AN EFFICIENT METHOD FOR DENIAL OF SERVICE ATTACK DETECTION USING GENETIC ALGORITHM

L.K. Siva Sankari[1], Dr. D. C. Joy Winnie Wise[2], B. Priya [3]

PG Scholar[1], Professor and Head[2], Assistant Professor[3]

Department of Computer Science and Engineering

Francis Xavier Engineering College ,Tirunelveli (India)

ABSTRACT

At the present time, it is very vital to maintain a high level security to make certain harmless and reliable communication of information between various institutions. In Highly Active Networks, the occurrence of disruptive or suspected Network Attacks leads to enormous destruction of data. Denial of Service Attack Detection System aims at observing the attacks on the Internet from normal use of it. It is a crucial part of the network security system. The new guard system is suitable for efficient implementation for the detection of Denial of Service (DoS) attacks. The proposed method presents a Genetic Algorithm (GA) to detect the Denial of Service attacks. A DoS attack is a type of attack in which the intruder makes the system resources too busy to reject other users from accessing. The Genetic Algorithm enables to learn something for themselves that initiates the process of natural Selection. It is used to generate practical resolution for making the solution as a perfect. The GA uses a development process that contains the selection, crossover and mutation techniques to identify the DoS attacks. This detection approach is very accurate and efficient in the detection of DoS. The proposed system achieves a better performance. By using this algorithm, the detection of the attack is very efficient.

Index Terms: Denial of Service Attack, Genetic Algorithm, Normalization

I. INTRODUCTION

A Denial-of-Service (DoS) attack is a test to make a device or network resource engaged to its planned users. Although the means to carry out to motives for the targets of a DoS attack vary and it generally contains the efforts to provisionally or indefinitely break off or delay services of a host connected to the Internet.

The Perpetrators of DoS attacks are typically destination sites or services hosted on prestigious web servers for e.g. credit card payment gateways, banks and even root name servers. Denial-of-service threats are also frequent in business and are sometimes dependable for website attacks.

One of the common methods of attack involves inundation of the target machine with external communications requests so much so that it cannot respond to legitimate traffic or responds so slowly as to be yielded basically unavailable. Sometimes the attacks are usually led to a server burden. DoS attack can be implemented by either forcing the destination computer to rearrange or disobedient its resources so that it cannot provide its proposed service or blocking the contact media between the proposed users and the injured party cannot communicate adequately.

Denial-of-service attacks are considered as an abuse of the Internet Architecture Board's Internet appropriate use policy and go against the acceptable use policies of nearly all Internet service providers. A wireless sensor network (WSN) of spatially distributed independent sensors to supervise corporal or environmental conditions such as the temperature, sound, pressure, etc. and to kindly pass their information through the network to a main location. Mostly the modern networks are bi-directional and also to make operational control of sensor activity.

The improvement of wireless sensor networks was provoked by military applications such as battlefield observation, and some other networks are used in many consumer applications are industrial process monitoring, machine health monitoring, and so on.

In the field of artificial intelligence in a computer science a Genetic Algorithm (GA) enables to learn something for themselves that imitate closely the process of natural selection. This is also sometimes called a meta heuristic and is routinely used to generate the constructive solutions to search problems. Genetic algorithms are belong to the outsized class of enlargement algorithms which produce solutions to optimization problems using methods that are inspired by natural development like that mutation, selection and crossover. Genetic algorithms are find application in bioinformatics and other fields.

In an arithmetic approach, it is used to analysis the sharing of network traffic to recognize the normal network traffic behavior is planned. The algorithm is used as the distribution parameter of Gaussian mixture distribution model. It also suggests a method to recognize anomalies in network traffic is based on a non classified α-stable first-order model and statistical suggestion testing.

In other case, classification of anomaly based intrusion detection is presented. Different techniques are used in Anomaly based IDS like the Statistical anomaly detection, Knowledge based detection, Data-mining based detection, and Machine learning based detection. Statistical modeling is used for detecting intrusions in electronic information systems.

In a paper, a Network Intrusion Detection using SNORT is presented. The Snort is open source network intrusion avoidance and the discovery system. It is used mainly to monitor network traffic and generate alerts when threats are detected.

In Existing, Multivariate Correlation Analysis (MCA) systems are used to detect the attacks. The attacks are detected based on the principle of abnormality based detection in attack recognition, by checking network activities. The major limitation is a more complicated and labor severe task. It cannot manage fully exploit relationships. To avoid this limitation this paper proposed the genetic algorithm for DoS detection.

Genetic Algorithms is mainly based on production of rules to detect denial of service attacks on the system. It is very accurate method and efficient. The rest of this paper discussed about details of the proposed methodology.

II.METHODOLOGY

In this chapter discuss about the proposed methods in detail. The Diagram shows the process of proposed system.

This is the First Step to Detect the Denial of Service Attack. A DataSet is stored with Protocol, SourceIP, Source port, Destination IP, Destination port, Packet size, Action, Time. Then the Dataset is Split into two Phases. They are Testing Phase and Training Phase. The Training Phase acts as a pattern to detect the Denial of Service Attack for the Testing Phase.
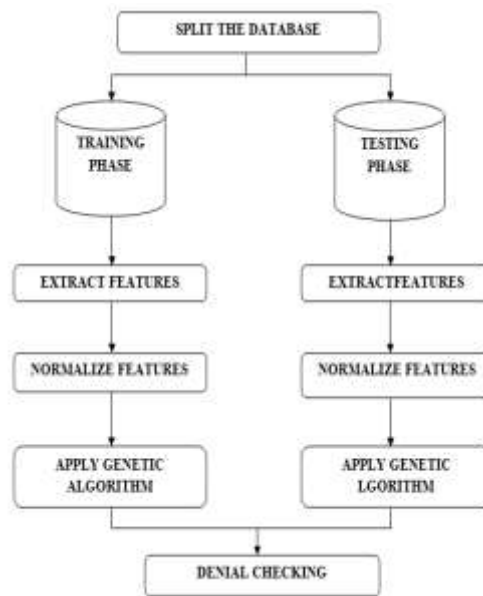
Fig: 2.1 The Overall diagram of proposed method.

The Dataset contents are now extracted for the detection of Denial of Service attack. The Features which are needed are SourceIP, DestinationIP, Action, Packet size, Time. After extracting the features, the data are stored into Separate table.

2.1 Normalization

From the Extracted features, the normalization step takes place. Normalization is performed with the Initial population. The Action performed is taken in case, to place the status that request accepted and reply received. Using this Normalized status is calculated.

2.2 Initialize Population

Initially many individual solutions are randomly generated to form an initial population. The population size is depends on nature of the trouble but naturally includes hundreds or thousands of possible solutions. In common the population is generated randomly that allowing the entire range of possible solutions. The solutions are the starting point in areas where best possible solutions are likely to be found.

The process starts from an initial population of at random produced individuals. The population is evolved by the number of generations while increasingly improving the behavior of the individuals by increasing the fitness value as the measure of quality.

Genetic Algorithm

2.3 Selection

During the generation of selection, cross over, and mutation are one after the other applied to each individual with certain qualities. Initially, the numbers of best-fit individuals are selected based on a user-defined fitness function. The remaining entities are selected and paired with each other. Each individual pair produces the one young entity by moderately give up for their genes around one or more randomly selected crossing points. Finally, a certain number of entities are selected and the mutation operations are applied. In the selection phase where population individuals with better fitness are selected otherwise it gets damaged.

2.4 Crossover

A Crossover operator is used to form new strings to obtain a better string. The process creates different individuals in the consecutive generations by joining material from two individuals of the earlier generation. The two strings involved in the crossover operation are known as parent and the follow-on strings are known as children strings. The crossover operator rejoins good sub-strings from good strings together optimistically to create an enhanced substring. Crossover is a process where each couple of entities selects accidentally participates in exchanging their parents with each other until a total new population has been generated.

2.5 Mutation

Mutation adds new data in a random way to the genetic process and eventually helps to avoid getting fascinated. Every time the population tends to become standardized, it is a hand that introduced the diversity in the population due to repeated use of reproduction and crossover operators. Mutation is the process of randomly disappointing genetic information. When the bits are being copied from the existing string to the new string, it operates at the bit point and there is chance that each bit may become changed. The probability of mutation usually a reasonable small value is called as mutation probability. The mutation operator alters a string in the vicinity expecting a better string.

III.CONCLUSION AND FUTURE WORK

In Networks, Security became an essential one. Several attacks occur in the network. DoS attack is one of the deadly attack. The proposed method developed a Genetic Algorithm or the Detection of denial of service attack. This method is effective and not a time consuming. The Dataset which stores the internal details of packet transmission in the network helps us in this algorithm. This method will be very constructive for the attack detection in today's changing attack methodologies. If the systems are updated dynamically with the data, then this method will be very effective. Thus the detection of DoS attack can be performed successfully.

Several future research directions can be investigated. In future, shall make use the classification techniques. The prevention mechanism may be handled. This project can also be extended as real world application.

REFERENCES

[1] Z. Tan, A. Jamdagni, X. He, P. Nanda, and R.P. Liu, "Denial-of- Service Attack Detection Based on Multivariate Correlation Analysis," *Proc. Conf. Neural Information Processing,* pp. 756-765, 2011.

[2] Yu J., Lee H., Kim M. –S. and Park D. (2008), "Traffic Flooding Attack Detection with SNMP MIB Using SVM," *Computer Comm.*, Vol. 31, No. 17, pp. 4212-4219.

[3] Garca-Teodoro P., Daz-Verdejo J., Maci-Fernndez G. and Vzquez E. (2009), "Anomaly-Based Network Intrusion Detection: Techniques, Systems and Challenges," *Computers and Security*, Vol. 28, pp. 18-28.

[4] D.E. Denning, "An Intrusion-Detection Model," *IEEE Trans. Software Eng.*, vol. TSE-13, no. 2, pp. 222-232, Feb. 1987.

[5] Hu W., Hu W. and Maybank S. (2008), "AdaBoost-Based Algorithm for Network Intrusion Detection," *IEEE Trans. Systems, Man, and Cybernetics Part B*, Vol. 38, No. 2, pp. 577-583.

[6] Lee K., Kim J., Kwon K. H., Han Y. and Kim S. (2008) , "DDoS Attack Detection Method Using Cluster Analysis," *Expert Systems with Applications,* Vol. 34, No. 3, pp. 1659-1665.