Journal of Information & Optimization Sciences
ISSN 0252-2667 (Print), ISSN 2169-0103 (Online)
Vol. 45 (2024), No. 8, pp. 2071–2079
DOI : 10.47974/JIOS-1651

Managerial perspectives : Utilizing MLP-CNN for predicting and classifying DDoS attacks

S. V. Devika *
Department of Electronics and Communication Engineering
Hyderabad Institute of Technology and Management
Hyderabad 501401
Telangana
India

Bhuvan Unhelkar †
Muma College of Business
University of South Florida
N. Tamiami Trail Sarasota
Florida 8350
USA

S. Siva Shankar §
Department of Electronics and Communication Engineering
KG Reddy College of Engineering and Technology
Hyderabad 500075
Telangana
India

Prasun Chakrabarti ‡
Department of Electronics and Communication Engineering
Sir Padampat Singhania University
Udaipur 313601
Rajasthan
India

* *E-mail:* **drdevikasv@gmail.com (Corresponding Author)**
† *E-mail:* **bunhelkar@usf.edu**
§ *E-mail:* **drsivashankars@gmail.com**
‡ *E-mail:* **drprasun.cse@gmail.com**

S. Arvind [@]
Department of Computer Science and Engineering
Hyderabad Institute of Technology and Management
Hyderabad 501401
Telangana
India

Abstract

In today's interconnected internet landscape, monitoring for misuse by malicious users is crucial. DDoS attacks are a highly prevalent malicious technique; it is a transaction that attempts to flood a server's normal traffic, network, or services. The last few years have witnessed a decrease in network availability with higher detection rates and complexity. Recently, ML-based detection methods have emerged as one of the most prominent approaches. This paper introduces a Multilayer Perceptron and Convolutional Neural Network (MLP-CNN) for classifying and predicting DDoS attacks. By injecting various DDoS attacks into regular data, an extensive dataset is compiled. The proposed model combines CNN with MLP, and its performance is assessed using a confusion matrix. Experimental results demonstrate the model's efficiency with 97% accuracy, 96% precision, and 96.5% recall. The detection time for 41 attributes is 2 seconds, and for 9 attributes, it is 0.2 seconds.

Subject Classification: *68T01, 68T07.*

Keywords: *Machine learning, MLP-CNN, DDoS attack detection, Normal data, Managerial aspects.*

1. Introduction

In Q1 2018, DDoS attacks reached staggering proportions, with over 1 trillion bytes of traffic used to target GitHub, highlighting the challenge of analyzing such large volumes using traditional methods like Wireshark [1]. This underscores the need for distributed frameworks for quick traffic filtering and analysis [2].

DDoS attacks exploit protocol flaws to disrupt authorized users' access to services, targeting protocols like DNS, HTTP, and TCP [3][4]. Spam-based attacks affect SMS and email systems, while botnet-based attacks, such as Sogou-Bot and Zeus-Bot, use command and control servers to launch timed assaults, causing significant network damage.

DDoS attacks pose a major risk to advanced computer networks, aiming to incapacitate resources for intended users [5]. They overwhelm targets, often using IP spoofing to flood them with requests, rendering them inaccessible even to legitimate users [6]. Signature-based intrusion

[@] *E-mail:* **scarvi@rediffmail.com**

detection methods struggle with raw network traffic traces lacking attack labels, necessitating more expensive and less effective detection approaches.

The complexity of DDoS attack strategies poses challenges for fast and accurate detection, highlighting the importance of extracting key characteristics from network traffic to differentiate attack behaviours from normal activity. Machine learning offers supervised and unsupervised methods for this task, with supervised learning involving an initial learning phase using labelled data to classify typical and unusual situations, such as DDoS attacks, while unsupervised learning groups data as it arrives, examining clustered data to identify irregular situations like DDoS attacks.

2. Related works

For SDN setups, some frameworks and methods have been put out to improve DDoS attack detection and prevention capabilities. Varghese and colleagues proposed the D3 framework. Praseed et al., [7] uses DPDK in SDN to enable intelligent data layer management and enhance the efficiency of IDS against DDoS attacks. L. Zhou et al. [8] introduce Entropy rate measurement (ERM), surpassing existing techniques in DDoS detection accuracy. Xu et al. [9] present a modular K-means++ and Fast K-Nearest Neighbors DDoS detection solution, demonstrating improved detection precision in SDN environments. Yin et al. [10] outline an SD-IoT architecture with a cosine similarity-based DDoS detection method, ensuring IoT security amidst diverse devices. Kalkan et al. [11] evaluate JESS for SDN defence against DDoS attacks, highlighting its statistical efficacy. Lima et al. [12] Propose a statistically motivated methodology for DDoS protection validated through experiments. Deepa et al. [13] provide a mixed machine learning model for controller defense to increase the precision of DDoS attack detection. Assis et al. [14] have introduced HWDS with Game theory that combines anomaly detection and GT-based decision-making capability for autonomous SDN defence against DoS/DDoS attacks. Sahi et al. [15] have proposed CS_DDoS for the public cloud DDoS TCP flood attack prevention, which results in LS-SVM classification with very high accuracy. Francois et al. [16] introduce FireCol, an architecture for DDoS attack prevention with minimal overhead and effective protection. Chen et al. [17] propose a distributed method for traffic-flow-level DDoS flooding attack detection, demonstrating high accuracy and scalability in ISP core networks [18-21].

3. MLP-CNN-based classification and prediction of DDOS attacks

As shown in Figure 1 The MLP-CNN-based DDoS Attack Classification and Prediction involves gathering data from DDoS attack tools like Trinoo, Stacheldraht, TFN, and TFN2K, simulating various attack styles. The dataset includes DDoS attack and regular traffic data with 41 properties derived from raw network traffic, categorized into traffic, content, and intrinsic attributes. Preprocessing steps involve cleaning and transforming raw data, including normalization and standardization, to improve quality [22-24]. Feature selection techniques are used to identify crucial features, with the top nine attributes chosen using information gain-based selection out of 41. With the application of layers of CNN and MLP, an MLP-CNN classification approach is proposed to classify the training and test split dataset. The precision and recall of models in relation to the confusion matrix will be checked [25][26].

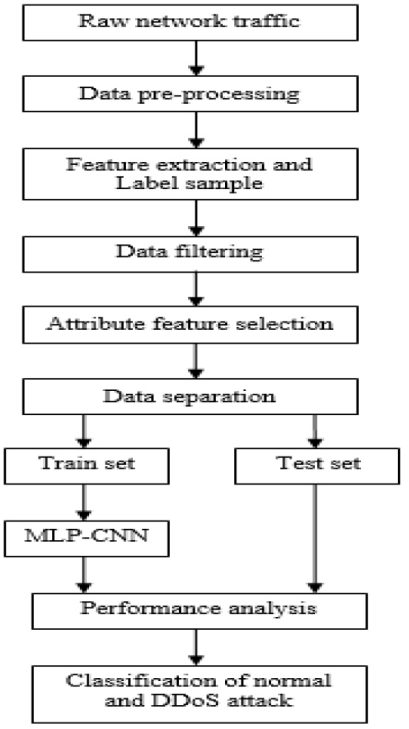

Figure 1

Workflow of MLP-CNN Based Classification And Prediction

$$E_n = \sum_{a=1}^{m} \sum_{b=1}^{m} -\ln\ln|(V(a,b))| \times V(a,b) \quad (1)$$

4. Results and discussion

The TELECOM Institute collected a dataset for analyzing and detecting DDoS attacks, containing both attack data and regular network traffic. This dataset includes network connections between source and target IP addresses, represented by TCP packets with predetermined start and stop times. 25% of the dataset was set aside for testing and 75% for training. Model performance was evaluated using a confusion matrix, comparing actual and predicted labels to assess precision.

1) True Negative (TN) – quantity of regular flows that are appropriately categorized.
2) True Positive (TP) – number of accurately identified attack streams.
3) False Positive (FP) - the amount of regular flows that are misclassified as attacks.
4) False Negative (FN) - amount of attack streams that are mislabeled as typical.

Measures like accuracy, recall, and precision are used to assess the performance of the work that is presented.

Accuracy:

$$Accuracy = \frac{TP+TN}{TP+TN+FN+FP} \tag{1}$$

Recall:

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

Precision:

$$Precision = \frac{TP}{TP+FP} \tag{3}$$

The MLP-CNN model's performance in DDoS attack classification is compared with KNN, MLP, RF, and CNN models in Table 1.

Figure 2 compares the precision and recall performance parameters, while Figure 3 presents the accuracy comparison analysis.

When it comes to classifying DDoS attacks, the MLP-CNN model performs better than others. As the attribute count decreases, accuracy diminishes, highlighting key attributes. Figure 4 shows the time for detection using 41 and 9 attributes.

Table 1

Analyzing comparative performance

Used Classifiers	Accuracy (%)	Precision (%)	Recall (%)
RF	89	89.5	90
KNN	85	86	84
MLP	88	86	87
CNN	90	89	88
MLP-CNN	97	96	96.5

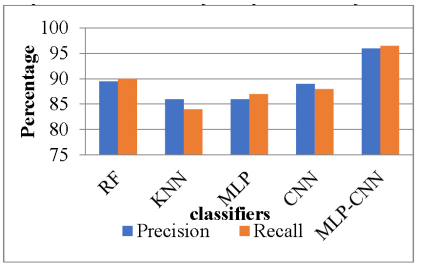

Figure 2

Comparative analysis in terms of precision and recall parameters

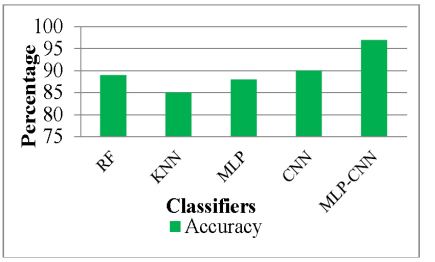

Figure 3

A comparison study concerning accuracy

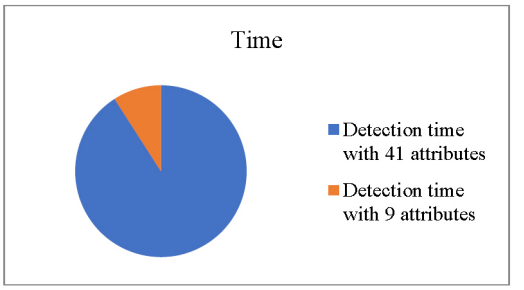

Figure 4

Time required for detection of ddos attacks

The model performs well with high accuracy, precision, and recall: 97%, 96%, and 96.5% respectively. Detection times are 2 sec with 41 attributes and 0.2 sec with 9 attributes.

5. Conclusion

This paper presents a Multilayer Perceptron and Convolutional Neural Network (MLP-CNN) model for classifying and predicting DDoS attacks as part of the TELECOM Institute's DDoS attack study and detection project. To reduce dimensionality and improve detection accuracy, feature selection is essential for managing the increasing amount of data utilized for DDoS attack detection. Nine crucial criteria were selected from a total of 41 features to quickly identify DDoS attacks. 25% of the dataset was set aside for testing and 75% for training. To evaluate the model's performance, evaluation criteria including accuracy, precision, and recall were employed. yielding impressive results: Accuracy 97%, Precision 96%, and Recall 96.5%. Notably, detection time reduced from 2 seconds with 41 attributes to 0.2 seconds with 9 attributes, highlighting the model's efficiency.

References

[1] M. Wang, Y. Lu, and J. Qin, "Source-based defense against DDoS attacks in SDN based on sFlow and SOM," *IEEE Access,* vol. 10, pp. 2097–2116 (2021).

[2] M. Tholkapiyan, S. Ramadass, J. Seetha, A. Ravuri, P. Vidyullatha, S. S. Shankar, and S. Gore, "Examining the Impacts of Climate Variability on Agricultural Phenology: A Comprehensive Approach Integrating Geoinformatics, Satellite Agrometeorology, and Artificial Intelligence," *International Journal of Intelligent Systems and Applications in Engineering,* vol. 11, no. 6s, pp. 592–598 (2023).

[3] F. Hussain, "A Two-Fold Machine Learning Approach to Prevent and Detect IoT Botnet Attacks," *IEEE Access* (2021), doi: 10.1109/ACCESS.2021.3131014.

[4] H. E. Khodke, M. Bhalerao, S. N. Gunjal, S. Nirmal, S. Gore, and B. J. Dange, "An Intelligent Approach to Empowering the Research of Biomedical Machine Learning in Medical Data Analysis using PALM," *International Journal of Intelligent Systems and Applications in Engineering* (2023).

[5] S. Thota and D. Menaka, "Importance of Machine Learning Algorithms to Detect Botnet DDoS Attacks," 2022 ICAISS, Trichy, India, doi: 10.1109/ICAISS55157.2022.10011016.

[6] S. Gore, G. S. Dhindsa, S. Gore, N. S. Jagtap, and U. Nanavare, "Recommendation of Contemporary Fashion Trends via AI-Enhanced Multimodal Search Engine and Blockchain Integration," ICESC (2023).

[7] A. Praseed and P. S. Thilagam, "DDoS attacks at the application layer: Challenges and research perspectives for safeguarding web applications," *IEEE Communications Surveys & Tutorials,* vol. 21, no. 1, pp. 661–685 (2018).

[8] M. Lopez-Martin, B. Carro, A. Sanchez-Esguevillas, and J. Lloret, "Network traffic classifier with convolutional and recurrent neural networks for Internet of Things," *IEEE Access,* vol. 5, pp. 18042–18050 (2017).

[9] Ismail, "A Machine Learning-Based Classification and Prediction Technique for DDoS Attacks," *IEEE Access* (2022), doi: 10.1109/ACCESS.2022.3152577.

[10] Aljuhani, "Machine Learning Approaches for Combating Distributed Denial of Service Attacks in Modern Networking Environments," IEEE Access.

[11] T. V. Phan and M. Park, "Efficient Distributed Denial-of-Service Attack Defense in SDN-Based Cloud," *IEEE Access*, vol. 7, pp. 18701–18714 (2019), doi: 10.1109/ACCESS.2019.2896783.

[12] K. A. Simpson, S. Rogers, and D. P. Pezaros, "Per-host DDoS mitigation by direct-control reinforcement learning," *IEEE Transactions on Network and Service Management,* vol. 17, no. 1, pp. 103–117 (2019).

[13] J. E. Varghese and B. Muniyal, "An efficient IDS framework for DDoS attacks in SDN environment," *IEEE Access*, vol. 9, pp. 69680–69699 (2021).

[14] L. Zhou, K. Sood, and Y. Xiang, "ERM: An accurate approach to detect DDoS attacks using entropy rate measurement," *IEEE Communications Letters,* vol. 23, no. 10, pp. 1700–1703 (2019).

[15] Y. Xu, H. Sun, F. Xiang, and Z. Sun, "Efficient DDoS detection based on K-FKNN in software-defined networks," *IEEE Access,* vol. 7, pp. 160536–160545 (2019).

[16] D. Yin, L. Zhang, and K. Yang, "A DDoS attack detection and mitigation with software-defined Internet of Things framework," *IEEE Access,* vol. 6, pp. 24694–24705 (2018).

[17] N. Y. Duodu and W. Patel, "Advanced EHR system in homes-in-schools' automation using internet of things and machine learning," *Journal of Information and Optimization Sciences*, vol. 43, no. 8, pp. 1953–1962 (2022).

[18] K. Kalkan, L. Altay, G. Gür, and F. Alagöz, "JESS: Joint Entropy-Based DDoS Defense Scheme in SDN," *IEEE Journal on Selected Areas in Communications* (2018), doi: 10.1109/JSAC.2018.2869997.

[19] N. A. Lima and M. P. Fernandez, "Towards an Efficient DDoS Detection Scheme for Software-Defined Networks," *IEEE Latin America Transactions* (2018), doi: 10.1109/TLA.2018.8528249.

[20] V. Deepa, K. M. Sudar, and P. Deepalakshmi, "Detection of DDoS Attack on SDN Control plane using Hybrid Machine Learning Techniques," ICSSIT, Tirunelveli, India (2018), doi: 10.1109/ICSSIT.2018.8748836.

[21] M. V. O. De Assis, A. H. Hamamoto, T. Abrão, and M. L. Proença, "A Game Theoretical Based System Using Holt-Winters and Genetic Algorithm with Fuzzy Logic for DoS/DDoS Mitigation on SDN Networks," *IEEE Access* (2017), doi: 10.1109/ACCESS.2017.2702341.

[22] A. Benhadid, "Iterative algorithms for general variational inequalities involving relaxed Lipschitz operators," *Journal of Information and Optimization Sciences*, vol. 43, no. 8, pp. 1909–1914 (2022).

[23] A. Sahi, D. Lai, Y. Li, and M. Diykh, "An Efficient DDoS TCP Flood Attack Detection and Prevention System in a Cloud Environment," *IEEE Access* (2017), doi: 10.1109/ACCESS.2017.2688460.

[24] J. François, I. Aib, and R. Boutaba, "FireCol: A Collaborative Protection Network for the Detection of Flooding DDoS Attacks," *IEEE/ACM Transactions on Networking* (2012), doi: 10.1109/TNET.2012.2194508.

[25] Y. Chen, K. Hwang, and W. S. Ku, "Collaborative Detection of DDoS Attacks over Multiple Network Domains," *IEEE Transactions on Parallel and Distributed Systems,* vol. 18, pp. 1649–1659 (2007), doi: 10.1109/TPDS.2007.1111.

[26] F. A. Abdulghani and N. A. Z. Abdullah, "Hybrid deep learning model for Arabic text classification based on mutual information," *Journal of Information and Optimization Sciences*, vol. 43, no. 8, pp. 1901–1908 (2022), doi: 10.1080/02522667.2022.2060910.

Received February, 2024