Bandwidth based Distributed Denial of Service Attack Detection using Artificial Immune System

[1]M.Yasodha, [2]S. Umarani

[1]PG Scholar, Department of Information Technology, Maharaja Engineering College, Coimbatore

[2]Assistant Professor, Department of Information Technology, Maharaja Engineering College, Coimbatore

Abstract: Distributed Denial of Service (DDoS) attack cause a serious threat to the security of the network. There are two kinds of DDoS attack: Bandwidth dependent DDoS attack and resource consumption dependent DDoS attack. The Bandwidth dependent DDoS attack intrudes the network operation by creating congestion in the network by transmitting huge volume of traffic. Thus in this paper an efficient attack detection model has been proposed which analyses the traffic flow in the network and based on this information an artificial immune system is developed to classify the traffic into normal traffic and attack traffic. Simulations are performed to evaluate the effectiveness of the proposed approach.

Keywords: DDoS, Bandwidth based DDoS, Artificial Immune System.

Reference to this paper should be made as follows: [1]M.Yasodha, [2]S. Umarani (2015) 'Bandwidth based Distributed Denial of Service Attack Detection using Artificial Immune System ', *International Journal of Inventions in Computer Science and Engineering*, Volume 2 Issue 6 June 2015.

1 Introduction

A denial of service attack is described as a comprehensive attempt made by an attacker to stop genuine users from utilizing the preferred services. The distributed setup includes the "many-to-one" aspect that causes these attacks to be more challenging to prevent. A distributed denial of service (DDoS) attack constitutes four components: victim, daemon agents, control master program and the real attacker. A victim is an intended host that has been selected to receive the impact of the attack. A daemon agent is an agent program that executes the attack on the intended recipient [1]. The attack daemons are generally installed on the host computers. These daemons influence both the host and the target system. The process of installing the daemons needs the attacker to acquire access and penetrate the host systems [2]. The job of control master program is to handle the attack. Finally, the legitimate attacker utilizing this control master program stays behind the happenings of the attack.

Basically there are two kinds of attack practices accompanied by DDoS attack: bandwidth and the resource consumption DDoS attack. In bandwidth consumption DDoS attack, the aggressive traffic introduced by the negotiated hosts that are controlled by the hackers are combined into a single huge flood that devastates the victim [3]. During resource consumption DDoS attack, the hackers leak the network protocol or system security such as the methods of Teardrop, land and SYN flood. This results in system resource starvation [4]. According to a recent survey, the bandwidth DDoS attack is the most widely utilized DoS approach. Most bandwidth DDoS attacks are based on a simple notion: flooding and reflection. Flooding attacks creates a substantial damage as the attacker employs adequate number of agents to cause huge bandwidth consumption resulting in packet loss .

It is challenging to safeguard a system after the attacker has launched the DDoS attack. Thus, it is imperative to identify the DDoS attack in earlier stage. Thus our paper focuses on the early identification of DDoS attack. Here, an efficient attack detection model has been proposed which analyses the traffic flow (number of packets, number of octets and number of flows) in the networkand based on this information an artificial immune system is developed to classify the traffic into normal traffic and attack traffic.

II. Related Works

In paper[5] proposed a detection system for the DoS attack using multivariate correlation analysis (MCA) for classifying the network traffics by mining the geometric correlation features of the network.In this the (MCA) classification uses anomaly based detection for recognition of the DOs attacks. For improving the performance of the system they used a triangle-area-based technique .Additionally they compared the technique with KDD Cup 99 data set,to examine the performance and accuracy of system.

In [6] a push back scheme has been used to defend against Distributed Denial-of-Service (DDoS) attacks. To detect the presence of attacker, the target server delivers a puzzle that disseminates the traffic. When the client is capable of solving the puzzle, it is considered as a genuine traffic and is permitted into the server.

The author [7] suggests a prevention and detection system of DDoS attack which is fitted in the leaf router to watch and prevent the DDoS attacks. This leads to less overhead that brings more immune strength to overcome from the

attacks. Since the synchronization is a concern for the sender and receiver in terms of traffic, in order to detect the synchronization of flooding attack, a new non- parametric CUSUM algorithm is executed. Then a fast identification technique is utilized to recognize the normal users from the attackers and forward the IP packets. The experimental results of the proposed system is compared with the existing system and that shows that the proposed system identifies the attacks in early stage and take appropriate steps to resolve the attacks.

Internet stability is interfered with the dangerous outcome of Distributed denial of service attack (DDoS). the examination of current DDOS attack detection techniques and approaches are presented in [8]. Futhermore, the author presents a data mining algorithm based DDoS attack detection model. The network packet protocol status model and the net traffic model is extracted using the apriority and FCM algorithm. The experimental results bring promising results among the DDoS attack detection models.

In [9] anomaly traffic detection is carried out depending on the features of the network and a support vector machine based classifier has been employed to detect the attacker presence.

III. Proposed Ddos Detection Model

Bandwidth based DDoS attack causes bottleneck in the network with huge traffic flow. This type of attacks may damage or degrade the link between the target networks (or) self-directed systems and the internet. The DDOs attacks can be done with agents and handlers selection and communication of information. Thus it is necessary to detect the DDOs attack to avoid performance degradation in the network. For the attack detection, we proposed a method using artificial immune system classifier for classifying the networks traffics as normal or attack based on network traffic features. In this detection system, the features like Entropy of port number and IP address of the destination and source, entropy and occurrence rate of type of the packets (ICMP, UDP, and TCP) and total packets that is being transferred are gathered from the network and are processed and passed to distinct the traffic type.

The status about the traffic types are stored in the database from which are passed as a trained data to artificial immune system classifier to classify the networks with normal (or) attack traffic. From this attacksare detected with less computation time, more accuracy and negligible error rate. Fig 1 shows the proposed detection model for DDOs attack.

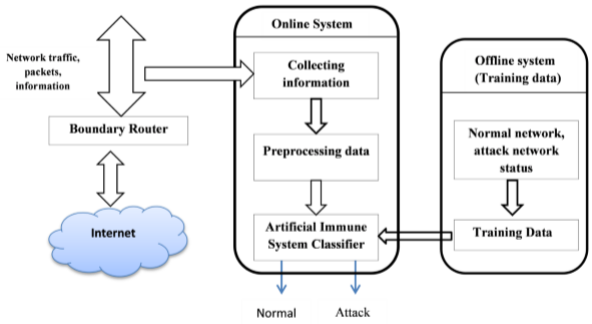

Fig 1 Proposed DDOs detection model

IV. Artificial Immune System Based Method For Ddos Attack Detection

Our proposed attack detection model extracts the features like Entropy of port number and IP address of the destination and source, entropy and occurrence rate of type of the packets (ICMP, UDP, and TCP) and total packets that is being transferred are gathered from the network.T

The extracted features are fed to the AIS classifier to classify the traffic as normal traffic or attack traffic.

A. Feature Selection For Ddos Detection

The features mainly considered for the DDOS detection are as follows:

1. Entropy of destination IP address and port number
2. Entropy of packet type
3. Entropy of source IP address and port number
4. Number of packets
5. Occurrence rate of packet type (ICMP, UDP, and TCP).

Basically the attacker, distribute the packets in the network in order to infringe and gain access of the machine with security frailty. The attacker can also modify the datagram which supports protocols like ICMP, UDP, and TCP andpasses to the network in which IP address of source and destination plays important forpackets transmission. In order to trace the changes in the entropy is introduced.

The entropy can be calculated by H,

$$H = \sum_{i=1}^{n} P_i log_2 P_i$$

Where,

Pi=Probability of choice

n=independent symbols

When the entropy is introduced the occurrence rate of source and destination IP address interchangeably increases and decreases. Thus to detect that occurrence rate is the measured for detecting of the DDOs attack initialization also calculated. Additionally the entropy of packet type also analyzed for specifying the flooding attacks of various protocols.

B. Artificial Immune System Classifier

The Artificial Immune System (AIS) based classification [3] is simulated by the features derived from the network[10]. The features like destination IP address, source IP number, packet type, port number are considered. For the classification, two types of datas are considered as normal or attack.

In AIS engine, the features values are transformed into binary strings of length 134 with zero padding where needed. The maximum and minimum values of the fields and the binary string length are listed in the table 1.

Table 1 Minimum and Maximum Values of Fields

Name of the Field	Minimum and Maximum Value	Binary Strings Length
Destination IP Address	0.0.0.0 - 255.255.255.255	38 bits
Source IP Address	0.0.0.0 - 255.255.255.255	38 bits
Destination Port No	0 – 65535	16 bits
Duration	0 – 999 seconds	10 bits
Protocol	0 – 65535	16 bits
Source Port No	0 – 65535	16 bits

Training phase

The set ofbinary strings that are converted randomly are trained to differentiate as normal or attack in network. For training we use Negative Selection algorithm for filtering the normal traffic and the attack in the network. The filtering process uses difference of the pattern matching algorithm refers r-CB (Contiguous bits) algorithm. It drops the traffic that correlates with the normal value and then generates other network packets transmission in its place. Then same algorithm is used for training the attacks in the network. In that relationship between the varying binary string and randomly created binary string are evaluated until the threshold limit.

Testing phase

After the training process is completed, the fitness value concept is used to differentiate the normal and the attack based on threshold value. If the value exceeded the threshold limit that it is said to be attack in the network. It the value in the database matches with the randomly generated binary string it is said to be the normal traffic in thenetwork.Fig2showstheAISengine.

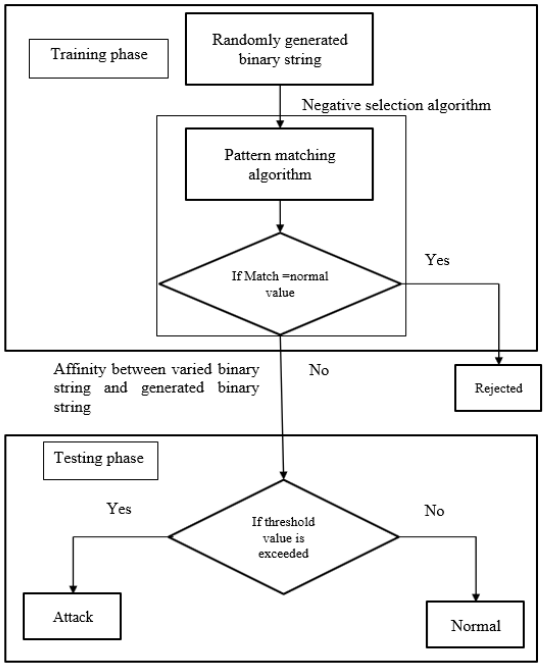

Fig 2 AIS Engine

V. Result Analysis

For result analysis, we consider 100 test elements for estimating the accuracy and error rate of the Artificial Immune System and kNN Classifier algorithm. The accuracy of the Artificial Immune System for normal traffic is same for the both type of the classifiers. As been observed that, our proposed system has accuracy of 99.75% and has less error rate of 0.25%.In kNN classifier method, the accuracy for detecting attacks is less and their error rate also higher than the proposed system.It proves that our proposed classfier method detects the attack in networks approximately that theexisting classifier method .Table 2 shows the accuracy and Error rate of the Artificial Immune System and kNN Classifier algorithm.

Table 2 Accuracy and Error rate of the Artificial Immune System and kNN Classifier algorithm.

Network class	Overall Accuracy		Overall Error rate (%)	
	AIS	kNN	AIS	kNN
Normal	100	100	100	0
Attack	99.68	98.84	0.32	1.15

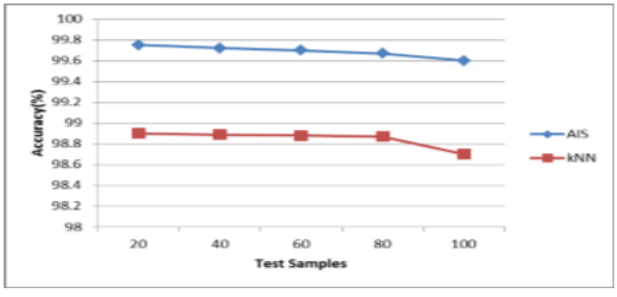

Fig 3 Accuracy

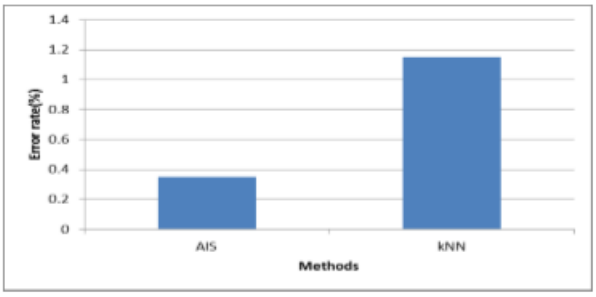

Fig 4 Error Rate

A .Computational Time

Fig 5 describes the computational time of the Artificial Immune System and kNN Classifier algorithm. The time requires for classification of the normal and attacks is little higher in kNN than Artificial Immune System due to the similarity degree computation and also vector space model.

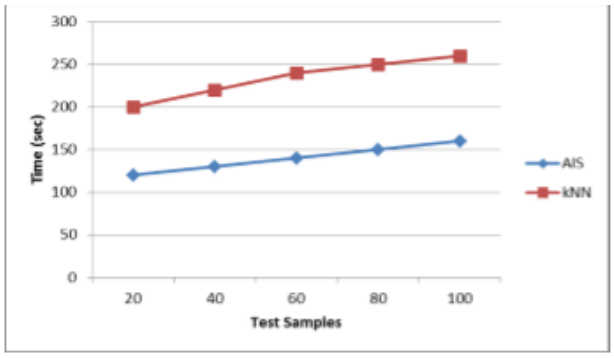

Fig 5 computational time

VI. Conclusion

We proposed a detection method for DDOs attacks in the network using Artificial Immune System classifier. This method can be implemented on the network for detecting the networks traffics as normal and attack. Many attack detection methods are introduced but they lacks in detecting the accurate class of traffic. The AIS based classifier method classifies the traffic as normal or attack based on the features like port address, IP address and packet type. Moreover our proposed system proved it has better accuracy and less error rate than the existing classification methods. Additionally being simple method it provides packets transmission with less computational time.

References

[1]Hoai-Vu Nguyen and Yongsun Choi, "Proactive Detection of DDoS Attacks Utilizing k-NN Classifier in an Anti-DDos Framework", International Scholarly and Scientific Research & Innovation,2010.

[2]Moti Geva, Amir Herzberg, andYehoshua Gev, "Bandwidth Distributed Denial ofService: Attacks and Defenses", IEEE Computer and Reliability Societies,2014.

[3] Wesam Bhaya, Mehdi Ebady Mana, "AProactive DDoS Atack Detection Approach Using Data Mining Cluster Analysis", Journal of Next Generation Information Technology,2014.

[4] Kanwal Garg , Rshma Chawla ,"Detection Of DDOS Attacks using Data Mining", International Journal of Computing and Business Research, 2011.

[5]Zhiyuan Tan , ArunaJamdagni ,Xiangjian He , Priyadarsi Nanda , Ren Ping Liu ," A System for Denial-of-Service Attack Detection Based on Multivariate Correlation Analysis,"IEEE Transactions on Parallel & Distributed Systems ,pp: 447-456, vol.25, Issue 02, 2014.

[6]Saravanankumarasamy and .R.Asokan, "Distributed Denial of Service (DDOS) Attacks Detection Mechanism", International Journal of Computer Science, Engineering and Information Technology, 2011.

[7]Yi Zhang, Qiang Liu ; Guofeng Zhao A real-time DDoS attack detection and prevention system based on per-IP traffic behavioral analysis, IEEE International Conference On Computer Science and Information Technology (ICCSIT), VOL 2,2010.

[8]RuiZhong and GuangxueYue "DDoS Detection System Based on Data Mining" ,Proceedings of the Second International Symposium on Networking and Network Security (ISNNS '10) Jinggangshan, P. R. China, 2-4, pp. 062-065, April2010.

[9]BasantAgarwal , Namita Mittal, "Hybrid Approach for Detection of Anomaly Network Traffic using Data Mining Techniques", Procedia Technology, 2012.

[10]Kevin Leung, France Cheong, and Christopher Cheong,"Generating Compact Classifier Systems Using a Simple Artificial Immune System", IEEE Transactions on Systems, Man, and Cybernetics,2007.