Meta-Reinforced Graph-Aware Secure SDN Framework Using Hybrid GWCC-Chaos Cryptography and Energy-Aware Routing

Nagaraju Tumakuru Andanaiah
Electronics Engineering Department, Faculty of Engineering & Technology, JAIN (Deemed-to-be University), Kanakapura Main Road, Bengaluru 562112, Karnataka, India | Department of Electronics & Communication Engineering, Government Engineering College, Ramanagara 562159, Karnataka, India
nagarajuta76@gmail.com (corresponding author)

Malode Vishwanatha Panduranga Rao
Department of Computer Science & Engineering, Faculty of Engineering & Technology, JAIN (Deemed-to-be University), Kanakapura Main Road, Bengaluru 562112, Karnataka, India
r.panduranga@jainuniversity.ac.in

Received: 12 July 2025 | Revised: 2 August 2025 | Accepted: 15 August 2025

 DOI: https://doi.org/10.48084/etasr.13328

ABSTRACT

The rapid growth of Internet of Things (IoT) devices, 5G connectivity, and data-driven services has increased the demand for intelligent, secure, and energy-efficient network infrastructures. Static routing choices, inflexible behavior, and high processing requirements of security schemes pose challenges in traditional Software-Defined Networking (SDN) models. In this paper, we present a new SDN framework in which Meta-Reinforcement Learning (Meta-RL) and Graph Attention Networks (GATs) are combined to support dynamic, topology-aware, and energy-efficient routing. Meta-RL enables the SDN controller to quickly adapt to changes in network conditions through prior knowledge, and GAT improves the learning process by focusing on the most relevant topological characteristics. The framework employs a hybrid cryptographic model based on Genus Weierstrass Curve Cryptography (GWCC), combined with chaotic map encryption to provide secure data transmission without adversely affecting real-time performance. The combined architecture enhances entropy and reduces processing latency. The proposed system is implemented and tested on a Mininet-based platform with a multi-hop structure using an OpenFlow topology. The results show significant improvements in throughput, latency, packet delivery ratio, energy efficiency, and Area Under the Curve (AUC) compared with current models, including Deep Q-Network (DQN), Q-learning-based Routing (QLR), and Elliptic Curve Cryptography (ECC)-based routing.

Keywords-Meta-Reinforcement Learning (Meta-RL); Graph Attention Networks (GATs); energy-efficient routing; hybrid cryptography; chaotic map encryption

I. INTRODUCTION

The explosive rise in the number of innovative technologies, including the Internet of Things (IoT), fifth-generation (5G) mobile networks, and Artificial Intelligence (AI)-based services has dramatically increased the complexity and magnitude of network traffic [1]. The demand for real-time responsiveness, low latency, and high throughput has never been higher as the digital ecosystems continue to grow in scale. However, traditional network infrastructure based on fixed deployment and manual configuration processes is not suitable to meet the fast-changing needs of modern communication systems [2]. Such traditional methods are not flexible or scalable enough to accommodate dynamic workloads and unpredictable traffic patterns.

In this regard, Software-Defined Networking (SDN) has become an effective framework for network transformation, facilitating manipulation of the network in a centralized setting and programmable resource distribution [3]. The decoupling of the data and control planes by SDN provides network operators with a more flexible and scalable mechanism for managing infrastructure, as shown in Figure 1. Despite these benefits, SDN continues to pose technical challenges. Three fundamental problems remain unsolved: (1) how to dynamically adjust routing policies as network topologies vary, (2) how to transmit data with optimal energy efficiency, especially in dense and high-traffic networks, (3) how to design lightweight yet robust security structures that do not degrade performance. Current solutions are often inadequate because they rely on predetermined Machine Learning (ML) models, which cannot adapt to real-time network conditions [4, 5].

Traditional cryptographic approaches, while effective in securing communications, are computationally heavy and therefore unsuitable for latency-sensitive systems like SDN. These limitations necessitate a smarter, holistic solution for routing, resource optimization, and security [6].

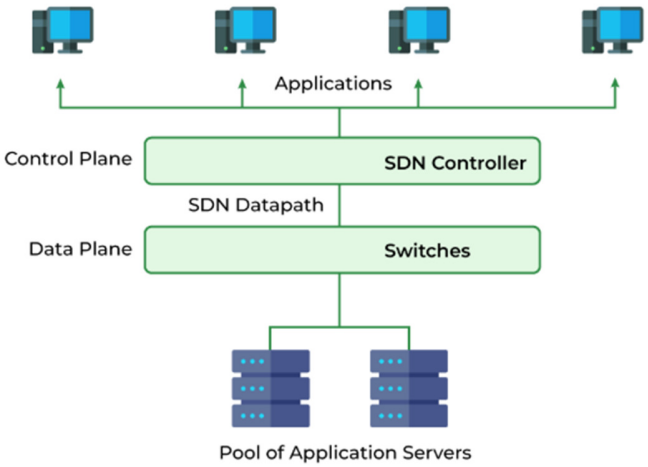

Fig. 1. SDN architecture.

The IoT has rapidly evolved into a transformative technology, significantly impacting numerous industries by enabling connectivity among a wide array of devices, from household gadgets to complex industrial systems [7]. These devices communicate and exchange data with each other and broader systems over the internet, leading to enhanced automation and improved operational efficiency. However, the heterogeneous nature of devices within SDN-based Wireless Sensor Network (WSN) IoT environments introduces several challenges, particularly in security, deployment adaptability, and energy management [8]. Integrating SDN with WSN-IoT has become increasingly important, offering a robust framework to manage these challenges effectively.

One key advancement in this domain is the incorporation of ML algorithms, which has attracted significant research interest [9]. ML-driven approaches encompass a variety of techniques, including classification models, predictive analytics for anticipating network behavior, and real-time rule optimization based on current network conditions. By analyzing historical routing patterns, ML algorithms can make accurate predictions about future network states, enabling more intelligent and adaptive routing strategies [10]. These intelligent models take into account multiple factors, such as energy limitations, congestion levels, and node availability, when determining routing paths, ultimately improving energy efficiency and data transmission reliability.

In one study, Deep Reinforcement Learning (DRL) was applied to dynamic task scheduling and assignment within SDN to reduce network latency and improve energy usage while respecting application-specific constraints [11]. This approach treats task management as an energy-aware deep learning problem and has shown promising outcomes in optimizing overall performance. Further research has explored the integration of Q-routing algorithms within SDN architectures to improve routing efficiency in large-scale IoT deployments [12]. This method has demonstrated improvements in packet delivery ratio, latency, and energy efficiency, making it highly effective for managing high-volume data transmission in complex IoT networks.

To achieve energy efficiency, Reinforcement Learning (RL) techniques have been incorporated into SDN architectures, enabling networks to dynamically adapt routing strategies in response to real-time traffic patterns and energy consumption levels. RL algorithms allow agents to learn optimal policies through trial and error, interacting with the environment to maximize cumulative rewards [13]. In energy-aware routing, RL algorithms can be trained to make routing decisions that minimize energy consumption while satisfying performance constraints, such as latency and bandwidth requirements [14]. In SDN, this translates to controllers learning to make optimal routing decisions based on network states and feedback signals, including energy consumption metrics from devices, traffic flow statistics, and performance indicators [15].

Elliptic Curve Cryptography (ECC) offers a compelling alternative to traditional public-key cryptosystems like Rivest–Shamir–Adleman (RSA), particularly in resource-constrained environments [16]. ECC's strength lies in the difficulty of solving the elliptic curve discrete logarithm problem, which allows for smaller key sizes compared with RSA while maintaining equivalent security levels [17]. This characteristic makes ECC well-suited for SDN deployments, where network devices often have limited processing power and memory [18]. ECC can be applied for secure key exchange protocols, digital signatures to authenticate control plane messages, and encryption of transmitted data. Its efficiency reduces computational overhead, minimizing the impact on network performance. Within ECC, Weierstrass curves are widely adopted due to their mathematical properties and ease of implementation [19]. These curves, defined by a specific equation, facilitate efficient point addition and scalar multiplication, which are fundamental to ECC-based cryptographic protocols.

Recent research has focused on leveraging ML techniques, particularly Graph Neural Networks (GNNs) such as Graph Attention Networks (GATs), to enhance security in SDN environments [20]. The growing complexity of network infrastructures and the evolving threat landscape necessitate intelligent security solutions that can adapt to new attacks and proactively mitigate risks. Graph-based ML techniques are motivated by the inherent graph-like structure of networks, where nodes represent devices and edges represent communication links [21]. By representing network traffic patterns and security events as graphs, these techniques can capture complex relationships that traditional methods may miss.

ML and Deep Learning (DL) methods have become increasingly popular for identifying and mitigating threats in network infrastructures [22]. Intrusion Detection Systems (IDS) benefit from ML, as models can learn and adapt to new situations based on data. One area where GATs contribute to secure routing in SDN is the detection and mitigation of routing

anomalies [23]. By analyzing traffic patterns and identifying deviations from normal behavior, GATs can detect malicious activities, such as DoS attacks, traffic redirection, and data injection attacks [24-26]. GATs can learn the relationships between network nodes and identify anomalous traffic flows that may indicate security breaches [27]. By learning the characteristics of normal and malicious traffic patterns, GATs can effectively classify traffic and prioritize security alerts, reducing the burden on human analysts. Furthermore, GATs can be used to optimize routing paths to compromised links, enhancing network resilience and security [28].

To overcome these challenges, this paper proposes a new SDN architecture that is intelligent and secure, accommodating three modern subsystems: (1) Meta-Reinforcement Learning (Meta-RL) to quickly adjust policies according to varying network conditions and leverage previous learning experiences, (2) GATs to learn topological representations and predict optimal routes based on network graph structure, and (3) a hybrid cryptographic scheme that combines Genus Weierstrass Curve Cryptography (GWCC) with chaotic map encryption for lightweight, high-security encryption suitable for dynamic networks. The routing intelligence integrates GAT and Meta-RL, enabling the system to analyze traffic flow and underlying graph structure in real time, yielding precise and efficient route predictions. Consequently, the SDN controller can flexibly adapt routing paths to minimize latency and congestion during high traffic loads or unexpected topological changes. Simultaneously, the security layer introduces chaos-based key generation resistant to differential and linear attacks. GWCC integration provides a small cryptographic footprint, suitable for SDN devices with constrained resources.

To validate the proposed solution, Mininet, a popular network emulation framework, was employed for simulations in a multi-hop OpenFlow-based SDN topology. Performance was evaluated in terms of throughput, latency, energy usage, and crypto-resilience. The findings demonstrate that the proposed system outperforms current state-of-the-art techniques, maintaining a high packet delivery rate and minimizing latency during bursty traffic events and congestion. Energy efficiency was also significantly enhanced, addressing one of the main limitations of conventional SDN implementations.

II. METHODOLOGY

In this section, a detailed description of the basic building blocks that make up the proposed SDN architecture is offered. Three important modules are integrated into the architecture (Figure 2): Meta-RL to support the quick and intelligent adaptation of routing strategies to changing network dynamics, GAT to gain topology-understanding, feature extraction, and informed decision-making capabilities by modeling the relationships between network nodes, and a hybrid cryptographic scheme to provide lightweight yet secure data transmission across the network using GWCC in conjunction with chaotic map encryption. All of these factors are essential to improving the overall flexibility, effectiveness, and security of the SDN landscape.

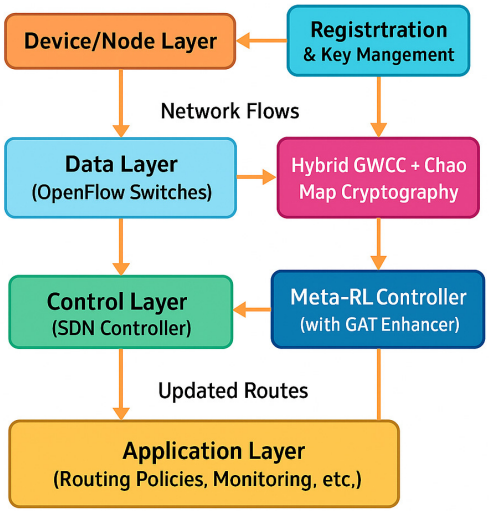

Fig. 2. Functional diagram of the proposed SDN method.

In contrast to conventional RL approaches, Meta-RL equips the agent with the capability to not only learn from a broad distribution of prior experiences but also to rapidly adjust to new network topologies and unforeseen traffic patterns. This adaptability is particularly valuable in dynamic SDN environments, where real-time changes in topology or traffic demand quick and effective decision-making. Figure 3 shows the workflow and key steps of the Meta-RL method.

To enable rapid adaptation, we use the Meta-RL algorithm with a Model-Agnostic Meta-Learning (MAML) framework. MAML is appropriate for problems characterized by the need to learn quickly with sparse data, as it optimizes the initialization parameters of the agent so that minimal adaptation during fine-tuning is necessary to work on previously unseen tasks effectively. During the meta-learning stage, the agent is trained across a wide variety of simulated SDN environments created using Mininet. Each environment represents a different network topology or traffic scenario. The agent learns an initial policy, denoted by the parameter set θ, which is optimized to be sensitive to future task-specific updates. This ensures the policy does not overfit to any single environment but is general enough to be quickly adapted when needed.

When the network undergoes changes, such as a new traffic burst, the learned policy θ is updated into a task-specific version θ' using gradient descent. After completing updates across several task instances, the meta-parameters θ are refined by aggregating the gradients obtained from all task-specific adaptations. This ensures that θ continues to serve as an efficient starting point for future adaptations. The meta-update is given by (1):

$$\theta = \theta - \beta \nabla_\theta \sum_{task} L_{task}(f_{\theta'}) \quad (1)$$

To guide the learning process, a custom reward function is defined to reflect multiple performance objectives within the SDN context. It takes the form in (2):

$$R = w_1 \cdot PDR - w_2 \cdot Latency - w_3 \cdot Energy \quad (2)$$

Here, PDR stands for packet delivery ratio, and w_1, w_2, w_3 are tunable weights assigned to prioritize different network goals, such as throughput, delay minimization, and energy efficiency. The policy θ', once adapted to the current network state, is employed by the SDN controller to dynamically determine optimal routing paths. This allows the controller to respond in real time to varying network conditions, significantly improving the quality of service and overall resource utilization.

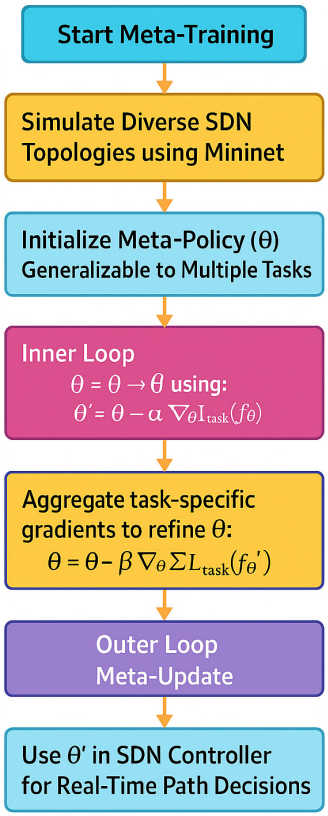

Fig. 3. Workflow and key steps of the Meta-RL method.

To ensure the security of both the control and data planes in SDN, a comprehensive hybrid cryptographic approach is introduced. This proposed scheme combines the strengths of two distinct cryptographic strategies: GWCC and chaotic map-based encryption, offering both robust security and lightweight implementation suitable for real-time network environments. To further enhance the unpredictability and randomness of the cryptographic process, the system incorporates a chaotic map, specifically the logistic map. This nonlinear function is defined as in (3):

$$x_{n+1} = r \cdot x_n(1 - x_n), \quad 0 < r \leq 4 \tag{3}$$

This mathematical expression generates a chaotic sequence when the parameter r is chosen appropriately. The sequence exhibits sensitive dependence on initial conditions, making it ideal for generating pseudo-random numbers. The simulation environment is summarized in Table I.

TABLE I. SIMULATION CONFIGURATION

Parameter	Configuration
Simulation tool	Mininet
Network topology	10 OpenFlow switches, 50 hosts
Controller	Floodlight with integrated Meta-RL and GAT modules
Link bandwidth	Configurable between 10 Mbps and 1 Gbps
Link delay	Randomized between 2 ms and 50 ms
Packet loss rate	Configurable between 0.01% and 1%

III. RESULTS AND DISCUSSION

This section evaluates the effectiveness of the proposed intelligent and secure SDN framework by comparing it with existing routing and cryptographic methods. The simulations were conducted in a Mininet-based virtualized SDN environment using a multi-hop OpenFlow topology consisting of 10 switches and 50 hosts. The performance was analyzed across various metrics including latency, throughput, energy consumption, encryption/decryption time, and routing accuracy.

The Area Under the Curve (AUC) score comparison in Figure 4 demonstrates that the proposed model, integrating Meta-RL, GAT, and hybrid GWCC-chaotic cryptography, achieves the highest routing accuracy with an AUC score of 0.985. This indicates superior decision-making capability in dynamic network conditions. In contrast, traditional models like Energy-Sensitive Reinforcement Learning with Genus Weierstrass Curve Cryptography (ESR-RL+GWCC) (0.98), Deep Q-Network (DQN) (0.95), and Q-learning-based Routing (QLR) (0.92) show gradually decreasing performance due to slower adaptability and limited context awareness. ECC-based and static OpenFlow routing approaches perform the worst, with AUC scores of 0.88 and 0.82, respectively, highlighting their inadequacy for real-time, intelligent SDN environments.

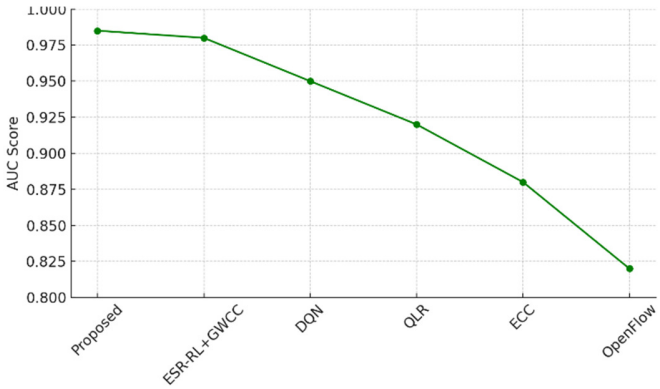

Fig. 4. AUC score comparison of different SDN models.

Figure 5 illustrates the encryption and decryption times for different SDN models, highlighting the computational efficiency of each cryptographic approach. The proposed model, which combines GWCC with chaotic map encryption, exhibits the lowest encryption (1.1 ms) and decryption times (0.9 ms), making it the most suitable for real-time secure communication. In comparison, ESR-RL+GWCC shows

slightly higher processing times, whereas traditional models such as DQN, QLR, and ECC demonstrate a steady increase in both metrics due to more complex or less optimized cryptographic operations. The OpenFlow model records the highest encryption (3.0 ms) and decryption (2.8 ms) times, indicating its inefficiency in handling secure transmissions under time-sensitive conditions.

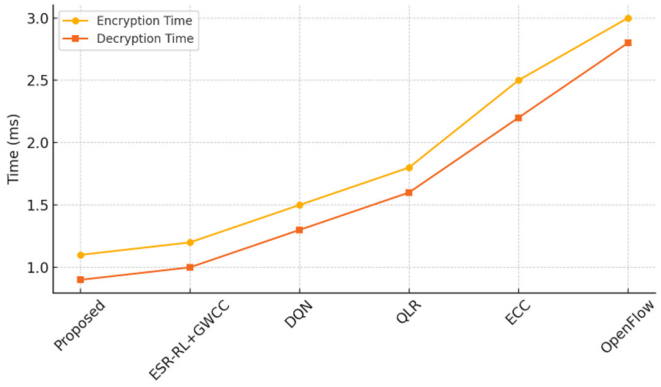

Fig. 5. Encryption and decryption times of different SDN models.

Figure 6 presents the energy consumption per packet across various SDN routing approaches. The proposed model, integrating Meta-RL, GAT, and hybrid GWCC-chaotic cryptography, achieves the lowest energy usage at approximately 0.31 J/packet, demonstrating its efficiency in resource-constrained environments. ESR-RL+GWCC also performs relatively well but consumes slightly more energy. Traditional reinforcement learning methods like DQN and QLR exhibit increasing energy requirements due to less optimized routing and lack of topology-aware adjustments. ECC-based routing and the basic OpenFlow approach show the highest energy consumption, with OpenFlow reaching 0.62 J/packet, indicating inefficient routing and lack of energy-awareness.

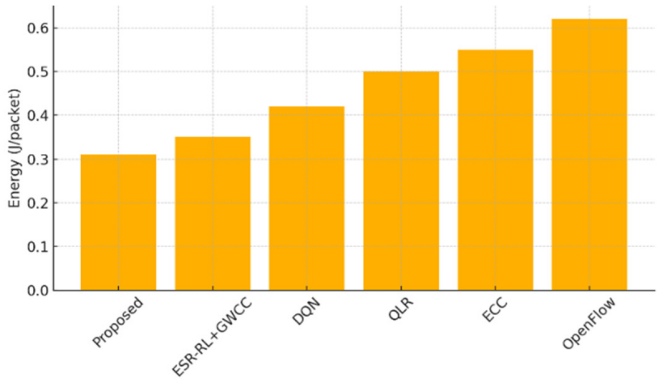

Fig. 6. Energy consumption per packet of different SDN models.

The throughput comparison in Figure 7 clearly shows that the proposed framework delivers the highest data transmission rate, achieving over 1020 Mbps. This superior performance is attributed to the integration of Meta-RL and GAT, which dynamically optimize routing paths based on real-time network conditions. ESR-RL+GWCC follows closely, whereas DQN and QLR exhibit moderate throughput due to slower adaptability and less efficient route prediction. Traditional methods such as ECC-based and OpenFlow routing yield the lowest throughput, with OpenFlow falling below 600 Mbps, highlighting its limitations in dynamic, high-load environments.

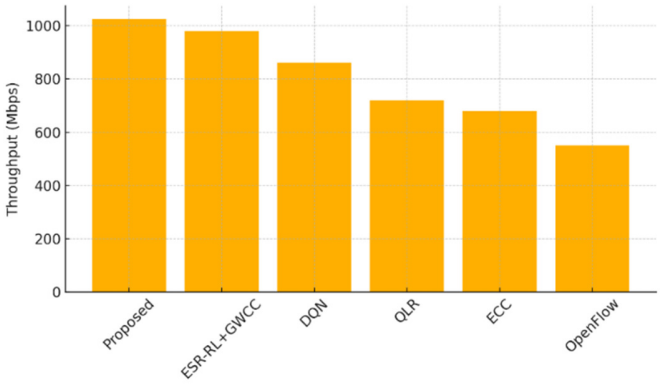

Fig. 7. Throughput comparison of different SDN models.

The experimental results demonstrate that the proposed SDN framework, which combines Meta-RL, GAT, and hybrid GWCC-chaotic cryptography, outperforms existing models across all evaluated metrics. It achieves the highest throughput and packet delivery ratio while maintaining low latency and energy consumption. The encryption and decryption times are significantly reduced due to the lightweight hybrid cryptographic design. Furthermore, the model delivers superior routing accuracy, as indicated by its top AUC score, owing to the adaptive learning capabilities of Meta-RL and the topology-aware insights from GAT.

IV. CONCLUSION

This paper proposes an efficient and intelligent architecture for Software-Defined Networking (SDN) that addresses major challenges in current network settings, namely routing flexibility, energy consumption, and secure data transmission. By integrating Meta-Reinforcement Learning (Meta-RL) and Graph Attention Networks (GATs), the proposed framework enables the SDN controller to implement topology-aware routing decisions in real time based on the network context. This results in significant improvements in network throughput, latency, and packet delivery in dynamic networks.

To maintain security that is both lightweight and robust, the framework employs a hybrid cryptographic scheme that combines Genus Weierstrass Curve Cryptography (GWCC) with chaotic map encryption. This combination maximizes entropy and minimizes computational overhead, making it well suited for time-sensitive and resource-constrained environments such as SDN deployments.

Simulation results using Mininet in a multi-hop OpenFlow network demonstrate that the proposed framework outperforms baseline models, including Energy-Sensitive Reinforcement

Learning with Genus Weierstrass Curve Cryptography (ESR-RL+GWCC), Deep Q-Network (DQN), Q-learning-based Routing (QLR), Elliptic Curve Cryptography (ECC)-based routing, and standard OpenFlow across metrics such as energy consumption, encryption/decryption time, and Area Under the Curve (AUC) score.

Future research will focus on generalizing the proposed system to actual hardware deployments in real-world networks. This will support open infrastructures by leveraging Network Function Virtualization (NFV) frameworks to enable scalable and dynamic service chaining in SDN implementations. In addition, efforts will a aim to enhance the framework's resilience against emerging cyber threats, including zero-day attacks, through continuous learning and adversarial training methods. These advances will facilitate the deployment of intelligent, dynamic, and secure SDN in critical infrastructure networks.

REFERENCES

[1] D. A. Zainaddin, Z. M. Hanapi, M. Othman, Z. Ahmad 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, https://doi.org/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, Apr. 2024, Art. no. 100728, https://doi.org/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, https://doi.org/10.1109/ACCESS.2024.3393548.

[4] R. Wazirali, R. Ahmad, and S. Alhiyari, "SDN-OpenFlow Topology Discovery: An Overview of Performance Issues," *Applied Sciences*, vol. 11, no. 15, Aug. 2021, Art. no. 6999, https://doi.org/10.3390/app11156999.

[5] Md. 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, Aug. 2023, Art. no. 100822, https://doi.org/10.1016/j.measen.2023.100822.

[6] A. Narwaria and A. P. Mazumdar, "Software-Defined Wireless Sensor Network: A Comprehensive Survey," *Journal of Network and Computer Applications*, vol. 215, Jun. 2023, Art. no. 103636, https://doi.org/10.1016/j.jnca.2023.103636.

[7] S. Jagadeesan, C. N. Ravi, M. Sujatha, S. S. Southry, J. Sundararajan, and Ch. 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*, Erode, India, 2023, pp. 375–380, https://doi.org/10.1109/ICSCDS56580.2023.10104874.

[8] 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, Dec. 2023, Art. no. 110105, https://doi.org/10.1016/j.comnet.2023.110105.

[9] B. Sellami, A. Hakiri, S. B. Yahia, and P. Berthou, "Energy-aware task scheduling and offloading using deep reinforcement learning in SDN-enabled IoT network," *Computer Networks*, vol. 210, Jun. 2022, Art. no. 108957, https://doi.org/10.1016/j.comnet.2022.108957.

[10] 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, https://doi.org/10.1109/JIOT.2020.3002427.

[11] P. Prasada, Sathisha, and K. Shreya Prabhu, "Novel Approach in IoT-Based Smart Road with Traffic Decongestion Strategy for Smart Cities," in *Advances in Communication, Signal Processing, VLSI, and Embedded Systems: Select Proceedings of VSPICE 2019*, Nitte, Karnataka, India, 2020, pp. 195–202, https://doi.org/10.1007/978-981-15-0626-0_16.

[12] 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, https://doi.org/10.1109/JIOT.2021.3102130.

[13] L. R. S. Campos, R. D. Oliveira, J. D. Melo, and A. D. D. Neto, "Overhead-Controlled Routing in WSNs with Reinforcement Learning," in *Intelligent Data Engineering and Automated Learning - IDEAL 2012: 13th International Conference*, Natal, Brazil, 2012, pp. 622–629, https://doi.org/10.1007/978-3-642-32639-4_75.

[14] V. Singh, S.-S. Chen, M. Singhania, B. Nanavati, A. kumar kar, and A. Gupta, "How are reinforcement learning and deep learning algorithms used for big data based decision making in financial industries–A review and research agenda," *International Journal of Information Management Data Insights*, vol. 2, no. 2, Nov. 2022, Art. no. 100094, https://doi.org/10.1016/j.jjimei.2022.100094.

[15] H. Ju, S. Kim, Y. Kim, and B. Shim, "Energy-Efficient Ultra-Dense Network With Deep Reinforcement Learning," *IEEE Transactions on Wireless Communications*, vol. 21, no. 8, pp. 6539–6552, Aug. 2022, https://doi.org/10.1109/TWC.2022.3150425.

[16] J. Singh and S. Behal, "Detection and mitigation of DDoS attacks in SDN: A comprehensive review, research challenges and future directions," *Computer Science Review*, vol. 37, Aug. 2020, Art. no. 100279, https://doi.org/10.1016/j.cosrev.2020.100279.

[17] G. Logeswari, S. Bose, and T. Anitha, "An Intrusion Detection System for SDN Using Machine Learning," *Intelligent Automation & Soft Computing*, vol. 35, no. 1, pp. 867–880, Jun. 2022, https://doi.org/10.32604/iasc.2023.026769.

[18] G. S. Quirino, A. R. L. Ribeiro, and E. D. Moreno, "Asymmetric Encryption in Wireless Sensor Networks," in *Wireless Sensor Networks - Technology and Protocols*, M. A. Matin, Ed. London, United Kingdom: IntechOpen, 2012, ch. 10, https://doi.org/10.5772/48464.

[19] A. M. Awaludin, H. T. Larasati, and H. Kim, "High-Speed and Unified ECC Processor for Generic Weierstrass Curves over GF(p) on FPGA," *Sensors*, vol. 21, no. 4, Feb. 2021, Art. no. 1451, https://doi.org/10.3390/s21041451.

[20] R. Swami, M. Dave, and V. Ranga, "Software-defined Networking-based DDoS Defense Mechanisms," *ACM Computing Surveys*, vol. 52, no. 2, Apr. 2019, Art. no. 28, https://doi.org/10.1145/3301614.

[21] L. Zhang, "Research on Control Algorithm Theory and Visual Recognition Algorithm of Network Devices," in *2023 IEEE 6th International Conference on Information Systems and Computer Aided Education*, Dalian, China, 2023, pp. 956–961, https://doi.org/10.1109/ICISCAE59047.2023.10393786.

[22] T. E. Ali, Y.-W. Chong, and S. Manickam, "Machine Learning Techniques to Detect a DDoS Attack in SDN: A Systematic Review," *Applied Sciences*, vol. 13, no. 5, Mar. 2023, Art. no. 3183, https://doi.org/10.3390/app13053183.

[23] S. Ennaji, F. D. Gaspari, D. Hitaj, A. Kbidi, and L. V. Mancini, "Adversarial Challenges in Network Intrusion Detection Systems: Research Insights and Future Prospects." arXiv, Oct. 22, 2024, https://doi.org/10.48550/arXiv.2409.18736.

[24] Q. Liu, H. Ruan, H. Li, X. Li, and X. Wang, "REAL-GUARD: A Machine Learning based Real-time Mechanism for Combining Packet and Flow Features to Mitigating Network Attacks in SDN," in *Proceedings of the 2020 International Conference on Cyberspace Innovation of Advanced Technologies*, Guangzhou, China, 2021, pp. 451–458, https://doi.org/10.1145/3444370.3444612.

[25] D. S. Ahmed, A. A. Abdulhameed, and M. T. Gaata, "A Systematic Literature Review on Cyber Attack Detection in Software-Define Networking (SDN)," *Mesopotamian Journal of CyberSecurity*, vol. 4, no. 3, pp. 86–135, Nov. 2024, https://doi.org/10.58496/MJCS/2024/018.

[26] P. Almasan, J. Suárez-Varela, B. Wu, S. Xiao, P. Barlet-Ros, and A. Cabellos-Aparicio, "Towards Real-Time Routing Optimization with Deep Reinforcement Learning: Open Challenges," in *2021 IEEE 22nd International Conference on High Performance Switching and Routing*,

Paris, France, 2021, pp. 1–6, https://doi.org/10.1109/HPSR52026.2021.9481864.

[27] M. H. Alanazi, "G-GANS for Adaptive Learning in Dynamic Network Slices," *Engineering, Technology & Applied Science Research*, vol. 14, no. 3, pp. 14327–14341, Jun. 2024, https://doi.org/10.48084/etasr.7046.

[28] X. Mai, Q. Fu, and Y. Chen, "Packet Routing with Graph Attention Multi-Agent Reinforcement Learning," in *2021 IEEE Global Communications Conference (GLOBECOM)*, Madrid, Spain, 2021, pp. 1–6, https://doi.org/10.1109/GLOBECOM46510.2021.9685941.