International Journal of Enhanced Research in Management & Computer Applications, ISSN: 2319-7471
Vol. 2 Issue 5, May-2013, pp: (37-42), Available online at: www.erpublications.com

Knowledge Based System for Detection and Prevention of DDoS Attacks using Fuzzy logic

Amit Khajuria[1], Roshan Srivastava[2]

[1]M. Tech Scholar, Computer Science Engineering, Lovely Professional University, Punjab, India
[2]Asst Prof, Computer Science Engineering, Lovely Professional University, Punjab, India

Abstract: DDoS Attacks are associated with numerous challenges like security, performance of system etc where resources are shared by many users. Our research's main aim is to detect and prevent DDoS attacks using Knowledge based system using Neuro Fuzzy Logic. The aim is to provide a proactive DDoS detection and defense mechanism by proposing knowledge based system in Adaptive Neuro Fuzzy Inference System by training the data over true and false data packets in a network. Anfis trains the data and the attack data can be detected from large datasets. This detection system can detect many DDoS attack and prevent the network from attacks.

1.1 Introduction

DDoS may be called an advanced version of DOS in terms of denying the important services running on a server by flooding the destination sever with a large number of packets such that the target server is not able to handle it. If an attacker mounts an attack from a single host it would be classified as a DoS attack. In fact, any attack against availability would be classed as a Denial of Service attack. On the other hand, if an attacker uses many systems to simultaneously launch attacks against a remote host, this would be classified as a DDoS attack .The attackers have the power to control the flow of information by allowing some available at certain times. The DDoS attack is run by three functional units:

A Master

A Slave and

A Victim.

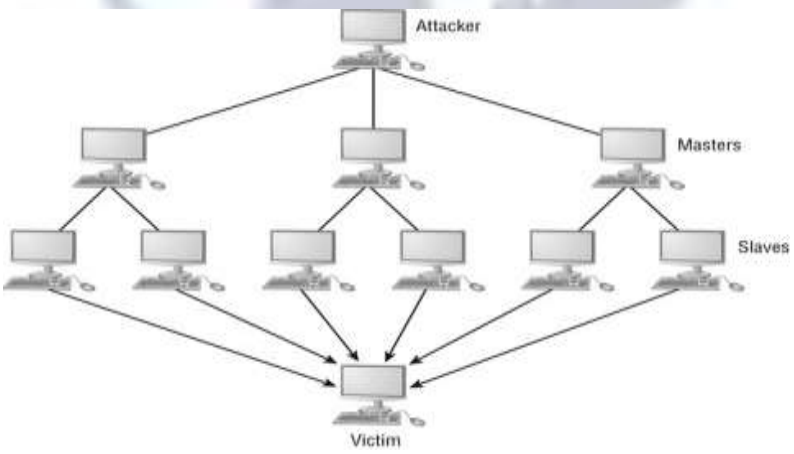

Fig1: DDoS Attack Architecture

1.2 DDoS Attack Classifications

There are two main classes of DDoS attacks:

Bandwidth depletion

Resource depletion

A bandwidth depletion attack is designed to flood the victim network with unwanted traffic that prevents legitimate traffic from reaching the victim system. A resource depletion attack is an attack that is designed to tie up the resources of a victim system. This type of attack targets a server or process at the victim making it unable to legitimate requests for service.

1.3 Knowledge Based System

Knowledge-based expert systems, solves the query that been executed by the human intelligence and use artificial intelligence knowledge to execute the problems. The expert system represents the expertise knowledge as rules within the computer. These rules and data can be called on when needed to solve large problems in real world. Human has to read and interpret the knowledge for it to be used not like the books that has tremendous amount of knowledge. Traditional computer programs perform tasks using conventional decision-making where as logic containing little knowledge other than the basic algorithm for solving that required problem and the necessary boundary conditions. These systems can explain the reasoning process by back-traces and handle the levels of confidence and provide the uncertainty to the conventional programming that can't be handled manually. The program knowledge is often modified as part of the programming code, the program has to be changed and then rebuilt according to the knowledge changes.

1.4 Fuzzy Logic

For this implementation in our paper ANFIS Tool is used to train the data and perform the certain error plotting to check the data for validation Fuzzy Logic is conceptual and easy to learn. The mathematical calculations in Fuzzy Logic are easy to implement and the reasoning behind them is very simple. Fuzzy Logic can implement the external sources without any functionality and starts the work wherever the outer source has been ended, it never discards the previous imprecise values and run again like other computation. Fuzzy builds the understanding into the process rather than tacking it onto the end by carefully inspecting each and every aspect of the problem. It can model the nonlinear data in linear form and brings the meaningful aspects. Even by deploying the random input- output dataset Fuzzy can create a match between them. There are many adaptive techniques that are employed in Fuzzy toolbox and help in generating the relation between the data. Adaptive Neuro-Fuzzy Inference System is one of the main tools in Fuzzy.

2. Implementation

2.1 Data Generation

For this research dataset is gathered from Knowledge Discovery and Data Mining Tools Competition. The dataset was build such that it contains both bad data as well as good data to predict the anomalies in the network and train the system and make it efficient enough to detect the false data and prevent the network. This database contains a standard set of data, which includes a wide variety of packet transferred that been helpful for the research. This properties present how the data been transferred between the producer and consumers.

feature name	description	Type
duration	length (number of seconds) of the connection	Continuous
Protocol type	type of the protocol, etc.	Discrete
service	network service on the destination, e.g., http, telnet, etc.	Discrete
Src bytes	number of data bytes from source to destination	Continuous
Dst bytes	number of data bytes from destination to source	Continuous
flag	normal or error status of the connection	discrete
land	1 if connection is from/to the same host/port; 0 otherwise	Discrete
Wrong fragment	number of ``wrong'' fragments	Continuous
urgent	number of urgent packets	Continuous

2.2 Anfis

The false and true data provides to the fuzzy logic and anfis train the system to distinguish between false and true data. The true data assigns as 1 and false data assigns as -1.

Anfis trains the system for different type of attacks and when the normal data rises, it show the false data and discard them before entering in the secure connections. Anfis build many rules to distinguish between the normal and false data packets and make the system strong.

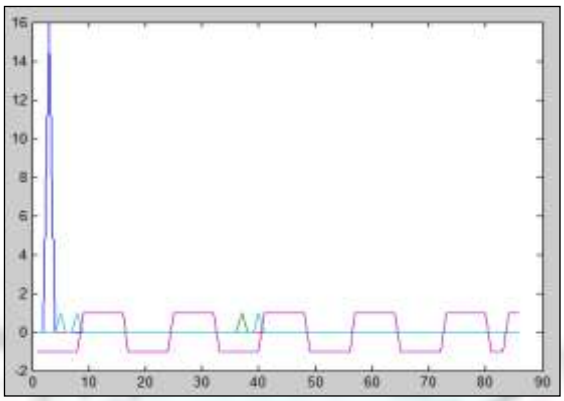

Fig 2.1: Data above line represents true and below is false.

2.3 Fis generation

Fis provide many functions to build the model strong. We can provide many functions to build the system for this thesis I have provided 3 member functions to each input which can produce 3*3*3*3 rules can be made. More or less number of member functions can be provided a system can be built. By providing less member function we can build a rules but they are less and cannot make the system strong enough to distinguish each and every parameter of the input, and if the member functions are more than the rule build are more and system will become complex and will gradually decrease the time efficiency of the model. There are many member functions provided in Fis. For this thesis Gaussmf is used.

2.4 Rule Generation

Rule generation in anfis is made according to the number of input provided. In our thesis we have provide 4 inputs to the anfis and 81 rules are formed, if we provide 5 input then 243 will be generated. According to these rules the data packets will be checked whether they are true or false and the result be generated by calculating the error.

Fig 2.2: 81 Rules Generated

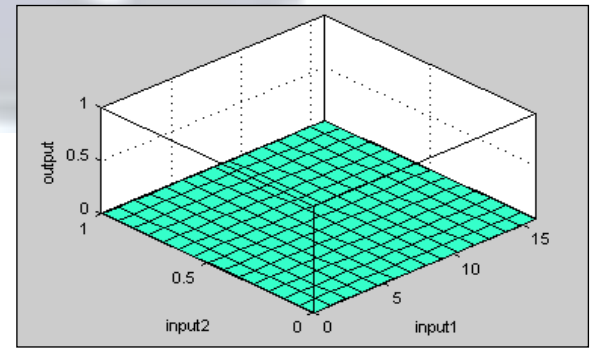

Fig 2.3: Surface Viewer

2.5 Training with Epochs

Different number of epochs been provided to train the data. For every value different error rate come. For this thesis we take 30 epochs and for multiple variations 20 and 40 epochs have been used. Epochs provide the different iterations for the system.

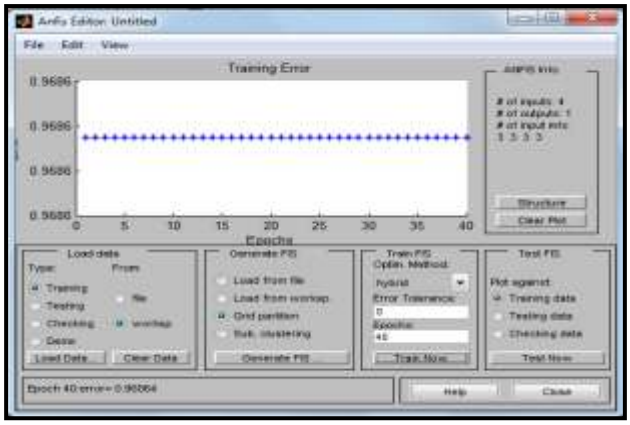

Fig 2.4: training with 30 epochs

Training can be done with using any number of epochs but proper number of epoch will help in reducing the error in training and build our system strong.

2.6 Input Dataset

Dataset used for performing the implementation is very large contains thousands of instances. The dataset contain both true and false data. The dataset contains packet data for many DDoS attacks that commonly occurs in the connections. The dataset is subdivided into sub datasets for different type of DDoS attacks. Each dataset contain different DDoS attack data types and their instances are different. These instances in dataset differ from UDP flood to SYN flood and for all other attack types.

3. Results

Different type of packet data is provided to check the error in the data and detect the false data. The false data can be detected and been discarded by the model. The false data from the normal connection passed through different training set. Different dataset been passed to calculate the efficiency of the model. The false data be representing by -1 and be discarded by the system while the data that is true as 1 will allow to be transmit.

Different error plotting generated using different type of dataset for each scenario. The data packets differ for each attack and also the variations in the graph.

3.1 Error plotting

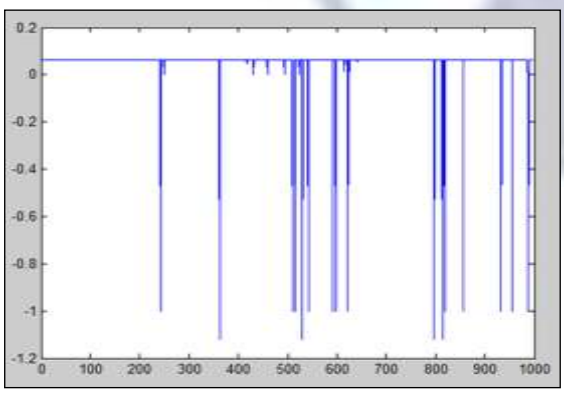

Fig 3.1: Error plotting for Udp flood

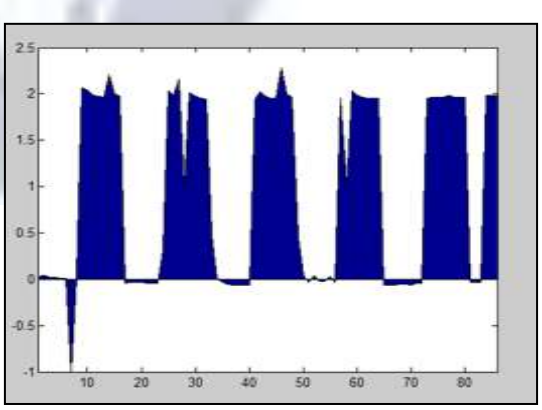

Fig 3.2: Error plotting for each data entry in dataset

For Udp flood attack an error rate of.9688 is noted. This is a great significance of using ANFIS to detect the false data and been discarded gradually by the system.

For ICMP attacks an error rate of .9715 is noted. The figure shown below shows the error plotting for this attack. This dataset contain true data and false data in the same proportion.

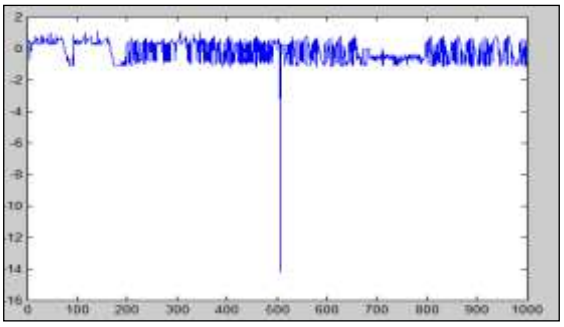

Fig 3.3: Straight line shows proper working

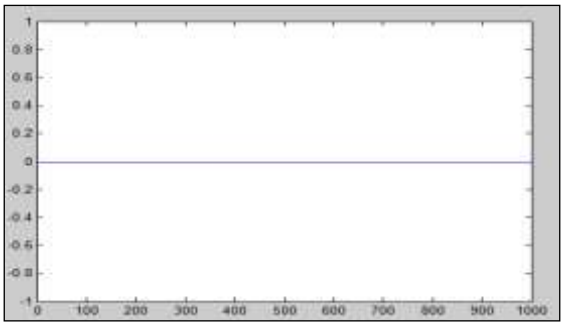

Fig 3.4: True and false data in equal proportion

The datasets in our research contain the initial parameters for the false data packets as well as for the true data packets, so that the graph shows the proper variations For Checking and testing the system, the model is checked for the linear data and shows straight line. This shows no variations in the data packets and the data travel in a secure way. The figure below shows the execution of linear dataset.

Table shows the results for the different type of data packets errors built during our research.

UDP	.9688
ICMP	.97312
SYN flood	.97486
TCP	.86732
Distributed	.91329

4. Simulations

Simulation being built for our research in order to get more information about the working model. The simulations are build over UDP flood data packets. The curve shows that the effect of false data in the dataset. The curve build is on the negative side and represents the false data.

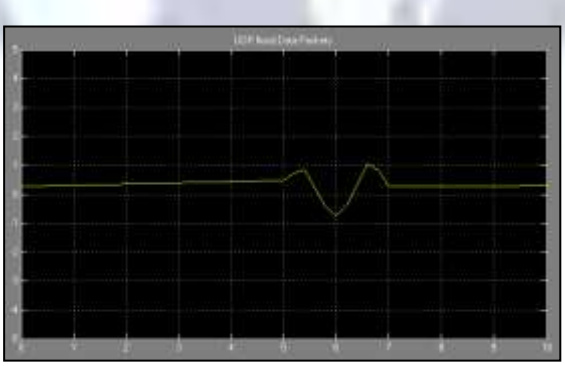

Fig 4.2:Varaition for the data

5. Future work

This is a knowledge based system to detect and prevent the DDoS attack and built in Fuzzy logic. There are certain type of data packets are passed through and been detected. This system is knowledge based and in future more types of data packets can be added to the system to build it more strongly and even large datasets may be used to train the system for detecting the false data. This model currently working on some the main DDoS attack types and more attacks can be added to system to make in strong. Even online testing can also be capable in this system by enhancing it.

6. Conclusion

The aim of this thesis is to detect and prevent the connection from DDoS attacks by knowledge based system using Fuzzy Logic. The whole scenario is built in Adaptive Neuro Fuzzy Inference System. This system provides detection of various DDoS attack and help in securing the connections. The ANFIS training provide less error rate while training the system and helps in detecting smaller data packets also. This system is powerful GUI and can be used at payment gateways to avoid unwanted traffic.

7. References

[1]. Zhengmin Xia, Songnian Lu and Jianhua Li (2010) Enhancing DDoS Flood Attack Detection via Intelligent Fuzzy Logic.
[2]. Ping Du Ping, Xia Ching (2010)" DDOS defense as a network Service".
[3]. Idziorek Joseph, Cowan Elfhard (2011) "Insecurity of cloud utility model".
[4]. Lua Ruiping, Lucy Liu (2011) "Mitigating DDoS Attacks with Transparent and Intelligent Fast-Flux Swarm Network"
[5]. Bhadauria, Ramesh (2010) "Security Issues in Cloud Computing and Associated Mitigation Techniques.
[6]. Kashyap, H. J. and Bhattacharyya, D. K. (2012) A DDoS attack detection mechanism based on protocol specific traffic features.
[7]. Shakeri Baharak, Mohd (2011) "Availability of cloud system under DDOS attacks".
[8]. Kumar(2011) "Improving Network Performance and mitigate DDOS attacks using Analytical Approach under
[9]. Collaborative Software as a Service Cloud Computing Environment".
[10]. Sardana, Anjali (2009) "An auto-responsive honey pot architecture for dynamic resource and QOS adaptation in DDOS attacked networks".
[11]. Srinivas Mukkamala, Andrew H. Sung,(2004) "A Framework for Denial of Service Attacks" IEEE International Conference on Systems, Man and Cybernetics,
[12]. William W. Streilein , David J. Fried, Robert K. Cunningham, "Detecting Flood based Denial-of-Service Attacks with SNMP/RMON" , MIT Lincoln Laboratory.
[13]. Charalampos Patrikakis, Michalis Masikos, and Olga Zouraraki , "Distributed Denial of Service Attacks", National Technical University of Athens,
[14]. Michael Negnevitsky(2008) "Artificial Intelligence: A Guide to Intelligent Systems.
[15]. Zhang, G., Jiang, S., Wei, G., and Guan, Q. (2009) A prediction-based detection algorithm against distributed denial-of-service attacks.
[16]. Xia, Z., Lu, S., Li, J., and Tang, J. (2010) Enhancing DDoS flood attack detection via intelligent fuzzy logic.
[17]. Yu, S., Zhou, W., Doss, R., and Jia, W. (2011) Traceback of DDoS attacks using entropy variations.
[18]. Nguyen, H.-V. and Choi, Y. (2010) Proactive detection of DDoS attacks utilizing k-NN classifier in an Anti-DDoS framework.