Cuckoo Filter & Remote Firewall: A mechanism for mitigation of Distributed Denial of Service attacks

Vishal V. Mahale[1], Ms. Deepali B. Gothawal[2]

*[1]Department of Computer Engineering
D.Y.Patil College of Engineering & Research Center
Akurdi, Pune, India
vishalmahale27@gmail.com
[2]Department of Computer Engineering
D.Y.Patil College of Engineering & Research Center
Akurdi, Pune, India
dgohil.1519@gmail.com*

---***---

Abstract - *In this paper we present a co-operative cross layer mechanism for mitigation of DDoS attack, as all the mechanism to mitigate the DDoS attack are applied at the single single layer or multi-layer. To enhance the overall security against DDoS attack, cross-layer approach will be the constructive solution. Combination of Device-Driver Packet Filter (Cuckoo Filter) and Remote Firewall will form the cross layer approach. Device driver level packet filtering is designed to kill harmful network traffic before it consumes the processing resource for higher network protocol layers at a server. To protect access links from DDoS attacks by dropping harmful network traffic before they get into the link the remote firewall is designed with a cross-layer control. The performance of the cross layer defense mechanism is checked through extensive simulation in java. The simulation demonstrated that implementing packet filtering at the device driver would be powerful under intense DDoS attacks.*

***Key Words*: DDoS(Distributed Denial of Service Attack), Cuckoo filter, Remote Firewall, high-rate and low-rate attacks.**

1. INTRODUCTION

DDoS attacks are the most common hurdle the internet services facing today. Several tools are their which sweep over the servers by setting out Denial of Service attacks. Due to enhancement in the technology and advanced techniques, it has become easy for the attackers to launch the DDoS attacks. When the network is big, it is hard to detect the DDoS attacks. That's why DDoS attacks are now becoming severe threats causing big amount of losses to Internet today. The below piechart[1] shows the DDoS attacks done by the attackers on different sites.

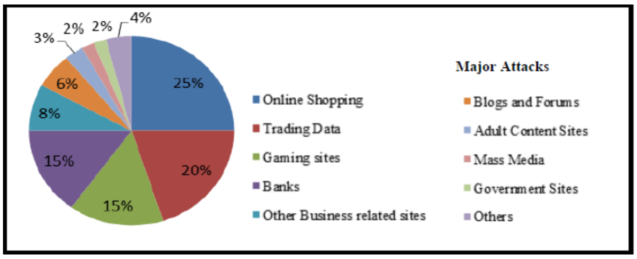


Fig-1: Pie chart showing DDoS Attacks on Major Websites[1]

In the recent years, the attackers are becoming more sophisticated and organized [2][3] DDoS attacks are challenging to handle.Denial-of-Service (DoS) attack is qualified by an explicit attempt by an attacker to prevent authorized users of a service from getting that service [1]. The extension to DoS attack is the Distributed Denial-of-Service (DDoS) attack. By flooding a huge number of attack packets to a target machine, with the simultaneous collaboration of hundreds or thousands, or even more computers that are spread all over the Internet DDoS attack is commenced. The DDoS attack traffic engage the resources of the network and hence the authorized user request will be discarded as the resources are consumed by the attackers at the server end.

DoS attack is classified on the basis on flooding as[4]: high rate and low rate attack. In High-rate attack large amount of traffic is send to the victim to deny the service. In Low-rate attack small quantity of traffic is organized to the victim to elude detection. The main difference in high-rate and low-rate attack is the attack rate only. Their name itself implies high-rate attack has a higher average rate; low-rate attack has a lower average rate.

In this paper we developed a cross layer mechanism which will mitigate the high and low rate DDoS attacks with high performance. We are using device driver packet filtering (with CUCKOO filter) and remote firewall. In the device driver level packet filtering, flooding network traffic will be blocked before they consume the processing resources for higher protocol layers, like network, transport, and application layers. At the other end the remote firewall is setup which can be configured remotely. This firewall is implemented at Internet service provider's (ISP's) edge router ahead of the access link. The firewall will drop possibly harmful network traffic before they get into the system.

2. LITERATURE SURVEY

In many existing mechanisms which are deployed at network layer the attacks are detected by analyzing the protocol header information, packet arrival rate and many more parameters. Detection depends on the difference in the main IP parameters, like source IP address, source destination pair, hop count, next protocol field and combination of multiple attributes. A cryptographic technique that enables the tracing of attack source in provided in the intelligent router based hardened network which is proposed in [5]. A hop count based technique where received IP packet is plunged if huge difference exists between its hop count & the estimated values is proposed in [6]. Probabilistic means are used to find malicious packets in Differential Packet Filtering against DDoS Flood Attacks [7]. Overlay network is proposed by Keromytis et al [8] through which the authorized traffic is sent. Secure Overlay Service (SOS) network changes its topology constantly to prevent DDoS and can survive even if few key nodes are attacked.

A document popularity scheme is proposed in [9] where an anomaly detector based on hidden semi-Markov model is used for spotting the attacks. To avoid application layer DDoS attacks DDoS shield structure is show in [10], DDoS shield detects the features of HTTP sessions and applies rate-limiting as the mitigation mechanism. In [11] Relative entropy based detection method is proposed. Click ratio of the web object is considered as the main parameter and cluster method is used to obtain the click ratio features. The detection is made by calculating the relative entropy for the extracted features. A simple system is proposed in [12] in which the access is given to only those users who solve the puzzles. This method consider that only human can determine the distorted images, but the machine cannot. An information theory based detection mechanism is shown in [13] where the distance of the package distribution activity among the fishy flows is used to distinguish flooding attacks from legitimate access. In [14] Defense against Tilt DoS attack is described. Throughout a session DAT analyzes user's characteristics to find normal and malicious users. DAT renders differentiated services to users based on their characteristics. Divide and conquer strategy is proposed is an advanced entropy-based scheme [15], where the different rate DDoS attacks are classified into various categories and each one is dealt with an appropriate method. The classification is mainly based on the deviation of the entropy from the defined thresholds.

One solution for high-rate attack is Ingress/egress filtering, this prevents the spoofed packet from being injected in to the public internet domain[16]. [17,18,19] discuss one more example hiding the location of servers from the attackers.[20,21,22,23] shows how charging the cost for using resources at server host can avoid high-rate attack, this slowdowns the attacking traffic in reaching the targets.

Traceback [24,25,26,27] is one of the solution for low-rate attack. Once a flow of excess traffic is detected at the router, it traces a chain of routers back towards the source of the traffic in the upstream to stop such traffic at the router that is closest to the origin [28]. Another good solution for low rate attack is packet filtering at the server[29,30,31].

The solution listed above has few strengths and weaknesses. Ingress/egress filtering drops the spoofed packets before they enter the network domain. Although this is effective technique in preventing the attack, many administrator do not use this solution as it does not protect the own network. One more problem with ingress filtering is that it's not effective to DDoS, as attackers use bots to hide the origin of attack. Hiding the locations of the servers from attackers [17, 18,19] keeps attacking traffic from instantly reaching them. Main challenge in local packet filtering is in how to differentiate valid and attacking traffic, which is catchy task[32,33]. Especially in DDoS attacks and flash crowds, recognizing them is quite difficult as the only difference between them is in purpose but not the contents in many cases [34].

From the Literature survey it is found that all the existing mechanism are implemented on single layer mostly and very few multilayer mechanisms are implemented for mitigation of DDoS attack. While progress has been made in preventing or at least significantly lessening the impact of various security vulnerabilities, real progress in fighting DDoS is still missing. The Single and multi layer mitigation mechanism gives good results but the systems are more vulnerable to attacks as in single layer mechanism if the security is breached once then the attacker get access to the servers. This motivated us to design a better mitigation mechanism called Cross-layer mechanism. Proposed mechanism aims at providing uninterrupted service for genuine users. In general applying a particular technique in a single or multilayer layer is incapable to avoid both the high rate and low rate attacks. This leads to the necessity of the cross layer technique. Deploying cross layer technique at either source end or victim end will not provide effective solution. So it is necessary to integrate network level mitigation at the source end and application level mitigation at the victim end.

3. PROPOSED SYSTEM

Our proposed system compromised of two disjoint solutions, device driver packet filtering (using CUCKOO filter) for high-rate DDoS attack and remote firewall for low-rate DDoS attack. We are using CUCKOO filter for packet filtering to eliminate runtime processing overhead in filtering. The main reason for performing packet filtering in the device driver is that malicious packets are dropped at the soonest possible time before they are treated by the upper layers in a protocol stack. Executing packet filtering in the device driver will stop malicious packets from consuming processing resource. Packet filtering in the device drivers have to deal with one challenge, i.e. filtering includes finding a matching filtering rule for each packet, and this must be performed in short time because of following reason.

1. If packet filtering takes much time for filtering, it will be the bottleneck in filtering packets. If it becomes the bottleneck, this lead to chances of flooding-based DDoS attacks.

To meet with the short filtering delay requirement, we applied a CUCKOO filter to the packet filter in the device driver. A basic cuckoo hash table consists of an array of buckets where each item has two individual buckets fixed by hash functions h1(x) and h2(x). It serves as a lookup table for combinations of a source IP address, a source TCP port, and a destination TCP port that have been flagged as potentially malicious by the administrator via the control panel or by the heuristic function. Using a CUCKOO filter, the table aiming filtering rules & the overhead for exploring the matching rule will be cut down. CUCKOO filter allows O(1) search delay.

The reason behind using the CUCKOO filter is:

1. IP addresses can be add and remove dynamically;
2. It provides better lookup functioning than traditional Bloom filters, even when close to full (e.g., 95% space utilized);
3. It is easy to employ the CUCKOO filter as compare to other filters like the quotient filter; and
4. In many practical applications it uses less space than Bloom filters, if the target false positive rate Ɛ is less than 3%.

As IPv4 address space comprises of 232 unique addresses, during the extreme DDoS attack it is not possible to submit the all 232 addresses. In CUCKOO filter the the probability of false positives is calculated by the number of different source addresses actually submitted to the filter. 0.3% of the 232 addresses will be submitted to the filter.

Our designed firewall has a control panel through which the filtering configurations can be done. The administrator can specify the source IP addresses, destination ports and the communication/transport protocol. The device driver level packet filtering using CUCKOO filter can be used at both ISP's edge routers and local gateway routers.

4. PERFORMANCE ANALYSIS

4.1 Modeling

The proposed system is performance is tested using java simulations by developing the cross layer control loop using the Cuckoo filter and remote firewall. Figure 4 below shows the sample network considered for the experimental results.

The network model (fig. 2) consist of' n' distributed LAN sites LAN1,LAN2,...,LANn. Each LAN site is connected to the external network through their respective edge routers R1, R2, ..., Rn. The edge routers link the LAN site to the ISP through ISP edge router RSP(I). The server is accessible only through the ISP edge router RSP(II). The access control policy of the ISP performs traffic conditioning and policing on the traffic entering the core network. Flooding attacks are launched only from the edge of the Internet.

4.2 Design

Various experiments are performed to measure the benefits of Cuckoo filter and remote firewall compare to those performed by single layer and multi-layer mechanisms.

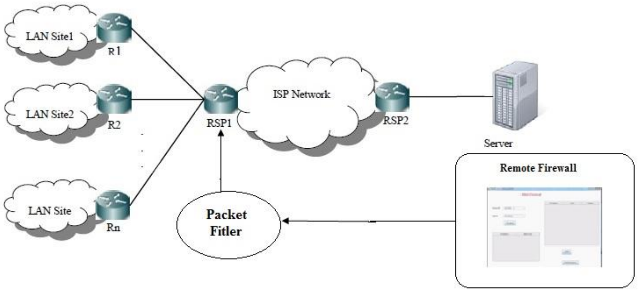


Fig. 2: Network Model

The Configurations for the designed are:

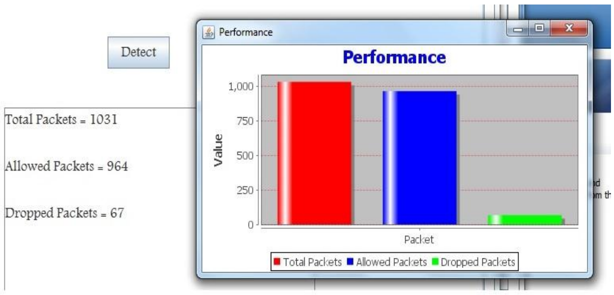
- Packet filtering was performed based on the source address, the destination address and destination port in the header of each incoming IP packet.
- The throughput is defined as the number of packets computed by the firewall at the ISP router (including both dropped and forwarded).
- A fixed packet size of 64 bytes is used for all the experiments.
- The CUCKOO filter was used to reduce the overhead in packet filtering. Use of the CUCKOO filter was necessary to perform packet filtering in the device driver layer.

4.3 Results

When the system is stable and the authorized user request for the data, the servers responds to the request of the user by providing the access to the data.

A sample data set consisting of the source IP, destination IP, protocol, source and destination port, capture length, packet length, connection time is used to measure the performance of the system. Figure.3 shows the graphs generated from the sample dataset 1 consisting of 1031 entries, according to the rule in the firewall only the 964 packets are allowed to access the system and 67 packets are dropped as they does not satisfies the firewall condition.

Figure.4 shows that when the DDoS attack is intense then also our system handles the packets with good efficiency. The data set consist of 3746 packets among which maximum number of packets is malicious and our system is able to handle such request also. Only 317 legitimate packets are allowed from this data set rest 3429 packets are dropped.



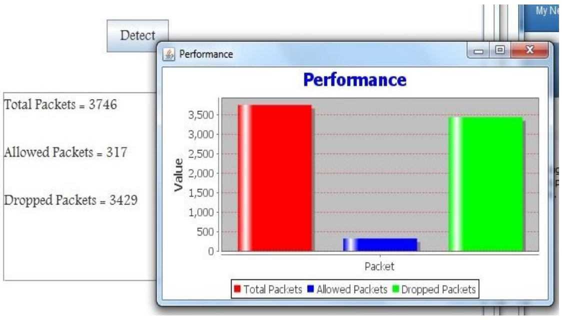
Detect

Total Packets = 1031

Allowed Packets = 964

Dropped Packets = 67

Fig. 3: Performance on data set 1



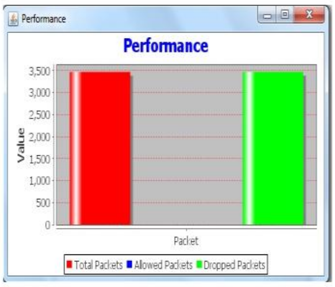
Detect

Total Packets = 3746

Allowed Packets = 317

Dropped Packets = 3429

Fig. 4: Performance on data set 2



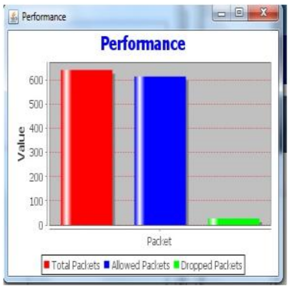
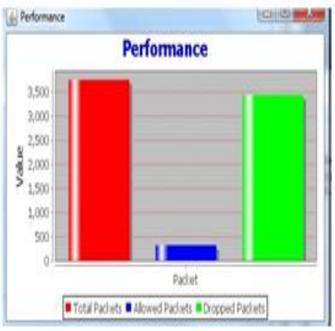


Fig. 5(a) High Rate attack

Fig. 5(b) Low rate attack

Figure 5 and 6 shows the performance of the propose system in high rate attack and low rate attack scenario with different data sets.



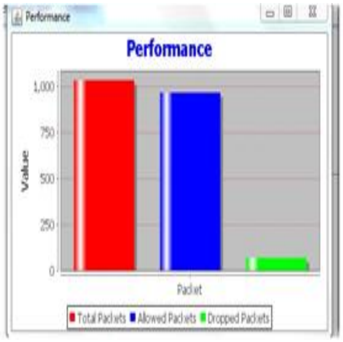


Fig. 6(a) High Rate attack

Fig. 6(b) Low rate attack

5. CONCLUSION AND FUTURE SCOPE

In our proposed system CUCKOO filter and remote firewall is used to overcome the disadvantages of the existing systems which are studied in the literature survey. The architecture is implemented using Java and JPCAP libraries. Propose system performance is measured by comparing the packet dropping rate with the single and multi-layer mechanisms and as per the results gained, it is found that cross layer mechanism works more effectively in intense DDoS attack as compare to the existing systems. We can verify the system performance in real time / practical applications.

In future the system performance can enhanced by using combinations of single, multi and cross layer mechanism as per the requirements.

REFERENCES

[1] "www.kaspersky.ru/downloads/pdf/ddosattacksengprint.pdf .".

[2] R. naraine, " Massive ddos attack hit dns root servers, http://www.internetnews.com/devnews/article.".

[3] A. harrison, "Cyber assaults hit buy.com, ebay, cnn, and amazon.comupterworld," Feb 9 2000.

[4] Gong CHENG Qi LI LIU, Xiao-ming and Miao ZHANG. A comparative study on ood dos and low-rate dos attacks,the journal of china universities of posts and telecommunications, vol. 19, 2012, pp. 116-121, 2012.

[5] Zhang, S., Dasgupta, P., Denying Denial-of-Service Attacks: A Router Based Solution, *Proceedings of theInternational Conference on Internet Computin*, 2003.

[6] Haining Wang, Cheng Jin, Kang G. Shin, Defense Against Spoofed IP Traffic Using Hop-Count Filtering, *IEEE Transactions on Networking*, Vol. 15, No. 1, 2007, pp. 40-53.

[7] Tanachaiwiwat, S., Hwang, K., Differential packet filtering against DDoS flood attacks, *Proceedings of the ACM Conference on Computer and Communications Security*, 2003.

[8] A.D. Keromytis, V. Misra, D. Rubenstein, SOS: an architecture for mitigating DDoS attacks, *Selected Areas in Communications, IEEE Journal*, Vol. 22, No. 1, 2004.

[9] Yi Xie, Shun-Zheng Yu, Monitoring the Application-Layer DDoS Attacks for Popular Websites, *IEEE/ACM*

Transactions on Networking, Vol. 17, No. 1, 2009, pp. 15-25.

[10] Supranamaya Ranjan, Ram Swaminathan, Mustafa Uysal,Antonio Nucci, Edward Knightly, DDoS-Shield: DDoS Resilient Scheduling to Counter Application Layer attacks, *IEEE/ACM Transactions on Networking*, Vol. 17, n. 1, 2009, pp. 26-39.

[11] Jin Wang, Xiaolong Yang, Keping Long, A New Relative Entropy Based App_DDoS Detection Method, *Proceedings of the IEEE Symposium On Computer and Communications*, 2010.

[12] Kandula, S., Katabi, D., Jacob, M., Berger, A.,W., Botz-4-sale: surviving organized DDoS attacks that mimic flash crowds, *Proceedings of the 2nd* Networked Systems Design and Implementation, 2005.

[13] Yu, S., Zhou, W., Doss, R., Information theory based detection against network behavior mimicking DDoS attack, *Proceedings of the IEEE Communications Letters* , 2008, pp. 319.

[14] Huey-Ing Liu, Kuo-Chao Chang, Defending systems Against Tilt DDoS attacks, Proceedings of the 6th International Conference on Telecommunication Systems, Services, and Applications, 2011.

[15] Zhang, J., Qin, Z., Ou, L., Jiang, P., Liu, J., Liu, A. X., An advanced entropy-based DDOS detection scheme, *Proceedings of the International Conference on Information Networking and Automation*, 2010.

[16] P. Ferguson and D. Senie, "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing," *RFC-2267*, January 1998.

[17] M. Srivatsa and L. Ling, "Mitigating Denial-of-Service Attacks on the Chord Overlay Network: A Location Hiding Approach," *IEEE Transactions on Parallel and Distributed Systems*, vol. 20, no. 4, pp. 512-527, April 2009.

[18] A. Stavrou, D. Cook, W. Morein, A. Keromytis, V. Misra, and D. Rubenstein, "WebSOS: An Overlaybased System for Protecting Web Servers from Denial of Service Attacks," *The International Journal of Computer and Telecommunications Networking*, vol. 48, no. 5, pp. 781-807, 2005.

[19] J. Kurian and K. Sarac, "Provider Provisioned Overlay Networks and Their Utility in DoS Defense," *Proceedings of IEEE Global Telecommunications Conference*, pp. 474-479, November 2007.

[20] M. Walfish, M. Vutukuru, H. Balakrishnan, D. Karger, and S. Shenker, "DDoS Defense by Offense," *ACM Transactions on Computer Systems*, vol. 36, no. 4, pp. 303-314, October 2006.

[21] D. Bernstein, "SYN Cookies," URL: *http://cr.yp.to/syncookies.html*, September 1996.

[22] D. Mankins, R. Krishnan, C. Boyd, J. Zao, and M. Frentz, "Mitigating Distributed Denial of Service Attacks with Dynamic Resource Pricing," *Proceedings of IEEE Annual Computer Security Applications Conference*, pp. 411-421, December 2001.

[23] N. Fraser, D. Kelly, R. Raines, R. Baldwin, and B. Mullins, "Using Client Puzzles to Mitigate Distributed Denial of Service Attacks in the Tor Anonymous Routing Environment," Proceedings of IEEE International Conference on Communications, pp. 1197-1202, June 2007.

[24] C. Huang, M. Li, J. Yang, and C. Gao, "A Real-time Traceback Scheme for DDoS attacks," *Proceedings of International Conference on Wireless Communications, Networking and Mobile Computing*, pp. 1175-1179, September 2005.

[25] T. Peng C. Leckie and K. Ramamohanarao, "Adjusted Probabilistic Packet Marking for IP Traceback," *Proceedings of the International Networking Conference*, pp. 697-708, May 2002.

[26] S. Savage, D. Wetherall, A. Karlin, and T. Anderson, "Practical Network Support for IP Traceback," *Proceedings of the Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications*, pp. 295-306, August 2000.

[27] J. Ioannidis and S. Bellovin, "Implementing Pushback: Router-Based Defense Against DDoS Attacks," *Proceedings of Network and Distributed Systems Security Symposium*, pp. 79-86, February 2002.

[28] H. Fujinoki, "Cached Guaranteed-Timer Random- Drop against TCP SYN-flood Attacks and Flash Crowds," *Proceedings of the IASTED International Conference on Communication, Network, and Information Security*, pp. 162-169, October 2005.

[29] T. Peng, C. Leckie and K. Ramamohanarao, "Protection from Distributed Denial of Service Attack Using History-based IP Filtering,"*Proceedings of the IEEE International Conference on Communications*, pp. 1-5, May 2003.

[30] X. Chen and J. Heidemann, "Flash Crowd Mitigation via an Adaptive Admission Control Based on Application-Level Measurement," *ACM Transactions on Internet Technology*, vol. 5, no. 3, pp. 532-569, August 2005.

[31] Y. Li, L. Guo, Z. Tian, and T. Lu, "A Lightweight Web Server Anomaly Detection Method Based on Transductive Scheme and Genetic Algorithms," *Computer Communications*, vol. 31, pp. 4018-4025, August 2008.

[32] K. Li, W. Zhou, P. Li; J. Hai, and J. Liu, "Distinguishing DDoS Attacks from Flash Crowds Using Probability Metrics," *Proceedings of International Conference on Network and System Security*, pp. 9-17, October 2009.

[33] J. Lemon, "Resisting SYN Flood DoS Attacks with a SYN Cache," *Proceedings of USENIX BSDCon*, pp. 89-98, April 2002.

[34] S. Kandula, D. Katabi, M. Jacob, and A. Bergerm, "Botz-4-Sale: Surviving Organized DDoS Attacks that Mimic Flash Crowds," *Proceedings of the Symposium on Networked Systems Design and Implementation*, pp. 287-300, May 2005.

BIOGRAPHIES

Vishal V. Mahale pursuing Master's in Computer Engineering from DY Patil College of Engineering. His area of interest is Networking and Information Security.

Ms. Deepali Gothawal completed her Master's in Computer Engineering from DY Patil College of Engineering and have UG and PG teaching experience of 10 years. Guided 13 ME students and have 11 publications in conferences and journals of National and International repute. Her area of interest is Networking.