ENHANCED THE COMPUTER NETWORK PERFORMANCE USING BACK PROPAGATION NEURAL NETWORK

Kanwarpal Singh[1]
M.Tech (Scholar)
Department of Information Security
Chandigarh Engineering College
Landran, (Punjab) India
kpsdhaliwal92@gmail.com[1]

Dr. Shashi Bhushan[2]
Professor
Department of Information Technology
Chandigarh Engineering College
Landran, (Punjab), India
shashibhushan9@gmail.com[2]

Abstract — **A network is a group of devices such as printer, computer and other devices which are connected to exchange the data from one place to another place. All these devices joined to resources and compute electrical linking. For communication, devices send and receive data through radio waves, signals, cables and satellites. The computer network comes under three categories: local area network, wide area network and hybrid network. While exchanging information or private data, the main concern is security. Security plays a crucial role on the networks for enhancement of system, privacy and to save data from the hackers and attackers. The usually security on network proved authentication, integrity and availability. When data is transferred from one device to another, the attacks extracts the data and use according to their requirement. On the internet, several kinds of attacks occurred that affect the system and data. Active and Passive Attacks are mostly occurred which are consist of various other harmful attacks like masquerade, message modification, denial of service, Sybil attack and eavesdropping. DDoS Attack is a distributed denial of service attack. The attacker generates the huge number of traffic of unwanted request at the network to minimize the user access to resources.**

In this research work, a solution is obtained by the use of BFOA algorithm that improved the performance of network and for mitigate the flood attack, optimized BPNN is used. BFOA is bacteria foraging optimization algorithm that used fitness function for detection and after that, a assessment value generate from the threats. BPNN is back propagation neural network that is a stimulated organization algorithm. BPNN includes the neurons as a processing unit and these are arranged in the multiple layers. It mainly consists of three layers as input layer, hidden layers and the output layer. To demonstrate the performance parameters, end to end delay and energy consumption decreased whereas throughput, number of sessions and packets delivery increased dramatically.

Keywords : —DDoS attack; NN (neural Networks); BFOA; BPNN.

I. INTRODUCTION

A computer network consists of a collection of computers, printers and other tools that is connected jointed so that they can communicate with each other. We can also say that 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**].** There are three basic types of networks.

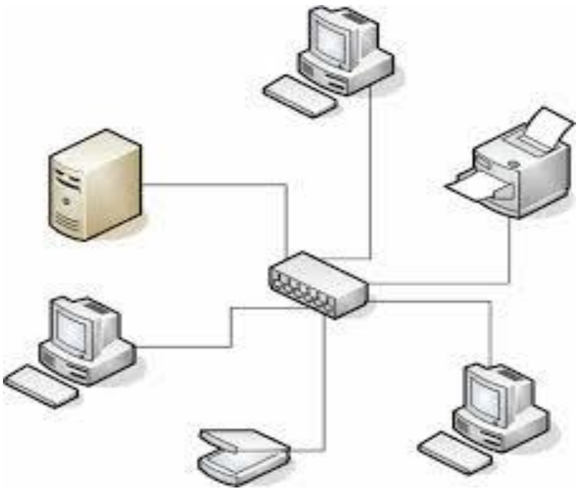

Fig.1. Computer Network [1].

A. 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 a Local Area Network (LAN). LAN transfer data with a rapidity of several megabits per second (106 bits per second). The broadcast medium is usually a coaxial wire. LAN links computers, i.e., software and hardware, in the similar area for the reason of sharing data. Usually LAN relates to 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& other data exchange evaluate to stand-alone computers. Because of this information exchange mainly on the business & government association are using.

B. Wide Area Networks: 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 in Bombay, Madras, Bangalore and Calcutta. Here district centers are linked to headquarters from end to end WAN. The distance between computers connected to WAN is better. Therefore the broadcast medium used is usually telephone lines, microwaves and satellite links [2].

C. Hybrid Network: between the LAN and WAN structures, the discovery of hybrid networks is introduced 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 requirement to access business Web sites has produced 2 classifications known as intranets & extranets [3] [4].

DDoS (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 [5] 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 occured, 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 [6].

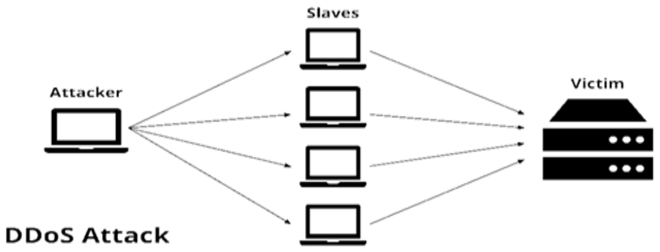

Fig. 2. DDoS Attack [15]

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.

DDoS Attack halts the machines and affects the bandwidth of internet connections. It used extremely tiny computers that are distributed in large number. Other problem is related to unawareness regarding different kinds of attacks [7]. To mitigate these types of attacks Bacterial foraging algorithm is applied that generated a fitness function and being capable to produce assessment values against harmful attacks.

In section I, the overview of research work explained related to computer networks and its categories such as LAN, WAN and Hybrid. In II, section all the related research work is studied and explained with its research a gaps and used techniques. In section III a common discussion about the most occurring problems and issues are given. Further, section IV related to the proposed work to alleviate the DDoS attack. In V section, the obtained results are discussed. Section VI described that the conclusion and future scope in DDoS Computer Network.

II. RELATED WORK

Theerasak Thapngam et al., 2011 [8] proposed a behavior 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 cite the repeatable sorts of the packet arrivals. The widespread simulations were tested for the accuracy of detection. They then achieved experiments with numerous data sets and our results affirm that the projected technique can differentiate transfer of an attack basis of sincere traffic with a quick response.

Jae-Hyun Jun et al., 2011 [9] described as, 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 networks, such as the internet, difficulties effective discovery method. Therefore, an intrusion detection system on large network is needed for effective real-time detection. In these broadsides, 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.

V.K Soundar Rajam et al., 2013 [10] proposed 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.

Shakti Arora et al., 2014 [11] defined as, these mechanisms doesn't 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.

MeghnaChhabra et al., 2014 [12] 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.

III. PROBLEM FORMULATION

DDoS attack is an accepted growth from the SYN Flood. The idea overdue this attack is meeting Internet connection bandwidth of several 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 approaches, and then organizes the attack from all the dissimilar 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.

The major problem is when an attacker will try to attack the system, threat would be detecting by bacterial foraging 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. The gaps in DDOS protection start with awareness. Most organizations are not aware of the gap between the potential threats in their industry and their existing protection level. Using vast experience with DDoS attacks, we map you specific network protection status against the threats [7]. By thoroughly evaluating and measuring your DDoS readiness and implementing re-commendations you minimize risks. Instead of suffering expensive outages during DDoS attack, you can harder you systems in advance and know exactly how to react. You can cut you investment in DDoS mitigate solutions with evaluation and gear selection, instead of making hasty decisions under pressure following an attack.

IV. PROPOSED WORK

In the proposed work the main objective is on a set of purposes with are linked with the milestones of the process. The main objectives are mentioned below-

1) To Study of DDOS Attack and previous algorithms.
2) To Design and implement UDP network in Flood attack for the detection (BFOA) and Prevention using BPNN classifier.
3) Evaluate the performance parameters like number of sessions, delay, packet delivery and throughput etc.

A. Scope of Study: A typical Distributed Denial of Service (DDoS) scenario, an attacker aims at taking down a service. Several computers are mobilized into an attack force [21]. These computers (called zombies or secondary victims) have previously been compromised by the attacker. When an assault is fruitful, the targeted service develops unavailable to its legitimate users. Researchers have been exploring different possibilities of DDoS countermeasures for several years, but these may not have been nearby to real-world implementers who want to comprehend the scope of possible solutions.

*A. Methodology:*The proposed work steps explained below:

Step 1: Initialize the server scenarios or network architecture.

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

Step 3: User sent the request of the Web Server if Web server is free then accept the Request then further request send 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 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.

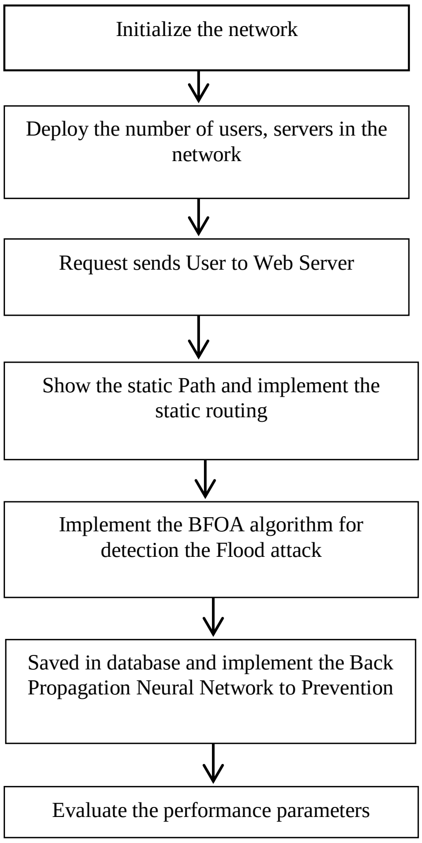
Initialize the network
Deploy the number of users, servers in the network
Request sends User to Web Server
Show the static Path and implement the static routing
Implement the BFOA algorithm for detection the Flood attack
Saved in database and implement the Back Propagation Neural Network to Prevention
Evaluate the performance parameters

Fig.3. Proposed Flowchart

Step 6: Apply the bacteria foraging algorithm for Detect the Flood Attack and performance define through the parameters like through put, packet sent etc.

Step 7: 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.

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

V. RESULT EXPLANATION

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. Therefore the used tools are

1) Least amount of 3 GB of RAM
2) Intel Pentium III Processor or over
3) MATLAB R2010a

MATLAB is a high appearance, language of technological computing. It incorporates calculation, apparition, and programmed environment. In addition, MATLAB is modern programming language surroundings: it has complex data structures, contains built-in editing and debugs tools, and supports object oriented programming. These factors make MATLAB a commendable tool for teaching and research.

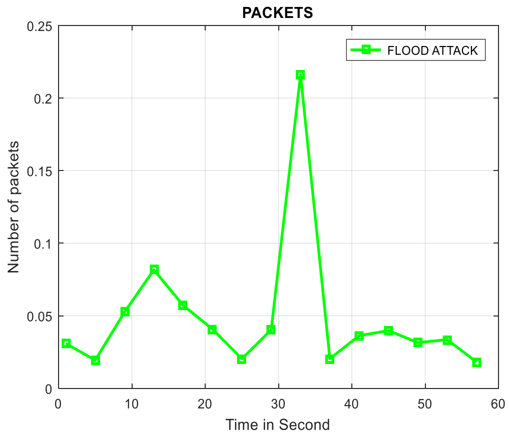

Fig.4. Packets with Attack

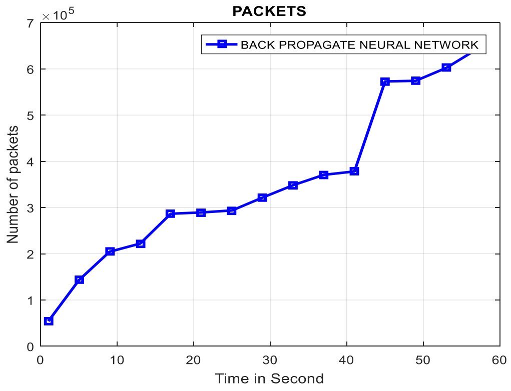

Fig. 5. Packets with BPNN

Fig.4. Described that the packet sent in the time according with a DDoS attack. Fewer Packets has sent because of the attack present in the server time and fig. 5 described that the packet sent in the time according using back propagation neural network. More packets have sent in the server side.

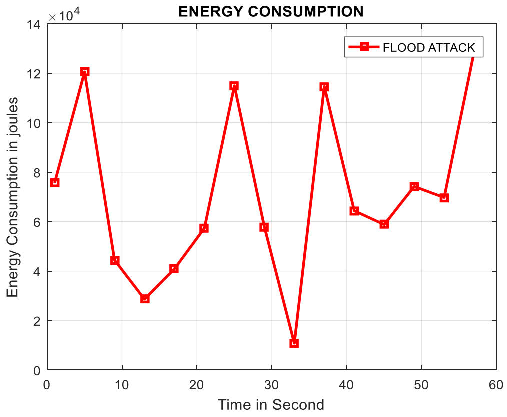

Fig.6. Energy Consumption

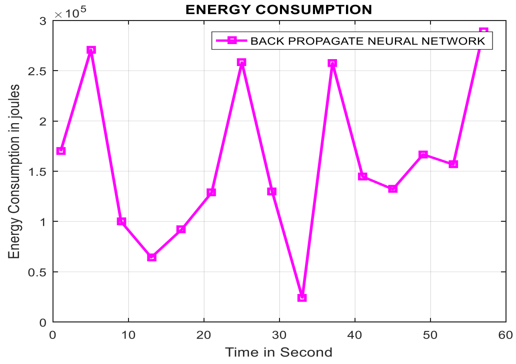

Fig. 7 Energy Consumption (joules) with BPNN

Fig.6. defines that that the Energy consumption parameter with DDoS attacks. AN increase the energy Consumption because of the attack has presented. The above figure defines that the Energy consumption parameter with BFO algorithm and Fig 7. Defines that the Energy consumption parameter with a back propagation neural network. Reduce the maximum energy consumption because of classification technique and mitigate the attacker effect.

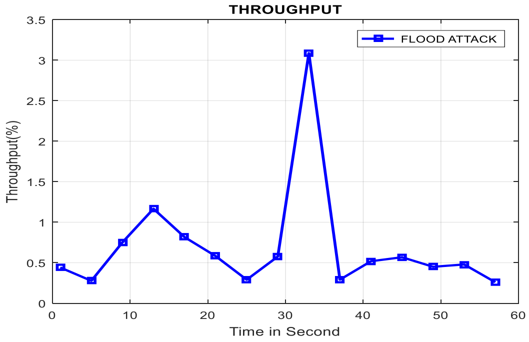

Fig. 8. Throughput Percentage with attack

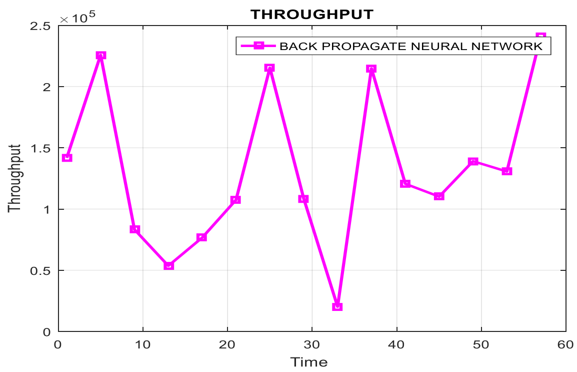

Fig. 9. Throughput with BPNN

DDoS attack presents the decrease the throughput performance. The above figure described the throughput means accuracy of the web server according to the time. Fig. 9 uses of back propagation neural network that increases the performance in the server side present.

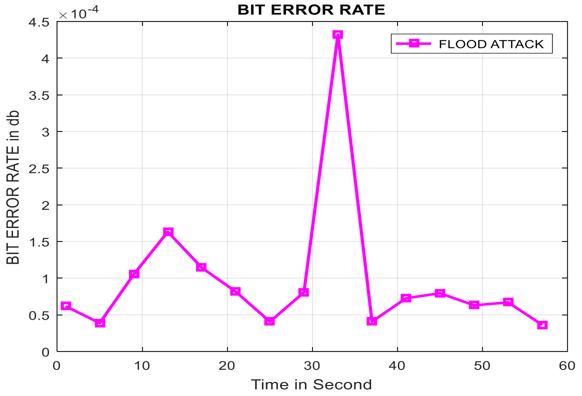

Fig. 10. Bit error Rate with attack.

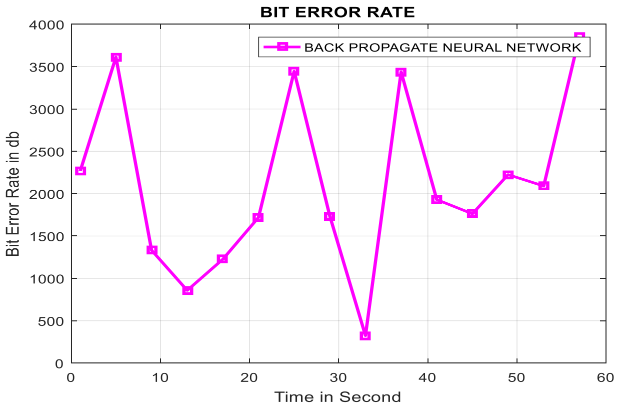

Fig. 11. Bit error Rate with BPNN

Fig.10. Described that the bit error rate parameter means hacker sent the request in the unnecessary request in the server side and fig. 11. Described that Server get hang and increase the overload along with delay in the server side. So, Back Propagation neural network prevention or mitigates the attacker effects and helps to reduce the error ration in the server.

II. Comparison of Parameters of Existing or Proposed Work

In this section the comparison of parameters are shown.

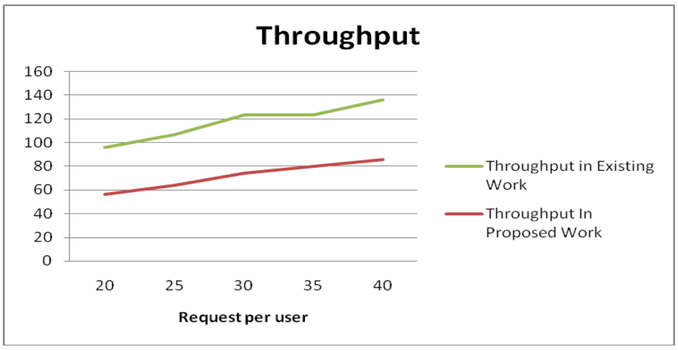

Fig. 12 Comparison of Throughput

Above figure defines the comparison between proposed work and existing work with FLOOD 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 FLOOD attack values is 40 and we achieved throughput with attacker value is 56.

TABLE I. Comparison of Throughput

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

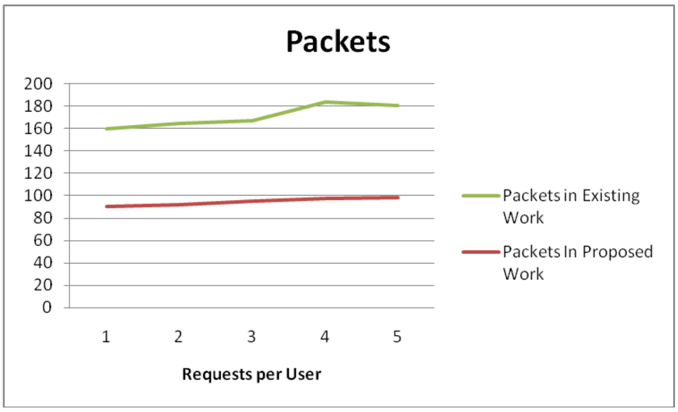

Fig. 13 Comparison of Packets

Above figure defines the comparison between proposed work and existing work with FLOOD 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 II. Comparison of Packets

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

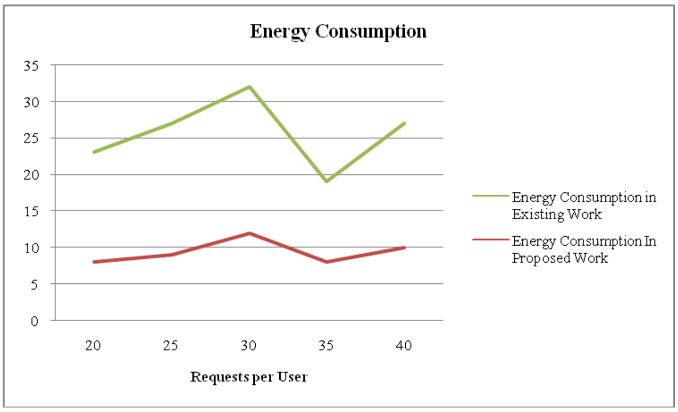

Fig.14. Comparison of Energy Consumption

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 III. Comparison of Energy Consumption

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

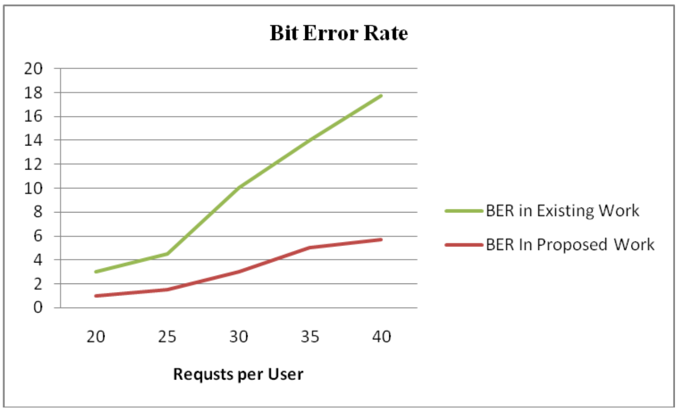

Fig. 15. Comparison of Bit Error Rate

Above figure defines the comparison between proposed work and existing work with FLOOD classifier. We improve the performance parameters of the BER with attack. Base paper BER in classifier values is 5.7 and we achieved BER with classifier value is 12.

TABLE IV. Comparison of Bit Error Rate

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

VI. CONCLUSION

The requirement of security and privacy increased day by day. Mostly the data is preferred to be sent and received through internet. It is a widely used way of communication. However, there are various concerns about the data such as privacy, authentication, integrity and safely arrival of data packets to the destination. While data transferred from one device to another the attacks occurred that halt the system and network. They came under various forms but in this research work, the main focus is on DDoS attacks that generate the unwanted requests to obtain the flooding at the network. After DDoS attack, the availability of resources is decremented. To overcome the problems of DDoS attack, BFOA and optimized BPNN algorithms are applied to enhance the performance of existing work which are obtained by SVM. The results after using these methods evaluates the improved throughput, sessions, packet delivery incremented and bit error rate, delay is mitigated.

In the future, the network dependent on more software to and there are various security systems that require security from different kinds of attacks. In the future, the security system become more flexible, scalable that support to the huge number of data centers. Main application areas are electronic toll plaza, automatic security systems

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] 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.

[6] 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.

[7] Mirkovic, Jelena, Gregory Prier, and Peter Reiher. "Attacking DDoS at the source." Network Protocols, 2002.Proceedings.10th IEEE International Conference on.IEEE, 2002.

[8] 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.

[9] 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.

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

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

[12] 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.