Early DDoS Attack Detection Using Lightweight Deep Neural Network

Ahmed F. Almukhtar[1,*], Noor D. AL-Shakarchy[2], Mais Saad Safoq[1]

[1]Department of Information Technology, Faculty of Computer Science and Information Technology, University of Kerbala, Iraq

[2]Department of Computer Science, Faculty of Computer Science and Information Technology, University of Kerbala, Iraq

Emails: ahmed.almukhtar@uokerbala.edu.iq; noor.d@uokerbala.edu.iq; mais.s@uokerbala.edu.iq

Abstract

In the digital age, e-commerce platforms are critical components of the global economy, facilitating seamless transactions and interactions between businesses and consumers. The digital infrastructure of these institutions is frequently attacked, either to hack or disrupt online services, leading to significant financial losses and damage to reputation. The most famous of these attacks are DDoS attacks, which lead to an increase in the volume of traffic to the platform's website beyond the capacity of the servers, thus causing the platform to respond slowly and crash and customers to be unable to access it. The increase in these attacks causes significant material damage to institutions, whether in the loss of revenues or the cost of responding to attacks. This work presents a robust DDoS attacks early detection model that can be adopted on e-commerce platforms using a lightweight one-dimension Convolutional neural network. The proposed model leverages the efficiency of deep learning with the lightweight architecture to analyze network traffic in real time, identifying patterns indicative of an impending DDoS attack. The balance between high detection accuracy with computational efficiency makes it suitable for real-time implementation in diverse e-commerce environments. DNN is trained on a comprehensive dataset of network traffic, encompassing both normal and attack scenarios, to ensure it can distinguish between legitimate traffic spikes and malicious activity. DDoS Evaluation Dataset CIC-DDoS2019 and CICIDS2017 are used in the experimental and accuracy achieved 0.98 and 0.99 in these two datasets respectively.

Keywords: Distributed Denial of Service (DDoS); One Dimensional Convolutional Neural Network (1D CNN); Convolution layer; Max pooling Layer; Dropout layer; Normalization

1. Introduction

An application layer distributed denial of service (DDoS) attack targets the functional capabilities and applications on a network and effectively disrupts services. Its advanced techniques and its targeting of the upper layer of the network structure, where the focus is on disabling or undermining the capabilities of applications and services to function properly, characterize this type of attack. The early detection enables proactive arrangements to alleviate the impact of DDoS attacks, such as traffic filtering and resource allocation adjustments, thereby ensuring the continuous availability and performance of e-commerce services and taking effective measures to defend against this complex type of attack [1]. The main effects of DDoS attacks on the application layer include [2]:

- Disable access to the service: The application-layer DDoS attacks are leading to undermining users' ability to access the targeted application or service. This disables the basic functionality of the application and prevents users from accessing the content or services provided.
- Loss of data and information: A DDoS attack at the application layer may cause data or information loss, especially if the attack is accompanied by additional techniques such as hacking attacks or the use of security vulnerabilities in the application.

DOI: https://doi.org/10.54216/FPA.190228
Received: December 08, 2024 Revised: February 01, 2025 Accepted: March 01, 2025

- Effect on performance: A DDoS attack can significantly reduce application performance, as it overloads servers and infrastructure, causing slow response times and increased loading times.
- Loss of confidence: The effects of DDoS attacks can cause a loss of trust by users and customers, especially if the service is frequently intercepted.
- Response costs: To restore service to normal after a DDoS attack, companies and organizations may require enormous efforts and additional costs to enhance security and prepare for such future attacks.
- Impact on reputation: A DDoS attack at the application layer can have a negative impact on the reputation of an organization or site, especially if the service relies heavily on continuous availability and good performance.

Using the lightweight architecture of convolutional neural networks comes with several technical and practical benefits, which can make them a good choice in application cases that require good performance and efficient operation on a variety of devices based on [3]:

- Efficiency in operation: Lightweight architectures are simple and resource-efficient, enabling models to run more efficiently on a variety of devices.
- Training speed: Lightweight networks are relatively faster in training due to their simplicity and reduced number of computational units required.
- Quick response: Thus, due to simplicity and lightness, light networks can be more responsive to real-time data analysis.
- Low memory consumption: Lightweight models are memory efficient, which helps in running them on devices with limited resources.
- Easy transportation: Lightweight templates can be easily moved between different devices, making them convenient to move around and use on a variety of devices.
- Improving performance in limited environments: In resource-constrained environments, light networks are better able to achieve good performance without increasing resource consumption.
- Ease of optimization and integration: Simplicity in architecture makes optimization and integration easier and more flexible.

This paper presented a new Lightweight architecture CNN model to detect normal network traffic benign) or abnormal ones (anomalous/DOS attack). The proposed CNN model includes real-time monitoring, behavioral analysis, and anomaly detection, all integrated into one model. This model uses time histories (records) to understand the temporal patterns of traffic at the application layer as well as analyze user behavior to detect abnormal (anomalous) patterns or attacks. The spatial features (salient features) extracted from data, such as digital data related to the time frequencies can contribute to improving network security as well as the effectiveness of response to ongoing and advanced DDoS attacks. The contributions of this paper are:

- ✓ Present an E-commerce Platforms Protection model based on Early DDoS Attack Detection. By implementing this system, e-commerce platforms can achieve heightened resilience against DDoS attacks, maintaining operational continuity and customer trust in the face of evolving cyber threats.
- ✓ Design a new lightweight architecture of 1D-CNN model that can provide high efficiency with limited computing resources.

2. Related Work

The literature review contains rich content on different methods used to identify the application layer Distributed Denial of Service (DDoS) attacks. DDoS attacks are increasing and becoming more complex, causing major difficulties for internet-enabled networks. Various machine learning and deep learning approaches were used for the DDoS detection and many difficulties and challenges emerged associated with this field [1,2]. Most of these attacks cannot be identified due to their hidden nature, in addition to the availability of easy-to-use tools that can be used in these attacks. These researchers contribute worthy knowledge on the DDoS attacks and explain immediate methods for defeating them.

Ahmed et al. detect a DDoS attack based on using multi-layer Perceptron model [6]. This system showed a high performance in identifying and detecting the attacks. The combination of the Cuckoo Search Algorithm and Radial Basis Function adopted in [7] as an approach for DDoS attack detection, the proposed system shows an enhanced

DOI: https://doi.org/10.54216/FPA.190228
Received: December 08, 2024 Revised: February 01, 2025 Accepted: March 01, 2025

performance of the machine learning approach and comparable results with the state-of-the-art methods, scoring 96.9% accuracy.

A Decision Tee algorithm and the Gini index feature selection technique were investigated as an approach for DDoS attacks detection in [8]; the proposed strategy performed well in comparison with other methods and obtained 98% accuracy rate considering a minimum number of features selected. A user feature selection approach was investigated in [9]; in their research Bravo and Mauricio proposed a real-time detection technique to predict the attack online. The selected features depend on the user's identity, whether it was a tool or an actual user. A Stacked Autoencoder deep learning technique is adopted in [10] to extract strict features for DDoS attacks detection in the application layer; the proposed technique resulted with an accuracy 98.99%.

Li et al. [11] presented a deep learning model for detecting DDoS attacks in real-time in the Software-Defined Network (SDN). The model extracts the features from the network traffic and predicts the expected attack. In [12], Liao et al. extracted a feature vector composed of two types of features from the user login information to represent a sparse vector that was applied to the (SVD-RM) algorithm for detecting the attacks in the application layer. Muse and Abebe [13] built a system using different machine learning techniques and contributed to the literature review as a comprehensive knowledge to distinguish between the attack of application-layer DDoS and the flash crowds; they adopted a decision tree that performed well and obtained 99.445% F1 score accuracy,

In [14] the researchers investigate different machine learning approaches and consider the RBPBoost algorithm for the recognition of the DDoS attacks; the adopted mechanism performed well and obtained a recognition rate of 99.4%. Sharif et al. [15] proposed a machine learning system to enhance the DDoS caused by different available toolkits; the detection approach depends on selecting the appropriate set of features; the result of the system was promising, with a scored recognition rate of 99.9%. Tripathi and Hubballi [16] investigate DDoS attacks at the application level as well as provide a comprehensive overview of the defence mechanisms available.

In [17], Wei Zhou et al. introduce a methodology for the detection of distributed denial of service (AL-DDoS) attacks and defence strategies during thick traffic over the web. The methodology requires building a Real-time Frequency Vector (RFV) and adopting it to express the traffic as a continuous system; via analysing the entropy of AL-DDoS attacks and flash crowds, the system can identify real AL-DDoS attacks. Adedeji et al. [18] provide a brief explanation of the methods and approaches used to detect DDoS attacks in the Internet of Things. This includes available methods in machine learning in addition to deep learning models. Zeebaree et al. [19] contribute a detailed review of the defence and detection of application layer distributed denial of service (DDoS) attacks. The review illustrates the difference between Dos, DDoS attacks, and the conclusion that DDoS is a critical issue over the Dos. Another attempt handled by Bahashwan et al. [20] examined several resources that adopted machine learning and deep learning approaches for detecting DDoS attacks in software-defined networking (SDN). The resource investigates the existing methods of attack detection that contribute to improving SDN security.

A Systematic Review examined in [21] covered a variety of machine learning and deep learning techniques adopted for the detection of distributed denial-of-service (DDoS) attacks in software-defined networks (SDN). The review also highlights the usability of different techniques and evaluation measurements in the underlined research.

3. The Proposed Lightweight DDoS Detection Model

His work presents E-commerce platform protection based on Early Application-Layer DDoS Attack Detection by using a one-dimensional convolutional neural network model with a new lightweight architecture. This model can analyse input data to discover relationships or patterns that contribute to classification decision-making. The proposed model includes real-time traffic monitoring, behavioural analysis through packet inspection and analysing the application-layer requests, and anomaly detection by interpreting the relevant features of the unknown behavior for anomalies (abnormalities) detections in the application-layer requests, all integrated into one model. The lightweight nature of 1D-CNN deep neural networks is utilized to learn patterns and characteristics of normal and malicious traffic for real-time anomaly detection and classification of incoming traffic. Figure 1 block diagram outlines the main components of a proposed system.

DOI: https://doi.org/10.54216/FPA.190228
Received: December 08, 2024 Revised: February 01, 2025 Accepted: March 01, 2025

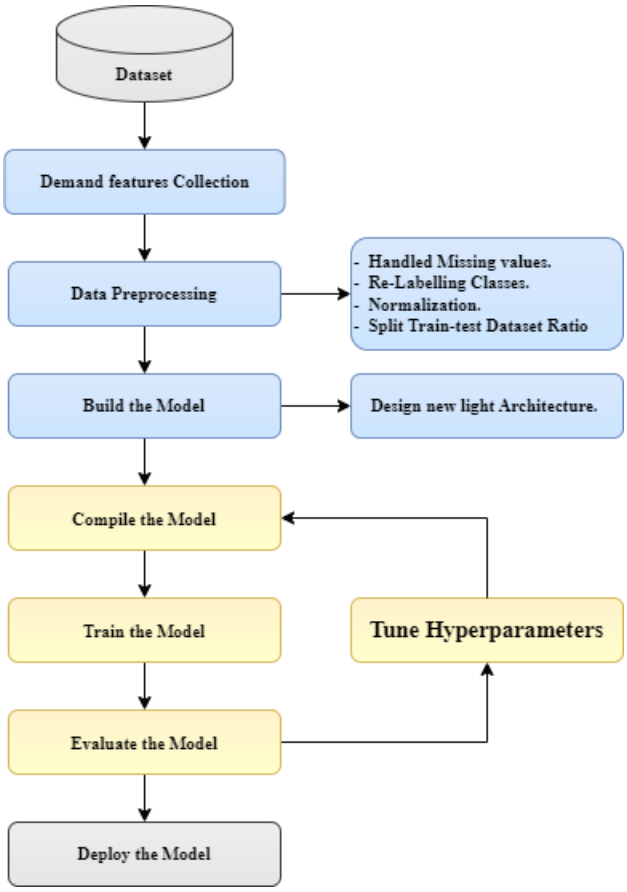

Figure 1. The Action Steps Block Diagram of the Proposed Lightweight DDoS Detection Model.

A. Dataset

The CIC-DDoS2019 and CICIDS2017 datasets are a comprehensive dataset created by the Canadian Institute for Cybersecurity (CIC) to provide a detailed and realistic set of DDoS attack scenarios for research and evaluation purposes. This work was implemented with two datasets: the DDoS Evaluation Dataset (CIC-DDoS2019 [22] and CICIDS2017 [23]).

B. Demand features Collection

Firstly, a labelled dataset containing examples of both Benign: normal and DDoS traffic at the application layer is collected. Demand features are computed by examining the new requests.

C. Data preprocessing

Some necessary transformations are processed on data. The first step is handling the missing values based on ignoring data with more missing entries and replacing other missing values in the dataset by imputing using the 'interpolation' technique to estimate unknown data points between two known data points. According to the Application-Layer DDoS Dataset, that has three classes "DDoS slow loris", "DDoS Hulk" and "BENIGN": it is re-labeling these classes to binary traffic classes "normal/BENIGN" and "DDoS/malicious."

To avoid overfitting and improve the performance and generalization capabilities of the proposed model, the data-resampling step must be done in the dataset to ensure that each class has a similar number of samples. The data-resampling step is used to address class imbalance issues in the dataset, where some classes have significantly fewer samples than others do. It involves manipulating the dataset's distribution by under-sampling the majority class (decreasing the number of samples).

Large integer value inputs can lead to disruption or slow down the learning process. To avoid these large values and remove differences in the magnitude of values, a normalization process is adopted, and the input data are scaled to a standard range.

DOI: https://doi.org/10.54216/FPA.190228
Received: December 08, 2024 Revised: February 01, 2025 Accepted: March 01, 2025

The last pre-processing step is to Split the Dataset to ensure fairly and truly assess the performance of the model. The Dataset is divided into three parts with 80:10:10 for training, validation, and test sets consequently. Therefore, 80% of the original dataset is for training, 10% for validation, and 10% for testing.

D. Build the model

This step Designs a suitable architecture for the light-deep neural network. A typical architecture might consist of a few layers to keep it lightweight. The existing DDoS detection methods have a long prediction time; therefore, these methods are not suitable for real-time applications, which rely on the speed of prediction. For that, the attempt to simplify the model and reduce its complexity proposed a 1D CNN model with a new lightweight architecture to detect the status of arrival requests to e-commerce Platforms: normal or DDoS. The small number of neurons (parameters) in the proposed 1D CNN model makes it usable and deployed with limited resources devices, as well as faster training and execution.

Increased accuracy decreased execution time, and implementation with reasonable hardware capability are the main goals of the proposed model. The stages of the model can be illustrated in Figure 2. The details of stacked layers can be illustrated throw Table 1. The convolutional and pooling layers analyzed the collection of Demand features and reduced the number of these features by extracting the salient ones. Then fully connected layers performed the detection step by classifying the extracted feature as a normal request or abnormal request.

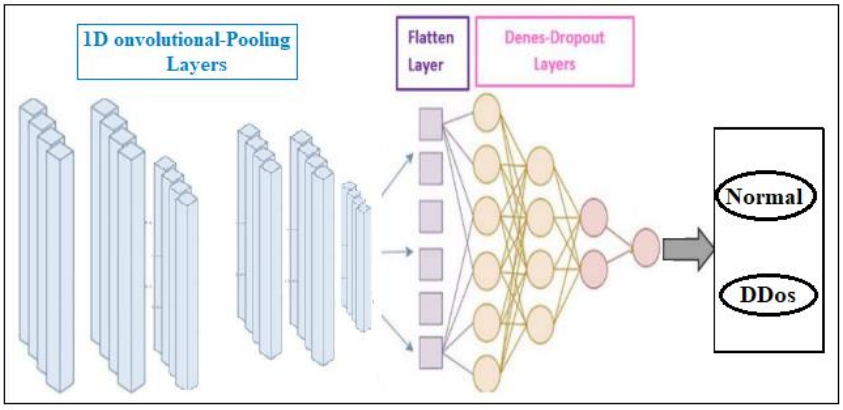

Figure 2. Application-Layer DDoS Detection 1D CNN model.

Table 1: The proposed model summary.

No.	Layer (type)	Output shape	parameters
1	reshape_1 (Reshape)	(None, 78, 1)	0
	conv1d_1 (Conv1D)	*(None, 78, 255)*	*2040*
2	conv1d_2 (Conv1D)	((None, 78, 128)	*163328*
	max_pooling1d_1	*(MaxPooling1 (None, 39, 128))*	*0*
3	conv1d_3 (Conv1D)	*(None, 39, 64)*	*24640*
4	conv1d_4 (Conv1D)	*(None, 39, 32)*	*6176*
5	conv1d_5 (Conv1D)	*(None, 39, 24)*	*2328*
	max_pooling1d_2	*(MaxPooling1 (None, 19, 24)*	0
6	flatten_1 (Flatten)	*(None, 456)*	0
7	*dense_1 (Dense)*	*(None, 500)*	*228500*

DOI: https://doi.org/10.54216/FPA.190228
Received: December 08, 2024 Revised: February 01, 2025 Accepted: March 01, 2025

	dropout_1 (Dropout)	*(None, 500)*	0
8	dense_2 (Dense)	*(None, 100)*	*50100*
	dropout_2 (Dropout)	*(None, 100)*	0
9	*dense_3 (Dense)*	*(None, 1)*	*101*
Total params: 477,213 Trainable params: 477,213 *Non-trainable params: 0*			

E. **Compile the Proposed Model:**

Fine-tuning the hyperparameters is done in this stage to optimize the model's performance. The loss function used is "binary cross-entropy" the metric is "accuracy" and other hyperparameters are set based on trial and error. The best-fixed values are shown in Table 2.

Table 2. The Proposed Model Hyperparameters

Hyperparameter	**Value**
Learning Rate	0.001
decay	1e-6
momentum	0.9
Batch size	*200*
Loss func.	Binary cross-entropy
metric	accuracy

F. Train the Proposed Model:

The model is training using the training set to learn the input patterns and that learning performance is evaluated during the training process using the validation set to avoid overfitting. The performance of a proposed model over time can be presented and imagine how well it is learning and optimizing from the training and validation data consequently. The result of this proposed model behaviour can be shown in Figure 3.

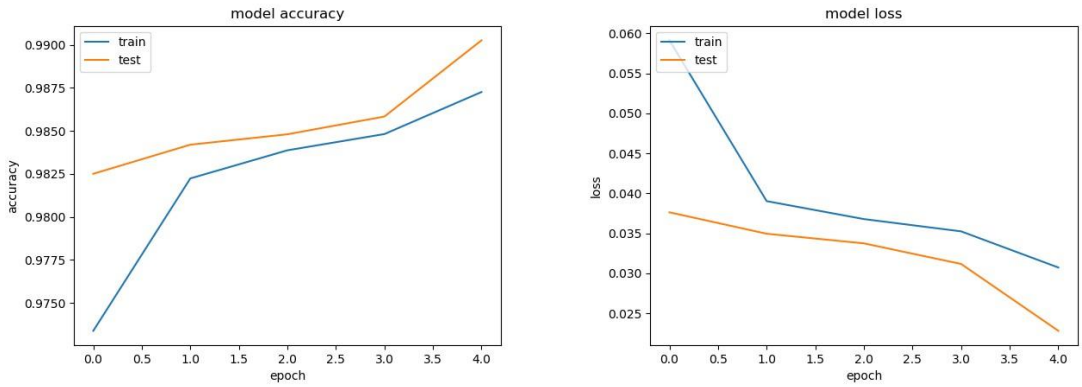

Figure 3. The Learning curve behavior during the training process.

G. Results and Evaluate the Model:

To address the class imbalance, improve model performance, mitigate biases, and enhance interpretability an oversampling process is done; Table 3 reflects this process. The performance metrics (accuracy and loss functions) are used to estimate the overall model performance and training Progress. These metrics can provide insights into how well the model is learning. The results of these two metrics are presented in Table 4.

DOI: https://doi.org/10.54216/FPA.190228
Received: December 08, 2024 Revised: February 01, 2025 Accepted: March 01, 2025

Evaluating a deep learning model on testing data is an essential step to assess its generalization to new, unseen data and demonstrate its ability to detect Application-Layer DDoS attacks with high precision and low false-positive rates. Various metrics are used to measure overall effectiveness such as the model's accuracy, precision, recall, macro average, and weighted average.

The results of these metrics over two used datasets can be presented in Table 5 and Table 6. The confusion matrix of these datasets is presented in Figures 4 and 5.

Table 3: Oversampling process of two used datasets.

Dataset name		**Training set**			**Testing set**		
		Total	**BENIGN**	**DoS**	**Total**	**BENIGN**	**DoS**
Dataset1	**Original**	2830735	557646	2273089	566147	111486	454661
	resampling	3636856	1818428	1818428	909322	454661	454661
Dataset2	**Original**	809360	370623	438737	346868	159294	187574
	resampling	877474	438737	438737	375148	187574	187574

Table 4: The Performance metrics of two used datasets.

Dataset name	**Training set**				**Testing set**			
	Accuracy	**Loss Function**	**Execution Time/ seconds**	**Execution Time%**	**Accuracy**	**Loss Function**	**Execution Time/ seconds**	**Execution Time%**
Dataset 1	0.983	0.053	362.23	0.009 %	0.983	0.054	93.04	0.01%
Dataset 2	0.992	0.023	87.15	0.01 %	0.992	0.023	37.43	0.009%
Average	0.987	0.038	-	-	0.987	0.038	-	-

Table 5: Evaluation metrics of dataset1.

Class	precision	Recall	F1-Score	support
BENIGN	0.98	0.99	0.98	454661
DoS	0.99	0.98	0.98	454661
accuracy			0.98	909322
macro avg	0.98	0.98	0.98	909322
weighted avg	0.98	0.98	0.98	909322

Table 6: Evaluation metrics of dataset2.

Class	precision	Recall	F1-Score	support
BENIGN	0.99	1.00	0.99	187574
DoS	1.00	0.99	0.99	187574
accuracy			0.99	375148
macro avg	0.99	0.99	0.99	375148
weighted avg	0.99	0.99	0.99	375148

DOI: https://doi.org/10.54216/FPA.190228
Received: December 08, 2024 Revised: February 01, 2025 Accepted: March 01, 2025

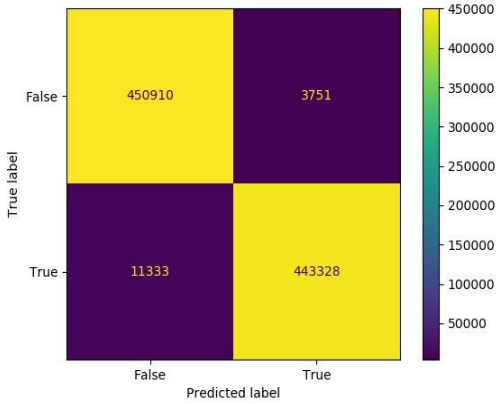

Figure 4. Confusion matrix of dataset1.

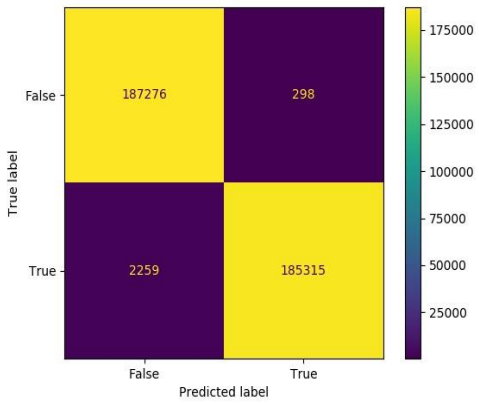

Figure 5. Confusion matrix of dataset2.

Finally, a comparison of some related works with the proposed model is presented in Table 7 below

Table 7: A comparison of some related works with the proposed model

Authors & Reff.	**Year**	**Method**	**Accuracy**
Beitollahi et al. [7]	2022	Cuckoo Search Algorithm and Radial Basis Function	96.9 %
Bouke et al. [8]	2023	Decision Tee algorithm and the Gini index feature selection technique	98 %
Yadav and S. Subramanian [10]	2016	Stacked Auto Encoder deep learning	98.99 %
Proposed Model	**2024**	**Lightweight 1D CNN**	99.2%

6. Conclusion

Providing a reliable and efficient solution for early DDoS attack detection, enhances the security posture of e-commerce platforms, safeguarding them against disruptions and ensuring a seamless user experience. Addressing the numerous risks and possible outcomes connected to these kinds of cyber threats by providing early DDoS detection in real-time. Some major conclusions are obtained during this work.

A proposed model with Lightweight architecture provides computationally efficient, that could emphasize the scalability of the proposed solution and led to real-time detection in large-scale networks. Convolution layers provide the ability to analyze network traffic data and extract the salient features that refer to abnormal traffic and related the relationship between them to set the DDoS pattern. According to the graph of "Relu" function, the use of this function in nonlinear hidden layers is led to passing robust features (greater than zero) and eliminate weak features (less than zero set to zero) and thus it strengthens robust features and weakens weak features. After several layers the most robust features will be retained which represent the basic features that help enhance decision-making.

In the future, the model can extend to Multi-Modal Approaches based on investigating the effectiveness of combining multiple modalities of data, such as network logs, packet headers, or behavioural features, in the detection process. Multi-modal approaches may provide a more comprehensive view of the network and improve detection accuracy. Another future work that can be done is identifying the DDoS attack types as well as with detection to accelerate the response and find solutions of these cyber-attacks.

Funding: "No funds, grants, or other support was received"

Conflicts of Interest: "The authors declare no conflict of interest."

DOI: https://doi.org/10.54216/FPA.190228
Received: December 08, 2024 Revised: February 01, 2025 Accepted: March 01, 2025

References

[1] S. F. University, S. H. Rubin, M. H. Smith, and L. Trajkovic, "Distributed Denial of Service Attacks," in *2000 IEEE International Conference on Systems, Man, and Cybernetics*, vol. 3, no. 10.1109/ICSMC.2000.886455, pp. 2275–2280, 2000.

[2] E. C. and R. Groves, *Distributed Denial of Service (DDoS) Practical Detection and Defense*, 1st ed. USA: O'Reilly Media.

[3] Y. He and T. Li, "A lightweight CNN model and its application in intelligent practical teaching evaluation," *MATEC Web Conf.*, vol. 309, p. 05016, 2020.

[4] M. Jiang, C. Wang, X. Luo, M. Miu, and T. Chen, "Characterizing the impacts of application layer DDoS attacks," in *2017 IEEE International Conference on Web Services (ICWS)*, pp. 500–507, 2017.

[5] V. Durcekova, L. Schwartz, and N. Shahmehri, "Sophisticated denial of service attacks aimed at the application layer," in *2012 ELEKTRO*, pp. 55–60, 2012.

[6] S. Ahmed et al., "Effective and efficient DDoS attack detection using deep learning algorithm, multi-layer perceptron," *Future Internet*, vol. 15, no. 2, p. 76, Feb. 2023.

[7] H. Beitollahi, D. M. Sharif, and M. Fazeli, "Application layer DDoS attack detection using cuckoo search algorithm-trained radial basis function," *IEEE Access*, vol. 10, pp. 63844–63854, 2022.

[8] M. A. Bouke, A. Abdullah, S. H. Alshatebi, M. T. Abdullah, and H. El Atigh, "An intelligent DDoS attack detection tree-based model using Gini index feature selection method," *Microprocessors and Microsystems*, vol. 98, p. 104823, Apr. 2023.

[9] S. Bravo and D. Mauricio, "DDoS attack detection mechanism in the application layer using user features," in *2018 International Conference on Information and Computer Technologies (ICICT)*, pp. 97–100, 2018.

[10] S. Yadav and S. Subramanian, "Detection of application layer DDoS attack by feature learning using stacked autoencoder," in *2016 International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT)*, pp. 361–366, 2016.

[11] C. Li et al., "Detection and defense of DDoS attack–based on deep learning in OpenFlow-based SDN," *International Journal of Communication Systems*, vol. 31, no. 5, Mar. 2018.

[12] Q. Liao, H. Li, S. Kang, and C. Liu, "Application layer DDoS attack detection using cluster with label based on sparse vector decomposition and rhythm matching," *Security and Communication Networks*, vol. 8, no. 17, pp. 3111–3120, Nov. 2015.

[13] B. A. Muse and S. L. Abebe, "Application layer DDoS attack detection in the presence of flash crowd," *Zede Journal*, vol. 38, no. 1, pp. 75–91, Dec. 2020.

[14] P. A. Raj Kumar and S. Selvakumar, "Distributed denial of service attack detection using an ensemble of neural classifier," *Computer Communications*, vol. 34, no. 11, pp. 1328–1341, Jul. 2011.

[15] D. M. Sharif, H. Beitollahi, and M. Fazeli, "Detection of application-layer DDoS attacks produced by various freely accessible toolkits using machine learning," *IEEE Access*, vol. 11, pp. 51810–51819, 2023.

[16] N. Tripathi and N. Hubballi, "Application layer denial-of-service attacks and defense mechanisms," *ACM Computing Surveys*, vol. 54, no. 4, May 2021.

[17] W. Zhou, W. Jia, S. Wen, Y. Xiang, and W. Zhou, "Detection and defense of application-layer DDoS attacks in backbone web traffic," *Future Generation Computer Systems*, vol. 38, pp. 36–46, Sep. 2014.

[18] K. B. Adedeji, A. M. Abu-Mahfouz, and A. M. Kurien, "DDoS attack and detection methods in internet-enabled networks: Concept, research perspectives, and challenges," *Journal of Sensor and Actuator Networks*, vol. 12, no. 4, p. 51, Jul. 2023.

[19] S. R. M. Zeebaree, K. H. Sharif, R. Muhamad, and M. Amin, "Application layer distributed denial of service attacks defense techniques: A review," *Academic Journal of Nawroz University*, vol. 7, no. 4, pp. 113–117, Dec. 2018.

DOI: https://doi.org/10.54216/FPA.190228
Received: December 08, 2024 Revised: February 01, 2025 Accepted: March 01, 2025

[20] A. A. Bahashwan, M. Anbar, S. Manickam, T. A. Al-Amiedy, M. A. Aladaileh, and I. H. Hasbullah, "A systematic literature review on machine learning and deep learning approaches for detecting DDoS attacks in software-defined networking," *Sensors*, vol. 23, no. 9, p. 4441, May 2023.

[21] T. E. Ali, Y.-W. Chong, and S. Manickam, "Machine learning techniques to detect a DDoS attack in SDN: A systematic review," *Applied Sciences*, vol. 13, no. 5, p. 3183, Mar. 2023.

[22] I. Sharafaldin, A. H. Lashkari, S. Hakak, and A. A. Ghorbani, "Developing realistic distributed denial of service (DDoS) attack dataset and taxonomy," in *2019 IEEE 53rd International Carnahan Conference on Security Technology (ICCST)*, Chennai, India, 2019.

[23] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, "Toward generating a new intrusion detection dataset and intrusion traffic characterization," in *2018 4th International Conference on Information Systems Security and Privacy (ICISSP)*, Portugal, Jan. 2018.

DOI: https://doi.org/10.54216/FPA.190228
Received: December 08, 2024 Revised: February 01, 2025 Accepted: March 01, 2025