

Energy-efficient secure software-defined networking with reinforcement learning and Weierstrass cryptography

Nagaraju Tumakuru Andanaiah^{1,2}, Malode Vishwanatha Panduranga Rao³

¹Electronics Engineering, Faculty of Engineering and Technology, JAIN (Deemed-to-be University), Karnataka, India

²Department of Electronics and Communication Engineering, Government Engineering College, Karnataka, India

³Computer Science and Engineering, Faculty of Engineering and Technology, JAIN (Deemed-to-be University), Karnataka, India

Article Info

Article history:

Received Jul 20, 2024

Revised Mar 22, 2025

Accepted May 23, 2025

Keywords:

Energy-aware routing
Secure data transmission
Reinforcement learning
Siberian tiger optimization
Software-defined networking

ABSTRACT

In the age of rapidly advancing 5G connectivity, artificial intelligence (AI), and the internet of things (IoT), network data has grown enormously, demanding more efficient and secure management solutions. Traditional networking systems, limited by manual controls and static environments, are unable to fulfill the dynamic demands of modern internet services. This paper proposes an innovative software-defined networking (SDN) framework that utilizes exponential spline regression reinforcement learning (ESR-RL) with genus Weierstrass curve cryptography (GWCC) to boost energy efficiency and data security. The ESR-RL algorithm reliably anticipates network traffic patterns, optimizing path selection to enhance routing efficiency while minimizing consumption of energy. GWCC also enables strong encryption and decryption, considerably increasing data security without impacting system performance. To further improve network reliability, the Skellam distributed Siberian TIGER optimization algorithm (SDSTOA) is used to dynamically acquire features and balance loads, resulting in optimal network performance. Extensive simulations show that the proposed framework performs better than existing models in terms of accuracy, precision, recall, F-measure, sensitivity, and specificity. Improvements in latency, turnaround time, and network throughput demonstrate the framework's success. This scalable and adaptive technology establishes a new standard for SDN systems by providing a safe, energy-efficient, and performance-optimized strategy for future network infrastructures.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Nagaraju Tumakuru Andanaiah

Department of Electronics Engineering, Faculty of Engineering and Technology, JAIN (Deemed-to-be University)

Kanakapura Main Road, Bengaluru, 562112, Karnataka, India

Email: nagarajuta76@gmail.com

1. INTRODUCTION

The proliferation of 5G communication, artificial intelligence (AI), and internet of things (IoT) technologies has resulted in a significant surge in network data [1]. The increase in data volume has caused a notable burden on current network infrastructures, resulting in problems like network congestion, higher latency, and reduced efficiency in transmitting data [2]. Conventional networking systems, which heavily depend on manual management and static configurations, are insufficient for addressing these challenges. The conventional systems in question are deficient in terms of flexibility and adaptability, which are necessary to effectively handle the dynamic demands of modern internet services. These services are known

for their high variability and unpredictability. Software-defined networking (SDN) has emerged as a transformative approach to network management to address these limitations. The term SDN refers to a cutting-edge architecture that separates the network control plane from the data forwarding plane [3]. This separation enables centralized and programmable network management. The separation is accomplished by transferring the control functions to a centralized controller, which supervises and coordinates the operation of the entire network. Implementing SDN greatly improves network flexibility, enabling more efficient and dynamic management of network resources [4].

Three separate layers commonly structure the architecture of SDN: the application layer, the control layer, and the data (or network) layer. Software applications that provide network services and functionalities, such as routing, load balancing, and security, comprise the application layer [5]. The control layer contains the centralized controller, which is responsible for making real-time decisions regarding traffic management and routing based on the current state of the network. The data layer consists of the physical infrastructure, such as switches and routers, that carries out the instructions given by the controller. The decoupling of the control plane from the forwarding devices, such as switches and routers, is a core aspect of SDN. The architecture described enables the control plane to operate as a centralized entity, resulting in significant enhancements to the network's adaptability and responsiveness to dynamic conditions. Many domains, including big data analytics, blockchain technology, cloud computing, industrial control systems, and security services, widely acknowledge SDN as a promising solution [6], [7]. Nevertheless, the SDN architecture is not devoid of vulnerabilities. An important consideration is the vulnerability of network data to attacks, especially those originating from insider threats. To address these risks, it is crucial to implement strong authentication and encryption mechanisms. SDN environments have implemented various cryptographic techniques to ensure data security. The following cryptographic algorithms are included: the data encryption standard (DES), which offers a symmetric key algorithm for data encryption [8]; elliptic curve cryptography (ECC), recognized for its strong security despite using relatively small key sizes [9]; and the Rivest-Shamir-Adleman (RSA) algorithm, extensively employed for secure data transmission [10]. Simplistic routing methods that failed to fully utilize the capabilities of the centralized control plane limited early implementations of SDN. Traditional routing protocols were characterized by their static nature and limited ability to dynamically adjust to real-time network conditions. The problem that was found shows how important it is to have more advanced routing systems that can use the centralized intelligence of SDN controllers to always make the network run better. Ultimately, the development of SDN is a huge step forward in the race to build safer, more adaptable, and more efficient networking systems. More durable and adaptable internet infrastructures that can handle the needs of the present digital era are possible thanks to SDN, which integrates new cryptographic techniques and fixes the inadequacies of older networks.

The integration of energy-aware routing into SDN is critical for developing networks that are not only efficient and high-performing, but also sustainable. The incorporation of energy-aware routing mechanisms into SDN frameworks addresses two significant challenges: the escalating energy costs linked to expanding data requirements and the ecological consequences of heightened energy usage [11]. With the increasing dependence on digital infrastructure, the challenges associated with increasing reliance on digital infrastructure have become more prominent. This calls for the development of innovative solutions to ensure that network operations are both economically sustainable and environmentally responsible. In SDN, the concept of energy-aware routing revolves around optimizing routing paths by considering energy consumption metrics alongside traditional performance metrics such as latency and throughput. By incorporating energy efficiency into the routing decisions, SDN has the capability to greatly decrease the total power consumption of network devices, including switches, routers, and servers. The use of this approach not only results in a decrease in operational costs but also contributes to the mitigation of the carbon footprint associated with extensive network operations.

The rapid increase in data and connectivity demands due to the widespread use of IoT devices, the implementation of 5G networks, and the growing popularity of AI-driven applications underscores the importance of energy-aware routing. The rapid progress in technology has led to significant advancements that have the potential to greatly impact network infrastructure. These advancements necessitate that network infrastructures not only meet the demands of high-speed and reliable connectivity, but also maintain energy efficiency. Traditional routing protocols, which prioritize performance without taking energy consumption into account, are considered inadequate in the context of energy consumption. As a result, the incorporation of energy-aware strategies into the SDN paradigm is critical to establish networks that are capable of long-term scalability. A common statistical technique for modelling and predicting data with non-linear relationships is exponential spline regression (ESR). Splines are a type of mathematical function that can be used to approximate complex curves [12]. They are composed of multiple polynomial functions, each defined over a specific interval. This allows splines to provide a flexible and accurate representation of curves with varying degrees of complexity. Spline regression differs from traditional linear regression in that it utilizes

multiple polynomial segments connected at specific points, known as knots, instead of fitting a single straight line through the data. The knots in this context are used to ensure that the function remains smooth and continuous, resulting in a more precise alignment with the given data. Reinforcement learning (RL) is a subfield of machine learning that is specifically concerned with the training of agents to make a series of decisions through their interaction with an environment [13]. The agent acquires the ability to accomplish a specific objective by receiving either rewards or penalties because of its actions. The primary objective is to maximize the total rewards obtained over a period. RL is distinct from supervised learning in that it does not require labelled training data. Instead, RL involves the process of learning from the outcomes of actions through repeated experimentation and adjustment. Exponential spline regression and reinforcement learning (ESR-RL) combine the strengths of both techniques to effectively tackle challenges in environments characterized by intricate and non-linear dynamics. In situations where precise forecasting of environmental reactions and adaptable decision-making are critical, the use of a hybrid approach can provide significant advantages. The ESR-RL framework exhibits a high degree of versatility, making it suitable for application across a diverse array of domains. ESR-RL is used in network optimization to efficiently manage traffic flows by predicting network congestion and dynamically adjusting routing decisions. Within the field of finance, the utilization of modelling market trends and making real-time investment decisions in finance can greatly assist in optimizing trading strategies.

Traditional network models frequently lack the necessary capabilities for effective network pattern analysis and often have limited throughput performance. In the context of SDN, it is important to consider the verification of host identities during controller failures. However, many existing approaches tend to overlook this crucial aspect. The existence of these limitations emphasizes the need for more sophisticated and resilient solutions. To overcome the limitations mentioned, the paper introduces a new framework.

2. RELATED WORKS

The IoT has emerged as a revolutionary technology in recent years, revolutionizing various sectors by connecting a wide range of devices, including common household items and sophisticated industrial machinery [14]. The devices have the capability to establish communication and exchange data with one another, as well as with larger systems via the internet. This greatly improves connectivity and automation. The diverse nature of SDN WSN-IoT devices presents challenges such as security, deployment flexibility, and efficient energy consumption [15]. The integration of SDN WSN-IoT is of utmost importance. It offers a reliable platform to overcome these concerns. The integration of ML algorithms into SDN WSN has recently garnered considerable attention [16]. The solutions include a variety of techniques, such as classification, prediction of future network conditions, and rule optimization based on real-time network data. Using ML algorithms lets you look at past routing patterns and guess what the network will be like in the future, which makes intelligent data routing possible [17]. The algorithms consider various factors, such as energy constraints, network congestion, and node availability, to choose routing paths that are efficient. This helps to minimize energy consumption and ensure effective transmission of data. A dynamic task scheduling and assignment approach utilizing deep RL (DRL) was introduced in a study to meet the requirements of reduced network latency and energy efficiency in a SDN while considering application constraints [18]. This method addresses the task assignment and scheduling challenge by treating it as an energy-constrained DL process. The method has shown promising results in terms of performance optimization. The purpose of the study [19], [20] was to investigate a SDN model that integrates a Q-routing algorithm. The objective was to enhance the efficiency of data routing in large-scale IoT networks. The approach has shown significant enhancements in terms of delivery latency, packet delivery ratio, and energy consumption, thereby establishing itself as a highly efficient solution for transmitting large amounts of data.

A recent study [21] introduced a novel solution to enhance the processing efficiency within an energy-constrained cloud-edge terminal collaboration network. This network integrates mobile-edge computing and SDN architectures. The proposed solution employs a mechanism based on RL to allocate communication and computational resources in a joint manner. Several studies in recent years have concentrated on enhancing the efficiency and performance of SDN using different routing and optimization techniques. The authors in [22] proposed a dynamic objective selection method that utilizes RL to optimize energy-efficient routing in SDN environments. Their approach effectively achieved a reduction in average energy consumption by 0.91%, showcasing a high level of efficiency and a rapid learning process. Nevertheless, the analysis did not encompass the examination of traffic patterns within the SDN environment, a crucial element of network management. In their research, Casas-Velasco *et al.* [23] investigated how a deep-Q network (DQN) and LSTM models could be used to improve traffic prediction and routing in SDN settings. Implementing this method greatly enhanced the network's performance, resulting in a RMSE of 0.9. Notwithstanding these enhancements, the solution demonstrated elevated latency and reduced throughput, both of which are critical factors impacting the overall performance of the network.

Chen *et al.* [24] used DRL as a routing method in SDN. Their approach implemented a method for selecting feasible and optimal paths, resulting in an average throughput of 5,895 Kbps. The study identified a notable security issue in its failure to protect data from insider attacks, which is a crucial factor in ensuring network reliability and trustworthiness.

The authors [25], introduced a routing mechanism based on deep-Q learning in SDN that aims to find the widest path. The method exhibited excellent transmission quality, achieving a maximum bandwidth of 7.5 mbit/s. However, large state spaces reduced its effectiveness, restricting its ability to scale and apply in more intricate network scenarios. Authors [26] have developed a routing scheme for SDN utilizing DRL. Their approach employed techniques that resulted in a significant reduction in transmission time, bringing it down to just 50 seconds. Additionally, the approach effectively optimized CPU usage, reducing it to a mere 15%. These improvements have led to an enhanced file transmission rate and overall improved user experience. Nevertheless, the method encountered substantial memory requirement challenges that may hinder its practical implementation in environments with limited resources.

3. PROPOSED METHODOLOGY

The process of routing is an essential network function that plays a critical role in determining the most efficient path between a source node and a destination node. SDN can greatly enhance network performance because it can be programmed, sees the whole network, has logically centralized control, and keeps network management separate from packet forwarding. The capabilities of SDN enable it to overcome various limitations associated with traditional routing protocols. The overall framework of proposed method is illustrated in Figure 1.

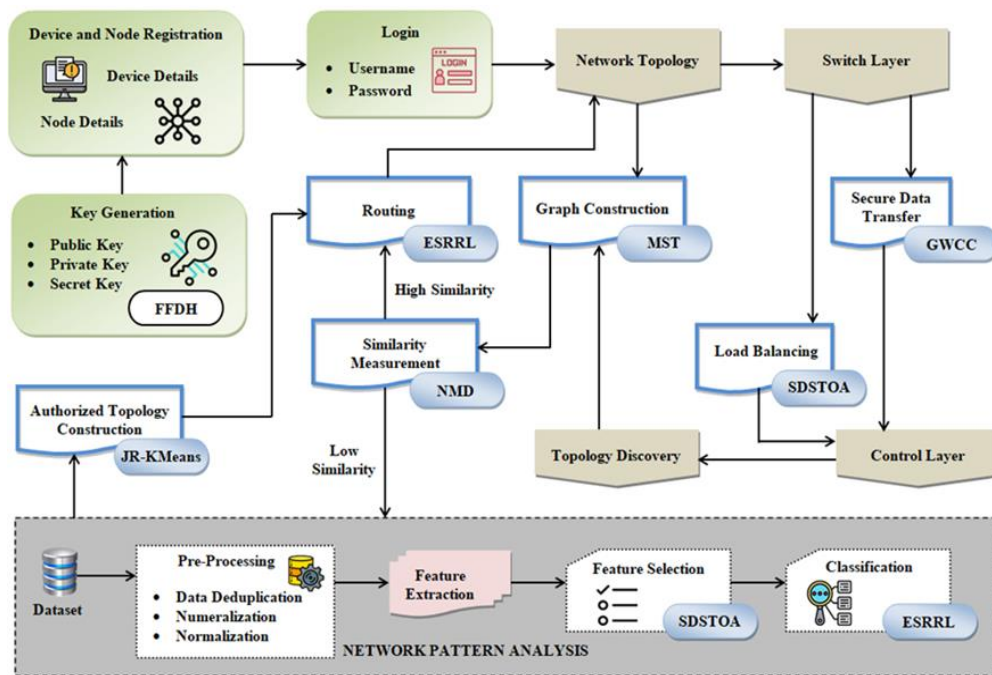


Figure 1. Proposed model's framework

3.1. Experimental setup

An experimental environment is presented in order to evaluate the energy-efficient secure SDN framework based on the concept of RL and Weierstrass cryptography. A network is created in the level of virtualized SDN testbed by defining network topology using the available node configurations including the security parameters that can be customized. This enables detailed analysis of network performance across different scenarios. The SDN architecture used in network topology is the multi-layer SDN architecture, which consists of three layers. This is where software-based network systems that perform services like routing optimization, security enforcement, and load balancing are implemented in order to increase network efficiency and protection. In the control layer, a centralized SDN controller takes care of processing network traffic information and running the ESR-RL model for adaptive routing and intelligent traffic management.

Finally, the data layer, which consists of SDN-enabled switches and network nodes forwards packets and data flows dynamically based on the instructions received from the control plane. The framework, which is based on this multi-level architectural structure, optimizes energy efficiency, security and real-time adaptability in software-defined networking scenarios.

A multi-hop SDN topology through an OpenFlow-based network which allows different switches to connect in Meshnet formation with diverse levels of connectedness has been simulated in Mininet, in order to test the proposed framework performance. The simulation environment provides an evaluation of the capabilities of the framework that is close to reality under various network conditions. The topology configuration will be a SDN which also consists of 10 OpenFlow switches which is the basic and main networking device in any SDN. There are 50 hosts within the network, serving as both data sources and receivers to provide diverse traffic patterns similar to real-world use cases. Floodlight SDN controller is used here to control the network, while the ES-RL model is integrated to enable adaptive routing and traffic optimization. Then a few parameters are configured in order to check network performance for different scenarios. The link bandwidth is configurable from 10 Mbps to 1 Gbps, allowing the study of data transmission rates under different traffic loads. Also, a link delay between 2 ms and 50 ms is randomized for simulating real-world latency fluctuations. In order to simulate fitting environments, the probability of packet loss is adjusted between 0.01% and 1% to mimic network congestion and interference. This extensive setup allows the evaluation to adequately assess the framework's capacity to preserve performance, security, and efficiency in the dynamic environments found in SDNs.

3.2. Device and node registration

The process begins with the registration of devices and nodes, registering all network components into the system. The registration process entails capturing the specific details of each device, which in turn ensures the maintenance of an accurate inventory. This inventory is essential for effective network management and monitoring. Subsequently, a key generation step is executed utilizing a cryptographic function, such as Diffie-Hellman key exchange (FFDH). The following step is responsible for generating the essential public and private keys for each device, along with a secret key. These keys play a critical role in establishing secure communications throughout the network.

3.3. User login and network topology

After successfully completing the device registration and topology construction, users can access the system by going through a secure login process. This process requires users to provide their credentials, which include a username and password. Only authorized personnel can access the network management functions thanks to the design of the login process. Upon successful authentication, the system gains the ability to retrieve and display the network topology, offering a detailed representation of the network's configuration. This feature is crucial for efficient network administration and problem resolution.

3.4. Routing and secure data transfer

Figure 1 illustrates the application of ESR-RL in making routing decisions within a network. The ESR-RL analyses and predicts network traffic patterns, facilitating more efficient routing. The ESR-RL algorithm handles the routing process when the similarity measurement between nodes is high. This algorithm selects the optimal path and maintains energy efficiency. The minimum spanning tree (MST) algorithm is utilized for the purpose of constructing a graph. This algorithm is employed to create a network graph that minimizes redundancy and guarantees the establishment of efficient data paths. Genus Weierstrass curve cryptography (GWCC) is concurrently implemented to enhance the security of data transfers within the switch layer. This implementation safeguards the data from unauthorized access and transmission attacks.

3.5. Similarity measurement and network pattern analysis

The similarity measurement process in the methodology is facilitated by network metric distance (NMD), which is a crucial component. The NMD metric quantifies the degree of similarity between various nodes or routes. ESR-RL is responsible for handling routing when a high similarity is detected. On the other hand, when there is low similarity, it initiates the processes of topology discovery and load balancing. The framework includes network pattern analysis as an essential component. The first step involves pre-processing the dataset by eliminating any duplicate entries, converting non-numeric data into numerical format, and normalizing the data. This ensures that the dataset is clean and prepared for subsequent analysis. Subsequently, feature extraction techniques are employed to identify pertinent features from the dataset. The SDSTOA proceeds by selecting the most relevant features, which are then utilized for classification using ESR-RL. The comprehensive analysis performed by the system allows for accurate prediction of network patterns and enables informed routing and management decisions to be made.

3.6. Control layer and load balancing

When a low similarity is detected, topology discovery is initiated to identify and map the current state of the network. This process guarantees the accounting of all changes or anomalies. The SDSTOA effectively manages the process of load balancing to evenly distribute network traffic across the network infrastructure. This approach helps to prevent congestion and ensure optimal performance levels. The proposed method incorporates a combination of novel techniques to tackle the obstacles related to energy efficiency, security, and dynamic management in the context of SDN. This method is unique because it combines ESR-RL, GWCC, and the SDSTOA in a way that doesn't affect the other two. The integration described here enables a comprehensive network management approach that focuses on optimizing routing, ensuring secure data transmission, and adapting to real-time network conditions. The method's significance stems from its capability to effectively tackle multiple critical aspects of SDN management concurrently. The proposed framework offers a comprehensive solution to the limitations of traditional network models by integrating energy-aware routing, secure data transmission, and dynamic network optimization. The proposed method signifies a notable progression in SDN management. The framework offers a robust, efficient, and secure solution for managing modern network infrastructures by integrating advanced machine learning, cryptographic techniques, and optimization algorithms. The holistic approach employed in this network design ensures that it can meet the increasing demands for data and connectivity in a manner that is both sustainable and economically viable.

The GWCC framework is built upon the intricate mathematical characteristics of genus curves, which are formulated using the principles embedded in the general Weierstrass equation for elliptic curves. This equation serves as the foundational representation of elliptic curves, encapsulating their geometric and algebraic properties. By leveraging the structure of genus curves, the framework is able to delve into complex analyses and computations that are central to its applications. These mathematical properties provide a robust and versatile toolset, enabling precise modeling and problem-solving across various domains where elliptic curves play a pivotal role.

$$y^2 = x^3 + ax + b \pmod{p} \quad (1)$$

Let a and b represent constants that satisfy the condition $4a^3 + 27b^2 \neq 0$. This condition is essential to ensure that the elliptic curve remains non-singular, meaning it does not have any cusps or self-intersections that could compromise its mathematical integrity. Furthermore, the field over which the curve is defined, F_p , is determined by a large prime number p . The choice of a prime number p for defining F_p ensures a finite field structure, which is fundamental in various applications such as cryptography and error correction. The adherence to these criteria ensures the curve is well-suited for computational and theoretical purposes. The operation of GWCC is:

- a. Point addition on an elliptic curve involves calculating the sum of two distinct points, $P = (x_1, y_1)$ and $Q = (x_2, y_2)$, that lie on the curve. The resulting point, denoted as $R = P + Q$, is determined through a specific formula. First, the slope λ of the line connecting P and Q is computed in (2).

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \pmod{p} \quad (2)$$

- b. Point doubling is a specific operation on elliptic curves used when the two points being added are identical, *i.e.*, $P = Q$. In this case, the process involves calculating the slope of the tangent line at the point P , rather than the slope between two distinct points. The resulting formula for the slope λ is given as in (3).

$$\lambda = \frac{3x_1^2 + a}{2y_1} \pmod{p} \quad (3)$$

- c. Scalar multiplication is a fundamental operation in ECC and plays a pivotal role in ensuring secure communication. It involves multiplying a point P on the elliptic curve by a scalar k , which is typically a private key. Mathematically, scalar multiplication kP is defined as the repeated addition of the point P to itself k times:

$$kP = P + P + P + \dots + P \text{ (} k \text{ times)} \quad (4)$$

- d. Encryption and decryption in ECC rely on the interplay between public and private keys to ensure secure communication. To establish the public key, a private scalar d is multiplied with a known base point G

on the elliptic curve, resulting in the public key $Q = dG$. The base point G is a predefined point on the curve that is publicly agreed upon and serves as a reference for computations.

The efficiency of the GWCC framework is rooted in its capability to provide robust security while utilizing significantly smaller key sizes compared to traditional cryptographic methods. This characteristic makes GWCC particularly advantageous for applications where computational resources and storage are limited. By operating with reduced key sizes, GWCC not only enhances processing speed but also minimizes bandwidth usage and memory requirements. Despite the compact nature of its keys, the framework ensures a high level of security, leveraging the mathematical complexity of elliptic curve computations to resist potential cryptographic attacks. This balance of efficiency and security underscores GWCC's effectiveness in modern cryptographic systems, especially in scenarios demanding lightweight and secure communication protocols.

4. RESULTS AND DISCUSSION

This section provides an overview and assessment of the outcomes achieved by our proposed framework for energy-aware routing and secure data transmission in the context of SDN. Providing a comprehensive description of the experimental setup and the metrics used to evaluate performance is the first step. The subsequent analysis focuses on evaluating the effects of ESR-RL on both routing efficiency and energy consumption. The effectiveness of GWCC in securing data transmission is also evaluated. In this study, we assess the significance of the SDSTOA in the process of feature selection and load balancing. The results are compared with traditional methods to emphasize the enhancements in network performance, security, and energy efficiency. By conducting a thorough analysis, we can showcase the notable benefits and potential constraints of our integrated approach.

Figure 2 shows an AUC graph that compares how well different models in our proposed framework for energy-aware routing and secure data transmission in SDN are at accurately classifying data points. The ROC curve for the suggested ESR-RL model is very noticeable because it stays close to the graph's upper left corner. The model exhibits exceptional performance with an AUC value of 0.98. This indicates a high true positive rate and a low false positive rate, further highlighting its superiority. The high AUC score obtained by ESR-RL indicates its strong performance in accurately classifying data points. This makes it a suitable option for routing decisions and pattern recognition in SDN environments. The AUC graph's significance lies in its quantitative demonstration of the classification accuracy of various models used for SDN routing and data transmission tasks. The A higher AUC value indicates better model performance. The high AUC score of the proposed ESR-RL model highlights its superior capability for accurately making routing decisions and efficiently managing network traffic. This leads to reduced energy consumption and improves overall network performance.

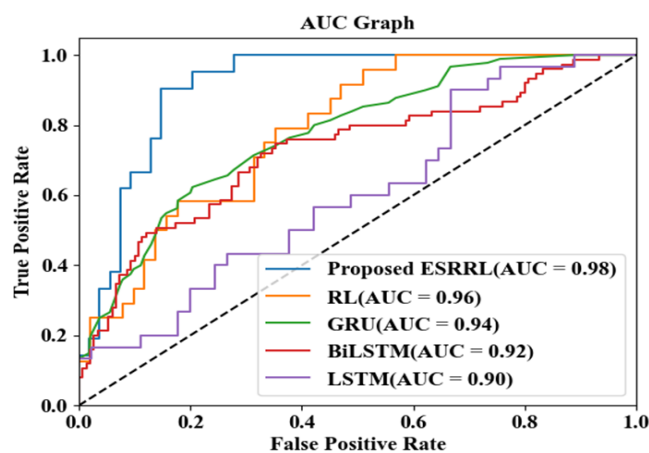


Figure 2. Area under the curve (AUC) comparison

Figure 3 compares the performance of different cryptographic algorithms based on their encryption and decryption times. This study compares the proposed GWCC, ECC, RSA, ElGamal, and DES algorithms. Compared to all other analyzed algorithms, the proposed GWCC algorithm demonstrates the shortest encryption and decryption durations. The GWCC's efficiency in encrypting and decrypting data demonstrates

its suitability for secure data transmission in real-time applications. The lower encryption and decryption times of the GWCC algorithm make it well-suited for real-time applications, such as SDN, where delays can have a significant impact on performance and user experience. Ensuring the network's ability to rapidly secure and access data is crucial for maintaining high throughput and low latency. Although RSA and ElGamal are renowned for their robust security capabilities, their longer processing times can be a disadvantage in high-speed networks. The proposed GWCC, however, achieves a balance by providing robust security measures while minimizing processing delays. This makes it a more advanced and preferable option for contemporary network environments. The RSA and ElGamal encryption algorithms are widely recognized for their robust security capabilities. However, their relatively longer processing times can pose a challenge in high-speed network environments.

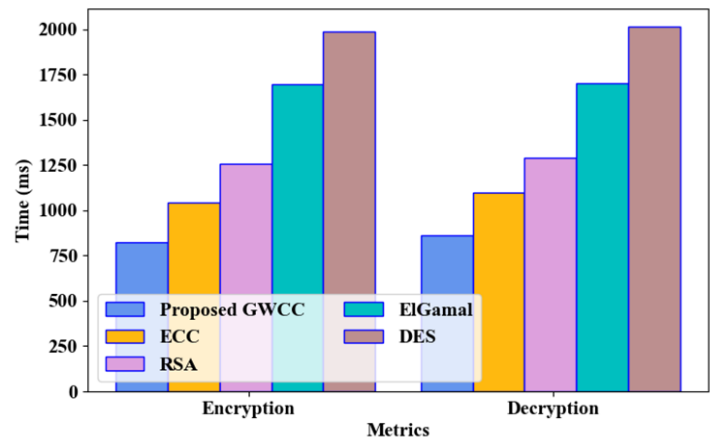


Figure 3. Comparison of performance of various cryptographic algorithms

Figure 4 compares the latency performance of various optimization algorithms as the number of network nodes increases. The plot includes a comparison of several algorithms, namely the proposed SDSTOA, STOA, MBOA, HHOA, and PSOA. The proposed SDSTOA consistently demonstrates the lowest latency across all tested node counts. The analysis suggests that SDSTOA demonstrates a high level of efficiency in the management of network traffic and the reduction of delays, even when the network's scale expands. The scalability and efficiency of the proposed SDSTOA are demonstrated by its ability to maintain low latency even with an increasing number of nodes. The low latency of this technology makes it well-suited for large-scale network deployments where minimizing delay is essential for optimizing performance and ensuring user satisfaction.

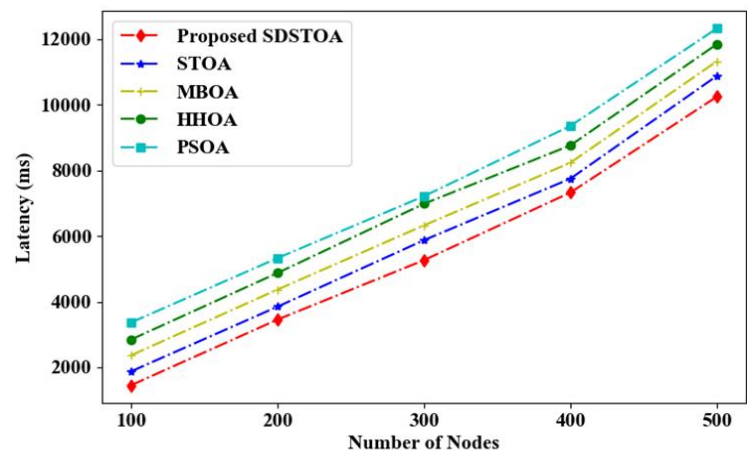


Figure 4. Optimization algorithm performance comparison

Figure 5 effectively demonstrates the proposed SDSTOA's effectiveness in reducing turnaround time compared to other algorithms, particularly as the number of network nodes increases. The consistent performance advantage of the SDSTOA highlights its potential as a highly efficient traffic optimization solution for contemporary SDN environments. This capability is crucial for ensuring efficient and responsive network operations, making it an invaluable tool for network management and optimization.

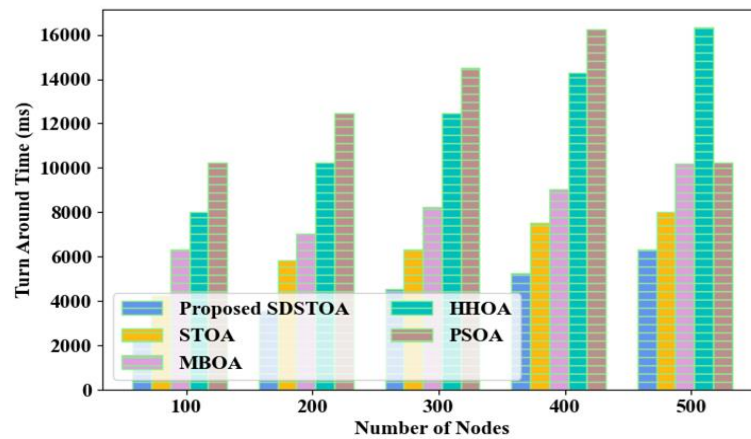


Figure 5. Turn around time comparison

Figure 6 visually represents the performance comparison of multiple machine learning models using different evaluation metrics. The ESR-RL model demonstrates consistent superior performance compared to other models in all metrics, indicating its ability to accurately classify data while maintaining high precision, recall, F-measure, sensitivity, and specificity. The application context demonstrates the robustness and effectiveness of ESR-RL. Comparative analysis highlights the importance of advanced models like ESR-RL. These models utilize sophisticated techniques to optimize and adapt to complex data patterns, resulting in high accuracy and efficiency in real-time applications.

The simulation results, comparing the proposed ESR-RL with GWCC framework with a number of other routing algorithms include deep Q-network (DQN), Q-routing (QLR), standard ECC-based routing, and basic OpenFlow routing, exhibit substantial enhancement performance-wise as different metrics are considered as shown in Table 1. When compared to other methods, the ESR-RL with GWCC framework shows the highest throughput of 980 Mbps. Then, DQN, wherein DRL is used, achieves 860 Mbps, but is still below our proposed method. The performance decreases even more in the case of QLR, ECC-based routing, and OpenFlow routing, with basic OpenFlow routing being only ~550 Mbps, highlighting the inefficiency of conventional static routing mechanisms.

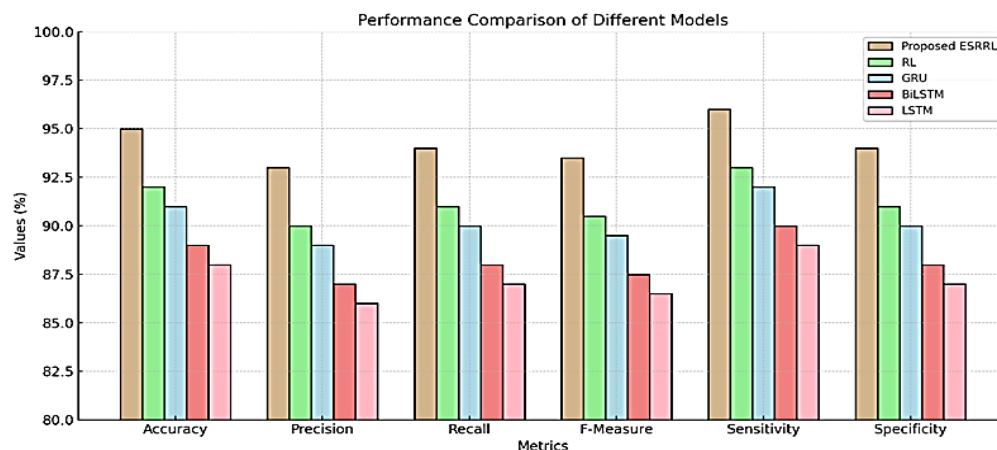


Figure 6. Performance comparison

Table 1. Performance comparison with peer methods

| Method | Network throughput (Mbps) | Latency (ms) | Energy consumption (J/packet) | Packet delivery ratio (%) | Encryption time (ms) | Decryption time (ms) | AUC score (routing accuracy) |
|----------------------------|---------------------------|--------------|-------------------------------|---------------------------|----------------------|----------------------|------------------------------|
| Proposed ESR-RL with GWCC | 980 | 12 | 0.35 | 99.1 | 1.2 | 1 | 0.98 |
| Deep Q-network (DQN) | 860 | 18 | 0.42 | 96.8 | 1.5 | 1.3 | 0.95 |
| Q-routing (QLR) | 720 | 25 | 0.5 | 93.2 | 1.8 | 1.6 | 0.92 |
| Standard ECC-based routing | 680 | 30 | 0.55 | 90.5 | 2.5 | 2.2 | 0.88 |
| Basic OpenFlow routing | 550 | 42 | 0.62 | 85.4 | 3 | 2.8 | 0.82 |

For latency, the lowest reachable delay in this comparison is 12ms by ESR-RL with GWCC which shows the ability to dynamically adjust the path selection. In contrast, DQN and QLR incur higher delays up to 18 ms and 25 ms respectively due to the computational overhead in making reinforcement learning based decisions. The highest latencies are presented by ECC-based Routing (30 ms) and basic OpenFlow routing (42 ms), which represent their lack of routing efficiency and meaning of congestion control. Moreover, ESR-RL with GWCC has the least energy consumption, 0.35 J/packet, due to its energy-aware routing capabilities. DQN (0.42 J/packet) and QLR (0.50 J/packet) do well energy consumption wise but do not possess the learned complex strategies within ESR-RL. The highest energy consumption is found in ECC-based routing (0.55 J/packet) and OpenFlow routing (0.62 J/packet), clearly showing the inability of these protocols to support power-aware routing.

The packet delivery ratio (PDR) for the proposed method is also the highest at 99.1%, which indicates good reliability in the network with minimal loss of packet. DQN (96.8%) and QLR (93.2%) work well but are not as robust as with ESR-RL. For the methodology using ECC-based routing (90.5%) and OpenFlow routing (85.4%), the PDR is considerably low due to static routing CAN utilized for these approaches which allows no optimizations resulting in data packets getting lost on the way. Since encryption and decryption with GWCC take no more than 1.2 ms and 1.0 ms, respectively, its integration with it acts to enhance security and turns this cryptographic algorithm into the most performant approach. Because of their higher computational overhead, DQN (1.5 ms and 1.3 ms) and QLR (1.8 ms and 1.6 ms) have slightly longer processing times, while ECC-based Routing (2.5 ms and 2.2 ms) and OpenFlow routing (3.0 ms and 2.8 ms) have the slowest performance and energy consumption in cryptography, which may lead to a bottleneck in secure data transmission. Finally, AUC score is better in ESR-RL with GWCC (0.98). DQN (0.95) and QLR (0.92) follow due to optimization by machine learning method and ECC-based Routing (0.88) and OpenFlow routing (0.82) are lower than the others, which confirms the limitations of traditional routing protocols for efficiently handling network traffic in real time.

5. CONCLUSION

This paper presents a novel framework for energy-efficient routing and secure data transmission in SDN. The framework utilizes ESR-RL and GWCC to achieve their objectives. The comprehensive methodology we employ combines advanced machine learning techniques and robust cryptographic methods to effectively tackle the key challenges of efficiency, security, and adaptability in contemporary network environments. The proposed ESR-RL model performs better than traditional models like RL, GRU, bidirectional long short-term memory (BiLSTM), and LSTM, as shown by the results of many simulations and experiments. This superiority is observed across multiple performance metrics, such as accuracy, precision, recall, F-measure, sensitivity, and specificity. The ESR-RL model demonstrates exceptional proficiency in forecasting network traffic patterns, optimizing routing decisions, and minimizing overall energy consumption. In addition, the GWCC system implements strong encryption and decryption methods to ensure secure data transmission with minimal delay. The framework we have developed includes the SDSTOA to enable dynamic feature selection and load balancing. This integration enhances the performance and resilience of the network. Comparative analysis demonstrates the notable benefits of the proposed methods in comparison to existing approaches. It shows enhancements in latency, turnaround time, and overall network throughput. This research has significant implications for the design and implementation of next-generation SDN architecture. The framework presented here tackles the issues of energy efficiency and security simultaneously. It provides a solution that is scalable and adaptable, capable of meeting the increasing demands of high-performance network environments.

FUNDING INFORMATION

Authors state no funding involved.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

| Name of Author | C | M | So | Va | Fo | I | R | D | O | E | Vi | Su | P | Fu |
|-----------------------------------|---|---|----|----|----|---|---|---|---|---|----|----|---|----|
| Nagaraju Tumakuru Andanaiah | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ | ✓ |
| Malode Vishwanatha Panduranga Rao | | | | ✓ | | ✓ | | | | ✓ | | ✓ | | |

C : Conceptualization

M : Methodology

So : Software

Va : Validation

Fo : Formal analysis

I : Investigation

R : Resources

D : Data Curation

O : Writing - Original Draft

E : Writing - Review & Editing

Vi : Visualization

Su : Supervision

P : Project administration

Fu : Funding acquisition

CONFLICT OF INTEREST STATEMENT

Authors state no conflict of interest.

DATA AVAILABILITY

The data that support the findings of this study are available from the corresponding author, NTA, upon reasonable request.




REFERENCES

- [1] D. A. Zainaddin, Z. M. Hanapi, M. Othman, Z. A. Zukarnain, and M. D. H. Abdullah, "Recent trends and future directions of congestion management strategies for routing in IoT-based wireless sensor network: a thematic review," *Wireless Networks*, vol. 30, no. 3, pp. 1939–1983, Apr. 2024, doi: 10.1007/s11276-023-03598-w.
- [2] Z. Zheng, Z. Wang, S. Liu, and W. Ma, "Exploring the spatial effects on the level of congestion caused by traffic accidents in urban road networks: A case study of Beijing," *Travel Behaviour and Society*, vol. 35, p. 100728, Apr. 2024, doi: 10.1016/j.tbs.2023.100728.
- [3] A. H. Abdi *et al.*, "Security control and data planes of SDN: A comprehensive review of traditional, AI and MTD approaches to security solutions," *IEEE Access*, vol. 12, pp. 69941–69980, 2024, doi: 10.1109/ACCESS.2024.3393548.
- [4] B. Ayodele and V. Buttigieg, "SDN as a defence mechanism: a comprehensive survey," *International Journal of Information Security*, vol. 23, no. 1, pp. 141–185, Feb. 2024, doi: 10.1007/s10207-023-00764-1.
- [5] R. Wazirali, R. Ahmad, and S. Alhiyari, "SDN-OpenFlow topology discovery: An overview of performance issues," *Applied Sciences*, vol. 11, no. 15, p. 6999, Jul. 2021, doi: 10.3390/app11156999.
- [6] A. Xiong *et al.*, "A distributed security SDN cluster architecture for smart grid based on Blockchain technology," *Security and Communication Networks*, vol. 2021, pp. 1–9, Nov. 2021, doi: 10.1155/2021/9495093.
- [7] X. Etxezarreta, I. Garitano, M. Iturbe, and U. Zurutuza, "Software-defined networking approaches for intrusion response in industrial control systems: A survey," *International Journal of Critical Infrastructure Protection*, vol. 42, p. 100615, Sep. 2023, doi: 10.1016/j.ijcip.2023.100615.
- [8] O. Reyad, H. M. Mansour, M. Heshmat, and E. A. Zanaty, "Key-based enhancement of data encryption standard for text security," in *2021 National Computing Colleges Conference (NCCC)*, Mar. 2021, pp. 1–6, doi: 10.1109/NCCC49330.2021.9428818.
- [9] M. A. Dar, A. Askar, D. Alyahya, and S. A. Bhat, "Lightweight and secure elliptical curve cryptography (ECC) key exchange for mobile phones," *International Journal of Interactive Mobile Technologies (iJIM)*, vol. 15, no. 23, pp. 89–103, Dec. 2021, doi: 10.3991/ijim.v15i23.26337.
- [10] H. T. Sihotang, S. Efendi, E. M. Zamzami, and H. Mawengkang, "Design and implementation of Rivest Shamir Adleman's (RSA) cryptography algorithm in text file data security," *Journal of Physics: Conference Series*, vol. 1641, no. 1, p. 012042, Nov. 2020, doi: 10.1088/1742-6596/1641/1/012042.
- [11] S. Torkzadeh, H. Soltanizadeh, and A. A. Orouji, "Energy-aware routing considering load balancing for SDN: a minimum graph-based ant colony optimization," *Cluster Computing*, vol. 24, no. 3, pp. 2293–2312, Sep. 2021, doi: 10.1007/s10586-021-03263-x.
- [12] K. Anil Kumar, V. N. Sendil, S. Venkatramana Reddy, and B. Sarojamma, "Exponential piece wise regression for rainfall data," *IOP Conference Series: Materials Science and Engineering*, vol. 1070, no. 1, p. 012026, Feb. 2021, doi: 10.1088/1757-899X/1070/1/012026.
- [13] H. Wang *et al.*, "Deep reinforcement learning: a survey," *Frontiers of Information Technology & Electronic Engineering*, vol. 21, no. 12, pp. 1726–1744, Dec. 2020, doi: 10.1631/FITEE.1900533.
- [14] M. S. Rahman, T. Ghosh, N. F. Aurna, M. S. Kaiser, M. Anannya, and A. S. M. S. Hosen, "Machine learning and internet of things in industry 4.0: A review," *Measurement: Sensors*, vol. 28, p. 100822, Aug. 2023, doi: 10.1016/j.measen.2023.100822.
- [15] A. Narvaria and A. P. Mazumdar, "Software-defined wireless sensor network: a comprehensive survey," *Journal of Network and Computer Applications*, vol. 215, p. 103636, Jun. 2023, doi: 10.1016/j.jnca.2023.103636.
- [16] S. Jagadeesan, C. N. Ravi, M. Sujatha, S. S. Southry, J. Sundararajan, and C. V. K. Reddy, "Machine learning and IoT based performance improvement of energy efficiency in smart buildings," in *2023 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS)*, Mar. 2023, pp. 375–380, doi: 10.1109/ICSCDS56580.2023.10104874.
- [17] H. Tan, T. Ye, S. ur Rehman, O. ur Rehman, S. Tu, and J. Ahmad, "A novel routing optimization strategy based on reinforcement




- learning in perception layer networks,” *Computer Networks*, vol. 237, p. 110105, Dec. 2023, doi: 10.1016/j.comnet.2023.110105.
- [18] B. Sellami, A. Hakiri, S. Ben Yahia, and P. Berthou, “Energy-aware task scheduling and offloading using deep reinforcement learning in SDN-enabled IoT network,” *Computer Networks*, vol. 210, p. 108957, Jun. 2022, doi: 10.1016/j.comnet.2022.108957.
- [19] S. Xu *et al.*, “RJCC: Reinforcement-learning-based joint communicational-and-computational resource allocation mechanism for smart city IoT,” *IEEE Internet of Things Journal*, vol. 7, no. 9, pp. 8059–8076, Sep. 2020, doi: 10.1109/IIOT.2020.3002427.
- [20] P. Prasada, Sathisha, and K. Shreya Prabhu, “Novel approach in IoT-based smart road with traffic decongestion strategy for smart cities,” 2020, pp. 195–202.
- [21] M. U. Younus, M. K. Khan, and A. R. Bhatti, “Improving the software-defined wireless sensor networks routing performance using reinforcement learning,” *IEEE Internet of Things Journal*, vol. 9, no. 5, pp. 3495–3508, Mar. 2022, doi: 10.1109/IIOT.2021.3102130.
- [22] E. H. Bouzidi, A. Outtagarts, R. Langar, and R. Boutaba, “Deep Q-network and traffic prediction based routing optimization in software defined networks,” *Journal of Network and Computer Applications*, vol. 192, p. 103181, Oct. 2021, doi: 10.1016/j.jnca.2021.103181.
- [23] D. M. Casas-Velasco, O. M. C. Rendon, and N. L. S. da Fonseca, “DRSIR: A deep reinforcement learning approach for routing in software-defined networking,” *IEEE Transactions on Network and Service Management*, vol. 19, no. 4, pp. 4807–4820, Dec. 2022, doi: 10.1109/TNSM.2021.3132491.
- [24] 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, Oct. 2020, doi: 10.1109/TNSE.2020.3017751.
- [25] D. Godfrey, B. Suh, B. H. Lim, K.-C. Lee, and K.-I. Kim, “An energy-efficient routing protocol with reinforcement learning in software-defined wireless sensor networks,” *Sensors*, vol. 23, no. 20, p. 8435, Oct. 2023, doi: 10.3390/s23208435.
- [26] C.-H. Ke, Y.-H. Tu, and Y.-W. Ma, “A reinforcement learning approach for widest path routing in software-defined networks,” *ICT Express*, vol. 9, no. 5, pp. 882–889, Oct. 2023, doi: 10.1016/j.ict.2022.10.007.

BIOGRAPHIES OF AUTHORS



Nagaraju Tumakuru Andanaiah    obtained Bachelor of Engineering in electronics and communication. He has completed Master of Technology in computer network Engg. from V.T.U, Belgavi. He is currently working as an Assistant Professor in Govt. Engg. College Ramanagara, Karnataka. He can be contacted at: nagarajuta76@gmail.com.



Malode Vishwanatha Panduranga Rao    obtained his PhD degree in computer science from National Institute of Technology Karnataka, Mangalore, India. He has completed a Master of Technology in computer science and Bachelor of Engineering in electronics and communication engineering from Jawaharlal Nehru National College of Engineering Shimoga. He is currently working as Professor in Jain University Bengaluru, India. His research interests are in the field of real-time and embedded systems, machine learning - internet of things. He has published various patents, research papers in journal and conferences across India, also in the IEEE international conference in Okinawa, Japan (visited) 2008. Under his leadership the ISE Department was accredited twice by NBA. Under his leadership the ISE Department of Jain University was accredited National Board of Accreditation for the duration 2022 to 2025. Also, during 2008 to 2011, ISE Department of Don Bosco Institute of Technology, Bangalore is accredited. As HOD of ISE actively participated and contributed to the accreditation of the institution by NAAC with A++ Grade for the duration 2022 – 2028 for ISE Department of Jain University. He has authored two reference books on Linux Internals. He is the life member of Indian Society for Technical Education and IAENG. Now from past three years, he has published 12 Indian patents, and one patent granted for 20 years, three patents are stepping towards grant status. Three research scholars under his guidance were awarded a PhD degree. Two more research scholars submitted thesis. He can be contacted at email: r.panduranga@jainuniversity.ac.in.