

ISSN Print: 2664-8776
ISSN Online: 2664-8784
IJRE 2026; SP-8(2): 09-13
www.engineeringpaper.net
Received: 09-08-2026
Accepted: 06-10-2026
Published: 14-11-2026

Preeti Saini
Department of Engineering & Technology, DPG Degree College, Gurugram, Haryana, India

Chanchal Rohilla
Department of Engineering & Technology, DPG Degree College, Gurugram, Haryana, India

Corresponding Author:
Preeti Saini
Department of Engineering & Technology, DPG Degree College, Gurugram, Haryana, India

Recent Advancement in Multidisciplinary innovation and research RAMIR-26

AI-driven adaptive traffic engineering and secure resource optimization in software-defined networks

Preeti Saini[1], Chanchal Rohilla[2]

DOI: https://www.doi.org/10.33545/26648776.2026.v8.i2a.86308

Abstract

Abstract—The increasing heterogeneity of modern communication infrastructures, coupled with unprecedented growth in latency-sensitive and bandwidth-intensive applications, has exposed significant limitations in conventional network management approaches. Static routing policies and rule-based optimization techniques often fail to adapt to rapidly changing traffic dynamics, resulting in inefficient resource utilization, elevated energy consumption, and increased vulnerability to sophisticated cyber threats. This study proposes an adaptive Artificial Intelligence (AI)-driven traffic engineering framework for Software-Defined Networks (SDNs) that integrates Deep Reinforcement Learning (DRL) with real-time network telemetry to enable autonomous routing, congestion mitigation, and intelligent anomaly detection. The proposed architecture continuously monitors network conditions, predicts traffic fluctuations, and dynamically reallocates forwarding paths while preserving Quality of Service (QoS) and minimizing operational overhead. A multi-objective optimization model is incorporated to simultaneously improve throughput, reduce end-to-end latency, optimize link utilization, and decrease energy expenditure across distributed network environments. Furthermore, the framework embeds a lightweight security intelligence layer capable of identifying abnormal traffic patterns and responding to emerging attacks without compromising network performance. Experimental evaluation under diverse traffic scenarios is designed to compare the proposed approach with conventional shortest-path routing, static SDN routing, and learning-based traffic engineering strategies. The evaluation considers throughput, end-to-end latency, packet loss, link utilization, energy consumption, scalability, convergence time, and anomaly-detection performance. The proposed framework provides a unified basis for secure, autonomous, and sustainable network orchestration for cloud computing, Internet of Things (IoT), edge computing, and future sixth-generation (6G) communication ecosystems.

Keywords: Software-Defined Networking, Artificial Intelligence, Deep Reinforcement Learning, Traffic Engineering, Network Telemetry, Congestion Control, Anomaly Detection, Quality of Service, Energy Efficiency, 6G

1. Introduction

Modern communication networks are increasingly characterized by heterogeneous devices, variable traffic demands, cloud and edge services, IoT deployments, and latency-sensitive applications. Traditional networks are difficult to configure and reconfigure when traffic load, failures, or service requirements change. SDN addresses part of this challenge by separating control logic from forwarding devices and exposing programmable interfaces for dynamic network management (Kreutz *et al.*, 2015) [1], (Rajahalme *et al.*, 2015) [2].

Although SDN provides centralized visibility and programmability, conventional SDN traffic engineering may still depend on shortest-path computation, static policies, or manually designed heuristics. Such mechanisms can be inadequate when traffic patterns change rapidly. Recent research demonstrates that DRL can learn routing policies directly from network states and can optimize objectives such as delay, packet loss, throughput, bandwidth utilization, and QoS (Chen *et al.*, 2021) [3]– (Wang *et al.*, 2024) [4].

Pei *et al.* proposed an efficient DRL-based traffic-engineering method for SDN that dynamically addresses congestion and uses online link selection (Pei *et al.*, 2024) [5]. Kim *et al.* used DRL to learn link weights that balance end-to-end delay and packet loss (Kim *et al.*, 2022) [6]. More recent work has explored QoS-driven DRL routing, dynamic fuzzy routing, and graph-based DRL approaches for more robust routing under changing topology and traffic conditions (Aguirre Sanchez *et al.*, 2024) [7], (Wang *et al.*, 2024) [4], (Wang *et al.*, 2024) [8].

26648784, 2026, 8(2), Downloaded from https://www.doi.org/10.33545/26648776.2026.v8.i2a.86308 by International Journal of Research in Engineering on [14/11/2026]. See the Terms and Conditions (https://www.engineeringpaper.net) for rules of use; OA articles are governed by the applicable Creative Commons License

Security must also be integrated into intelligent network management. SDN's programmability and centralized control introduce security concerns, including DDoS attacks and abnormal traffic that can affect both data-plane performance and controller resources (Ali *et al.*, 2023) [9]– (Perumal *et al.*, 2023) [10]. Recent surveys confirm growing interest in machine learning and deep learning for detecting attacks in SDN environments (Ali *et al.*, 2023) [9], (da Silva Ruffo *et al.*, 2024) [11].

The uploaded 6G review further emphasizes that future intelligent networks must jointly address QoS, latency, reliability, scalability, energy efficiency, AI security, and adaptive control rather than treating these dimensions independently (Ali *et al.*, 2026) [12]. The second uploaded paper demonstrates the broader value of combining AI, edge intelligence, security, and heterogeneous connectivity in dynamic environments (Islam *et al.*, 2026) [13]. These observations motivate the integrated framework proposed in this study.

1.1 Motivation

- Static routing cannot respond optimally to rapidly changing traffic conditions.
- Shortest-path routing may overload selected links even when alternative capacity exists.
- Single-objective traffic engineering can improve one metric while degrading another.
- Security detection is often separated from routing decisions.
- AI-based routing must account for computational overhead and the reliability of telemetry.
- Energy consumption should be considered alongside throughput, latency, and resilience.

1.2 Research objectives

- Develop an AI-driven adaptive traffic-engineering framework for SDN.
- Integrate real-time network telemetry with a DRL routing agent.
- Optimize throughput, latency, packet loss, link utilization, and energy consumption jointly.
- Introduce a lightweight anomaly-detection layer that can influence routing decisions.
- Evaluate the framework under normal, burst, congested, failure, and attack-oriented traffic conditions.
- Compare the proposed approach with conventional and learning-based routing baselines.

1.3 Main contributions

- A telemetry-driven SDN architecture for closed-loop intelligent traffic engineering.
- A DRL-based routing policy that uses multidimensional network state information.
- A multi-objective reward function combining performance, congestion, energy, and security terms.
- An integrated anomaly-intelligence layer for security-aware routing.
- A reproducible Mininet/Ryu-oriented experimental methodology.
- A research framework suitable for cloud, IoT, edge, and future 6G networking environments.

2. Related work

2.1 Software-defined networking and traffic engineering

SDN separates control logic from the forwarding infrastructure and enables programmable network behavior (Kreutz *et al.*, 2015) [1], (Rajahalme *et al.*, 2015) [2]. This architectural separation creates an opportunity for centralized traffic engineering because the controller can collect network state and modify forwarding rules. However, centralized visibility alone does not solve the optimization problem. Traffic engineering must continuously respond to link utilization, demand variation, failures, and QoS requirements.

The literature on SDN traffic engineering has evolved from conventional optimization and multipath methods toward learning-based approaches. Recent DRL research shows that an agent can learn routing policies from network state and optimize multiple performance objectives (Chen *et al.*, 2021) [3]– (Zhang *et al.*, 2023) [14].

2.2 DRL-based routing

Chen *et al.* introduced RL-Routing for SDN traffic engineering with throughput and delay as key objectives (Chen *et al.*, 2021) [3]. Kim *et al.* proposed a DRL routing optimization method that learns link weights based on traffic load and network performance (Kim *et al.*, 2022) [6]. Pei *et al.* proposed EfficientTE, which uses PPO-based DRL and online link selection to address traffic-engineering congestion (Pei *et al.*, 2024) [5].

Sanchez *et al.* developed a QoS-driven DRL routing method that considers link and queue metrics and evaluates performance using an SDN prototype (Aguirre Sanchez *et al.*, 2024) [7]. Wang *et al.* proposed DFRDRL, combining dynamic fuzzy routing with DRL and traffic-matrix prediction for latency and bandwidth guarantees (Wang *et al.*, 2024) [4]. Zhang *et al.* investigated multipath routing using DRL in SDN (Zhang *et al.*, 2023) [14]. These studies demonstrate the feasibility of intelligent routing but also indicate opportunities for broader integration of security and energy objectives.

2.3 AI-based security in SDN

SDN can be targeted by DDoS attacks because of the importance of the controller and the flow-management mechanisms. A systematic review by Ali *et al.* categorizes ML and DL techniques for DDoS detection in SDN (Ali *et al.*, 2023) [9]. Ruffo *et al.* reviewed deep-learning-based anomaly and intrusion detection for SDN and identified datasets, preprocessing, model selection, and evaluation metrics as important research considerations (da Silva Ruffo *et al.*, 2024) [11]. Other studies have investigated DNN-based DDoS detection and hybrid deep-learning approaches (Elubeyd *et al.*, 2023) [15], (Perumal *et al.*, 2023) [10].

The proposed framework differs by using security information as an additional input to the traffic-engineering decision process rather than treating anomaly detection as an isolated application.

2.4 Energy-aware intelligent networking

Energy efficiency is increasingly important in large-scale communication systems. RESDN demonstrated that SDN can dynamically redirect traffic and optimize energy-related network utilization while maintaining acceptable network performance (Assefa *et al.*, 2019) [16]. More recent intelligent networking work also combines routing adaptation with energy considerations (Andanaiah *et al.*, 2025) [17]. The proposed framework incorporates energy as one of the optimization objectives instead of optimizing routing only for delay or throughput.

3. Research gap

The reviewed literature establishes strong evidence for DRL-based SDN routing, QoS-aware traffic engineering, AI-based anomaly detection, and energy-aware network management. Nevertheless, these research directions are frequently evaluated separately. The present study targets the intersection of four requirements: adaptive routing, multi-objective traffic engineering, lightweight security intelligence, and energy-aware decision making.

4. Proposed AI-driven SDN framework

The proposed framework consists of five logical layers: network infrastructure, telemetry and monitoring, AI intelligence, SDN control, and service/application. The design follows the SDN principle of pro

26648784, 2026, 8(2), Downloaded from https://www.doi.org/10.33545/26648776.2026.v8.i2a.86308 by International Journal of Research in Engineering on [14/11/2026]. See the Terms and Conditions (https://www.engineeringpaper.net) for rules of use; OA articles are governed by the applicable Creative Commons License

grammable centralized control (Kreutz *et al.*, 2015) [1], while adding learning-based decision making and security intelligence.

4.1 Network infrastructure layer

This layer contains OpenFlow-capable switches, hosts, edge nodes, IoT devices, cloud servers, and communication links. The network is represented as a graph $G = (V, E)$, where V denotes nodes and E denotes links.

4.2 Telemetry and monitoring layer

The telemetry subsystem collects link bandwidth, packet rate, queue length, latency, packet loss, jitter, link utilization, flow statistics, and security-related indicators. These observations are normalized and passed to the AI layer. The telemetry interval should be selected so that it captures meaningful traffic changes without creating excessive controller overhead.

4.3 AI intelligence layer

Traffic prediction module: estimates short-term traffic demand.
DRL traffic-engineering module: selects forwarding actions.
Anomaly-detection module: identifies abnormal traffic patterns.
Policy manager: applies QoS and security constraints before controller installation.

4.4 SDN control layer

The SDN controller receives the selected routing action and translates it into forwarding rules. It also collects post-action telemetry and feeds the observed outcome back to the learning process, thereby creating a closed-loop control mechanism.

4.5 Service layer

The service layer represents cloud applications, IoT services, edge applications, video traffic, industrial applications, and future 6G services with different QoS requirements.

5. Mathematical formulation

Let the network be represented by $G = (V, E)$. For each link e∈E, utilization is defined as:

$$U_e(t) = B_e^{\text{used}}(t)/B_e^{\text{capacity}}$$

The state observed by the DRL agent at time t is defined as:

$$S_t = \left[D_t, L_t, P_t, U_t, Q_t, E_t, A_t\right]$$

where D_t is traffic demand, L_t is latency, P_t is packet loss, U_t is link utilization, Q_t is queue state, E_t is energy state, and A_t is the anomaly/security state.
The action a_t represents a routing or forwarding configuration selected by the agent. The multi-objective reward is defined as:

$$R_t = w_1 T_t - w_2 L_t - w_3 P_t - w_4 U_t - w_5 E_t - w_6 A_t$$

where T_t is normalized throughput and $w_1,...,w_6$ are non-negative weights with $\Sigma w_i = 1$. The weights can be tuned according to the application profile.
For a DQN implementation, the target value can be represented as:

$$y_t = r_t + \gamma \max_{a'} Q\left(s_{t+1}, a'; \theta -\right)$$

and the training loss is:

$$L(\theta) = E\left[\left(y_t - Q\left(s_t, a_t; \theta\right)\right)^2\right]$$

6. DRL-based traffic engineering algorithm

The proposed agent follows the observe–decide–act–learn loop. The algorithm can be implemented using DQN for discrete path choices or PPO/Actor-Critic methods when a larger or continuous action space is required.
Initialize SDN topology and controller.
Initialize the DRL policy and replay/experience mechanism.
Collect real-time telemetry.
Normalize the network state.
Estimate short-term traffic demand.
Calculate anomaly/security indicators.
Construct the state vector S_t.
Generate feasible candidate paths.
Select a routing action using the DRL policy.
Apply QoS and security constraints.
Install forwarding rules through the SDN controller.
Measure the resulting network performance.
Calculate the multi-objective reward.
Store the transition and update the DRL model.
Repeat until convergence or continuous deployment.

7. Lightweight security intelligence

The security module monitors flow-level features such as packet rate, byte rate, connection frequency, source-destination behavior, port distribution, and sudden deviations from normal traffic. An anomaly score can be represented as:

$$A(x) = ||x - \widehat{x}||$$

where x is the observed feature vector and $\hat{x}$ is the reconstructed or predicted normal representation. If $A(x) > \tau$, the flow is classified as anomalous. The anomaly score is then supplied to the routing agent as a penalty or constraint.
Possible responses include rerouting legitimate traffic away from congested or suspicious links, rate limiting suspicious flows, isolating an anomalous source, or triggering a higher-level inspection mechanism. The security layer should remain lightweight so that attack detection does not become a new source of routing delay.

8. Experimental methodology

• A reproducible emulation-based experiment is recommended. The primary environment can use Mininet for network emulation, Ryu or another OpenFlow controller for control-plane implementation, Python for orchestration, and PyTorch/TensorFlow for DRL. iPerf3 or D-ITG can be used to generate traffic. The experimental design should report topology, number of switches and hosts, link capacities, traffic distributions, DRL hyperparameters, training episodes, and evaluation seeds.

8.1 Traffic scenarios

- Normal traffic: moderate and relatively stable demand.
- Bursty traffic: sudden increase in flow demand.
- Congestion: multiple high-volume flows competing for limited capacity.
- Link failure: one or more links become unavailable.
- Attack traffic: abnormal high-rate or suspicious flows are injected.

8.2 Baseline methods

- Shortest-path/Dijkstra routing.
- Static SDN routing.
- ECMP or multipath routing.
- Conventional load-balanced routing.
- Existing DRL routing method.

2664878, 2026, 8(2), Downloaded from https://www.doi.org/10.33545/26648776.2026.v8.i2a.86308 by International Journal of Research in Engineering on [14/11/2026]. See the Terms and Conditions (https://www.engineeringpaper.net) for rules of use; OA articles are governed by the applicable Creative Commons License

- Proposed multi-objective DRL routing.

10. Experimental results and discussion

This section must contain measured results after implementation. Numerical values from other papers must not be transferred to the proposed SDN framework. The uploaded B-AIoA paper, for example, reports transportation-specific values such as 23.7% congestion reduction and 17.2% emissions reduction; these are not results of the present SDN study and therefore are not reused as experimental claims (Islam *et al.*, 2026) [13].

The following table is a reporting template for the actual experiment:

The expected analytical interpretation is that the proposed approach should adapt more effectively to burst traffic and congestion because its routing policy is conditioned on current telemetry. However, this expectation must be validated experimentally. Any claim of percentage improvement should be calculated from the measured results and reported with the experimental configuration and statistical variation.

11. Comparative analysis

The central research question is whether integrating routing, QoS, security, and energy information in a single learning objective provides a more balanced solution than optimizing one metric at a time. The comparison should therefore include both performance averages and robustness under changing conditions.

- Compare average and 95th-percentile latency.
- Compare throughput under increasing traffic load.
- Compare maximum and average link utilization.

Measure packet loss during congestion and recovery after failures.
Measure controller/agent processing overhead.
• Evaluate anomaly detection without and with routing feedback.
Perform an ablation study by removing the energy and security terms from the reward.

12. Ablation study

An ablation study is recommended to demonstrate the contribution of each proposed component. Four configurations can be compared:

- DRL without security or energy terms.
- DRL + energy-aware reward.
- DRL + security-aware reward.

Full proposed multi-objective DRL framework.
This design will help determine whether improvements arise from DRL alone or from the integrated multi-objective architecture.

13. Limitations

DRL training can require substantial computation and representative network data.
A model trained on one topology may not generalize directly to unseen topologies.
Telemetry delay or inaccurate measurements can lead to suboptimal decisions.
Security models can be affected by class imbalance and previously unseen attacks.
Frequent route changes can introduce control-plane overhead and transient packet disruption.
Energy estimation in a virtualized testbed may differ from physical-device energy consumption.

14. Future scope

Graph Neural Network and Graph Transformer representations for topology-aware DRL.
Multi-agent DRL for distributed or multi-domain SDN.
Federated learning for privacy-preserving network intelligence.
Explainable AI for controller decisions.
Adversarially robust DRL against manipulated telemetry.
Digital-twin-assisted training before deployment.
Integration with edge computing and network slicing.
Physical SDN testbed validation and deployment in 5G/6G environments.

15. Conclusion

This paper presents a research framework for adaptive AI-driven traffic engineering in Software-Defined Networks. The framework integrates real-time telemetry, Deep Reinforcement Learning, multi-objective optimization, and lightweight anomaly intelligence within a closed-loop SDN architecture. In contrast to fixed routing strategies, the proposed design allows forwarding policies to adapt to traffic dynamics, congestion, failures, QoS requirements, and security conditions.

The research is grounded in the uploaded studies' emphasis on adaptive AI, security, scalability, energy efficiency, heterogeneous environments, and intelligent control, while incorporating recent SDN-specific DRL and security literature (Ali *et al.*, 2026) [12], (Islam *et al.*, 2026) [13], (Chen *et al.*, 2021) [3]– (Assefa *et al.*, 2019) [16]. The proposed experimental methodology provides a reproducible basis for determining whether the integrated framework can improve network performance and resilience. Actual numerical results should be added only after the SDN experiments are executed.

References

1. Kreutz D, Ramos FMV, Veríssimo PE, Rothenberg CE, Azodolmolky S, Uhlig S. Software-defined networking: A comprehensive survey. Proceedings of the IEEE. 2015;103(1):14-76.
2. Rajahalme J, DHC *et al.* Software-Defined Networking (SDN): Layers and Architecture Terminology. RFC 7426, IETF. 2015.
3. Chen YR, Rezapour A, Tzeng WG, Tsai SC. RL-Routing: An SDN routing algorithm based on deep reinforcement learning. IEEE Transactions on Network Science and Engineering. 2021.
4. Wang Y, Othman M, Choo WO, Liu R, Wang X. DFRDRL: A dynamic fuzzy routing algorithm based on deep reinforcement learning with guaranteed latency and bandwidth for software-defined networks. Journal of Big Data. 2024;11:150.
5. Pei X, Sun P, Hu Y, Li D, Chen B, Tian L. Enabling efficient routing for traffic engineering in SDN with deep reinforcement learning. Computer Networks. 2024;241:110220.
6. Kim G, Kim Y, Lim H. Deep reinforcement learning-based routing on software-defined networks. IEEE Access. 2022;10:18121-18133.
7. Aguirre Sanchez LP, Shen Y, Guo M. DQS: A QoS-driven routing optimization approach in SDN using deep reinforcement learning. Journal of Parallel and Distributed Computing. 2024;188:104851.
8. Wang Y, Othman M, Choo WO, Liu R, Wang X. DFRDRL: A dynamic fuzzy routing algorithm based on deep reinforcement learning with guaranteed latency and bandwidth for software-defined networks. Journal of Big Data. 2024;11:150.
9. Ali TE, Chong YW, Manickam S. Machine learning techniques to detect a DDoS attack in SDN: A systematic review. Applied Sciences. 2023;13(5):3183.
10. Perumal K, Arockiasamy K. Optimized deep neural network based DDoS attack detection and bait mitigation process in software defined network. Concurrency and Computation: Practice and Experience. 2023;35(12):e7692.
11. da Silva Ruffo VG, Lent DMB, Komarchesqui M, Schiavon VF, de Assis MVO, Carvalho LF, Proença Jr ML. Anomaly and intrusion detection using deep learning for software-defined networks: A survey. Expert Systems with Applications. 2024;256:124982.
12. Ali T, Al-Khalidi M, Bashir AK. Intelligent and secure mobility management for 6G networks: A systematic review of AI-driven and physical-layer solutions. Alexandria Engineering Journal. 2026;145:253-286.

26648784, 2026, 8(2), Downloaded from https://www.doi.org/10.33545/26648776.2026.v8.i2a.86308 by International Journal of Research in Engineering on [14/11/2026]. See the Terms and Conditions (https://www.engineeringpaper.net) for rules of use; OA articles are governed by the applicable Creative Commons License

13. Islam R, Bose R, Khan AA, Emara AM, Roy S, Shaikh ZA, Sutradhar S. Blockchain-driven autonomous internet of auto in smart cities in India: A secure and intelligent framework for next-generation urban mobility. Energy Reports. 2026;15:109307.
14. Zhang Y, Qiu L, Xu Y, Wang X, Wang S, Paul A, Wu Z. Multi-path routing algorithm based on deep reinforcement learning for SDN. Applied Sciences. 2023;13(22):12520.
15. Elubeyd H, Yiltas-Kaplan D. Hybrid deep learning approach for automatic DoS/DDoS attacks detection in software-defined networks. Applied Sciences. 2023;13(6):3828.
16. Assefa BG, Özkasap Ö. RESDN: A novel metric and method for energy efficient routing in software defined networks. arXiv preprint arXiv:1905.12219. 2019.
17. Andanaiah NT, Rao MVP. Energy-efficient secure software-defined networking with reinforcement learning and Weierstrass cryptography. International Journal of Electrical and Computer Engineering. 2025;15(4).
18. Yang GY, Wang F, Yeh KH. GNN-enhanced traffic anomaly detection for next-generation SDN-enabled consumer electronics. arXiv preprint arXiv:2510.07109. 2025.

How to cite this article: Saini P, Rohilla C. AI-driven adaptive traffic engineering and secure resource optimization in software-defined networks. *International Journal of Research in Engineering*. 2026;SP-8(2):09-13. doi: https://www.doi.org/10.33545/26648776.2026.v8.i2a.86308

26648784, 2026, 8(2), Downloaded from https://www.doi.org/10.33545/26648776.2026.v8.i2a.86308 by International Journal of Research in Engineering on [14/11/2026]. See the Terms and Conditions (https://www.engineeringpaper.net) for rules of use; OA articles are governed by the applicable Creative Commons License