Defending DDoS Attack: Implementation of SFQ with CBQ and MLADS

Prof. Gayathri. R
School of Computer Science and Engineering
VIT university
Chennai-600127,Tamilnadu, India

Karthick. M
School of Computer Science and Engineering
VIT university
Chennai-600127,Tamilnadu, India

***Abstract*—The internet infrastructure is vulnerable to most serious types of attacks due to its flexibility and no proper IP verification. One of the most serious attack is DDoS(Distributed Denial of Service attack). In DDoS attack, target web server will be continuously flooded with bogus packets. To provide mitigation against that attack Stochastic Fairness Queueing (SFQ) algorithm and Class Based Queueing(CBQ) algorithm is proposed as a countermeasure to defend the Distributed Denial of Service attack. SFQ uses Round Robin method by creating multiple buckets and giving chances for each bucket to be served in its turn thereby increasing the efficiency. CBQ makes the incoming traffic to share bandwidth equally among them, after being classified and grouped by classes. The traffic is made to pass through CBQ and then to SFQ since SFQ cannot determine interactive flow from bulk traffic. Additionally, we use Machine Learning Automatic Defense System (MLADS) which is based on Flexible Deterministic Packet marking (FDPM) to trace back the source of the DDOS attack. In this paper, we implement SFQ with CBQ and MLADS to effective mitigation of DDOS attack.**

***Key Terms*—DDOS – FDPM - MLADS – SFQ - CBQ**

I. INTRODUCTION

In today's internet world, Security becomes the major concern. Among other security issues, Distributed Denial of Service (DDOS) attack becomes more prevalent. DDOS attack is an attempt to make the network resources unavailable to the legitimate user which is done by flooding the targeted server with unwanted packets hence the server will be busy in processing those bogus packets.

Unlike other attacks, defending DDOS is not quite easy. DDOS is attempted by taking control of large number of hosts that poses vulnerability in the security mechanisms and tries to install slave programs in those identified systems. Finally, DDoS is launched against the targeted system by sending the large amount of data packets or requests. Thereby it creates the traffic in the network results in network slow down or server crash.

Hence in this paper we use the SFQ algorithm to prevent the large amount of traffic by scheduling the transmission of packets. This is done by creating a hash buckets and assigning each packet to a bucket based on the hash value and sending it in a Round-Robin fashion. SFQ in turn mitigates the DDOS attack by reducing the traffic. Along with that we use CBQ algorithm that shares the bandwidth equally, and group the incoming traffic into classes and classification is done based on their priority, interface or origin.

Not only that a technique called Machine Learning Automatic Defense System is used to detect the source of the DDOS attack by marking the fragment field in the IP header which in turn finds the source of the attack. By using these techniques we can mitigate an impact of this attack on network up to a certain level.

II. OVERVIEW OF DDOS

Not like before, nowadays DDOS attack causes huge impact on the network. Many works related to the prevention of this DDOS attacks is been done. The impact of DDOS attacks are severe than the normal denial of service attack. DDOS attack are performed by taking control of over thousands of systems with poor security in the network and then making use of them at a right time to send the data packets or requests to a target system and making them to respond for those large number of requests which makes the server to slow down.

The computers used for performing this attack does not that they are controlled by the remote host or an attacker. Those computers are called Zombies and the group of Zombie computers is called as Botnet. It not like the normal DOS attack, the impact will be severe than it. It is impossible to prevent the attack by blocking the single IP address and also it is difficult to separate the legitimate traffic from attack traffic. Hence, it is needed to take necessary steps to avoid or prevent the network from DDOS attack.

III. RELATED WORK

Many works have been done to mitigate the DDOS attack. Previous experiments implement a Light Weight Tunneling protocol (LOT).In which the LOT deployed gateways automatically establishes an efficient tunnel to secure connection. It provides security by dropping the spoofed packets.

Further, it implement quotas , identifying and blocking packets from different networks and also it uses near-source quotas to reduce packet loss and congestion by filtering large

traffic before it leaves the network. It sets certain filtering rules to filter the certain packets and inter-gateway congestion detection mechanism is used to detect when the packets are get dropped before reaching the destination. These methods help in defending DDOS attack.

In Botnet-based Distributed Denial of Service, a bunch of computers are controlled by a remote host using the software program called BOTS which is installed in those computers. During the attempt of DDOS attack these computers are made to send a large amount of data packets to a target system to make the target down or degrade the performance or crash it.

In Machine Learning Automatic Defense system, packets in small number are used to trace the source by marking the packets and this process is termed as Flexible Data Packet Marking, this helps in filter the attack traffic from legitimate traffic. It has ability to change the length of the marking field based on the load of the routers. These features make the FDPM to give the better performance than the other IP traceback schemes with less resource requirements.

This FDPM has two functionality one is offline training system and the other is online filtering system. Offline Training system is based on Back-propagation algorithm. It collects traffic information and trains the neural network. The Online Filtering system makes the quick decisions to trace the attack signals. Since both the online filtering system and offline training system are used in the attack source end, the attack traffic can be dropped before reaching the destination.

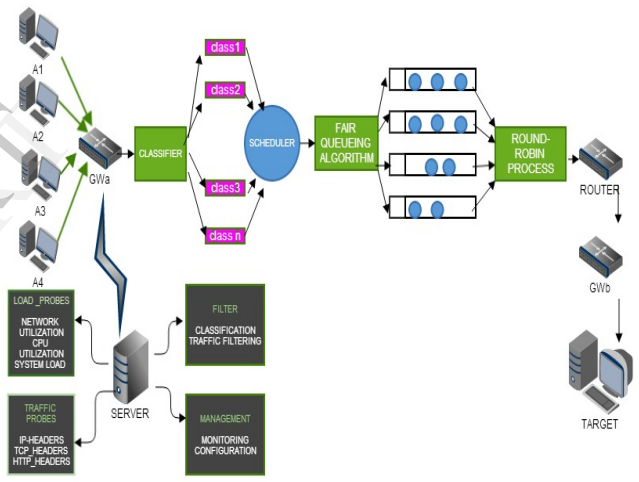
In SFQ, the packets are enqueued in a hash buckets and then it is dequeued in the round-robin fashion in which each hash buckets get a chance for dequeueing.SFQ denotes the flow. In which a traffic is divided into large number of FIFO queues. Then the traffic is sent in round –robin manner giving each conversation a chance. This in turn helps in preventing the flooding attacks and also mitigates the DDOS attack. It is not the best Fairness Queueing algorithm but it works fair in queueing and also it requires a less number of calculations.

In information theory based metrics, they uses two phases one is Behaviour monitoring and another is detection. In behavior monitoring, the user's web usage is monitored during non-attack cases. In Detection phase, the variations in the requests are identified and a limitation is set to block the service of the malicious users. Along with this, a scheduler is used to schedule a session based on the priority of the user. In this way , DDOS attack is mitigated.

In CBQ, it consists of two mechanisms one is Weighted Round Robin (WRR) which provides the weight nothing but priority for the queue based on that the traffic is made to pass through and the another one is Link-sharing scheduler which shares the bandwidth among the queues and also controls the classes and suspends if it exceeds the allocated rate.CBQ divides the incoming traffic and group them in to classes using classifier and schedule the classes based on their priority. With this the traffic is controlled and the transmission delay is reduced.

IV. PROPOSED WORK

In LOT, traffic is not controlled up to the level so in our paper a technique called Stochastic Fairness Queueing algorithm in which it creates a hash buckets, each packet enter the queue and it is sent through the network based on the Round-Robin fashion in which each bucket has its turn. This in turn reduces the traffic but SFQ alone cannot handle bulk traffic hence we include another queueing algorithm called Class Based Queueing(CBQ) groups the traffic based on their priority, interface or origin and shares the bandwidth among them. With this we can control the traffic and also improves the efficiency of the network and also we implement the Machine Learning Defense Automatic System which is used to detect the source of the attack by marking the fragment field in the IP header. In fig.1 ,we show how the SFQ with CBQ and MLADS is implemented in which the packets sent from the source is passed through the gateway GWa in which the MLADS techniques which is based on Flexible Data Packet Marking (FDPM).



IMPLEMENTATION OF SFQ with CBQ and MLADS

In which the process like packet marking in fragment field of the IP header is done and setting the constraints for traffic filtering in which the data packets which are not based on the conditions are dropped and then the data packet undergoes the Class Based queueing algorithm which separates the incoming traffic into various classes and then group them according to their priority, interface or origin. Based on their priority the traffic is made to pass through and undergoes the another queueing process which is Stochastic Fairness Queueing algorithm in which the hash buckets are created in which the packets are stored and then dequeued in the round-robin manner giving a chance for each bucket.

After that the packets are dequeued from the buckets and passed to the network to reach the destination. In this way we reduce the traffic in the traffic which in turn reduces the chance of DDOS attack and also by packet marking we traceback the source of the attack by which we can block the

attacker and prevent the host from further attacks. In this way these methods combinely provides the better efficiency and security for the network.

V. CONCLUSION

In this paper, we have proposed how the Class Based Queueing algorithm along with Stochastic Fairness Queueing algorithm and Machine Learning Automatic Defense System have been implemented in a network to mitigate the impact of DDOS attack on a network to provide the better efficiency of the network by filtering the unwanted data packet and by controlling the traffic over the network.

I. FUTURE ENHANCEMENT

In this paper we proposed a solution for DDoS mitigation which combines the techniques of Class Based Queueing, Stochastic Fairness Queueing algorithm and Machine Learning Automatic Defense system. Although combining these techniques results in effective mitigation but it leaves the question of efficiency in terms of time and process overhead. Hence in future we attempt to minimize the overhead in the current measure by modifying either the time slice or the scheduling algorithm for better performance.

REFERENCES

1. Gilad, Y. and Herzberg, A. 2012." LOT: A defense against IP spoofing and flooding attacks". ACM Trans. Inf. Syst. Secur. 15, 2, Article 6 (July 2012).
2. S. Renuka Devi and P. Yogesh,"Detection of Application layer DDOS attack using Information theory based metrics" David C. Wyld, et al. (Eds): CCSEA, SEA, CLOUD, DKMP, CS & IT 05, pp. 217–223, 2012.
3. Haining Wang, Member, IEEE, Cheng Jin, and Kang G. Shin, Fellow, IEEE,"Defense Against Spoofed IP Traffic using Hop-Count Filtering", IEEE/ACM Transactions on Networking , VOL. 15, NO. 1, FEBRUARY 2007.
4. Minho Sung, Jun (Jim) Xu , Member, IEEE, Jun Li, and Li (Erran) Li, Member, IEEE ,"Large-Scale IP Traceback in High-speed Internet:Practical Techniques and Information-Theoretic Foundation" IEEE/ACM Transactions on Networking vol. 16, no. 6, december 2008.
5. Yu Ming," Mitigating Flooding-Based DDoS Attacks by Stochastic Fairness Queueing", Advances in information Sciences and Service Sciences(AISS),Volume4, Number6, April 2012.
6. K.Subhashini, G.Subbulakshmi,"Tracing sources of DDOS attacks in IP Network using Machine Learning Automatic Defense System", International Journal of Electronics Communication and Computer Engineering ,Volume 3, Issue (1) NCRTCST, ISSN 2249 –071X.
7. Kejie Lu , Dapeng Wu , Jieyan Fan , Sinisa Todorovic , Antonio Nucci," Robust and efficient detection of DDoS attacks for large-scale internet", Computer Networks 51 (2007) 5036–5056.
8. Anup Bhange, Amber Syad, Satyendra Singh Thakur," DDoS Attacks Impact on Network Traffic and its Detection Approach", International Journal of Computer Applications (0975 – 8887) Volume 40– No.11, February 2012.
9. Maciej Korczy nski ,Lucjan Janowski and Andrzej Duda," An Accurate Sampling Scheme for Detecting SYN Flooding Attacks and Portscans", 978-1-61284-231-8/11 ©2011 IEEE.
10. Haining Wang, Student Member, IEEE, and Kang G. Shin, Fellow, IEEE," Transport-Aware IP Routers:A Built-In Protection Mechanism to Counter DDoS Attacks", IEEE Transactions On Parallel And Distributed Systems, vol. 14, no. 9, September 2003.
11. Fulvio Risso,"Decoupling Bandwidth and Delay Properties In Class Based Queueing ",1530-1346/01© 2001 IEEE.
12. Johanna Nieminen, Marko Luoma, Olli-Pekka Lamminen and Antti Paju,"Implementation and Simulation of DBHPD and CBQ scheduling - A Comparative Study", 1-4244-0353-7/07©2007IEEE.