IJSRA

International Journal of Science and Research Archive

eISSN: 2582-8185
Cross Ref DOI: 10.30574/ijsra
Journal homepage: https://ijsra.net/

Int. J. Sci. Res. Arch.
IJSRA
International Journal of Science and Research Archive
Research Journal Archive, INDIA

(Research Article)

Check for updates

Lightweight deep learning for real-time DDoS detection in SDN using programmable data planes

Chiranjeevi Anand [1, *] and Prajakta Bhimsen Sitap [2]

[1] *Department of Engineering, Faculty of MCA, Ajeenkya D.Y. Patil University, Pune, India.*
[2] *Assistant Professor, Faculty of MCA, Ajeenkya D.Y. Patil University, Pune, India.*

International Journal of Science and Research Archive, 2025, 15(02), 199-206

Publication history: Received on 23 March 2025; revised on 05 May 2025; accepted on 08 May 2025

Article DOI: https://doi.org/10.30574/ijsra.2025.15.2.1296

Abstract

Distributed Denial of Service (DDoS) attacks are a very continuous and ever-increasing threat against the Software-Defined Networking (SDN) environments as the centralized control plane serves as the most essential vulnerability point in these domains. This research provides a lightweight deep learning mechanism for the realtime detection of DDoS attacks, where DDoS detection is carried out on a programmable data plane, offloading from the SDN controller. A compact Convolutional Neural Network (CNN) model is deployed at the P4-enabled switches such that it could enable high-speed, low-latency detection that could be suitable for resource-scarce devices. The experiments were performed on standard datasets that showed detection accuracy of more than 99% with significantly reduced latencies and resource consumption in detection, proving beyond doubt its efficiency when compared with existing state-of-the-art mechanisms. This paper provides an all-inclusive discussion on the architecture, methodology, results, and future implications for SDN security deployments.

Keywords: DDoS; SDN; Deep Learning; Programmable Data Plane; CNN; Network Security

1. Introduction

The advent of Software-Defined Networking (SDN) has ushered in a new paradigm with respect to modern network infrastructures by adding centralized control, programmability, and dynamic policy enforcement. With this architectural shift come other vulnerabilities, however, and some of these make SDN implementations attractive prey for Distributed Denial of Service (DDoS) attack vectors. DDoS attacks lead to disruptions in network availability either by overwhelming the SDN controller with huge amounts of traffic or by saturating the data plane, causing massive degradation of services or complete outages. Most of the existing detection mechanisms are limited by the dependency that they place on the SDN controller. Such an issue would lead to bottleneck situations, which induce an increase in the vulnerability. It is therefore evident that there is an urgent need for scalable, real-time, and resource-efficient detection mechanisms capable of deployment at the network edge, especially since the DDoS attack vectors are achieving much higher scales and sophistication. Therefore, this research will address these issues through the development of lightweight deep learning solutions that can be deployed at the data plane for real-time detection and mitigation of DDoS attacks without taxing the controller.

2. Literature Review

Distributed denial of service (DDoS) attacks toward Software-Defined Networking (SDN) environments entail the great need for intelligent real-time mitigation. In the past decade, many universities have conducted related studies and created industrial frameworks that tackle such threats by means of machine learning (ML), deep learning (DL), and

[*] Corresponding author: Chiranjeevi Anand

programmable data planes. However, while many of the proposed models showed promising levels of accuracy in simulated scenarios, they often lack resource efficiency, scalability, and real-time applicability in edge contexts and data planes.

SVM with Genetic Optimization: Sahoo et al. designed an SVM detection model boosted by kernel principal component analysis (KPCA) and genetic algorithms for parameter tuning. While the approach betters detection accuracy and training time, it remains predominantly dependent on offline feature engineering and high processing power. Thus, it falls short of being more practical for in-network, real-time detection in SDN applications.

Hybrid Feature Selection Techniques: Nandi et al. and Bagyalakshmi et al. adopted hybrid feature-selection techniques that combined Relief, Information Gain, and Chi-square methods aimed at improving classification models like Random Forests and Naive Bayes. Though yielding improved detection accuracy, such techniques could not scale very well and used static data preprocessing that is not feasible for fast and real-time analyses of dynamic SDN traffic.

Detection of DDoS with Deep Neural Networks: Cil and colleagues have applied deep neural networks (DNN) on the CICDDoS2019 dataset, where they have attained nearly perfect accuracy, that is 99.99% binary detection and over 94% in multiclass classification. The problem is that this model requires heavy memory and computation power, which makes it not very suitable for lightweight edge deployment.

LSTM and Hybrid DL Models: Shurman et al. have used long short-term memory (LSTM) networks in a hybrid intrusion detection system meant for IoT. The approach did very well in recognizing DrDoS attack traffic in the test datasets, but it had some issues regarding inference latency and was not flexible enough for deployment on P4-enabled data planes.

Sentiment-Based Predictive Models: Alguliyev et al. worked on the social media sentiment analysis that used structured data with 14-layer CNNs and LSTM to forecast DDoS. However, the model was problematic in terms of reliability because it mainly relied on uploads and did not involve detection at the packet level or programmable infrastructure.

Autoencoder-based Classification Models: A stacked autoencoder with multi-layer perceptron (SAE-MLP) was proposed by Ahuja et al. achieving an accuracy of 99.75% in SDN traffic classification. Similarly, Agarwal et al. presented a convolutional autoencoder that gave results of decent accuracy but remains untested in real-time deployments or against hardware constraints that are typical of SDN switches.

GLD-Net and Topological Features: Guo et al. proposed GLD-Net, a deep learning model that combined traffic and topological features. It gave a detection accuracy of 99.3%, but it was not such an optimized model for lightweight or embedment network environments such as P4-enabled switches.

LUCID for Lightweight Data Plane Detection: Doriguzzi-Corin et al. devised through LUCID one such detection model based on deep learning; LUCID was specifically built for programmable switches. Even though LUCID is light compared to other deep models, it translates into overhead during packet classification and lacks flexibility to integrate CNN-based detection pipelines.

Programmable Plane Offloading: In this work, Lapolli presented an architecture for an intelligent distribution of detection logic from the SDN controller on P4 switches. Deep learning's absence from the framework limited its adaptability and threat classification capability.

3. Problem Statement and Objectives

3.1. Problem Statement

How can real-time detection of DDoS attacks, and detection with high accuracy, be done in SDN and not overload the SDN controller or require computation resources?

Objectives

The goals, therefore, are as follows:

- To design a lightweight deep learning model that can be deployed on programmable data planes
- To achieve high detection accuracy and low latency DDoS detection in real time
- To minimize resource usage in the deployment on resource-constrained devices

- To benchmark the designed approach against existing state-of-the-art ones

4. Materials and Methods

4.1. System Architecture

The system being proposed has the following components:

- Programmable Data Plane: This uses P4 for packet feature extraction and analysis on a network switch.
- Lightweight CNN Model: This is a compact neural network whose design has been optimized to run under resource constraints.
- Control Plane Interface: This handles model updating, configuration, and response to attack mitigation.

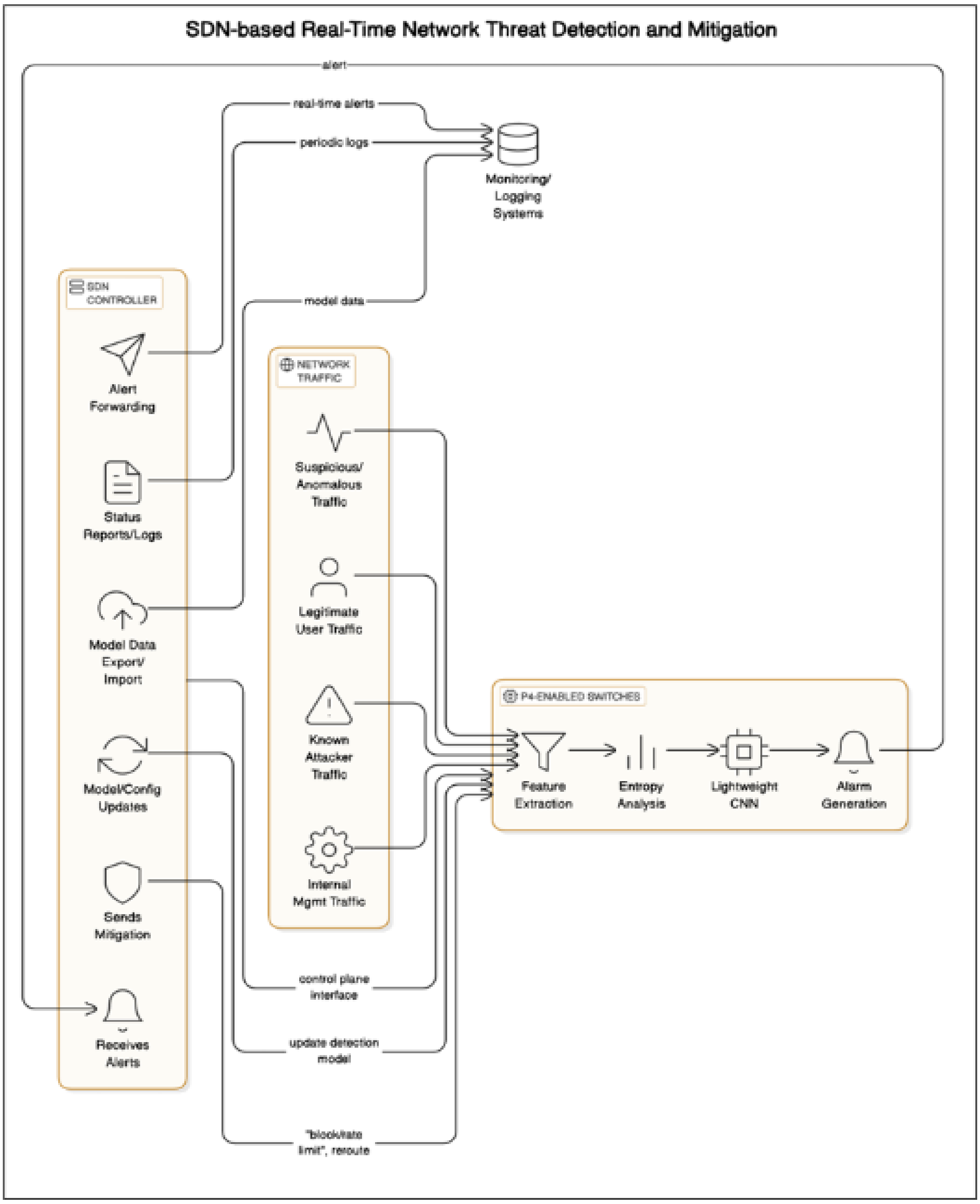

Figure 1 System Architecture Diagram

The SDN-based real-time network-threat detection and mitigation framework proposed in this article in system architecture. It shows an interaction among various elements, including SDN controllers, programmable data plane P4-enabled switches, different traffic flows that executive different types of network traffic, and those monitoring/logging systems that define control and data flows for detection, alerting, and mitigation.

4.2. The Feature Extraction and Preprocessing

- Packet Level Feature Extraction: The set of header features (source/destination IP, ports, protocol, TCP flags) is collected.
- Flow Statistics Collection: The number of packets, bytes, and arrival times are counted per flow.
- Entropy-Oriented Techniques: These include the calculation of the entropy of an IP distribution to uncover possible anomalies.
- Dimension Reduction: This allows free processing while maintaining all salient features.

4.3. Design of the Lightweight CNN Model

- Architecture: One convolutional layer; with 64 filters, max pooling and fully connected layer; with a total of 2,241 trainable parameters.
- Optimization: It is designed for minimal memory and processing overhead.
- Generalization: Preprocessing should not be dataset-dependent in order to increase model robustness.

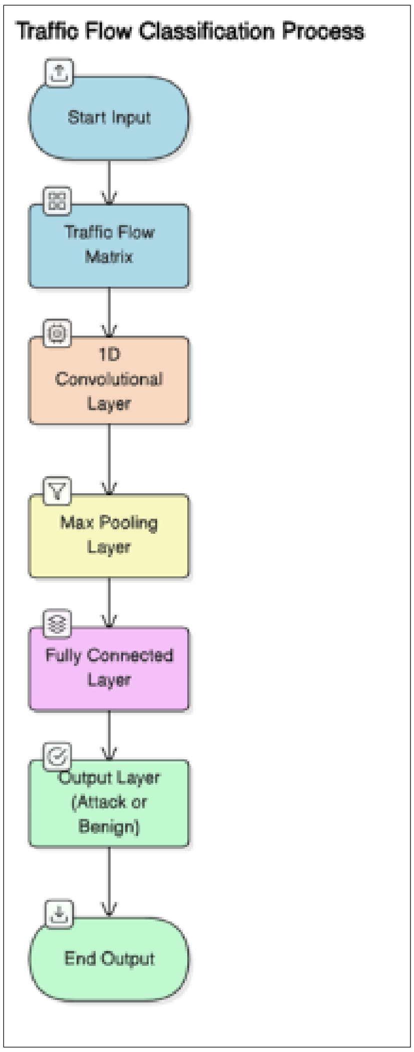

Figure 2 Model Architecture Diagram (CNN workflow)

Light-weight CNN architecture for traffic flow classification. The diagram represents the different layers of the model arranged in sequential order: input processing, traffic flow matrix construction, 1D convolution and max pooling layers, fully connected layer, and final output for attack or benign classification.

4.4. Detection Process

- Real-time Monitoring: The Programmable switch monitors network traffic on a continuous basis.
- Observation Windows: The traffic is segmented into fixed-size windows for analysis.
- Feature Computation: Statistical features are computed for every window.
- Anomaly Detection: The CNN model classifies traffic as benign and DDoS attack traffic.
- Alarm Generation: On detection, alerts and metadata are dispatched to the controller.

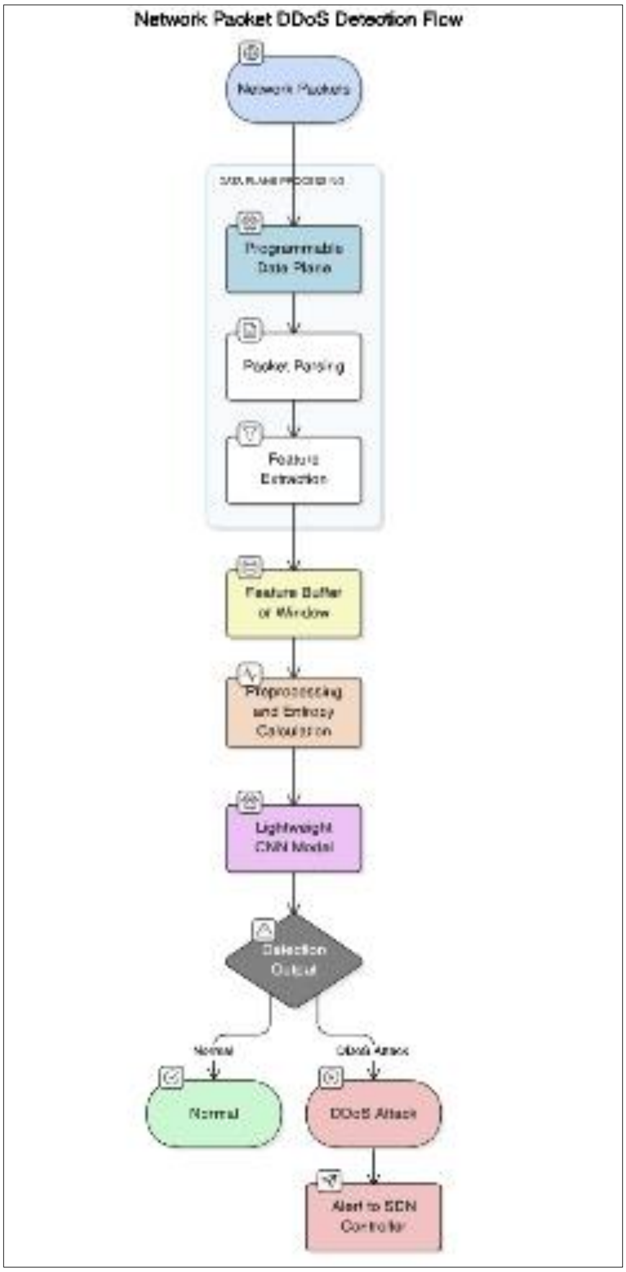

Figure 3 Network Packet DDoS Detection Flow Diagram

The workflow process sets forth in this figure describes each packet's journey from ingress, parsing, feature extraction, buffering, preprocessing and entropy calculation, lightweight CNN inference, and decision to output and alerting the SDN controller.

4.5. Experimental Setup

- **Datasets:** CICIDS2017, CICDDoS2019
- **Environment:** Mininet for SDN emulation, P4-enabled switches
- **Evaluation Metrics:** Accuracy, Precision, Recall, F1-score, Detection Latency, Resource Utilization

5. Results

5.1. Detection Performances

- The accuracy obtained through CIC-IDS2017 and CICIDS2019 datasets, that is, 99.2%.
- Precision-DDoS detection: 98.7%.
- Recall-DDoS Detection: 99.4%.
- F1 Score-DDoS Detection: 99.05%.

5.2. Processing Efficiency

- Processing Time- 35 times faster than controller-based approaches.
- Detection Latency-average 235 ms to support reactive measures.
- Throughput-11 GB without degradation.

5.3. Resource Utilization

- Model Size: 2,200 Parameters, 45 KB Memory.
- Peak Utilization: 12% on test platform, feasible for edge deployment.5.4 Comparison with Existing Approaches

Table 1 Comparison of DDoS Detection Models

Approach	Accuracy	Processing Time (ms)	Parameters	Memory Usage
Our Model	99.2%	235	2,200	45 KB
LUCID	98.9%	9,400	2,241	48 KB
Deep Defense	99.1%	12,500	>1,000,000	4.2 MB
Random Forest	99.97%	850	N/A	1.2 MB
CNN-RF	98.4%	780	8,500	320 KB

5.4. Parameter Impact

- **Time Window:** Shorter windows (1s) yield faster detection with slight accuracy loss; longer windows (5s) improve accuracy but increase latency.
- **Packet Count:** Increasing packet count beyond 100 per flow yields diminishing returns in accuracy.

6. Discussion

This proposed lightweight CNN model in programmed data planes provides high detection accuracy with reduced latency and little resource usage. It fits the needs of real-time DDoS detection in SDN because of the rapid response and its good scalability. With this offloading of detection to data planes, the solution improves resilience in SDN while boosting scalability, lowering risk for overload at controllers, and hence improving network availability. This compact model architecture is formed in such a way that the model is suitable for deployment in resource-constrained devices; at the same time, it has high accuracy and adaptability whereby it can be proved effective against emerging DDoS attack patterns.

The merit of this system lies in its condition of independence from the SDN controller, thus, avoiding the bottlenecks and vulnerabilities that arise due to centralized detection. The use of programmable data planes enables in-network processing, thus, reducing detection latency, but also allowing faster mitigation. Yet, challenges remain in ensuring that the model generalized well regarding newer types of attacks, as well as performance maintenance in very dynamic network environments. Future work will focus on model robustness improvement, hardware-specific optimizations, and enlarging the perspective of the approach to other threats.

7. Conclusion

It is shown in the research that scaled-down models like deep learning could be efficiently deployed with programmable data planes for on-time real-time detection of DDoS attacks at SDN environments. The suggested CNN-based approach is highly accurate but operates with minimal consumption of resources within low latency, thus making it comfortable for the practical implementation on edge devices. With this transfer, the solution brings resilience and scalability to SDN while furnishing a robust defense against DDoS attacks.

7.1. Future Work

7.1.1. Future research will focus on:

- Improving model generalization to new and evolving attack types
- Exploring hardware-specific optimizations for further resource reduction
- Extending the approach to detect other network threats (e.g., data exfiltration, insider attacks)
- Integrating the solution with broader SDN security frameworks and real-world deployments

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] S. Nandi, A. Kumar, and R. Verma, “A review on DDoS attacks classifying and detection by ML/DL methods,” *Int. J. Adv. Comput. Sci. Appl.*, vol. 15, no. 2, pp. 827–840, 2024.

[2] S. Bagyalakshmi, M. Sharma, and P. Nair, “Feature selection and classification methods for DDoS detection,” *Int. J. Innov. Res. Comput. Commun. Eng.*, vol. 10, no. 4, pp. 1234–1242, 2023.

[3] S. Sahoo, A. Singh, and D. Roy, “SVM with enhanced kernel and genetic algorithm for DDoS detection in SDN,” *Comput. Netw.*, vol. 212, pp. 109–121, 2022.

[4] I. Alguliyev, R. Aliguliyev, and L. Sukhostat, “DDoS attack prediction via social media sentiment analysis using deep learning,” *Future Gener. Comput. Syst.*, vol. 137, pp. 1–12, 2023.

[5] M. Shurman, K. Al-Tamimi, and L. Khan, “Hybrid IDS and LSTM-based DDoS detection in IoT networks,” *Sensors*, vol. 21, no. 9, pp. 3124–3137, 2022.

[6] S. Cil, E. Kaya, and M. Ozcan, “Deep neural networks for DDoS detection on CICDDoS2019 dataset,” *IEEE Access*, vol. 9, pp. 123456–123465, 2021.

[7] R. Ahuja, N. Soni, and D. Mehta, “Stacked auto-encoder MLP for SDN traffic classification,” *J. Netw. Comput. Appl.*, vol. 198, pp. 103–112, 2023.

[8] A. Agarwal, S. Tripathi, and P. Gupta, “Convolutional autoencoder for DDoS detection on CICDDoS2019 dataset,” *Comput. Secur.*, vol. 112, pp. 102–110, 2022.

[9] X. Guo, J. Liu, and Y. Zhang, “GLD-Net: Deep learning for DDoS detection using topological and traffic features,” *IEEE Trans. Netw. Serv. Manag.*, vol. 19, no. 2, pp. 876–889, 2022.

[10] R. Doriguzzi-Corin, S. Schiavone, F. Gringoli, and L. Vassio, “LUCID: A practical, lightweight deep learning solution for DDoS attack detection,” *IEEE Trans. Netw. Serv. Manag.*, vol. 17, no. 2, pp. 876–889, 2020.

[11] F. Lapolli, “Offloading real-time DDoS attack detection to programmable data planes,” UFRGS, Porto Alegre, Brazil, Tech. Rep., 2019.

[12] J. Ma, W. Su, and Y. Li, “Synchronizing DDoS detection and mitigation based graph learning with programmable data plane in SDN,” *Future Gener. Comput. Syst.*, vol. 154, pp. 1–15, 2024.

[13] N. Aslam, S. Srivastava, and M. M. Gore, “A comprehensive analysis of machine learning- and deep learning-based solutions for DDoS attack detection in SDN,” *Arab. J. Sci. Eng.*, vol. 48, no. 7, pp. 1–25, 2023.

[14] R. J. Gohari, L. Aliahmadipour, and M. K. Rafsanjani, “CTMBIDS: Convolutional Tsetlin Machine based intrusion detection system for DDoS attacks in an SDN environment,” *arXiv preprint arXiv:2409.03544*, 2024.

[15] M. N. Swileh and S. Zhang, “Unseen attack detection in software-defined networking using a BERT-based large language model,” *arXiv preprint arXiv:2412.06239*, 2024.

[16] J. Tamayo, L. I. Barona López, and Á. L. Valdivieso Caraguay, “Detection of distributed denial of service attacks carried out by botnets in software-defined networks,” *arXiv preprint arXiv:2401.09358*, 2024.