The Comparative Study of the DDOS Attack in Web Server based in Cyber Security in WSN

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

Abstract-- 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. 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.We implement firstly Initialize the server scenarios or network architecture. Secondly User sent the request of the Web Server if Web server is free then accepts the Request then further request sends the application server. Application Server reverts back to the Web server then web server reply the user. Attacker will come and hack the information means server will be down or increase the delay and overload of the server. 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 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.

Keywords-- DDos Attacks, Web Server, Genetic Algorithm and Back Propagation Neural Network.

I. INTRODUCTION

A network is a collection of two or more computer systems which are linked together to communicate with one another. It is a telecommunication network that agrees computers to exchange data. In computer networks, networked computing devices pass data to each other along data networks. The connections between nodes are established using either cable media or wireless media. The best known computer network is the Internet [1]. Different systems share resources available in the network. Shared resources can be of software type or hardware type. The devices that form network to exchange data are called network nodes. These nodes can include hosts such as personal computers, phones, servers as well as hardware. Computer networks differ on the base of physical media used to communicate their signals, the communication protocols used to organize network traffic, the size of the network, topology used in the network. Networks can be categorised as following [2]:

1. Transmission media based networks like wired networks (communication takes place through wires) and wireless networks (communication takes place wirelessly).
2. Network Size based networks like MAN, LAN and WAN.

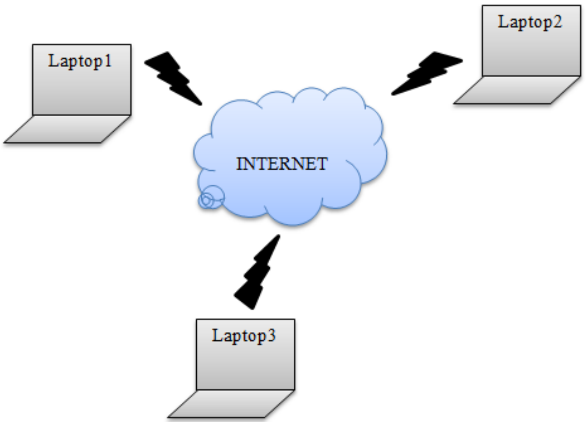

Fig 1: Representation of the Network

A. *Wireless Sensor Network*

A wireless sensor network sometimes called a wireless sensor and actuator network are spatially dispersed autonomous sensors to monitor physical or conservational conditions, such as temperature, sound, pressure, etc. and to submissively pass their data through the network to a main location. The more contemporary networks are bi-directional, also authorising control of sensor activity. The expansion of wireless sensor networks was motivated by military requests such as battlefield investigation; today such networks are used in many trade and consumer applications, such as industrial process monitoring and control, machine health checking, and so on[3].

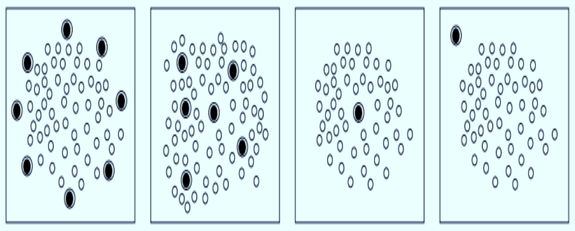

Fig 2: Sensor Network

- Cooperative Network of large amount of loosely connected nodes
- Wireless Communication medium
- Deployed only once
- Dispersed system tasked to sample environment for sensory information.
- Traffic moves Several Hops.

B. *Cyber Security*

Cyber security, also mentioned to as information technology safety, attentions on defensive computers, networks, packages and data from inadvertent or illegal access, change or obliteration. Importance of the cyber security i.e with the rising volume and complexity of cyber-attacks, on-going attention is compulsory to protect searching business and particular information, as well as protection general security [4].

The work is managed as gives Introduction and overview of the Wireless Sensor Network, Web Server and Cyber Security in section I; a study of the literature of these approaches and techniques for to improve the performance and to analyses and identify the Attack using Genetic Algorithm in Web server module in section II. It defined that the DDos Attack in section III. It used for proposed algorithm or simulation is described in section III succeeded by the research technique. Here discussed the problem formulation in section IV, The evaluation of performance parameters and consequences in section V followed by the conclusion and future scope in section VI.

II. Related Work

V.K SoundarRajam et.al,2013 [4] This paper 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 design information with summary false positive rate. **Ahmad Sanmorino et.al,2013 [5]** In this study, they discussed 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.**Bing Wang et.al, 2014 [6]** In this article, started by examined the security impact, in particular, the impact on DDoS attack defence 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 and a supple control structure to allow fast and specific attack reaction.**Shakti Arora et.al,2014 [7]** In this 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 individual 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 [8]** In this described as, the purpose of this study is to understand the flaws of prevailing solutions to fight the DDoS attack and a novel scheme is being providing 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.**SarraAlqahtani et.al,2015 [9]** This paper advocated a DDoS attack uncovering approach for service clouds and develops efficient algorithms to resolve the creating 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.

III. Distributed Denial of Services

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 [10] systems, such as network bandwidth and totalling power. 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.

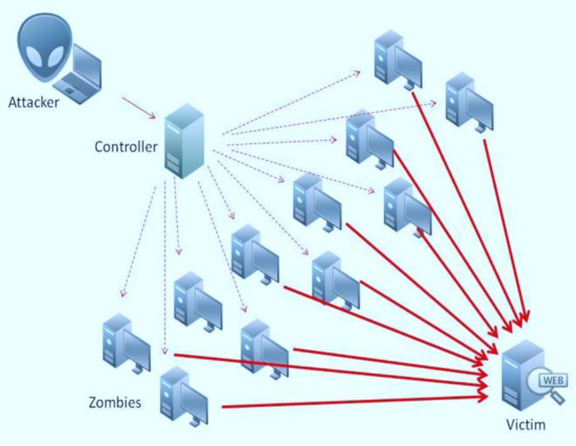

Fig 3: Distribution Denial of Services

Distributed Denial of Service attacks have posed a massive [11] 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 [12].

IV. OBJECTIVES

This thesis includes a set of purposes that is associated with milestone of this process. The objectives are declared below.

1. To Study of DDoS Attack and previous algorithms.
2. To implement algorithms for the detection and prevention of DDOS attack.
3. Compare the performance parameters with the existing Approach.

V. PROPOSE WORK

The proposed work steps explained in 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.

Step 6: Apply the Genetic Algorithm for Detect the DDoS Attack and performance define through the parameters like through put, packet sent etc.

Genetic algorithm is computer programs that simulator the processes of natural evolution in order to solve difficulties 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 biological re-combination between two 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 organized.

The Genetic Procedure is a model of machine knowledge which derives its performance from image of the processes of Evolution in environment. This is done by the creation within a machine of a Populace of Individuals represented by Chromosomes, in spirit a set of character strings that are similar to the base-4 chromosomes that we see in our own DNA. The individuals in the populace then go through a process of evolution.

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.

This Neural Network is a multi-layered, feed forward 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. Evaluate the performance parameters like Throughput, Packet sent etc.

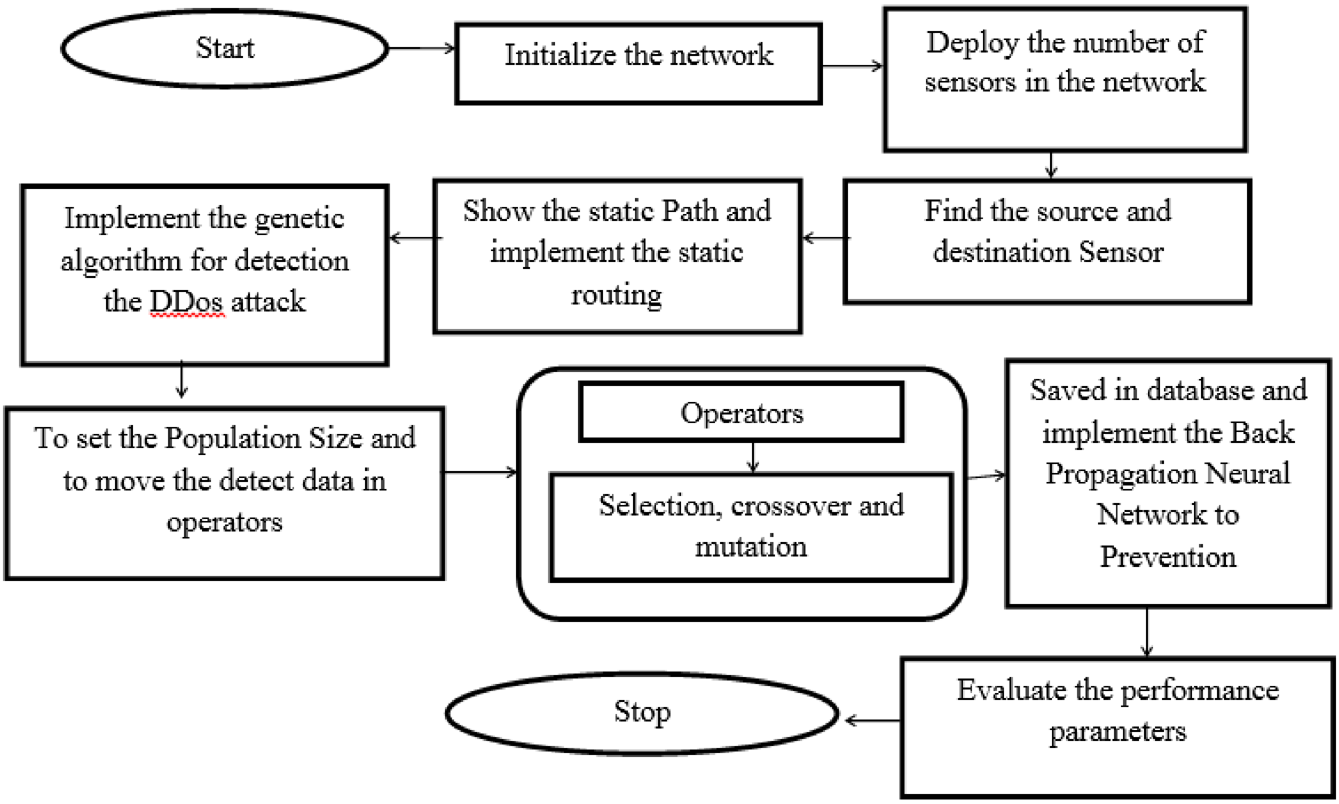
Start
Initialize the network
Deploy the number of sensors in the network
Find the source and destination Sensor
Show the static Path and implement the static routing
Implement the genetic algorithm for detection the DDos attack
To set the Population Size and to move the detect data in operators
Operators
Selection, crossover and mutation
Saved in database and implement the Back Propagation Neural Network to Prevention
Evaluate the performance parameters
Stop

Fig 4: Proposed Flow Chart

A. Pseudo Code of Genetic Algorithm

```
Input :
    a)  population size A
    b)  Elitism rate B
    c)  Mutation C
    d)  Iterations/gens D
Output: Solution Y
//Definition
    1.  Initialize A randomly solution feasible;
    2.  Save all the random solution in the population popl;
    3.  For i=1 to D do
    // elitisim
    Number of elitism ne=A.B;
    Select the positive outfit ne solutions in popl and save in popl;
    // Crossover
    Number of crossover Nc-(A-ne)/2;
    For j=1 to nc do
    Random selection two solutions X1 and X2;
    Save X3 and X4 to popl;
    End for
    //Mutation
    For j=1 to ns do
    Selct a solution Xi from popl;
    Mutation each bit of Xi with the feasible output by modifying Xj';
    End if
    Change Xj with Xj n popl;
    End for
    // Changing
    Change popl=popl1+popl2;
    End for
    // Refining the fit solution.

    Return the fit output x in popl;
```

B. Pseudo Code of Fitness Function

```
    // Intialization the fitness Fucntion

    a)  Fs= each Features of chromosomes
    b)  Ft=Total Features of Chromosomes
    And
    c)  E= Classification error rate

        Input: fvalue
        Output: Fs,Ft, e
```

```
iffs<ft
fs=0;
else
ft=1;

end if
```

C. *Steps defined in Genetic Algorithm*

- Initialize random population od n genes
- Fitness calculate fitness of each genes x in the population
- Novel population define a novel population by repeat following steps until the novel population is fully complete.

a) Initialize two parent genes from population acc. To their fit value
b) Crossover with a divide probability cross over the further child to form new offspring
c) With a last modification probability mutate novel of string in every locus.
d) Place novel offspring in the latest algorithm.
e) use new genes population for a new run of the algorithm.

VI. CONCLUSION

Network layer DDoS attacks are effectively generated and distinguished by proposed genetic algorithm used in real time difference detection system designed using BPNN with best validation performance. BPNN training results the classical file which consists of sets of normal behavior. During Back Propagation Neural Network testing, classification system classifies the incoming flows as attack or normal flow by using model file created during training. Validation check and testing are used for classification. Best performance produces the better classification accuracy as compared to other functions. Genetic algorithm used for detection and BPNN used for classification. Increase the performance in Packet sent and throughput.

REFERENCES

[1]. 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.

[2]. 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.

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

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

[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]. Anantvalee, Tiranuch, and Jie Wu. "A survey on intrusion detection in mobile ad hoc networks." Wireless Network Security.Springer US, 2007. 159-180.

[8]. 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.

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

[10]. Jae-Hyun Jun, Hyunju Oh, andSung Kim. "Real time detection and classification of DDoS attacks using Enhanced SVM with string kernels." Recent Trends in Information Technology (ICRTIT), 2015 International journals on. IEEE, 2015.

[11]. Watteyne, Thomas, and Kristofer SJ Pister. "Wireless Sensor Networks: Technology Overview." The Internet of Things: Connecting Objects to the Web (2013): 53-95.

[12]. Haykin, Simon, and Neural Network. "A comprehensive foundation." Neural Networks 2.2004 (2004).