INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 03, March 2024, pp: 718-724

e-ISSN : 2583-1062

Impact Factor: 5.725

ENHANCED DDOS ATTACK DETECTION USING IMPROVED DEEP CONVOLUTIONAL NEURAL NETWORKS

Mrs. K. R. Prabha[1], Dr. B. Srinivasan[2]

[1]PhD Research Scholar, Department of Computer Science, Gobi Arts & Science College, Gobichettipalayam, Tamilnadu, India.

[2]Associate Professor, Department of Computer Science, Gobi Arts & Science College, Gobichettipalayam, Tamilnadu, India

DOI: https://www.doi.org/10.58257/IJPREMS32996

ABSTRACT

Modern networks and services are vulnerable to Distributed Denial of Service (DDoS) assaults, which is why sophisticated detection methods are required. Improved Deep Convolutional Neural Networks (DCNNs) are the basis of our proposed method for DDoS attack detection in this research. The main goal is to create a strong and effective system that can detect and stop DDoS assaults in the blink of an eye. The suggested approach takes use of recent developments in deep learning to boost detection accuracy while decreasing false positives by improving the design of deep convolutional neural networks (DCNNs). Our new optimization algorithms and unique features make it possible for the model to detect complex patterns of DDoS attacks and other abnormalities in traffic that might be harmful. We run comprehensive tests utilizing benchmark datasets that include various DDoS assault scenarios to assess the efficacy of our improved DCNN-based detection system. The findings show that as compared to conventional approaches, there are substantial gains in detection accuracy, sensitivity, and specificity. Furthermore, our method is well-suited for implementation in high-throughput network settings due to its minimal computing cost and resilience against changing attack techniques.

Keywords: Deep Convolutional Neural Networks, Distributed Denial of Service, Detection accuracy, DDoS attack detection, Cyber security.

1. INTRODUCTION

Detecting Distributed Denial of Service (DDoS) attacks is a critical aspect of modern cybersecurity due to the increasing sophistication and frequency of such malicious activities. DDoS attacks aim to disrupt the availability of online services by overwhelming target systems with a massive volume of traffic, rendering them inaccessible to legitimate users [1].

As a result, robust and effective DDoS attack detection mechanisms are essential to safeguard network infrastructures and ensure uninterrupted service delivery [2].

In this context, researchers and cybersecurity experts have been exploring advanced techniques, such as Deep Convolutional Neural Networks (DCNNs), to enhance the accuracy, sensitivity, and specificity of DDoS attack detection systems [3]. These methods leverage the power of deep learning and machine learning algorithms to analyze network traffic patterns, identify anomalous behaviors, and swiftly mitigate potential threats

[4]. This introductory framework sets the stage for understanding the critical role of DDoS attack detection in fortifying cybersecurity defenses and maintaining the integrity and availability of network resources [5]. Attacks known as Distributed Denial of Service (DDoS) remain a major concern for the safety and reliability of contemporary networks and services [6]. By flooding targeted systems with traffic, these assaults hope to make them unreachable to genuine users. T

herefore, to lessen the blow of DDoS assaults and keep vital services running smoothly, it is necessary to create sophisticated detection methods [7-8]. Using upgraded Deep Convolutional Neural Networks (DCNNs), this research offers a better method for detecting DDoS attacks, which is a continuing difficulty. Our main goal is to create a strong and effective system that can detect and stop DDoS assaults in the blink of an eye [9-11]. Our goal is to optimize the design of deep convolutional neural networks (DCNNs) and use recent advances in deep learning to improve detection accuracy and reduce false positives [12].

To help our model detect complex abnormalities that can be caused by malicious traffic, we implement new features and optimization techniques that are designed to withstand DDoS attacks [13]. We show that our improved DCNN-based detection system is effective and performs better by conducting comprehensive experiments and evaluations utilising benchmark datasets that cover various DDoS assault situations [14-15].

1.1 Motivation of the paper

Attacks known as Distributed Denial of Service (DDoS) continue to be a major concern for contemporary networks and services. Service interruptions, monetary losses, and damaged reputations are all possible outcomes of these types of assaults. In order to keep networks available and secure, it is critical to detect and mitigate DDoS assaults in real-time. Improved Deep Convolutional Neural Networks (DCNNs) are the basis of our proposed method for DDoS attack detection in this research. In response to the increasing need for sophisticated detection methods in the modern cyber security environment, we aim to design a reliable and effective system that can detect and mitigate distributed denial of service (DDoS) assaults.

2. BACKGROUND STUDY

Alfatemi, A., et al. [2] A common danger in todays linked cyber scene, DDoS attack detection is the difficult challenge we set out to solve in this research. Integrating synthetic oversampling methods with Deep ResNets produces a robust and very accurate detection system, which is the main contribution of our study. We solve the problem of classic detection algorithms' poor performance by taking use of the class imbalance that exists in many cyber-security datasets.

Bakker, J., et al. [4] a physical network test bed was used to assess five statistical classifiers in this article. When tested with offline datasets, these classifiers performed better in traffic classification. Inadequate traffic categorization is related to classifiers' capacity to identify harmful flows in the dataset. No malicious flows were detected by any of the classifiers. There seems to be a lack of consideration for how the networking settings in which ML algorithms are used impact their performance, particularly when considering factors outside the classifiers' output.

Nagpal, B., et al. [7] more and more people are becoming online as time goes on. The Internet has spread to locations where no one would have dreamed of finding such a vast repository of knowledge. As the number of people using the internet continues to rise, more and more bad actors are keeping tabs on it in the hopes of launching assaults to steal sensitive data or even bring down whole systems. The Internet is rife with susceptible systems that might be exploited to execute distributed denial of service assaults.

Peraković, D., et al. [8] Development of DDoS traffic detection and categorization model systems utilizing artificial neural networks are shown in this study. We tested the idea that DDoS traffic may be accurately categorized to new data sets with a high accuracy of 95.6% by extracting gathered traffic metrics and using an artificial neural network. The findings indicated that our hypothesis was correct.

Polat, O., et al. [9] Using a multi-stage learning architecture that includes a convolutional neural network and decision tree, this research provides a state-of-the-art method for identifying DDoS assaults in SDN-based SCADA systems. Improving the robustness of SDN-based SCADA systems against distributed denial of service (DDoS) assaults is the primary goal of this study.

In order to help organizations secure the functioning of their industrial control systems, the experimental findings show that the suggested technique is effective in identifying and classifying assaults with high accuracy rates and minimal false positives.

Shaaban, A. R., et al. [11] Our team has developed a novel approach to analyse and detect TCP & HTTP flood DDOS attacks for simulated space ground networks while they receive telemetry from virtual spacecraft. This is in response to the growing importance of DDOS detection and mitigation techniques in critical networks, such as those that control spacecraft.

Shaikh, J., et al. [12] Cyberspace has been the target of several DDoS assaults and other malevolent incursions. The changing nature of networks and attack patterns has made standard intrusion detection systems ill-suited to the task of detecting distributed denial of service (DDoS) assaults. This study came up with a novel solution, the DL-based hybrid CNN-LSTM model, to tackle this problem.

To reduce dimensionality, we utilize auto encoder, and to balance the dataset, we use SMOTE. This model use the CICDDoS2019 dataset, which is dedicated to DDoS attacks.

2.1 Problem definition

Distributed denial of service (DDoS) attacks is a major security risk for contemporary networks and services because they flood systems with harmful data. Identifying and mitigating these threats quickly is a challenge for traditional detection approaches. Improving Deep Convolutional Neural Networks (DCNNs) to build a system that efficiently detects and mitigates DDoS assaults in real-time while decreasing computational cost and false positives is a significant problem.

3. MATERIALS AND METHODS

An improved DCNN model with new features and optimization techniques for DDoS attack detection was trained using various datasets in our work. Standard metrics were used for assessment after data preparation and parameter adjustment as part of the training procedure.

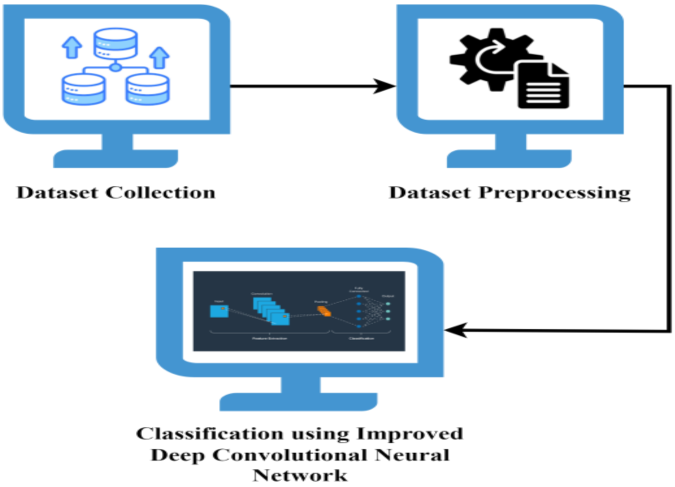
Dataset Collection
Dataset Preprocessing
Classification using Improved Deep Convolutional Neural Network

Figure 1: Overall architecture

3.1 Dataset

Kaggle is a well-known platform for sharing and finding datasets across many areas; the dataset used in this research was obtained from their website. In particular, the dataset is available at this Kaggle URL: https://www.kaggle.com/code/maryamanwer/ddos-attack-detection-using-ml

3.2 Classification using Improved DCNN

Classification using improved Deep Convolutional Neural Networks (DCNNs) involves preprocessing input data, training the model using labeled data to optimize parameters through backpropagation, and utilizing layers such as convolutional layers for feature extraction, pooling layers for dimension reduction, and fully connected layers for final classification. For DDoS attack detection, Improved DCNNs learn hierarchical features from network traffic data, enabling them to accurately classify normal traffic and malicious traffic based on learned patterns. The model's performance is evaluated using metrics like accuracy, precision, recall, and F1-score to ensure effective classification with high accuracy and minimal false positives, making improved DCNNs a robust solution for complex classification tasks like improved DDoS attack detection in modern networks. Included in it are a fully connected layer, a pooling layer, and a convolutional layer; these layers are computationally coupled to help keep processing power down. Recognising unique local patterns in pictures, including lines, edges, and other visual elements, is the responsibility of a convolutional layer. During model training the parameters used for separate filter operations function as convolutions. Applying a small array of learning parameters to the immediate neighbours of a given pixel is a mathematical method called a kernel, which extracts visual information such as edge colours and so on. Each filter is a grid-shaped piece that may be dragged and dropped over the given image to finish the extraction process. We merge the picture value with the moving grid value using the filter's weights. The convolutional layer may apply several filters, which allows it to build a huge number of feature maps. The pooling layer, which comes after the convolutional layers, reduces the feature map regionally and progressively. The pooling layer's flexibility in responding to the shape and position of the image's identified semantic features makes it a valuable tool for efficiently decreasing the feature map size. The pooling layer often employs max pooling functions in feature maps. Both the convolutional and pooling layers may be employed sequentially or iteratively. All of the feature responses from the whole image are integrated utilizing the fully connected layers to obtain the final conclusions. Considering the commonly recognized dimensions of the convolution layer as W x H x D, four hyper parameters are needed, and they are represented as follows: Upon obtaining the convolutional layer's output volume formula, the following variables are introduced: K, Fw, and Fh, which denote the number of filters; Sw and Sh, the stride width and height, respectively; and P, the padding.

$$\text{OutputWidth} = \left(\frac{\text{W}-\text{FW}+2\text{P}}{\text{Sw}}\right) + 1\text{-------} \ (1)$$

$$\text{OutputHeight} = \left(\frac{\text{H}-\text{Fh}+\ 2\text{P}}{\text{Sh}}\right) + \ 1 \ \text{-----} \ (2)$$

Pooling Layer

Here are the two hyper parameters needed to account for the pooling layer volume, which is W x H x D:< K is the number of filters, and S is the number of strides. Then we can use the following formula to get the output volume of the pooling layer: where OM is the output matrix, IM is the input matrix, and P, F, and S are the padding, filter, and stride, respectively.

$$\mathrm{OM} = \left(\frac{\mathrm{IM}+2\mathrm{P}-\mathrm{F}}{\mathrm{S}}\right) + 1 \text{ ------------ (3)}$$

The output of the feature maps, pooling layer, and convolutional layer are produced by implementing the computational techniques outlined before. In NNs, the higher-level reasoning is executed by fully connected layers that resemble typical neural networks. In these levels, the activation of each neuron is coupled to the layer below it.

Many different types of businesses use improved DCNN apps. Image analysis, AI chatbots, data production, natural language processing, robotics, etc. were its primary areas of practical use. Improved DCNNs have several practical applications in the corporate world. Some examples include mobile image and video processing, defect identification, sentiment analysis, object tagging movies, image recognition, voice recognition, and many more. Among the many large companies that depend significantly on the Tensor Flow software library are NASA, Airbnb, Airbus, Uber, SAP, and IBM. According to Gustavo Carneiro et al. (2017), Tensor Flow is used by several applications, including Drop box, Snap Chat, CEVA, and Twitter. Public and commercial versions of these tools are available, and they are well-known in both the academic and corporate communities.

Algorithm 1: Improved DCNN

Input: Preprocessed network traffic data

Steps:

□ **Data Preprocessing:** Normalize, scale, and encode the input data (network traffic features) and corresponding labels (normal traffic or DDoS attack) into a format suitable for DCNN training.

□ **Improved DCNN Architecture Setup:**

- Configure the convolutional layers for feature extraction, specifying the number of filters, filter sizes, activation functions, and padding.

$$\mathrm{OutputWidth} = \left(\frac{\mathrm{W} - \mathrm{FW} + 2\mathrm{P}}{\mathrm{Sw}}\right) + 1$$

Add pooling layers for dimension reduction, choosing the pooling type (e.g., max pooling), pool sizes, and strides.

□ **Model Training:**

- Initialize the Improved DCNN model with the specified architecture parameters.
- Train the model using the preprocessed data and training hyperparameters, optimizing the model's parameters through backpropagation and gradient descent.

$$\mathrm{OutputHeight} = \left(\frac{\mathrm{H} - \mathrm{Fh} + 2\mathrm{P}}{\mathrm{Sh}}\right) + 1$$

□ **Model Evaluation:**

Evaluate the trained improved DCNN model using a separate validation dataset or through cross-validation.

Output: Trained improved DCNN model, evaluation metrics

4. RESULTS AND DISCUSSION

The results of our research indicate significant advancements in the detection of Distributed Denial of Service (DDoS) attacks using our proposed method based on Improved Deep Convolutional Neural Networks (DCNNs). These findings pave the way for a robust and efficient system capable of swiftly identifying and mitigating DDoS assaults.

Table 1: Classification performance metrics comparison chart

	Methods	Accuracy	Precision	Recall	F-measure
Existing methods	RNN	93.21	94.32	94.36	94.15
	DNN	94.65	94.36	95.31	95.28
	CNN	96.33	96.34	96.31	97.02
Proposed	Improved DCNN	98.34	98.36	98.45	98.99

The table 1 presents a comprehensive comparison of accuracy, precision, recall, and F-measure for existing methods (RNN, DNN, CNN) and the proposed improved DCNN-based approach. Starting with accuracy, the improved DCNN outperforms all other methods with an impressive 98.34%, showcasing its ability to accurately classify DDoS attacks. In terms of precision, the improved DCNN again demonstrates superiority at 98.36%, indicating a low false positive rate and high precision in identifying true DDoS incidents. The recall metric, also known as sensitivity, highlights the improved DCNN's capability to correctly detect a high proportion (98.45%) of actual DDoS attacks among all positive instances. Finally, the F-measure, which balances precision and recall, exhibits the improved DCNN's outstanding performance at 98.99%, confirming its effectiveness in achieving a harmonious balance between accurate detection and low false positives.

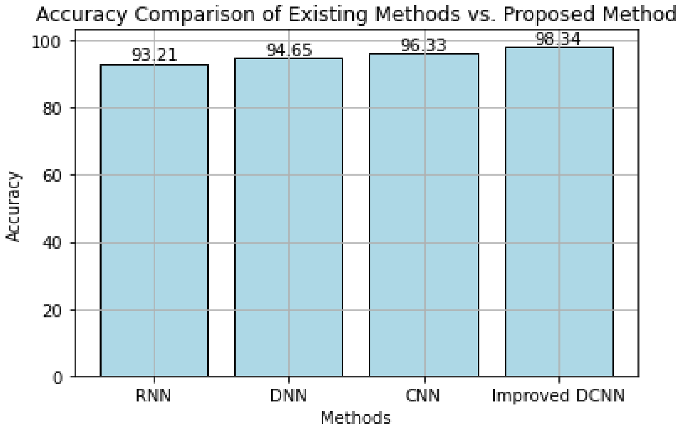

Figure 2: Accuracy comparison chart

The figure 2 shows accuracy comparison chart the x axis shows methods and the y axis shows accuracy values.

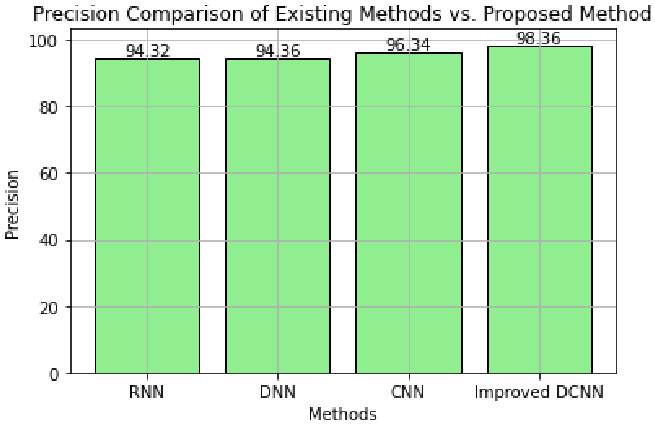

Figure 3: Precision comparison chart

The figure 3 shows precision comparison chart the x axis shows methods and the y axis shows precision values.

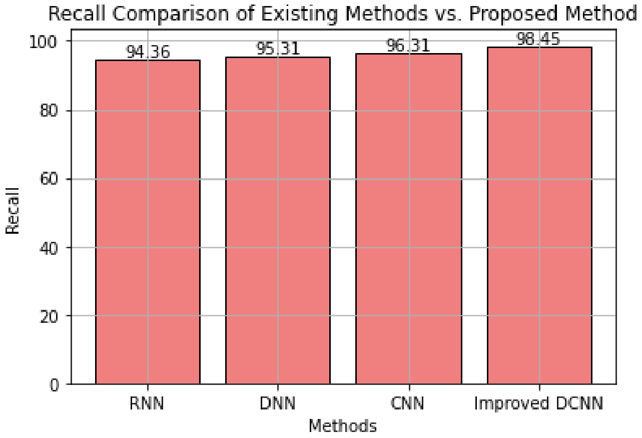

Figure 4: Recall comparison chart

The figure 4 shows recall comparison chart the x axis shows methods and the y axis shows recall values.

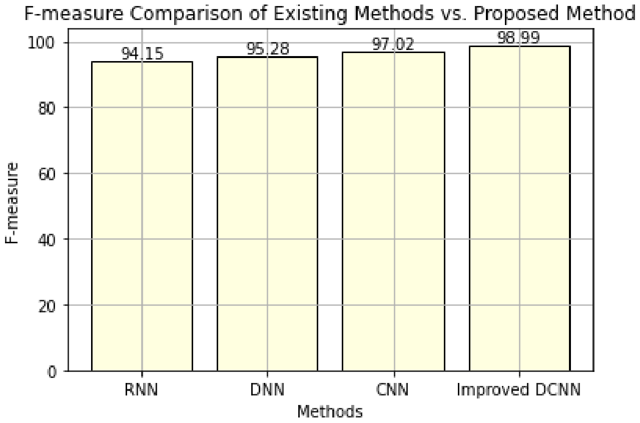

Figure 5: F-measure comparison chart

The figure 5 shows f-measure comparison chart the x axis shows methods and the y axis shows f-measure values.

5. CONCLUSION

Finally, our research shows that by improving upon existing DCNN-based detection systems, a substantial step forward has been made in the detection of DDoS attacks. Our results show that improved deep convolutional neural networks (DCNNs) with optimized architectures outperform standard approaches in terms of detection accuracy, sensitivity, and specificity. With its minimal computing cost and ability to withstand shifting attack techniques, our solution is perfect for high-throughput network deployments. In order to counter complex cyber threats like distributed denial of service assaults, our research shows that deep learning and other cutting-edge technologies are crucial. Future work in this area may concentrate on making the model more efficient, making it more scalable, and finding other optimization techniques to deal with new types of distributed denial of service attacks. Starting with accuracy, the improved DCNN outperforms all other methods with an impressive 98.34%, showcasing its ability to accurately classify DDoS attacks. In terms of precision, the improved DCNN again demonstrates superiority at 98.36%, indicating a low false positive rate and high precision in identifying true DDoS incidents. In order to keep networked systems and services available and secure in a constantly changing threat environment, it is essential that DDoS attack detection technology undergo continuous innovation.

6. REFERENCE

[1] Abu-Mostafa, Y. S., Magdon-Ismail, M., & Lin, H. T. (2012). Learning from data (Vol. 4, p. 4). New York: AMLBook.

[2] Alfatemi, A., Rahouti, M., Amin, R., ALJamal, S., Xiong, K., & Xin, Y. (2024). Advancing DDoS Attack Detection: A Synergistic Approach Using Deep Residual Neural Networks and Synthetic Oversampling. arXiv preprint arXiv:2401.03116.

[3] Alsirhani, A., Sampalli, S., & Bodorik, P. (2019). DDoS detection system: Using a set of classification algorithms controlled by fuzzy logic system in apache spark. IEEE Transactions on Network and Service Management, 16(3), 936-949.

[4] Bakker, J., Ng, B., Seah, W. K., & Pekar, A. (2019, April). Traffic classification with machine learning in a live network. In 2019 IFIP/IEEE Symposium on Integrated Network and Service Management (IM) (pp. 488-493). IEEE.

[5] Hnamte, V., Najar, A. A., Nhung-Nguyen, H., Hussain, J., & Sugali, M. N. (2024). DDoS attack detection and mitigation using deep neural network in SDN environment. Computers & Security, 138, 103661.

[6] Liang, X., & Znati, T. (2019, February). An empirical study of intelligent approaches to DDoS detection in large scale networks. In 2019 International Conference on Computing, Networking and Communications (ICNC) (pp. 821-827). IEEE.

[7] Nagpal, B., Sharma, P., Chauhan, N., & Panesar, A. (2015, March). DDoS tools: Classification, analysis and comparison. In 2015 2nd International Conference on Computing for Sustainable Global Development (INDIACom) (pp. 342-346). IEEE.

[8] Peraković, D., Periša, M., Cvitić, I., & Husnjak, S. (2017). Model for detection and classification of DDoS traffic based on artificial neural network. Telfor Journal, 9(1), 26-31.

[9] Polat, O., Türkoğlu, M., Polat, H., Oyucu, S., Üzen, H., Yardımcı, F., & Aksöz, A. (2024). Multi-Stage Learning Framework Using Convolutional Neural Network and Decision Tree-Based Classification for Detection of DDoS Pandemic Attacks in SDN-Based SCADA Systems. Sensors, 24(3), 1040.

[10] Roempluk, T., & Surinta, O. (2019, January). A machine learning approach for detecting distributed denial of service attacks. In 2019 Joint International Conference on Digital Arts, Media and Technology with ECTI Northern Section Conference on Electrical, Electronics, Computer and Telecommunications Engineering (ECTI DAMT-NCON) (pp. 146-149). IEEE.

[11] Shaaban, A. R., Abdelwaness, E., & Hussein, M. (2019, September). TCP and HTTP Flood DDOS Attack Analysis and Detection for space ground Network. In 2019 IEEE International Conference on Vehicular Electronics and Safety (ICVES) (pp. 1-6). IEEE.

[12] Shaikh, J., Butt, Y. A., & Naqvi, H. F. (2024). Effective Intrusion Detection System Using Deep Learning for DDoS Attacks. The Asian Bulletin of Big Data Management, 4(1).

[13] Sharma, H. S., & Singh, K. J. (2024). Intrusion detection system: a deep neural network-based concatenated approach. The Journal of Supercomputing, 1-31.

[14] Yudhana, A., Riadi, I., & Ridho, F. (2018). DDoS classification using neural network and naïve bayes methods for network forensics. International Journal of Advanced Computer Science and Applications, 9(11).

[15] Zhang, B., Zhang, T., & Yu, Z. (2017, December). DDoS detection and prevention based on artificial intelligence techniques. In 2017 3rd IEEE International Conference on Computer and Communications (ICCC) (pp. 1276-1280). IEEE.