*International Journal of Engineering & Technology*, 7 (1.2) (2018) 6-8

International Journal of Engineering & Technology

*Website: www.sciencepubco.com/index.php/IJET*

***Research paper***

# Dos invasion at network by intruder; protection mechanism by "anti-dos invasion firewall"

**Govindaraj. S [1] *, V.Khanaa.S [2], C. Rukkumani [3]**

[1] *Research Scholar, Bharath Institute of Higher Education and Research*
[2] *Professor, Department of CSE, Bharath Institute of Higher Education and Research*
**Corresponding author E-mail: iiirpublication@gmail.com*

**Abstract**

Every cyber-warfare done by criminal perpetrators motto is not to know information and data, but are interested in denial of service assaults which never attempt to breach the security or firewall, Rather to intend the network surge for particular span of time and denial of access which ultimately target end legitimate user through two method of DOS attack (crash service or flooding service).The main problem with the "Denial Of Service" attack that it will lead to network surge or corruption of data which is transfer or processed from source to destination via some transmission techniques through network.

***Keywords***: *Dos; Network; Invasion; Intruder; Anti-Dos Invasion Firewall. Spectral Estimation; Coefficient Estimation; LMS; RLS; Improved RLS; Power Spectral Design; PDF.*

## 1. Introduction

The "Denial of Service" invasion is done by intruder and they may try for network surge which will disrupt normal flow the source and destination targeting specific span of period which will ultimate affect the overall processing that network. At that time span they may try to hack or corrupt the data which is being transferred between systems through network. The main problem with the "Denial of Service" attack that it will lead to network surge or corruption of data which is transfer or processed from source to destination via some transmission techniques through network. There are various techniques of DOS attack which are prevented by n number of defence mechanism for combating the "Denial of Service" attack with current trend of world.

I). Related work

V.Priyadharshini, Dr.K. Kuppusamy have proposed a new cracking algorithm is implemented to stop that DDOS attacks. The algorithmic design a practical DDOS defense system that can protect the availability of web services during severe DDOS attacks. The proposed system identifies whether the number of entries of client exceeds more than five times to the same sever, then the client will be saved as an attacker in blocked list and the service could not be provided. So algorithm protects legitimate traffic from a huge volume of DDOS traffic when an attack occurs [1].

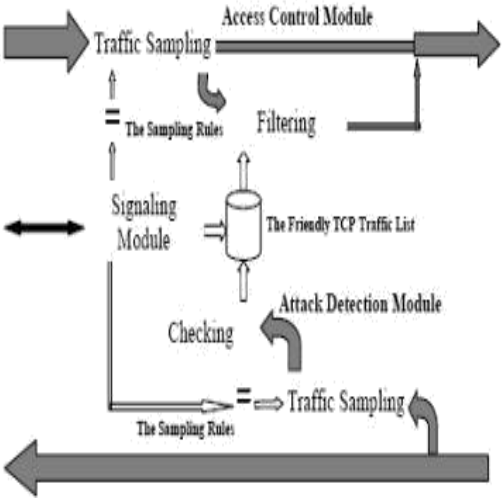
S.Malathi and Dr.K.Kuppusamy have proposed DDoS attacks to prevent our files, the concept of file watcher, IP watcher and firewall are used. File watcher is responsible to monitor the file stored in the home directory and analyze the modification made in the file. In addition, the IP address that modifies the file can be detected by IP watcher. When the client sends request to modify the file, the file watcher deny the service provided to the user and thus prevent the file from attack. The IP Address of the client who sends attack on the file is blocked by adding its address to the blocked list of the firewall. The clients who's IP Address are in the blocked list can't have permission to access the file further. Thus the file is prevented from the attacks. In his paper, a new method has been proposed to watch the activities taken in tne file and to prevent the file from modifications by other users. [2]

Vyas Sekar, Nick Duffield, Oliver Spats check, Kobus van der Merwe and Hui Zhang have proposed the design space for in-network DDoS detection and propose a triggered, multi-stage approach that addresses both scalability and accuracy. Our contribution is the design and implementation of LADS (Large-scale Automated DDoS detection System). The attractiveness of this system lies in the fact that it makes use of data that is readily available to an ISP, namely, SNMP and Net flow feeds from routers, without dependence on proprietary Hardware solutions. We report our experiences using LADS to detect DDoS attacks in a tier-1 ISP [3]

There are significant work done to protect victims from DDoS attacks by active filtering method [4].

Kandula et al proposed a system to protect a web cluster from DDoS attacks by CAPTCHAs in which the users who solve the puzzles can only get access to the services. This method assumed that human users can identify the distorted images, but the machine can't [5].

In StackPi, a packet is marked deterministically by routers along its path towards the destination. The victim can associate Stackpi marks with source IP addresses to detect source IP address spoofing [6].




A Multi-Queue Algorithm for DDoS Attacks.

Algorithm for gateway and router to prevent DDoS attacks. The algorithm combines two simple congestion control methods. Simulation results show that our algorithm efficiently increases thethroughput of normal flows under DDoS attacks comparing to common Drop Tail algorithm.

1) Drop tail algorithm ->

Drop Tail algorithm implement in the link with responsive flow for detect the TCP packet flow. Drop Tail became a failure since unresponsive UDP packets will occupy most of the queue there by causing responsive flows packets to be drop.

2) Random early detection (RED) ->

Random Early Detection is implemented on the unresponsive flow link. For detect the UDP packet Flow. The objective of this mechanism is to minimize packet loss and queuing delay, maintain high link utilization and remove biases against burst sources. It is implemented on a router or gateway to control congestion caused by DDoS. [7]

II). Proposed system

This paper approach is based on creating an 'ANTI-DOS INVASION FIREWALL' as defence system which will kept between the data transferred or processed from source and before it reaches destination target. The data transmitted will be also encrypted for anti-invasion purpose from intruders of network transmission which will be decrypted only after reaching targeted destination from source system.

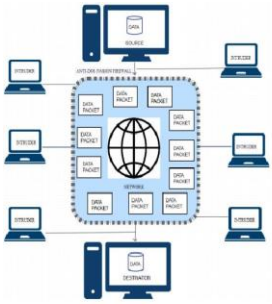
The goal of this paper is for making new technology to combat DOS attack by intruders in network. Our new technology comprises of "ANTI-DOS INVASION FIREWALL" which combats against attack and also protects the data getting malicious or infected by intruder for cyber warfare intend by criminal perpetrators. The aim of DOS attack is to cripple the network service and steal the data.

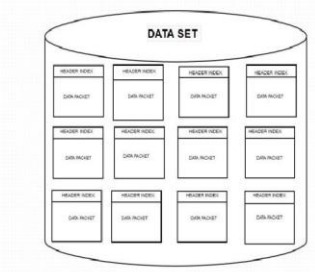
## 2. Methodology

### 2.1. Anti-dos invasion firewall algorithm

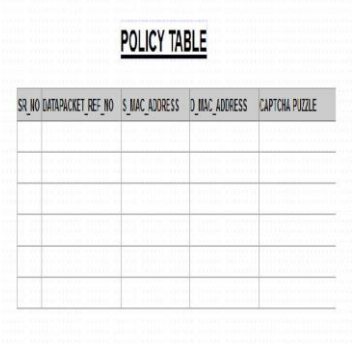
Initiate Process transmission DP=Data packet reference number; T=Traffic enter into the network; S=Source MAC address; D=Destination MAC address; CP=Captcha puzzle;
CA=Captcha Acknowledge; HI=Header
Index; HI=DP+CP;
Accept inbound traffic
{
Analyze each time HI,
If (T==S||T==D) then,
{
Proceed to check Captcha
If (CP==CA)
{
Accept the request from the Source Send the response to Source. Permission Granted For Access.
}
Else
{
Request Transmission Again!!!
}
}
Else
{
Add that T as intruder,
Display: "Access Permission Denied"
}
}
Terminate Process Transmission

### 2.2. Block diagram










### 2.3. Anti-dos invasion firewall procedure

- Transmit data from source to destination
- Divide the transmission data into data packets
- Add header index to each data packet
- Header index will contain 'MAC address' of sender & receiver ,data packet reference number & captcha
- To grant access credential's to each data packet have to solve CAPTCHA puzzle at each data packet
- Accept inbound traffic
- Analyze header index
- Load policy table of header index
- Compare 'MAC addresses' as well as 'captcha puzzle' with policy table
- Validate each data packet policy
- If validation is true
- Then allow inbound traffic & Grant access credential's for data access
- Else reject inbound traffic
- Skip rejected inbound traffic
- Check next inbound traffic in spool

## 3. Conclusion

According to our research paper we can manage "Denial of service" using our methodology "ANTI-DOS INVASION FIREWALL" which Consists of Mac Address Filtering from the in-

bound traffic at network entry point .The firewall checks the header index of data packet which comprises of source and destination MAC Address, Data packet Header reference no. , Captcha puzzle.

The inbound traffic will be validated with "ANTI-DOS INVASION FIREWALL" which uses policy table to compare inbound traffic at entry point or exit point of network if the inbound traffic MAC Address does not matches it will be added to intruder list and considered as invasion threat alert at network.

Once the validation of MAC Address is complete the inbound traffic which matches will be allowed to access captcha puzzle; Incase captcha solved by that user doesn't get approved then the user will be prompted for as "Alert: two more try remaining!!!" for captcha otherwise the user will blocked and will be added to intruder list further access will denied completely.

## References


[1] V.Priyadharshini, ""Prevention of DDOS Attacks using New Cracking Algorithm"," international Journal of Engineering Research and Applications(IJERA), vol. 2, no. 3, May-June 2012.

[2] C. K. Kuppusamy.S.Malathi, "("An effective prevention of attacks using giTime frequency algorithm under ddos")"," International Journal of network Security&Its Applications (INSA), vol. 3, no. 6, November 2011.

[3] V. Sekar, ""Large-scale Automated DDoS detection System"," AT&tLabs-Research-AnnualTech'06, 2006.

[4] R. B. A. W. Z. Dong Xuan, ""A Gateway-based Defense System for Distributed DoS Attacks in High-Speed Networks"," IEEE, pp. 5-6, June 2001.

[5] D. J. &. B. S.Kandula, ""Botz-4-sale: surviving organized DDoS attacks that mimic flash crowds"," NSDI-Networked Systems Design and Implementation.

[6] S. &. Y. Perrig.A, ""StackPi: a new defense mechanism against IP spoofing and DDoS attacks"," CMU echnical Report, 2003.

[7] U. M. a. J. H. G. Thatte, ""Parametric Methods for Anomaly Detection In Aggression Traffic","