Journal Of Harmonized Research (JOHR)

Journal Of Harmonized Research in Engineering
2(1), 2014, 15-19

ISSN 2347 – 7393

Original Research Article

NETWORK TRAFFIC CLASSIFICATION USING ARTIFICIAL NEURAL NETWORK (ANN)

Rohit Khandelwal*, Abhinav Srivastava, Md.Ejaz Uddin

BE, Dept. of E&TC, V.I.I.T, Pune-48.

Abstract- In today's world there is a tremendous increase in volume of the information exchanged on internet, so subsequently its misuse has also increased. Most of the internet applications such as traffic controls, lawful interceptions and intrusion detections poses high requirement of traffic classification model. This thesis we present a low cost Network traffic classification model, which can be used to classify traffic at a host node. The feature of our design is to classify legitimate traffic with the Denial of Service (DoS) traffic based on the analysis using Artificial Neural Network.

Keywords- Artificial Neural Network (ANN), Denial of Service (DoS), Internet Control Message Protocol (ICMP), User Datagram Protocol (UDP), Transmission Control Protocol (TCP)

1. Introduction:-

A system intrusion is any attempt to attack a system and compromise its security aspects such as integrity, confidentiality, or availability. A model like ours of network classification is implemented to detect an intrusion when it occurs. The responsibility of such model includes monitoring traffic as it passes through a network and analyzes it and detects predefined patterns of attack or abnormal behaviors that could be caused due to system attacks. Host based classification models are deployed on a host computer which monitors continuously the processes that are running inside the host. The classification model monitors the changes to a number of variables on the host, to detect an attack. It then compares the values of the variables to the threshold values and any deviation from the threshold values results in the model sending a result. One of the major security issues which arises today is to reduce the impact of Denial of Service (DoS) or Distributed Denial of Service (DDoS) and similar many other different attacks. The reason, such attacks have

For Correspondence:
29rohitkhATgmail.com
Received on: February 2014
Accepted after revision: February 2014
Downloaded from: www.johronline.com

become so prominent is that it is easy to use DoS tools such as trinoo (Dittrich 1999), as they are easily available on the internet. So, even normal users can perform DoS attacks with minimal efforts [5]. DoS/DDoS attacks involve sending attack traffic to a victim computer so that its resources get exhaust. It is a deliberate act done so that the availability of services get degraded. A Denial of Service attack consumes a victim's system resource such as network bandwidth, CPU time and memory, the extent to which these resources get depleted depends upon the volume of attack traffic. Some general DoS/DDoS attacks include ICMP flooding, UDP flodding, TCP SYN attack and smurf. Therefore it is very necessary to prevent attacks for the upmost availability of our resources. This paper is organized as follows. Section 2 outlines the previous studies in the area of DoS attack detection. Section 3 describes the structure of our proposed system. Section 4 describes the implementation of our system. Section 5 discusses issues and concludes the paper.

2. Related Work

There have been many previous studies carried out to prevent the problem of intrusion, such as ICMP trace back, Intension driven ICMP trace back, there have been lightweight detection methods discussed for the detection of Denial of Service attacks. In general, solutions for these kind of attack includes mechanisms such as ingress filtering or egress filtering, aggregate based congestion control or rate limiting (ACC), Probabilistic marking, IP hashing, Deterministic tunnel marking, SYN cache and SYN cookie for TCP flooding at server node. There are also many Intrusion detection systems such as Snort, Lancope and StillSecure. Algorithms based detection methods have also been discussed.

3. Proposed System

The flow of mechanism will be divided into three parts which includes capturing of the packets, training them using Artificial Neural Network and then comparing the results with the other data set of packets.

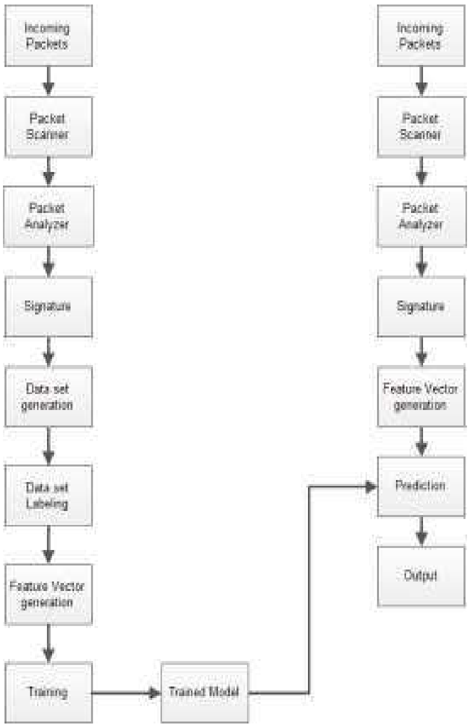


Fig 1. Flow diagram

For the first part we will use a packet sniffer or third party tool to acquire packets from a network. A packet sniffer is a program that can visualize any information which passes over the network. Our packet sniffer is based on Jpcap. Jpcap is used as a tool to acquire and analyze network traffic.

It has an API which is used to build packet capturing applications based on Java. Jpcap is based on winpcap/libpcap. WinPcap/Libpcapallows us to capture and transmit network packets bypassing the protocol stack. After the process of scanning the packets there will be need to analyze them and in the process extract signatures. Extracted signatures from the scanned packets will be useful in generating a vast data set. The generation of the data set will let us allow labeling the records as good or bad. The data set will then be converted to an integer (feature matrix / array) so that the final data set is ready.

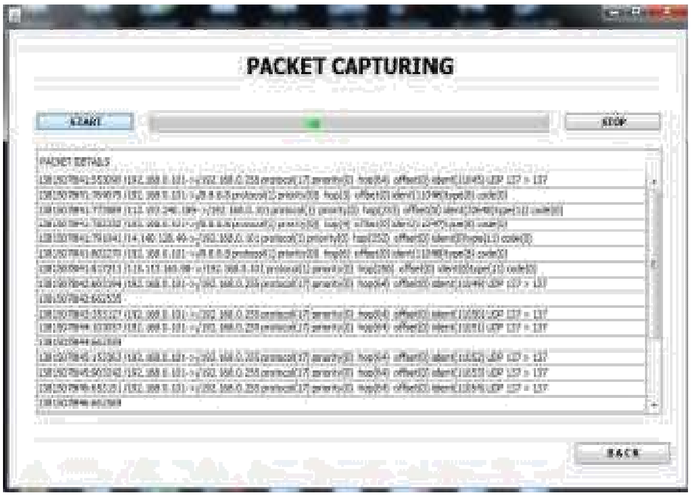
Training will be done using the labeled data set. We will be using Artificial Neural Networks (ANN) as our training algorithm. The data set will be provided as the input to Artificial Neural

Network (ANN). The saved trained output will be then used for comparison purposes.

The final part includes the recognition of the attack packets. Recognition will be done by comparing the trained data set with the unlabeled data set

4. Implementation and Result

As discussed, our mechanism is divided into three parts. For the first part we will be using a packet sniffer or a third party tool such as wireshark to log the traffic that will be flowing over the network. If we use a third party tool then the output of the tool itself will be a set of extracted signatures. The extracted signatures will then be labeled as good or bad. After the process of labeling the data set has to be converted into an integer this process is known as feature vector generation, this will be the final set that we would be applying at the input of Artificial Neural Networks (ANN) for its training.



PACKET DETAILS

```
[illegible]
```

Fig 2. Packet sniffer

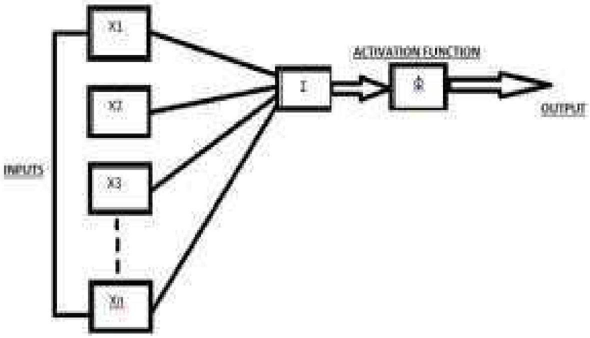


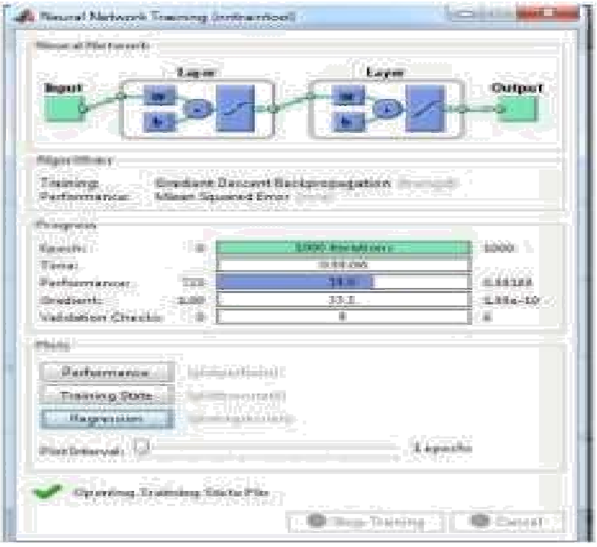
Fig 3. A perceptron configuration

This configuration is called as artificial neuron configuration, also known as perceptron configuration. It models a neuron by taking a weighted sum of inputs and then sending the output. The output can be either 0 or 1.The output will be 1 if the weighted sum of the input is greater than the adjustable threshold value otherwise it will be 0. The values of the inputs (x1, x2, x3,…xn) and also the connection weights (w1,w2,w3,…wn) in figure are real values which can be both be positive (+) and negative (-). Learning in perceptron is a process which includes modifying the input weight and bias, where bias is an adjustable threshold processor. When an input is given to a perceptron it computes a binary function of the given input. We can make a perceptron learn by repeatedly studying examples presented to it. The learning rule of a perceptron can be indicated by equation 1, where For all inputs j:

$$X (j) = X (j) + [A-T] * q (j) \qquad (1)$$

Where X is the vector of weights, q is the input vector which we present to the network, A should have been the correct result of the neuron and T is the actual output of the neuron.

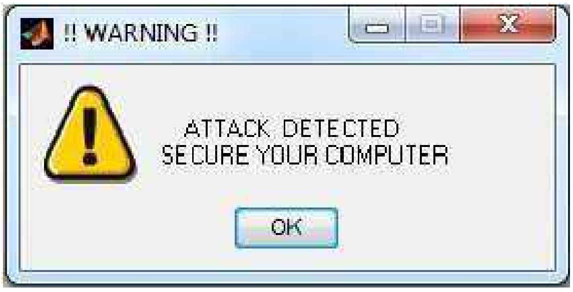
So to train the data set, vectors from the set are presented to the to the network one after other. If the network's output is correct no change is made otherwise using the perceptron learning rule the weights and biases are updated. When the entire vectors pass through it without any error, training is complete.



Training: Gradient Descent Backpropagation
Performance: Mean Squared Error

Fig 4. Sample Analysis of humps function to indicate training and performance of ANN in matlab

After the training of the data set we now compare its output with the some other unlabeled set of data. Firstly we load the trained network values. Then we load the unlabeled data set which may or may not be violating the standard network protocols. We then apply the data records one by one to Artificial Neutral Networks (ANNs) and evaluate output. If a data by the analysis module seems to violate a specific protocol then particular details about the network packet/packets will be popped up by the system with the help of appropriate graphical user interface.


!! WARNING !!

ATTACK DETECTED
SECURE YOUR COMPUTER

Fig 5.A sample GUI for our result

5. CONCLUSION

In this paper we propose a new intrusion detection approach using Artificial Neural Networks. Various aspects of DoS attack were listed. To prevent oneself against these types of attacks one must detect the occurrence correctly. Regardless of how well security of a particular network is planned it is inherently susceptible to DoS/DDoS or some other kind of attacks . The mechanism we discussed helps to accurately detect the attacking packets and thus prevents from the harms of such kind of attacks. With some modifications this project can help to mitigate DoS/DDoS problems at real time .

6. ACKNOWLEDGMENT

The study, concept and project is guided by
Asst. Prof. A. W. Ingle

7. REFERENCES

1. (MAY 2007) "A Divide-and- Conquer Strategy for Thwarting DistributedDoS Attacks" Ruiliang Chen, Student Member, IEEE, JungMin Park, Member, IEEE, and Randolph Marchany, Member, IEEE (IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 18, NO. 5.)
2. "Detection and Defense against DDoS Attack with IP Spoofing" Mr. I. B.Mopari M.E. Student Vishwakarma Institute of Technology, Pune, India Prof S.G.Pukale Vishwakarma Institute of Technology, Pune, India Prof M.L.Dhore, Vishwakarma Institute of Technology, Pune, India (Proceedings of the 2008International Conference on Computing, Communication and Networking(ICCCN2008)
3. "Defending Against TCP SYN Flooding Attacks under Different Types of IP Spoofing" Wei Chen Department of Computer Science Hong Kong University of Science and Technology Clear Water Bay, Kowloon, Hong Kong and Dit-Yan Yeung, Computer School Wuhan University Wuhan 430072, Hubei, China
4. Prof. Radha S. Shirbhate Prof. Pallavi A. Patil "Network Traffic Monitoring Using Intrusion Detection System" Volume 2, Issue 1, January 2012 ISSN: 2277 128X
5. Qijun GU Peng Liu, "Denial of Service Attacks"
7. G. Jacob Victor Dr. M Sreenivasa Rao Dr. V. CH. Venkaiah "Intrusion Detection Systems - Analysis and Containment of

False Positives Alerts" International Journal of Computer Applications (0975 – 8887) Volume 5– No.8, August 2010

8. MeeraGandhi, S.K.Srivatsa "Detecting and preventing attacks using network intrusion Detection systems"
9. J.Udhayan, RAnitha, Department of mathematics and Computer Applications, PSG College of Technology, Coimbatore, India "Demystifying and rate Limiting ICMP hosted DoS/DDoS Flooding Attacks with Attack Productivity Analysis"
10. G.Prashanth, V.Prashanth, P.Jayashree, N.Srivasan Department of Information Technology, MIT Campus, Anna University "Using Random Forests For Network-based Anomaly detection at Active routers" IEEE-International Conference on Communications and Networking, Signal Processing, Madras Institute of Technology.