An Optimized Technique for Detection and Prevention of DDoS Attacks using GA and BPNN

Harpinder Kaur[1], Dr. Bikrampal Kaur[2]
[1]*M.Tech Scholar,* [2]*Professor*
CSE department, Chandigarh Engineering College, Landran

Abstract - Distributed denial-of-service attack (DDoS Attack) is one of the kinds of attacks that use multiple hosts as attacker against a system. There is dissimilarity between Distributed Denial-of-Service (DDoS Attack) and Denial-of-Service (DoS Attack). DDoS attacks are spread, meaning spread by multiple hosts, while the DoS attack is one-on-one. DoS attacks require a powerful host, either from the source or operating system used to carry out the attack. . DDoS attacks are thrown by generating a tremendously large quantity of traffics and they quickly tire resources of target systems, such as system bandwidth and computing control. In this study, we debate how to handle DDoS attacks in the form of discovery method based on the pattern of flow entries and handling mechanism by layered firewall. In proposed work to detection mechanism is proposed to detect DDoS attacks by Genetic Algorithm and prevention using Back Propagation Neural Network. The Genetic Procedure is a model of machine knowledge which derives its performance from image of the processes of Evolution in environment. Apply the optimization technique to detect the attack and classification technique for prevention using Back Propagation Neural Network. Back propagation network has two stages, training and testing. During the training time, the network is "shown" sample contributions and the correct classifications. It will generate the two modules in the single network according to weight and bias. The First Module is the Training part and second one is Testing or analysis of the training module. Evaluate the performance parameters like Energy Consumption, Packet sent, Throughput and Bit Error Rate. Compare the performance parameters of proposed work and previous work.

Keywords - DDoSAttack, Genetic algorithm, Back propagation Neural Network, Cyber Security and Optimized performance parameters.

I. INTRODUCTION

Today network security is most common problem for whole world. Because so many problems are occur in our network security systems .so maintaining the information is very difficult and big issue. With these problems some interrupts can occur on the local system or network based system. Without security measures and controls in place our data might be subjected to an attack. Now a day's several attacks are evolve [1]. The Dos attack is the most popular attack in network and internet. DDoS attack has caused severe damage to servers and will cause even greater intimidation to the growth of new internet services. Traditionally, DDoS attacks are carried out at the network layer, such as ICMP flooding, SYN flooding, and UDP flooding, which are call Network layer DDoS attacks [2]. In Application layer DDoS attacks zombies attack the injured party web servers through HTTP GET requests (e.g., HTTP Flooding) and pulling large picture files from the sufferer server in overwhelming numbers. A DDoS attack has two stages named deployment and attack. In this attack program must first be deployed on one or more compromised hosts before an attack is possible. A DDoS attacker uses several computers to launch a coordinated DDoS attack against one or many targets. Then attack is launched indirectly by many compromised computing systems by sending a stream of useless aggregate traffic meant to explode victim property. As a side effect these attacks regularly create network congestion on the way from a source to the main point or target thus disrupting normal Internet operations. Figure 2 shows the DDoS attack process and components [3]. Intruder can perform DDoS attack either as flooding attack or as logical attack. In flooding DDoS attack, massive quantity of legitimate looking data packets are sent to victims, with the aim of decreasing legitimate users' bandwidth, thereby preventing allowed users from accessing a service. Logical attack uses a precise feature of the rules or the application installed at the target machine so as to consume an excess quantity of its resources[4]. The major motives behind DDoS attack could be criminal, commercial, or ideological in nature.A usual DDoS attack structure is explain in Figure 1. [5]

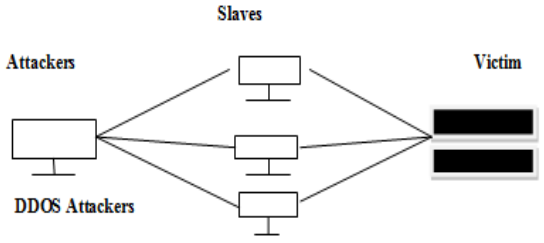

Fig.1: DDoS Attack Structure

Distributed Denial of Service attacks have posed a massive hazard to the Internet. Researching development of recognition and doubt against DDoS attacks results in not only the advance of data security systems, but also continually attack tools enhanced by skilled attacker in order to avoid these safety systems. Various DDoS attack tools

and their late publications come to the fore and DDoS field quickly becomes more and more difficult. Thus, it is of huge implication to state DDoS attack in an abstract and formal method and to categorize them in a scalable classification [6].

Distributed Denial of Service attack comes under Cyber security is the body of technologies, processes and practices considered to protect system, computers, agenda and data from attack, break or unauthorized admission. In a compute situation, the term safety implies cyber safety. Organization and user's assets include connected computing strategy, personnel, transportation, submission, services, telecommunications systems, and the totality of transmitted & stored data in the cyber atmosphere. Cyber security strives to ensure the achievement& maintenance of the safety property of the organization and user's assets against relevant security risks in the cyber atmosphere. The general safety objectives comprise the following:

- Availability
- Integrity,
- Authenticity
- Non-repudiation [7].

Cyber security involves protecting that information by preventing, identify and responding to theattacks.

In proposed work we implement the Genetic algorithm for attack detection with the help of fitness function.Genetic algorithm in computer programs that simulator the procedures of natural evolution in arrange to solve complexity and to model evolutionary systems.Different types of three operators: (i) The selection operator selects those chromosomes in the populace that will be allowed to duplicate with better chromosomes creating on average more spring than less ones. (ii) Crossover exchanges subparts of two chromosomes, roughly replicating organic re-combination among 2 single gene organismsand ; (iii) Mutation casually changes the allele values of some positions in the chromosome; and transposal reverses the order of a connecting section of the chromosome, thus re-arranging the order in which genes are organised [8].

Secondly, implement the prevention technique used for back propagation neural network.Usually, the Back propagation network has two stages, training and testing. During the training time, the network is "shown" sample contributions and the correct classifications. For example, the input might be an encoded request to web server and application server, and the production could be represented by a code that corresponds to the name of the network or server.

II. RELATED WORK

SarraAlqahtani et.al; 2015[9] described the scalability and dynamic configuration of service clouds can be susceptible to Distributed Denial of Service (DDoS) attacks. The attack on web services happen a performance decrease in the cloud applications or can shut them down. This paper advocates a DDoS attack detection method for service clouds and improves efficient algorithms to resolve the originating service for the attack.**MeghnaChhabra et.al; 2014 [10]** The purpose of this study was to understand the flaws of existing solutions to combat the DDoS attack and a novel scheme was being provided with its validation to reduce the effect of DDoS attack in MANET Environment. As Internet users are increasing day through day, it is becoming more prone to attacks and new hacking techniques.**Monowar H. Bhuyan et.al;[11]** In this paper empirically evaluate many information metrics, namely, Hartley entropy, Shannonentropy, Renyi's entropy and Comprehensive entropy in their capabilityto detect low-rate DDoS attacks. These metrics can be used todescribe characteristics of network traffic and an appropriatemetric facilitates structure an effective model to detect low-rateDDoS attacks. And use MIT Lincoln Laboratory and CAIDADDoS datasets to illustrate the efficacy and effectiveness of eachmetric for detecting mainly low-rate DDoS attacks. **Christos Douligeris et.al; 2004 [12]** the Denial of Service (DoS) attacks constitute one of the major threats and among the hardest security problems in Internet. This paper presents a structural approach to the DDoSProblem through developing a classification of DDoS attacks and DDoS defense mechanisms. Furthermore, main features of each attack and security system category are defined and compensations and disadvantages of each proposed scheme are outlined. The aim of the paper is to place less order into the existing attack and defense apparatuses, so that a better understanding of DDoS attacks can be achieved and subsequently more efficient and actual algorithms, methods and procedures to combat these attacks may be developed.**Ahmad Sanmorino et.al 2013 [13]**the distributed denial-of-service attack (DDoS Attack) was one of the kind of attacks that use multiple hosts as attacker against a system. There was a difference amid DistributedDenial-of-Service (DDoS Attack) and Denial-of-Service (DoSAttack). In this study discuss howto handle DDoS attacks in the form of detection method based onthe pattern of flow entries and handling mechanism using layeredfirewall.

III. DDOS ATTACK IN WEB SERVER FACTS AND FIGURES

Distributed denial of service operations remains one of the most popular types of attack, according to a statement from Kaspersky Labs. The occurrences are relatively simple to orchestrate, and extremely difficult to defend against, making them one of the most favoured tools for an attacker, be they a nation-state like China or an activistset like Anonymous.DDoS attacks are used to interrupt a computer network's ability to function by flooding it with information, thus rejecting service to authentic users. DDoS attacks are also highly under-reported, according to Kaspersky's research.Kaspersky intelligences the following data on DDoS attacks from the second quarter of this year [14]:

- ***Figures:*** The longest DDoS attack persisted 60 days, 1 hour, 21 minutes and 9 seconds. The highest number of DDoS attacks against a single site was 218.
- ***Attacks by Country:*** 89% of DDoS traffic was generated in 23 countries. The US & Indonesia complete up a combined 11% of attack traffic [15].

IV. PROPOSED AND RESULT ANALYSIS

The proposed work steps explained in below: Initialize the server scenarios or network architecture.Deploy the nodes or you can say create users, application server and web server.User sent the request of the Web Server if Web server is free then accepts the Request then further request sends the application server. Application Server reverts back to the Web server then web server reply the user. Whenever, it could send the request of the web server. Web server creates the unique identity of the web server which is called as session. Information transfer user to web server and web server to application server. Attacker will come and hack the information means server will be down or increase the delay and overload of the server.Apply the Genetic Algorithm for Detect the DDoS Attack and performance define through the parameters like through put, packet sent etc. In Genetic Procedure is a model of machine knowledge which derives its performance from image of the processes of Development in environment. This is done by the establishment within a machine of a Populace of Individuals represented by Chromosomes, in spirit a set of character strings that are similar to the base-4 chromosomes that we see in our own DNA. The individuals in the populace then go through a process of evolution.Apply the classification technique using Back propagation Neural Network. It will generate the two modules in the single network according to weight and bias. First Module name Training part and second one testing or you can say analyses the training module. Evaluate the performance parameters like Throughput, Packet sent etc.Compare the performance parameters proposed work and previous work.

Pseudo Code in BPNN Algorithm

```
Input: Training set= Ga_features, target, hidden neurons,
Iterationsmax, weights, bias
Output: Network
start
network initialize net1
threshold ≤ T
[ro,co]= size(Ga_features)
for  i =1:ro
training_set=cat(1,1:50);
end
for  j=1:co
target (j)=j;
end
training_set =double(training_set);
for( i > 1, i ≤ Tmax, i++)
do
net1=newff(training_set,target,10);
net1.trainParam.epochs=100;
net=train(net1,training_set,target);
while
backpropagateerror(net1,net,Network);
end
end
```

We described the result in DDoS attack, GA and BPNN algorithm in below table and graph.

Table no: 1 Comparison between Energy Consumption of Existing work and Proposed Work

Requests per user	Energy Consumption In Proposed Work	Energy Consumption in Existing Work
10	8	15
15	9	18
20	12	20
25	8	11

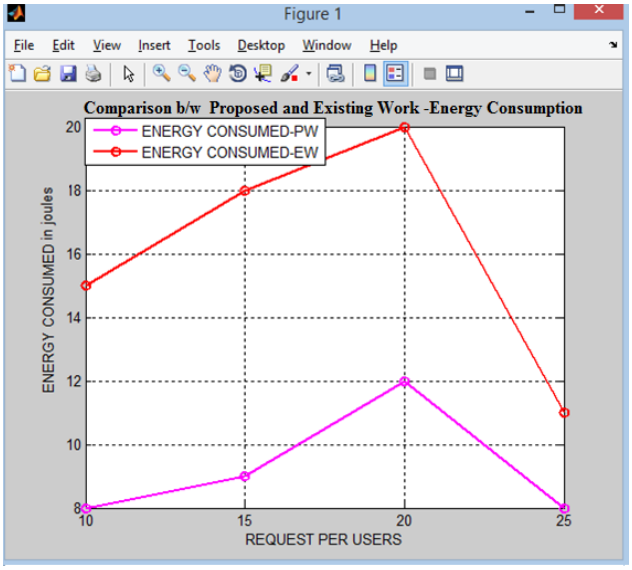

Fig.2 Comparisons between Energy Consumption

The above define the energy consumption means in existing work energy consume more the attack had come then decrease the energy in the web server side.Energy consumption parameter with back propagation neural network. Maximum reduce the energy consumption because of classification technique and mitigate the attacker effect.The quality amount of energy consumption in a process or system, by an organization or society. The energy consumption of the process was very costly so we were in a position where we had to ensure our efforts.

Table no: 2 Comparison between Packets sent of Existing work and Proposed Work

Requests per user	Packets In Proposed Work	Packets in Existing Work
10	90	70
15	92	73
20	95	72
25	97	87

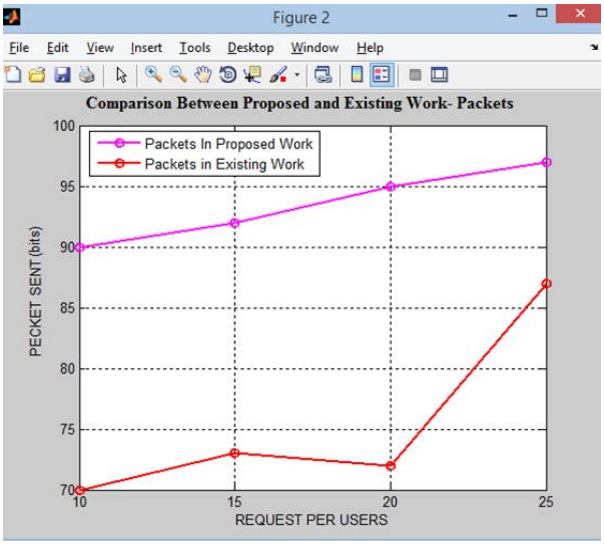

Fig.3 Comparison Between Packets Sent

Above figure defines the comparison between proposed work and existing work with DDOS attack. We improve the performance parameters of the packet size with attack.Base paper throughput in packet size values is 70 and we achieved throughput with attacker value is 90.More Packets has sent in the server side. To prevent the attack present in the server time.Apacket is a segment of data sent from one processer or device to another over a network. A packet contains the source, destination, size, type, data, and other useful info that helps packet get to its destination and read.

Table no: 3 Comparison between Throughput of Existing work and Proposed Work

Requests per user	Throughput In Proposed Work	Throughput in Existing Work
10	56	40
15	64	43
20	74	49
25	80	43

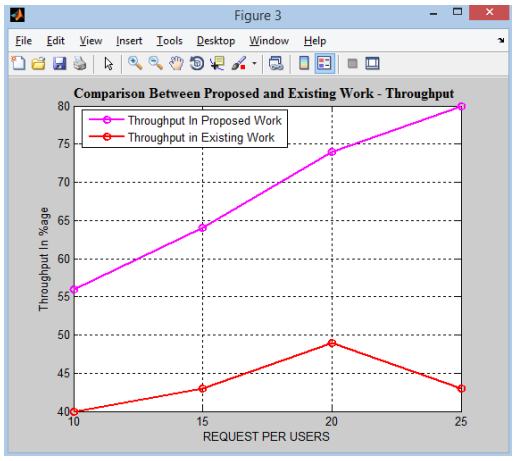

Fig.4 Comparison between Throughput

Above figure defines the comparison between proposed work and existing work with DDOS attack. We used for number of user request 20,25,30,35 and 40 requests. We improve the performance parameters of the throughput with attack.Base paper throughput in DDOS attack values is 40 and we achieved throughput with attacker value is 56.Back propagation Neural Network increases the performance in the server side present. In data transmission, network throughput is the quantity of data moved successfully from one place to alternative in a given time period, and typically measured in bits per second (bps), as in megabits per second (Mbps) or gigabits per second (Gbps).

Table no: 4 Comparison between Bit Error Rate of Existing work and Proposed Work

Requests per user	BER In Proposed Work	BER in Existing Work
10	1	2
15	1.5	3
20	3	7
25	5	9

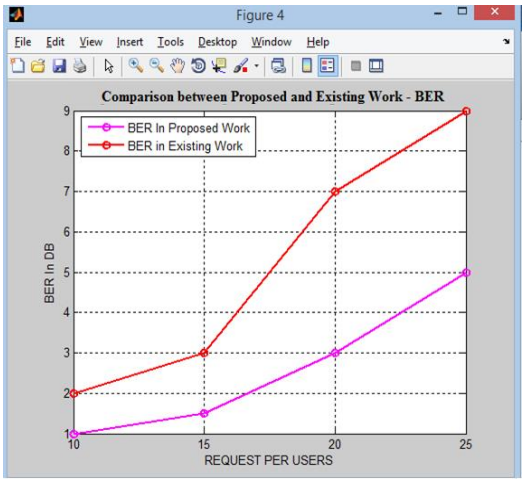

Fig.5.Comparison between Bit Error Rate

Above figure defines the comparison between proposed work and existing work with DDOS classifier. We improve the performance parameters of the throughput with attack.Base paper throughput in classifier values is 93 and we achieved throughput with classifier value is 98.5.bit error rate parameter means hacker send the request in the unnecessary request in the server side. Server get hang and increase the overload of the network side. Delay Also increase in the server side. So, Back propagation neural network prevention or mitigate the attacker effects and helps to reduce the error ration in the server. The number of bit errors is the number of received bits of a data stream over communication channels that have been altered due to noise, interference, distortion or bit synchronization mistakes. ... BER is a unit less performance measure, often expressed as a percentage.

V. CONCLUSION AND FUTURE SCOPE

DDoS attacks are effectively generated and distinguished by proposed genetic algorithm used in real time difference detection system designed using BPNN with best validation performance. BPNN training results the classical file which consists of sets of normal behaviour. During Back propagation Neural Network testing, classification system classifies the incoming flows as attack or normal flow by using model file created during training. Validation check and testing are used for classification. Best performance produces the better classification accuracy as compared to other functions. Genetic algorithm used for detection and BPNN used for classification. Increase the performance in Packet sent and throughput.For further research expected to resolve this matter, by implementing the proposed solution into the real network. In the real network there are several factors that can cause packet drop such as signal degradation, channel congestion, and faulty networking hardware. All that needs to be taken and measured how much influence on our proposed method. Also if it will be implemented in a real network, we need to adjust our simulation with the configuration and real condition of the infrastructure in the field.In future new variations in DDoS attacks such as port scan and DNS spoofing will be employed to maintain the detection accuracy towards best and will implement the detection technique used Bee colony algorithm.

VI. REFERENCES

[1]. Frean, Marcus. "The upstart algorithm: A method for constructing and training feedforward neural networks." *Neural computation* 2, vol. 2 ,pp. 198-209, 1990.

[2]. Goldberg, David E., and John H. Holland."Genetic algorithms and machine learning." *In Proceedings of the sixth annual conference on Computational learning theory* ,vol.2 pp. 95-99, 1988.

[3]. Han, Young-Tae, Nam-SeokKo, Min-Gon Kim, and Hong-Shik Park. "Vulnerability of small networks for the TTL expiry DDoS attack." In*Computing, Communications and Applications Conference (ComComAp), 2012*, vol.2, pp. 147-149. IEEE, 2012.

[4]. Ramamoorthi, A., T. Subbulakshmi, and S. Mercy Shalinie. "Real time detection and classification of DDoS attacks using enhanced SVM with string kernels." In *Recent Trends in Information Technology (ICRTIT), 2011 International Conference on*, vol.4,pp. 91-96. IEEE, 2011.

[5]. Jun, Jae-Hyun, Hyunju Oh, and Sung-Ho Kim. "DDoS flooding attack detection through a step-by-step investigation." In *Networked Embedded Systems for Enterprise Applications (NESEA), 2011 IEEE 2nd International Conference on*, vol.5,pp. 1-5. IEEE, 2011.

[6]. Meghanathan, Natarajan. "A Tutorial on Network Security: Attacks and Controls." *arXiv preprint arXivvol.3,:pp.1412.6017*, 2014.

[7]. Mirkovic, J., Prier, G. and Reiher, P., 2002, November. Attacking DDoS at the source. In *Network Protocols, 2002. Proceedings. 10th IEEE International Conference on* vol.12,pp. 312-321. IEEE, 2002.

[8]. Mittal, Akash, Ajit Kumar Shrivastava, and Manish Manoria. "A review of DDoS attack and its countermeasures in TCP based networks." *International Journal of Computer Science and Engineering Survey* 2.vol.4,pp.177 ,2011.

[9]. Alqahtani, Sarra, and Rose F. Gamble. "DDoS Attacks in Service Clouds." In *System Sciences (HICSS), 2015 48th Hawaii International Conference on*, pp. 5331-5340. IEEE, 2015.

[10]. Chhabra, Meghna, and B. B. Gupta. "An efficient scheme to prevent DDoS flooding attacks in mobile ad-hoc network (MANET)." *Research Journal of Applied Sciences, Engineering and Technology* 7, no. 10 (2014): 2033-2039.

[11]. Bhuyan, Monowar H., D. K. Bhattacharyya, and Jugal K. Kalita. "Information metrics for low-rate DDoS attack detection: A comparative evaluation." In *Contemporary Computing (IC3), 2014 Seventh International Conference on*, pp. 80-84. IEEE, 2014.

[12]. Douligeris, Christos, and AikateriniMitrokotsa. "DDoS attacks and defense mechanisms: classification and state-of-the-art." *Computer Networks* 44, no. 5 (2004): 643-666.

[13]. Sanmorino, Ahmad, and SetiadiYazid. "Ddos attack detection method and mitigation using pattern of the flow." In *Information and Communication Technology (ICoICT), 2013 International Conference of*, pp. 12-16. IEEE, 2013.

[14]. Thapngam, Theerasak, Shui Yu, Wanlei Zhou, and GlebBeliakov. "Discriminating DDoS attack traffic from flash crowd through packet arrival patterns." In *Computer Communications Workshops (INFOCOM WKSHPS), 2011 IEEE Conference on*, vol1, pp. 952-957. IEEE, 2011.

[15]. Qin, Xi, TonggeXu, and Chao Wang. "DDoS Attack Detection Using Flow Entropy and Clustering Technique." In *2015 11th International Conference on Computational Intelligence and Security (CIS)*, vol.no. 9,pp. 412-415. IEEE, 2015.