International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 03 | Mar 2020 www.irjet.net p-ISSN: 2395-0072

Network Traffic Monitoring and BotNet Detection using K-ANN Algorithm

Sayali Zalte[1], Saloni Chavare[2], Rumana Kazi[3], Kulkarni Shripad[4]

[1,2,3]Student, Dept. of Computer Science & Engineering, BMIT, Solapur, Maharashtra, India
[4]Professor, BMIT College of Engineering, Solapur, Maharashtra, India

---***---

Abstract - *Due to increase of the cyber threats, we have made cyber security paramount for protecting personal and private information to get move secure network in the real time information, we have to provide the most highly secure network environment, network traffic monitoring and the most important threats detection system that is varied from the enterprise networks. In this paper we have concept for the issue of handling the large amount of network traffic data for the enterprise system it can simultaneously provide real time monitoring.*

Basically we introduced and evaluated on threat detection which is highly intensive network traffic for real time and we utilizes K-ANN (Kohonen Artificial Neural Network) algorithm detection of abnormal network activities. Remote device which is directly connect seed to server and has authority to monitoring and modifying the network activity. To avoid all the above problems we can set up WLAN with the serves machine which can handle and monitor the LAN network.

Key Words: **Threat Detection, Network Monitoring, K-ANN Algorithm.**

1. INTRODUCTION

Cyber-crime is a major issue these days. From last few years many researchers have done research on network forensics to reduce the cyber-crime. Network forensics is the forensic science that studies the network traffic and analyzes it for the detection of network attacks. A controller called bot-master controls Botnets. There is a need to detect the network attacks and to prevent them. In developing effective threat monitoring systems, there are two major hurdles. First, the amount of data available to the threat monitoring system is massive. This rate of data creation and transfer is impossible for traditional data analysis platforms to effectively process. Second, detection systems, and the resulting defensive actions taken, are only effective if they can detect intrusions accurately and in a timely manner, minimizing the impact of the attacks. This system should be able to characterize, track, and mitigate security threats in a timely fashion. The millions of devices generate a big amount of data streams, needs to be managed, processed, transferred and stored in a secure real-time way. Detect botnet based on traffic analyzing network traffic activity using machine learning. Traffic analysis methods do not depend on the packets payload, which means that they can work with encrypted network communication protocols. Network traffic information can usually be easily recover from various network devices without affecting significant network performance or service availability.

2.OVERVIEW

A. Existing System

From the existing system [1], experimental data indicates that the developed system can achieve performance with the k-means clustering algorithm. It can have detection rate is 91.8% and false positive rate is 1.8%.

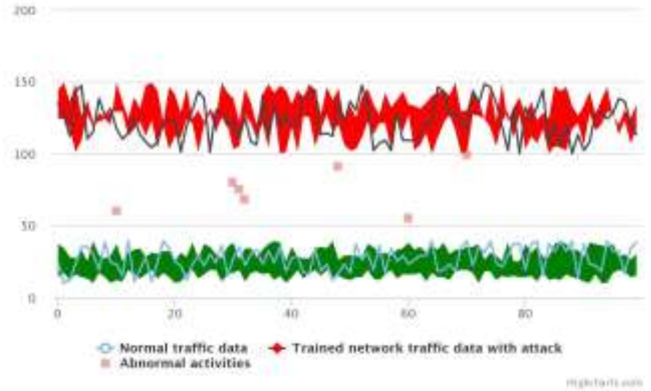


Figure 1: Streaming based threat detection.

B. Drawbacks of Existing System.

It takes more time to analyze the streaming data. Hence it is time consuming process and also requires the high end devices. Infrastructure is expensive. It requires much complex system.

C. Need of Kohonen Artificial Neural Network

We used K-ANN supervised algorithm. So it provide the predefine result set to the predicted result and match the both results and decides the behavior of the network and provide decision to the user.

3.MATHEMATICAL MODEL

Step 1: Then-dimensional weight vectors w1, w2, . . .,wm of the m computing units are selected at random. An initial radius r, a learning constant η, and a neighborhood function φ are selected.

Step 2: Select an input vector ξ using the desired probability distribution over the input space.

Step 3: The unit k with maximum excitation is selected (i.e. the distance between (w_i and ξ) is minimal, i = 1, . . .,m).

Step 4: The weight vectors are updated using the neighborhood function and the update rule.

Step 5: Stop if the maximum number of iterations has been reached; otherwise modify η and φ as scheduled and continue with step 1.

$$\mathrm{w}_i \leftarrow \mathrm{w}_i + \eta\phi(i,k)(\xi - \mathrm{w}_i), \quad \text{for} \quad i = 1, \ldots, m.$$

4. PROPOSED SYSTEM

A.Architectural Diagram.

A botnet is a collection of computers which is connected to the Internet they have been controlled remotely by an intruder (the bot-master) via malicious software called bots. The system consist of different attacks DDOS, HTTP attack, IP spoofing, HTTP header, http header with multiple IP. Middleware consist of botnet detection system which consist of java packet capture library and Win P cap library, which is meant to detect network traffic through these libraries.

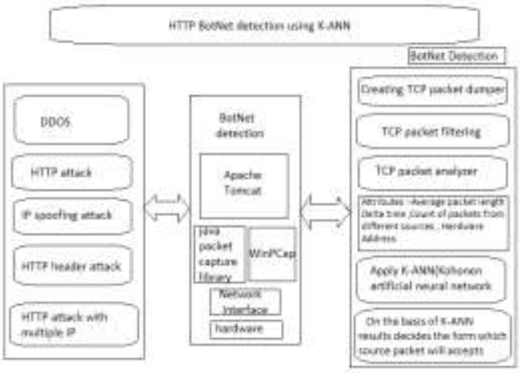

HTTP BotNet detection using K-ANN
BotNet Detection
DDOS
HTTP attack
IP spoofing attack
HTTP header attack
HTTP attack with multiple IP
BotNet detection
Apache Tomcat
Java packet capture library
WinPCap
Network Interface
hardware
Creating TCP packet dumper
TCP packet filtering
TCP packet analyzer
Attributes :-Average packet length Delta time ,Count of packets from different sources , Hardware Address
Apply K-ANN/Kohonen artificial neural network
On the basis of K-ANN results decides the form which source packet will accepts

Figure 2: System Design Architecture.

While a significant amount of research has been accomplished on botnet analysis and detection, several challenges remain unaddressed, such as the ability to design detectors which can cope with new forms of botnets. Detect botnet based on traffic and analyzing network traffic behavior using machine learning. Traffic behavior analysis methods do not depend on the packets payload, which means that they can work with encrypted network communication protocols. Network traffic information can retrieved from network devices without affecting network performance. The final stage of our architecture is to detect bot across network by applying K-ANN algorithm on the real time packet information which is gathered by JPCAP and Win P cap library.

B.Auto-Network Interface Detection Module

The type of network is detected by using Auto-Network Interface Detection Module whether it is wired or wireless.

C.Packet Capture Module

This module is also called as packet analyzer as well as network analyzer, protocol analyzer or packet sniffer this phase actually piece of computer program that can intercept and logs traffic that passes over a digital network or a part of network. As data streams across the network the sniffer captures each packet and is needed decodes the packet raw data, showing the values of various fields in the packet and analyzes its content or other specification. This is done using JP NET CAP, Win P Cap.

D.Dump File Module

TCP dumper prints the content of network packets. It also read packets from a NIC (network interface card) or from a previously created saved packet. TCP dumper writes packets to standard output. It is also possible to use TCP dump for the specific purpose of intercepting. It also displays the communication of another user or computer.

E.Packet Filter

It has an attribute payload and two operations classify Traffic into Groups and Separate IRC and HTTP traffic that separates the IRC traffic from the HTTP traffic. Flow Classification Engine class is composed of Flow Based Data Reduction class and Machine Learning Techniques class. In this KDD cup date set with KANN algorithm used to train and filter the packet.

F. Notification

Once any malicious activity is detected by the system it will be indicated and system administrator operators will receive the detailed information immediately. The necessary actions to isolate the access servers or network devices can then be taken.

5. ALGORITHM

Kohonen Artificial Neural Network:

Function of self-organizing of neural network is divided in three stages:

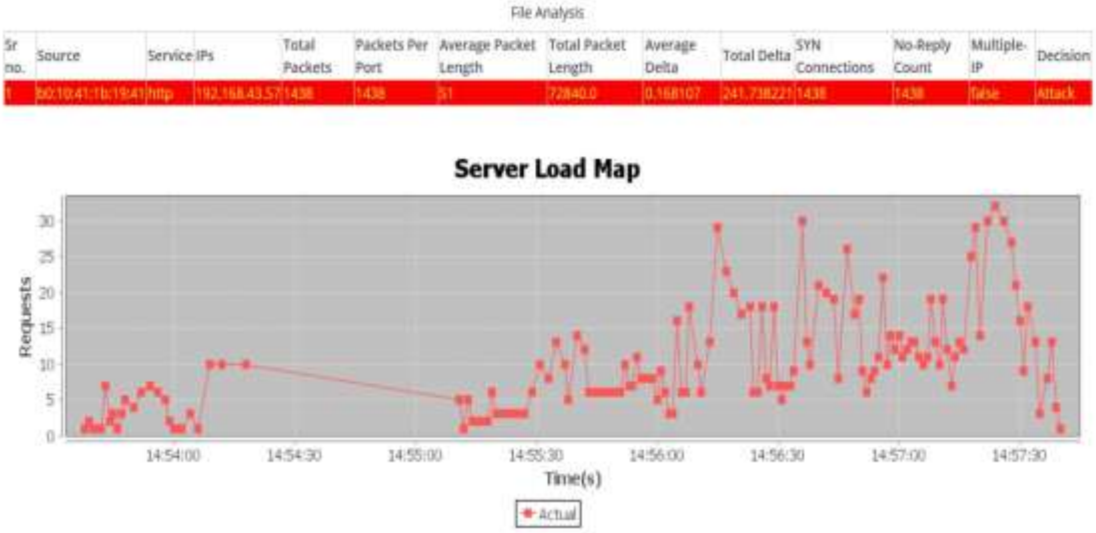
- Construction
- Learning

- Identification

System, which is supposed to catch functioning of self-concerned network, should consist of few basic elements. First of them is a matrix of neurons which are stimulated by input signals. Those signals should describe some attributes of effects which occur in the surrounding. Thanks to that description the net is able to group those effects. Information about events is translated into impulses which copy neurons. Group of signals transferred to every neuron doesn't have to be identical, even its number may be various. However they have to realize one condition: surely define those events.

One more part of the net is a mechanism which defines the stage of comparison of every neuron's wage and input signal. Moreover it assigns the unit with the best match - the winner. At the beginning the wages are small random numbers. It's important that no symmetry may occur. While learning, those wages are being modification in the best way to show an internal structure of input data. However there is a risk that neurons could link with some values before groups are accurately recognized. Finally self-organizing process is that the net is able to suit wages values of leading neuron and his neighbors, according to response strength. Net topology can be defined in a very simple way by determining the neighbors of every neuron. Let's call the unit whose response on stimulation is maximal the image of this incentive. Then we can presume that the net is in order, if topologic relations between input signals and their images are identical.

6. RESULT



File Analysis

Sr no.	Source	Service	IPs	Total Packets	Packets Per Port	Average Packet Length	Total Packet Length	Average Delta	Total Delta	SYN Connections	No-Reply Count	Multiple-IP	Decision
1	b0:10:41:1b:19:41	http	192.168.43.57	1438	1438	51	72840.0	0.168107	241.738221	1438	1438	false	Attack

Figure 3: Result Analysis.

The result in the figure 3 shows that there are 1438 packets received from IP 192.168.43.57 with SYN connections and it no reply with count 1438.So the system has no time to provide ACK to every SYN connection as well delta time is also very less.

Server load map shows the request format with respect to time.

7.CONCLUSION

In this paper application monitors network traffic using Kohonen algorithm. Kohonen algorithm helps for considering different attributes and produces predicted results for packet attributes. This analysis will helps in detect the type of attack and it will notify to the admin.

8. FUTURE WORK

Network is a major part of any organization. So in order to maintain network securely we need to explore each possible vulnerability in the network. So we are going to analyze the number of different possible threats and will try to detect those threats with our application.

9. REFERENCES

[1] A Streaming-Based Network Monitoring and Threat Detection System Zhijiang Chen, Hanlin Zhang, William G. Hatcher, James Nguyen, Wei Yu, 2016.

[2]A Systematic Study on Peer-to-Peer Botnets Ping Wang, Lei Wu, Baber Aslam and CliC. Zou School of Electrical Engineering Computer Science University of Central Florida Orlando, Florida 32816, USA.

[3] An Accurate Threat Detection System through Real-Time Stream Processing Antonio Gonzalez Pastana Lobato, Martin Andreoni Lopez, Otto Carlos M. B. Duarte University-dade Federal do Rio de Janeiro - GTA/COPPE/UFRJ - Rio de Janeiro, Brazil.

[4]Localization Attacks to Internet Threat Monitors: Modeling and Countermeasures Wei Yu, Nan Zhang, Xinwen Fu, Riccardo Bettati, and Wei Zhao, 2008.

10. ACKNOWLEDGEMENT

This research was supported by BMIT College of engineering Solapur. We are thankful to our guide Prof. Shripad Kulkarni who provided his expertise in the areas of our project.