Comparative Analysis of Real-Time Prevention And Detection DDoS Attacks on Computer Network

Kanwarpal Singh[1], Dr. Shashi Bhushan[2]
M.Tech (Scholar), Professor
Department of Information Tehcnology, Chandigarh Engineering College, Landran, Punjab, India

Abstract – DDoS attack is a constant serious threat to the computer internet security. Various servers of several; companies have been the victims of such new type of attacks like as DDoS (SYN and FLOOD) attack is derived from the lower layers. APP layer depends on DDoS attacks use genuine Hyper Text Transfer Protocol requests after installed of TCP (Transport Control Protocol) three paths hand-shaking and over-whelms the victim resources like as a CPU (central Processing Unit), Memory, Disk and DB (database) bandwidth. In network layer depend on DDoS attack send the SYN and FLOOD attack UDP and ICMP REQs to the main server and exhausts the network bandwidth. Normal User Profile is designed form user's access nature instanced which is the base-line to differentiate DDOS attacks from crowd or rush. The main objective of this paper is to compare the real time prevention and classification method using BFOA, BPNN and SVM (Support Vector Machine). An experimental test bed with 7 application servers and 3 users and main server (Base Station) is used to generate the detection and classification these attacks (DDOS and SYN) with normal crowd. The system is tested with real-time traffic and the classification throughput and packet delivery rate is found to be greater than the machine learning methods.

Keywords:- DDOS attacks, Computer Network, UDP, TCP protocols and BFOA and SVM algorithm.

I. INTRODUCTION

Flood attacks have been one of the most relevant occurring intruders that badly issue the stability of the computer internet. Computer security main requirements on three columns:-

(i) Confidentiality
(ii) Availability and
(iii) Integrity [1]

The main threats in computer network security research are gap of confidentiality, authenticity failure and intruder denial of service.

The DOS (Denial of service) term was originally created by GLIGOR in an OS (Operating System) context, but it shows service of un-availability. It has been utilized in security research. Unlike the random losses which tend to affect a less number of nodes at a time Denial of service attack are designed to bring down all request nodes giving a particular service [2]. It involving more than single computer and more than one network to mount an attack on a main target in a co-ordinated manned is called DDOS (Distributed Denial of Service) attack.

The main threats to CS (Cyber Secuirty) is DDoS attacks in which target networks are attacked with high-volumne of attack data packets originating from a huge number of machines[3].

The objective of such attacks is to overload the victim with crowd of data packets and reduce it. In capable of performing normal services for genuine users[4].

IDS (Intrusion Detection System) is utilized to monitor computer network and sytem activities for attacks events or policy violations and produces reports to a MS (Management Station). ID is the procedure of monitoring the events occurring in CS (Computer System) or network and studying them for signs of possible incidents, which are damages threats of violatin of computer security policies, acceptable use policies or standard security.

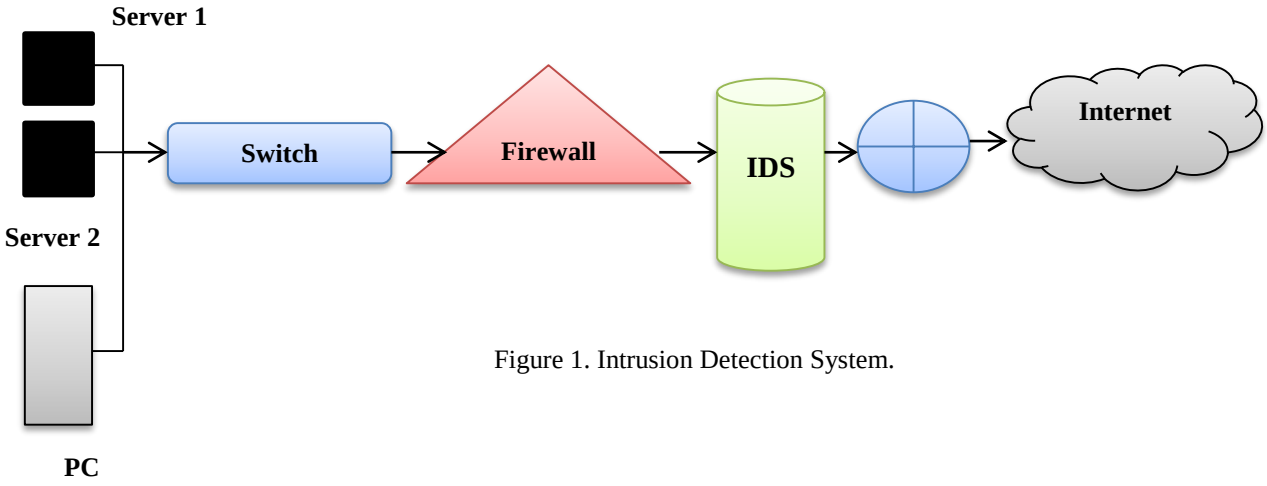

Figure 1. Intrusion Detection System.

There are two main keys of IDS (Intrusion Detection System's):-

(i) Network based and
(ii) Host based IDS[5].

In network depends IDS , the sensors are located at block points in the network to be considered, given at network perimeter. The Sensor caputes all network traffic or rush and analyses the content of individual data packets for malicious traffic.

In host based system, the sensor normally consists of a software agent, which considers all event of the host on which it is created, adding FS (File System), WLs (Web Logs) and Kernel [6].

Detection of Illegimate Distributed Denial of Services traffic presents a issue in protection of information and Communication resources. Continuous increase of Distributed Denial of Services attacks, since its first appearance in 2k is a direct evidence of rising issue, despite the continuous research of issue area and development of the novel detection and prevention methods that are used for a particular class of attack. But detection of ddos traffic, their correct classification (BPNN and BFOA) for applying methods of protection also represents a issue [7].

The main objective of this comparative study is to develop a structure of system depend on BFOA and BPNN for detection of DDoS attack (Traffic) and classification and optimization process in order to increase the throughput rate of detection of certain layers of ddos traffic and application of relevant methods of prevention. In existing work, SVM with string kernel used for better protection and reduce the load of the network.

In this research paper, explained the comparative study with proposed algorithm (BFOA and BPNN) and existing algorithm (SVM and ESVM). In this comparative paper , enhance the performance metrics like as a throughput, energy and end to end delay.

II. LITERATURE SURVEY

In this section, studied lots of paper and find the previous techniques and security methods. Distributed Denial of Service (DDoS) attacks have been a main apprehension for website owners for a while. All types of sites, from small to big, have been taken down and reserved offline because of them.

Shuyuan Jin et al., 2004 [8] discussed the effects of multivariatecorrelation analysis on the DDoS detection and proposes anexample, a covariance analysis model for detecting SYN floodingattacks. The simulation results show that this method is highlyaccurate in detecting malicious network traffic in DDoS attacksof different intensities. This method can effectively differentiate between normal and attack traffic. Indeed, this method can detect even very subtle attacks only slightly different from normal behaviours. **Lan Li and Gyungho Lee , 2005 [9]** presented a systematic method for DDoS attack detection. DDoS attack can be considered a system anomaly or misuse from which abnormal behaviour is imposed on network traffic. Attack detection can be performed via abnormal behaviour identification. Network traffic characterization with behaviour modelling could be a good indication of attack detection. Aggregated traffic has been found to be strong burst across a wide range of time scales. Wavelet analysis is able to capture complex temporal correlation across multiple time scales with very low computational complexity. They utilize energy distribution based on wavelet analysis to detect DDoS attack traffic. Energy distribution over time will have limited variation if the traffic keeps its behaviour over time (i.e. attack-free situation) while an introduction of attack traffic in the network will elicit significant energy distribution deviation in a short time period. **Bing Wang et al., 2015 [10]** examined the security impact, in particular, the impact on DDoS attack defences mechanisms, in an enterprise network where both technologies are adopted. They find that SDN technology can actually help enterprises to defend against DDoS attacks if the defences architecture is designed properly. To that end, we propose a DDoS attack mitigation architecture that integrates a highly programmable network monitoring to enable attack detection and a flexible control structure to allow fast and specific attack reaction. To cope with the new architecture, they propose a graphic model based attack detection system that can deal with the dataset shift problem. **Theerasak Thapngam et al., 2011 [11]** problems lead to defences systems requiring various detection methods in order to identify attacks. Moreover, DDoS attacks can mix their traffics during flash crowds. By doing this, the complex defences system cannot detect the attack traffic in time. In this paper, they proposed a behaviour based detection that can discriminate DDoS attack traffic from traffic generated by real users. By using Pearson's correlation coefficient, our comparable detection methods can extract the repeatable features of the packet arrivals. The extensive simulations were tested for the accuracy of detection. **Keunsoo Lee et al., 2007 [12]** generated enormous packets by a large number of agents and can easily exhaust the computing and communication resources of a victim within a short period of time. They proposed a method for proactive detection of DDoS attack by exploiting its architecture which consists of the selection of handlers and agents, the communication and compromise, and attack. They look into the procedures of DDoS attack and then select variables based on these features. **BrijBhooshan Gupta et al., 2011 [13]** employed to estimate number of zombies involved in a DDoS attack. The method does not depend on the frequency of attack and hence solves the problem of low detection precision and weak detection stability of ANN which occurs when used for low frequent attack estimation. The sample data used to train the feed forward neural networks is generated using

NS-2 network simulator running on Linux platform. **Wei Ren et al., 2007 [14]** studied the attacking principles based on analysis of the network capacity and classify these attacks into four categories: pulsing attack, round robin attack, self-whisper attack, and flooding attack. Then propose a defences scheme that includes both the detection and response mechanisms. The detection signals include the frequency of receiving RTS/CTS packets, frequency of sensing a busy channel (signal interference), and number of RTS/DATA retransmissions. The response scheme is based on the ECN marking mechanism. Through extensive ns2 network simulations, we demonstrate the existence of high good put and delay jitters under the pulsing attack mode.

III. PROPOSED RESEARCH GAP

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 [15]. 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.

The existing network device interfaces are closed and collaboration among multiple vendor software is a challenging issue. It creates a barrier for creating innovations in the networking. Due to the emerging trend of Internet, the network conditions are changing tremendously. It is difficult to perform real world experiments (deployment of new protocol) in a large production environment.

OpenFlow switch checks the incoming packet (packet header fields such as source port, destination port, source IP address, destination IP address etc.) against the flow entries, if a match is found then the specified action can be executed. Otherwise, the packet will be sent to the controller using PacketIn control message. When a large number of spoofed IP addresses packets are sent together, there will not be a match found in flow table and packet will be sent to the controller. Using this processing delay the malicious attacker can modify the flow entries and make the legitimate packet to be dropped, clone the flow table entries which leads to overflow in the flow table. There will not be enough memory space to accept the new flow instructions given by the controller. The controller tries to process the legitimate and spoofed packets continuously and its resources are exhausted. This can be described as DDoS attack against the controller. Under this attack [16], the controller becomes unreachable and it will not be able to process the new legitimate packets. Our approach treats this scenario as launching DDoS attack after establishing the connection between switch and controller.

Our 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.

IV. SIMULATION EXPERIMENTAL

In this describe the result analysis with attack, detection and prevention using Back Propogatinal Neural Network with BFOA. Compare the performance parameters with Throughput and packet sent etc.

In this research paper, BPNN and BFOA algorithm with network and application layer DDoS attack are indentified. BPNN with multiple layers are used to classify the attack from traffic which shows effective results in optimization and classification. Now, the packet count is used as the main parameter of detection with recover the packet losses and BPNN algorithm used to prevent the data packet and traffic issues resolved. The classification system phases are :-

(i) Normal Profile Creation (User Account).
(ii) Request Sent
(iii) Web server
(iv) Application Server
(v) Session
(vi) Attack generation
(vii) Pre-processing
(viii) Detection (BFOA)
(ix) Prevention or classification System
(x) Performance analysis.

Training Result is defined in Table 1. BPNN with BFOA and SVM (Existing algorithm) are number of layers and filter the data packets optimal values are fixed for the hidden neurons using iterations and error procedure.

TABLE 1: - TRAINING RESULTS

Hidden Neurons	Iterations	Best performance	Gradient	Mutation	R(Regression)
20	5	4.441e-09	5.2316e-08	1e-08	1

Testing section are Simulation Time are showed in Table 2. BPNN with BFOA compared with SVM algorithm.

Performance Metrics	Proposed Work (BPNN with BFOA)	Existing Work (SVM)
Throughput (%)	86	50
BER (Bit Error Rate) dbs	5.7	12
Packets (%)	98	83
Energy (j)	10	17

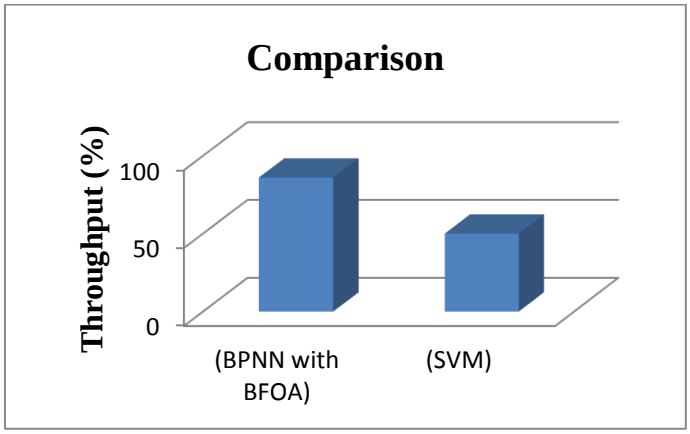

Figure 2. Throughput (%) with proposed and exitsing algorithm

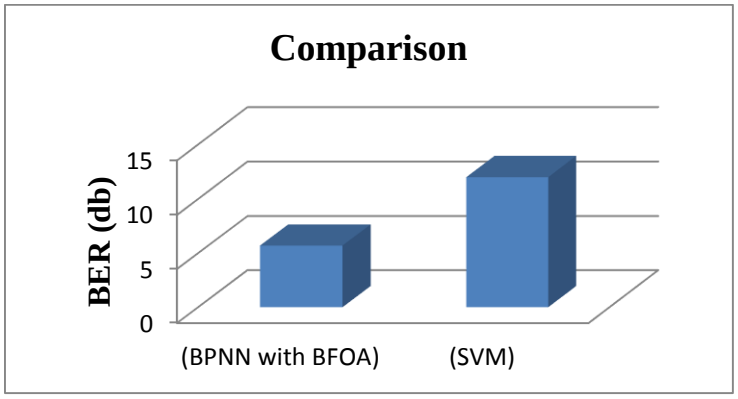

Figure 3. Bit Error Rate with Proposed (BPNN with BFOA) and Existing algorithm (SVM)

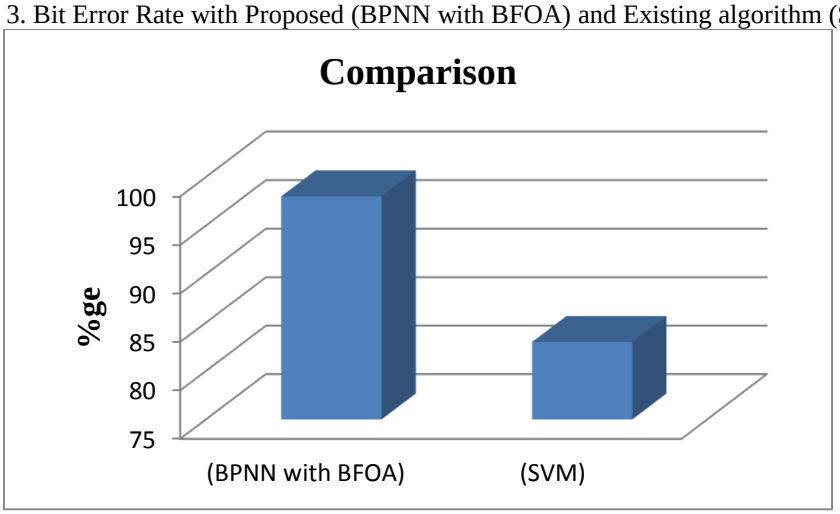

Figure 4. Packet with proposed (BFOA with BPNN) algorithm and Existing Algorithm (SVM)

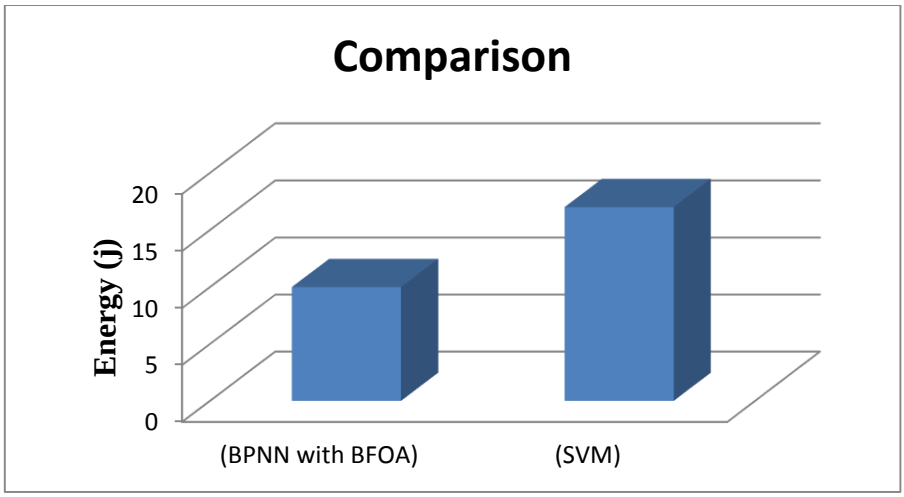

Figure 5. Compariosn Energy (j) with Proposed (BFOA with BPNN) algorithm and existing algorithm (SVM)

Figure. 2 shows the comparison of BFOA with BPNN with other DDoS attack detection. BPNN and BFOA results the better classification and detection results as compared to other SVM algorithm. In proposed work improve the performance parameters of the throughput with DDoS attack. Base paper throughput in FLOOD attack values is 40 and we achieved throughput with attacker value is 56. Figure 4 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. The above figure 5 define the energy consumption means in existing work energy consume more the attack had come then decrease the energy in the web server side. comparison between proposed work and existing work with FLOOD classifier. Figure 3 improve the performance parameters of the BER with attack. Base paper BER in classifier values is 5.7and we achieved BER with classifier value is 12.

V. CONCLUSION AND FUTURE SCOPE

In this paper, conclude the comparative study of the research work with various detection and protection (BFOA, BPNN) algorithm and SVM algorithm. 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 proposed work, we compared with the performance parameters like bit error rate value in proposed work 5.7 db and existing work value is 12 db. In energy consumption performance parameter value 10 joules and existing work value is 17 joules.

The future scope , can implement a clustering approach to detect the attacker moves in less time and save the user energy and efforts. Clustering algorithm will use to divide the request into two groups like Cluster 1 and Cluster 2. In this cluster will send request according to the server reply and enhance the accuracy rate and less overload the server and willnot exceed the session limit.

VI. REFERENCES

[1]. Li, M.,"Change trend of averaged Hurst parameter of traffic under DDOS flood attacks", *Computers & security*, vol *25*, no3, 2006, pp-213-220.

[2]. Bishop, M. A. ,"*Introduction to computer security* ",(Vol. 50). Boston: Addison-Wesley, 2005.

[3]. Kim, D. S., & Park, J. S.," Network-based intrusion detection with support vector machines", In *International Conference on Information Networking* (pp. 747-756). Springer, Berlin, Heidelberg,2003.

[4]. Peraković, D., Periša, M., Cvitić, I., & Husnjak, S.,"Model for detection and classification of DDoS traffic based on artificial neural network", *Telfor Journal*, vol *9*, *no.*1,pp- 26, 2017.

[5]. Kaur, P., Kumar, M., & Bhandari, A.," A review of detection approaches for distributed denial of service attacks". *Systems Science & Control Engineering*, vol *5*, no 1, pp- 301-320, 2017.

[6]. Garcia-Teodoro, P., Diaz-Verdejo, J., Maciá-Fernández, G., & Vázquez, E.,"Anomaly-based network intrusion detection: Techniques, systems and challenges", *computers & security*, vol *28*, no 1-2,pp- 18-28,2009.

[7]. Kumar, P. A. R., & Selvakumar, S.," Detection of distributed denial of service attacks using an ensemble of adaptive and hybrid neuro-fuzzy systems", *Computer Communications*, vol *36*, *no.* 3,pp- 303-319, 2013.

[8]. Jin, Shuyuan, and Daniel S. Yeung. "A covariance analysis model for DDoS attack detection." In *Communications, 2004*

IEEE International Conference on, vol. 4, pp. 1882-1886. IEEE, 2004.

[9]. Li, Lan, and Gyungho Lee. "DDoS attack detection and wavelets." *Telecommunication Systems* vol 28, no. 3-4, 2005, pp: 435-451.

[10].Wang, Bing, Yao Zheng, Wenjing Lou, and Y. Thomas Hou. "DDoS attack protection in the era of cloud computing and software-defined networking." *Computer Networks* vol 8, no. 1, 2015,pp : 308-319.

[11].Thapngam, Theerasak, Shui Yu, Wanlei Zhou, and Gleb Beliakov. "Discriminating DDoS attack traffic from flash crowd through packet arrival patterns." In *Computer Communications Workshops (INFOCOM WKSHPS), 2011 IEEE Conference on*, vol 4, no.3, 2011, pp. 952-95.

[12].Lee, Keunsoo, Juhyun Kim, Ki Hoon Kwon, Younggoo Han, and Sehun Kim. "DDoS attack detection method using cluster analysis." *Expert systems with applications, vol* 34, no. 3 , 2008, pp: 1659-1665.

[13].Gupta, Brij Bhooshan, Ramesh C. Joshi, and Manoj Misra. "ANN Based Scheme to Predict Number of Zombies in a DDoS Attack." *IJ Network Security* vol 14, no. 2 , 2012, pp: 61-70.

[14].Ren, Wei, Dit-Yan Yeung, Hai Jin, and Mei Yang. "Pulsing RoQ DDoS attack and defense scheme in mobile ad hoc networks." *International Journal of Network Security* , vol 4, no. 2 ,2007, pp: 227-234.

[15].Mirkovic, Jelena, Gregory Prier, and Peter Reiher. "Attacking DDoS at the source." Network Protocols, 2002.Proceedings.10th IEEE International Conference on.IEEE,vol 2, no. 2, 2002, pp:123-130.

[16].Ioannidis, John, and Steven M. Bellovin, "Implementing Pushback: Router-Based Defense Against DDoS Attacks." In *NDSS*, vol. 2, no.2 , 2002, pp: 23-34.