Detection of DDOS Attack by Quasi-Newton Back propagation Algorithm

Roheen Qamar[1], Fareed Ahmed Jokhio[2], Baqir Ali Zardari[3], Abdul Wahid Memon[2], Javed Akhtar Unar[3],

[1]Dept. Of Computer Science, QUEST Nawabshah Pakistan
[2]Dept. Of Computer System Engineering, QUEST Nawabshah Pakistan
[3]Dept. Of Information Technology, QUEST, Nawabshah, Pakistan
roheen.qamar04@yahoo.com

ABSTRACT. The main objective of DDoS attacks is to compile different internet-wide systems with infected zombies / agents and form botnets of the network. These zombies are intended to attack a specific target or network with different types of packets. A self-installed trojan controls remotely the infected systems controlled by either an attacker or self-installed trojans scheduled to launch packet floods. The purpose of this paper is to detect DDoS attacks in this context. We have selected an Quasi-Newton backpropagation algorithm to detect DDoS attacks by using a feedforward neural network.

Keyword: DDoSAttacks,ANN,KDD

1. Introduction

DDoS is a type of DOS attack which uses different compromised systems to target a single system that causes a Denial of Service (DoS) attack, sometimes infected with a trojan. Victims of a DDoS attack consist of the targeted end system as well as all computers maliciously used and run by the attacker in the distributed attack. The incoming traffic that floods the target in a DDoS attack comes from many different sources— maybe hundreds of thousands or more. This effectively prevents the attack simply by blocking a single IP address; however, it is very difficult to differentiate when spread across so many points of origin These are often referred to as "zombie computers" They form what is known as a "botnet" or network of bots. These are used to flood targeted websites, servers, and networks with more data than they can accommodate [1].

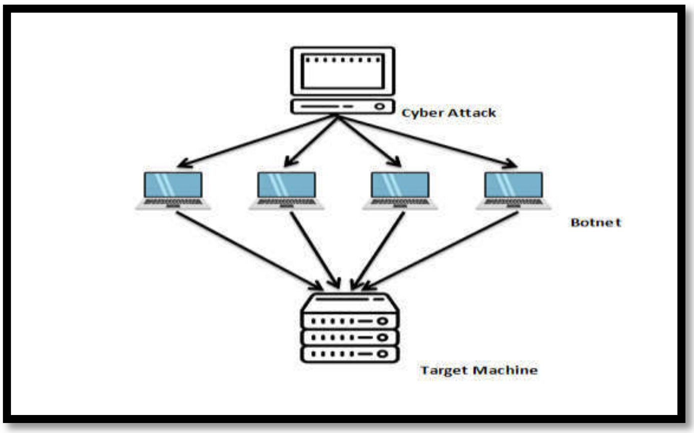

Figure.1: Architecture of a DDoS attack

There are many kinds of attacks on the DDoS. Popular attacks include: the target will be overwhelmed with massive amounts of junk data by the bandwidth attack. This results in a lack of network bandwidth and resources for equipment as well as a complete denial of service. Traffic flooding attacks send a huge amount of TCP, UDP and

ICPM packets to the target. Legitimate applications are lost and these assaults may be caused by malware exploitation. In Application Attacks knowledge messages can deplete funds in the application layer, leaving device facilities of the target unavailable [2].

2. Artificial Neural Network

Artificial neural networks are one of the main methods used in machine learning. As the "neural" part of their name suggests, they are brain-inspired systems designed to replicate the way we beings think. Neural networks consist of input and output layers and (mostly) a hidden layer of units that transform the input into something that can be transformed by the output layer. There are several types of neural networks, each with their own specific cases of use and levels of complexity. The most common type of neural network is a neural feed forward network, where information travels in one direction from input to output [5].

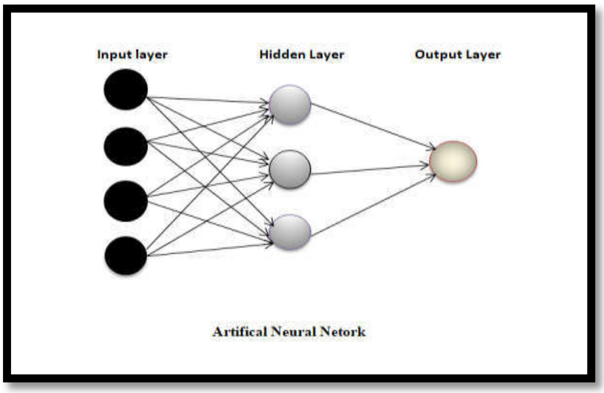

Fig.2:Artificial Neural Network

2.1 Feed Forward Neural Network

The feed forward neural network was the first and easiest form of artificial neural network designed. In this network, the data moves from the initial nodes to the invisible nodes (if any) and the output nodes in only one direction. The network has no cycles or loops. Perception is a single-layer neural network and Neural Networks is called a multi-layer perception. Perception is a linear (binary) classifier. It is also used for supervised learning. It helps to classify the information provided by the input. The sum of input products and their weights are calculated in a feed forward neural network. This is then provided to the output. Here's an example given of a single-layer neural network feed forward [8].

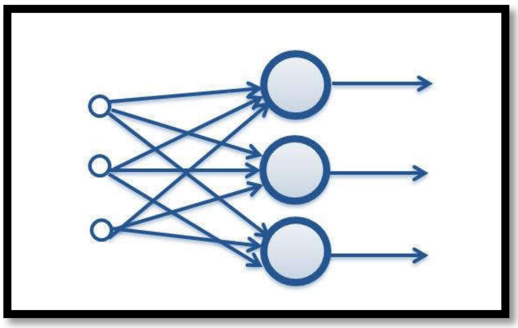

Fig.3: Feed Forward Neural Networks

3. Background Work

Mukhopadhaya, S Polle [1] recognize different kinds of DoS attacks and then propose a new methodology to simulate and used the artificial neural network in MATLAB and training the KDD data set in neural network after training the results shows that which neural network is best for the detection of DOS.

Saied, A., Overill, R. E [2] This research is aimed at detecting and mitigating known and unknown DDoS assaults before reaching the victim. To detect recognized and unknown DDoS attacks and the capacity of DDoS attackers to crash or overload a target, we chosen DDoS attacks due to deficiencies in current methods compared to other security domains.

Li, J., Liu, Y., [3] this paper describes a DDoS attack detection technique based on neural networks based on artificial intelligence. In this technique, server resource assessment and network traffic, it has better outcomes to detect DDoS attack to train ordinary or abnormal detection capacity.

Ali, O., & Cotae, P [5]This research discusses Artificial Neural Networks (ANN) as a machine learning solution for Denial of Service Attacks (DoS) and Distributed Denial of Service Attacks (DDoS) intrusion detection systems. The proposed method used the back propagation of the Bayesian Regularization (BR) and the scaled downward propagation algorithm of the conjugate gradient (SCG). The network has been trained and tested using the CICID2017 dataset sub-set that meets the criteria of the real world. The input data set characteristics that best characterize each attack and ordinary network traffic have been carefully selected. The result revealed that the suggested technique used Bayesian regulation effectively to detect DoS / DDoS. The outcome disclosed that the suggested technique effectively used Bayesian Regularization to detect DoS / DDoS assaults with a precision of 99.6 percent and scaled conjugate gradient descent of 97.7 percent.

Kale, M., & Choudhari, [6] This paper discusses the attacks on DDoS. Current machine learning approaches such as neural classifiers can detect such attacks on DDoS. Such classifiers lack the capacity to generalize, resulting in lower performance resulting in high false positives. This paper tests the quality of the choice of a comprehensive set of machine learning algorithms. He proposed classification algorithm. Hence, the system must be trained and tested in such a way that it learns by observing the aberrant patterns associated with the network traffic and classify the incoming traffic as an attack or normal.Training time depends on the number of times the classifier requires training, which, in effect, depends on the average square error between iterations hitting the global minimum. Training is improved by eliminating overlapping data and keeping only samples of training adjacent to the boundary of judgment. Often, since the output vector number is smaller, the training time is lower. It is therefore clear that the RBP Boost algorithm will be ideal for a setting in real time.

MohdYusof [18] He suggested digital tools for the protection of DDoS. He classifies forms of DDoS attacks and methods of security. This paper reviews the Detection and Defense Algorithms of Different Types of DDoS Attacks. They presents an overview of the existing detection and defense algorithms to mitigate four types of DDoS attacks and they are the (UDP) user data gram flood, (SYN) synchronize flood, Ping of Death and Smurf attack. The paper analyzes systems vulnerability targeted by TCP (Transmission Control Protocol) segments when SYN flag is ON, which gives space for a DoS (Denial of Service) attack called SYN flooding attack or more often referred as a SYN flood attack.

4. IMPLEMENTATION

We implemented the system as a dataset training / test, processing data set, determining the NN architecture, training the system and testing the system in five different phases. The following figure shows the diagrammatic sequence of our execution.

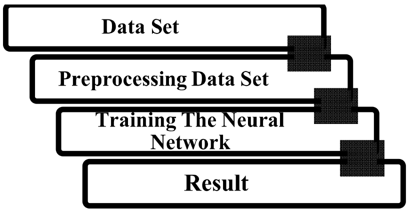

Fig.4: Implementation Phases

5. Experimental Result

We used the MATLAB for this work. First we clean the KDD data set and give the values of Protocol, Attacks and Flags. Then we develop neural network model and training the KDD data set using ANN. when the training is complete we got the results of DDoS attacks. In this paper trainbfg algorithm is used it is a network training function that updates weight and bias values according to the BFGS quasi-Newton method.

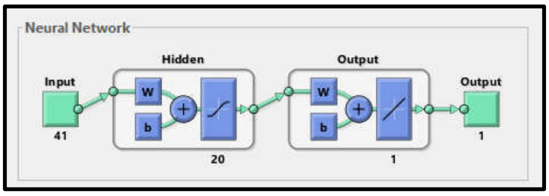

Fig.6: Neural Network

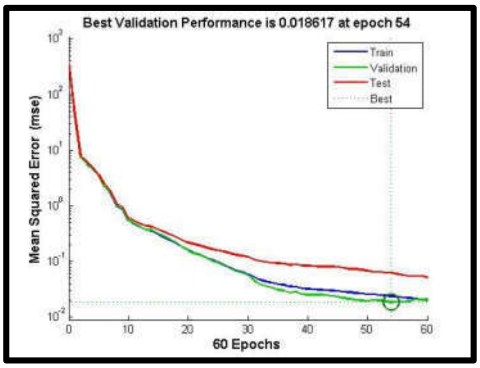

Fig.8: Validation Performance

Performance of the feed forward neural network showing that validation is goes on optimizing the threshold. The best validation performance is 0.018617 at epoch number 54.

6. Conclusion

In this paper we used feed forward neural network for the detection of DDoS Attack and trainbfg algorithm is used for this training in Matlab tool box.in future work different algorithm and neural network is used to compare that which network and algorithm is best for detection of DDoS Attack.

References

1. Ahmad, 1. Abdullah, A. B., and Alghamdi. "Artificial neural network approaches to intrusion detection: a review." In Proceedings of the 8th Wseas international Conference on Telecommunications and informatics, 2009.

2.Saied, A., Overill, R. E., & Radzik, T. (2016). “Detection of known and unknown DDoS attacks using Artificial Neural Networks”. *Neurocomputing*, *172*, 385-393.

3.Li, J., Liu, Y., &Gu, L. (2010, November). “DDoS attack detection based on neural network. In *2010 2nd International Symposium on Aware Computing”* (pp. 196-199). IEEE.

4. Mirkovic, J., Robinson, M., Reiher, P., & Oikonomou, G. (2005). “Distributed defense against DDOS attacks”. *University of Delaware CIS Department technical report CIS-TR-2005-02*, 1-12.

5.Ali, O., & Cotae, P. (2018, November). “Towards DoS/DDoS Attack Detection Using Artificial Neural Networks”. In *2018 9th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)* (pp. 229-234). IEEE.

6.Kale, M., & Choudhari, D. M. (2014). “DDOS attack detection based on an ensemble of neural classifier”. *International Journal of Computer Science and Network Security (IJCSNS)*, *14*(7), 122.

7. Nazario, J. (2008). “DDoS attack evolution. *Network Security”*, *2008*(7), 7-10.

8. Gupta, B. B., Joshi, R. C., & Misra, M. (2012). “ANN Based Scheme to Predict Number of Zombies in a DDoS Attack”. *IJ Network Security*, *14*(2), 61-70.

9.D.M.Choudhari 1Associate Prof, Department of Computer Science and Engineering ISSUE-2, 2014 “DDOS Attack Detection Based On Ensemble of Neural Classifier” VOLUME-1, PP.1-7

10.Mukhopadhayay, I., Polle, S., & Naskar, P. (2014). “Simulation of Denial of Service (DoS) Attack using Matlab and Xilinx”. *IOSR Journal of Computer Engineering (IOSR-JCE).*

11. Peraković, D., Periša, M., Cvitić, I., & Husnjak, S. (2016, November). “Artificial neuron network implementation in detection and classification of DDoS traffic”. In *2016 24th Telecommunications Forum (TELFOR)* (pp. 1-4). IEEE.

12.Mirkovic, J., Prier, G., & Reiher, P. (2002, November). “Attacking DDoS at the source”. In *10th IEEE International Conference on Network Protocols, 2002. Proceedings.* (pp. 312-321). IEEE.

13.Douligeris, C., & Mitrokotsa, A. (2004). “DDoS attacks and defense mechanisms: classification and state-of-the-art. *Computer Networks”*, *44*(5), 643-666.

14Aljumah, A., & Ahamad, T. (2016). “A novel approach for detecting DDoS using artificial neural networks”. *International Journal of Computer Science and Network Security*, *16*(12), 132-138.

15.Xie, Y., & Yu, S. Z. (2006, June). “A novel model for detecting application layer DDoS attacks”. In *First International Multi-Symposiums on Computer and Computational Sciences (IMSCCS'06)* (Vol. 2, pp. 56-63). IEEE.

16. Mirkovic, J., & Reiher, P. (2004). “A taxonomy of DDoS attack and DDoS defense mechanisms”. *ACM SIGCOMM Computer Communication Review*, *34*(2), 39-53.

17.Noh, S., Lee, C., Choi, K., & Jung, G. (2003, March). “Detecting distributed denial of service (ddos) attacks through inductive learning”. In *International Conference on Intelligent Data Engineering and Automated Learning* (pp. 286-295). Springer, Berlin, Heidelberg.

18. Mohd Azahari Mohd Yusof, Fakariah Hani Mohd Ali, and Mohamad Yusof Darus‖ Detection and Defense Algorithms of Different Types of DDoS Attacks‖