IJRECE VOL. 4 ISSUE 4 OCT.-DEC. 2016 ISSN: 2393-9028 (PRINT) | ISSN: 2348-2281 (ONLINE)
DOI: 10.13140/RG.2.2.22314.62402

Robust Technique to mitigate DDOS Attack in Web network using BPNN

Pallavi Sharma[1], Maninder Kaur[2]
M.Tech (Scholar), Assistant Professor
Department of Electronics Communications and Engineering, Doaba Institute of Engineering and Technology, kharar

Abstract-- Distributed Denial of Service attack is an incessant critical threat to the internet. Application layer DDoS Attack is resulting from the lower layers. Request layer based DDoS attacks use HTTP requests after formation of TCP three way hands shaking and overwhelms the target resources, such as sockets, CPU, memory, disk, record bandwidth. . The problem found that DDoS attack is an accepted growth from the Synchronize (SYN) Flood. This attack is converging Internet connection bandwidth of many types of machinery upon one or a few machines. Usually, the attacker installs the remote attack database on weakly protected processors using Trojan horses and intrusion methods, and then coordinates the attack from all the different computers at once. The problem is when an attacker will try to attack the system, threat would be detected by Genetic Algorithm and with the help of its fitness function it would harvest an assessment value out of that risk. In Optimization technique used to detection purpose with the help of fitness function and classification using prevention with the help of targets. The classification generates three graph first is best performance evaluate w.r.t MSE, validation checks and average performance 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 – Distributed Denial of Services, Genetic Algorithm, Classifier and Performance parameters.

I. INTRODUCTION

A computer network consists of a collection of computers, printers & other tools that is connected jointly so that they can communicate with each other. A system consists of 2 or more computers that are associated in order to contribute to resources (such as printers and CDs), replace files or allow electronic connections. The computers on a network may be linked through cables, telephone lines, radio waves, satellites or infrared light beams [1**]**

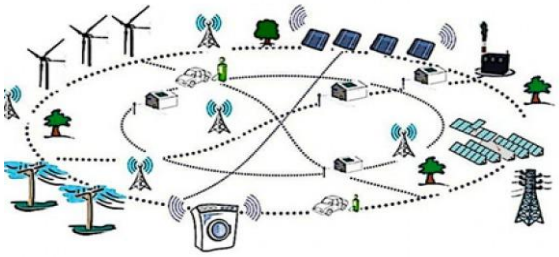

Fig.1 Networks

II. TYPES OF NETWORK

1) Local Area Network

The system used to be linked computers in a only space, space within a building or buildings on 1 site are called Local Area Network (LAN). LAN transfer data with a rapidity of several megabits per second (106 bits per second). The broadcast medium is usually coaxial wire. LAN links computers, i.e. software & hardware, in the similar area for the reason of sharing data. Usually LAN relate with computers within a limited geographical area because they must be linked by a cable, which is quite expensive. People operational in LAN get more ability in data dispensation, work dispensation and other data exchange evaluate to stand-alone computers. Because of this information exchange mainly of the business & government association are using LAN.

Fig.2 LAN Network

DOI: 10.13140/RG.2.2.22314.62402

2) *Wide Area Network*

The term Wide Area Network (WAN) is used to explain a computer system spanning a regional, national or global area. For example, for a great corporation the headquarters might be at Delhi and regional branches at Bombay, Madras and Bangalore. The distance between computers connected to WAN is better. The broadcast medium used is usually telephone lines, microwaves and satellite links [2]

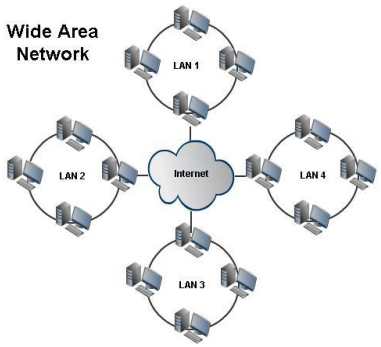

Fig.3 WAN Network

3) Hybrid Network

Between the LAN and WAN structures, hybrid networks are discovered such as campus area nets (CANs) & metropolitan area networks (MANs). In addition, a fresh form of system type is emerging describe home area networks (HANs). The access to business Web sites has produced 2 classifications known as intranets & extranets.

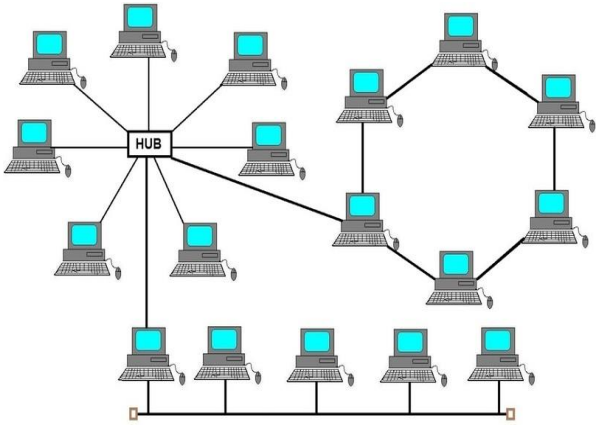

Fig.4 Hybrid Network

III. ADVANTAGES OF NETWORK

The reliability of system is high because the collapse of one computer in the system does not influence the performance of other computers. Addition of new computer to network is simple.

- High rate of information broadcast is probable.
- Peripheral devices like attractive disk and printer can be shared by additional computers
- This network uses coaxial cables for information broadcast.
- Unique integrated route chips called organizer are used to join equipment to the cable**[3]**

IV. DISADVANTAGES OF NETWORK

- If the communication line fails, the whole system breaks down
- Since there are already huge number of people who are using computer networking in distribution some of their files & resources, the safety would be always at risk. There might be illegal activities that will happen that is require to be aware & be careful all the time.
- Since computer networking is a process operated throughout computers, populace are already relying extra of the works of the computer quite than exerting an attempt for their works**[4]**

V. TYPES OF ATTACKS

A helpful means of classify safety attack is in terms of Active attack and Passive attack. A passive attack attempts to monitor the information from the system but does not affect system resources. An active attack attempts to harm system resources and their operations.

➢ ***Passive attack***

Passive attack is in nature of attic dropping on, or monitor of broadcast. Passive attacks include traffic analysis, monitoring of unprotected infrastructure, decrypting weakly encrypted transfer, & capturing authentication information such as passwords. Passive interception of network procedure enables challenger to see upcoming actions. Passive attacks result in the disclosure of information or data archive to an attacker devoid of the consent or knowledge of the user.

➢ ***Active attack***

It involves some adjustment of the information Stream or formation of the false stream. Attacker tries to bypass or break into secured systems. This can be complete through worms, stealth, or viruses, Trojan horses. Active attacks include attempts to circumvent or crack protection features, to set up malicious code, and to steal or modify information. These attacks are mounted alongside a system backbone, use information in transfer, electronically penetrate an enclave, or attack an authorized remote consumer during a try to connect to a cooperative. Active attacks subdivided into four categories; masquerade, replay, modification of message, and denial of service

DOI: 10.13140/RG.2.2.22314.62402

- ***Spoof attack***

In a spoof attack, the hacker tries to access the network IP address. Before gaining access to the system with applicable IP address, the attacker can modify, reroute, or delete the data.

- ***Buffer run over***

A buffer run over attack is when the attacker drives more data to system than is expected. A shield run over attack generally results in the attacker gaining administrative access to the system in a command punctual or shell.

- ***Exploit attack***

In this kind of attack, the attacker knows of a security problem within an operating system or a section of software & leverages that information by exploiting the vulnerability.

- ***Password attack***

An attacker attempts to break the passwords store in a system account database or a password-protected file. There are three major kind of password attacks: a brute-force attack, a dictionary attack, & a hybrid attack.**[5]**

- ***Smurf Attack***

A perpetrator can launch the Smurf attack by sending a spoofed Echo-Request memo to a network's transmitting IP address. The spoofed Echo-Request memo has the victim's IP talk to as the source IP address. Hence, each host receiving the broadcast Echo-apply for message will drive an Echo-Reply memo to the victim. The victim will be overwhelmed with a flood of Echo-Reply post.

VI. RELATED WORK

V.K Soundar Rajam et al. in 2013 [6] proposed a trace back mechanism with an actual optimization algorithm termed ACOPID in autonomous system with DPM inflicts two major advantages. They had predicted the complete attack path and efficiently tracing the DDoS attack source. Our contribution is on host IP trace back with DPM based on autonomous system to trace back the DDoS attack source with the marking information with reduced false positive rate. **Ahmad Sanmorino et al. in 2013 [7]** described how to handle DDoS attacks in the form of discovery method based on the design of flow entries and handling mechanism using layered firewall. Tests carried out using three scenarios that is simulations on normal network environment, unsecured network, and secure network. Then, analyzed the simulations result that has been done. The method used successfully filtering incoming packet, by released packets from the assailant when DDoS attack happen, while still be able to receive packets from legitimate hosts.**Bing Wang et al. in 2014 [8]** proposed by examining the security impact, in particular, the impact on DDoS attack defense mechanisms, in an enterprise network where both technologies are adopted. They found that SDN technology can really help enterprises to defend against DDoS attacks if the defines architecture is designed properly. To that end, they proposed a DDoS attack mitigation architecture that integrates a highly programmable network monitoring to qualify attack detection & a supple manage organization to allow fast and specific attack reaction.**Shakti Arora et al. in 2014 [9]** proposed mechanisms that does not suit to MANET resource constraints because of introduction of substantial traffic load to argument and verifying keys. Because of such problems ad hoc networks have their own vulnerabilities that are not always undertaken by these wired network security solutions. Distributed Denial of Service attacks have also become a problem for Internet using computer system. **Meghna Chhabra et al. in 2014 [10]**In this described as, the purpose of this study is to understand the flaws of prevailing solutions to combat the DDoS attack and a novel scheme is being provided with its authentication to reduce the effect of DDoS attack in MANET Environment. As Internet users are growing day by day, it is becoming more prone to attacks and new riding techniques. People are accessing material and communicating with each other on the move. **Sarra Alqahtani et al. in 2015 [11]** described a DDoS attack uncovering approach for service clouds and develops efficient algorithms to resolve the originating service for the attack. The detection approach had composed of four levels such that each level detects symptoms of DDoS attacks from its local data.

VII. ISSUES IN DDOS ATTACK

- DDoS attack is an accepted growth from the SYN Flood. The idea overdue this attack is converging Internet connection bandwidth of many types of machinery upon one or a few machines.
- This way it is likely to use a large array of smaller widely distributed computers to create the big flood effect. Usually, the attacker installs his remote attack database on weakly protected processors using Trojan horses and intrusion methods, and then coordinates the attack from all the different computers at once.
- This makes a brute force flood of malicious "nonsense" Internet traffic to swamp and devour the target server's or its network connection bandwidth. This means packet flood contends with, and overwhelms, the network's valid traffic so that "good packets" have a low probability of enduring the flood. The network's servers become cut off from the rest of the Internet, and their service is denied.
- Our problem is when an attacker will try to attack the system, threat would be detecting by genetic algorithm and with the help of its fitness function it would produce an assessment value out of that threat. That assessment value would be considered by Back Propagation Neural Network and it would prevent it by giving us a maximum throughput hence making our network more efficient.

VIII. DDOS ATTACK

DOI: 10.13140/RG.2.2.22314.62402

Distributed denial of service operations remains one of the most popular type 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 activist set 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. Distributed Denial of Service attacks have emerged as one of the most severe threats between others. The strength of DDoS attacks has turned into stronger according to advancement of network infrastructure. DDoS attacks are thrown by generating a tremendously large quantity of traffics and they quickly tire resources of target [7] systems, such as system bandwidth and computing control. DDoS defences mechanism can be classified into four classes which are prevention, uncovering, mitigation, and response. When DDoS attack occur, first step to spoil DDoS attacks is the detection and it should be done as fast as possible. However, it is difficult to differentiate between Distributed Denial of Service attack and ordinary traffics, since DDoS attack traffics frequently do not hold horrible contents in the packets. Moreover, attackers copy their source address to cover up their location and to create DDoS attacks more refined. DDoS detection schemes should assurance both short detection delay and high detection rates with low false positives [8].

IX. PROPOSED TECHNIQUES

In this section, we discussed the Genetic used for detection and Classification used for prevention.

a) Genetic Algorithm

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:

- The selection operator selects those chromosomes in the populace that will be allowed to replicate with better chromosomes producing on average more spring than less ones.
- Crossover exchanges subparts of two chromosomes, roughly replicating organic re-combination among 2 single gene organisms;
- 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 [12].

.

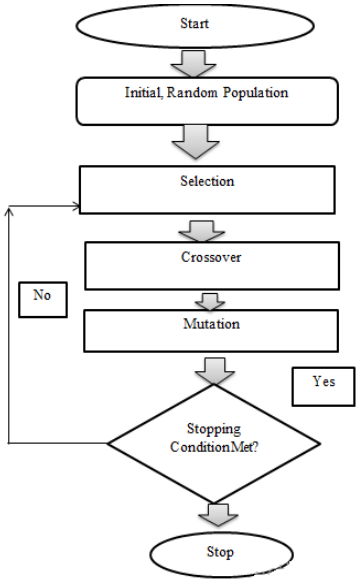

Fig.5 Genetic Algorithm Flow Chart

b) Prevention using Back Propagation Neural Network

This Neural Network is a multi-layered, back propagation neural network and is by far the most extensively used. It is also measured one of the greenest and most general methods used for supervised training of multi-layered neural networks. Back propagation mechanism by resembling the non-linear relationship between the input and the output by adjusting the load values internally. It can further be generalized for the input that is not included in the training patterns.

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 image of a face, and the production could be represented by a code that corresponds to the name of the person [7].

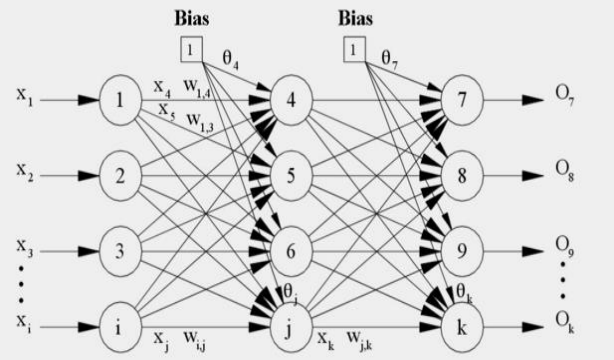

Fig.6 Back Propagation Neural Network

DOI: 10.13140/RG.2.2.22314.62402

X. RESULT AND DISCUSSION

We describe the result analysis with attack, detection and prevention using Back Propagation Neural Network. Compare the performance parameters with Throughput and packet sent etc.

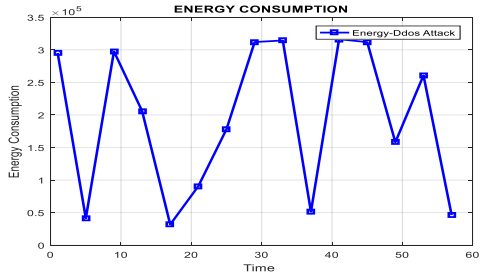

Fig.7 Energy Consumption in joules with DDoS Attack

The above figure defines that the Energy consumption parameter with DDoS attacks. AN increase the energy Consumption because of attack has presented.

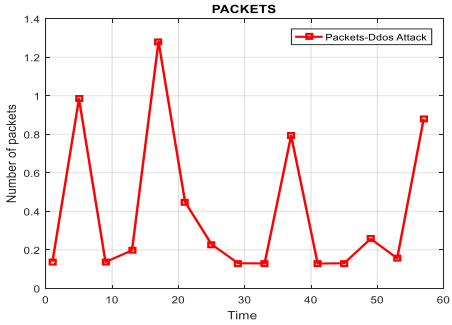

Fig.8 Packets with DDoS Attack

The above figure described that the packet sent in the time according with DDoS attack. Fewer Packets has sent because of the attack present in the server time.

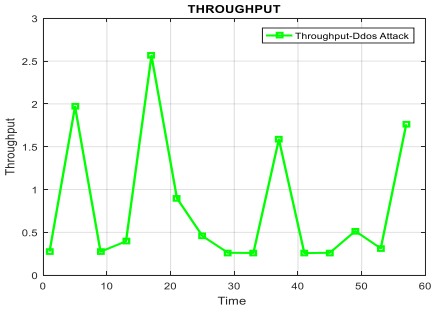

Fig.9 Throughput (%) with DDoS Attack

The above figure described the throughput means accuracy of the web server according to the time. DDoS attack presents the decrease the throughput performance.

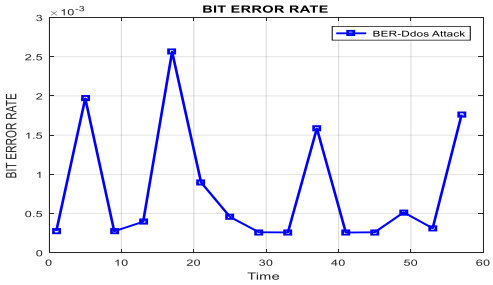

Fig.10 Bit Error rate (db) with DDoS Attack

The above figure described that the 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.

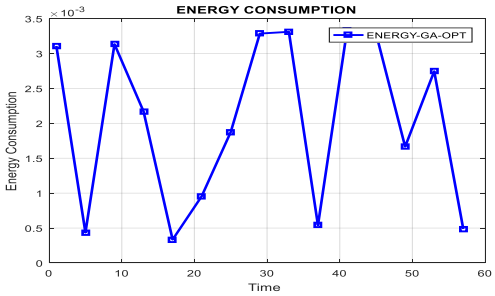

Fig.11 Energy Consumption in joules using Genetic Algorithm

The above figure defines that the Energy consumption parameter with genetic algorithm. Minimum reduce the energy consumption because of genetic algorithm find the attacker.

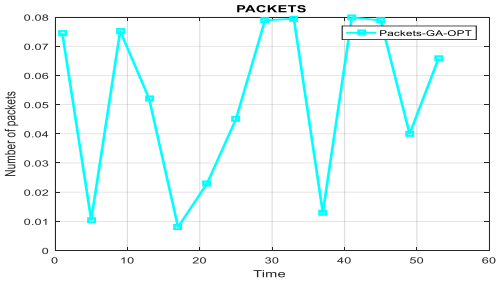

Fig.12 Packets using Genetic Algorithm

DOI: 10.13140/RG.2.2.22314.62402

The above figure described that the packet sent in the time according with genetic algorithm. Maximum Packets has sent and to detect an attack present in the server time.

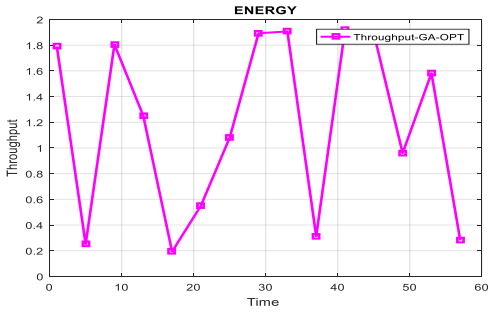

Fig.13 Throughput (%) using Genetic Algorithm

The above figure described the throughput means accuracy of the web server according to the time. Genetic algorithm increases the performance in the server side present.

Fig.14 Bit error rate (db) using Genetic Algorithm

The above figure described that the 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, genetic algorithm helps to reduce the error ration in the server.

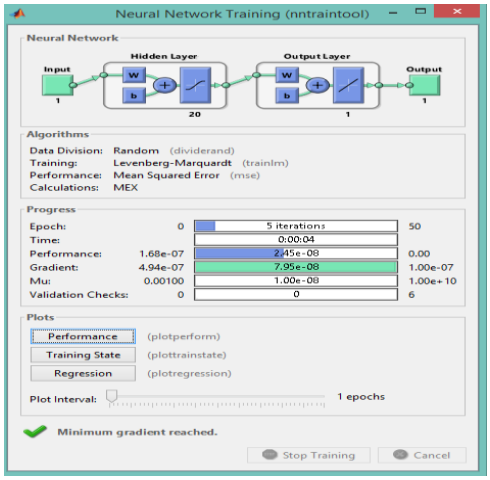

Fig.15 Back Propagation Neural Network

The above figure shows that the classification technique to improve the server performance according to the training module and testing module.

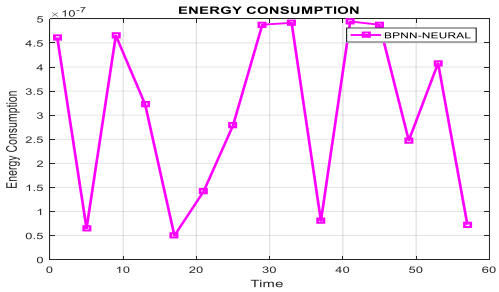

Fig.16 Energy Consumption in joules with Back propagation Neural Network

The above figure defines that the Energy consumption parameter with back propagation neural network. Maximum reduce the energy consumption because of classification technique and mitigate the attacker effect.

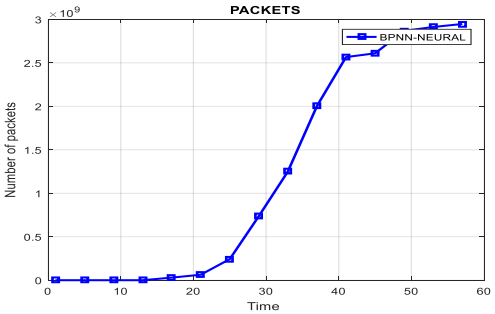

Fig.17 Packets with Back propagation Neural Network

DOI: 10.13140/RG.2.2.22314.62402

The above figure described that the packet sent in the time according using back propagation neural network. More Packets has sent in the server side. To prevent the attack present in the server time.

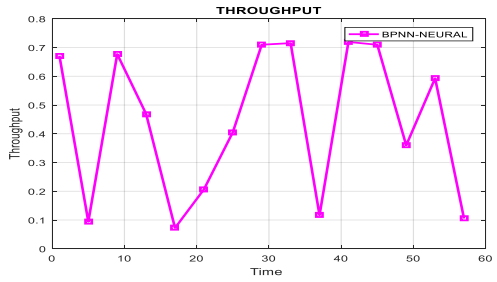

Fig.18 Throughput(%) with Back propagation Neural Network

The above figure described the throughput means accuracy of the web server according to the time. Back propagation Neural Network increases the performance in the server side present.

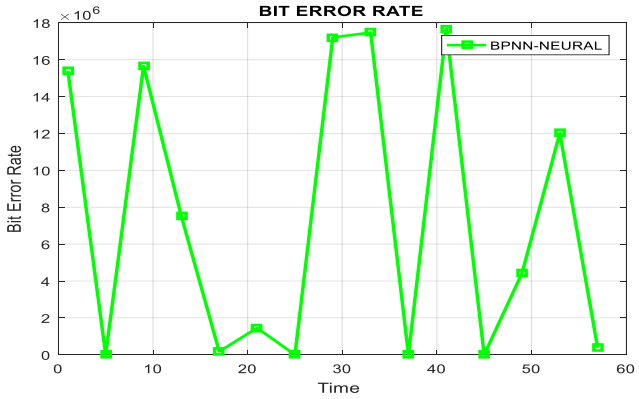

Fig.19 Bit Error Rate (db) with Back propagation Neural Network

The above figure described that the 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.

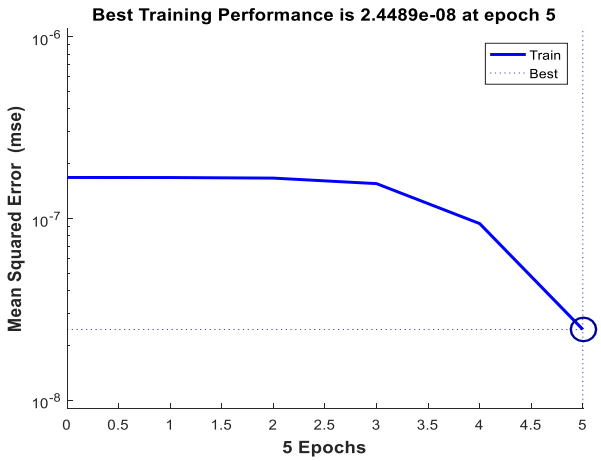

Fig.20 Best Training performance

The above graph described that the best validation performance according to the number of iterations corresponding to the mean square error rate.

e

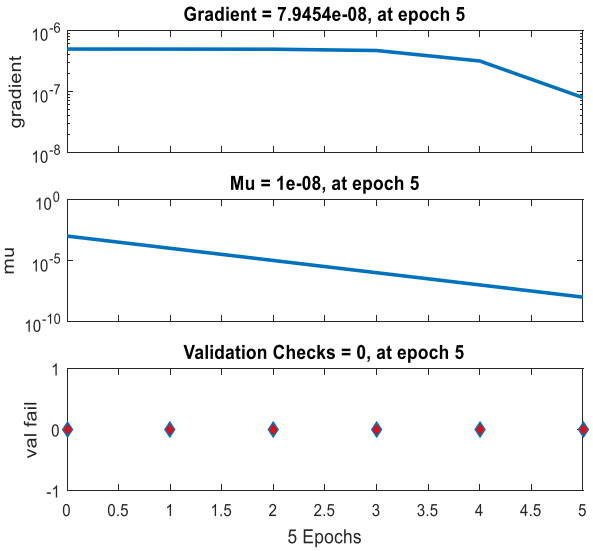

Fig.21 Performance (gradient, mutation and validation fails)

The above figure described that the validation process and define the first gradient, mutation and validation failure according to the 7 epochs.

DOI: 10.13140/RG.2.2.22314.62402

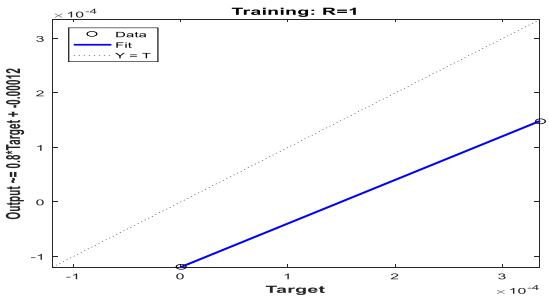

Fig.22 Training state

Above figure described that the training state defines the attacker free data will train the web server.

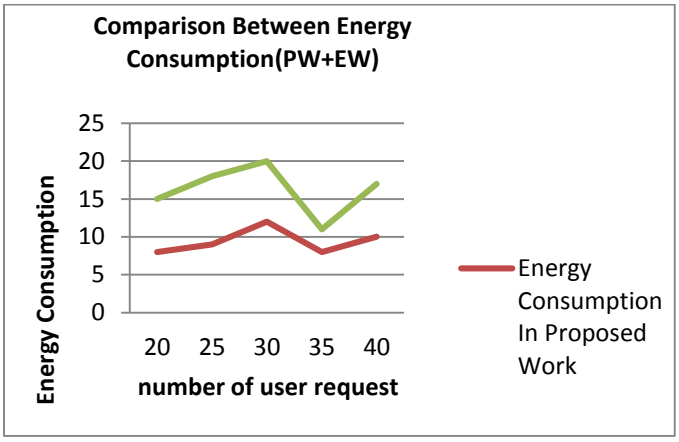

Fig.23 Comparison Between Energy Consumption

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.

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
20	8	15
25	9	18
30	12	20
35	8	11
40	10	17

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

Requests per user	Packets In Proposed Work	Packets in Existing Work
20	90	70
25	92	73
30	95	72
35	97	87
40	98	83

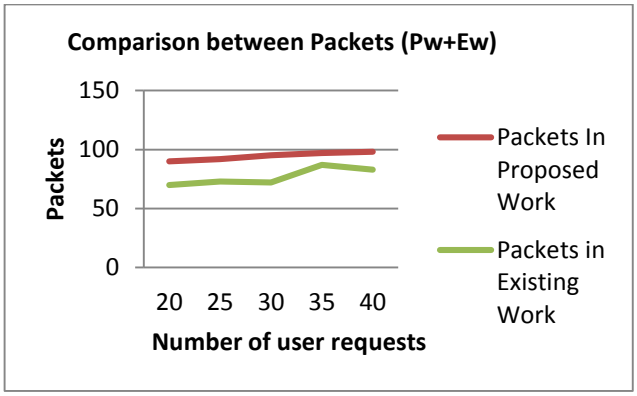

Fig.24 Comparison Between Packets Sent

DOI: 10.13140/RG.2.2.22314.62402

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.

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

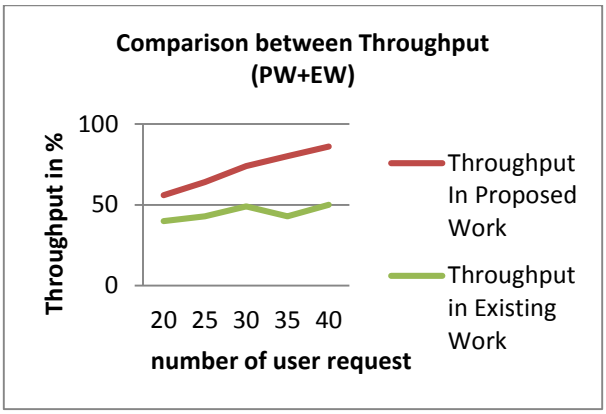

Fig.25 Comparison between Throughput

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.

Table no: 3 Comparison between Bit Error Rate of Existing work and Proposed Work

Requests per user	BER In Proposed Work	BER in Existing Work
20	1	2
25	1.5	3
30	3	7
35	5	9
40	5.7	12

Requests per user	Throughput In Proposed Work	Throughput in Existing Work
20	56	40
25	64	43
30	74	49
35	80	43
40	86	50

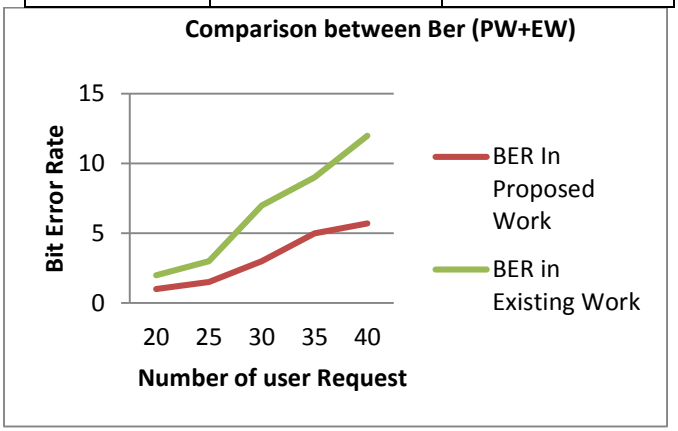

Fig.26 Comparison between Bit Error Rate

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.

XI. CONCLUSION

Request and Network layer DDoS attacks are effectively generated and distinguished by proposed genetic algorithm used in real time difference detection system designed using FFNN 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

DOI: 10.13140/RG.2.2.22314.62402

detection and BPNN used for classification. Increase the performance in Packet sent and throughput.

REFERENCES

[1]. Comer, Douglas E. Computer networks and internets. Prentice Hall Press, 2008.

[2]. Chun, Dorothy M. "Using computer networking to facilitate the acquisition of interactive competence." System 22.1 (1994): 17-31.

[3]. Wellman, Barry, et al. "Computer networks as social networks: Collaborative work, telework, and virtual community." Annual review of sociology (1996): 213-238.

[4]. Tu, Jack V. "Advantages and disadvantages of using artificial neural networks versus logistic regression for predicting medical outcomes."Journal of clinical epidemiology 49.11 (1996): 1225-1231.

[5]. Stallings, William. Cryptography and network security: principles and practices. Pearson Education India, 2006.

[6]. SoundarRajam, V. K., et al. "Autonomous system based traceback mechanism for DDoS attack." Advanced Computing (ICoAC), 2013 Fifth International Conference on.IEEE, 2013.

[7]. Sanmorino, Ahmad, and SetiadiYazid. "Ddos attack detection method and mitigation using pattern of the flow." Information and Communication Technology (ICoICT), 2013 International Conference of.IEEE, 2013.

[8]. Bhuyan, Monowar H., Dhruba Kumar Bhattacharyya, and Jugal Kumar Kalita. "Information metrics for low-rate DDoS attack detection: A comparative evaluation." Contemporary Computing (IC3), 2014 Seventh International Conference on. IEEE, 2014.

[9]. Anantvalee, Tiranuch, and Jie Wu."A survey on intrusion detection in mobile ad hoc networks." Wireless Network Security.Springer US, 2007.159-180.

[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 7.10 (2014): 2033-2039.

[11].Alqahtani, Sarra, and Rose Gamble."DDoS Attacks in Service Clouds."System Sciences (HICSS), 2015 48th Hawaii International Conference on.IEEE, 2015.

[12].Goldberg, David E., and John H. Holland."Genetic algorithms and machine learning." Machine learning 3.2 (1988): 95-99.