Applied Mathematics & Information Sciences
An International Journal

http://dx.doi.org/10.18576/amis/200110

Optimization Algorithms for Path Routing and Security in Software-Defined Networking (SDN)

Ali Azawii Abdul Lateef[1,2,*], *H. A. El Shenbary*[1], *Ashraf A. Gouda*[1], *and Mohammed Abdel Razek*[1]

[1] Department of Mathematics and Computer Science, Faculty of Science, Al-Azhar University, Cairo, Egypt
[2] Department of Administrative and Financial Affairs, University of Anbar, Anbar, Iraq

Received: 2 Sep. 2025, Revised: 22 Nov. 2025, Accepted: 2 Dec. 2025
Published online: 1 Jan. 2026

Abstract: One of the most significant technologies that has clearly brought about considerable and remarkable changes in the world of communications, especially in network environments, is Software-Defined Networking (SDN).It has improved and increased the flexibility of these networks and the ability to manage their resources through intelligently dividing their layers into the control layer (control plane) and the data layer (data plane), which provides new and distinct ways to handle this data to meet some of the needs of these environments. Along with all of this, there are also challenges for which modern, practical solutions must be found that are compatible with the changes and development of these networks today, such as scalability and adaptability to these variables. Of particular importance are the security issues that these environments may face, which consequently threaten their integrity and reliability, guidance to instability. Artificial intelligence (AI) technologies and other technologies within this concept, such as Machine learning (ML) and Deep learning (DL), have provided distinct capabilities for solving complex problems in SDN environments and are currently at the forefront of technologies addressing these problems.Among the problems currently prevalent in these environments, which are comprehensively reviewed in this research paper, are dynamic traffic patterns in these environments (SDN), along with a review of modern methods used to improve these problems at all levels. This paper also focuses on ways to integrate these technologies (AI) and others and their role in developing and improving effective security methods against modern cyber threats to increase the security of these networks. The tangible contribution made by this work is one of the most important goals sought to achieve by increasing understanding of these technologies and SDN environments and developing them to be more efficient, flexible, and highly secure, in addition to increasing the widespread use of these environments in various fields.

Keywords: Software-Defined Networking, SDN, path routing optimization, security enhancement, machine learning techniques, control plane, data plane, cyberthreats, routing algorithms, SDN vulnerabilities.

1 Introduction

SDN is a modern technology that has greatly changed the network management way, through the amazing separation of control plane and data plane.[1]. This separation has clearly provided several important benefits: centralized control, network programmability, and network flexibility. This process has improved overall network performance, particularly in the areas of path routing optimization and network security.Inefficient use of network resources, high latency, and the potential for network security issues are some of the challenges that standard routing algorithms attempt to solve in order to adapt to dynamic traffic.[2]. The centralized control architecture in SDN networks has led to the continuous emergence of unique challenges in the process of optimizing path routing due to the above-mentioned architecture, and although this centralization provides distinct and essential advantages such as the ability to accurately and completely monitor the network, which leads to choosing the optimal path by making a set of smart and efficient decisions, traditional routing protocols are often insufficient to address these challenges, which motivates research into new optimization methods. All of this requires the availability of advanced and modern algorithms on an ongoing basis to obtain the desired improvement in the field of path routing optimization. The restrictions of regular networks architecture in terms

* Corresponding author e-mail: aliazawii@uoanbar.edu.iq

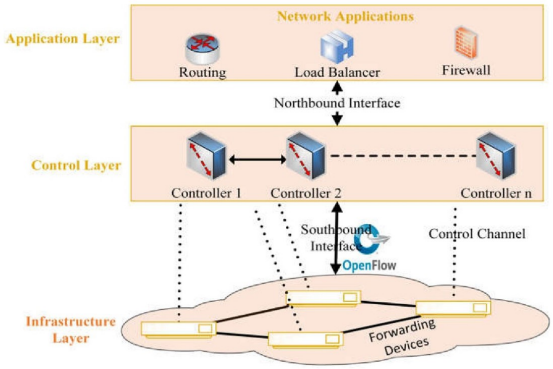

Fig. 1: Standard SDN architecture [5]

of control, scalability, and management were solved when SDN came along [3]. Recently, a new approach has been introduced to manage networks of different types. The control plane can actually include a standalone SDN controller or multiple SDN controllers that cooperate with each other to act as a central SDN controller [4]. However, the standard process for separating SDN levels is illustrated in Figure 1. Many functions can be used through the SDN model according to the needs of the network administrator, such as load balancing, traffic engineering, path routing, etc. [6]. In addition to the above, machine learning has been widely used to improve the performance of SDN in several areas, including resource management [7,8], intrusion detection systems [9], and other important security purposes[10]. Google B4, NTT's edge gateways, and Microsoft's public cloud are just a few examples of the significant benefits and advantages that come from using SDN in modern network architectures [11].

In addition to all the advantages of using SDN mentioned above, the most important of which is the centralized management of networks, which led to the advocacy of most users, industrial practitioners and academics, all due to the great security concern at all levels, especially in modern networks such as cloud networks and peer-to-peer networks. Therefore, despite all of this, there are many security challenges facing SDN networks, including scalability, reliability, control and response time [12].Therefore, the main concern currently for SDN layers is the possibility of escalating security attacks. Due to the multi-layer architecture of SDN, it turns out that the security threats are different and vary according to the layer, as the SDN layers face different security challenges according to the layer. The threats facing the application layer, which is also called the management layer, are the firewall, access control, intrusion detection and prevention system, and load balancing [13].

The review papers were carefully read, especially those that dealt with the related work to SDN and machine learning techniques and their impact on improving the architectures performance, such as path routing optimizations, network performance, and security.

K. M. Muheden, et al. explored deep learning techniques including supervised learning, unsupervised learning, and deep learning that can improve the functions of SDN. The researcher concluded that supervised learning is able to provide multi-functional and representative learning applicable to several network tasks [14].

S. Faezi, et al. collected researches from various academic databases from 2016 to 2023, focusing on the integration of machine learning technologies and SDN architecture, and how its techniques are applied within SDN architectures to enhance various aspects, including network performance, efficiency, and security [15].

J. Arevalo Herrera, et al focused-on machine learning techniques and deep learning to address security issues within SDN to improve security, including traffic optimization and classification and intrusion detection, which leads to overall network improvement, as various research papers published during the years from 2013 to 2019 were addressed which clearly demonstrated the integration between these techniques and the SDN architecture [16].

V. G. da Silva Ruffo, et al explained the basic steps in developing network intrusion detection systems (NIDS) by using Deep learning techniques to enhance security in SDNs, including datasets, the preprocessing of these datasets, and parameter tuning. This work highlights the growing trend in research in the field of SDN security [17].

A. A. Mahdi, et al provides an overview of machine learning enhancement of traditional network security but does not extend its analysis to SDN because it does not delve into machine learning applications with good results in SDN, focusing on intrusion detection, anomaly detection, and malware analysis. The advantages and disadvantages of different machine learning techniques are indicated [18].

K. M. Muheden, et al explored the potential of machine learning techniques to improve the functions of SDN and address several challenges, including improving data traffic and resource allocation, in addition to addressing how to separate the levels in these networks to improve the overall performance of the network. It also explained in an analytical manner the activity of these techniques, addressing the strengths and limitations of each technique, including the need for an accurate dataset and computational resources. Finally, it called for continuing research and exploration to address current limitations and improve the overall performance of the network [19].

R. Farahi analyzed the SDN architecture and explored the load balancing challenges within this architecture. After that, a good classification of AI-powered load balancing approaches is presented. In addition, the effectiveness metrics of these techniques are included.

Then, emerging trends and challenges are identified as future research to improve network performance by enhancement load balancing with AI techniques in SDN environments [20].

In their literature review, M. S. Farooq, et al. analyzed SDN networks from several aspects, including security, by reading several papers, identifying the potential security attacks and vulnerabilities at SDN layers, and suggesting possible solutions, challenges, and future directions for more secure SDN networks by adopting valuable defense strategies [21].

Machine learning (ML) has become a major and important factor for improving path routing and security in SDNs. A survey conducted by (Amin et al.) explored the role of these techniques in improving both in SDNs. These techniques have been classified into: supervised learning, unsupervised learning, and reinforcement learning with taking in consideration the traffic classification, quality of service (QoS) management, and intrusion and anomaly detection. All these was done through reviewing more than 200 papers, where currently focus on the research gaps at the. Although they focused on the performance improvement process, especially path routing, and continued to focus on security improvement mechanisms of SDNs and emphasizing on the current real need for robust and advanced evaluation procedures that would increase the security of the network architecture. This provides a basis for our research and other future research that should interact and integrate between network security and performance, which in turn enhances the adoption of a comprehensive approach to machine learning in improving the two basic parts mentioned above, which in turn improve overall performance of SDN [22].

Our survey is structured into three main sections, beginning with an introduction to (ML) techniques and SDN architecture, along with references to relevant previous work. The second section addresses the excellent survey conducted by Amin et al. on ML-based routing in the SDN environment. The path routing optimization processes in this environment were discussed using the techniques mentioned above, and what results have been reached from this process and its role in solving the environments challenges such as network scalability according to the important ways discussed in our review of machine learning-based path routing optimization methods.

As for the third section of our survey focused on security improvements in the SDN environment using machine learning (ML) techniques. A comparison was made between techniques that rely on data performance and ML techniques used to detect and mitigate cyber threats. Finally, these studies were reviewed and discussed in detail, highlighting open challenges and how to leverage ML technologies in the SDN environment, and identifying the future directions for path routing improvements and security enhancements.

2 SDN Path Routing Optimization

2.1 Routing challenges overview

SDN networks face several challenges that delay their deployment, impacting overall network performance and delaying their deployment. Nevertheless, they give important benefits in dealing with these obstacles and offering an appropriate environment for experts and enterprises using cloud environments. [23]. This part covers into exhaustive detail about these issues and how to resolve them.

The ability to scale of the controller, separation of networks, and decoupling are among the most major obstacles facing the SDN environment, were fully solved in the most recent studies. The centralized nature of the controller in the SDN environment may result to a single point of failure. As networks expand, they become more difficult to isolate and split up, which means they need more parts to be isolated. [24].

One of the most important strategies for the success and operation of SDN-based routing is the potential for security changes and cyber attacks on systems, especially Internet of Things (IoT) systems. Therefore, a comprehensive understanding of these challenges, along with controlling and maintaining the environment securely, is essential.[25]. Below are the most important techniques used to improve the routing path based on (ML) tools, which were presented by most of the recent related researches that focused on finding solutions based on (DL) tools and mechanisms to improve the quality of service (QoS), and were classified accordingly as follows:

2.2 Recent Routing Optimization Approaches

The ant colony algorithm and which falls under the general category of metaheuristic algorithms and the use of memory-overcoming mutation method, J. Chen, et al. [26] presented a method to improve the dynamic nature of SDNs, integrating it with the K-means clustering method to achieve network partitioning feature, which increases execution time and reduces space wastage. Their results showed a serious improvement over dynamic networks, reducing packet loss and network congestion, and saving time.

Also in [27] M. D. Tache, et al. provided an extensive discussion of modern techniques that have enhanced SDN networks which has been achieved by using a variety of algorithms.The study discusses tasks like dynamic routing, load balancing, traffic effectiveness, and redirection delay reduction, pointing out both the obstacles and solutions in SDN optimization .

2.3 Machine Learning-Based Solutions

G. Kim et al. in [28]. created a local network framework based Deep Reinforcement learning (DRL) algorithm for

SDN networks.The findings demonstrated that the suggested route selection technique exceeds standard hop-count routing as well as traffic-demand-based RL strategies across various network structures.

In SDN, R. Amin et al.[22] studied the application of ML methods for routing improvement. The essay discusses SDN routing selection potential and challenges using ML applications for supervised, unsupervised, and reinforcement learning.

2.4 QoS-Aware Routing Techniques

P. Kamboj, et al. [29] give a QoS-sensitive dynamic multi-path routing solution aimed for bettering the QoS of applications that use high bandwidth in a SDN environment. The suggested strategy involves the following stages: separating the flow, routing it via several routes, and organizing it. In the initial stage, establish where to separate the incoming flows so that the network can use multipath routing. In the second stage, proposed a greedy heuristic technique for producing a cost function to route the divided sub-flows. then in the third stage, a way to reorder incoming sub-flows has been suggested ,that come from different paths so that the process ordered at the final point and remains the same. The tests conducted indicate that the suggested strategy increases network performance due to 22% as opposed to the standard methods. Additionally, the suggested approach produces a 24% decrease in QoS-violated flows versus the benchmark schemes.

M. Rostami et al. [30] examined various QoS-aware load balancing techniques in SDN. The study highlights how SDN technology efficiently distributes network resources to workloads, increasing network performance and QoS.

To address routing obstacles, certain methodologies have emerged, such as DLR, besides to the ”knowledge base network (KDN)”, which seeks to produce modern learning methods that are capable for adapting to the dynamic needs of networks. Q. He et al.[31] put forward a successful approach for combining the framework of a graph neural network (GNN) with DRL, called Message Passing Deep Reinforcement Learning (MPDRL), which uses the properties of GNNs to capture network dynamics.The main objective of all of the mentioned above is to balance network traffic, which usually leads to improving network performance. The authors carried out three experiments on architecture on ISP networks, obtaining results which show that MPDRL greatly enhances network efficiency, unlike other methods.

Q. He et al.[31] proposed an efficient hybrid system based on combining DRL with a ”Graph Neural Network (GNN)” architecture. The purpose system used to find a suitable environment that balances network traffic and improves its performance. The results of this system which is implemented on three Internet service provider (ISP) architecture, demonstrated significant improvements in performance compared to traditional systems.

J. Chen et al.[32] proposed a nature-inspired algorithm based on the natural behavior of the African vulture. The proposed algorithm, called the African Vulture Routing Optimization (AVRO) algorithm” for SDN environments, helped in selecting the appropriate path based on the intelligent and comprehensive optimization solutions it provided with high convergence speed to mitigate the local optimization problem that generally affects the network performance.The results of this optimization showed that this routing algorithm has better network awareness and approximately 17% performance improvement, outperforming DRL algorithms and outperforming traditional routing systems by approximately 70%.

J. C. Altamirano et al. [33] put forward a ”Generative Adversarial Networks” ”GAN-enhanced DRL-based routing optimization framework” that addresses the long duration of training of DRL models. This method boosts up agent learning via GANs. It cuts down on training expenses while achieving network throughput and traffic improvement.

L. P. Aguirre Sanchez et al. [34] suggested using DRL In SDN to improve routing and QoS through ”QoS-Driven Routing Enhancement (DQS)”. DQS uses several DRL agents to disperse traffic, reducing convergence times and maintaining scalability. Docker-driven OpenFlow reduces final delay by 20% to 30% over baseline techniques.

The concern of overestimating bias was fixed by implementing a different DL technique called ”Delayed Double Deep Deterministic Policy Gradient (TD3)”, which was offered byP. Kulshreshtha, et al. [35] They looked at and contrasted DDPG (the existing approach) and TD3 (the proposed approach). TD3 was shown to work much better with less latency.

K. Hamzah [50] developed a Deep Q Network (DQN) combination system for realizing smart routing and automated encryption of data to identify and counteract security risks, all in real time. The results showed that this system could improve network flow, handle different types of data traffic well, and protect the network from security risks.

S. Singh [51] aim to use the actual SDN network data received from the SDN controller to take the real-time data collected by the SDN controller to make the appropriate path routing dynamically. They used dynamic routing techniques for SDN in wide area networks (SDN-WAN). The results showed that this approach performed excellent routing by determining the best path to the destination using the SFOP algorithm with SDN-WAN resources efficiently.

Table 1: Comparative Analysis of Routing Optimization Approaches in SDN

Research/ Year	Algorithm Used	Objectives	Implementation Tools	Performance Metrics	Strengths	Limitations
[22] (2021)	Supervised, Unsupervised, and Reinforcement Learning	Categorize ML techniques for SDN routing optimization	TensorFlow, PyTorch	Routing accuracy, network efficiency	Comprehensive analysis of ML applications in SDN	Does not provide specific implementation details
[28] (2022)	Deep Reinforcement Learning (DRL)	Optimize routing by balancing end-to-end delay and packet loss	TensorFlow, Mininet, OpenFlow	Delay, packet loss, throughput	Learns optimal routing policies, adapts to network dynamics	Training requires significant time and resources
[29] (2022)	Multipath QoS-Aware Routing	Ensure QoS guarantees in SDN-based networks	Mininet, Open Daylight	Jitter, bandwidth utilization, latency	Improves QoS for real-time applications, optimizes flow distribution	Increased computational complexity
[26] (2024)	Hybrid Meta-Heuristic (Ant Colony + Box-Covering + K-Means)	Improve dynamic routing, reduce congestion, optimize performance	Simulation in SDN environments	Packet loss, latency, throughput	Handles dynamic changes efficiently, improves routing decisions	Computational overhead for large networks
[30] (2024)	Load Balancing Algorithms	Distribute network resources efficiently for better QoS	SDN Controllers (POX, Ryu)	Load distribution, response time, throughput	Enhances network performance and reliability	May not adapt well to sudden traffic surges
[31] (2024)	Message Passing Deep Reinforcement Learning (MPDRL)	Achieve load balancing and optimize network traffic using GNN-enhanced DRL	Python, TensorFlow, Mininet	Network load balancing, throughput, latency	Effectively utilizes network topology information, improves routing decisions dynamically	High computational complexity due to GNN message passing
[32] (2024)	African Vulture Routing Optimization (AVRO)	Improve network routing using AVOA metaheuristic optimization	Python, SDN controllers	Convergence speed, network awareness, throughput	Fast convergence, strong global optimization capability, 16.9% better than DRL, 71.8% better than traditional routing	Algorithm performance depends on population initialization and optimization phase tuning
[33] (2024)	GAN-enhanced Deep Reinforcement Learning (DRL+GAN)	Accelerate DRL training for SDN routing optimization	Containernet, OpenAI Gym	Training time, throughput, route optimization efficiency	GAN module accelerates DRL training, making real-world deployment feasible	GAN training requires fine-tuning to prevent mode collapse
[34] (2024)	QoS-Driven Routing Optimization (DQS)	Optimize routing and QoS efficiency using DRL in SDN	Docker-based OpenFlow prototype	End-to-end delay, throughput, traffic distribution	Reduces convergence times, maintains scalability, 20–30% reduction in delay	Complexity in handling diverse traffic classes

[50] (2025)	Deep Q-Network (DQN), Autoencoder	Integrate intelligent routing optimization and real-time anomaly detection in SDN environments	Python (TensorFlow/Keras), Mininet emulator	Network efficiency, detection accuracy, adaptability	Simultaneous routing optimization and threat detection; dynamically adapts to diverse traffic patterns	High computational complexity and potential latency in large-scale SDN environments
[51] (2025)	ML Algorithm, SFOP (Shortest Feasible Optimal Path)	Develop a dynamic routing method for SDN-WAN leveraging SDN programmability and centralized control to optimize routing and QoS	Python-based SDN controller with OpenFlow interface	Link utilization, QoS, routing efficiency, resource utilization	Adapts routing decisions in real-time using controller feedback; enhances network stability and responsiveness	High computational complexity; scalability challenges in large SDN-WAN deployments

2.5 Research Gaps and Recent Challenges

1. **Scalability Problems:** Network complexity is increasing due to scalability issues in SDN networks, that is the problem currently faced by current routing enhancement algorithms.
2. **Real-Time Adaptability:** finding constructive and adaptive solutions to mitigate today's shortages due to the high demand for dynamic technologies that adapt to changing network requirements and traffic data.
3. **Security Concerns:** Due to the rapid and massive development of cyberattacks, there is a need for robust and reliable security technologies to address these threats that can target SDN environments, such as DDoS attacks.
4. **Integration and Interoperability Challenges:** To improve the overall performance of the SDN environment, it is necessary to find distinct solutions that can provide interoperability and seamless integration between SDN control components and protocols, as this is a very important point.
5. **Energy Efficiency:** There is a continues need for energy-efficient routing solutions to reduce power consumption in large SDN deployments.
6. **Limited Real-World Deployments:** Most solutions are tested in simulated environments, and there is a need for more real-world implementation and validation.

3 Security Optimization in SDN

3.1 Overview of security challenges in SDN

SDNs are advanced networks that allow for centralized and programmable network management based on the separation of the control plane from the data plane. However, despite the many advantages offered by SDN, such as flexibility and good use of resources, it faces many difficulties and security challenges that make it more vulnerable to these challenges[36]. The following are some of these challenges that have been addressed in most research sources and can be summarized as follows:

a.Centralized Control Plane Vulnerability:
The centralized nature of the SDN control plane makes it a prime target for attacks. If compromised, an attacker can disrupt the entire network[37].

b. Control Plane Threats:
One of the most significant concerns and problems that it may lead to a complete system shutdown of SDN environment. This can occur due to attacks that may affect the control plane in these environments.[38].

c. DoS and DDoS Attacks:
: The reason for service unavailability in SDN environments is their vulnerability to large attacks that consume huge resources by overwhelming the centralized control with massive traffic[39].

d. Device Redirection Attacks:
T emporary or major disruptions can occur due via access to the network infrastructure containing switches and access point devices, which are vulnerable to cyber attacks [38].

e. Communication Vulnerabilities:
Disabling some protocols responsible for network security, such as TSL, can lead to communication channels being compromised [36].

f. Fake Traffic Flows:
Service in SDN environments can be disrupted by flooding channels with fake traffic flows sent by attackers who intend to disrupt the service [36].

g. Open Programmable APIs:
The use of open programmable APIs provides flexibility but also introduces new vulnerabilities that must be managed with robust protocols. [37].

3.2 Recent security optimization approaches

There is currently a technical explosion in network management caused by SDN, which has clearly established the process of separating the data plane from the control plane as mentioned earlier, and despite all of this, it faces renewed security challenges on a daily basis. Therefore, SDN is working on finding new methods to improve security and improve scalability while taking into account security risks. Here are some of the latest methods and technologies:

a. **Enhancing Security by Blockchain Integration:**
Security enhancements using blockchain technology are being integrated with SDN to enhance the security of these networks and provide transparency to their operations. It works to renew security rules and prevent tampering with network infrastructure and logs, thus ensuring robustness, monitoring, and reducing single points of failure [40].

A distributed denial of service mitigation system was used to leverage the centralized control features of SDN and the decentralized security services of blockchain to enhance distributed security based on SDN blockchain using neural networks to address potential cyber challenges and attacks [41]
R. Jmal, et al. [42] Presented a technique for integrating the SDN environment and blockchain technology (BC), which was used in the field of the Internet of Energy (IoE). This model of integrating the SDN environment, the Internet of Energy, and the blockchain provided very important benefits. First, the integration of the blockchain with the SDN directly improves the SDN network, and second, it improves the decentralization of the SDN in one case and improves the network security in another case, which led to reducing access to single points of failure. In addition, other issues such as energy consumption and the possibility of network expansion were discussed as future directions that can be worked on to show other results.

b. **AI for Threat and Anomaly Detection and prevention:**
AI, ML, and DL technologies combined with SDN make it much easier to find abnormalities and possible cyber breaches in real time. This is done by employing detailed and accurate network traffic analysis to reduce and eliminate these threats. Where bad flows or illegal access to data can be found, and where distributed denial of service assaults can be found. This makes it easier to find things and lets you take steps to improve security before a network breakdown happens. [43].

c.**Advanced Encryption & Authentication techniques to enhance SDN Security:**
Security is improved by using modern technologies within SDNs by implementing multi-level security systems by leveraging centralized control of these networks, in addition to improving and expanding encryption and authentication techniques by enhancing communication between SDN layers and encrypting all transmitted data and configuration data to prevent tampering and access to this data and ensuring its confidentiality, integrity, and authenticity [44].
Cyber threats were detected and mitigated in SDN-IoT environments using a deep learning algorithm that combines a deep neural network (DNN) and long short-term memory (LSTM). The four layers: infrastructure, data, control, and application, each of which plays a critical role in anomaly detection and prevention [45].
G. F. Scaranti, et al. [46] introduced an advanced Intrusion Detection System (IDS) for Software-Defined Networking (SDN), utilizing an unsupervised stream clustering algorithm for effective real-time attack detection without the need for labeled data and achieved high detection accuracy, with over 99.60% f-measure rates in identifying DDoS and port scan attacks. The system employs the DenStream algorithm, allowing continuous adaptation to new threats without pre-labeled data, this IDS enhances security against evolving threats, establishing a strong foundation for future research in adaptive security solutions.
P. Hadem, et al. [47] this research established an SDN-based intrusion detection system (IDS) using SVMs for anomaly detection, achieving 95.98% accuracy on the full NSL-KDD dataset(Network Security Laboratory - Knowledge Discovery in Databases) and 87.74% accuracy on selected sub-features. This method achieves resource efficiency and detection accuracy by selectively processing logs in the controller using memory structures, improving performance by 9.76% compared to file-based logging and saving 90-95% of memory space compared to full logging. IP address tracking ensures accurate identification of attack sources, bypassing inaccurate detection barriers, and avoiding incorrect blocking of legitimate network traffic.

d.**Secure Communication Protocols:**
Unifying encryption techniques and implementing mutual authentication protocols ensures good data security against forgery and tampering. All this is done by continuing improvements to communication protocols between SDN planes by adding encryption and authentication to all data passing through these planes to provide robust security capabilities between control units and switches against potential attacks [48].
S. S. Mahdi, et al. [49], authors proposed a hybrid quantum key distribution protocol to reinforce SDN security. By combining classical and quantum key

distribution methods, the protocol aims to secure the OpenFlow channel between the controller and data plane. This dual-security approach leverages the inherent physical and computational security features of quantum mechanics, effectively safeguarding OpenFlow communications against potential threats.

In all of the above, there are other ways to improve the security of software-defined networks, and it is expected that there will be a need to develop and improve this security.
Here is the structured table 2 summarizing recent research papers on Security Optimization Approaches in SDN based on the literature review:

Table 2: Comparative Analysis of Routing Optimization Approaches in SDN

Research / Year	Algorithm Used	Security Focus on	Detection Rate Results	Implementation Tools	Environment	Strengths	Limitations
[44] 2020	Multi-level Encryption & Authentication	Data confidentiality, integrity, authenticity	N/A	Secure SDN framework	SDN	Prevents unauthorized access and tampering	Processing overhead on encryption mechanisms
[47] 2021	SVM-based IDS for anomaly detection	Intrusion detection in SDN	95.98% accuracy on full NSL-KDD dataset	NSL-KDD dataset analysis	SDN	Saves 90-95% memory space compared to full logging	Trade-off between accuracy and false positives
[46] 2022	Unsupervised Stream Clustering IDS	Real-time attack detection	99.6% accuracy in detecting DDoS & port scans	DenStream algorithm in SDN	SDN	Highly accurate detection without labeled data	May struggle with new, unseen attack patterns
[49] 2022	Hybrid Quantum Key Distribution	Secure OpenFlow channel in SDN	N/A	Quantum + Classical key distribution	SDN	Quantum-resistant security	Practical deployment challenges
[41] 2023	Blockchain + Neural Networks	DDoS mitigation using decentralized security services	High detection accuracy	SDN-Blockchain hybrid model	SDN	Combines centralized SDN control with decentralized security	Requires computational resources for AI processing
[43] 2023	AI-based Anomaly Detection	Malicious flow detection, unauthorized access prevention	High detection rate	Deep Reinforcement Learning in SDN	SDN	Faster and more accurate than traditional methods	Requires training data and computational resources
[40] 2024	Blockchain-based security integration	Network security, transparency, tampering prevention	N/A	SDN-Blockchain framework	SDN	Prevents single points of failure, ensures secure rule updates	Scalability concerns and energy overhead

[42] 2024	Blockchain in IoE systems	Security and scalability in IoE-SDN networks	N/A		IoE-SDN model	IoE Enhances security and decentralization	Scalability and performance bottlenecks
[45] 2025	DNN + LSTM for anomaly detection	Cyber threat detection in SDN-IoT environments	High accuracy, low false positive rate	Deep learning in SDN-IoT	SDN-IoT	Adapts to dynamic threats	High computational cost
[48] 2025	Secure Communication Protocols	Strengthening SDN control-data plane security	N/A	Encryption + Mutual authentication protocols	SDN	Ensures robust protection against attacks	Key management challenges

3.3 Research Gaps and Challenges

Despite the advancements in SDN security optimization, several research gaps and challenges remain:

1. **Scalability and Performance Overhead:** Many proposed solutions, particularly those integrating blockchain or AI, introduce significant computational and energy overhead, making large-scale deployment challenging.

2. **Real-time Threat Detection:** While AI and deep learning methods improve detection accuracy, their ability to respond in real-time under high-traffic conditions needs further refinement.
3. **Data Privacy and Integrity:** Ensuring secure communication protocols and encrypted data transmission is crucial, but key management and encryption overhead pose challenges.

4. **Adaptability to Evolving Threats:** Security mechanisms must continuously adapt to new attack vectors, requiring dynamic and self-learning security frameworks.

5. **Integration with Existing Network Infrastructures:** Many SDN security solutions require modifications to existing architectures, which may not be feasible for all network operators.

6. **Resource Efficiency:** AI and ML-based detection methods often require extensive training datasets and computational power, which can limit deployment in resource-constrained environments.

7. **Quantum Security Challenges:** Quantum key distribution techniques offer a high level of security, but their practical implementation in SDN faces significant challenges, most notably infrastructure constraints and high implementation costs.

Therefore, it is imperative to find innovative solutions to address these gaps, contributing to the development of more robust and efficient security frameworks for these networks.

4 Future Research Directions and Conclusion

4.1 Future Trends

Previous studies have shown that SDN will get better and more integrated in the future by working with AI, ML, and DL technologies to make path routing and data security better. This development and integration involve suggesting and enhancing real-time algorithms to make these networks more adaptable to changes and easier to set up. It also includes constantly making these networks safer to protect them from new security and cyber threats. Also, it's important to deal with problems that will make the network run better, keep them safe, and lower costs. This can be done by making sure that the parts of these networks always need energy-saving technologies and efficient operation procedures.

4.2 Conclusion

Finally, we need to remember that there are still many big issues to solve, even if SDNs are making a lot of progress in improving path routing and data security. Some of the issues that need to be solved are real-time adaptability, better scalability, and the use of AI, ML, and DL technologies to make these networks perform better.
The future direction should focus on making these networks more secure so they can keep up with rapid growth. They should also incorporate entire technologies that will boost their overall performance, which will help them spread to more areas.

Acknowledgement

The authors are grateful to the anonymous referee for a careful checking of the details and for helpful comments that improved this paper.

References

[1] T. Dargahi, A. Caponi, M. Ambrosin, G. Bianchi, and M. Conti, "A survey on the security of stateful SDN data planes," IEEE Communications Surveys & Tutorials **19**, 1701–1725 (2017).

[2] A. Shirmarz and A. Ghaffari, "Performance issues and solutions in SDN-based data center: a survey," J Supercomput **76**, 7545–7593 (2020).

[3] N. Feamster, J. Rexford, and E. Zegura, "The road to SDN: an intellectual history of programmable networks," ACM SIGCOMM Computer Communication Review **44**, 87–98 (2014).

[4] D. Alberto Priano, M. C. Abeledo, J. Guevara, M. Marsicano, F. Sergio Bruschetti, and I. Giniger, "Comparative Analysis of SDN Controllers: A Study on Installation, Protocols Interaction, Network Topologies Monitoring, and GUI Experience," Review of Computer Engineering Studies **10**, 3 (2023).

[5] "https://www.opennetworking.org/sdn-definition," (2021).

[6] F. Bannour, S. Souihi, and A. Mellouk, "Distributed SDN control: Survey, taxonomy, and challenges," IEEE Communications Surveys & Tutorials **20**, 333–354 (2017).

[7] S. Il Kim and H. S. Kim, "Dynamic service function chaining by resource usage learning in SDN/NFV environment," in 2019 International Conference on Information Networking (ICOIN), IEEE, 485–488 (2019).

[8] J. Xu, J. Wang, Q. Qi, H. Sun, and B. He, "IARA: An intelligent application-aware VNF for network resource allocation with deep learning," in 2018 15th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON), IEEE, 1–3 (2018).

[9] J. Xu, J. Wang, Q. Qi, H. Sun, and B. He, "IARA: An intelligent application-aware VNF for network resource allocation with deep learning," in 2018 15th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON), IEEE, 1–3 (2018).

[10] P. Somwang and W. Lilakiatsakun, "Computer network security based on support vector machine approach," in 2011 11th International Conference on Control, Automation and Systems, IEEE, 155–160 (2011).

[11] S. Natarajan, A. Ramaiah, and M. Mathen, "A software defined cloud-gateway automation system using OpenFlow," in 2013 IEEE 2nd International Conference on Cloud Networking (CloudNet), IEEE, 219–226 (2013).

[12] M. Jammal, T. Singh, A. Shami, R. Asal, and Y. Li, "Software defined networking: State of the art and research challenges," Computer Networks **72**, 74–98 (2014).

[13] A. Voellmy, H. Kim, and N. Feamster, "Procera: A language for high-level reactive network control," in Proceedings of the first workshop on Hot topics in software defined networks, 43–48 (2012).

[14] K. M. Muheden, R. N. Othman, R. S. Hawezi, S. M. J. Abdalwahid, O. S. Mustafa, and S. W. Kareem, "Exploring the Synergy: A Review of Machine Learning Techniques in Software Defined Networking (SDN)," in ITM Web of Conferences, EDP Sciences, 01016 (2024).

[15] S. Faezi and A. Shirmarz, "A comprehensive survey on machine learning using in software defined networks (SDN)," Human-Centric Intelligent Systems **3**, 312–343 (2023).

[16] J. Arevalo Herrera and J. E. Camargo, "A survey on machine learning applications for software defined network security," in Applied Cryptography and Network Security Workshops: ACNS 2019 Satellite Workshops, SiMLA, Cloud S&P, AIBlock, and AIoTS, Bogota, Colombia, June 5–7, 2019, Proceedings 17, Springer, 70–93 (2019).

[17] da Silva Ruffo, V. G., Lent, D. M. B., Komarchesqui, M.,Schiavon, V. F.,de Assis, M. V. O., Carvalho, L. F., Proença Jr, M. L., "Anomaly and intrusion detection using deep learning for software-defined networks: A survey," Expert Syst Appl, 124982 (2024).

[18] A. A. Mahdi, "Machine learning applications of network security enhancement," Computer Science & IT Research Journal **5**, 10.

[19] K. M. Muheden, R. N. Othman, R. S. Hawezi, S. M. J. Abdalwahid, O. S. Mustafa, and S. W. Kareem, "Exploring the Synergy: A Review of Machine Learning Techniques in Software Defined Networking (SDN)," in ITM Web of Conferences, EDP Sciences, 01016 (2024).

[20] R. Farahi, "A comprehensive overview of load balancing methods in software-defined networks," Discover Internet of Things **5**, 6 (2025).

[21] M. S. Farooq, S. Riaz, and A. Alvi, "Security and privacy issues in software-defined networking (SDN): A systematic literature review," Electronics (Basel) **12**, 3077 (2023).

[22] R. Amin, E. Rojas, A. Aqdus, S. Ramzan, D. Casillas-Perez, and J. M. Arco, "A survey on machine learning techniques for routing optimization in SDN," IEEE Access **9**, 104582–104611 (2021).

[23] M. Jammal, T. Singh, A. Shami, R. Asal, and Y. Li, "Software defined networking: State of the art and research challenges," Computer Networks **72**, 74–98 (2014).

[24] S. Katragadda, "Software-Defined Networking Challenges and Research Opportunities for Future Interest," Int J Res Appl Sci Eng Technol **13**, 1288–1295 (2025), doi: 10.22214/ijraset.2025.66353.

[25] Rahdari A ,Jalili A, Esnaashari M, Gheisari M,Vorobeva A , Fang Z ,Sun PKorzhuk V , Popov IWu Z, Tahaei H"Security and Privacy Challenges in SDN-Enabled IoT Systems: Causes, Proposed Solutions, and Future Directions," Computers, Materials & Continua **80**, 2511–2533 (2024), doi: 10.32604/cmc.2024.052994.

[26] J. Chen, W. Xiao, H. Zhang, J. Zuo, and X. Li, "Dynamic routing optimization in software-defined networking based on a metaheuristic algorithm," Journal of Cloud Computing **13**, 41 (2024), doi: 10.1186/s13677-024-00603-1.

[27] M. D. Tache (Ungureanu), O. Păscuțoiu, and E. Borcoci, "Optimization Algorithms in SDN: Routing, Load Balancing, and Delay Optimization," Applied Sciences **14**, 5967 (2024), doi: 10.3390/app14145967.

[28] G. Kim, Y. Kim, and H. Lim, "Deep Reinforcement Learning-Based Routing on Software-Defined

Networks," IEEE Access **10**, 18121–18133 (2022), doi: 10.1109/ACCESS.2022.3151081.

[29] P. Kamboj, S. Pal, S. Bera, and S. Misra, "QoS-Aware Multipath Routing in Software-Defined Networks," IEEE Trans Netw Sci Eng **10**, 723–732 (2023), doi: 10.1109/TNSE.2022.3219417.

[30] M. Rostami and S. Goli-Bidgoli, "An overview of QoS-aware load balancing techniques in SDN-based IoT networks," Journal of Cloud Computing **13**, 89 (2024), doi: 10.1186/s13677-024-00651-7.

[31] He, Q., Wang, Y., Wang, X., Xu, W., Li, F., Yang, K., Ma, L., "Routing Optimization With Deep Reinforcement Learning in Knowledge Defined Networking," IEEE Trans Mob Comput **23**, 1444–1455 (2024), doi: 10.1109/TMC.2023.3235446.

[32] J. Chen, W. Xiao, H. Zhang, J. Zuo, and X. Li, "Dynamic routing optimization in software-defined networking based on a metaheuristic algorithm," Journal of Cloud Computing **13**, 41 (2024), doi: 10.1186/s13677-024-00603-1.

[33] J. C. Altamirano, M. Guitouni, H. Hassan, and K. Drira, "Routing optimization based on DRL and Generative Adversarial Networks for SDN environments," in NOMS 2024-2024 IEEE Network Operations and Management Symposium, IEEE, 1–5 (2024), doi: 10.1109/NOMS59830.2024.10575453.

[34] L. P. Aguirre Sanchez, Y. Shen, and M. Guo, "DQS: A QoS-driven routing optimization approach in SDN using deep reinforcement learning," J Parallel Distrib Comput **188**, 104851 (2024), doi: 10.1016/j.jpdc.2024.104851.

[35] P. Kulshreshtha and A. K. Garg, "Traffic Optimization and Optimal Routing in 5G SDN Networks Using Deep Learning," 33–41 (2024), doi: 10.1007/978-981-99-8661-3_3.

[36] A. Ahmad, E. Harjula, M. Ylianttila, and I. Ahmad, "Evaluation of Machine Learning Techniques for Security in SDN," in 2020 IEEE Globecom Workshops (GC Wkshps, IEEE, 1–6 (2020), doi: 10.1109/GCWkshps50303.2020.9367477.

[37] C.-Y. J. Peng, K. L. Lee, and G. M. Ingersoll, "An Introduction to Logistic Regression Analysis and Reporting," J Educ Res **96**, 3–14 (2002), doi: 10.1080/00220670209598786.

[38] I. Ahmad, S. Namal, M. Ylianttila, and A. Gurtov, "Security in Software Defined Networks: A Survey," IEEE Communications Surveys & Tutorials **17**, 2317–2346 (2015), doi: 10.1109/COMST.2015.2474118.

[39] S. Nanda, F. Zafari, C. DeCusatis, E. Wedaa, and B. Yang, "Predicting network attack patterns in SDN using machine learning approach," in 2016 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN), IEEE, 167–172 (2016), doi: 10.1109/NFV-SDN.2016.7919493.

[40] H. Lakhlef, T. Lerner, A. Kebir, N. El Atia, X. Du, and V. Ingardin, "Blockchain-Enabled SDN Solutions for IoT: Advancements, Discussions, and Strategic Insights," in 2024 IEEE Symposium on Computers and Communications (ISCC), IEEE, 1–6 (2024), doi: 10.1109/ISCC61673.2024.10733649.

[41] R. Jmal, W. Ghabri, R. Guesmi, B. M. Alshammari, A. S. Alshammari, and H. Alsaif, "Distributed Blockchain-SDN Secure IoT System Based on ANN to Mitigate DDoS Attacks," Applied Sciences **13**, 4953 (2023), doi: 10.3390/app13084953.

[42] Hayyolalam, V., Zekiye, A., Abuzahra, H., Özkasap, Ö., Karakus, M., Guler, E.,Uludag, S., "Synergistic Integration of Blockchain and Software-Defined Networking in the Internet of Energy Systems," in 2024 6th International Conference on Blockchain Computing and Applications (BCCA), IEEE, 420–427 (2024), doi: 10.1109/BCCA62388.2024.10844451.

[43] C. Kannan, R. Muthusamy, V. Srinivasan, V. Chidambaram, and K. Karunakaran, "Machine learning based detection of DDoS attacks in software defined network," Indonesian Journal of Electrical Engineering and Computer Science **32**, 1503 (2023), doi: 10.11591/ijeecs.v32.i3.pp1503-1511.

[44] S. Achleitner, Q. Burke, McDaniel, Thomas, and Srikanth. Krishnamurthy, "MLSNet: A Policy Complying Multilevel Security Framework for Software Defined Networking," 10.48550/arXiv.2009.10021 (2020).

[45] H. Moh'd S. Hatamleh, A. M. A. Alnaser, S. S. Saloum, A. Sharadqeh, and J. S. Alkasassbeh, "PictureGuard: Enhancing Software-Defined Networking–Internet of Things Security with Novel Image-Based Authentication and Artificial Intelligence-Powered Two-Stage Intrusion Detection," Technologies (Basel) **13**, 55 (2025), doi: 10.3390/technologies13020055.

[46] G. F. Scaranti, L. F. Carvalho, S. Barbon, J. Lloret, and M. L. Proença, "Unsupervised online anomaly detection in Software Defined Network environments," Expert Syst Appl **191**, 116225 (2022), doi: 10.1016/j.eswa.2021.116225.

[47] P. Hadem, D. K. Saikia, and S. Moulik, "An SDN-based Intrusion Detection System using SVM with Selective Logging for IP Traceback," Computer Networks **191**, 108015 (2021), doi: 10.1016/j.comnet.2021.108015.

[48] M. Shahzad, S. Rizvi, T. A. Khan, S. Ahmad, and A. A. Ateya, "An Exhaustive Parametric Analysis for Securing SDN Through Traditional, AI/ML, and Blockchain Approaches: A Systematic Review," International Journal of Networked and Distributed Computing **13**, 12 (2025), doi: 10.1007/s44227-024-00055-8.

[49] S. S. Mahdi and A. A. Abdullah, "Enhanced Security of Software-defined Network and Network Slice Through Hybrid Quantum Key Distribution Protocol," Infocommunications journal **14**, 9–15 (2022), doi: 10.36244/ICJ.2022.3.2.

[50] K. Hamzah, "Optimizing Software-Defined Networking (SDN) Performance Through Machine Learning-Based Traffic Management," *Journal of Al-Qadisiyah for Computer Science and Mathematics* **17**, (2025), doi: 10.29304/jqcsm.2025.17.22193.

[51] S. Singh and K. Sharma, "A New Dynamic Routing Approach for Software Defined Network," *International Journal on Recent and Innovation Trends in Computing and Communication (IJRITCC)* **13**(1), 1–5 (January 2025).

Ali Azawii Abdul Lateef is a lecturer at the College of Computer Science and Information Technology, University of Anbar. He holds a B.S. in Computer Science (Software Branch) from the University of Technology, Baghdad (2007), and an M.Sc. in Computer Science from the University of Anbar (2020). His research interests include Artificial Intelligence (AI), Information Security, and Deep Learning.

H. A. El Shenbary obtained his B.Sc. and M.Sc. degrees from Al-Azhar University, Cairo, Egypt. He holds a Ph.D. in Computer Science (2020) and is currently an Assistant Professor at Al-Azhar University. His research areas include image processing, biometrics, AI, and pattern recognition.

Ashraf A. Gouda is an Assistant Professor in Computer Science at Al-Azhar University. He holds a Ph.D. in Computer Science from Budapest University of Technology and Economics, Hungary (2005). His research interests include physics-informed neural networks, AI, IoT, quantum machine learning, quantum computing, and optimization techniques.

Mohammed Abdel Razek is a Professor of Computer Science at Al-Azhar University. He holds a Ph.D. in Computer Science-Artificial Intelligence from the University of Montreal, Canada (2004). His research focuses on AI techniques in e-learning, medicine, cybersecurity, and IoT. He has published over 80 papers and serves as an editor/reviewer for various journals and conferences.