ISSN: 2321-8169
020 – 023

An Efficient Approach to Detect and Mitigate Denial of Service Attack

Vishal Kale
Mtech second year Computer Science Department
Vidharbha Institute Of Technology
Nagpur, India
vishal.kale1209@gmail.com

Prof. Pravin Kulurkar
Assi. Professor Computer Science Department
Vidharbha Institute Of Technology
Nagpur, India
pravinkulurkar@gmail.com

Abstract— Todays internet suffering from the distributed denial of service attack. Dos is very recent and popular and has tremendous effect on internet. Dos has different types to effect the integrity, availability, and security of an any architecture. Today's process to eliminate the Dos is not too much effective. So it essential to detect and mitigate the Denial of service attack. So this paper proposes a system to detect and eliminate the denial of service attack. To eliminate the denial of service attack Token Bucket Algorithm (TBA) is using. In this paper we showing the simulation of different parameter using network simulator NS2.

Keywords- *Distributed denial of service attack, Token bucket algorithm*

*****

I. INTRODUCTION

Today there more upcoming technology and research going on so that a normal people can enjoy the internet fast. Today everyone confident that internet is very fast and secure. But in reality the current internet is prone to attacks. Attackers exploit the existing network infrastructure and their benefits for illegal activities. DDoS attacks are characterized by surge of traffic without packet content signature from millions of zombies mostly with forged source address. Internet is a complex network due to changes in network traffic load, mix of traffic, mix of congestion control actions, on/off flows because of which the statistics of arriving traffic is not stationary. The available link bandwidth varies in accordance with the statistics of the input traffic. Various sophisticated DDoS attack tools are available in Internet so known attack pattern can be detected easily whereas the reasons for new attacks remain undiscovered. Collecting and analysing huge amounts of traffic logs after attack can't help in detecting new attacks. DDoS attack is very complex since it is distributed in nature where a master owns millions of insecure machines called zombies who act according to the master command to overwhelm the victim (Internet servers) with huge volume of packets. So it needs immense effort to propose a solution that defends DDoS attack very effectively and efficiently. Defence mechanism is robust if and only if it has an efficient detection methodology. But the problem lies in the basic understanding of what attack traffic will look like. A need for DDoS impact metric arises which takes in account of several network performance metrics like packet loss, latency, link utilization and throughput. These network performance metrics serve as an effective indicator that reflects anomalous changes very well. Most predominant attacks are flooding attacks which are a Distributed Denial of Service leading to resource damages. The garbage packets which follow UDP protocol affect the legitimate TCP packets and hence this unidirectional traffic accounts for aggregate traffic at the router . It is one of the most serious problems on the Internet. A master (attacker) recruits many machines (zombies) to send garbage of packets thus launching a DDoS attack. Huge volume of unwanted traffic is generated to consume the bottleneck link in the victim network. A DDoS attack will eventually shut down the Internet servers by exhausting resources thereby denying access to legitimate users.

An efficient defensive mechanism for DDoS attacks is essential to detect and defend as quickly as it could. To achieve this, researchers need a deep understanding of dynamics of the packets, traffic traces which can depict realistic data, characteristics of the attack traffic, statistics of data flow, a platform where they can run their experiments without any complications. DDoS defence evaluation can provide a large improvement in the state of the art for DDoS defence evaluation and a significant step towards a common evaluation methodology. The immediate task of DDoS defence is to provide enormous bandwidth to legitimate users when there is an attack. Unfortunately most current defence approaches cannot efficiently detect and filter out the attack traffic. The proposed approach discussed in this paper finds the network anomalies, deploy the system at distributed routers, identify the attack packets, and then filter them. Thus the legitimate traffic throughput is improved and attack traffic throughput is reduced. The proposed Token Bucket Algorithm (TBA) can perform well in mitigating DDoS attack traffic precisely and effectively.

II. RELATED WORK

To achieve the objective of this project, we have proposed technique called Token bucket Algorithm (TBA) for detection and mitigation of denial of services attack . The token bucket is an algorithm used in packet switched computer networks and telecommunications networks. It can be used to check that data transmissions, in the form of packets, conform to defined limits on bandwidth and burstiness (a measure of the unevenness or variations in the traffic flow). The token bucket can be used in either traffic shaping or traffic policing. In traffic policing, nonconforming packets may be discarded (dropped) or may be reduced in priority (for downstream traffic management functions to drop if there is congestion). In traffic shaping, packets are delayed until they conform. Traffic policing and traffic shaping are commonly used to protect the network against excess or excessively bursty traffic. We are showing our result with the help of the network simulator (NS2) with different parameter.

Token Bucket:

- The Token Bucket Algorithm can apply at router for the congestion control.
- The Token Bucket Algorithm compare allow the output rate vary depending on the size of burst.
- In this algorithm the buckets holds token to transmit a packet, the host must capture and destroy one token.
- Tokens are generated by a clock at the rate of one token every Dt sec.
- Idle hosts can capture and save up tokens (up to the max. size of the bucket) in order to send larger bursts later.

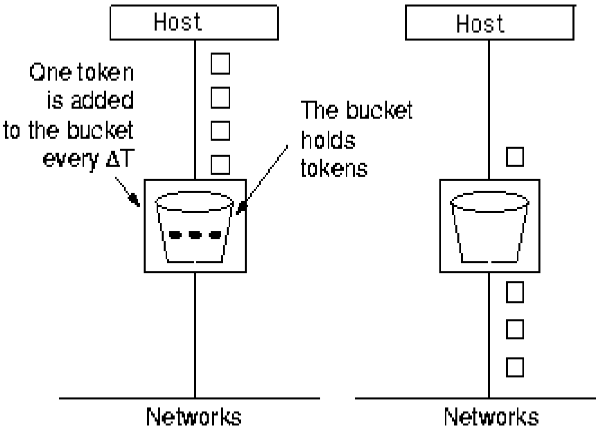

Fig 1.Working of Token Bucket Algorithm

The architecture consists of one server and many client. Different client will send the request through different router. The token bucket algorithm is applied at the router.

ALGORITHM

Step - 1 : A token is added at every Δt time.

Step - 2:The bucket can hold at most b-tokens. If a token arrive when bucket is full it is discarded.

Step - 3 : When a packet of m bytes arrived m tokens are removed from the bucket and the packet is sent to the network.

Step – 4 : If less than n tokens are available no tokens are removed from the buckets and the packet is considered to be non-conformant.

The non conformant packet may be enqueued for subsequent transmission when sufficient token have been accumulated in the bucket.

If C is the maximum capacity of bucket and ρ is the arrival rate and M is the maximum output rate then Burst Length S can be calculated as

$C + \rho S = MS$

III. PROBLEM DEFINITION

In the existing system there is used of IBRL(Interfaced Based Rate Limiting) Algorithm for the detection and mitigation of Ddos but there is fixed rate transmission of packet to check the detection of attack[13]. Due to the used of fixed rate the packet drop increased at the router of legitimate user. Also DDoS attacks appeared as a serious threat to the Internet in the history and have since experienced a rapid development of techniques to prepare and perform the attack and to avoid detection. However, it is maturing to the point where even unsophisticated intruders could do serious damage.

IV. PROJECT OBJECTIVES

The objective of proposed techniques is
1 .To provide the available bandwidth to the user.

2. To provide the system which efficiently detect and filter out the attack on architecture.

3. To keep a server free from serving the unwanted request.

4. To reduce processing time of request from the legitimate user.

V. INVESTIGATIONAL OUTCOME

To achieve the objective of this project, we have proposed following techniques;
-We are showing our result with the help of network simulator (NS2). We are using AODV protocol in the network for communication. The simulation model consist of two scenario in the diagram listed below.

1- Normal Architecture

2- Attack on Architecture.

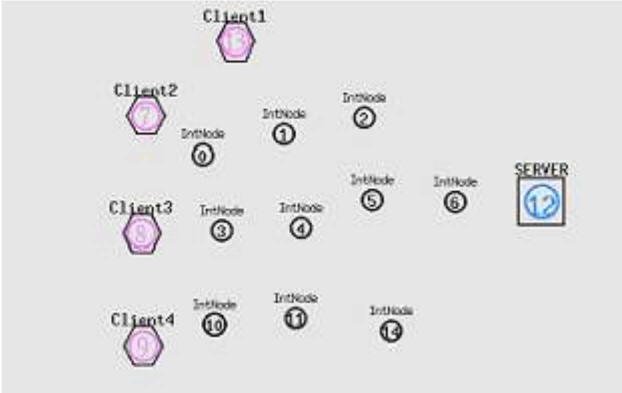

Fig 2. Normal Architecture

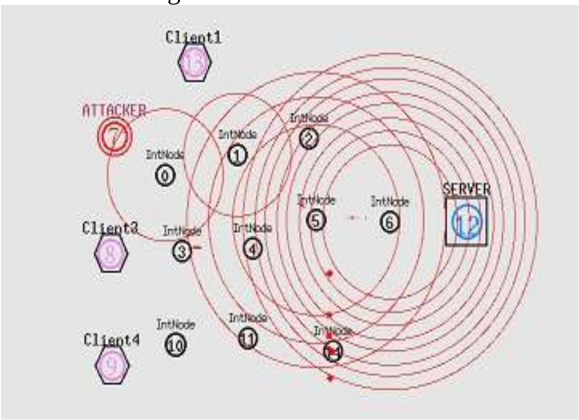

Fig 3. Attack on Architecture

V. VI. SIMULATION RESULT

I. LATENCY

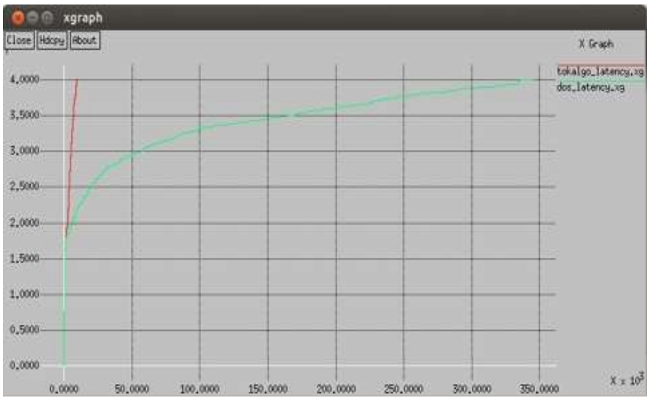

Fig 4. Latency

Latency is the amount of time a message takes to traverse a system. It is the time taken for a packet to travel from a host to another.

So,means it is time vs time graph ie. on x-axis there is time (sec) from which packet starts to traverse and on y-axis there is time(sec) at which traversing process end.

II.DELAY

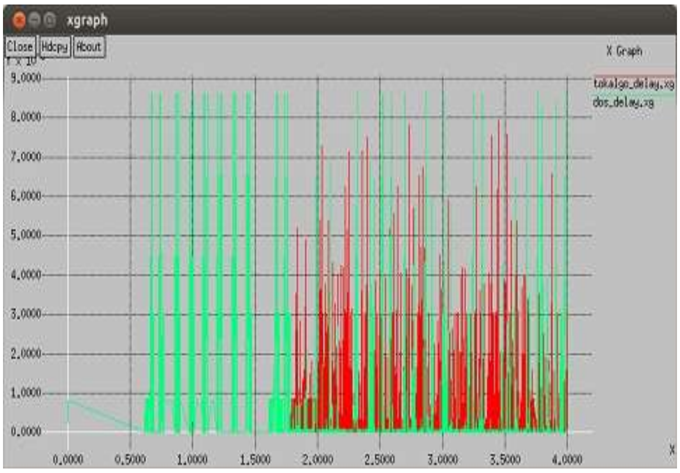

Fig 5.Delay

The average time taken by a data packet to arrive in the destination is called delay. It also includes the delay caused by route discovery process and the queue in data packet transmission. Only the data packets that successfully delivered to destinations that counted. In above graph, x-axis shows the time in sec and y-axis shows the time in ms.

III.THROUGHPUT

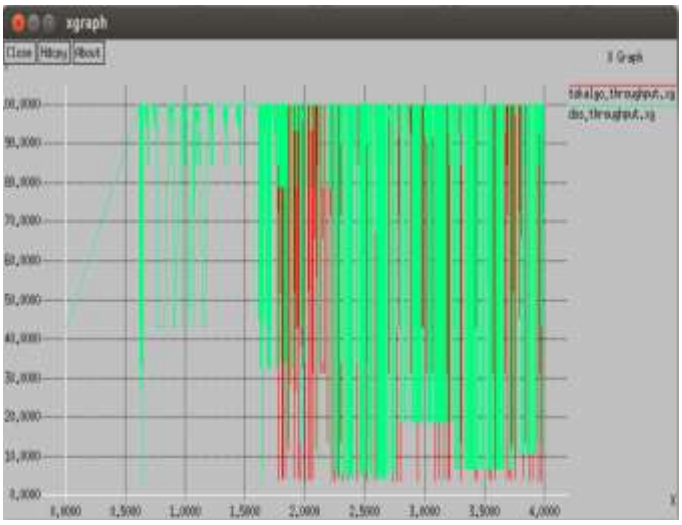

Fig 6. Throughput

The network throughput is the average of successful message delivery over a communication channel. The throughput is usually measured in bits per second or data packets per time slot. In above graph,x-axis shows time in sec and y-axis shows average throughput in bits/sec.

IV.JITTER

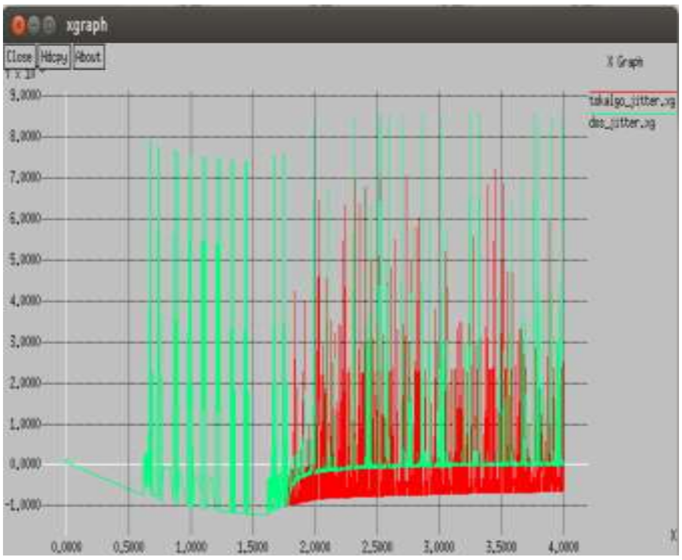

Fig 7.Jitter

Jitter is **defined** as a variation in the delay of received packets. In the above graph, x-axis shows the time in sec and y-axis shows the jitter.

VI. CONCLUSION

This paper proposes a technique to prevent the server from the distributed denial of service attack. In this paper we are showing client server architecture under the distributed denial of service attack. The complete elimination of dos attack is infeasible. This paper will show simulation of different affected parameter under Dos Attack and can become quite significant.

REFERENCES

[1] F. Liang and D. You, “Using Adaptive Router Throttles against Distributed Denial-of -Service Attacks”, Journal of Software, vol.13, issue. 7, pp. 1120-1127, 2002.

[2] K. Argyraki and D. Cheriton, “Active Internet Traffic Filtering: Real- Time Response to Denial-of-Service Attacks”, USENIX, 2005.

[3] J. Mirkovic, B. Wilson, A. Hussain, S. Fahmy, P. Reiher, R. Thomas and S. Schwab, “Automating DDoS Experimentation”, in Proc. of the DETER workshop, August 2007.

[4] J. Mirkovic, E. Arikan, S. Wei, S. Fahmy, R. Thomas and P. Reiher, “Benchmarks for DDoS Defense Evaluation”, in MILCOM, 2006.

[5] J. Mirkovic and P. Reiher, “A Taxonomy of DDoS Attacks and Defense Mechanisms”, ACM SIGCOMM Computer Communications Review, vol. 34, issue.2, pp.39-54, April 2004.

[6] R.Mahajan, S. Bellovin, S. Floyd, V. Paxson and S. Shenker, “Controlling High Bandwidth Aggregates in the Network”, ACM Computer Communications Review, vol.32, issue.3, pp. 62-73, July 2002.

[7] D.K.Yau, J.C. Lui, F. Liang and Y. Yam, “Defending against Distributed Denial-of-Service Attacks with Max-Min Fair Server- Centric Router Throttles. ACM Transaction on Networking”, vol. 13, issue.1, pp.29- 42, February 2005.

[8] J.Mirkovic, M. Robinson, P. Reiher and G. Oikonomou, “Distributed Defense against DDoS Attacks”, University of Delaware CIS Department Technical Report CIS-TR-2005-02, 2005.

[9] Yinan Jing, Xueping Wang, Xiaochun Xiao and Gendu Zhang, “Defending Against Meek DDoS Attacks By IP Traceback-based Rate Limiting”, Global Telecommunications Conference, GLOBECOM '06. IEEE, December 2006.

[10] M.Sung and J. Xu, “IP Traceback-based Intelligent Packet Filtering: A Novel Technique for Defending against Internet DDoS attacks”, in Proc. of 10th IEEE ICNP, Paris, France, November 2002.

[11] F.Kargl, J. Maier and M. Weber, “Protecting Web Servers from Distributed Denial of Service Attacks”, in Proc. of 10th International World Wide WebConference, May 2001.

[12] Monika Sachdeva, Krishan Kumar, Gurvinder Singh and Kuldip Singh, “Performance Analysis of Web Service under DDoS Attacks”, IEEE International Advance Computing Conference (IACC 2009) Patiala, India, 6-7, March 2009

[13] B.S. Kiruthika Devi, G. Preetha, S. Mercy Shalinie,”DDoS Detection using Host-Network based Metrics and Mitigation in Experimental Testbed ” ICRTIT-2012