TRJ VOL. 2 ISSUE 4 JULY-AUG 2016 ISSN: 2454-7301 (PRINT) | ISSN: 2454-4930 (ONLINE)
DOI: 10.13140/RG.2.2.26339.76325

An Investigation in DDoS Attack in the Web Server Network Using Genetic Approach and Classifier (FFNN)

Gurleen Kaur[1], Gurjot Singh Sodhi[2]
[1]M.Tech (Student), [2]Assistant Professor
Shaheed Udham Singh College of Engineering and Technology, Tangori, Mohali

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 legitimate HTTP requests after formation of TCP three way hands shaking and overwhelms the target resources, such as sockets, CPU, memory, disk, record bandwidth. We found the problem 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.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 harvest an assessment value out of that risk.. An anomaly detection mechanism is proposed in this paper to detect DDoS attacks using Genetic Algorithm and prevention using feed forward neural network. Apply the optimization technique for detect the attack and prevention classification technique using Feed Forward Neural Network.

Keywords **-** Distributed Denial of Service attack, HTTP, Genetic Algorithm, SYN and Flood Attack.

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. Cyber Security is the body of technologies, processes & practices considered [1] 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 and [2] 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 [3]:

- Availability
- Integrity, which may take in authenticity & non-repudiation
- Discretion

Cyber security involves protecting that information by preventing, identify and responding [4] to the attacks.
There are lots of risks; some are more serious than others. Among these dangers are viruses remove the whole system, someone observance into the system and altering files, someone using the computer to attack others, or a big shot robbery of the credit card information and making unauthorized purchases. Unfortunately, there is no [5,6] 100% assurance that still with the best safety measures some of these things would not happen, but there are steps that can be taken to minimize the chances [7,8].

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 [9] of network infrastructure. DDoS attacks are thrown by generating a tremendously large quantity of traffics and they quickly tire resources of target [14] systems, such as system bandwidth and computing control. DDoS defences mechanism can be classified into four classes which are prevention, uncovering, mitigation, and response [10]. 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 [15].

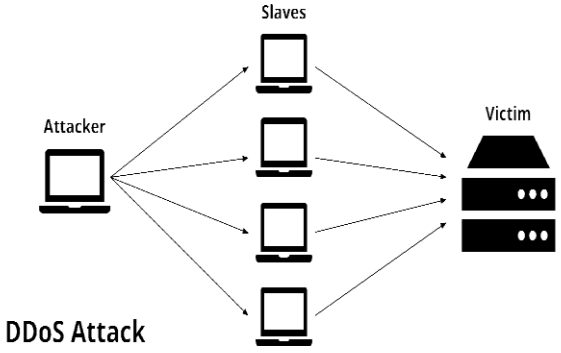


Fig.1: DDoS Attack

DOI: 10.13140/RG.2.2.26339.76325

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.

II. RELATED WORK

Theerasak Thapngam et al. in 2011[10] proposed a behaviour based detection that can distinguish DDoS attack traffic from traffic produced by real users. By using Pearson's correlation coefficient, those comparable detection methods can citation the repeatable sorts of the packet arrivals. The widespread simulations were tested for the accuracy of detection. They then achieved experiments with numerous datasets and our results affirm that the projected technique can differentiate transfer of an attack basis from sincere traffic with a quick response.

Jae-Hyun Jun et al. in 2011[11] described the DDoS attack which is consuming all of the computing or communication resources necessary for the service, is known very difficult to protect. The threat posed by network attacks on large network, such as the internet, difficulties effective discovery method. Therefore, an intrusion detection system on large network is need to effectual real-time detection. In these broadside, implemented the entropy-based detection mechanism against DDoS attacks in order to agreement the transmission of normal traffic and prevent the flood of abnormal traffic.

Akash Mittal et al. in 2011[21] proposed the different techniques of DDoS & its countermeasures by dissimilar methods such as Bloom Filter, Trace Back method, Independent Component Analysis and TCP Flow Analysis.

Young-Tae Han et al. in 2012 [12] described the effect of the TTL Expiry DDoS attack with the attack scenario in the tested consisted with commercialized network equipment's.

V.K Soundar Rajam et al. in 2013 [13] 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 [14] 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, analysed 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.

III. PROBLEM STATEMENT AND FACT /FIGURES

DDoS attack is an accepted growth from the Synchronize (SYN) Flood. The attack is converging Internet connection bandwidth of many types of machinery upon one or a few machines. 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. It creates Internet traffic to swamp 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 delay. The system servers become cut off as of the rest of the Internet, and their service is denied.

Fact and Figures of DDOS Attack

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.

Kaspersky intelligences the following data on DDoS attacks from the second quarter of this year:

- **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.

III. SIMULATION MODEL

The proposed work steps explained in below:

Step 1: Initialize the server scenarios or network architecture.

DOI: 10.13140/RG.2.2.26339.76325

Step 2: Deploy the nodes or you can say create users, application server and web server.

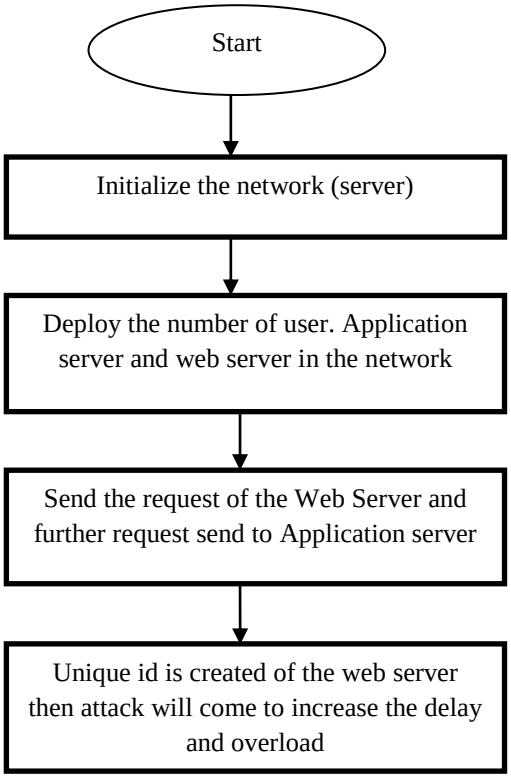


Fig.2: Process of the DDOS perform the Web server

Step 3: User sent the request of the Web Server if Web server is free then accepts the Request then further request is send to the Application server. Application Server reverts back to the Web server then web server reply the user.
Step 4: Whenever we can send the request of the web server. Web server creates the unique identity of the web server which is called as session.
Step 5: Information Transfers from User to Web Server and from Web Server to the Application Server. Attacker will come and hack the information means server will be down or increase the delay and overload of the server.
Step 6: Apply the Genetic Algorithm to Detect the DDoS Attack and performance define through the parameters like Throughput, Packet sent etc.
Step 7: Apply the Classification technique using Feed Forward 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.

Step 8: Compare the performance parameters proposed work and previous work.

IV. RESULT AND DISCUSSION

We are discussing the result of this research work; we used the simulation tool MATLAB. The subsequent Development Tools has been used in the expansion of this work. There may also be other tools which can be used in this development as it depends person to person and his interest. (i) Least amount of 8 GB of RAM (ii) Intel Pentium III Processor or over and (iii) MATLAB R2013a. We describe the result analysis with attack, detection and prevention using Feed Forward Neural Network. Compare the performance parameters with Throughput and packet sent etc.

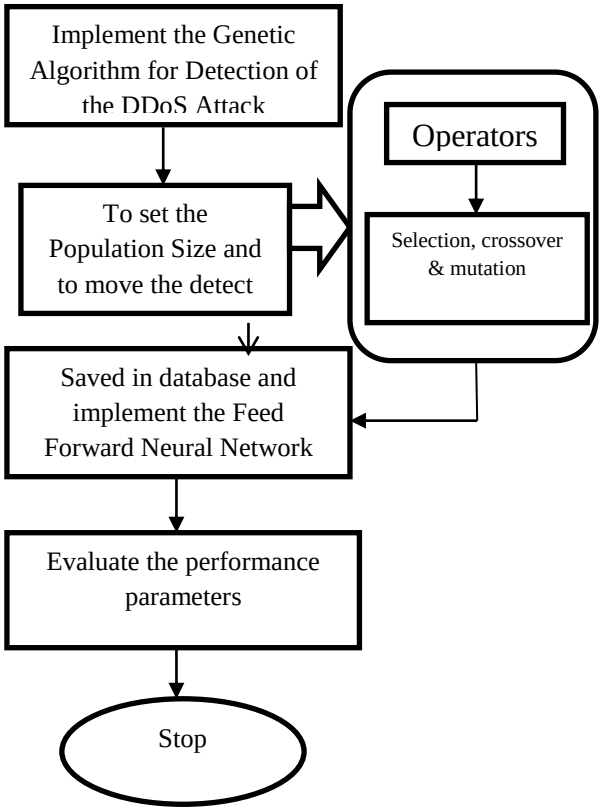
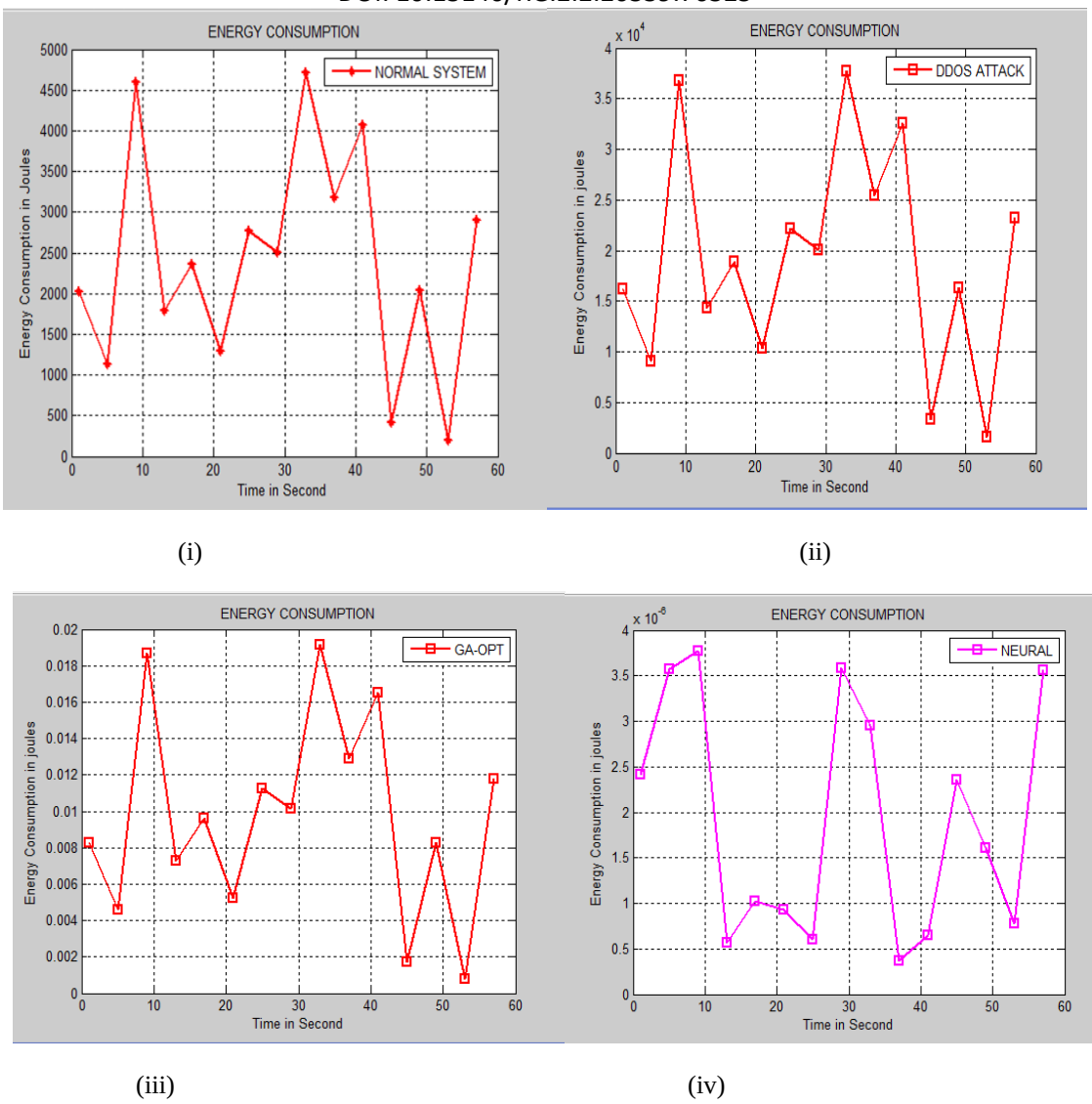


Fig.3: Process of Proposed Techniques

DOI: 10.13140/RG.2.2.26339.76325



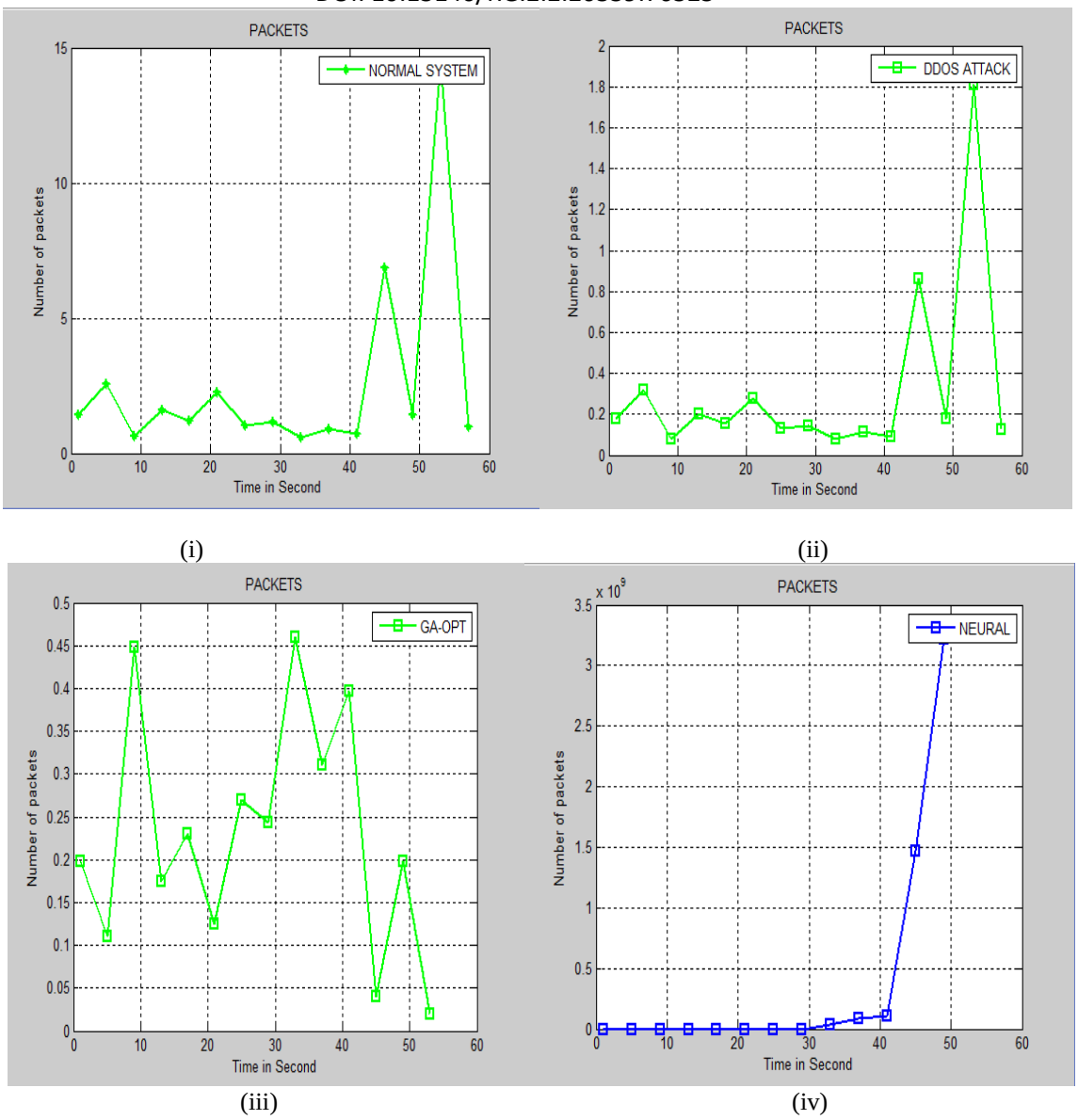
(i) (ii)

(iii) (iv)

Fig.4: (i) Energy Consumption in joules in Normal System , (ii) Energy Consumption in joules with DDoS Attack and (iii) Energy Consumption in joules using Genetic Algorithm and (iv) Energy Consumption in joules with Feed Forward Neural Network

The above figure 4(i) defines that the Energy consumption parameter with Normal system works. The normal system is working the energy Consumption because of attack free performance has presented. The above figure 4(ii) defines that the Energy consumption parameter with DDoS attacks. AN increase the energy Consumption because of attack has presented. The above figure 4(iii) defines that the Energy consumption parameter with genetic algorithm. Minimum reduce the energy consumption because of genetic algorithm find the attacker. The above figure 4(iv) defines that the Energy consumption parameter with feed forward neural network. Maximum reduce the energy consumption because of classification technique and mitigate the attacker effect.

DOI: 10.13140/RG.2.2.26339.76325



(i) (ii)

(iii) (iv)

Fig.5: (i) Packets in Normal System (ii) Packets with DDoS Attack (iii) Packets using Genetic Algorithm and (iv) Packets with Feed Forward Neural Network

The above figure 5(i) described that the packet sent in the time according with attack free system working. Normal Packets has sent because of the attack free system present in the server time. The above figure 5(ii) 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. The above figure 5(iii) 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. The above figure 5(iv) described that the packet sent in the time according using feed forward neural network. More Packets has sent in the server side. To prevent the attack present in the server time.

DOI: 10.13140/RG.2.2.26339.76325

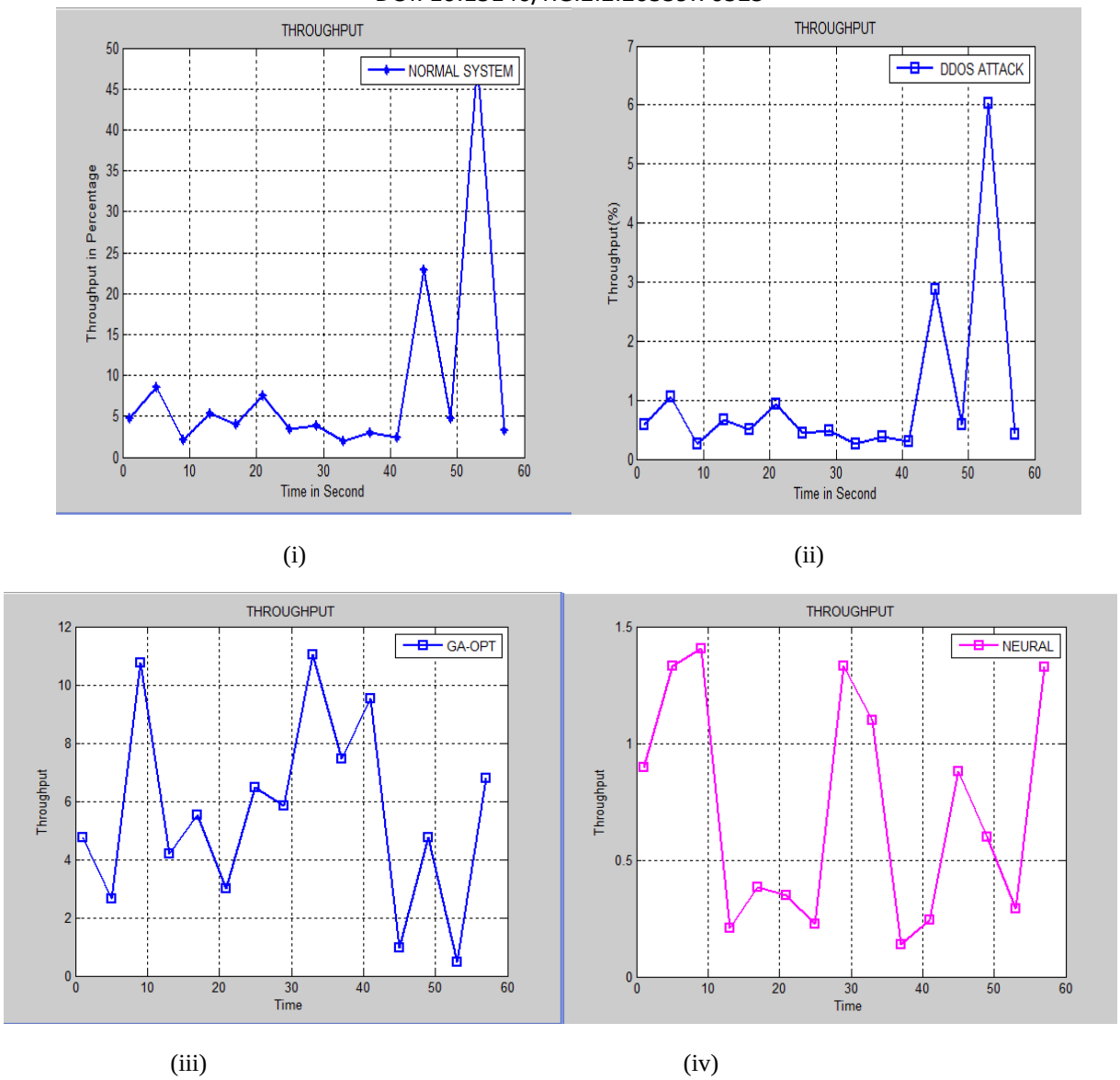
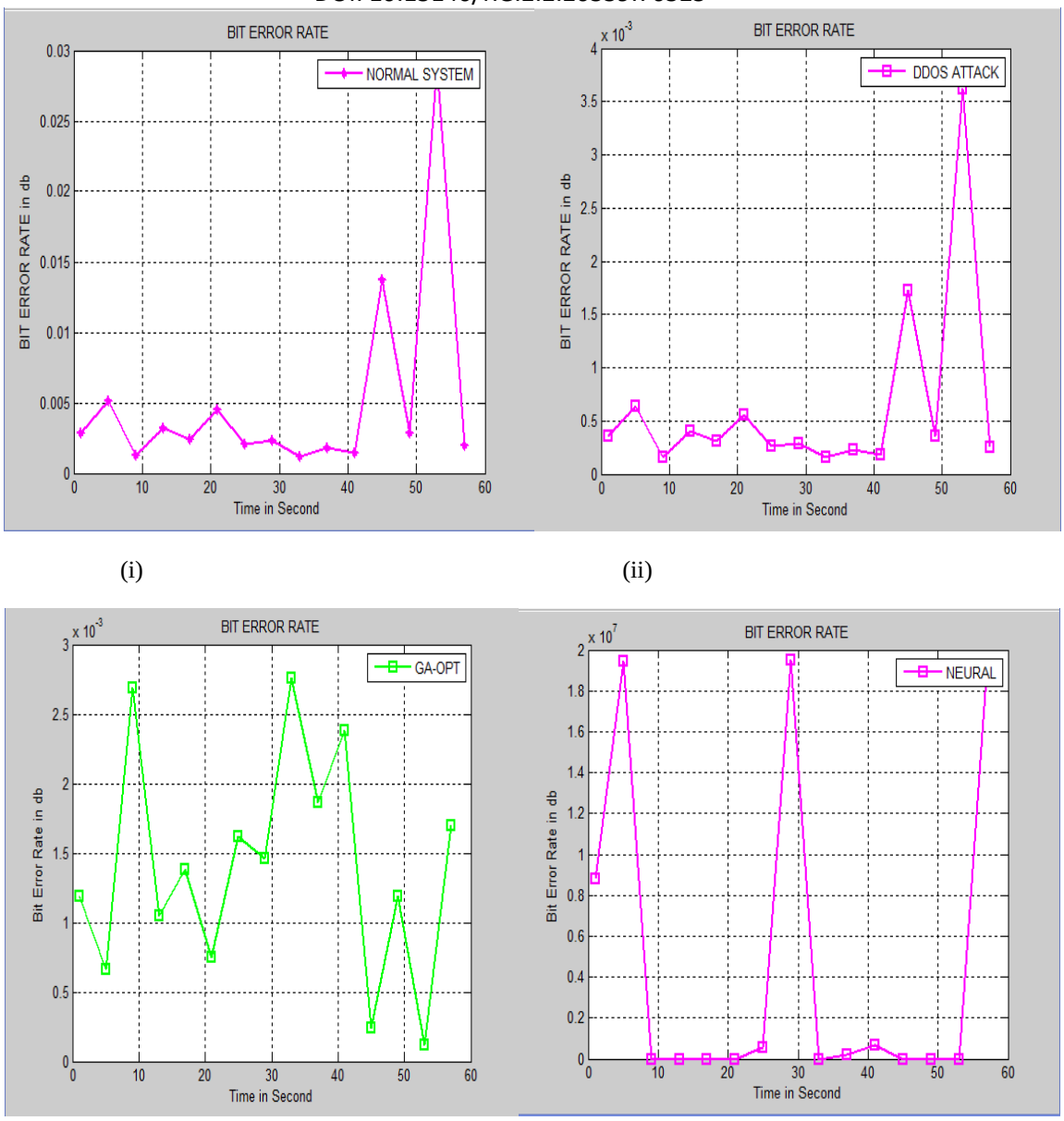


Fig.6: (i) Throughput (%) in Normal System (ii) Throughput (%) with DDoS Attack (iii) Throughput(%) using Genetic Algorithm and (iv) Throughput(%) with Feed Forward Neural Network

The above figure 6(i) described the throughput means accuracy of the web server according to the time. Attack free system presents the throughput performance. The above figure 6(ii) described the throughput means accuracy of the web server according to the time. DDoS attack presents the decrease the throughput performance. The above figure 6(iii) described the throughput means accuracy of the web server according to the time. Genetic algorithm increases the performance in the server side present. The above figure 6(iv) described the throughput means accuracy of the web server according to the time. Feed forward Neural Network increases the performance in the server side present.

DOI: 10.13140/RG.2.2.26339.76325



(i) (ii)

(iii) (iv)

Fig.7: (i) Bit error rate (db) in Normal System (ii) Bit Error rate (db) with DDoS Attack (iii) Bit error rate (db) using Genetic Algorithm and (iv) Bit Error Rate (db) with Feed Forward Neural Network

The above figure 7(i) described that the bit error rate parameter means number of bits send the server side. Server gets normal working because of attack free server. The above figure 7(ii) 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. The above figure 7(iii) 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. The above figure 7(iv) 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, Feed forward neural network prevention or mitigate the attacker effects and helps to reduce the error ration in the server.

DOI: 10.13140/RG.2.2.26339.76325

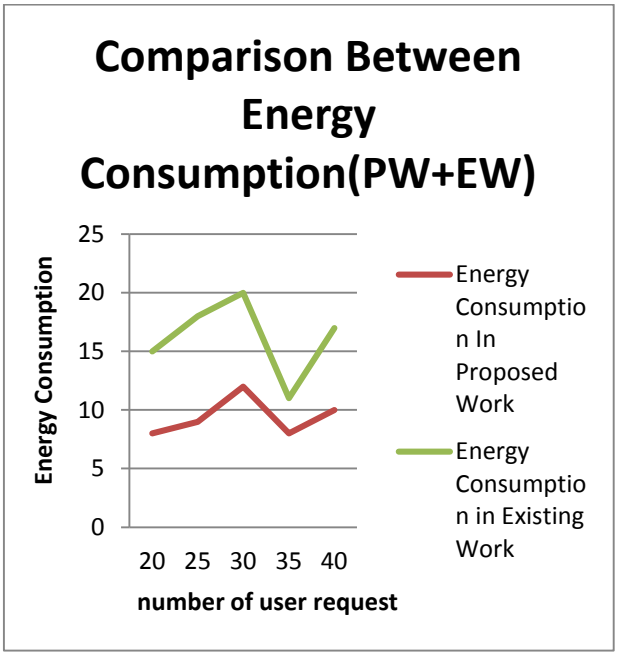


Fig.8: Comparison between Energy Consumption (Existing and Proposed Work)

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.

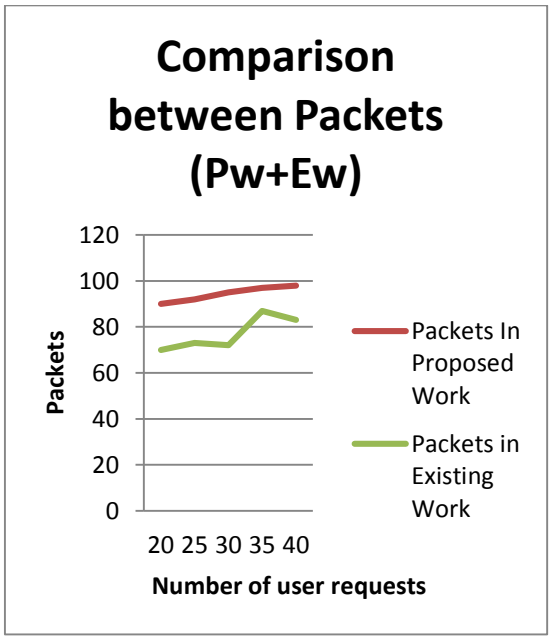


Fig.9: Comparison between Packets Sent (Existing and Proposed Work)

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.

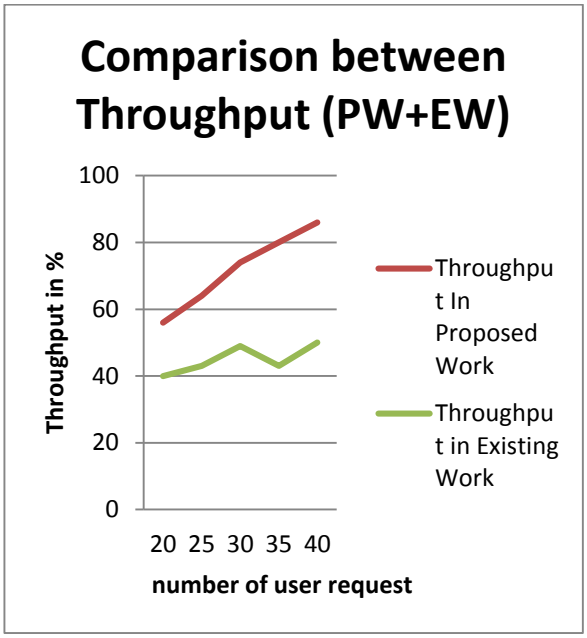


Fig.10: Comparison between Throughput (Existing and Proposed Work)

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.

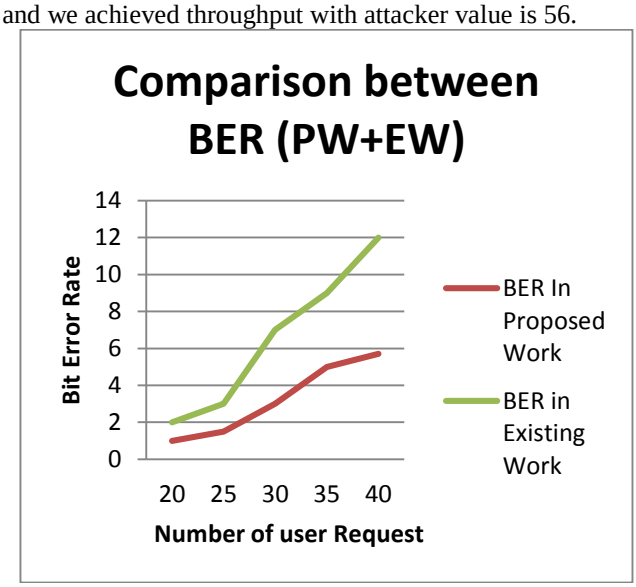


Fig.11: Comparison between Bit Error Rate (Existing and Proposed Work)

Above figure defines the comparison between proposed work and existing work with DDOS classifier. We improve the performance parameters of the throughput with attack.

DOI: 10.13140/RG.2.2.26339.76325

Base paper throughput in classifier values is 93 and we achieved throughput with classifier value is 98.5.

V. CONCLUSION AND FUTURE SCOPE

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. FFNN training results the classical file which consists of sets of normal behaviour. During Feed Forward 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 FFNN used for classification. Increase the performance in Packet sent and throughput.In future new variations in DDoS attacks such as port scan and DNS spoofing will be employed to maintain the detection accuracy towards best. Bfo algorithm can be used to improve the energy consumption and packet delivery.

VI. 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]. Moslehi, Khosrow, and Ranjit Kumar."A Reliability Perspective of the Smart Grid." IEEE Trans. Smart Grid 1.1 (2010): 57-64.

[6]. NEEDHAM, ATTRIBUTED BY ROGER, and Butler Lampson. "Network Attack and Defense." white paper (2008).

[7]. Røstad, Lillian. "An extended misuse case notation: Including vulnerabilities and the insider threat." XII Working Conference on Requirements Engineering: Foundation for Software Quality, Luxembourg. 2006.

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

[9]. Meghanathan, Natarajan. "A Tutorial on Network Security: Attacks and Controls." arXiv preprint arXiv:1412.6017 (2014).

[10].Thapngam, Theerasak, et al. "Discriminating DDoS attack traffic from flash crowd through packet arrival patterns." Computer Communications Workshops (INFOCOM WKSHPS), 2011 IEEE Conference on.IEEE, 2011.

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

[12].Han, Young-Tae, et al. "Vulnerability of small networks for the TTL expiry DDoS attack." Computing, Communications and Applications Conference (ComComAp), 2012.IEEE, 2012.

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

[14].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.

[15].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.