SHAREit.

Scientific Hub of Applied Research in Engineering & Information Technology

Received: 22.07.2024 Revised: 09.08.2024 Accepted:14.08.2024

check for updates

Research Article

Detection of DDoS Attacks in Networks Using CRNN

S Priya[*1], A Neela Madheswari [2], S R Saranya [3], C Suganthi [1]

[1] *Department of CSE, Muthayammal College of Engineering, Namakkal, Tamilnadu, India.*

[2] *Department of CSE, Mahendra Engineering College, Namakkal, Tamilnadu, India.*

[3] *Department of AI&DS, Muthayammal College of Engineering, Namakkal, Tamilnadu, India.*

The main objective of this paper is to detect DDoS attacks in network through Deep Learning techniques. Distributed Denial of Service (DDoS) imposes possible threats which exhaust the resources to make it unavailable for the legitimate user by violating one of the security components [1]. In the field of DDoS attacks, as in all other areas of cyber security, attackers are increasingly using sophisticated methods [2]. Various machine learning techniques could be used to address the security issues effectively and efficiently. In this paper, we present a new technique for combination of deep learning models that can be used for network traffic. We show that a Recurrent Neural Network (RNN) combined with a Convolutional Neural Network (CNN), CRNN (Convolutional Recurrent Neural Network) model provides best detection results. A complete study is presented on several architectures that integrate a CNN and an RNN, including the impact of the features chosen and the length of the network flows used for training.

Keywords: DDoS, Cyber-security, CRNN, cyber attacks, Recurrent Neural Network, Convolutional Neural Network, network traffic.

1. Introduction

A network can have both legal and illegal users (hackers). Hacker is the one who exploits and access another one's data in illegal way [3]. A Distributed Denial-of-Service (DDoS) attack is a cybercrime that attempts to disrupt a server, network, or service by flooding it with internet traffic. The goal is to overwhelm the target and make it unable to respond to legitimate requests, forcing it offline. DDoS attacks can be measured in gigabits per second (Gbps) or packets per second (PPS), and 20 to 40 Gbps can be enough to shut down most networks. Symptoms of a DDoS attack include: Slow network performance, Inability to access a website, and Unavailability of a website.

Correspondence should be addressed to
S Priya ; priyasankarnkl@gmail.com

The traditional methods alone are not enough to detect the attacks in the networks. In this paper, Machine learning (ML) techniques are used to prevent DDoS attacks by analyzing network traffic patterns, identifying anomalies, and mitigating threats in real-time. Machine Learning model is capable of learning automatically from the trained dataset without the involvement of humans.

Neural networks imitate the function of the human brain in the fields of Data science, Artificial intelligence, machine learning, and deep learning, allowing computer programs to recognize patterns and solve common issues. Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) can analyze time-series data of network traffic to detect complex patterns associated with DDoS attacks.

In this paper, the features of Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) are combined to increase the performance.

2. Related Works

Machine learning algorithms like SVM, Decision Trees, Naïve Bayes, K-means, etc., have been used to detect the DDoS attacks and traffics. Network traffic patterns have been analyzed to detect DDoS attack [5].

The CNN layer consists of input layer (convolutional, activation function, pooling, fully connected) layers and output layer as in Fig.1.

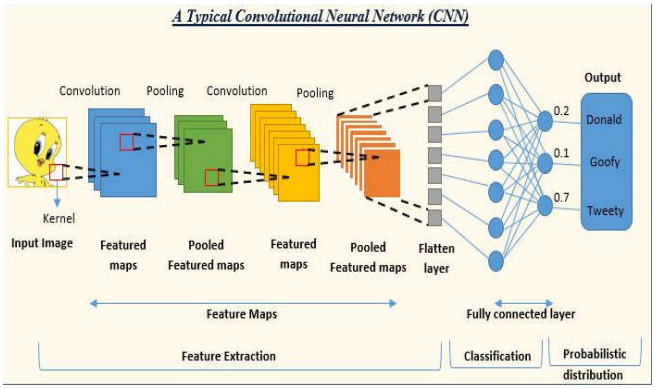

Fig.1. CNN layers

CNNs are effectively used to detect and classify the DDoS traffic into normal and threat information with an accuracy of 99% [4].

RNNs are designed to handle sequential data by maintaining a memory of previous inputs through their hidden states, making them suitable for time-series data as in Fig.2.

RNNs is used to detect the DDoS attack to improve the detection performance [7].

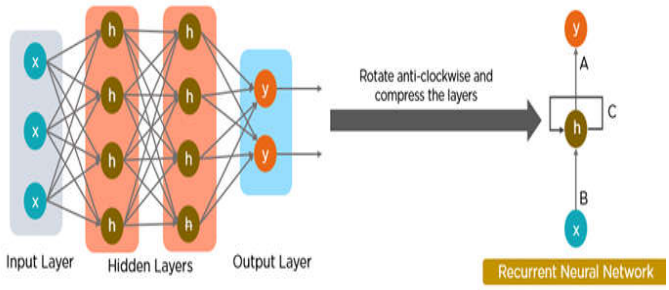

Fig.2. RNN layers

RNNs can analyze sequences of network traffic data, capturing temporal dependencies and patterns that evolve over time. By learning the normal patterns of network traffic, RNNs can detect deviations that may indicate a DDoS attack. RNNs can predict future traffic patterns and identify potential anomalies before they lead to significant disruptions.

In practice, CNNs and RNNs can leverage the strengths of both architectures.

3. System Overview

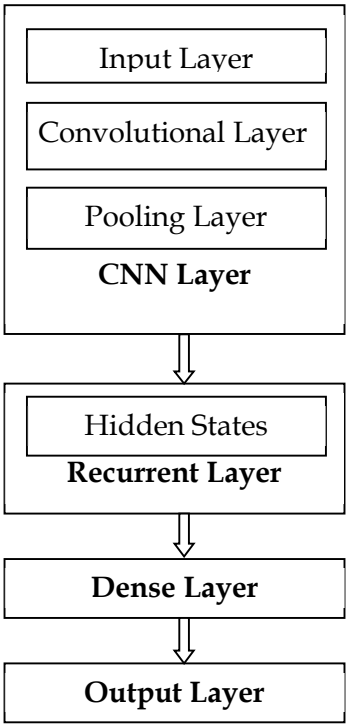

Fig.3. CRNN Architecture

3.1. Feature Extraction from Network Traffic

Convolutional layers can be used to extract spatial features from raw network traffic data. These features might include patterns in packet sizes, IP addresses, header information, or frequency of specific protocols [15]. Recurrent layers can capture temporal dependencies in network traffic. For instance, they can model the sequence of packet arrivals or the flow of requests over time. As in Fig.3.

- Input Layer: The raw network traffic data, typically represented as a time-series, is fed into the model.
- Convolutional Layers: These layers apply filters to the input data to extract local features. For network traffic, these features can represent packet-level patterns or short sequences of traffic behavior.

• Pooling Layers: These layers reduce the dimensionality of the feature maps generated by the convolutional layers, preserving the most important information while reducing computational complexity.

3.2. Behavioral Analysis

RNNs are effective at recognizing patterns in sequential data. In the context of DDoS attacks, they can identify unusual sequences of requests or anomalies in traffic patterns that may indicate an ongoing attack. By integrating CNNs and RNNs, the model can learn to detect both sudden spikes in traffic (detected by CNNs) and sustained patterns of abnormal behavior over time (detected by RNNs), which are typical indicators of DDoS attacks.

• Recurrent Layers: The output from the CNN is passed to RNN layers. These layers capture the temporal dependencies and patterns in the extracted features.

• Hidden States: RNNs maintain hidden states that remember previous inputs, enabling the model to understand the context and evolution of traffic patterns over time.

3.3. Adaptability to Varying Attack Patterns

DDoS attacks can vary widely in their nature and execution. A hybrid model can adapt to different types of attacks by learning diverse features and temporal patterns, making it more robust compared to models based solely on CNNs or RNNs.

3.4. Real-time Detection and Response

The ability of RNNs to process sequences in real-time is crucial for timely detection of DDoS attacks. Coupled with the efficiency of CNNs in extracting relevant features, the hybrid model can swiftly identify and respond to attacks as they occur.

3.5. Enhanced Accuracy and Efficiency

Integrating both architectures allows the model to achieve higher accuracy by leveraging their complementary strengths. CNNs excel at capturing spatial correlations and patterns, while RNNs are adept at capturing temporal dynamics, resulting in a more comprehensive understanding of network behavior.

3.6. Anomaly Detection

Beyond signature-based detection methods, a CNN-RNN hybrid model can detect anomalies based on deviations from learned normal patterns. This is particularly valuable for detecting novel or previously unseen attack strategies that do not match known attack signatures.

• Dense Layers: After the recurrent layers, the data is passed through fully connected (dense) layers to perform final classification.

• Output Layer: The final layer produces a probability score or a classification label indicating whether the input traffic is normal or indicative of a DDoS attack.

4. Analysis and Result

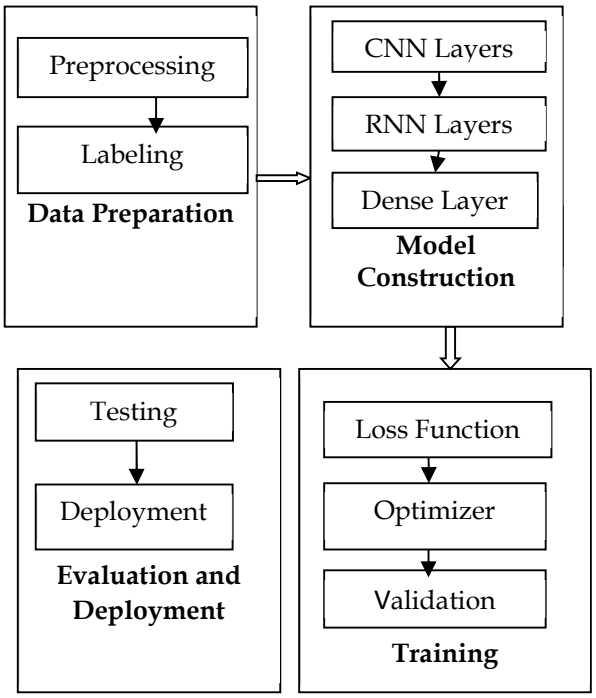

Fig.4. Implementation of CRNN

4.1. Data Preparation

Here, dataset stored in a CSV (Comma Separated Values) file is collected. This large dataset could be used utilized for different machine learning applications for instance classification of Network traffic, Network performance monitoring, Network Security Management, Network Traffic Management, network intrusion detection and anomaly detection.

This network traffic dataset consists of 6 features. Each instance contains the information of source and destination IP addresses, the majority of the properties are numeric in nature, however there are also nominal and date kinds due to the Timestamp.

Table.1 Dataset Features

Timestamp	Packet Size	Protocol	Source IP	Destination IP	Label
2024-07-09 10:00:00:00	1200	TCP	192.168.1.100	8.8.8.8	normal
2024-07-09 10:00:00:01	800	UDP	10.0.0.1	192.168.1.100	normal
2024-07-09 10:00:00:02	1500	TCP	192.168.1.100	8.8.8.8	attack
2024-07-09 10:00:00:03	700	UDP	10.0.0.2	192.168.1.100	normal

Duplicate entries are eliminated in the network traffic data. Forward Fill technique is used to fill or remove missing values

4.2. Data Transformation

To help in faster convergence during training, the dataset features are scaled to a standard range [0,1]. And the categorical data are converted into numerical format using one-hot encoding.

The network traffic data is normalized and segmented into fixed-size time windows. Labeled datasets containing both normal and malicious traffic samples are used for supervised learning.

Table.2 Prepared Data

Packet Size	Protocol TCP	Protocol UDP	Label	0	1	2	3	4	5	6
1200	1	0	normal	0.0	0.0	0.0	0.0	0.0	1.0	-1.0
800	0	1	normal	0.0	0.0	0.0	0.0	0.0	-1.0	0.0
1500	1	0	attack	0.0	0.0	0.0	0.0	0.0	1.0	-1.0
700	0	1	normal	0.0	0.0	0.0	0.0	0.0	-1.0	0.0

After normalization, the dataset is split into dataset for training and testing. 80% data is used for training and 20% data is used for testing.

4.3. Model Construction

The preprocessed data is then given to the convolutional layers to extract relevant features from each time window of traffic data (Fig.4). Further, the RNN and dense layers are added to process the sequence of extracted features, capturing temporal dependencies. The fully connected layer is incorporated to interpret the features and produce a final classification.

4.4. Training

In Convolutional Neural Networks (CNNs), the choice of a loss function plays a crucial role in training the network effectively. Cross-Entropy Loss (Log Loss) is the most common choice for classification tasks. It measures the performance of a classification model whose output is a probability value between 0 and 1.

$$\text{Cross Entropy Loss} = \frac{1}{N} \sum_{i=1}^{N} \sum_{c=1}^{C} y_{ic} \log (p_{ic})$$

where N is the number of samples, C is the number of classes, y_{ic} is 1 if sample i belongs to class c and 0 otherwise, and pic is the predicted probability that sample i belongs to class c.

For training, the dataset is given to cross-entropy for binary classification. Adam optimizer is used to minimize the loss during training. Then the dataset is segmented into training and validation sets to monitor the model's performance and avoid over-fitting.

4.5. Evaluation and Deployment

The model is evaluated on a separate test dataset to ensure its generalizability. Finally, the trained model is integrated into the network infrastructure for real-time DDoS detection.

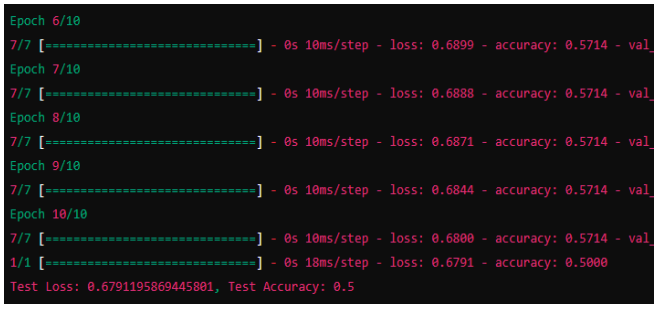

Fig.5. Model Evaluation Result

After training completes, the model is evaluated on the test data (X_test, y_test). Each epoch shows the training loss (loss) and accuracy (accuracy). val_loss and val_accuracy represent the loss and accuracy on the validation set (X_val, y_val).

Test Loss and Test Accuracy are printed based on the performance of the model on the test set. A Test Accuracy of 0.5 (or 50%) indicates that the model predicts the correct class 50% of the time on unseen test data.

5. Conclusion and Future Works

In this paper, DDoS (Distributed Denial of Service) attack is detected effectively using the CRNN architecture model. The test loss and accuracy are analyzed and evaluated based on the model's performance. From the obtained result, we found that CRNN model better detection with high accuracy.

For the future work, it is planned to add additional features for the dataset considered here. And it is planned to design an enhanced CRNN model by considering bidirectional RNN and more convolutional layers.

REFERENCE

[1] Nikhil Tripathi, Babu Mehtre, DoS and DDoS Attacks: Impact, Analysis and Countermeasures, 2013.

[2] Jai Dalvi, Vyomesh Sharma, Ruchika Shetty, Sujata Kulkarni, DDoS Attack Detection using Artificial Neural Network, IEEE 2021 International Conference on Industrial Electronics Research and Applications (ICIERA).

[3] S. S. Priya, M. Sivaram, D. Yuvaraj and A. Jayanthiladevi, "Machine Learning based DDOS Detection", 2020 International Conference on Emerging Smart Computing and Informatics (ESCI), pp. 234-237, 2020.

[4] Ahmed Ramzy Shaaban, Essam Abd-Elwanis, Mohamed Hussein, DDoS attack detection and classification via Convolutional Neural Network (CNN), IEEE 2019 Ninth International Conference on Intelligent Computing and Information Systems (ICICIS).

[5] T. Thapngam, S. Yu, W. Zhou, S. K. J. P.-t.-p. n. Makki, and applications, "Distributed Denial of Service (DDoS) detection by traffic pattern analysis," vol. 7, no. 4, pp. 346-358, 2014.

[6] R. Doshi, N. Apthorpe, and N. Feamster, "Machine learning ddos detection for consumer internet of things devices," in 2018 IEEE Security and Privacy Workshops (SPW), pp. 29-35, 2018.

[7] Omerah Yousuf, Roohie Naaz Mir, DDoS attack detection in Internet of Things using recurrent neural network, Volume 101, July 2022, 108034, Elsevier.

[8] Kazeem B. Adedeji, Adnan M. Abu Mahfouz, Anish M. Kurien, DDoS Attack and Detection Methods in Internet-Enabled Networks: Concept, Research Perspectives, and Challenges, 2023.

[9] Vinko Zlomislic, Kresimir Fertalj, Vlado Sruk Denial of service attacks: An overview, IEEE conference on Information Systems and Technologies, 2014.

[10] Vanitha K S, UMA S V, Mahidhar S K, Distributed denial of service: Attack techniques and mitigation, IEEE conference 2017.

[11] Zargar, S.T.; Joshi, J.; Tipper, D. A survey of defence mechanisms against distributed denial of service (DDoS) flooding attacks. IEEE Commun. Surv. Tutor. 2013, 15, 2046–2069.

[12] Khalaf, B.A.; Mostafa, S.A.; Mustapha, A.; Mohammed, M.A.; Abduallah, M.W. Comprehensive review of artificial intelligence and statistical approaches in distributed denial of service attack and defense methods. IEEE Access 2019, 7, 51691–51713.

[13] R. Swami, M. Dave, and V. Ranga, ‘‘DDoS attacks and defense mechanisms using machine learning techniques for SDN,’’ in Security and Privacy Issues in Sensor Networks and IoT. Hershey, PA, USA: IGI Global, 2020, pp. 193–214.

[14] Priyanka Kamboj, Munesh Chandra Trivedi, Virendra Kumar Yadav, Vikash Kumar Singh, Detection techniques of DDoS attacks: A survey, IEEE UP Section Conference on Electrical Computer and Electronics (UPCON), 2017, 675 – 679.

[15] Ahmed Adil Nafea, Mustafa Maad Hamdi, Baraa saad Abdulhakeem, Ahmed Thair Shakir, Mustafa S. Ibrahim Alsumaidaie, Ali Muwafaq Shaban, "Detection Systems for Distributed Denial-of-Service (DDoS) Attack Based on Time Series: A Review", 2024 21st International Multi-Conference on Systems, Signals & Devices (SSD), pp.43-48, 2024.