IJARSCT
ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

Impact Factor: 6.252

Volume 2, Issue 3, May 2022

Developing an Efficient Feature Engineering and Machine Learning Model for Detecting IoT-Botnet Cyber Attacks

Aishwarya Tingare[1], Akshay Desainipanikar[2], Amisha Devadiga [3], Prof. Mrs. Jyoti Raghatwan[4]
Students, Department of Computer Engineering[1,2,3]
Faculty, Department of Computer Engineering[4]
RMD Sinhgad School of Engineering, Pune, Maharashtra, India

Abstract: *Computers and networks have been under threat from viruses, worms and attacks from hackers since they were first used. In 2018, the number of devices connected to the Internet exceeded the number of human beings and this increasing trend will see about 80 billion devices by 2024. Securing these devices and the data passing between them is a challenging task because the number of IBAs is also increasing sharply year by year. To address this issue, a large number of defences against network attacks have been proposed in the literature. Despite all the efforts made by researchers in the community over the last two decades, the network security problem is not completely solved. In general, defence against network attacks consists of preparation, detection and reaction phases. The core element of a good defence system is an IOT Botnet Attack (IBA) Detection System (IBA-DS), which provides proper attack detection before any reaction. An IBA-DS aims to detect IBAs before they seriously damage the network. The term IBA refers to any unauthorised attempt to access the elements of a network with the aim of making the system unreliable.*

Keywords: IOT Botnet, Attack, LSTM, Detection System

I. Introduction

The most common significant threat to online service providers is distributed denial of service (DDoS) attack. It involves the attacker's ability to compromise the availability of web services offered by the targeted host. This is achieved by using attacking agents such as botnet and or compromised Internet of Things (IoT) devices to exhaust the victims computing capacity (Network Bandwidth, System and Application resources) preventing service availability to legitimate users.

According to few authors, the main victims for DDoS attack are organizations with online presence and the effect of DDoS attack to these organizations ranges from very simple problems to significant ones such as financial losses, compromise of national security and endangerment of human life.

A research conducted by Nexusguard in 2016, revealed that the frequency of DDoS attacks occurring has increased tremendously by 83% in the second quarter of 2016 [53]. The volatile increase in DDoS attack is attributed to several factors by various researchers. According to Mansfield-Devine, the increase in DDoS attacks is due to the attackers motivational factors such as money, politics, revenge, reputation and destruction to perform other attacks. Kshirsagar et al. said that the increase in DDoS attack is a result of hackers advancing in their attacking strategies, and continuously look for new vulnerabilities to exploit. Fallah et al. [8] and Kim et al. [43], also said that the high increase in DDoS attack is due to the inefficiency of the existing detection and mitigation techniques to filter legitimate packet from attack packets, the large volume of data used from spoofed source and the type of DDoS attack used by the attacker.

The alarming growth of DDoS attack over the years has attracted several research groups attentions to investigate and propose different detection techniques and countermeasures in the three aspect of DDoS attacks. These are namely, detection of existence of DDoS attack, classification of traffic as normal traffic or DDoS traffic and lastly, the mitigation response to the attack.

Sabrina et al. used RNN Ensemble, an Artificial Intelligence (AI) approach to help detect the various behaviours of DDoS attacks; Loukas et al. used Bayesian classifiers to compare four different implementations and Recurrent Random Neural Networks (r-RNN) to fuse real-time networking statistical data to distinguish normal traffic from DDoS attack traffic. Salah

DOI: 10.48175/IJARSCT-3700

et al. adopted an approach called the multi-Agent pattern recognition mechanism to detect DDoS attacks; Kim et al. [43] used the combined approach consisting of automatic feature selection using decision tree algorithm, and classifier generation module using neural networks to detect DDoS attacks. Saied et al. also used Artificial Neural Network (ANN) algorithm to detect and mitigate DDoS attack based on specific patterns that distinguishes attack traffic from genuine traffic, etc.

However, all the above-mentioned detection techniques become obsolete with the emergent of new attacking techniques and strategies which has different features or patterns. This is because the detection algorithms or techniques depend on packet features to train and detect DDoS attacks.

The concerns shown and contributions made by the various research groups have therefore attracted the attention of both the industry and academia sector to come up with a detection technique or mechanism which will serve as the first line of defense against DDoS attacks mitigation. This is because the research groups all support the fact that online services are under attack and therefore need an effective and efficient system to help detect the presence of DDoS attack on the network infrastructure so that the right mitigation techniques are applied before its devastating effects are experienced by users.

In view of the line of discussion, this research work focuses on using a Deep learning technique called Long Short-Term Memory (LSTM) Recurrent Neural Networks (RNN) to develop and train a tensor artificial intelligence (AI) model which will detect the presence of IoT Botnet attack traffic patterns on the network, and achieve a high detection accuracy, and a low false alarm rates.

LSTM RNN was chosen as the technique for this work because among the family of RNN techniques and existing conventional machine learning techniques, LSTM RNN is rated as the best. This rating is as results of its ability to learn longer historical features during training time.

Also, unlike the other techniques, LSTM is able to resolve the vanishing gradient problems associated with vanilla RNNs with BPTT by ensuring that a constant error is maintained to allow the RNN to learn over long time steps.

Lastly, LSTM has the ability to use its gated cell state, which makes it act like computers memory to make decisions on what data is allowed to be written to it, read from it and store data on it, to keep features of attacks learned from training process and make detection decisions based on this stored information on gated cell. Also, the LSTM has been able to achieve an accuracy rate of 97.996% [55] which the older machine learning technique has not been able to achieve.

Tensor Flow was also chosen as the machine learning implementation platform because it has a flexible architecture that supports CPU, GPU, Android and iOS. This makes it easy to port trained models to any other hardware without any code changes. It is also simple to train its mathematical functions useful for neural networks.

II. Literature Survey

Loukas et al. [1] research group technique for detecting DDoS attacks was based on three main factors which are, the study of statistical features of incoming DDoS attack traffic, Bayesian classifier to assess and predict the likelihood of an attack and the use of recurrent random neural network(r-RNN) which puts together all gathered information on incoming traffic to make a detection decision. This technique operates on the victim side of the attack. Their work revealed that the performance of the technique depended on how well the r-RNN was trained with different features of different DDoS attack packets. In deriving the features for training the r-RNN, the research group used both instantaneous and statistical characteristics of the incoming traffic which gives different results for normal and DDoS traffic.

Again, Loukas et al. [2] in another research work focus on using two schemes, namely, the biologically inspired Random Neural Network (RNN) and multiple Bayesian classifiers to detect and distinguish normal traffic from DDoS attack traffic. This technique works by selecting the detection features and compute estimates for the probability density functions in the form of histogram for the features and the likelihood ratios which serve as the first-level decision for each selected features. Next they calculate their high level decision by fusing the first level decisions with the RNN. And then implement the RNN with actual values and histogram categories of the features. The strength of this approach lies in the fact that, they are able to combine the RNNs discriminating capacity and approximation properties with the incoming traffics statistical data.

Sabrina et al. [3] proposed a detection procedure which is based on the use of observation and Artificial intelligence (RNN Ensemble) to detect DDoS attack at the client and intermediate nodes. The main reason for choosing this RNN Ensemble detection approach is that, DDoS attack have different behaviors at both client and intermediate nodes, and according to [38], ensemble will be able to help detect the various states of DDoS attack. The detection at the client node will be based on the observation of two main things; the number of rejected requests by an affected node and the changes in the victims

DOI: 10.48175/IJARSCT-3700

resource (CPU, Physical Memory and NIC) usage. These two features will be fed into the RNN ensemble to predict the state of the request whether it is a good or bad request.

Salah et al. [4] used a multi-agent pattern recognition mechanism to detect DDoS attack launched against the victim server in a distributed network fashion having multiple internet gateways. It works based on the principle of distributed multi-agents, performing attack detection at the various levels. The detection is based on the parameters extracted from observed network traffic. The agents collectively and in a coordinated manner produce a pattern of network traffic behavior upon which the proposed solution depends on to perform recognition. According to author, this solution is robust and fault-tolerant because it employs the use of multiple agents to detect attacks at each node, so the breakdown of any of this node wills not affect the operation and performance of the proposed model.

Kim et al. [5], used Cisco Systems NetFlow and two different data mining technique to detect the different types of DDoS attacks. The NetFlow provided seven unique and useful features on every data traffic that enters the network. This included the source IP address, destination IP address, source port, destination port, layer 3 protocol type, TOS byte (DSCP) and input logical interface (in Index). So they used the decision tree algorithm technique to automatically select the various features provided by the NetFlow to model the traffic pattern of the different DDoS attack types. The second technique used is the neural network technology. Author used this technique to classify DDoS attacks as normal or abnormal traffic using the automatic attributed produced by the decision tree algorithm. According to author, their results produce twice performance than the heuristic selection and also their approach produced better performance than the single data mining approach.

III. Proposed System Approach

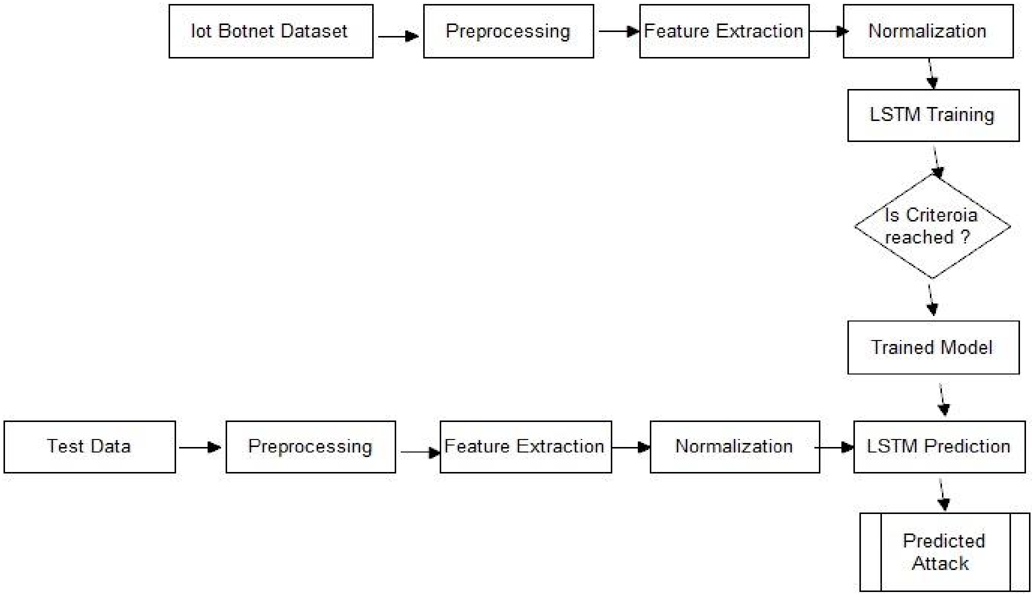

Figure 1: Block Diagram of Proposed System

- **Data Collection:** First step is to collect data. We will collect UNSW NB-15 dataset. This dataset has 4 CSV files of data records and each CSV file contains attack and normal records.
- **Data Preprocessing:** In this step we will clean the data. We will manipulate or drop the data before it is used to ensure or enhance performance.
- **Feature Extraction:** The aim of this step is to reduce the number of features in a dataset by creating new features from the existing ones (and then discarding the original features).
- **Normalization:** Normalization is a scaling technique in which values are shifted and rescaled so that they end up ranging between 0 to 1.This is also known as min-max scaling.
- **LSTM Training:** Finally we train our deep learning model using LSTM. This model will be used to make attack predictions.

DOI: 10.48175/IJARSCT-3700

IV. Methodology Used in Proposed System

4.1 LSTM

Long Short Term Memory networks usually just called LSTMs are a special kind of RNN, capable of learning long-term dependencies. and were refined and popularized by many people in following work.

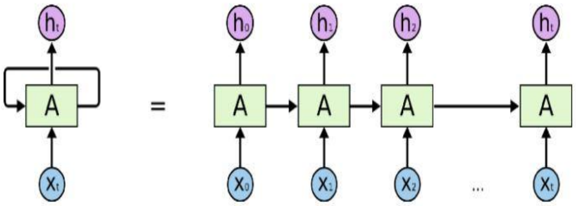

Figure: Architecture of LSTM

They work tremendously well on a large variety of sequence modelling problems, and are now widely used. LSTMs are explicitly designed to avoid the long-term dependency problem. Remembering information for long periods of time is their default behaviour. Let’s recall how an RNN looks As we saw in the RNN article the RNN unit takes the current input (X) as well as the previous input (A) to produce output (H) and current state (A).

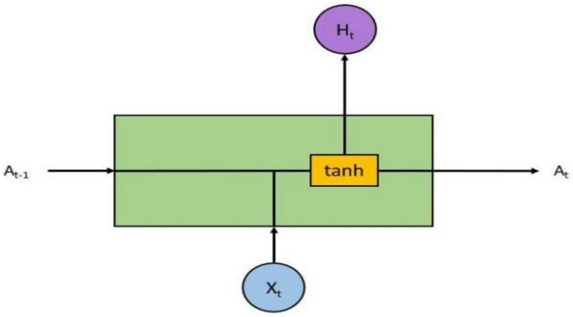

Figure: Architecture of One Block

LSTMs also have a similar structure though the internals have different components as compared to a single tanh (activation) layer in the RNN. There are 4 layers inside an LSTM block which interact together:

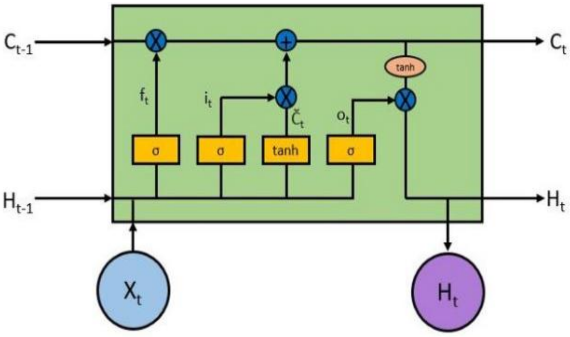

Figure. Layers of LSTM

At first it looks pretty complicated and intimidating but let’s tries to break it down and understand what the purpose of each layer and block is. The key to the operation of LSTM is the top horizontal line running from left to right enclosed in the highlight below. With some minor linear interactions along this line the cell state C allows information to flow through the entire LSTM unchanged which enables LSTM to remember context several time steps in the past. Into this line there are several inputs and outputs which allow us to add or remove information to the cell state. The addition or removal of information is controlled by gates. These are the sigmoid layers (Yellow boxes inside the RNN cell). They output numbers between zero and one, describing how much of each component should be let through. A value of zero means let nothing through, while a value of one means let everything through. An LSTM has three of these gates to control the cell state.

V. Conclusion

This paper work seeks to address two main questions posed in section 1.2 and also produces results which fulfill the research goals also posed in section 1.3 all in chapter one of this project work. In addressing these tasks, the ultimate goal was to detect Iot Botnet attacks on a network. To achieve these objectives, artificial intelligence, specifically, the Long Short-Term Memory (LSTM) Recurrent Neural Network (RNN), a machine learning technique and Google's second generation machine learning framework called TensorFlow was adopted and used. The evaluation of the produced model was performed on two computing platforms which are CPU and GPU. To address the research question, a CPU based tensorow environment was created and the algorithm was coded using tensorow APIs as well as following the mathematical computational formulas of LSTM architecture.

To determine the Accuracy and efficiency of the algorithm, it was evaluated against seven main parameters such as dataset size, epochs, learning rate, nodes, weights, and biases. There was a lot of iteration done to get the best results. Every iterations done involved assigning of different values to parameters such as datasets size and epochs while randomly generated values for weights and biases were used, layers, nodes and learning rate were held constant, until the best detection accuracy was achieved.

VII. Future Work

Intrusion Detection is becoming re-created as Intrusion Prevention. In the future, instead of detecting an intruder, detection systems will identify a suspicious event and let the system administrator or security officer decide whether to start an investigation. The automotive industry will need to incorporate defensive intrusion prevention and detection solutions into their cars, as the impact of attacks could be disastrous.

VIII. Acknowledgment

This work is supported in Lung Cancer Detection System for medical research and development of any state in India. Authors are thankful to Faculty of Engineering and Technology (FET), Savitribai Phule Pune University, Pune for providing the facility to carry out the research work.

References

[1]. G. Loukas, and O. Gulay. "Likelihood ratios and recurrent random neural networks in detection of denial of service attacks." 2007.

[2]. G. Oke, G. Loukas and E. Gelenbe, "Detecting Denial of Service Attacks with Bayesian Classifiers and the Random Neural Network," 2007 IEEE International Fuzzy Systems Conference, London, 2007, pp. 1-6.

[3]. A. B. M. A. A. Islam and T. Sabrina, "Detection of various denial of service and Distributed Denial of Service attacks using RNN ensemble," 2009 12th International Conference on Computers and Information Technology, Dhaka, 2009, pp. 603-608.

[4]. Z. A. Baig and K. Salah, "Multi-Agent pattern recognition mechanism for detecting distributed denial of service attacks," in IET Information Security, vol. 4, no. 4, pp. 333-343, December 2010.

[5]. M. Kim, H. Na, K. Chae, H. Bang, and J. Na: A Combined Data Mining Approach for DDoS Attack Detection, Lecture Notes in Computer Science, Vol. 3090, pp. 943-950, 2004.

DOI: 10.48175/IJARSCT-3700