# DDoS Attack Detection Using LSTM

## 1. Introduction

Distributed Denial of Service (DDoS) attacks have emerged as a significant threat actor in the recent past and deals with the aspect of availability and performance in cyberspace. These attacks refer to cases where attackers saturate a network, service or host, thus denying these services to legitimate users. Various and serious, including but not limited to, financial losses due to downtime, loss of customer trust and probable simple negative effects such as damage to reputation. Especially nowadays, in today's world, people and organizations depend on uninterrupted using and accessing online services, real-time detection and prevention of such attacks is crucial. Static and rule based or threshold-based detection methods commonly used in DDoS fails to extend its capability to adapt gradually changing features of DDoS attack flow leading to high false positive and false negative rates.

To this end, this project seeks to tackle these challenges by using the artificial intelligence in improving detection of DDoS threats. More specifically, it examines Long Short-Term Memory (LSTM) networks which are a sub-genre of Recurrent Neural Networks (RNN) that have been developed to address the long-term memory problem present in sequential data. LSTMs are highly effective in discovering patterns within time-stamped data and therefore in the identification of network traffic characteristic of DDoS attacks. This project applies LSTM models in a real-life scenario by emulating normal and DDoS traffic on a server together with traffic monitoring using appendages of Wireshark and Tcpdump. The utilization of AI techniques serves not only to enhance the reliability of threats' identification but also provide swift detection of potentially dangerous situations which greatly encouraged the protection of online services from DDoS attacks.

## 2. Literature Review

Experimental findings and innovations in DDoS attack detection based on deep learning frameworks demonstrate the expanding role of sophisticated AI systems in cyberspace protection. The paper proposed by the authors is entitled "A Hybrid Deep Learning Approach for Real-Time DDoS Detection in IoT Networks" published in IEEE 2023; The proposal describes a CNN-RNN model that utilizes both spatial and temporal data to identify the real-time attack characteristics. Considering the nature of the analyzed network traffic, where the temporal aspect plays a significant role in identifying the potential anomalies, this paper shows that the recurrent models like RNN can be a proper choice for traffic analysis.

A similar study conducted in the IEEE journal of 2023 is on "Deep Learning Based Intrusion Detection System for Internet of Things" where the author has also compared the CNN, RNN and LSTM algorithm among which there is more focus on the LSTM for learning the long-term dependencies in the traffic records. The studies show that LSTM outperforms CNN and RNN architectures for intrusion detection, including DDoS because of the LSTM's ability to learn sequential patterns over long periods and more extended time horizons, which is crucial to our project of DDoS identification in network traffic.

Lastly, "An Improved LSTM Model for DDoS Detection in Edge Computing Environments" (Wiley, 2022) offers an LSTM based model that is developed specifically to operate with minimal latency in edge computing systems, and with minimal resource demands. The presented study demonstrates how the indicated model works effectively in scenarios based on the principles of edge computing, where there are limited resources and, therefore, both high detection rates and minimal use of performance time are required. This is in line with our projects objective of producing a model that is adaptive in real time, for DDoS detection, that is fair in its utilization of Systems resources.

New methods in deep learning for DDoS detection show that the application of AI can greatly changes the prospects of network security threats. Recent research including the research conducted in IEEE in 2023 on the Hybrid of CNN-RNN for smart IoT devices reveal superior detection effectiveness but the research is constrained by efficiency for real time systems. Also, due to the capability of LSTM networks for capturing long-term dependencies in the traffic, the model has been suggested in another IEEE paper as being appropriate for traffic analysis. However, its application to real traffic is yet to be investigated further. Enhanced LSTM architectures for edge computing as described in a Wiley paper provide both performance and energy efficiency and majorly analyzed using emulation. These results, therefore, vindicate the use of LSTM for this job while calling for real-time application and functional testing a want that is missing from current trends.

## 3. Proposed Method

As for the proposed method for real-time DDoS detection, this paper elaborates on the preprocess of the dataset, training of the model, and analyzing of real-time traffic. Using herramienta Long Short-Termed Memory (LSTM), the system analyses network traffic and determines a pattern based on the sequential dependence. It comprises of developing a publicly accessible DDoS dataset, training the lstm model, emulating network traffic through a dummy server and real time traffic capture. That way, the detection of attacks is effective with low latency, allowing for the quick protection of the network against DDoS attacks in a changing environment.

The proposed method incorporates the following steps:

Step 1: Dataset Preparation and Preprocessing

For training and testing of LSTM model, a DDoS dataset available in public domain is retrieved. Hence, the most important features in packet, source IP address, destination

IP address, protocol type, and timestamp are extracted, and then the data is normalized to match the LSTM model and increase the training speed.

Step 2: Model Training and Evaluation

The used LSTM model is developed to predict patterns within sequential traffic data using its Long-Term Memory characteristics. The collected dataset is then divided into train and test sets Then the model is trained through one epoch Gayle. When it comes to measuring up the productivity of a model, then the following is employed Accuracy, Precision, Recall and the F1-score.

Step 3: Server simulation and traffic capture

An actual server is involved; a dummy server is created with a static IP in order to produce normal and attack traffic. Wireshark and tcpdump are two well-known open-source application often used to sniff on networks, and save the captured packets in a format know as pcap. The traffic is made of genuine concurrent HTTP requests and DDoS synthetic traffic generated by tools like HULK.

Step 4: Real-Time Data Integration

Specific captured PCAP files are parsed into acceptable format, CSV in order to harvest various features for predictions. It is used as a trained LSTM model alongside the process of capturing live traffic to be able to predict the malicious activity in real-time.

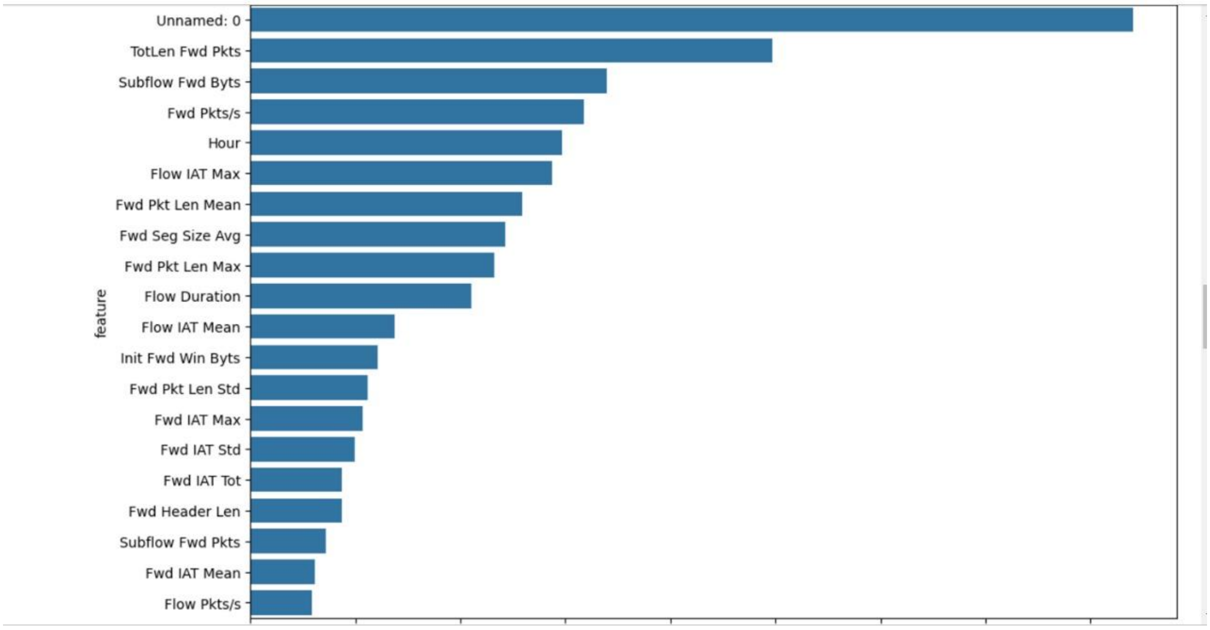
Step 5: Prediction and Mitigation

The LSTM model aims at involuted processing on the input and distinguish it either as a normal or malicious traffic. Foreign attacks are quickly marked to be blocked evidently showing prevention. Runtime startup time, system latency and error handling are observed for real-time analysis for practical use in active DDoS attack recognition.

## 4. **Implementation**

Dataset Preparation and Preprocessing

The first strategy of implementation involved selecting a raw dataset that consisted of samples of many and different network traffics, including the normal and malicious traffics. It was this dataset that was used in training as well as in as assessing the performance of the LSTM model. In order to prepare the raw data for use in the deep learning framework, some preprocessing was required. The basic data set is converted from unstructured format and important parameters of characteristics of network traffic were selected and abstracted. These features included; Packet Size, which provides the size of each packet; Source/Destination IPs which enhances identification of the traffic source and destination; Protocol Type: TCP/ UDP/ others; and Timestamp: time when each packet occurred. Normalization was also used on the features to help to adjust the values to the same level that makes sense for the training stage. This preprocessing stage filtering and normalizing the data to remove noise and make the dataset usable by the LSTM model in pattern recognition.



Random Forest for Feature Selection

Model Training and Evaluation

Due to the dependencies in the network traffic data, an LSTM network was used and trained on the preprocessed data set to detect temporal patterns. The training phase took 50 iterations, throughout which the mode's weights were modified in order to decrease prediction errors. The LSTM architectural design enabled the use of memory cell and hence useful in handling sequential data for network traffic anomaly detection. The model was then tested and had a 96% accuracy, therefore affording it considerable robustness. Metrics including precision, recall, F1-score and latency were used in performance assessment to give a general understanding of the performance of the algorithm. These figures confirmed the general capability of the model in a task of general separation of normal and malicious traffic with slight inaccuracies in the form of false positives and false negatives. The training accuracy plot displayed rising patterns; consequently, learning was achieved. The developed model was further evaluated for its performance on unseen data which were used to establish its applicability and effectiveness in real life use.

Sample Extracted Features

| Feature | Description |
|---|---|
| Packet Size | Size of the network packet |
| Source IP | IP address of the sender |
| Destination IP | IP address of the receiver |
| Timestamp | Time of packet capture |

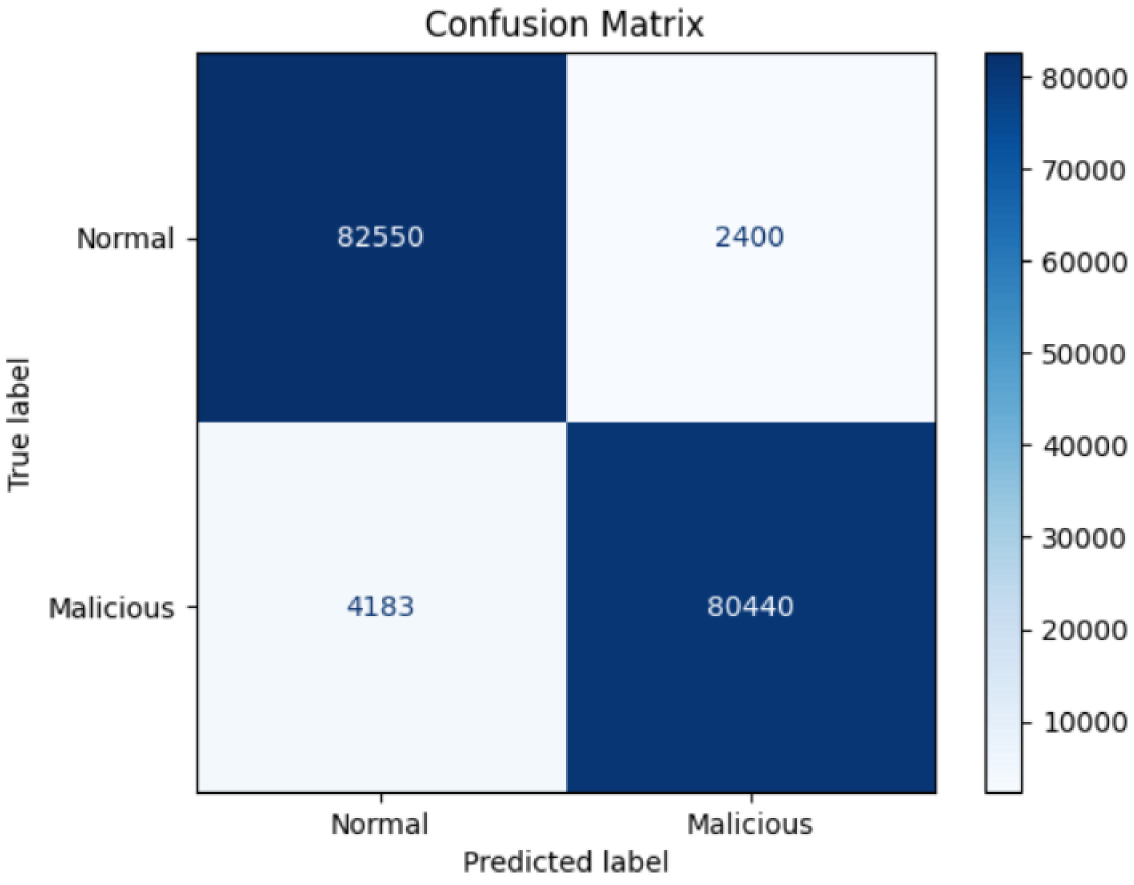
This detailed approach to implementation emphasizes the importance of structured data preprocessing and iterative model training, ensuring high performance in detecting DDoS attacks.

## 5. Results

The implementation's outcomes illustrate how well the LSTM model detects and classifies network activity as either malicious or genuine. To ensure the model's suitability for real-time situations, its efficiency was assessed using many significant measures, such as accuracy, precision, recall, and latency. In addition, the trained model's ability to handle a variety of dynamic network situations was confirmed by integrating it with live data from the simulated server. These results indicate the model has the potential to be an efficient DDoS detection solution.

The LSTM model effectively classified traffic with the following performance metrics:

- Accuracy: 0.96
- Precision: 0.97
- Recall: 0.95
- F1-Score: 0.96



Confusion Matrix for Traffic Classification

Real-time prediction was validated by integrating the model with live traffic from the simulated server. Both normal and attack traffic were accurately classified.

## 6. Discussion

Compared with other models, there is a strong expectation for the high effectiveness of the proposed LSTM-based framework for DDoS attacks detection using real-time data with high accuracy and good adaptability. The step-by-step approach of the entire task ranging from data acquisition and feature extraction to the model identification of traffic abnormalities were well enhanced by the structured methodology. Packet size, protocol types, and, more importantly, timestamps were the important inputs upon which LSTM could be trained and employed for temporal analyses of the network traffic. The framework's adaptability to various situations, such as normal operation and attack, shows the feasibility of the proposed approach for deployment in actual environments. But this scalability aspect poses a considerable issue; the behaviour of the framework in large and diverse datasets and under higher traffic circumstances still needs extensive investigation.

Future improvements will be focused on the presence of such issues as computational complexity and delays that are crucial for furthering processing of such data in real-time setting of edge and IoT. This can be resolved through other techniques like model pruning, quantization, or going for a small architecture takes less power without much of a hit in performance. Furthermore, associated multi-model ensembles with LSTM using the CNN architecture or attention-based mechanisms will also add to the model's robustness and detection systems. Such enhancements will help to make the framework more responsive and more appropriate for various types of cybersecurity applications for which quick detection is critical.

## 7. Conclusion

To this end, this project demonstrated how LSTM networks can be effectively deployed to build a DDoS detection framework capable of processing and classifying real network traffic. The structured approach—comprising dataset preprocessing, feature engineering, model training, and real-time integration—validated the system's ability to detect emerging patterns of malicious traffic. Simulating realistic network conditions with normal and DDoS traffic further confirmed the framework's applicability in addressing real-world cybersecurity challenges. Leveraging the sequential data processing capabilities of LSTM networks, the system accurately identified temporal patterns in network activity, achieving high detection rates for DDoS attacks.

The proposed method offers a practical and scalable solution for controlling DDoS threats, particularly in IoT and edge computing environments where real-time detection is essential. Nonetheless, opportunities for improvement remain, especially in enhancing scalability and optimizing resource usage for large-scale networks with diverse attack vectors. Future efforts will focus on increasing the system's ability to handle higher traffic volumes, reducing computational demands, and expanding its applicability to detect a wider range of attack types. These advancements will further bolster cybersecurity measures, ensuring the reliability and availability of online services.

## 8. Reference

1. Sumathi, S., Rajesh, R. and Lim, S., 2022. Recurrent and deep learning neural network models for DDoS attack detection. Journal of Sensors, 2022(1), p.8530312.

2. "Real-Time DDoS Attack Detection using Sketch-based Entropy Estimation on the NetFPGA SUME Platform," 2020 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC), Auckland, New Zealand, 2020, pp. 1566-1570.

3. Sathish, D. and Kavitha, A., 2024, July. DDoS Attack Detection Using Optimized Long Short-Term Memory Based on Improved Bacterial Foraging Optimization. In *2024 2nd International Conference on Sustainable Computing and Smart Systems (ICSCSS)* (pp. 568-573). IEEE.

4. Xinlong, L. and Zhibin, C., 2022. [Retracted] DDoS Attack Detection by Hybrid Deep Learning Methodologies. *Security and Communication Networks*, *2022*(1), p.7866096.

submitted by

Sidharth K – 231040