Journal of Computer Science

Original Research Paper

Deep Learning Approach to Mitigate DDoS Attacks in SDN

[1]Hema Surendrakumar Dhadhal, [2]Paresh Kotak, [3]Parvez Faruki and [4]Atul Gonsai

[1]Department of Information Technology, Lukhdhirji Engineering College, Morbi, India
[2]Dr S & S S Ghandhy College of Engineering and Technology, Surat, India
[3]A. V. Parekh Technical Institute, Rajkot, India
[4]Department of Computer Science, Saurashtra University, Rajkot, India

Article history
Received: 02-05-2024
Revised: 24-05-2024
Accepted: 27-05-2024

Corresponding Author:
Hema Surendrakumar Dhadhal
Department of Information Technology, Lukhdhirji Engineering College, Morbi, India
Email: hemadhadhal@gmail.com

Abstract: The rise of Distributed Denial of Service (DDoS) attacks remains a significant obstacle to network security and availability. This abstract presents a new hybrid model for DDoS mitigation in Software-Defined Networking (SDN) environments, combining a Semi-supervised Deep Extreme Learning Machine (Semi-Deep ELM) with a hybrid architecture. SDN's centralized control and programmability create an ideal platform for implementing advanced mitigation strategies. The hybrid model proposed integrates the semi-deep ELM approach, utilizing both labeled and unlabeled data to enhance DDoS detection accuracy, along with additional mechanisms for increased resilience and adaptability. By utilizing extreme learning machines and deep learning architectures within a hybrid framework, the model achieves improved robustness and scalability in combating various DDoS attacks as compared to existing models. It also discusses potential challenges and considerations, such as model complexity, resource allocation, and integration with existing network infrastructure. The proposed technique with DP-K-means clustering offers simplicity and efficiency in DDoS attack detection, especially in scenarios with limited labeled data and real-time detection requirements. The adoption of this hybrid model for DDoS mitigation in SDN uses the DP-KMC method for tighter clustering of benign traffic and hence detecting DDoS easily and faster. ERL-AlexNet mitigation provides faster mitigation using n! Wu-Manber algorithm thus presents a promising solution for strengthening network resilience and security, ensuring uninterrupted service delivery, and mitigating potential disruptions in today's dynamic cyber threat landscape. It enables the system to dynamically adapt its mitigation strategies based on evolving attack patterns and network conditions, thereby providing effective protection against a wide array of DDoS threats.

Keywords: Distributed Denial of Service Attacks, Douglas Pecker K-Means Clustering, ERL-AlexNet, Mitigation, n! Fox Wu-Manber Algorithm, Software Defined Networks

Introduction

In the realm of network security, Software-Defined Networking (SDN) has brought about new possibilities for dynamic and centralized network management. However, the advantages of SDN also bring forth challenges, particularly the heightened susceptibility to Distributed Denial of Service (DDoS) attacks. These attacks, characterized by flooding target networks with malicious traffic, pose significant risks to the availability and integrity of online services. Therefore, there is an urgent requirement for innovative and efficient DDoS mitigation techniques tailored specifically for SDN environments as stated by Dantas Silva *et al.* (2020). Our study introduces a fresh approach to mitigate DDoS attacks in SDN by utilizing a hybrid method that combines flow-based filtering and machine learning algorithms. Yuan *et al.* (2019) came up with DDoS mitigation strategies in SDNs that typically rely on flow-based filtering, which examines network traffic using predefined rules to detect and counteract malicious packets. While effective in certain scenarios, these methods may have to undergo difficulties as they deal with the rapidly changing nature of DDoS attacks and may result in high computational costs as stated by Ali *et al*. (2023). To overcome these challenges, our proposed method integrates machine learning algorithms into the flow-based filtering process, allowing the SDN controller to dynamically learn and adjust to emerging DDoS attack patterns in real time. Wang *et al*. (2018) have also mentioned this in their work. By utilizing historical traffic data and anomaly detection techniques, our method can accurately and efficiently identify and mitigate DDoS attacks, while reducing false positives and negatives. Furthermore, the hybrid approach we present offers numerous benefits over traditional methods. By merging flow-based filtering with machine learning, our method enhances the adaptability and responsiveness of DDoS mitigation in SDN, enabling proactive detection (as described in Singh and Behal, 2020) and mitigation of both known and emerging DDoS attack vectors. Additionally, the inclusion of machine learning algorithms empowers the SDN controller to effectively combat DDoS attacks as described by Agrawal *et al*. (2022).

Through this comparative analysis and the proposed method, we seek to provide thorough knowledge about the effectiveness of different DDoS mitigation methods, enabling network administrators and security professionals to make informed decisions when selecting and deploying mitigation strategies (Luo *et al*., 2016).

The major outcomes of the proposed work are:

- The proposed technique combines flow-based filtering with machine learning algorithms to achieve proactive and adaptive DDoS mitigation in SDN. It leverages the K-Means Clustering (KMC) algorithm for classifying and filtering network traffic
- While semi-supervised deep machine learning approaches offer high accuracy and adaptability, they may require extensive computational resources and labeled data for training
- The proposed technique with Douglas Pecker KMC offers simplicity and efficiency in DDoS attack detection, especially in scenarios with limited labeled data and real-time detection requirements
- The Wu-Manber pattern matching approach provides a straightforward classification of network traffic based on similarity to labeled instances, making it suitable for dynamic SDN environments

Thus, a novelty in our method lies in:

- Enhanced detection accuracy: By fusing multiple detection mechanisms, our approach reduces false positives and improves the identification of legitimate traffic
- Adaptive learning: Our system continuously evolves by learning from new attack patterns, ensuring robust protection against emerging threats
- Resource efficiency: Through intelligent resource allocation and prioritization, our method minimizes the computational overhead typically associated with DDoS detection
- Scalability: Designed to handle large-scale SDN environments, our approach can efficiently manage high volumes of network traffic without compromising performance

In summary, while semi-supervised machine learning approaches offer advanced detection capabilities, the proposed technique provides a practical and effective solution for DDoS attack mitigation in SDN environments.

Related Works

1. Semi-Supervised Autoencoders (AE):

Bårli *et al*. (2021) suggested an approach where semi-supervised autoencoders employ unsupervised learning to reconstruct regular network traffic and identify anomalies that could indicate potential DDoS attacks.

Result: Achieves a high level of accuracy in detection while minimizing false positives through the utilization of both labeled and unlabeled data during training. It uses reconstruction loss to detect malicious traffic as an anomaly.

Mittal *et al*. (2023); Ahmad *et al*. (2021) came up with a deep neural network that led to dimensionality reduction and feature extraction. The Autoencoders AE has layers as well as input (for encoding) and output (for decoding) layers. AE uses backpropagation to jointly train the encoder and the decoder. The encoder extracts the raw features and transforms the input into a low-dimensional abstraction. The decoder then reconstructs the original features into low-dimensional elements.

Result: It achieves high accuracy and precision:

2. Semi-Supervised Generative Adversarial Networks (GANs):

Shieh *et al*. (2022) proposed a method where semi-supervised GANs train a generator to produce normal network traffic and a discriminator to differentiate between real and generated traffic, thus, enabling the identification of anomalies.

Result: Enhances the detection of DDoS attacks by learning intricate data distributions and adapting to evolving attack strategies. More focus was on misclassification to generate accurate results.

Aldhaheri and Alhuzali (2023) proposed an IDS as a countermeasure in SDN. In this research, unlike other research, GAN design is used in the SDN environment by increasing the effect of the attack on the system. The model developed by them mitigates the effects of counterattacks and allows the model to accurately detect DDoS attacks.

Result: It enhances the accuracy of detection as compared to other similar schemes of using the CICDDoS 2019 public dataset:

3. Semi-Supervised Support Vector Machines (SVM):

Khuphiran *et al.* (2018) use a Semi-supervised SVM approach to utilize both labeled and unlabeled data to construct a decision boundary that separates normal from malicious network traffic. Fardusy *et al.* (2023) claimed the highest accuracy recall rate and f-score to detect DDoS attacks using both labeled and unlabeled data.

Result: Delivers effective detection of DDoS attacks, capable of handling imbalanced datasets and adjusting to varying levels of attack intensity.

Revathi *et al.* (2022) introduced a Discrete-Scalable Memory Support Vector Machine (DSM-SVM) and mitigation framework for SDN. Input is pre-processed using the spark standardization method to remove the unwanted missing values. Feature extraction is performed using a semantic multi-linear component analysis algorithm The DSM-SVM algorithm is employed to predict attacks with higher accuracy. Thus, the proposed model is trained and utilized for SDN detection and mitigation.

Result: It indicates that the presented model outperforms another algorithm, achieving improved accuracy:

4. Semi-supervised deep learning models:

Chen *et al*. (2023) utilized the DBN-LSTM attack method to detect and prevent DDoS attacks in SDN, incorporating Generative Adversarial Networks (GAN), Deep Belief Networks (DBN) and Long Short-Term Memory (LSTM). This approach aims to make the system less susceptible to adversarial attacks. Additionally feature extraction techniques, including semi-supervised deep learning models like DBN and CNN, leverage unlabeled data for pretraining deep architectures and to enhance classification performance.

Result: Provides high accuracy in detection and resilience to noisy data by utilizing unlabeled samples for feature learning and model initialization also results in fast feature selections.

Wei *et al*. (2021) successfully implemented DDoS attacks by developing a hybrid AR-MLP method the component AE in the proposed model provides the best results by identifying the most important factors with the human aid. The multilayer sensor network component of the proposed model addresses the speed and bias issues encountered during large-scale operations with noisy data.

Result: The expected outcomes of the model have outperformed in accuracy than other existing methods

By considering the pros and cons of the above methods we have come up with a novel solution to defend against DDoS attacks in SDN. The novelty of the solution is that the proposed method not only takes into consideration stationary devices but also mobile devices that are generating DDoS attacks. Again, it is mitigating attacks in less time and with greater efficiency. Also, the false alarm rates are decreased and the method is more accurate and better than the other existing methods.

Materials and Methods

Proposed Method

Step 1 Collection and preprocessing of data:

- Gather network traffic data from both mobile and stationary devices connected to the SDN infrastructure
- Include attributes such as packet size, protocol type, source and destination IP addresses and traffic volume
- Preprocess the data to standardize, scale and encode categorical attributes as needed

Step 2 Unsupervised feature learning using DELM:

- Employ a Deep Extreme Learning Machine (DELM) architecture for unsupervised feature learning
- Train the DELM model on the unlabeled network traffic data to extract high-level representations of the data without explicit labels

Step 3 Integration of semi-supervised learning:

- Integrate labeled data into the DELM model, which includes instances labeled as normal or DDoS Attacks
- Fine-tune the DELM model using semi-supervised learning techniques, such as self-training or co-training to adapt its representation to the labeled instances while leveraging the learned features from unlabeled data

Step 4 Dynamic adaptation of features:

- Incorporate dynamic attributes related to mobile devices, such as mobility patterns, signal strength, and connection stability, into the model
- Continuously update the model's representation based on the evolving characteristics of mobile devices and their interactions with the SDN infrastructure

Step 5 Intrusion detection and classification:

- Utilize the trained SDELM model to classify incoming network traffic from both mobile and stationary devices as either normal or malicious
- Apply threshold-based techniques or anomaly detection algorithms to identify DDoS attacks based on deviations from normal behavior

Step 6 Adaptive mitigation:

- Implement adaptive mitigation strategies within the SDN architecture to respond to detected DDoS attacks
- Dynamically adjust flow rules in SDN switches to redirect or drop suspicious traffic flows, mitigating the impact of DDoS attacks on network performance for both mobile and stationary devices

Step 7 Evaluation and validation:

- The proposed SDELM method is then evaluated for its performance using real-world DDoS attack scenarios involving both mobile and stationary devices
- Benchmark against existing techniques and validate the effectiveness of the approach considering detection accuracy, false positive rate, response time, and resource utilization

Step 8 Deployment and integration:

- Deploy the SDELM model within SDN infrastructures, integrating it with existing network management and security frameworks
- Ensure seamless integration with SDN controllers and switches to enable real-time monitoring and mitigation of DDoS attacks targeting both mobile and stationary devices

The proposed work comprises three phases: Data capturing, DDoS attack detection, and DDoS mitigation as shown in Fig. 2. Here, a decentralized software defined network framework is taken into consideration using local and universal controllers for a central point of connection. Initially, the users submit the packets to be transmitted in the network (Aldweesh *et al.*, 2020). At first, the data capturing module is executed by setting the access point with OpenFlow-enabled switches as their gateways The configuration enables all traffic generated by the connected devices to pass through the OpenFlow switch. The significance of this arrangement lies in the fact that it grants the local controller the authority to decide whether the traffic should be forwarded or dropped (Huang *et al.*, 2023). This decision is made with the help of the central limit theorem-based type 2 interval fuzzy techniques. Here, conventional type 2 interval fuzzy is selected for its membership functions. Still, the upper and lower bounds are selected randomly; hence, it was modified to follow the central limit theorem. It is termed the central limit theorem based on type 2 interval fuzzy. It is evaluated for decision-making time and then compared with conventional methods. Further, to ensure the effective management of this traffic, an out-of-band connection is utilized to direct the traffic, which passes through the switch to its corresponding local controller. Following this, the local controller collects and processes the traffic, extracting the essential features from the packets. For processing the traffic effectively, the K-means clustering algorithm is selected for its advantage of producing tighter clusters than hierarchical clustering. Still, the distance used was Euclidean distance as it produces losses when the dimensionality of data is very high. This is related to a phenomenon known as the curse of dimensionality. Hence, it is modified to the Douglas-Peucker algorithm for collecting optimal tolerance segmentation lines based on which clustering takes place. It is termed as Douglas-Peucker-K-Means Clustering (DP-KMC). Once this process is finished, the packets are discarded to release the memory resources and make it free.

The data from the extracted features is inputted to the detection module for DDoS detection, which operates on all local controllers. To execute DDoS attack detection, ELM_ERL-AlexNet is trained by utilizing the DDoS attack detection dataset. The model is trained by preprocessing the dataset, followed by feature extraction and classification. For classification, conventional Alex net was selected for its decreased error performance in previous classifications; still, its learning rate was low for high dimensional data. Hence, it is modified to an extreme learning machine-based Evolutionary Reinforcement Learning (ERL) algorithm. It is termed as ELM_ERL-ALexNet. ELM offers notable advantages primarily owing to its swift training process. ELM employs random initialization of parameters and reliance on straightforward matrix operations, resulting in a considerable reduction in training time. This approach differentiates it from other training methodologies that depend on slower gradient-based learning techniques. Upon detecting a DDoS attack by the ELM_ERL-ALexNet system, the attack mitigation module is activated, which is integrated into the local controllers. This module is designed to receive a roster of devices that have been identified as malicious. To address these attacks, distinct strategies are formulated that hinge on the nature of the devices involved distinguishing between Stationary Devices (SD) and Mobile Devices (MD). Stationary Devices, such as fixed smoke alarms within a building maintain a fixed position and are tied to specific access points. Once these devices are configured, they do not necessitate further Authentication and Authorization (AA) processes. In contrast, mobile devices, typified by smartphones carried by individuals, are not fixed in any location; they move about. Consequently, MDs need to undergo the AA process each time they enter the coverage area of an access point. For AA, the Wu-Manber (WM) algorithm is selected for its multi-pattern matching and fast-matching properties. Still, the shift value is always selected based on the LSB strings and its subtraction unit. This might mislead to unwanted decisions; hence, it is modified to use an optimization algorithm, taking the size of strings as input, and finding the minimum shift for matching. For this purpose, the Fox optimization algorithm is selected and it has the advantage of high exploration capability. But, still, the best position from prey is calculated randomly that was calculated using n! of the population. It is termed as n!-Fox optimized Wu-Manber (n!-Fox-WM). To efficiently manage these different device categories, the controller draws upon its comprehensive overview and categorizes malicious devices into SDs and MDs. The flowchart of the proposed model is depicted in Fig. 1. By considering both mobile and stationary devices in the DDoS attack mitigation strategy, this proposed method aims to provide comprehensive protection for the entire SDN infrastructure. Leveraging the capabilities of Semi-supervised Deep Extreme Learning Machines (SDELM), enhanced accuracy is achieved and improves the adaptability of DDoS attack detection (Haider *et al*., 2020; Gebremeskel *et al*., 2023), while effectively mitigating the impact of attacks on network performance for all connected devices.

Experimental Setup

This study took the widely accepted NSL-KDD and CIC-IDS 2019 and Mendeley 2020 datasets. These are data identified by the Canadian cyber security institute for investigations into intrusion.

The CIC-IDS2019 dataset contains both qualitative and quantitative data on traditional attacks. CICFlowMeter is used for network traffic analysis, including labeled flows, protocols and attacks over time, targets and the target IPs, and location port (CSV file). We have focused on DDoS traffic and use it to train ML-based DDoS attack detection. Table 1 shows the system specifications and the materials used for training and testing.

A total of 90,000 samples were uploaded for distribution, with a 60:40 split between malicious traffic and DDoS.

When the traffic is normal it is marked as 0 and DDoS attack traffic is marked as 1.

The data is split for training purposes (80%) and testing purposes (20%) using train test classification methods using the library scikit, with the test size = 0.02. Once separated, the data sample of 71000 were set for training and 19000 samples were set for testing. As given in the dataset, it is difficult to compare the features themselves to the learning network as their sizes are different and have continuous or discrete values.

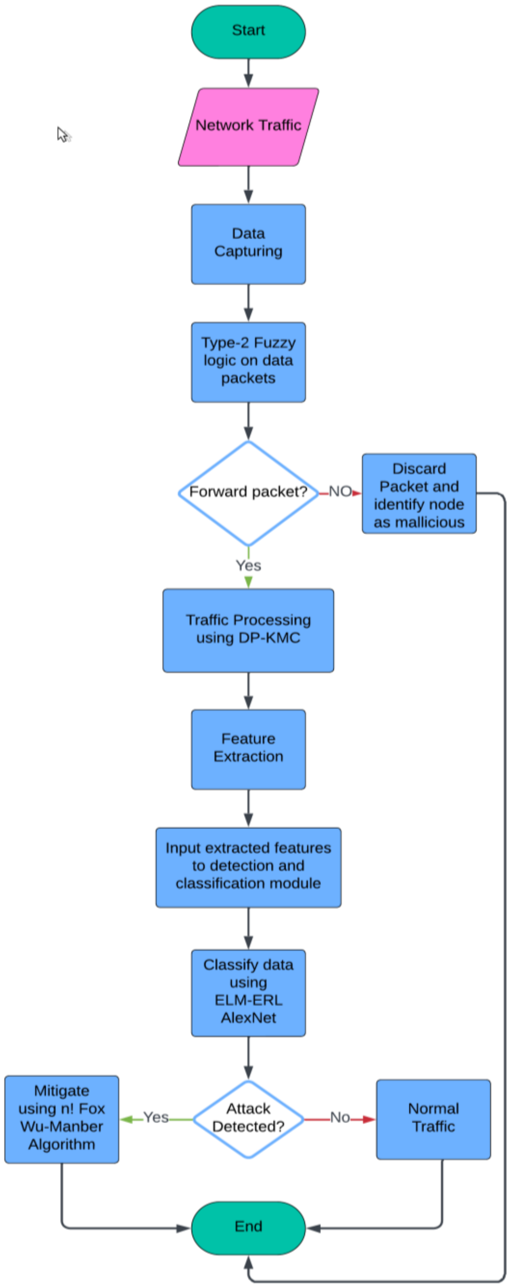

Start
Network Traffic
Data Capturing
Type-2 Fuzzy logic on data packets
Forward packet?
NO
Discard Packet and identify node as mallicious
Yes
Traffic Processing using DP-KMC
Feature Extraction
Input extracted features to detection and classification module
Classify data using ELM-ERL AlexNet
Attack Detected?
Yes
Mitigate using n! Fox Wu-Manber Algorithm
No
Normal Traffic
End

Fig. 1: Flowchart of the proposed system

Table 1: Material and system specifications

System manufacturer	Lenovo
Processor	Intel core i7 6700 CPU with 3.4 GHz
Memory	8GB
Operating system	Ubuntu 16.04
Emulator	Mininet 2.2.1
Controller	ODL and Ryu
Dataset	CICDDoS-2019, Mendely-2020
Switches	OpenFlow enabled switches
Libraries	Tensorflow 2.x, Keras, Pytorch 1.x, Scikit-Learn, Skfuzzy

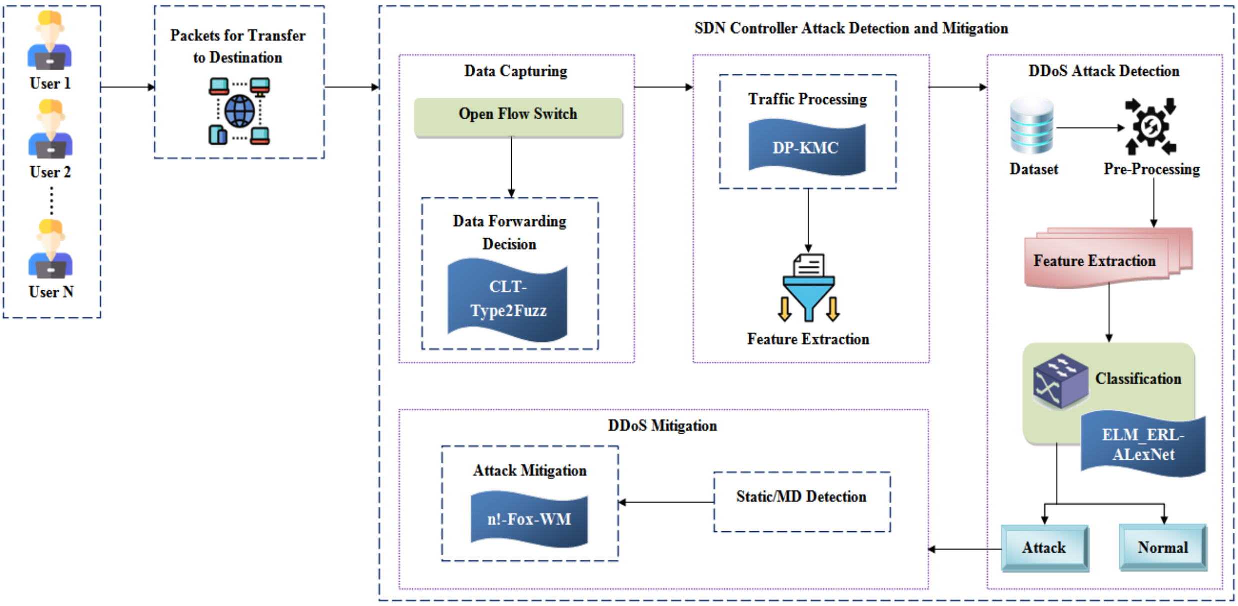


Fig. 2: Block diagram of proposed system

Results and Discussion

Evaluation Metrics

In this section, we have come up with the widely used evaluation metrics to measure the performance of ML and DL methods of intrusion detection. All the ranking metrics are derived from various attributes utilized in the confusion matrix (Fig. 3). The two-dimensional matrix provides the details about actual and predicted classes and includes the following:

i. True Positive (TP): Instances of data correctly classified by the classifier as an attack
ii. False Negative (FN): Data instances incorrectly
iii. predicted as normal instances
iv. False Positive (FP): Instances of data incorrectly
v. classified as an attack
vi. True Negative (TN): Instances correctly classified as normal instances

The diagonal confusion matrix indicates the correct predictions, while the off-diagonal elements are the wrong predictions of a particular classifier. Figure 3 shows these attributes of the confusion matrix. In an SDN environment, where real-time traffic analysis is crucial, the confusion matrix can help network administrators understand the reliability of the DDoS detection system. Helps in making informed decisions about adjusting thresholds or implementing additional security measures based on types of errors observed (Salem *et al*., 2022). The confusion matrix is used in attack prediction to identify the types of errors the model is making (false positive vs false negative). Also, it helps in understanding the trade-offs between different metrics. For e.g., increasing recall might reduce precision if more false positives are accepted to capture more true positives. Further, it provides insight into whether the model needs further tuning, additional data, or other features.

Precision: It is the ratio of correctly identified attacks to the total number of instances predicted as attacks:

$$Precision \ = \frac{TP}{TP+FP} \tag{1}$$

Recall: It is defined as the ratio of correctly classified attack instances to the total number of actual attack instances:

$$Recall \ = \frac{TP}{TP+FN} \tag{2}$$

False alarm rate: Also known as false positive rate, is defined as a ratio of incorrectly predicted attack samples to the total number of normal samples:

$$False\ Alarm\ Rate \ = \frac{FP}{FP+TN} \tag{3}$$

True negative rate: It is defined as the proportion of normal samples that are accurately identified out of a total number of normal samples:

$$True\ Negative\ Rate \ = \frac{TP}{TN+FP} \tag{4}$$

		Predicted class	
		Attack	Normal
Actual Class	Attack	True positive	False-negative
	Normal	False positive	True negative

Fig. 3: Confusion matrix for attack classification

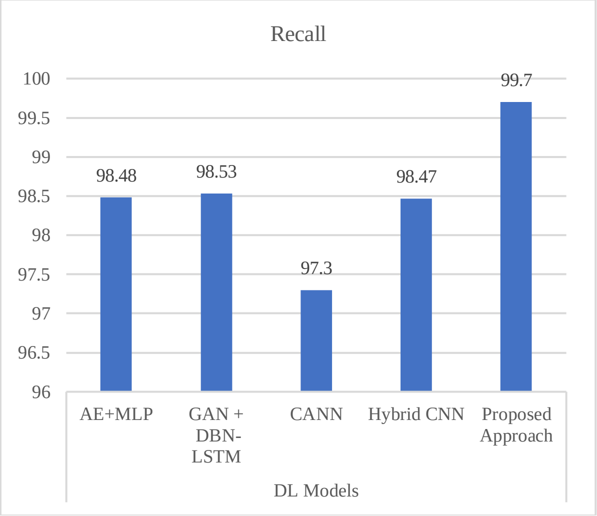


Fig. 4: Recall rate comparison

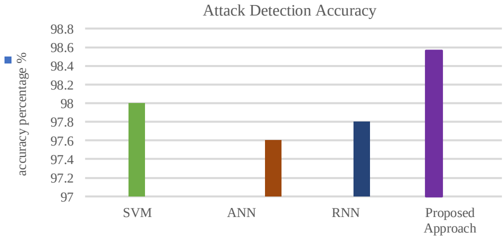


Fig. 5: Accuracy comparison

Accuracy: Also known as detection accuracy, is defined as the ratio of correctly classified samples to the total number of samples. It is widely used as a performance measure for a balanced dataset:

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad (5)$$

F1-Measure: It is a measure of the model's accuracy over the data set. It is defined as the harmonic mean of the model's precision and recall:

$$F1 - Measure = 2 \times \left(\frac{Precision \times Recall}{Precision + Recall}\right) \quad (6)$$

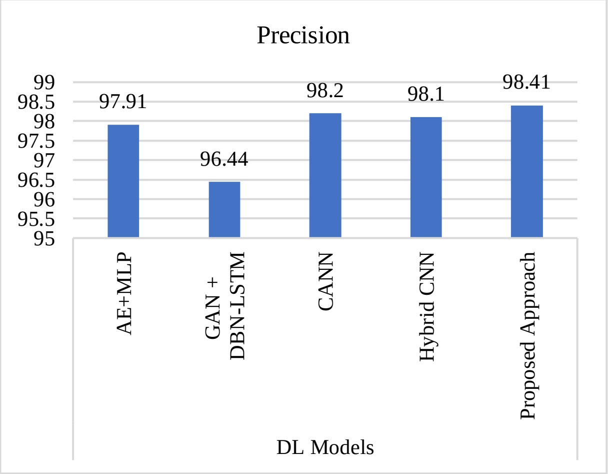
Table 2 gives a thorough comparison of different recent approaches to mitigate DDoS attacks in SDN. It is clearly visible that our approach is giving outstanding performance in classifying the packets as attack or benign ones, precision, and recall rates. The time required for attack detection is minimal as compared to other existing approaches and CPU utilization is minimal hence leading to saving of resources and generating better results. Trailing figures show the comparison of our proposed work with the existing approaches with respect to Recall Rate (Fig. 4) Accuracy (Fig. 5), precision, and f-measure (Figs. 6a-b).

Semi-supervised learning offers several advantages as compared to the other existing methods in terms of DDoS attack mitigation in SDN and therefore we have chosen semi-supervised learning due to its following advantages:

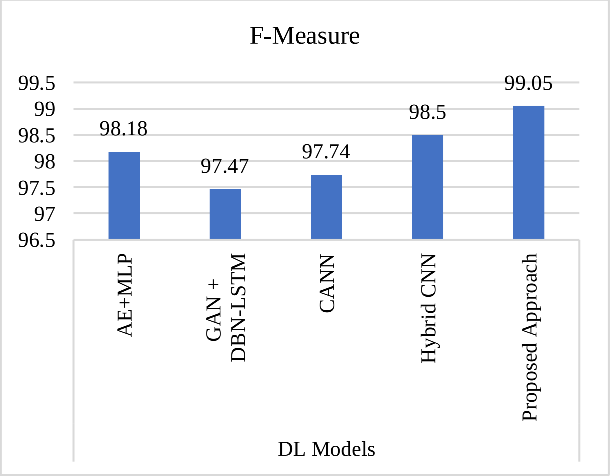
1. Leveraging unlabeled data: Semi-supervised techniques have the capability to utilize a significant amount of unlabeled data, which is often easily accessible in network settings, which enhances the generalization of the models. This in turn leads to the effective capture of data patterns, thus improving the performance ratio in terms of classifying normal and attack traffic
2. Cost efficiency: Acquiring labeled data for training machine learning models, particularly in security fields such as DDoS attack detection, can be both scarce and costly (Joëlle and Park, 2018). Semi-supervised learning diminishes the dependency on labeled data, making it a more cost-efficient approach by utilizing both labeled and unlabeled data for training purposes
3. Flexibility in dynamic environments: SDN environments are characterized by their dynamic nature, with network traffic patterns evolving continuously (Jiang *et al*., 2022). Semi-supervised learning techniques can easily adapt to changes in data distribution compared to supervised methods. This adaptability is crucial for effectively countering DDoS attacks in SDN, where attack patterns can change rapidly
4. Resilience to noise and outliers: Real-world network traffic data often contains noise and outliers (Tuan *et al*., 2020), which can negatively impact the performance of supervised learning models. Semi-supervised methods exhibit greater resilience to noise and outliers as they can learn from both labeled and unlabeled data, resulting in more accurate and robust models
5. Scalability: Semi-supervised learning approaches are well-suited for analyzing extensive datasets, making them ideal for processing large volumes of network traffic data in SDN environments. Thus, enables more comprehensive analysis and easier detection

Table 2: Comparison of Proposed system with current state-of-art

Author	Classification accuracy	Precision	Recall	F-measure	Detection time (min)	Train time (min)	CPU usage	Algorithm used
Our contribution	98.91	98.41	99.70	99.05	0.029	23.00	4.95%	Proposed
Tan *et al.* (2020)	98.85	98.10	98.47	98.50	0.061	39.52	6.02%	Hybrid KNN
Lin *et al.* (2015)	97.40	98.20	97.30	97.74	---	40.00	---	CANN
Chen *et al.* (2023)	91.23	96.44	98.53	97.47	---	---	---	GAN+DBN-LSTM
Wei *et al.* (2021)	98.34	97.91	98.48	98.18	---	---	---	AE+MLP



(a)



(b)

Fig. 6: (a) Precision comparison; (b) F-Measure comparison

Therefore, the integration of semi-supervised learning methods in DDoS attack mitigation for SDN can lead to more resilient, flexible, and cost-effective solutions that are better suited to the dynamic and complex nature of modern network environments (Rahman *et al*., 2019).

Thus, why the above-proposed model outperforms the other methods due to its simple structure, using semi-supervised learning can handle labeled and unlabeled data hence it produces faster results. The proposed technique combines flow-based filtering with machine learning algorithms to achieve proactive and adaptive DDoS mitigation in SDN. It leverages the DP K-Means Clustering (KMC) algorithm for the classification of network traffic. The Wu-Manber (WM) algorithm is selected for its multi-pattern matching and fast-matching properties, thus leading to faster attack detection. ELM_ERL-ALexNet offers notable advantages primarily owing to its swift training process. Mitigation leads to less false alarm rate and high precision.

Conclusion

In conclusion, the proposed approach for mitigating DDoS attacks in SDN using the Semi-supervised Deep Extreme Learning Machine (SDELM) model, which considers both mobile and stationary devices, offers a promising strategy for enhancing network security in dynamic settings. By leveraging the semi-supervised learning techniques, the model can effectively utilize both the labeled and unlabeled data to improve the accuracy and adaptability of DDoS attack detection and mitigation. The SDELM model provides numerous benefits compared to traditional methods, including improved utilization of unlabeled data, cost-effectiveness, adaptability to dynamic environments, resilience to noise and outliers, and scalability. These advantages position it as a suitable option for mitigating DDoS attacks in SDN environments where network traffic patterns may change rapidly and annotated data may be scarce.

Future Scope

While the proposed approach shows potential, there are various avenues for future research and development:

1. Enhanced model architecture: Explore the application of more deep learning architectures, such as Recurrent Neural Networks (RNNs) or transformers, to further improve the SDELM model's ability to capture temporal dependencies and complex patterns in network traffic
2. Dynamic adaptation: Develop mechanisms for the SDELM model to dynamically adjust to evolving network conditions and attack patterns in real-time, ensuring continuous and efficient mitigation of DDoS attacks
3. Integration with SDN controllers: Directly integrate the SDELM model with SDN controllers to facilitate seamless deployment and real-time decision-making, enabling automated mitigation of identified DDoS attacks
4. Evaluation in real-world environments: Perform comprehensive evaluation and validation of the

proposed approach in real-world SDN environments, considering diverse network topologies, traffic loads, and attack scenarios to evaluate its effectiveness and scalability.

Acknowledgment

There is no conflict of interest and no financial support from any other party.

Funding Information

The authors themselves have funded this manuscript.

Author's Contributions

Hema Surendrakumar Dhadhal: Participated in all the experiments, coordinated the data analysis generated the results, and contributed to the writing of the manuscript.

Paresh Kotak: Designed the research plan and helped to get the results.

Parvez Faruki: Helped in the modification of the manuscript and helped to get the workflow.

Atul Gonsai: Helped in result analysis.

Dataset Used

The datasets used are:

- https://www.unb.ca/cic/datasets/ddos-2019.html Sharafaldin *et al*. (2019)
- https://data.mendeley.com/datasets/yxzh9fbvbj/2 Ahuja *et al*. (2022)
- https://data.mendeley.com/datasets/hkjbp67rsc/1 Housman *et al*. (2020)
- https://data.mendeley.com/datasets/jxpfjc64kr/1 Ahuja *et al*. (2020)

Ethics

This article contains original and unpublished material. The authors confirm that no ethical issues are involved.

References

Agrawal, A., Singh, R., Khari, M., Vimal, S., & Lim, S. (2022). Autoencoder for Design of Mitigation Model for DDOS Attacks via M-DBNN. *Wireless Communications and Mobile Computing*, *2022*, 1–14. https://doi.org/10.1155/2022/9855022

Ahmad, Z., Shahid Khan, A., Wai Shiang, C., Abdullah, J., & Ahmad, F. (2021). Network intrusion detection system: A systematic study of machine learning and deep learning approaches. *Transactions on Emerging Telecommunications Technologies*, *32*(1), 1–29. https://doi.org/10.1002/ett.4150

Ahuja, N., Singal, G., & Mukhopadhyay, D. (2020). DDOS attack SDN Dataset [dataset]. In *Mendeley Data*. https://doi.org/10.17632/jxpfjc64kr.1

Ahuja, N., Singal, G., & Mukhopadhyay, D. (2022). ARP Poisoning and Flood attack in SDN [dataset]. In *Mendeley Data*. https://doi.org/10.17632/yxzh9fbvbj.2

Aldhaheri, S., & Alhuzali, A. (2023). SGAN-IDS: Self-Attention-Based Generative Adversarial Network against Intrusion Detection Systems. *Sensors*, *23*(18), 7796. https://doi.org/10.3390/s23187796

Aldweesh, A., Derhab, A., & Emam, A. Z. (2020). Deep learning approaches for anomaly-based intrusion detection systems: A survey, taxonomy, and open issues. *Knowledge-Based Systems*, *189*, 105124. https://doi.org/10.1016/j.knosys.2019.105124

Ali, T. E., Chong, Y.-W., & Manickam, S. (2023). Machine Learning Techniques to Detect a DDoS Attack in SDN: A Systematic Review. *Applied Sciences*, *13*(5), 3183. https://doi.org/10.3390/app13053183

Bårli, E. M., Yazidi, A., Viedma, E. H., & Haugerud, H. (2021). DoS and DDoS mitigation using Variational Autoencoders. *Computer Networks*, *199*, 108399. https://doi.org/10.1016/j.comnet.2021.108399

Chen, L., Wang, Z., Huo, R., & Huang, T. (2023). An Adversarial DBN-LSTM Method for Detecting and Defending against DDoS Attacks in SDN Environments. *Algorithms*, *16*(4), 197. https://doi.org/10.3390/a16040197

Dantas Silva, F. S., Silva, E., Neto, E. P., Lemos, M., Venancio Neto, A. J., & Esposito, F. (2020). A Taxonomy of DDoS Attack Mitigation Approaches Featured by SDN Technologies in IoT Scenarios. *Sensors*, *20*(11), 3078. https://doi.org/10.3390/s20113078

Fardusy, T., Afrin, S., Sraboni, I. J., & Dey, U. K. (2023). An Autoencoder-Based Approach for DDoS Attack Detection Using Semi-Supervised Learning. *2023 International Conference on Next-Generation Computing, IoT and Machine Learning (NCIM)*, 1–7. https://doi.org/10.1109/ncim59001.2023.10212626

Gebremeskel, T. G., Gemeda, K. A., Krishna, T. G., & Ramulu, P. J. (2023). DDoS Attack Detection and Classification Using Hybrid Model for Multicontroller SDN. *Wireless Communications and Mobile Computing*, *2023*, 1–18. https://doi.org/10.1155/2023/9965945

Haider, S., Akhunzada, A., Mustafa, I., Patel, T. B., Fernandez, A., Choo, K.-K. R., & Iqbal, J. (2020). A Deep CNN Ensemble Framework for Efficient DDoS Attack Detection in Software Defined Networks. *IEEE Access*, *8*, 53972–53983. https://doi.org/10.1109/access.2020.2976908

Housman, O. G., Isnaini, H., & Sumadi, F. D. S. (2020). SDN-DDOS (ICMP,TCP,UDP) [dataset]. In *Mendeley Data*. https://doi.org/10.17632/hkjbp67rsc.1

Huang, H., Ye, P., Hu, M., & Wu, J. (2023). A multi-point collaborative DDoS defense mechanism for IIoT environment. *Digital Communications and Networks*, *9*(2), 590–601. https://doi.org/10.1016/j.dcan.2022.04.008

Jiang, S., Yang, L., Gao, X., Zhou, Y., Feng, T., Song, Y., Liu, K., & Cheng, G. (2022). BSD-Guard: A Collaborative Blockchain-Based Approach for Detection and Mitigation of SDN-Targeted DDoS Attacks. *Security and Communication Networks*, *2022*(1), 1–16. https://doi.org/10.1155/2022/1608689

Joëlle, M. M., & Park, Y.-H. (2018). Strategies for detecting and mitigating DDoS attacks in SDN: A survey. *Journal of Intelligent & Fuzzy Systems*, *35*(6), 5913–5925. https://doi.org/10.3233/jifs-169833

Khuphiran, P., Leelaprute, P., Uthayopas, P., Ichikawa, K., & Watanakeesuntorn, W. (2018). Performance Comparison of Machine Learning Models for DDoS Attacks Detection. *2018 22nd International Computer Science and Engineering Conference (ICSEC)*, 1–4. https://doi.org/10.1109/icsec.2018.8712757

Lin, W.-C., Ke, S.-W., & Tsai, C.-F. (2015). CANN: An intrusion detection system based on combining cluster centers and nearest neighbors. *Knowledge-Based Systems*, *78*, 13–21. https://doi.org/10.1016/j.knosys.2015.01.009

Luo, S., Wu, J., Li, J., & Guo, L. (2016). A multi-stage attack mitigation mechanism for software-defined home networks. *IEEE Transactions on Consumer Electronics*, *62*(2), 200–207. https://doi.org/10.1109/tce.2016.7514720

Mittal, M., Kumar, K., & Behal, S. (2023). DL-2P-DDoSADF: Deep learning-based two-phase DDoS attack detection framework. *Journal of Information Security and Applications*, *78*, 103609. https://doi.org/10.1016/j.jisa.2023.103609

Rahman, O., Quraishi, M. A. G., & Lung, C.-H. (2019). DDoS Attacks Detection and Mitigation in SDN Using Machine Learning. *2019 IEEE World Congress on Services (SERVICES)*, 184–189. https://doi.org/10.1109/services.2019.00051

Revathi, M., Ramalingam, V. V., & Amutha, B. (2022). A Machine Learning Based Detection and Mitigation of the DDOS Attack by Using SDN Controller Framework. *Wireless Personal Communications*, *127*(3), 2417–2441. https://doi.org/10.1007/s11277-021-09071-1

Salem, F. M., Youssef, H., Ali, I., & Haggag, A. (2022). A variable-trust threshold-based approach for DDOS attack mitigation in software defined networks. *PLOS ONE*, *17*(8), e0273681. https://doi.org/10.1371/journal.pone.0273681

Sharafaldin, I., Lashkari, A. H., Hakak, S., & Ghorbani, A. A. (2019). Developing Realistic Distributed Denial of Service (DDoS) Attack Dataset and Taxonomy. *2019 International Carnahan Conference on Security Technology (ICCST)*, 1–8. https://doi.org/10.1109/ccst.2019.8888419

Shieh, C.-S., Nguyen, T.-T., Lin, W.-W., Huang, Y.-L., Horng, M.-F., Lee, T.-F., & Miu, D. (2022). Detection of Adversarial DDoS Attacks Using Generative Adversarial Networks with Dual Discriminators. *Symmetry*, *14*(1), 66. https://doi.org/10.3390/sym14010066

Singh, J., & Behal, S. (2020). Detection and mitigation of DDoS attacks in SDN: A comprehensive review, research challenges and future directions. *Computer Science Review*, *37*, 100279. https://doi.org/10.1016/j.cosrev.2020.100279

Tan, L., Pan, Y., Wu, J., Zhou, J., Jiang, H., & Deng, Y. (2020). A New Framework for DDoS Attack Detection and Defense in SDN Environment. *IEEE Access*, *8*, 161908–161919. https://doi.org/10.1109/access.2020.3021435

Tuan, N. N., Hung, P. H., Nghia, N. D., Tho, N. V., Phan, T. V., & Thanh, N. H. (2020). A DDoS Attack Mitigation Scheme in ISP Networks Using Machine Learning Based on SDN. *Electronics*, *9*(3), 413. https://doi.org/10.3390/electronics9030413

Wang, L., Li, Q., Jiang, Y., Jia, X., & Wu, J. (2018). Woodpecker: Detecting and mitigating link-flooding attacks via SDN. *Computer Networks*, *147*, 1–13. https://doi.org/10.1016/j.comnet.2018.09.021

Wei, Y., Jang-Jaccard, J., Sabrina, F., Singh, A., Xu, W., & Camtepe, S. (2021). AE-MLP: A Hybrid Deep Learning Approach for DDoS Detection and Classification. *IEEE Access*, *9*, 146810–146821. https://doi.org/10.1109/access.2021.3123791

Yuan, B., Zou, D., Yu, S., Jin, H., Qiang, W., & Shen, J. (2019). Defending Against Flow Table Overloading Attack in Software-Defined Networks. *IEEE Transactions on Services Computing*, *12*(2), 231–246. https://doi.org/10.1109/tsc.2016.2602861