve access control and routing integrity in SDN-IoT networks, demonstrating increased energy efficiency and malicious node detection [17]. Rui et al. introduced SRAIOT, a ML-driven secure routing model that segments IoT networks into subnets managed by SDN controllers, enabling real-time intrusion detection and improved attack mitigation [18].

Journal of Information Systems Engineering and Management
2025, 10(35s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Energy-efficient routing remains a significant focus in SDN research, particularly for data center networks (DCNs), wireless body area networks (WBANs), and vehicular ad hoc networks (VANETs). Cicioğlu et al. proposed ESR-W, an SDN-based routing algorithm optimized for WBANs, leveraging a fuzzy-based Dijkstra approach to improve energy efficiency while maintaining QoS [13]. In DCNs, Pathan et al. introduced a priority-based energy-efficient routing framework utilizing Mixed Integer Linear Programming (MILP) to optimize flow prioritization and load balancing [15]. For VANETs, Renuka et al. developed the SELAR algorithm, integrating SDN with 5G and fog computing to enhance mobility-aware routing while minimizing energy overhead [23]. Similarly, Moosavi et al. proposed an energy-efficient function placement model for hybrid SDN/NFV networks, introducing a Modified Viterbi Algorithm to reduce energy consumption by selectively deactivating underutilized network elements [25].

In mobile core and MPLS-based networks, SDN-driven routing mechanisms have been employed to optimize traffic engineering and scalability. Alidadi et al. introduced PSLC, a low-complexity SDN-MPLS routing algorithm that improves bandwidth utilization and reduces call blocking, making it suitable for 5G network optimization [14]. Ibrahim et al. proposed EARMLP, an energy-aware multi-level routing algorithm for SDN-based core networks that utilizes heuristic optimization techniques to achieve up to 70% energy savings [24]. Udayaprasad et al. presented an AI-driven SDN routing framework for Intelligent-IoT (I-IoT) networks, integrating GA, Particle Swarm Optimization (PSO), and Artificial Bee Colony techniques to enhance scalability and network lifespan [22].

For multimedia and delay-sensitive applications, SDN-based QoS-aware routing mechanisms have been explored. Gong et al. introduced FDBGR, a fuzzy logic-based delay-bandwidth routing algorithm designed for real-time video conferencing applications, outperforming traditional models in reducing latency and optimizing network load distribution [16]. These studies collectively demonstrate the potential of SDN in advancing intelligent, scalable, and energy-efficient networking solutions, particularly through the integration of RL, blockchain security, and multi-objective optimization techniques.

3. METHODOLOGIES

3.1 Cognitive Routing Algorithm Module

The CRAM routing system is built on Recurrent Neural Networks (RNN) and RL. It trains a new RNN at each Network Function Element (NFE) along the shortest path of a given flow. In this framework, each RNN neuron functions as an open port on an NFE, working collaboratively to generate routing predictions. The RNN operates in two modes: exploration, where it randomly selects an output port, and exploitation, where it chooses the neuron with the highest probability. If no existing RNN is available for the flow at the next NFE, a new one is trained to ensure optimal routing decisions.

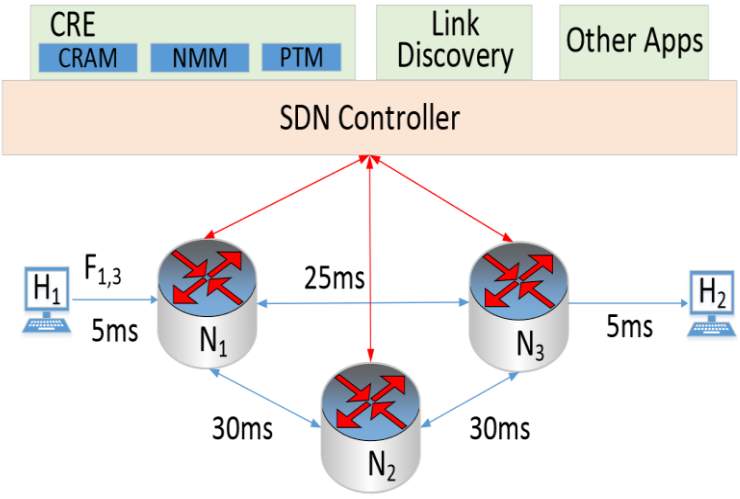

Figure 1. Architecture under Consideration

Journal of Information Systems Engineering and Management
2025, 10(35s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Excitation levels of individual neurons affect the choice of the next node in the NFE process during the exploitation phase. The potential of a neuron (qi) is determined using the ratio of its positive potential (λ^+) to the normalization factor (r), incorporating both positive (λ^+) and negative (λ^-) global potentials received from interconnected neurons. These potentials consider individual neuronal contributions and connection weights. The normalization factor (r) is computed by summing the positive and negative link weights for all neighbouring neurons. RL is employed to calculate the positive and negative weights of each link.

$$q_i = \frac{\lambda_i^+}{r_i + \lambda_i^-} \quad (1)$$

$$\lambda_i^+ = \sum_{j \in N} q_j w_{j,i}^+ + \Lambda_i^+ \quad \text{where } j \neq i \quad (2)$$

$$\lambda_i^- = \sum_{j \in N} q_j w_{j,i}^- + \Lambda_i^- \quad \text{where } j \neq i \quad (3)$$

$$r_i = \sum_{j \in N} \left[w_{i,j}^+ + w_{i,j}^- \right] \quad \text{where } j \neq i \quad (4)$$

To evaluate routing performance, the objective function $O_{sd}[t]$ is computed as an exponential moving average of past values, with a parameter α controlling the weight assigned to previous time steps. To prevent infinite growth, link weights are renormalized based on updated values. CRAM also maintains a record of previously identified paths for routing queries. If a route has been active beyond a defined threshold, the optimal available path is selected for actual traffic transmission, ensuring efficient and adaptive routing decisions.

$$O_{sd}[t] = \alpha O_{sd}[t-1] + (1-\alpha)(o_{sd}[t]) \quad \text{where } 0 < \alpha < 1 \quad (5)$$

3.2 Exponential Spline Regression RL Method

Routing is a fundamental network function responsible for determining the most efficient path between a source and a destination node. SDN significantly enhances network performance through its programmable nature, centralized control, and global network visibility, while also separating network management from packet forwarding. These capabilities allow SDN to address many of the limitations inherent in traditional routing protocols. The overall framework of the proposed method is depicted in Figure 2.

The process begins with registering devices and nodes, integrating all network components into the system. This registration captures detailed information about each device, ensuring an accurate inventory for effective network management and monitoring. Following registration, a cryptographic function, such as the Diffie-Hellman key exchange (FFDH), is used for key generation. This step creates essential public and private keys for each device, along with a secret key, which are crucial for establishing secure communication across the network.

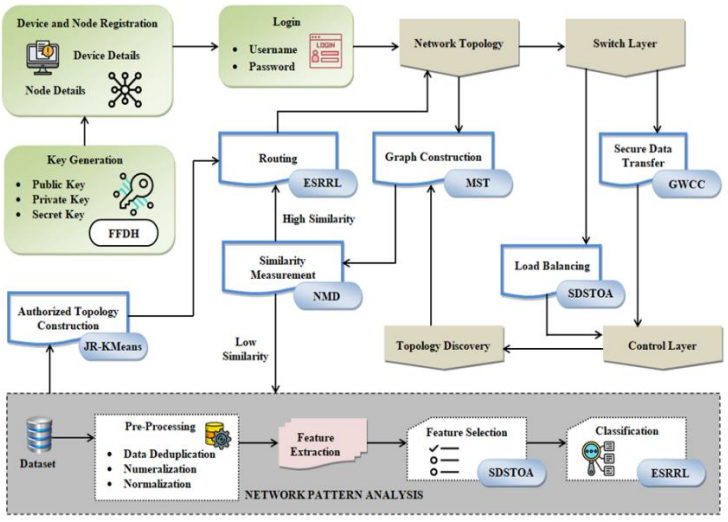

Figure 2. Secured Routing Framework

Journal of Information Systems Engineering and Management
2025, 10(35s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Once device registration and topology construction are complete, users can access the system through a secure login process requiring a username and password. This authentication mechanism ensures that only authorized personnel can utilize network management functions. Upon successful login, the system retrieves and displays the network topology, providing a comprehensive view of the network's configuration. This feature is essential for effective network administration and troubleshooting.

Figure 2 illustrates how the ESR-RL algorithm is applied to routing decisions within a network. By analysing and predicting network traffic patterns, ESR-RL enables more efficient routing. When the similarity measurement between nodes is high, the algorithm manages the routing process, selecting the optimal path while maintaining energy efficiency. To construct a network graph with minimal redundancy and efficient data paths, the Minimum Spanning Tree (MST) algorithm is utilized. Simultaneously, GWCC is implemented within the switch layer to enhance data transfer security, protecting against unauthorized access and transmission attacks.

The methodology utilizes Network Metric Distance (NMD) to measure similarity between nodes or routes, playing a critical role in the process. This metric quantifies similarity, allowing ESR-RL to manage routing when high similarity is detected. In cases of low similarity, the system initiates topology discovery and load balancing. Network pattern analysis is also an essential component of the framework. The process begins with dataset pre-processing, which includes removing duplicates, converting non-numeric data into numerical format, and normalizing the data to ensure accuracy. Feature extraction techniques are then applied to identify key attributes, followed by the Skellam Distributed Siberian Tiger Optimization Algorithm (SDSTOA), which selects the most relevant features. These features are then classified using ESR-RL. Through this comprehensive analysis, the system accurately predicts network patterns, enabling informed routing and management decisions.

The proposed method integrates innovative techniques to address challenges related to energy efficiency, security, and dynamic management in SDN. Its uniqueness lies in the seamless combination of ESR-RL, GWCC, and SDSTOA, ensuring that each component operates without disrupting the others. This integration enables a comprehensive network management approach focused on optimizing routing, securing data transmission, and adapting to real-time network conditions. The framework effectively addresses multiple critical aspects of SDN management simultaneously, providing a solution to the limitations of traditional network models. By incorporating energy-aware routing, secure data transmission, and dynamic network optimization, the method represents a significant advancement in SDN management. Through the integration of advanced ML, cryptographic techniques, and optimization algorithms, the framework offers a robust, efficient, and secure solution for modern network infrastructures. Its holistic design ensures it meets the growing demands for data and connectivity in a sustainable and cost-effective manner.

4. PERFORMANCE COMPARATIVE ANALYSIS

4.1 Simulation Setup

The proposed approach was tested with NS-3 and the SDN emulator Mininet. Within a 2000×2000-meter target area, the simulation environment included nodes moving in three separate groups each keeping a communication range of 100 meters. Although cluster movement speeds ranged from 0 to 25 m/s, nodes within each cluster moved at the same speed. M=5 channels made up the spectrum, and each one of them allowed one of two licensed primary users (PUs) within a 500-meter communication range. These land-based PU nodes' activity displayed an exponential on/off pattern with a 0.05 rate parameter.

4.2 End-to-end Delay

The comparative analysis of the proposed method against peer routing approaches highlights its efficiency in reducing end-to-end delay across varying network sizes, as shown in Figure 3. As the number of nodes increases, the proposed scheme consistently outperforms traditional SDN routing, RL-based routing, GA-based optimization, and load-balanced routing. The results indicate that load-balanced routing experiences the highest delay, followed by GA-based optimization, RL-based routing, and traditional SDN routing. The proposed scheme maintains the lowest delay across all scenarios, demonstrating its effectiveness in optimizing network performance. The findings suggest that

Journal of Information Systems Engineering and Management
2025, 10(35s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

integrating advanced optimization techniques into SDN routing can significantly enhance efficiency, particularly in networks with higher node densities.

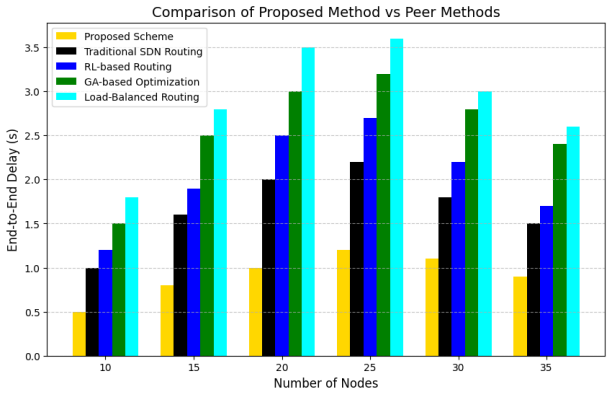

Figure 3. End-to-end Delay Performance

RL-based and genetic algorithm-based methods provide moderate enhancements over traditional routing; however, they do not match the performance of the proposed approach. These results emphasize the proposed scheme's efficiency in reducing latency, making it a strong candidate for time-sensitive SDN applications that require real-time data transmission.

This simulation shows how CRE finds, tracks, and modulates network paths in response to changing link latency using the topology shown in Figure 1. Ping starts conversation between source 1 and destination 2 when a new link is created. P1,2 = H1 → N1 → N2 → H2 and P2,1 = H2 → N2 → N1 → H1 are two initial paths the CRE sets. With the minimum hop count, these paths reach the shortest round-trip distance—130 ms. The first Ping encounters higher RTT because of the overhead involved in notifying the controller of new flows, computing best paths, and applying policies inside NFEs.

The CRE starts network monitoring combining RNN and RL after route establishment. By means of links L1,2 and L2,1, which link N1 to N2, a notable increase in delay is observed at the 10-second mark, so raising the delay from 20ms to 200ms and Ping RTT to 430ms. The CRE system detects these latency variances and constantly watches network conditions. In response, P2,1 makes the first route change choosing another path: P2,1 equals H2 → N2 → N3 → N1 → H1. This modification reduces the RTT to 260ms by the 18th Ping iteration, demonstrating the system's ability to adapt to dynamic network conditions and optimize performance. Figure 4 illustrates the delay monitoring for RTT between H1 and H2.

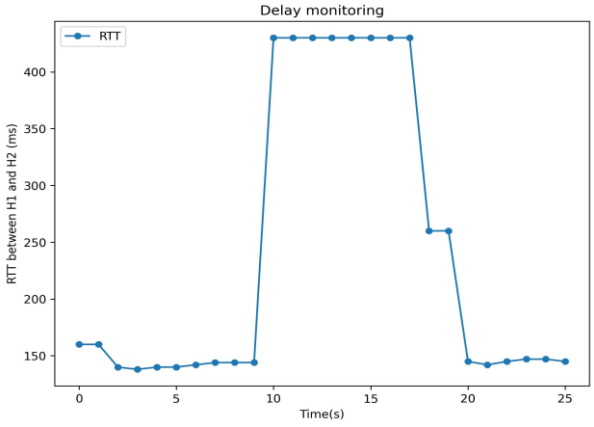

Figure 4. Delay Monitoring

Journal of Information Systems Engineering and Management
2025, 10(35s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

4.3 ESR-RLs Routing Efficiency

This analysis examines the impact of ESR-RL on routing efficiency and energy consumption, along with the effectiveness of GWCC in securing data transmission. Additionally, the role of SDSTOA in feature selection and load balancing is evaluated. The findings are compared with traditional methods to highlight improvements in network performance, security, and energy efficiency. A comprehensive evaluation helps demonstrate the significant advantages and potential limitations of the proposed integrated approach.

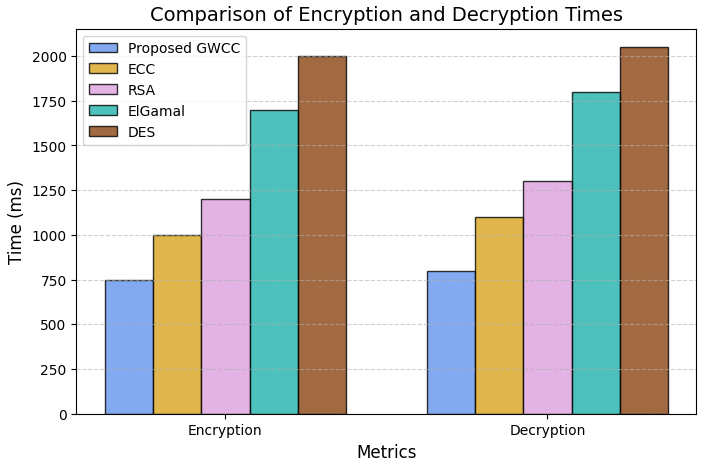

Figure 5. Encryption and Decryption Time Comparison

Figure 5 presents a performance comparison of various cryptographic algorithms based on their encryption and decryption times, including the proposed GWCC, ECC, RSA, ElGamal, and DES. Among these, GWCC demonstrates the shortest encryption and decryption durations, making it highly suitable for secure data transmission in real-time applications. Its efficiency in processing data ensures minimal delays, which is particularly beneficial for SDN, where performance and user experience are significantly impacted by latency. Rapid data encryption and decryption are essential for maintaining high throughput and low latency in network operations. While RSA and ElGamal are known for their strong security features, their longer processing times can be a limitation in high-speed networks. In contrast, GWCC strikes a balance between robust security and reduced computational overhead, making it a more effective choice for modern network environments.

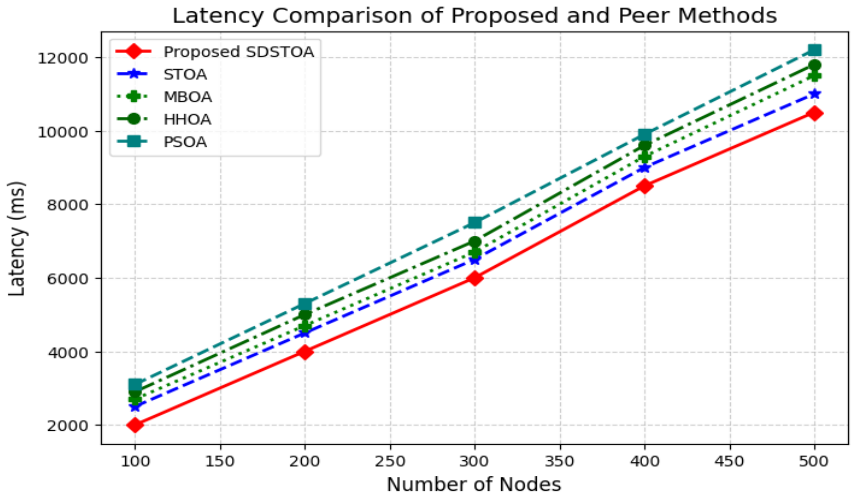

Figure 6. Latency Comparison

Journal of Information Systems Engineering and Management
2025, 10(35s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Figure 6 compares the latency performance of various optimization algorithms as the number of network nodes increases, including the proposed SDSTOA, along with STOA, MBOA, HHOA, and PSOA. The results indicate that SDSTOA consistently achieves the lowest latency across all tested node counts. This highlights its efficiency in managing network traffic and minimizing delays, even as the network scales. The ability of SDSTOA to maintain low latency with an increasing number of nodes demonstrates its scalability and effectiveness. Its low latency makes it highly suitable for large-scale network deployments where reducing delays is crucial for optimizing performance and enhancing user experience.

Table 1. Turn Around Time Comparison

Number of Nodes	Proposed SDSTOA (ms)	STOA (ms)	MBOA (ms)	HHOA (ms)	PSOA (ms)
100	3000	4000	5000	6000	7000
200	5000	7000	8000	10000	11000
300	7000	9000	11000	13000	14000
400	9500	11000	13000	15000	16000
500	12000	14000	16000	17000	17500

The comparative analysis of turn-around time across various routing methods shows notable differences in performance as the number of nodes increases. The proposed SDSTOA consistently achieves the lowest turn-around time, demonstrating its effectiveness in managing network traffic and processing requests efficiently. As the network size grows from 100 to 500 nodes, the turn-around time for STOA, MBOA, HHOA, and PSOA progressively increases, with PSOA experiencing the highest delay among all methods.

For smaller networks with 100 nodes, the difference between the proposed SDSTOA (3000ms) and other methods is relatively moderate. However, as the network scales, the performance gap becomes more pronounced, with PSOA reaching 17,500ms for 500 nodes—nearly 1.5 times higher than the proposed method. HHOA and MBOA also exhibit significant delays, indicating their inefficiency in handling larger networks. While STOA performs better than MBOA and HHOA, it still falls short compared to the proposed SDSTOA, making it less suitable for high-load scenarios.

This analysis underscores the proposed SDSTOA as the most scalable and efficient approach, maintaining significantly lower turn-around times than alternative methods. The increasing delays in PSOA and HHOA suggest that they are not well-suited for large-scale deployments, whereas the proposed SDSTOA offers superior adaptability and response efficiency in expanding network environments.

5. CONCLUSION

This study provides a detailed comparative analysis of routing optimization and security enhancement techniques in SDN. The proposed framework integrates ESR-RL for energy-efficient and adaptive routing, along with GWCC to ensure secure data transmission with minimal computational overhead. Extensive simulations demonstrate that the proposed approach significantly reduces latency, enhances network throughput, and improves encryption efficiency compared to traditional SDN routing, RL-based methods, genetic algorithm-based optimizations, and load-balancing techniques.

The findings indicate that the proposed SDSTOA consistently outperforms other methods in reducing turn-around time and end-to-end delay, making it highly suitable for large-scale and dynamic SDN environments. Additionally, the implementation of GWCC provides strong security without excessive processing overhead, offering a more efficient alternative to conventional encryption schemes such as RSA, ECC, and ElGamal. By integrating machine learning-based optimization with cryptographic security, the framework enhances network adaptability, making it well-suited for next-generation networking applications, including 5G, IoT, and cloud-based infrastructures.

Research Article

While the proposed approach offers significant advantages, further refinements could enhance scalability and fault tolerance in highly dynamic SDN environments. Future research may explore hybrid optimization techniques, the integration of federated learning for decentralized SDN control, and blockchain-enabled security frameworks to strengthen data integrity. The insights gained from this study contribute to the advancement of resilient, energy-efficient, and secure SDN architectures, addressing the evolving demands of modern digital communication networks.

REFRENCES

[1] R. Masoudi and A. Ghaffari, "Software defined networks: A survey," Journal of Network and Computer Applications, vol. 67, pp. 1–25, Mar. 2016, doi: 10.1016/j.jnca.2016.03.016.
[2] D. Kafetzis, S. Vassilaras, G. Vardoulias, and I. Koutsopoulos, "Software-Defined Networking Meets Software-Defined Radio in Mobile ad hoc Networks: State of the Art and Future Directions," IEEE Access, vol. 10, pp. 9989–10014, Jan. 2022, doi: 10.1109/access.2022.3144072.
[3] A. Swaminathan, M. Chaba, D. K. Sharma, and U. Ghosh, "GraphNET: Graph Neural Networks for routing optimization in Software Defined Networks," Computer Communications, vol. 178, pp. 169–182, Jul. 2021, doi: 10.1016/j.comcom.2021.07.025.
[4] O. Mohamed, T. Mahmoud, and A. Ali, "Software-defined network traffic routing optimization: A systematic literature review," Kafr El-Sheikh Journal of Information Sciences, vol. 4, no. 2, pp. 1–38, Nov. 2023, doi: 10.21608/kjis.2023.332129.
[5] J. Xie et al., "A survey of machine learning techniques applied to Software Defined Networking (SDN): Research issues and challenges," IEEE Communications Surveys & Tutorials, vol. 21, no. 1, pp. 393–430, Aug. 2018, doi: 10.1109/comst.2018.2866942.
[6] T. Mahboob, Y. R. Jung, and M. Y. Chung, "Optimized routing in software defined networks – a reinforcement learning approach," in Advances in intelligent systems and computing, 2019, pp. 267–278. doi: 10.1007/978-3-030-19063-7_22.
[7] F. Francois and E. Gelenbe, "Towards a cognitive routing engine for software defined networks," IEEE International Conference on Communications (ICC), pp. 1–6, May 2016, doi: 10.1109/icc.2016.7511138.
[8] F. F. Jurado-Lasso, K. Clarke, A. N. Cadavid, and A. Nirmalathas, "Energy-Aware routing for Software-Defined multihop wireless sensor networks," IEEE Sensors Journal, vol. 21, no. 8, pp. 10174–10182, Feb. 2021, doi: 10.1109/jsen.2021.3059789.
[9] E. Molina and E. Jacob, "Software-defined networking in cyber-physical systems: A survey," Computers & Electrical Engineering, vol. 66, pp. 407–419, May 2017, doi: 10.1016/j.compeleceng.2017.05.013.
[10] R. Imam, Q. M. Areeb, A. Alturki, and F. Anwer, "Systematic and Critical review of RSA based public key cryptographic schemes: past and present status," IEEE Access, vol. 9, pp. 155949–155976, Jan. 2021, doi: 10.1109/access.2021.3129224.
[11] V. A. Thakor, M. A. Razzaque, and M. R. A. Khandaker, "Lightweight Cryptography Algorithms for Resource-Constrained IoT Devices: A review, comparison and research opportunities," IEEE Access, vol. 9, pp. 28177–28193, Jan. 2021, doi: 10.1109/access.2021.3052867.
[12] Y.-R. Chen, A. Rezapour, W.-G. Tzeng, and S.-C. Tsai, "RL-Routing: an SDN routing algorithm based on deep reinforcement learning," IEEE Transactions on Network Science and Engineering, vol. 7, no. 4, pp. 3185–3199, Aug. 2020, doi: 10.1109/tnse.2020.3017751.
[13] M. Cicioğlu and A. Çalhan, "Energy-efficient and SDN-enabled routing algorithm for wireless body area networks," Computer Communications, vol. 160, pp. 228–239, Jun. 2020, doi: 10.1016/j.comcom.2020.06.003.
[14] A. Alidadi, S. Arab, and T. Askari, "A novel optimized routing algorithm for QoS traffic engineering in SDN-based mobile networks," ICT Express, vol. 8, no. 1, pp. 130–134, Dec. 2021, doi: 10.1016/j.icte.2021.12.010.
[15] Md. N. Pathan et al., "Priority based energy and load aware routing algorithms for SDN enabled data center network," Computer Networks, vol. 240, p. 110166, Dec. 2023, doi: 10.1016/j.comnet.2023.110166.
[16] J. Gong and A. Rezaeipanah, "A fuzzy delay-bandwidth guaranteed routing algorithm for video conferencing services over SDN networks," Multimedia Tools and Applications, vol. 82, no. 17, pp. 25585–25614, Jan. 2023, doi: 10.1007/s11042-023-14349-6.

Research Article

[17] S. Abbas, N. Javaid, A. Almogren, S. M. Gulfam, A. Ahmed, and A. Radwan, "Securing genetic algorithm enabled SDN routing for blockchain based internet of things," IEEE Access, vol. 9, pp. 139739–139754, Jan. 2021, doi: 10.1109/access.2021.3118948.

[18] K. Rui, H. Pan, and S. Shu, "Secure routing in the Internet of Things (IoT) with intrusion detection capability based on software-defined networking (SDN) and Machine Learning techniques," Scientific Reports, vol. 13, no. 1, Oct. 2023, doi: 10.1038/s41598-023-44764-6.

[19] Y. Zhang et al., "Multi-Path routing algorithm based on deep reinforcement learning for SDN," Applied Sciences, vol. 13, no. 22, p. 12520, Nov. 2023, doi: 10.3390/app132212520.

[20] N. Zabeehullah et al., "DQQS: Deep Reinforcement Learning-Based Technique for enhancing security and performance in SDN-IoT environments," IEEE Access, vol. 12, pp. 60568–60587, Jan. 2024, doi: 10.1109/access.2024.3392279.

[21] Y. Zhang, P. Li, W. Fan, and R. Wang, "QTSRA: A Q-learning-based Trusted Routing Algorithm in SDN Wireless Sensor Networks," 27th International Conference on Computer Supported Cooperative Work in Design, pp. 1881–1886, May 2024, doi: 10.1109/cscwd61410.2024.10580079.

[22] P. K. Udayaprasad et al., "Energy efficient optimized routing technique with distributed SDN-AI to large scale I-IoT networks," IEEE Access, vol. 12, pp. 2742–2759, Jan. 2024, doi: 10.1109/access.2023.3346679.

[23] K. Renuka, D. S. Roy, and K. H. K. Reddy, "An SDN empowered location aware routing for energy efficient next generation vehicular networks," IET Intelligent Transport Systems, vol. 15, no. 2, pp. 308–319, Jan. 2021, doi: 10.1049/itr2.12026.

[24] A. a. Z. Ibrahim, F. Hashim, A. Sali, N. K. Noordin, and S. M. E. Fadul, "A Multi-Objective routing mechanism for energy management optimization in SDN Multi-Control architecture," IEEE Access, vol. 10, pp. 20312–20327, Jan. 2022, doi: 10.1109/access.2022.3149795.

[25] R. Moosavi, S. Parsaeefard, M. A. Maddah-Ali, V. Shah-Mansouri, B. H. Khalaj, and M. Bennis, "Energy efficiency through joint routing and function placement in different modes of SDN/NFV networks," Computer Networks, vol. 200, p. 108492, Oct. 2021, doi: 10.1016/j.comnet.2021.108492.