JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue

JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)

An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Efficient Approach For Detection Of Iot-Botnet Cyber Attack Using Machine Learning

Akshata Zanje[1], Amit Kshirsagar[2], Akshay Wankhade[3], Himanshu Thakare[4]

Department of E&TC, SKNCOE, SPPU, Pune

[1]akshatazanje111@gmail.com

[2]amit.kshirsagar_skncoe@sinhgad.edu

[3]akshaywankhade664@gmail.com

[4]himanshuthakare12@gmail.com

***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 un-authorized attempt to access the elements of a network with the aim of making the system unreliable.

***Keywords*— IoT,botnets, machine learning, IDS, feature selection, LSTM, RNN**

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. 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. and Kim et al. 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 proposed nature inspired approach in this research is able:

- To automatically generate signatures (rules).
- To detect anomalous traffic.
- To Develop and analyze of a flexible LSTM based sequential learning technique
- To generate accurate and compact sequential layers for IBA detection by an effective genetic algorithm.

II. REVIEWOF LITERATURE

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.

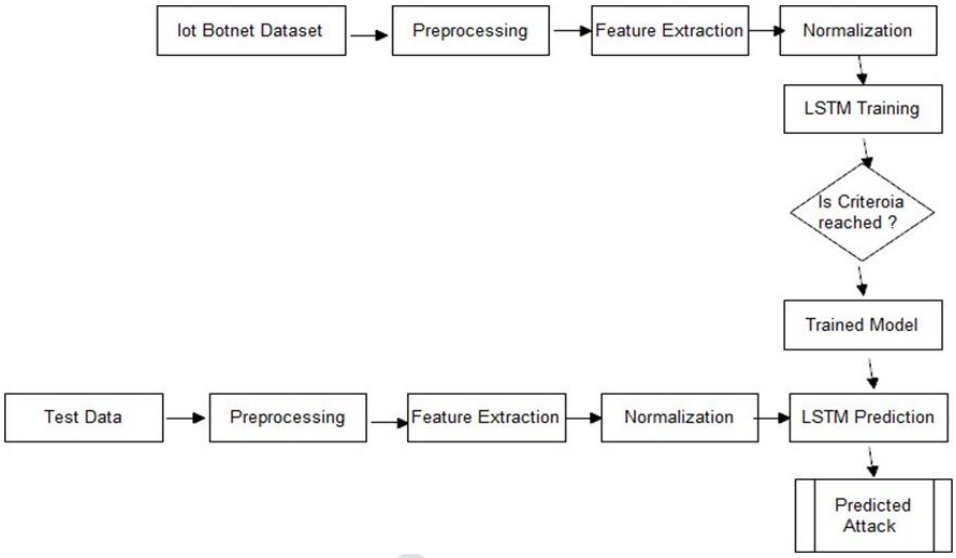
Again, Loukas et al. [2] in another research work focus on using two schemes, namely, the biologically inspired Random Neural Network (RNN) and multiple Bayesian classifiers to detect and distinguish normal traffic from DDoS attack traffic. This technique works by selecting the detection features and 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 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. BLOCK DIAGRAM



IV. BLOCK DIAGRAM DESCRIPTION

- Iot Botnet Dataset
- Bot-IoT is a recent and publicly available dataset that represents botnet attack traffic in Internet of Things (IoT) networks
- About 9,000 of the roughly 73,000,000 instances in the dataset are labeled as normal traffic.
- Preprocessing
- Data preprocessing, a component of data preparation, describes any type of processing performed on raw data to prepare it for another data processing procedure.
- Feature Extraction
- Feature extraction refers to the process of transforming raw data into numerical features that can be processed while preserving the information in the original data set.

V. IMPLEMENTATION SYSTEM

It provides an analysis of threat and alerts that concerns the security of the application or network. It is a way of collecting data through a security device that forms together in a centralized system. Designing a genetic-based rule learning classifier, which can automatically generate a concise set of easy to understand rules for IBA detection. This system decreases human effort in creating and maintaining rules for rule-based systems. Another goal of this research is to make the detection system adaptable to the changes in the real environment using an incremental learning approach.

VI. ALGORITHMS

1] LSTM:

Long short-term memory is an artificial neural network used in the fields of artificial intelligence and deep learning. Unlike standard feedforward neural networks, LSTM has feedback connections. Such a recurrent neural network can process not only single data points, but also entire sequences of data.

2] RNN:

A recurrent neural network (RNN) is a class of artificial neural networks where connections between nodes can create a cycle, allowing output from some nodes to affect subsequent input to the same nodes. This allows it to exhibit temporal dynamic behavior.

VII. RESULT AND DISCUSSION

VIII. 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.