DDOS Attack Detection in Networks Using LSTM And Bi-LSTM Approach

[1]RAKSHITHA S, [2]RUKSHITHAGOWDA KB, [3]SMITHA MANJUNATH NAIK, [4]SUHANA, [5]SHAMMI L

[1,2,3,4]Student, [5]Assistant Professor
Department of Computer Science
East Point College of Engineering and Technology, Bengaluru

Abstract: **As the world is becoming increasingly digitized, the need for protective measures against the attacks becomes more and more efficient. Distributed Denial of Service (DDoS) is one of the attacks that is turned into serious threat to the Internet. The automatic detection of DDoS attack packets is one of the key defence tactics. In this paper, we propose DeepLSTMDefense and DeepBiLSTMDefense models using LSTM and Bi-LSTM approach for detecting DDoS attacks based on deep learning. Deep learning approaches enable the automatic separation of high-level features from the low-level features, producing effective representation and interface. We create a recurrent deep neural network to recognize the patterns in sequences of network traffic and monitor network assault activities. Experimental results demonstrate better performance of DeepBiLSTMDefense model compared with DeepLSTMDefense model and other conventional machine learning approaches.**

Index terms**: Deep Learning, DDoS, RNN, LSTM, Bi-LSTM, DeepLSTMDefense, DeepBiLSTMDefense**

I. INTRODUCTION

DDoS or Distributed Denial of Service, refers to an intentional attempt by a hacker to block legitimate users from accessing a server or network resource by flooding it with artificial traffic.

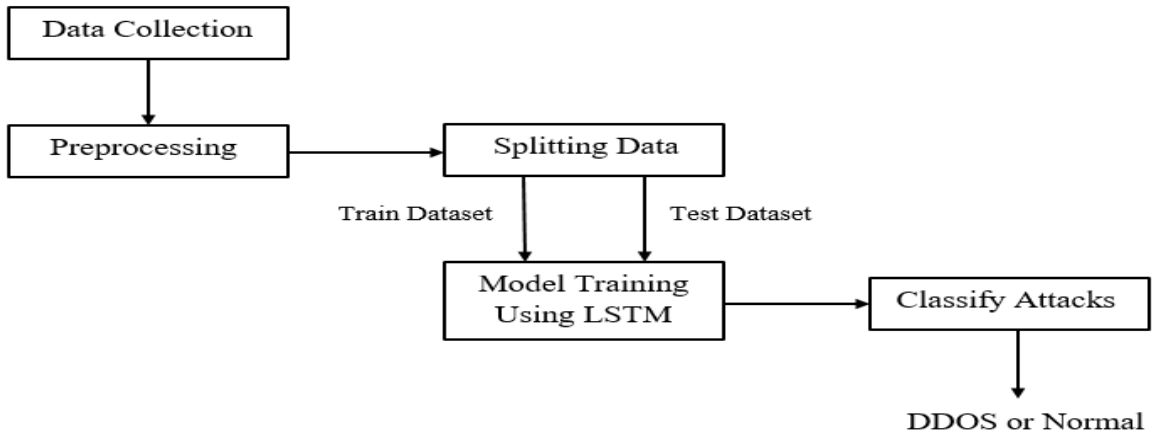
The majority of cyberattacks, including DoS and DDoS operations, are conducted by human-instructed systems (Bots or Botnets), which are made of numerous internets connected devices. One of the primary DDoS defence technique is DDoS detection [1]. However, it is challenging to automatically identify DDoS attacks because, in most instances, attack traffic is similar to legitimate traffic and attackers often attempt to imitate flash crowds. The rise in DDoS attacks makes it abundantly evident that there are still gaps in the timely detection, analysis and mitigation of DDoS attacks to ensure the availability of network services. They mainly aim to system resources and network bandwidth, ranging from Network layer to Application layer. Since the first DDoS attack occurred in 1999[2], DDoS has become a critical, widespread and rapidly evolving threat in the world. According to survey from Radware, DDoS is currently the largest threat (50% respondents in the survey) for organisations [3]. There ARE 24 DDoS attack vectors witnessed by Akamai in Q4 2015.Compared with Q4 2014, total DDoS attacks increase by 148.85% and multi vector attacks largely increase. Currently, main attack vectors include UDP flood, HTTP flood, SYN flood, ICMO, DNS etc. pose serious threats to both system and networks [6]

We propose a new detection and family classification approach-based onset of network flow features, we suggest a fresh method for detection and family classification. Finally, we list the most crucial feature sets for identifying various DDoS attack types along with their respective weights. According to the experimental findings, using deep learning models instead of shallow machine learning techniques on a small dataset reduced errors by 39.69%. We can even lower the error rate from 7.517% to 2.103% in a huge dataset. This demonstrates its capacity to learn from previous network packets.

II. SYSTEM ARCHITECTURE

1. DeepLSTMDefense Model

The figure 2.1 represents the architecture of DeepLSTMDefense model that makes use of LSTM deep learning approach. The model begins with data collection using CICDDoS2019 dataset, which is followed by preprocessing. Preprocessing is the removal of irrelevant data, labelling data etc. followed by the use of common scalar approach to produce preprocessed data. Split the data into



train and test sets. Now load the train dataset into model using LSTM for training. Once trained, the model can distinguish between normal and DDoS attacks.

2. DeepBiLSTMDefense Model

The figure 2.2 represents the architecture of DeepBiLSTMDefense model that makes use of Bi-LSTM deep learning approach. The model begins with data collection using CICDDoS2019 dataset, which is followed by preprocessing. Preprocessing is the removal of irrelevant data, labelling data etc. followed by the use of common scalar approach to produce preprocessed data. Split the data into train and teat sets. Now load the train dataset into model using Bi-LSTM for training. Once trained, the model can distinguish between normal and DDoS attacks.

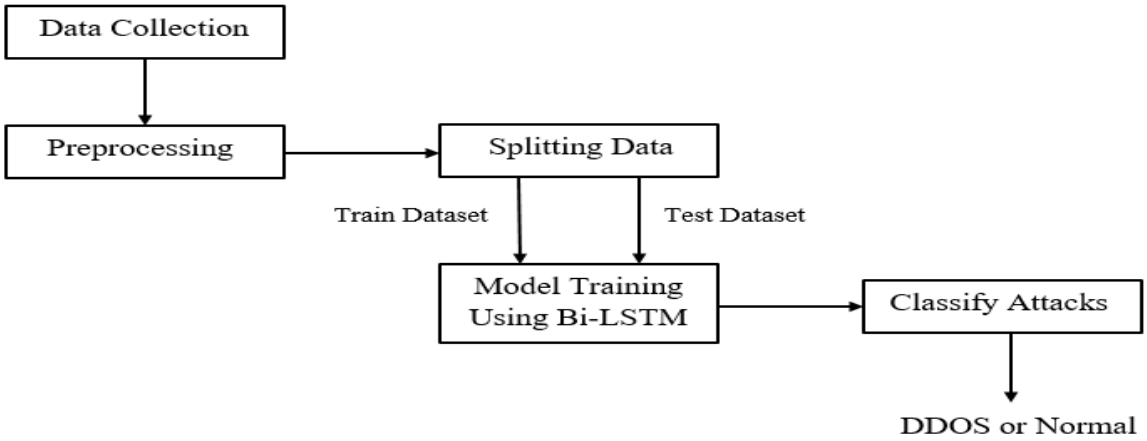


Figure 2.2: Architecture of DeepBiLSTMDefense

III. IMPLEMENTATION

1. LSTM

The abbreviation of LSTM is Long Short Term Memory. A form of recurrent neural network, LSTM is more memory efficient than conventional recurrent neural networks. The important information is saved and all irrelevant information is deleted in every single cell. Short term memory is a problem for conventional neural networks. By retrieving the crucial information and identifying patterns, LSRMs efficiently increase performance.

```
# for LSTM
# Plot training & validation accuracy values
plt.plot(history.history['accuracy'])
plt.plot(history.history['val_accuracy'])
plt.title('LSTM Model Accuracy')
plt.ylabel('Accuracy')
plt.xlabel('Epoch')
plt.legend(['Train', 'Test'], loc='lower right')
plt.savefig('LSTM Model Accuracy.png')
plt.show()

# Plot training & validation loss values
plt.plot(history.history['loss'])
plt.plot(history.history['val_loss'])
plt.title('LSTM Model Loss')
plt.ylabel('Loss')
plt.xlabel('Epoch')
plt.legend(['Train', 'Test'], loc='upper left')
plt.savefig('LSTM Model Loss.png')
plt.show()
```

Figure 3.1: Plotting of Training and Validation of Accuracy Values for LSTM

2. Bi-LSTM

The abbreviation of Bi-LSTM is Bidirectional Long Short-Term Memory. The practice of enabling any neural network to have the sequence information in both the directions backward and forward is known as Bi-LSTM. A Bidirectional LSTM differs from a conventional LSTM in input flows in two directions.

```
# For Bi-LSTM
# Plot training & validation accuracy values
plt.plot(history.history['accuracy'])
plt.plot(history.history['val_accuracy'])
plt.title('Bi-LSTM Model Accuracy')
plt.ylabel('Accuracy')
plt.xlabel('Epoch')
plt.legend(['Train', 'Test'], loc='lower right')
plt.savefig('Bi-LSTM Model Accuracy.png')
plt.show()

# Plot training & validation loss values
plt.plot(history.history['loss'])
plt.plot(history.history['val_loss'])
plt.title('Bi-LSTM Model Loss')
plt.ylabel('Loss')
plt.xlabel('Epoch')
plt.legend(['Train', 'Test'], loc='upper left')
plt.savefig('Bi-LSTM Model Loss.png')
plt.show()
```

Figure 3.2: Plotting of Training and Validation of Accuracy Values for Bi-LSTM

III. METHODOLOGY

We used two deep learning algorithms, namely LSTM and Bi-LSTM, to develop a DeepLSTMDefense and DeepBiLSTMDefense models. Using CICDDoS2019 dataset, we propose a new detection and family classification approach based on a set of network flow features. The most important feature sets to detect different types of DDoS attack with their corresponding weights are considered.

1. Data Collection: CICDDoS2019 contains benign and the most up-to-date common DDoS attack, which resembles the true real-world data (PCAPs). It also includes the results of the network traffic analysis with labelled flow based on the time stamp, source and destination IPs, source and estimation ports, protocols and attack (CSV files). Using CICDDoS2019 dataset, we propose a new detection and family classification approach based on a set of network flow features. The most important feature sets to detect different types of DDoS attack with their corresponding weights are considered.

2. Preprocessing of dataset: In this step the IP traffic data as input and outputs cleaned data. Data preprocessing is considered to be a critical task in machine learning as it may significantly improve the efficiency and effectiveness of the training process. It includes some essential tasks such as removal of irrelevant data, handling missing values, label conversion, categorification, and data normalization. Here the datasets has more than 50 features with more CSV files, we need to apply data cleaning technique, and take [TIME STAMP] [SOURCE IP] [DESTINATION IP] [SOURCE PORT] [DESTINATION PORT] as major features, rest features we need to be removed.

3. Working of Train Model: Model Built with each group connection in the data set, there are 49 characteristics that describe it, and there are 10 different results in the assault category. As a result, the output layer is layer 10 and the input layer node number is 49. Softmax is chosen by the output layer's classifier, Adam is chosen by the optimisation function, and "binary_crossentropy" is chosen by the loss objective function. To get the best parameters, choose the training subset for training. The learning rate, hidden layers, time steps, size of each batch, and number of epochs are the parameters that must be chosen. Using "grid _search" in the sklearn library to iterate through a grid search algorithm to experiment with different parameter combinations, determine the optimal parameters as follows:

- The sequence model of Keras was user
- To initialize the API function Sequential ().
- Adding two hidden Bi-directional LSTM layers, set the input dimension to 49 and the number of each hidden layer node was 128.
- In order to prevent the outfit in the training, the Dropout was set to 0.4.
- The Dense layer is added as the output layer, the number of nodes is 10.

4. Classification of Attacks: We develop the models utilizing LSTM and Bi-LSTM that can identify and categorize packets as either normal or DDoS attack.

IV. RESULTS

In this study, DDoS attack on networks are detected using the DeepLSTMDefense and DeepBiLSTMDefense models that have been proposed. Here we also compare the two models performance. Both models are tested and trained using the CICDDoS2019 dataset. The performance of the models has been evaluated using the confusion matrix, accuracy, and loss. And it can be seen in the graphs below. LSTM classifier has barely been outperformed by BiLSTM. DeepBiLSTMDefense model outperforms DeepLSTMDefense and the other machine learning models with an accuracy rate of 97%.

LSTM

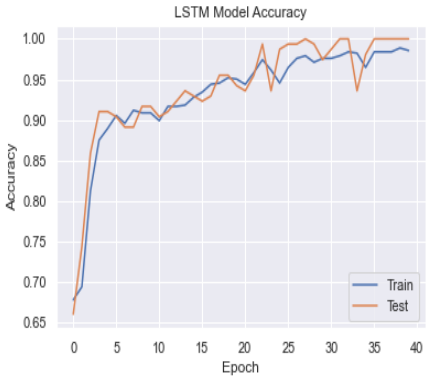


Figure 4.1.1
Test and Train Accuracy

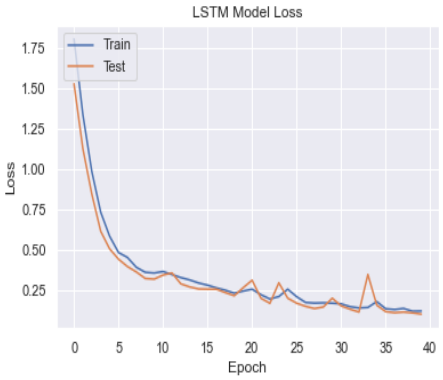


Figure 4.1.2
Test and Train Loss

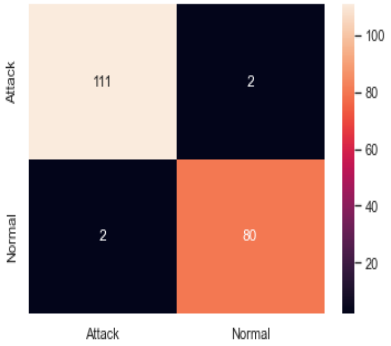


Figure 4.1.3
Confusion Matrix

Bi-LSTM

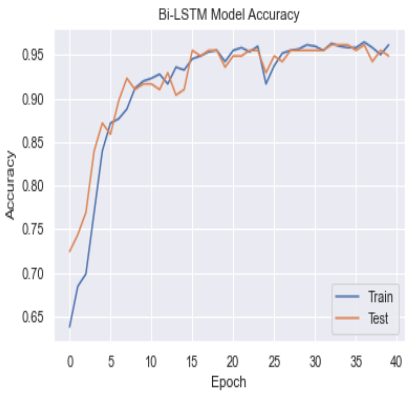


Figure 4.2.1
Test and Train Accuracy

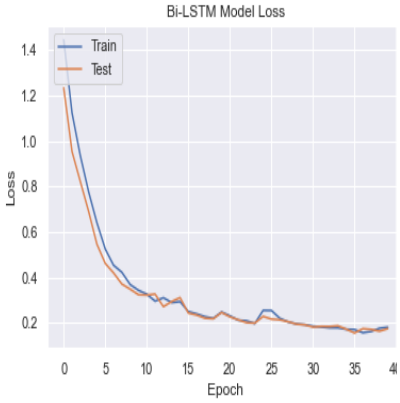


Figure 4.2.2
Test and Train Loss

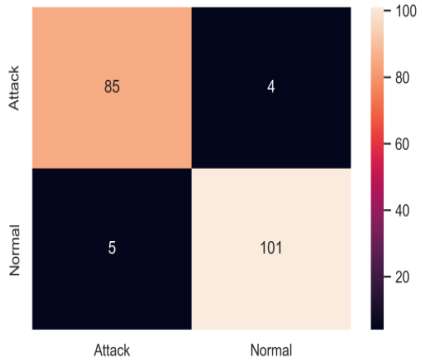


Figure 4.2.3
Confusion Matrix

V.CONCLUSION

The paper proposes a DDoS detection approaches called DeepLSTMDefense and DeepBiLSTMDefense, which formulates DDoS detection as a sequence classification problem and uses RNN (LSTM, BiLSTM) and fully connected layers. The experimental findings show that models reduces error rate compared to conventional machine learning approaches.

For future work, we plan to increase the diversity of DDoS vectors and system settings to test our model's robustness in different environments. The comparison will also include other shallow machine learning models.

REFERENCES:

1. V. D. Gligor, "A note on denial-of-service in operating systems," IEEE Transactions on Software Engineering, vol. 10, no. 3, pp. 320–324, 1984.
2. P. J. Criscuolo, "Distributed denial of service: Trin00, tribe flood network, tribe flood network 2000, and stacheldraht ciac-2319," DTIC Document, Tech. Rep., 2000.
3. Global application & network security report 2015-2016," Tech. Rep, 2016.
4. Introduction to Machine Learning with Python: A Guide for Data Scientists (Greyscale Indian Edition) Paperback – 1 January 2016 by Andreas Muller.
5. https://www.manning.com/books/deep-learning-with-python".
6. "Kaspersky DDoS intelligence report for q4 2015," Tech. Rep., 2016.