Suresh Gyan Vihar University Journal of Engineering & Technology
(An International Bi-Annual Journal)
Volume 8, Issue 1, 2022 , pp.6-9
ISSN: 2395-0196

DDoS Attack and Its Detection By LSTM Module

Madhav J.Salunkhe[1], O.S Lamba[2]

[1]Research Scholar, Suresh Gyan Vihar University, Jaipur

[2]Professor, Suresh Gyan Vihar University, Jaipur

Abstract: DDoS is a distributed denial of service attacks. A distributed denial of service is a malevolent attempt to disturb the ongoing traffic of a server or network by overwhelming the target with huge internet traffic. The DDoS attack will send multiple requests to the attacked web resource with the aim of exceeding the website's capacity to handle multiple request and prevent the website from functioning correctly. Distributed denial-of-service attacks target websites and online services. The aim is to overwhelm them with more traffic than the server or network can accommodate. The goal is to render the website or service inoperable**.**

Keywords: LSTM model, Feature extraction, Network traffic, Time window

I. Introduction

The Internet of things (IoT) bargains a mix of various sensors and items that can work together with one another with no human obstruction essential. The "things" in the IoT includes objects, for example, autos, microwaves, coolers, toaster, cools and so on, which gather valuable information from its surroundings with the assistance of sensors and transmit this to the next associated gadgets that take activities/choices dependent on it. As it were, it very well may be said that IoT is a design that includes brilliant installed gadgets that are associated with web so they can be controlled and activated by web. It is normal that by the 2020, around 25 billion articles will turn into the piece of worldwide IoT arrange [9], which will present new difficulties in verifying IoT frameworks. It will turn out to be obvious objective for programmers as these frameworks are frequently conveyed in uncontrolled and antagonistic condition. The principle security challenges in IoT condition are approval, protection, validation, confirmation control, framework adaptation, stockpiling, and organization [2]. There are security arrangements accessible as of now for Internet, which ought to be similarly pertinent to IoT organizes too. In any case, compelled assets, distinctive operational condition, and complex interconnectivity among tremendous number of gadgets in IoT make those security arrangements deficient.

II. Proposed Work

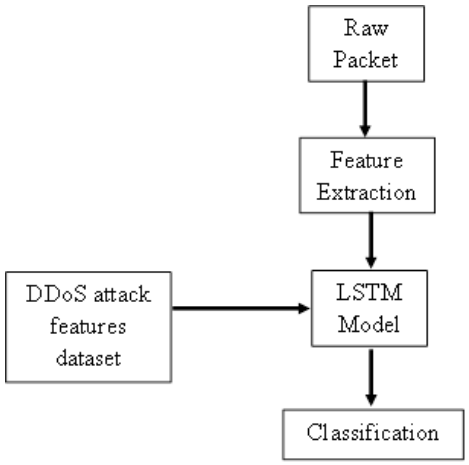
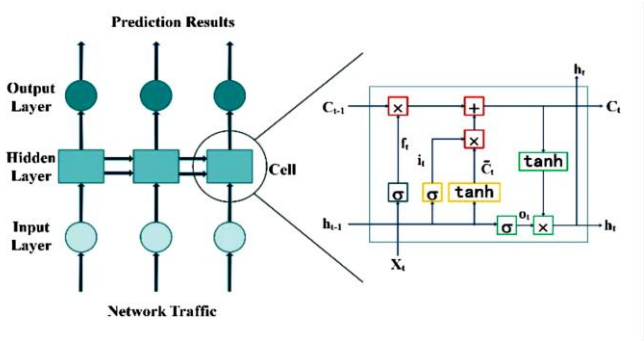


Figure 1: System work flow

Preprocessing:

We extract 10 features from the traffic, including source IP address, destination IP address, source port, destination port, protocol type, timestamp, duration, type of service, length and time to live. Because of the wide range of IP addresses, we use Bag of Word (BoW) [24] and feature hashing to convert IP address to a real vector. And for packets without port number information, such as ICMP packets, we set their port number to 0. After feature processing, we get a m x n data matrix, and a m x 1 label matrix, where m indicates the number of packets and n indicates the number of transformed features. The label value of 0 represents normal traffic, the label value of 1 represents attack traffic. Since the LSTM module requires the input of a three-dimensional matrix (batch_size, time_step, input_dimension), we convert the two-dimensional matrix into a three-dimensional matrix $(m - T + 1) \times T \times n$.Where, T is the time window, representing the state of a packet associated with the previous $(T - 1)$ packets. Figure 2 illustrates the process of feature extraction, transformation, and reorganization. X is data matrix, Y is label matrix.

LSTM Module:



We leverage the LSTM method to gain a prediction of DDoS. In this module, we enter the three-dimensional matrix into the input layer. After the operation of the hidden layer, the output layer outputs the prediction results. LSTM takes the form of a repeating cell chain. The cell contains four types of interactive neural networks that interact in a special way to enable the network to remember historical information. LSTM protects and controls the state of cells through input gate, output gate and forget gate. Figure 3 depicts the architecture for LSTM. The right of the figure is a LSTM cell. The blue is forget gate, the yellow is input gate, the green is output gate, and the red means cell state renewal.

In the LSTM module, we use two hidden layers of 256 neurons, a full connection layer of 256 neurons, which activation function is ReLU, and a full connection layer of 1 neuron which activation function is Sigmoid. The values of all parameters are the optimal values that we have chosen after many comparative experiments. The module uses the Sigmoid function to represent the prediction results of the last packet in the window: A value smaller than 0.5 is considered normal traffic, and a value bigger than 0.5 is considered attack traffic. However, we found that the prediction value closer to 0.5, the prediction accuracy lower. So, for the data with poor reliability of the prediction result, we use Bayes method for the second discrimination to improve the accuracy. For other data, if it is determined to

be attack traffic, we intercept it and send a warning to the service provider; otherwise, we forward it normally.

The intrusion detection evaluation dataset (ISCX2012) [23] is used for training LSTM module. This dataset is a benchmark intrusion detection dataset includes seven days of network activity. The data is selected of the fourth day, including 9,648,635 packets. It also provides label files. We set labels on the packets by comparing the fields of the packets in the '.pcap' file with the fields of the packets in the label file. Since most of them are normal traffic, we randomly select 120,000 normal packets and 120,000 attack packets to eliminate data Skewness. The training set includes 108,000 normal packets and 108,000 attack packets, and the test set includes 12,000 normal packets and 12,000 attack packets. In each experiment we resample to eliminate errors.

Feature Extraction:
MFCC Features

The first stage of speech recognition or event or command detection is to compress a speech signal into streams of acoustic feature vectors, referred to as speech feature vectors. The extracted vectors are assumed to have sufficient information and to be compact enough for efficient recognition[5].The concept of feature extraction is actually divided into two parts: first is transforming the speech signal into feature vectors; secondly is to choose the useful features which are insensitive to changes of environmental conditions and speech variation[6].However, changes of environmental conditions and speech variations are crucial in speech recognition systems where accuracy has degraded massively in the case of their existence. As examples of changes of environmental condition: changes in the transmission channel, changes in properties of the microphone, cocktail effects, and the background noise, etc. Some examples of speech variations include accent differences, and male-female vocal tract difference. For developing robust speech recognition, speech features are required to be insensitive to those changes and variations. The most commonly used speech feature is definitely the Mel Frequency Cepstral Coefficients (MFCC)features, which is the most popular, and robust due to its accurate estimate of the speech parameters and efficient computational model of speech[7].Moreover, MFCC feature vectors are usually a 39dimensional vector, composing of 13 standard features, and their first and second derivatives.

Performance Evaluation:

Time Window	Accuracy
5	**91.2%**
10	**92.5%**
20	**93.20%**
40	**95%**
70	**96.6%**
100	**96.8%**

.

III. Conclusion

This paper focuses on DDoS attacks on different IoT devices with considering features dataset and detection of attacks by using LSTM module.

References:

[1]. R. Das, A. Gadre, S. Zhang, S. Kumar and J. M. F. Moura, "A Deep Learning Approach to IoT Authentication," *2018* IEEE International Conference on Communications (ICC), Kansas City, MO, 2018, pp. 1-6.doi: 10.1109/ICC.2018.8422832

[2]. H. Jafari, O. Omotere, D. Adesina, H. Wu and L. Qian, "IoT Devices Fingerprinting Using Deep Learning," MILCOM 2018 - 2018 IEEE Military Communications Conference (MILCOM), Los Angeles, CA, USA, 2018, pp. 1-9. doi: 10.1109/MILCOM.2018.8599826

[3]. C. H. Liu, Q. Lin and S. Wen, "Blockchain-enabled Data Collection and Sharing for Industrial IoT with Deep Reinforcement Learning," in IEEE Transactions on Industrial Informatics. doi: 10.1109/TII.2018.2890203

[4]. A. Abeshu and N. Chilamkurti, "Deep Learning: The Frontier for Distributed Attack Detection in Fog-to-Things Computing," in IEEE Communications Magazine, vol. 56, no. 2, pp. 169-175, Feb. 2018. doi: 10.1109/MCOM.2018.1700332

[5]. Alsaidi and F. Kausar, "Security Attacks and Countermeasures on Cloud Assisted IoT Applications," 2018 IEEE International Conference on Smart Cloud (SmartCloud), New York, NY, 2018, pp. 213-217. doi: 10.1109/SmartCloud.2018.00043

[6]. M. E. Aminanto, R. Choi, H. C. Tanuwidjaja, P. D. Yoo and K. Kim, "Deep Abstraction and Weighted Feature Selection for Wi-Fi Impersonation Detection," in IEEE Transactions on Information Forensics and Security, vol. 13, no. 3, pp. 621-636, March 2018. doi: 10.1109/TIFS.2017.2762828

[7]. Rajendra B. Mohite and Dr. Onkar S. Lamba, “Blind Source Separation Survey”, in IJSTR vol.8, no.11, pp.340-344, Nov.2019.

[8]. Madhav J. Salunkhe and Dr. Onkar S. Lamba, “The basis of attack types, their respective proposed solutions and performance evaluation techniques survey”, in IJSTR vol.8, no.12, pp.2418-2420, DEC.2019.