Utilitas Mathematica

ISSN 0315-3681 Volume 122, 2025

BOTNET ATTACK DETECTION AND MITIGATION IN SDN USING DEEP LEARNING TECHNIQUE

SANKURI MANOHAR , Mtech Students, Department of CSE , Tirumala Engineering College , Narasaraopet, Email id : sankurimanu@gmail.com

KUPPANI SATHISH , Associate Professor, Department of CSE , Tirumala Engineering College, Narasaraopet. Email id : skuppani@gmail.com

ABSTRACT

Distributed denial of service (DDoS) attacks have been around for a while, and they're still a major problem for network security and availability. This abstract introduces a novel hybrid paradigm for Distributed Denial of Service (DDoS) mitigation in SDN settings. It incorporates a Semi-Deep Extreme Learning Machine (Semi-Deep ELM) with a hybrid architecture. Implementing advanced mitigation measures is made easier with SDN's programmability and centralised control. For better DDoS detection accuracy, the proposed hybrid model merges the semi-deep ELM method with additional mechanisms for increased robustness and adaptability, and with labelled and unlabelled data. The hybrid framework's utilisation of deep learning architectures and extreme learning machines increases the model's scalability and resilience in resisting various DDoS attacks, outperforming competing models. Model complexity, resource allocation, and interaction with the current network architecture are some of the potential issues and concerns that are covered. In cases when labelled data is few and real-time detection is essential, the proposed approach utilising DP-K-means clustering offers a straightforward and effective manner of detecting DDoS attacks. This hybrid design for DDoS mitigation in SDN makes DDoS detection easier and faster by employing the DP-KMC technique to cluster benign traffic more closely. Faster mitigation is possible with n, ERL-AlexNet! With the ever-evolving landscape of cyber threats, the Wu-Manber algorithm provides a practical solution to enhance network security and resilience, ensure uninterrupted service delivery, and minimise disruptions. It lets the system adapt its mitigation strategies to different attack patterns and network conditions, making it more resilient against DDoS attacks..

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

1. INTRODUCTION

New possibilities for centralised and dynamic network administration have emerged in the field of network security with the advent of software-defined networking (SDN). However, there are drawbacks to SDN as well, the most notable being the heightened susceptibility to Distributed Denial of Service (DDoS) attacks. These attacks pose serious risks to the availability and security of internet services because they flood targeted networks with malicious traffic. According to Dantas Silva et al. (2020), inventive and efficient DDoS mitigation techniques tailored to SDN systems are thus critically necessary.

By combining flow-based filtering with machine learning techniques, our research offers a new approach to reducing DDoS attacks in SDN. Software-Defined Networks (SDNs) can be used to mitigate distributed denial of service attacks (DDoS), according to Yuan et al. (2019). One method is flow-based filtering, which evaluates network traffic according to predefined criteria in order to detect and block harmful packets. Due to the ever-changing nature of DDoS attacks, these tactics may encounter obstacles, while they are beneficial in some cases.

will cause substantial computing costs, as shown by Ali et al. (2023)). In order to solve these issues, we provide a method that uses machine learning techniques in conjunction with flow-based filtering. This allows the SDN controller to constantly adapt to new patterns of DDoS attacks. The findings of Wang et al. (2018) are consistent with this observation. By combining anomaly detection methods with historical traffic data, our system can quickly and accurately identify DDoS attacks and neutralise them while reducing the number of false positives and negatives. In comparison to more traditional methods, the hybrid approach we suggest has a few benefits. In order to make DDoS mitigation in SDN more responsive and adaptable, our method combines flow-based filtering with machine learning. This allows us to proactively detect and mitigate both known and unknown DDoS attack paths, as described by Singh and Behal (2020). According to Agrawal et al. (2022), SDN controllers may effectively counter DDoS attacks by incorporating machine learning techniques. Network administrators and security experts can benefit from this comparative analysis and recommended strategy since it will help them make educated decisions when choosing and executing mitigation measures (Luo et al., 2016). Here are the main outcomes of the intended tasks:

Software-Defined Networking (SDN) proactive and adaptive DDoS mitigation is made possible with the proposed strategy, which combines flow-based filtering with machine learning approaches. It filters and categorises network traffic using the K-Means Clustering (KMC) algorithm. Although semi-supervised deep machine learning approaches are more flexible and accurate, they frequently require a lot of processing power and labelled data to train. In situations with limited labelled data and a need for real-time detection, the suggested method that makes use of Douglas Pecker KMC is both simple and efficient in detecting DDoS attacks. Suitable for dynamic SDN systems, the Wu-Manber pattern matching approach provides a transparent categorisation of network traffic through comparison to tagged instances. As a result, our approach is novel because of: Our approach reduces false positives and improves the identification of legitimate traffic by combining multiple detection methods, leading to improved detection accuracy. An ever-evolving resistance against new threats is ensured by our adaptive learning system, which constantly adapts by absorbing new assault patterns.

Efficient use of resources: By carefully allocating and prioritising resources, our method reduces the computational burden often associated with DDoS detection. Scalability: Our approach maintains performance integrity while expertly managing large volumes of network traffic; it was developed for vast SDN systems.

Finally, the proposed method provides a realistic and effective solution for DDoS attack mitigation in SDN environments, in contrast to the advanced detection capabilities offered by semi-supervised machine learning technologies..

2. Related Works

1. Semi-Supervised Autoencoders (AE): Bårli et al. (2021) developed a system that uses unsupervised learning to reconstruct regular network data and detect probable DDoS attacks. The results show that using both labelled and unlabelled data during training improves detection accuracy and reduces false positives. It uses reconstruction loss to identify malicious transmission as an abnormality. Mittal et al. (2023) and Ahmad et al. (2021) developed a deep neural network for dimensionality reduction and feature extraction. Autoencoders (AE) are made up of layers, which include encoding input layers and decoding output layers. AE trains the encoder and decoder simultaneously using backpropagation. The encoder extracts important information and converts the input into a low-dimensional representation. The decoder then reconstructs the original characteristics as low-dimensional components. As a result, it improves accuracy and precision.

2. Semi-Supervised Generative Adversarial Networks (GANs): Shieh et al. (2022) proposed an approach in which semi-supervised GANs train a generator to synthesise valid network traffic and a discriminator to distinguish between genuine and created traffic, allowing for anomaly detection. Result: Improves DDoS attack detection by understanding complex data distributions and adjusting to changing assault techniques. To achieve accurate results, a greater emphasis was made on misclassification. Aldhaheri and Alhuzali (2023) proposed an Intrusion Detection System as a mitigation approach for Software-Defined Networks. This study uses GAN design in the context of SDN, which distinguishes it from earlier studies.

by increasing the impact of the attack on the system. Their new methodology reduces the impact of counterattacks and allows for more precise identification of DDoS attacks. The results show improved detection accuracy when compared to other similar algorithms using the CICDDoS 2019 public dataset.

3. Semi-supervised Support Vector Machines (SVM): Khuphiran et al. (2018) use a semi-supervised SVM approach to develop a decision boundary that distinguishes between regular and malicious network traffic using both labelled and unlabelled data. Fardusy et al. (2023) demonstrated improved accuracy, recall rate, and F-score in detecting DDoS assaults with both labelled and unlabelled data. Result: Enables effective detection of DDoS attacks, is capable of handling imbalanced datasets, and can adjust to various degrees of attack intensity. Revathi et al. (2022) presented a Discrete-Scalable Memory Support Vector Machine (DSM-SVM) and a mitigation framework for Software-Defined Networking (SDN). To remove any unnecessary missing data, the input is pre-processed with the Spark standardisation approach. Semantic multi-linear component analysis is used to extract features. The DSM-SVM approach is used to forecast attacks with greater accuracy. Thus, the suggested model is trained and applied to the detection and mitigation of SDNs. The results show that the proposed model outperforms an alternative strategy, obtaining higher accuracy.

4. Semi-supervised deep learning models: Chen et al. (2023) used the DBN-LSTM attack methodology to detect and mitigate DDoS attacks in Software-Defined Networking (SDN), which included Generative Adversarial Networks (GAN), Deep Belief Networks (DBN), and Long Short-Term Memory (LSTM)

architectures. This strategy tries to improve the system's resilience against adversarial attacks. Furthermore, feature extraction approaches, including semi-supervised deep learning models like DBN and CNN, use unlabelled data to pretrain deep structures and improve classification accuracy. Result: Guarantees improved detection precision and robustness to noisy data by using unlabelled samples for feature learning and model initialisation, allowing for quick feature selection. Wei et al. (2021) effectively carried out DDoS attacks using a hybrid AR-MLP technique, with the AE component of the proposed model achieving optimal results by identifying the most crucial components with human interaction. The suggested approach's multilayer sensor network component tackles the speed and bias difficulties that arise in large-scale operations with noisy data.

Results

In terms of precision, the expected model results outperformed competing, currently employed approaches. We devised a novel method for protecting SDN from distributed denial of service attacks by comparing the benefits and drawbacks of the previously stated approaches. The proposed approach takes into account both fixed and mobile devices that are the source of distributed denial of service assaults. This is the inventive aspect of the solution. To summarise, it successfully and rapidly blocks attacks. Furthermore, our strategy outperforms and is more accurate than current methods. There has also been a decrease in false alarm rates.

2. Materials and Methods

Proposed Method

The first step involves the collect and preparation of data.

- Collect information on network traffic from mobile and stationary devices that are connected to the software-defined networking architecture.
- Incorporate characteristics such as the size of the packet, the kind of protocol, the source and destination IP addresses, and the amount of traffic.
- Depending on the circumstances, preprocess the data in order to standardise, scale, and encode categorical features.

Using DELM, the second step involves unsupervised feature learning.

- Unsupervised feature learning can be accomplished through the utilisation of a Deep Extreme Learning Machine (DELM) architecture.
- The DELM model should be trained on the data of the unlabelled network traffic in order to extract high-level representations of the data without the need of explicit labels.

Step 3: Integration of learning that is only partially supervised:

Data that has been labelled should be incorporated into the DELM model, which has instances that are labelled as either regular or DDoS Attacks.

Apply semi-supervised learning approaches, such as self-training or co-training, to the DELM model in order to fine-tune it so that it can adapt its representation to the instances that have been labelled while simultaneously utilising the features that have been learnt from unlabelled data.

Step 4: Dynamic adaptation of features: are dynamic characteristics that are associated with mobile devices in the model. Some examples of these characteristics are movement patterns, signal strength, and connection stability.

Maintain a consistent process of updating the model's representation in accordance with the ever-changing characteristics of mobile devices and the ways in which they interact with the SDN infrastructure.

The fifth step involves the detection and classification of intrusions.

For the purpose of classifying incoming network data from mobile and stationary devices as either normal or malicious, the trained SDELM model should be utilised.

Through the utilisation of threshold-based techniques or anomaly detection algorithms, it is possible to identify distributed denial of service assaults by identifying deviations from the typical activity.

Adaptive mitigation is the sixth step.

Develop and implement adaptive mitigation measures inside the SDN architecture in order to counteract the DDoS attacks that have been discovered.

The effects of distributed denial of service attacks (DDoS) on network performance for mobile and stationary devices can be mitigated by modifying flow rules in software-defined networking (SDN) switches dynamically in order to divert or delete suspicious traffic flows.

The suggested SDELM technique is next evaluated for its effectiveness by means of real-world DDoS assault scenarios that include both mobile and stationary devices. This is the seventh step in the evaluation and validation process. The detection accuracy, false positive rate, response time, and resource utilisation should all be evaluated in order to establish the usefulness of the strategy and confirm that it is a benchmark for existing methodologies. In the eighth step, deployment and integration, It is recommended to implement the SDELM model within SDN infrastructures, including it within the frameworks that are already in place for network management and security. Real-time monitoring and mitigation of distributed denial of service attacks (DDoS) directed at mobile and stationary devices should be made possible by ensuring a seamless interface with software-defined networking (SDN) controllers and switches.

Figure 2 illustrates the three stages that make up the proposed project: data collecting, detection of distributed denial of service attacks, and mitigation of DDoS attacks. We take a look at a framework for a decentralised software-defined network that makes use of both local and universal controllers to provide a central connecting point. According to Aldweesh et al.'s research from 2020, users are the ones that initially deliver the packets to the network for transmission. At the beginning of the process, the data capturing module is executed by configuring the access point with switches that are enabled with

OpenFlow function as gateways. It is possible for all of the traffic that is generated by the linked devices to pass via the OpenFlow switch because of the configuration. In accordance with Huang et al.'s 2023 research, this structure is significant since it gives the local controller the authority to decide whether or not to forward or drop the traffic. The central limit theorem serves as the foundation for the type 2 interval fuzzy techniques that are used to arrive at this conclusion. In order to determine its membership functions, the conventional type 2 interval fuzzy is selected. As a result of the fact that the upper and lower borders are selected at random, the central limit theorem was modified to better accommodate the situation. It is an example of what is known as the midway limit.

A theorem about fuzzy sets with intervals of type2. The time it takes to make a decision is the primary focus of the evaluation, which can then be contrasted with more conventional approaches. Additionally, in order to efficiently manage the traffic, an out-of-band connection is utilised. This connection directs the traffic through the switch to the appropriate local controller. Next, the local controller will collect and analyse the traffic, determining the essential characteristics of the packets based on the information they contain. In comparison to hierarchical clustering, the K-means clustering method is recommended for use in traffic processing because of its capacity to produce clusters that are more closely related to one another. Although the Euclidean distance was utilised, it is important to note that it suffers losses in situations where the dimensionality of the data is substantially high. The term "curse of dimensionality" refers to a phenomena associated with this particular instance. Therefore, it is modified to conform to the Douglas-Peucker algorithm, which is used to derive optimal tolerance segmentation lines. These lines are the foundation upon which clustering is built. A technique known as Douglas-Peucker-K-Means Clustering (DP-KMC) is the name given to this operation. Immediately after the end of this process, the packets are discarded in order to free up memory resources.

In order to identify distributed denial of service attacks (DDoS), the extracted feature data is sent into the detection module, which is functioning across all local controllers. For the purpose of facilitating DDoS attack detection, the ELM_ERL-AlexNet model is trained with the DDoS attack detection dataset. The training method for the model includes the preprocessing of the dataset, followed by the extraction of features and classification. However, it demonstrated a low learning rate for high-dimensional data, which led to its selection for classification. Conventional AlexNet was selected for classification because of its superior error performance regarding previous classifications. For this reason, it has been modified to correspond with an Evolutionary Reinforcement Learning (ERL) method that is based on extreme learning machines. The acronym ELM_ERL-AlexNet is used to refer to it. A substantial number of advantages are offered by ELM, mostly as a result of its speedy training process. Random parameter initialisation and straightforward matrix operations are utilised by ELM, which results in a significant reduction in the amount of time required for training. Different training strategies, such as those that rely on slower gradient-based learning algorithms, are differentiated from this approach. The attack mitigation module is activated and integrated into the local controllers when the ELM_ERL-ALexNet system detects a distributed denial of service attack (DDoS). This particular module is designed to take in a list of devices that have been categorised as harmful. It is necessary to differentiate between stationary devices (SD) and mobile devices (MD) in order to devise distinct tactics that can be used to defend against these attacks. These strategies are established depending on the features of the devices. There are certain access points that are related with stationary devices, such as smoke alarms that are

fixed within a building. These devices occupy a defined location within the building. Additionally, these devices do not require any additional Authentication and Authorisation (AA) procedures once they have been configured. Mobile gadgets, such as smartphones, on the other hand, are not stationary; rather, they are portable and may be moved around without restriction. As a consequence of this, medical professionals are required to finish the AA process anytime they cross into the coverage area of an Access point. The Wu-Manber (WM) algorithm was selected because of its high level of efficiency in quick matching and its ability to match multiple patterns simultaneously in AA. The LSB strings and the related subtraction unit are often responsible for determining the shift value in a consistent manner. This may result in conclusions that are not ideal; hence, it has been modified to make use of an optimisation technique that takes into account the length of strings as input and finds the minimal shift for matching. It is because of its higher exploration capabilities that the Fox optimisation method has been selected. The factorial of the population size, denoted by n!, is used to arrive at a random determination of the ideal position for animals to hunt. n!-Fox optimised Wu-Manber (n!-Fox-WM) is the name given to this particular technique. A thorough overview is utilised by the controller in order to classify harmful devices into SDs and MDs. This allows the controller to manage a variety of device categories in an effective manner. An illustration of the flowchart of the suggested model can be found in Figure 1. With the incorporation of both mobile and stationary devices into the DDoS attack mitigation strategy; this suggested method intends to provide comprehensive security for the full software-defined networking (SDN) infrastructure infrastructure. It has been demonstrated that the implementation of Semi-supervised Deep Extreme Learning Machines (SDELM) leads to enhanced precision and adaptability in the detection of Distributed Denial of Service (DDoS) assaults (Haider et al., 2020; Gebremeskel et al., 2023). Furthermore, this application effectively mitigates the impact of attacks on the overall performance of all connected devices.

4. Experimental Setup

For the purpose of this investigation, the datasets NSL-KDD, CIC-IDS 2019, and Mendeley 2020 were utilised. This information has been compiled by the Canadian Cyber Security Institute for the purpose of conducting investigations into intrusions. Data relevant to traditional attacks are included in the CIC-IDS2019 dataset, which includes both qualitative and quantitative characteristics. Through the transmission of labelled flows, protocols, and temporal data regarding assaults, as well as specifics on targets, target IPs, and location ports in a CSV file format, CICFlowMeter makes it possible to do network traffic analysis. The purpose of this project is to train machine learning models for the detection of distributed denial of service attacks by focussing on DDoS traffic. Table 1 provides an overview of the parameters of the system as well as the materials that were utilised for training and testing. The ratio of malicious traffic to distributed denial of service occurrences was sixty percent to forty percent, and a total of ninety thousand samples were submitted for dissemination. During normal circumstances, traffic is assigned a value of zero, however during DDoS attack situations, it is assigned. Using classification algorithms from the scikit-learn library, the dataset is divided into training subsets (eighty percent) and testing subsets (20 percent), with a test size of 0.02. Following the separation, a total of 71,000 samples were earmarked for training, while 19,000 samples were assigned for testing purposes. As a result of differences in size and the characteristics of the values, which might be

continuous or discrete, the dataset demonstrates that one encounters difficulties when attempting to compare the features to the learning network...

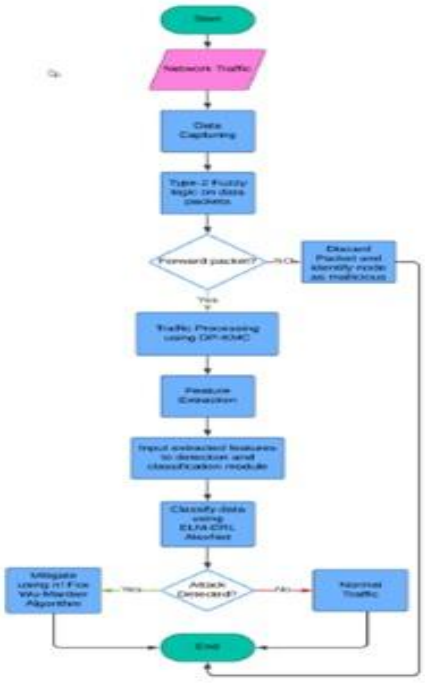

Fig. 1: Flowchart of the proposed system

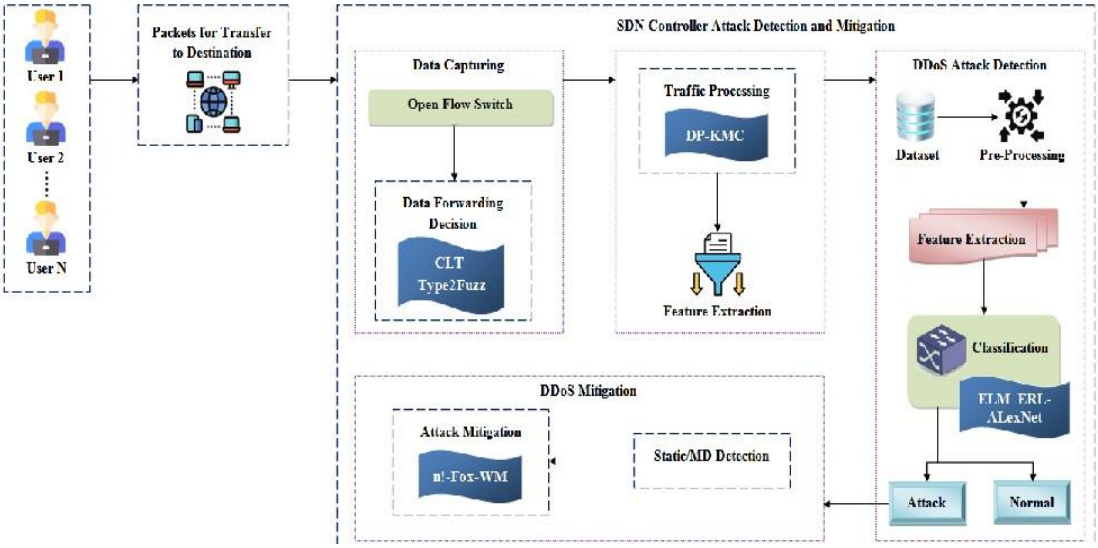

Fig. 2: Block diagram of proposed system

Table 1: Material and system specifications

System Manufacturer	Lenovo
Processor	Intel core i7 6700 CPU
Memory	8GB
OS	Ubuntu 16.04
Emulator	Mininet 2.2.1
Controller	ODL and RYu
Data set	CICDDos – 2019
Switch	Open flow enabled switches
Libraries	Tensor flow 2.x , Keras, Pytorch 1.x

5. Results and Discussion

Evaluation Metrics

This section outlines frequently used evaluation metrics for measuring the performance of machine learning and deep learning techniques in intrusion detection. All ranking metrics are based on the attributes utilized in the confusion matrix (Fig. 3). The two-dimensional matrix displays information about actual and predicted classes, including the following components:

i. True Positive (TP): Instances of data correctly classified by the classifier as an attack.

ii. False Negative (FN): Instances of data that are incorrectly classified.

iii. Categorized as normal instances

iv. False Positive (FP): Instances of data incorrectly classified as an attack.

v. True Negative (TN): Cases correctly classified as normal instances.

The diagonal entries of the confusion matrix denote accurate predictions, while the off-diagonal entries reflect erroneous predictions made by a particular classifier. Figure 3 depicts the features of the confusion matrix. In a Software-Defined Networking (SDN) environment, real-time traffic analysis is crucial; the confusion matrix assists network administrators in evaluating the reliability of the DDoS detection system.

Enables informed decision-making concerning the modification of thresholds or the introduction of supplementary security measures based on identified error types (Salem et al., 2022). The confusion matrix is utilized in attack prediction to categories error types.

The model generates both false positives and false negatives. It facilitates understanding the trade-offs between different metrics. Enhancing recall can result in decreased precision, as the acceptance of additional false positives may facilitate the identification of more true positives. Furthermore, it provides

insight into the need for model tuning, the acquisition of supplementary data, or the integration of additional features.

Precision denotes the ratio of correctly identified attacks to the total instances predicted as attacks.

Recall is the ratio of accurately identified attack instances to the total number of actual attack instances.

The false alarm rate, also known as the false positive rate, is defined as the ratio of incorrectly predicted attack samples to the total number of normal samples.

The true negative rate is defined as the proportion of accurately identified normal samples relative to the total number of normal samples.

		PREDICTED CLASS	
		ATTACK	NORMAL
ACTUAL CLASS	ATTACK	TRUE POSITIVE	FALSE NEGATIVE
	NORMAL	FALSE POSITIVE	TRUE NEGATIVE

Fig. 3: Confusion matrix for attack classification

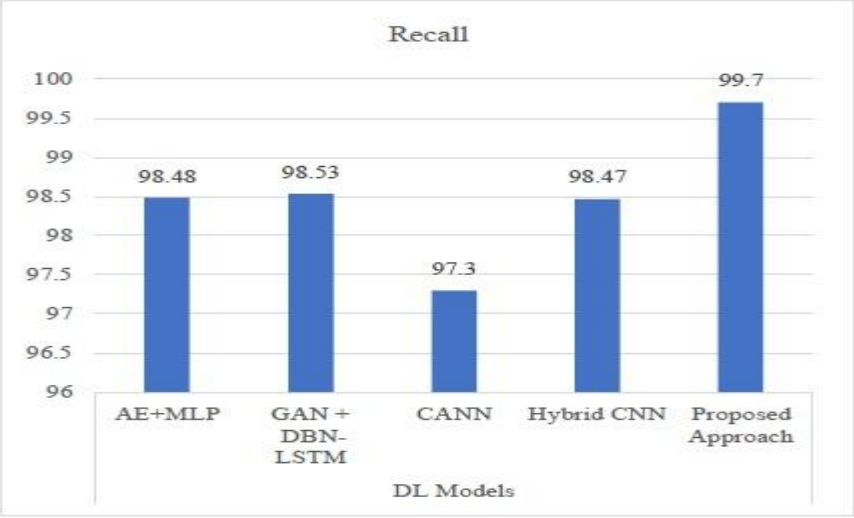

Fig. 4: Recall rate comparison

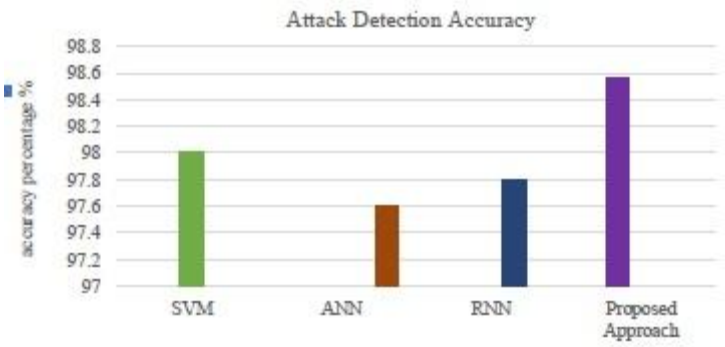

Fig. 5: Accuracy comparison

Accuracy, defined as the ratio of correctly identified samples to the total number of samples, is a critical metric in evaluation. It is frequently employed as a performance measure for a balanced dataset.

The F1-Measure quantifies the accuracy of the model across the dataset. The harmonic mean of the model's precision and recall characterises it.

Table 2 provides a detailed comparison of recent strategies for mitigating DDoS attacks in Software-Defined Networking (SDN). Our methodology exhibits superior efficacy in the classification of packets as either attacks or benign, as indicated by the precision and recall metrics. The duration required for attack detection is markedly less than that of alternative methods, and CPU utilisation is concurrently diminished, leading to resource conservation and enhanced results. The following figures present a comparative analysis of our proposed methodology relative to existing approaches, focussing on Recall Rate (Fig. 4), Accuracy (Fig. 5), Precision, and F-measure (Figs. 6a-b).

Semi-supervised learning offers specific advantages compared to alternative methods for addressing DDoS attacks in SDN, which is the rationale for its selection in our study based on the following benefits:

1. Semi-supervised techniques effectively utilise a significant amount of unlabelled data, often present in network environments, to enhance model generalisation. This leads to the efficient identification of data patterns, thereby improving the performance ratio for distinguishing between normal and attack traffic.

2. Cost efficiency: The procurement of labelled data for training machine learning models, particularly in security areas such as DDoS attack detection, is frequently constrained and costly (Joëlle and Park, 2018). Semi-supervised learning minimises dependence on labelled data, improving cost efficiency by utilising both labelled and unlabelled data for training purposes.

3. Flexibility in dynamic environments: Software-Defined Networking (SDN) environments exhibit dynamic characteristics, with network traffic patterns continuously evolving (Jiang et al., 2022). Semi-supervised learning techniques exhibit superior adaptability to changes in data distribution compared to

supervised methods. Adapting is crucial for effectively mitigating DDoS attacks in Software-Defined Networking (SDN) due to the swift evolution of attack patterns.

4. Robustness to noise and outliers: Network traffic data from real-world scenarios often contains noise and outliers (Tuan et al., 2020), which can negatively impact the performance of supervised learning models. Semi-supervised methods exhibit improved resilience to noise and outliers through the utilisation of both labelled and unlabelled data, resulting in the creation of more accurate and robust models.

Semi-supervised learning methods are efficient for analysing extensive datasets, making them appropriate for handling substantial amounts of network traffic data in Software-Defined Networking (SDN) contexts. Thus, it enables a more comprehensive analysis and streamlines detection..

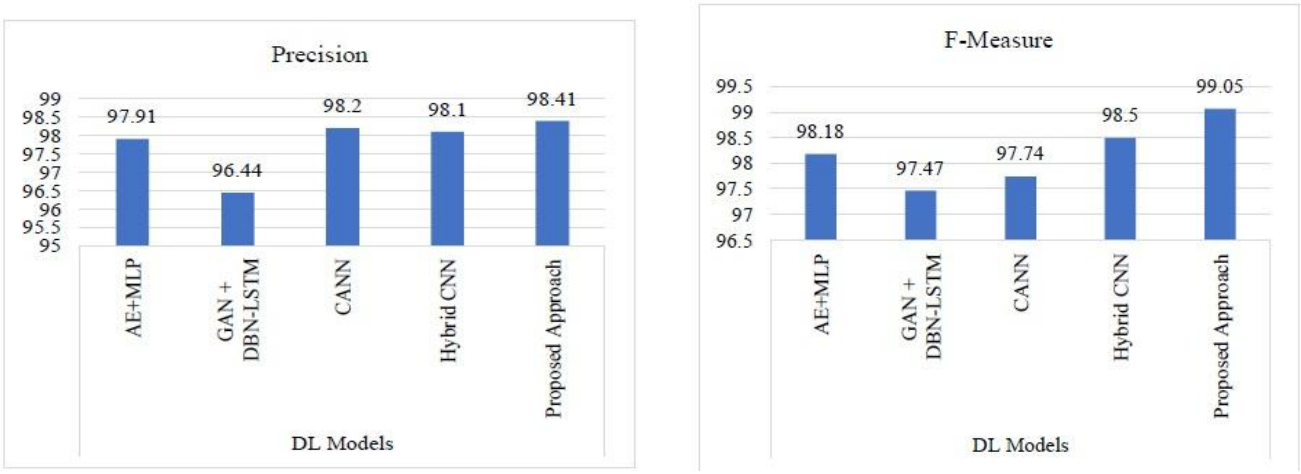

Fig. 6: (a) Precision comparison; (b) F-Measure comparison

The introduction of semi-supervised learning techniques into the mitigation of distributed denial of service attacks for software-defined networking (SDN) might result in solutions that are more robust, adaptive, and cost-effective, as stated by Rahman et al. as stated in their 2019 publication. Additionally, these solutions are better suited to the dynamic and complicated character of the contexts in which current networks operate.

Because of its easy structure, the model that was proposed earlier is superior to the other ways. This is because of the fact that it was simpler. In order to provide results more quickly, semi-supervised learning is able to analyse both labelled and unlabelled data. This ability allows it to process both types of data. In order to provide proactive and adaptive DDoS mitigation in software-defined networking (SDN), the suggested method combines flow-based filtering with machine learning techniques. This allows for protection against distributed denial of service attacks. DP K-Means Clustering is the algorithm that is utilised in this process.

The classification of network traffic is accomplished through the application of the KMC algorithm. After careful consideration, the Wu-Manber (WM) algorithm was selected because of its capabilities in multi-pattern matching and efficient matching features, which ultimately led to the acceleration of attack

detection. Numerous advantages are offered by ELM_ERL-ALexNet, the majority of which are attributable to its capacity for quick training. A decrease in the number of false alarms and an increase in precision are the outcomes of mitigation

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

Author	Classification Accuracy	Precision	Recall	F-Measure	Detection Time	Training Time	CPU Usage
Proposed	98.92 %	98.41 %	99.70%	99.05%	0.029	23.00	4.95%
Tan et al(2024)	98.65	98.10%	98.47%	98.50%	0.061	39.52	6.02%
Lin et al.(2020)	97.40%	98.20%	97.30%	97.74%	-	40.00	---
Chen et al (2023)	91.23%	96.44%	98.53%	97.47%	---	---	--
Wei et al.(2021)	98.34%	97.91%	98.48%	98.18%	--	--	--

6. Conclusion

A viable strategy for enhancing network security in dynamic environments is presented by the method that is suggested for addressing Distributed Denial of Service (DDoS) attacks in Software Defined Networking (SDN) through the Semi-supervised Deep Extreme Learning Machine (SDELM) model. This model takes into account both mobile and stationary devices. By utilising semi-supervised learning approaches, the model is able to successfully include both labelled and unlabelled data, which ultimately results in an improvement in the accuracy and adaptability of DDoS attack detection and mitigation. In comparison to more conventional approaches, the SDELM model has a number of benefits, including improved use of unlabelled data, cost-effectiveness, adaptation to shifting contexts, robustness against noise and outliers, and scalability. It is an appropriate approach for mitigating distributed denial of service assaults inside software-defined networking infrastructures, particularly in situations that are marked by quickly changing network traffic patterns and limited availability of annotated data, as the advantages that have been described indicate.

7. Future Scope

Despite the fact that the strategy that has been offered has the potential to be successful, there are now other prospects for further research and development.

1. Improved model architecture: In order to enhance the SDELM model's capability to capture temporal correlations and complicated patterns in network traffic, it is recommended to investigate the use of advanced deep learning architectures, such as Recurrent Neural Networks (RNNs) or transformers.

2. Dynamic adaptation: Establish methods that will allow the SDELM model to evolve in real time in response to shifting network conditions and attack patterns. This will ensure that DDoS attacks are effectively mitigated on a continuous basis.

3. Integration with SDN controllers: Incorporate the SDELM model directly into SDN controllers in order to ensure a smooth deployment and real-time decision-making, which will make it easier to automate the mitigation of known distributed denial of service threats.

4. Evaluation in real-world environments: In order to evaluate the effectiveness and scalability of the proposed technique, it is necessary to carry out a comprehensive evaluation and verification of the method in real-world software-defined networking (SDN) environments. This evaluation should take into consideration a variety of network topologies, traffic loads, and attack scenarios.

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)

8. REFERENCES

[1] 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.

[2] 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.

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

[4] 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

[5] 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

[6] 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

[7] 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

[8] 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

[9] 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

[10] 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

[11] 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

[12] 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

[13] 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

[14] 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

[15] 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

[16] 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.

[17] 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

[18] 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

[19] 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.

[20] 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.

[21] 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

[22] 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.

[23] 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