Survey Paper on Mitigation Mechanisms for Distributed Denial of Service Attacks

Vishal Mahale[1], **Deepali Gothawal**[2]

[1]Master of Computer Engineering, D. Y. Patil College of Engineering, Akrudi, Pune, India

[2]Department of Computer Engineering, D. Y. Patil college of Engineering, Akrudi, Pune, India

Abstract: ***Today Internet is experiencing one of the major attack called DDos attack. DDoS attack flood the victim with overwhelming amount of traffic to prevent the legitimate users from using network resources. Though security features integrated in the system, the acceptable level of security depends on the state of security in the rest of the global Internet. Till date all the mechanism that are used to less down the DDoS attack are implemented at the single layer. To embellish the security over the DDoS attack, a conjunctive defense mechanism will be creative solution. Providing mitigation either at source end or at victim end may not be a complete solution, in contrast crosslayer mitigation is active at both ends. The proposed systems use two methods to reduce the DDoS attacks: remote firewall and device driver level packet filtering. The remote firewall protects the access links from DDoS attacks by dropping the potentially harmful network traffic before they get into link and device driver packet filtering decimate harmful network traffic before it consumes the resources.***

Keywords: Comprehensive defense mechanism, self similarity defense mechanism, DDoS , High rate attack, Low rate attack**.**

1. Introduction

The most common hurdle the internet services facing today comes from DDoS attacks. There are various tools that overwhelm the servers by launching Denial of Service attacks. With increased technology and sophisticated techniques, it became easy for the attackers to launch these attacks. When it comes to large network environments, it becomes even harder to detect these attacks. Hence, these attacks have become serious threats causing huge revenue losses to the Internet today. As per [1], DDoS Attacks have been performed by the attackers on various sites as shown below in Fig. 1.1

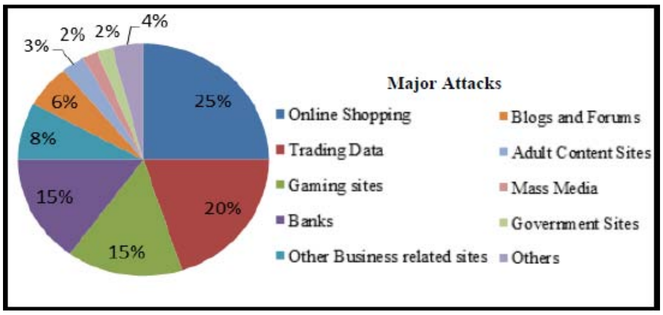

Figure 1.1: Pie chart showing DDoS Attacks on Major Websites[1]

DDoS attacks have gained challenge in the recent years because attackers are becoming more sophisticated and organized [2][3].

Denial-of-Service (DoS) attack is characterized by an explicit attempt by an attacker to prevent legitimate users of a service from using that service [1]. The Distributed Denial-of-Service (DDoS) attack is a notorious extension of the DoS attack. A DDoS attack is launched by flooding a large number of attack packets to a target machine, with the simultaneous collaboration of hundreds or thousands, or even more computers that are scattered all over the Internet. The attack traffic consumes the resources of the Network or the target machine, so that the legitimate requests will have to be discarded due to the lack of resources for either transportation or processing, such as bandwidth and receiving buffer at the server end.

There are two types of flooding DoS attacks [25]: high-rate attack and low-rate attack. High-rate attack sends a large amount of traffic to the victim to deny the service. Low-rate attack organizes a small quantity of traffic to the victim to elude detection. Attack rate is the main explicit difference between low-rate attack and high-rate attack. Just as their names imply, low-rate attack has a lower average rate, high-rate attack has a higher average rate.

2. Related Work

Many existing methodologies deployed at the network layer detect attacks by examining the protocol header information, packet arrival rate and so on. Detection is based on the deviation in the key IP parameters, e.g., source IP address, source destination pair, hop count, next protocol field and the combination of multiple attributes. Zhang and Dasgupta [4] proposed intelligent router based hardened network in which routers provide cryptographic techniques that enable the tracing of attack source. Wang, Jin, and Shin [5], proposed a hop count based solution where a received IP packet is discarded if huge difference exist between its hop count and the estimated value. In Differential Packet Filtering against DDoS Flood Attacks [6], probabilistic means are used to determine risky packets. Keromytis et al [7] proposed the overlay network through which the legitimate traffic is sent. Secure Overlay Service (SOS) network changes its topology dynamically to avoid DDoS and can survive even if few key nodes are attacked. The StackPi [8] DDoS defense scheme is a packet marking scheme that encodes complete path identification in each packet. The marking is same for all packets through a particular path. This marking can be used to block all subsequent packets arriving from the same path during attack. IP Traceback [9] describes a technique for tracing the source of anonymous packet flooded towards the victim. It allows a victim to identify the network path(s) traversed by attack traffic without requiring interactive operational support from Internet Service Providers (ISPs).

Ranjan et al. [10] proposed a DDoS Shield to mitigate application layer DDoS attacks, it detects the characteristics of HTTP sessions and employs rate-limiting as the mitigation mechanism. Yi Xie and Shun-Zheng Yu [11] proposed a document popularity scheme where an anomaly detector based on hidden semi-Markov model is used for detecting the attacks. Wang et al. [12] proposed a relative entropy based detection method. The click ratio of the web object is taken as the key parameter and cluster method is used to extract the click ratio features. The relative entropy is calculated for the features extracted and based on which detection is made. Yu et al. [13] proposed an information theory based detection mechanism in which the distance of the package distribution behavior among the suspicious flows is used to differentiate flooding attacks from legitimate access. Kandula et al. [14] proposed a system 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 cannot. Liu and Chang [15] proposed a DAT (Defense against Tilt DoS attack) scheme. DAT analyzes user’s characteristics throughout a session to determine normal and malicious users. It provides differentiated services to users based on their characteristics. In an advanced entropy-based scheme [16], divide and conquer strategy is proposed where the variable rate DDoS attacks are classified into different categories and each one is treated with an appropriate method. The classification is mainly based on the deviation of the entropy from the defined thresholds.

2.1 Real-Time DDoS Attack detection and prevention system Based on per-IP Traffic Behavioural Analysis

Based on per-IP behavioural analysis, a new DDoS detection system is realized. For each IP user, system will create records for every single IP user's sending and receiving traffic and judge whether its behaviour meets the normal principles. A specific packet identification technique is utilized to reach real-time flooding attack detection goal. A non-parameter CUSUM (Cumulative Sum) algorithm is applied to detect the abnormal behaviour of each IP. Based on a decision algorithm, each IP user will be classified as attacker, victim or normal user. After differentiating the attacker, the system will block its traffic and forward the normal user packets [17].

Based on per-IP traffic behaviour analyses, it is easier to differentiate the attackers from the normal users. As the approach needs less computation and memory, the system could be deployed for on-line DDoS detection and prevention. By applying the non-parameter CUSUM algorithm and decision algorithm, this system can detect attacks accurately at the earlier attack stage. The system can quickly filter the attack traffics and forward the normal traffics simultaneously by means of the fast identification technology. The system has high DDoS detection accuracy and short detection time. For DNS flooding attack and Smurf attack, the system can find out the attacks by checking the mismatch between the request packets and response packets.

The system does not immediately take defensive measures to stop the attack, but keep observing the suspected IP record. After the alarming of attacks counts more than three, the system starts to filter the traffic from the attackers. As most attackers spoof the source IP to unreachable addresses, the server cannot receive their ACK (Acknowledgement) packets to complete the TCP connection. Therefore, in the records, the number of transmitted ACK packets from attackers could not be updated. At the application layer stage, the data unload module can be eliminated. A flexible mechanism should be adopted in which from the suspicious IP, segregation of attackers and victims could be done instead of waiting for the counter value to reach 3.

2.2 Distributed defense framework for flooding based DDoS attacks

A distributed framework is proposed to defend against DDoS attacks. It has three major components: detection, traceback, and traffic control. A detection component of a victim-end defense system detects unusual changes of incoming traffic to identify hidden attacks. The traceback component mainly focuses on analyzing incoming traffic to identify the addresses of routers at the source end of the attack. When an attack is found to be in progress, the traceback component of the defense system at the victim end first identifies the edge routers at the source end using the Fast Internet Traceback (FIT) technique. The defense system at the victim end then sends alert messages to source-end nodes. When an alert message from a victim end is received at the source end, the traffic control component of the source end defense system is triggered to set up rate limits on the edge router of the source end to reduce the attack traffic that is forwarded towards the victim end [18].

2.3 Global detection of flooding based DDoS attacks using a cooperative overlay network.

A distributed defense infrastructure is proposed to detect DDoS attacks globally using a cooperative overlay network and a gossip-based information exchange protocol.
The overall approach is outlined below:

1) Each node makes an independent, local measurement of the victim bitrate.
2) All nodes participate in distributed averaging algorithm whereby they arrive at the average of their local measurements ideally they would all arrive at the same value.
3) Since the distributed averaging algorithm takes some time to complete, each node locally adjusts the resulting average by combining it with its latest local measurement.
4) The adjusted average is then multiplied by the number of overlay nodes and the result is taken to be the total victim traffic that originates from distance >=d to the victim. This is further corrected to account for victim traffic that cannot

be measured, i.e. traffic that originates from distance < d to the victim, to obtain the total victim bit rate.

5) Each node then locally tests whether the victim bit rate exceeds the victim's capacity. If at least 50% of nodes local tests are positive within a given time window then the node flags that an attack is happening at that time [19].

There may be not enough time for all packets to be communicated between all defense nodes in each round of the gossiping, i.e. the round time may be less than the required communication time. In this case, packets which arrive after the round are discarded. This leads to errors in the averaging process. Increasing the number of rounds, either by increasing the phase time or by decreasing the round time, leads to wastage of various network resources and increase of detection latency. The overlay does not measure packets that come from inside the overlay, i.e. traffic that comes from nodes at a distance less than the overlay distance from the victim. Increasing the round time and increasing the number of rounds generally increases the False Positive rate.

Attack packets may be sent within the overlay. In order to block these packets from reaching the victim some lightweight alert node should be deployed within the overlay. For early detection of attacks number of rounds should be less. Instead of discarding packets that arrive after the round, they can be put in a waiting queue where in the next round they can be picked up. This may not create error in the averaging process.

2.4 Integrated DDoS attack defense infrastructure for effective attack prevention

A general purpose DDoS defense technology is developed where the attack phases are analyzed along with the general characteristics of attacks. For each phase DDoS attack prevention requirements are proposed and the integrated DDoS attack defense infrastructure is suggested [20].

Focus is on general characteristics and infrastructure not on specific characteristics. Novel attacks can be detected. If the suggested requirements are developed and applied to current DDoS attack defense systems, then DDoS attack could be effectively blocked.

For Attack agent development phase prevention, the mechanism is dependent only on degree of law against hacking and DDoS attack. The C&C (Command & Control) server connection detection is not a majestic agent detection method. If very high amount of network traffic occurs, then software based analysis methods could not handle the situation and the analysis results can show high rate of false negatives. Source IP address could be spoofed. It is impossible to identify the exact IP address of attack systems. Therefore, access control list based packet blocking is impossible. For preventing the attack agent's development simply relying on the execution of the law will not bear fruit rather a protocol or a sensing device could be installed that might hinder the development of the attack agent. For agent control mechanism detection, additional analysis is inevitable. With the analysis, connection initiation mechanism should be identified first. IP spoofing could be detected by observing the massive traffic flow.

3. Discussions

All the techniques studied in the literature survey are implemented on single layers. In general applying a particular technique in a single layer is not capable to protect both the high rate and low rate attacks. This leads to the necessity of the multilayer technique. Hence a strong multilayer mechanism is needed to avoid the DDoS attack. To overcome the disadvantages of the previous single layer techniques a co-operative multi layer mechanism: Comprehensive defense mechanism and Self similarity defense mechanism will give effective solution.

3.1 Comprehensive defense mechanism

For this technique sample network is consider as shown in the fig3.1. The ISP edge router that connects a LAN site's edge router is also shared by other LAN sites edge routers. The ingress filtering [21] at the ISP edge router drops all packets with unknown and unroutable IP addresses and allows only packets with known subnet IP address in to the network.

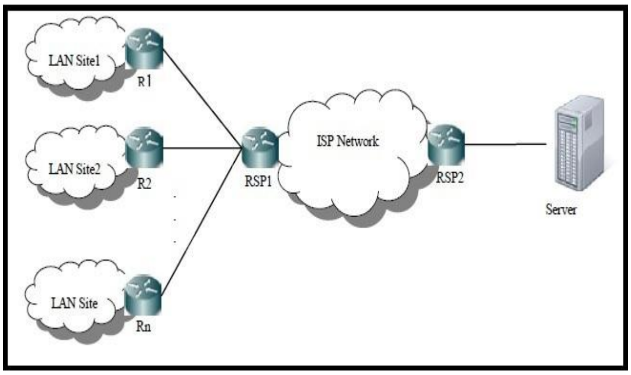

Figure 3.1: Sample Network

Hence flooding attack can only be launched by inserting large number of illegitimate packets with valid IP address. Those Packets with valid source IP address can be generated by outsider or by the insider of the LAN site, who is attached to the same edge router of the ISP. The outsider of the LAN site attacks by sending spoofed packets and the insider attacks by sending large amount of packets. As mentioned earlier, the Ingress filtering technique applied at the ISP edge router does not protect the ISP from the flooding of packets with legitimate address and spoofed address. The flooding of packets thus gaining access might exhaust the bandwidth available to the legitimate user. In general, most of the flooding protection systems consider only the edge network as the area to be protected. However for better service, the ISP network should also be protected in addition to the customer's edge LAN network.

The comprehensive defence mechanism includes a threshold based rate limiting and access tag based security mechanism. The simple threshold based rate limiting technique is applied at the LAN site edge to protect from the insider flooding attack. An Access Tag based defence mechanism is used to protect the critical resources against the outsider spoofed attack. The defence mechanism is placed at the edge routers of the ISP and LAN sites, in order to avoid congestion, resource exhaustion and to ensure protection from high rate flooding attack. The technique to protect the legitimate network traffic from flooding attack is below.

a) **Preprocessing step:** Threshold Values is fixed by analyzing the system log during non attack case. Based on the threshold value the packets are rate limited at the LAN site edge router
b) Then an access tag is attached to the forwarded packets for further screening. The access tag attached to the packet helps to find the legitimacy of the packet. The mechanism incorporates two process, access tag attaching process and access tag verification process, one at the LAN site edge router and the other at the ISP edge router respectively.
   - A random long integer 'N' and a key 'K' are pre shared through the secured channel between edge routers of the LAN sites and ISP.
   - In addition, the Hash algorithm 'H' (SHA-256) used for generating the access tag is also agreed. The LAN site edge router computes the Access tag for the received IP packet as in equation (1) and attaches it to the IP header.

Access Tag = HK((Timestamp ǁ Src-IP) XOR N)) …….(1)

- A concatenation of the timestamp and source IP provides a unique identifier. This unique identifier is XOR-ed with the random long integer 'N' and hashed using SHA-256 algorithm to produce a fixed length hash called the access tag which is appended to IP packet.
- The ISP edge router computes the Access Tag' for the received IP packet. ISP verifies the validity of the packet by comparing the generated Access Tag' with Access Tag present in the IP packet received.
- The packet is forwarded if both values are equal otherwise it is dropped.

This embedded Access Tag has more randomness and provides a stronger solution. The access tag filtering provides good throughput of legitimate traffic even during spoofed packet flooding. It gives helping hands to ISP in discarding as much potential spoofing attack packets as early as possible. Checking access tag is a comparatively light weight process.

3.2 Self Similarity Defense Mechanism

The source end mitigation can only avoid congestion by limiting the traffic entering the Internet but it cannot mitigate the low rate attacks completely. Such attacks can only be mitigated at the victim end. The low rate and distributed forms of flooding attack are coordinated floods of legitimate-looking requests to the sites in the web server. Often, botnet are usually the engines behind those attacks. The attacks are Launched from a large set of compromised hosts (bots) spread throughout the world. These sorts of attacks are difficult or impossible to block completely at the source end.

Research studies on botnet [22],[23] reveal that the attack traffic generated from the bots that belong to the same botnet is usually more similar to each other. The reason is that the attack tools to launch an attack are prebuilt programs which remain the same for all bots in a botnet. Therefore, the similarity among attack flows is much stronger than that of the legitimate flows. Based on this, self similarity based measure is employed at the victim end to counter the attack. Once the access to the server surges our detection mechanism comes to play to identify the malicious sessions. The detection mechanism is incorporated in a proxy server which is deployed just before the web server, thereby protecting the web server from direct flooding. Pearson Coefficient [24] is used as the distance metric to measure the similarity of any two suspected session flows. One of the impressive properties of the Pearson Coefficient is symmetric measurement ie., rXY = rY X. The symmetric property is most important in our work since the distance between the two suspicious flows computed at either end must be identical for the same pair of flows for taking decision. The distance calculation with respect to Pearson Coefficient is explained next.

Once a flooding is suspected at the proxy, correlation (similarity) among the incoming session flows is can be calculated. To calculate the distance among two sessions, all the incoming sessions for a period of time, say T are sampled. The number of requests coming through each session is counted for every sampling interval t within the sampling period T. Let X and Y (X + Y) be the probability distribution of the two sampled session ows with the same length n as in equation (2).

$$X = X1, X2,..., Xn; \; Y = Y1, Y2,..., Yn \qquad (2)$$

where n=T4t, represents the number of samples within the sampling period T.

Pearson correlation between the two session flows is defined

$$r_{xy} = \frac{\sum_{i=1}^{n}(x_i - \mu_x)(y_i - \mu_y)}{\sqrt{\sum_{i=1}^{n}(x_i - \mu_x)^2 \sum_{i=1}^{n}(y_i - \mu_y)^2}}$$

where µX and µY are the mean of the samples X and Y respectively. The value of the correlation coefficient may vary from 0 to 1. The value close to 1 means that the sessions are similar and it indicates the possibility of attack session. The value close to 0 indicates that the sessions are dissimilar and legitimate. Let td be the threshold for the discrimination, the sessions X and Y are considered malicious if rXY > td, otherwise, they are considered as legitimate flows. In general, there may be many (more than two) sessions during flooding. This means that there exist a number of different pair wise combinations among the incoming sessions. All possible pair wise comparisons are made and the final decision can be obtained from the overall result in order to improve the reliability of our decision. Let us assume that there are S number of incoming sessions. then there exist SC2 possible combinations. in other words, each session is compared with rest (S-1) sessions and the session is considered as malicious if more than 30% of the comparison results in attack.

4. Conclusion

In this paper we discussed the strategies implemented on single and multiple layer which are use to mitigate the DDoS attack. The study proves that multi-layer mechanism is best solution to mitigate DDoS attack as it overcomes the disadvantages of single layer mechanisms.

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

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

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

[7] 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.

[8] A.Yaar, A. Perrig, D. Song, StackPi: New packet marking and filtering mechanisms for DDoS and IP spoofing defense, *Selected Areas in Communications, IEEE Journal on*, Vol. 24, No. 10, 2006, pp. 1853-1863.

[9] Shui Yu, Wanlei Zhou, Robin Doss, Weijia Jia, Traceback of DDoS Attacks using Entropy Variations, *IEEE Transactions on Parallel and Distributed Systems*, Vol. 22, No. 3, 2011, pp. 412-425..

[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] 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.

[12] 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.

[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] 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.

[15] 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.

[16] 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.

[17] Guofeng Zhao YiZhang, QiangLiu. A real-time ddos attack detection and prevention system based on per-ip traffic behavioral analysis, ieee.

[18] Anwar Haque Yonghua You, Mohammad Zulkernine. A distributed defense framework for ooding-based ddos attacks.

[19] Thaneswaran Velauthapillai, Aaron Harwood and Shanika Karunasekera," Global Detection of Flooding-Based DDoS Attacks Using a Cooperative Overlay Network", Fourth International Conference on Network and System Security, IEEE, 2010.

[20] Yang-Seo Choi, Jin-Tae Oh, Jong-Soo Jang, Jae-Cheol Ryou," Integrated DDoS Attack Defense Infrastructure for Effective Attack Prevention.

[21] P. Ferguson, Network ingress filtering: Defeating denial of service attacks which employ IP source address spoofing, 2000.

[22] Stone-Gross, B., Cova, M., Cavallaro, L., Gilbert, B., Szydlowski, M., Kemmerer, R., Kruegel, C., Vigna, G., Your botnet is my botnet: Analysis of a botnet takeover, *Proceedings of the ACM conference on computer communication security*, 2009, pp. 635.

[23] Thing ,V. L. L., Sloman, M., Dulay, N., A survey of bots used for distributed denial of service attacks, *Proceedings of the International nformation Security Conference*, 2007, pp. 229.

[24] http://en.wikipedia.org/wiki/Pearson_productmoment correlation_coefficient

[25] 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.

Author Profile

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.