A Cooperative Multilayer End-Point Approach to Mitigate DDoS Attack

S. RENUKA DEVI, S. SARASWATHI, P. YOGESH
Department of Information Science and Technology,
College of Engineering Guindy, Anna University, Chennai. India.
renusaravanan@yahoo.co.in, sarasuthan@yahoo.co.in, yogesh@annauniv.edu

Abstract:- DDoS attacks constitute one of the major intimidating hardest security problems facing today's Internet. The goal is to flood the victim with overwhelming amounts of traffic, with the purpose of preventing legitimate users from using a victim computing system or network resources. Irrespective of the security features incorporated in the victim system, the acceptable level of security depends on the state of security in the rest of the global Internet. To enhance the overall security against DDoS attack, a cooperative defense mechanism will be the constructive solution. This paper proposes one such effective cooperative multilayer defense mechanism. Unlike other existing systems, our system is capable of handling various forms of DoS attacks. Providing mitigation either at source end or at victim end may not be a complete solution in contrast, our multilayer mitigation is active at both ends . The spoofing and high rate flooding attacks are limited at the source end by implementing comprehensive approach at the network layer and low rate flooding attack at the victim end by implementing Similarity based mechanism at the application layer simultaneously. The performance of the multilayer defense mechanism is validated through extensive simulation in NS-2. The real data sets are used for our analysis and the experimental results show that our scheme can efficiently detect DDoS.

Key-Words:- Flooding, Multilayer, Security, Spoofing, Access control, Network layer, Application layer.

1 Introduction

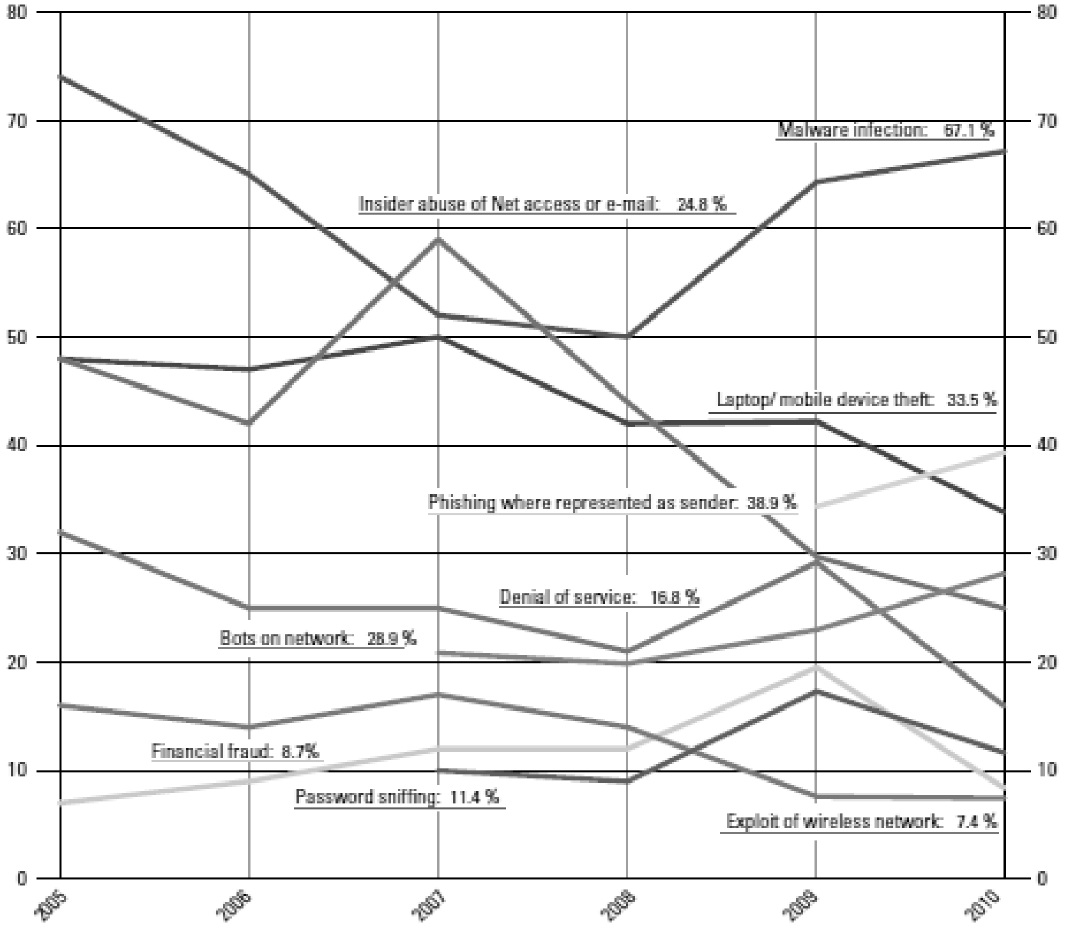
The Internet is an IP based open access system for forwarding packets with minimal processing through best effort service. The best effort service of the Internet forwards packet from any host to any other host irrespective of its legitimacy. Due to this nature, the Internet is susceptible to various kinds of passive and active attacks. Denial-Of-Service (DoS) is one such threatening attack towards the communication infrastructure.

The Computer crime and security survey 2010/2011 [1] projects the types of attack experienced during past few years. The graph[1] shown in Fig.1 gives a strong evidence to conclude that DoS attack and Bots on network constitute nearly 45.7 % of various security attacks. Even though extensive research has been carried over, the attack still persist. This motivated us to focus on defending such long persisting attacks.

DoS attacks flood the victim with a massive number of malicious packets to lock down the Internet services for the legitimate users. In an open environment such as the Internet, mounting DoS attacks consumes the resources like network bandwidth, sockets, CPU, memory, disk/database bandwidth and I/O bandwidth and prevent the services such as VoIP, Web service, VPN service, etc. Due to the advancement in telecommunication technology, Internet access is available at low cost leading to easy launch of DoS attack. DoS attack requires no special hardware or software vulnerability except the Internet connection.

A Distributed DoS (DDoS) is an advanced form of DoS attack. It is a multi-tiered configuration based on the master-slave principle. The master is the core attacker which invokes the slaves to flood the victim. The slaves are the compromised hosts. A large number of compromised hosts together direct packets towards the victim and prevent legitimate access.

There are two types of flooding DoS attacks [2]: 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.



2010 CSI Computer Crime and Security Survey

2010: 149 Respondents

Fig. 1. Types of attacks experienced

In both cases, the attackers intentionally lock the resources of the server and prevent the server from providing service to the authorized users. The attack detection is of crucial importance for providing uninterrupted service by the server. An important step to combat it is to increase the reliability of global communication network. The reliability of the communication network is influenced by the global cooperation from the source end to the victim end [3]. For the server to provide better service it should be protected from various security attacks by enforcing the cooperative security mechanism at different layers of the communication network.

Our aim is to provide a multilayer security so that when multiple layer works together they will bring a better mitigation for the entire system by protecting services provided by the server through the Internet. This paper provides mechanism for mitigating both high-rate and low rate attacks. Most of the high-rate can be captured at the source end of the attack by implementing a comprehensive approach at the network layer. The low rate attacks can be detected at the victim end of the attack by implementing Self Similarity based mechanism at the application layer simultaneously.

The remainder of this paper is organized as follows: In Section 2, we discuss various DDoS defense mechanisms at different layers. In section 3, we describe the network model under our consideration. In section 4, we elaborate the working principle of the proposed defense technique. In section 5, we present the simulation results. Finally, we summarize the work in section 6.

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 a complete path identification in each packet. The marking is same for all packet 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.

The literature survey shows that the existing mitigation mechanisms were implemented at one particular layer. It shows that a single layer mechanism will not be a complete solution to mitigate the DDoS attack. We propose a multilayer mitigation mechanism to overcome the shortcomings of the existing system.

3 Network model and assumptions

Fig. 2 depicts a sample network topology considered in our work. Our sample network consists 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 RSP1. The server is accessible only through the ISP edge router RSP2. 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.

We present our assumptions below in order to make our analysis simple and clear. We assume that:

1. The flooding traffic arises only from the edge networks through spoofing or compromised host.
2. Only one botnet targets the victim at any given time.
3. The network topology is linear and stable.
4. The adversary may be malicious outsider or compromised insider connected to the same ISP.
5. The attack traffic generated may flood the access link but cannot inundate the ISP network.
6. Shared secrets between edge routers are adequately protected against active and passive attacks.

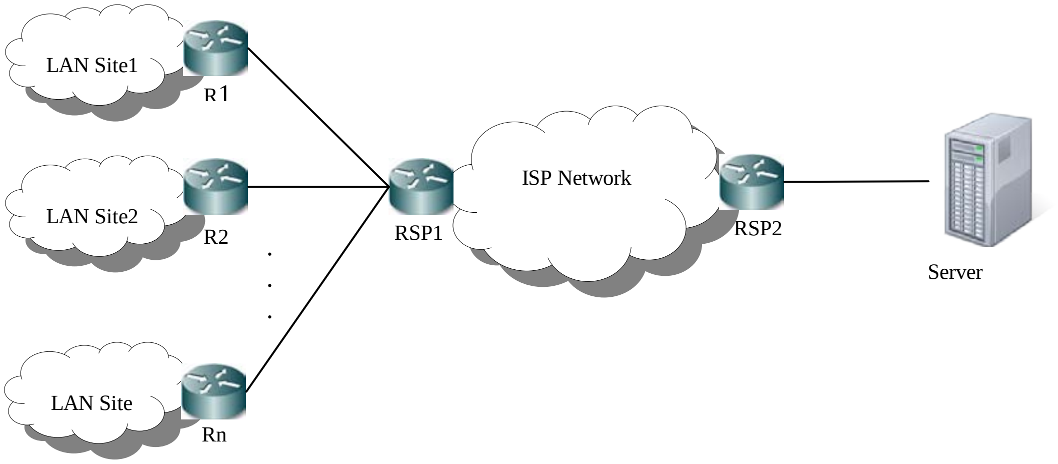


Fig. 2. Sample network

3.1 Vulnerability of the network model

IP-based networks are not perfect and the structure of IP itself makes them vulnerable to security breaches. One very important vulnerability is flooding attack. Flooding attack originating from the LAN targets the ISP network or the victim server of the sample network considered in Fig 2. The attack may be initiated by the malicious insider or outsider of the LAN. The traffic generated may be high-rate or low rate. The high-rate traffic targets the ISP network in particular and low-rate targets the server. In each instance, an unauthorized individual gain access to the critical resources. These security risks make secure communications over large IP networks, such

as the Internet, intimidating. To remedy the problem, we propose a multilayer defense mechanism.

4 Defense Technique

Proposed multilayer edge resource access control mechanism aims at providing uninterrupted service for genuine users. Most of the existing flooding mitigation techniques are deployed only at one particular layer. The literature study reveals that a cooperative multilayer mitigation technique or a hybrid approach may lead to effective protection from flooding attacks. The reason behind multilayer multilevel mitigation is to protect the ISP network and server as well.

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. Deploying multilayer technique at either source end or victim end will not provide effective solution. This fact motivated us to integrate network level mitigation at the source end and application level mitigation at the victim end.

During high rate flooding attack, individual LAN sites cannot effectively defend themselves without coordinating with their ISP. The LAN site on its own cannot block flooding attack traffic or attempt to clear upstream congestion to allow some of its desirable traffic to get through. These facts enforce the involvement of ISPs to handle spoofing and high rate flooding attacks. Our approach to this relies on comprehensive survivability techniques implemented at the source end edge routers to control the illegitimate packets entering the ISP network. Comprehensive defense mechanism is discussed in section 4.1.

Most of the low rate and distributed forms of attack at various LAN sites are beyond the reasonable scope of ISPs to fix at the source end. Generally these low rate traffics are generated by compromised bots. These attack traffic follow the legitimate pattern to evade detection. This insists another level of mitigation at the victim end's application layer to protect the server. Our approach to this relies on self similarity based defense technique for identifying and restricting the attack flows originating from the compromised bots. Self-similarity defense mechanism is discussed in section 4.2.

4.1 Comprehensive defense mechanism

The ISP edge router that connects a LAN site's edge router is also shared by other LAN sites edge routers. The ingress filtering [17] at the ISP edge router drops all packets with unknown and un-routable IP addresses and allows only packets with known subnet IP addresses into the 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 customers edge LAN network. We decide to include the ISP also in the mitigation process. We incorporate a comprehensive defense mechanism at the ISP and LAN sites edge router.

The comprehensive defense 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 defense mechanism is used to protect the critical resources against the outsider spoofed attack. The defense 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. We now describe our technique to protect the legitimate network traffic from flooding attack.

As a preprocessing step, a threshold value is fixed by analyzing the system log during non attack case. The overall threshold is computed based on the mean and the maximum absolute deviation of the number of packets for the sampled interval. Based on the threshold value the packets are rate limited at the LAN site edge router. 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. It avoids spoofed packets from entering into the SP network. 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 attach it to the IP header. 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 'N' is changed periodically by the edge routers to ensure freshness.

$$\text{Access Tag} = H_K((\text{Timestamp}\|\text{Src-IP}) \text{ XOR } N)) \quad (1)$$

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.

4.2 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 [18],[19] 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 remains 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. In this paper, Pearson Coefficient [20] 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., $r_{XY} = r_{YX}$. 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, we start to calculate the correlation (similarity) among the incoming session flows. To calculate the distance among two sessions, we sample all the incoming sessions for a period of time, say T. The number of requests coming through each session is counted for every sampling interval Δt within the sampling period T. Let *X* and Y (X ± *Y*) be the probability distribution of the two sampled session flows with the same length *n* as in equation (2).

$$X = \{X_1, X_2,..., X_n\}; \quad Y = \{Y_1, Y_2,..., Y_n\} \qquad (2)$$

where $n=T\Delta t$, represents the number of samples within the sampling period T.

Then the Pearson correlation between the two session flows is defined as

$$r_{XY} = \frac{\sum_{i=1}^{n}(X_i - \mu_X)(Y_i - \mu_Y)}{\sqrt{\sum_{i-1}^{n}(X_i - \mu_X)^2}\sqrt{\sum_{i-1}^{n}(Y_i - \mu_Y)^2}} \qquad (3)$$

where μ_X and μ_Y 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 t_d be the threshold for the discrimination, the sessions X and Y are considered malicious if $r_{XY} > t_d$, 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 pairwise combinations among the incoming sessions. All possible pairwise 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 ${}_SC_2$ 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.

5 Simulation results

Fig.3 shows the network topology considered for simulation. We implemented the comprehensive mitigation at the source end edge routers: Threshold based rate limiting at R1, R2, ..., Rn and Access Tag based defense at R1, R2, ..., Rn and RSP1. The self similarity defense mechanism is implemented at the proxy.

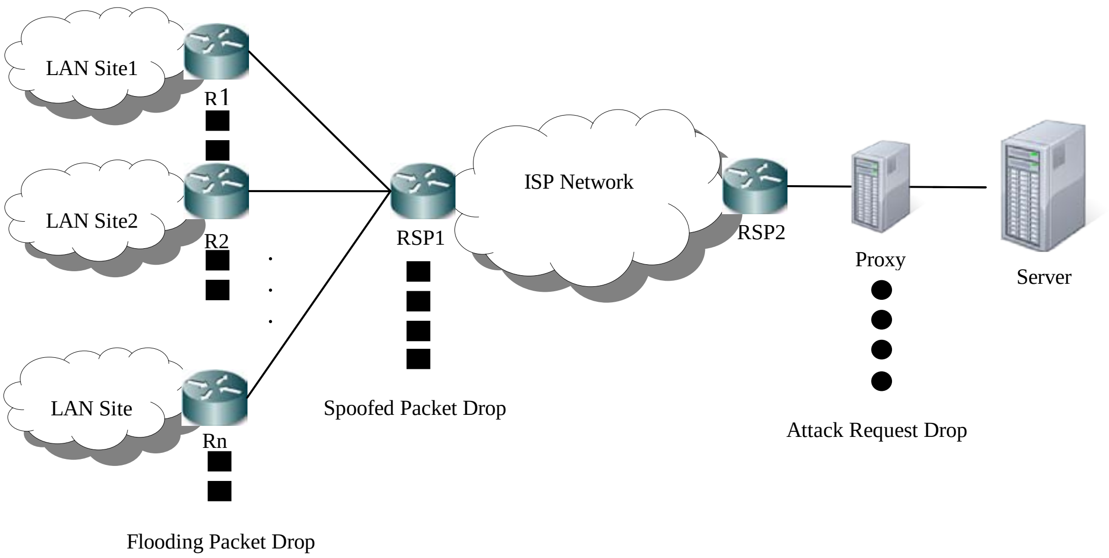


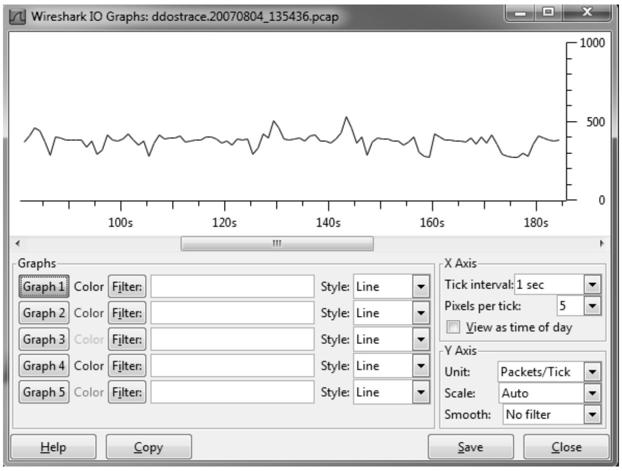
Fig. 3. Simulation topology with illegitimate drop

We evaluate the efficacy of the proposed multilayer mitigation mechanism in this section. We implement the comprehensive defense mechanism at the network layer and self similarity based defense mechanism at the application layer. In the experiment, we use the traces of CAIDA "DDoS Attack 2007" Dataset [21] and the "1998 FIFA World Cup" Dataset [22] as the representatives of flooding attacks and normal network traffic respectively. The simulation studies are carried out by varying the attack intensity giving equal weight to flooding and spoofing attack. The flash crowd during the 90th day of the FIFA World Cup dataset is examined. On a two hour interval (22.00 -23.59 hours of day 90), there exist 2289 number of users with 1,33,670 number of requests. The user request details are projected in Table 1. The user traces are randomly selected and are used for our simulation as normal flows.

Table 1. Number of requests and users involved during two hours of fifa world cup 1998

Number of requests	Number of users
<10	840
10 - 50	581
50-100	493
100-150	183
>150	192

For the high rate and low rate DDoS attack scenario, we use CAIDA dataset. From the analysis made on the CAIDA dataset, we classify the low rate and high rate DDoS attack traffic based on the number of packets per second (say, more than 10 000 attack packets per second can be considered as a high-rate attack and the rest as a low rate attack). The partial attack low rate and high rate scenario from the CAIDA dataset is shown in Fig. 4 and Fig. 5.

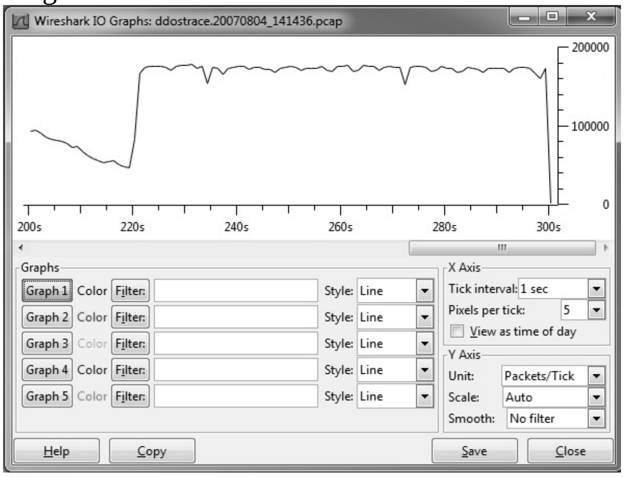

Wireshark IO Graphs: ddostrace.20070804_135436.pcap

Graph 1 Style: Line
Graph 2 Style: Line
Graph 3 Style: Line
Graph 4 Style: Line
Graph 5 Style: Line

X Axis
Tick interval: 1 sec
Pixels per tick: 5
□ View as time of day

Y Axis
Unit: Packets/Tick
Scale: Auto
Smooth: No filter

Fig. 4. Low-rate DDoS attack scenario from caida


Wireshark IO Graphs: ddostrace.20070804_141436.pcap

Graph 1 Style: Line
Graph 2 Style: Line
Graph 3 Style: Line
Graph 4 Style: Line
Graph 5 Style: Line

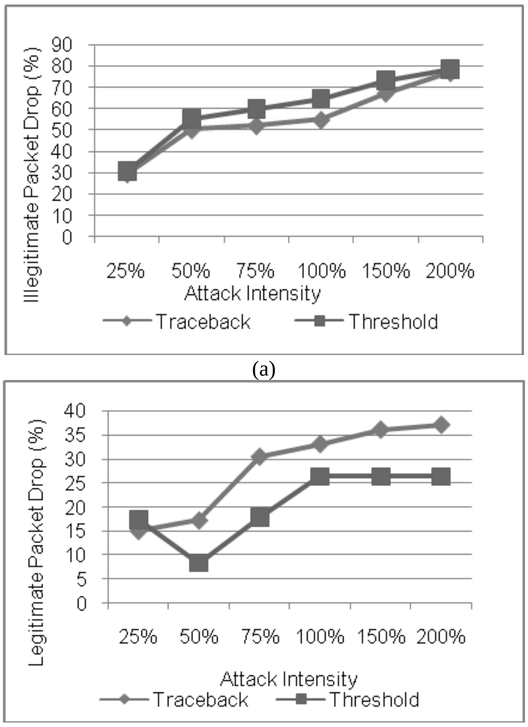
X Axis
Tick interval: 1 sec
Pixels per tick: 5
□ View as time of day

Y Axis
Unit: Packets/Tick
Scale: Auto
Smooth: No filter

Fig. 5. High-rate DDoS attack scenario from caida

Our initial task is to evaluate the performance of the system considering a single layer mitigation mechanism. First, we analyse the network layer comprehensive approach against the flooding attack. Then, we analyse the application layer self similarity approach against the low rate attack. Later on, we exhibit the effectiveness of the multilayer mitigation over single layer.

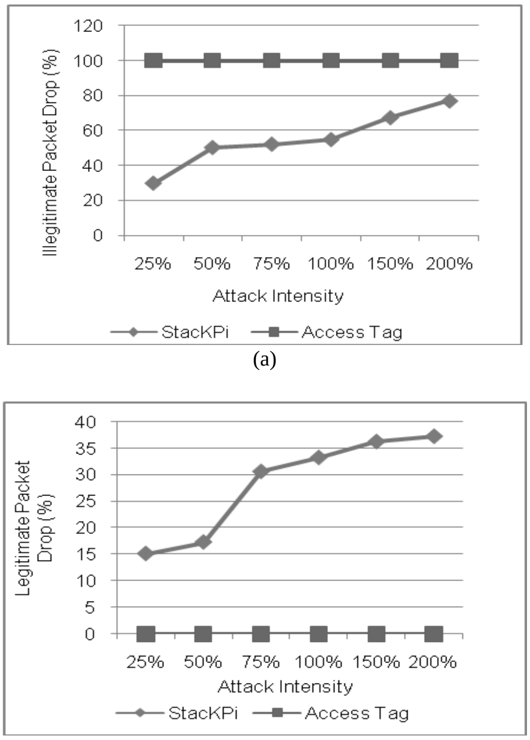
The performance analysis is made for the mitigation technique of the high rate flooding attack and spoofing attack separately and the results are shown in Fig. 6 and Fig. 7. Fig. 6(a) and Fig. 6(b) shows the packet drop for the high rate flooding attack. The comparison is made between threshold based rate limiting and traceback [9]. The analysis made on the packet drop shows that our threshold based rate limiting performs well under high rate flooding attack. However the threshold based rate limiting cannot detect the spoofing attack. On the other hand, the Access tag mechanism can detect spoofing with high accuracy as shown in Fig. 7(a) and Fig. 7(b) but cannot detect the high rate flooding attack from legitimate IP address. The comparison is made between Access tag mechanism and StackPi [8]. The comprehensive approach which incorporate both the mitigation will help in reducing the high rate as well as spoofed flooding attack as shown in Fig. 8.



(a)

(b)

Fig. 6. Threshold based packet drop



(a)

(b)

Fig. 7. Access tag based packet drop

We now analyse the performance of our comprehensive approach with each individual technique by inducing both high rate and spoofing attack. Fig. 8 shows the illegitimate packet received by different techniques. The graph proves that our comprehensive approach performs well with good detection accuracy.

We have analyzed and compared the proposed solution with the existing advanced entropy based technique at the application level and the results are shown in Fig. 9, Fig. 10 and Fig. 11 below. The high rate and low rate flooding attacks are considered for our analysis. Fig. 10 shows the percentage of illegitimate request drop. Our analysis shows that the existing technique detect and drop only the high rate flooding attacks effectively but they fail to detect the low rate attacks. In contrast, our technique performs effective detection on low rate attacks. Fig. 10 and Fig. 11 show that the self similarity mitigation results in low false positives and low false negatives.

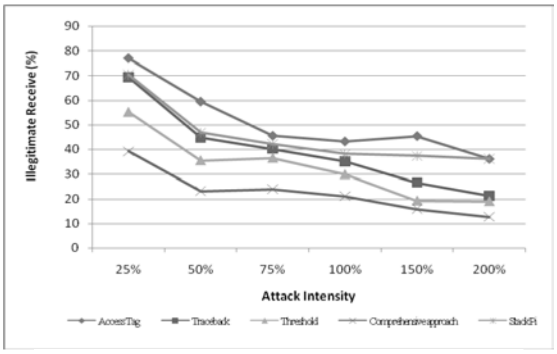


Fig. 8. Comparison with other techniques

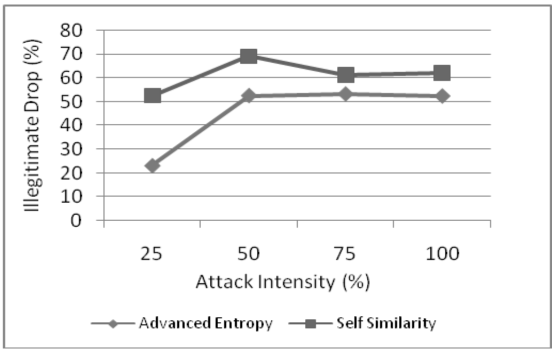


Fig. 9. Illegitimate drop

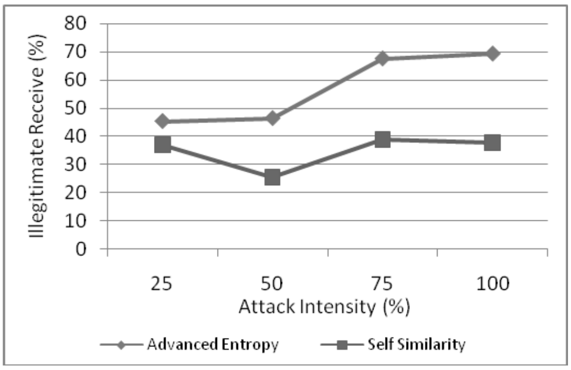


Fig. 10. False positives

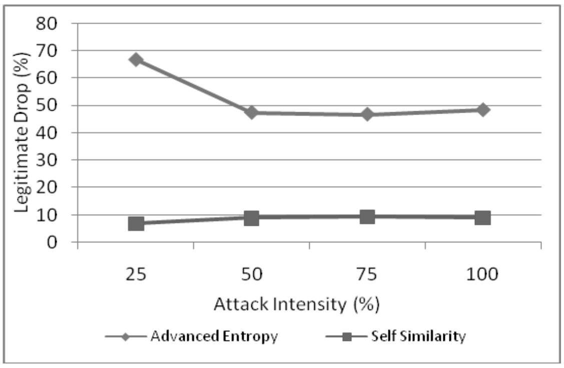


Fig. 11. False negatives

From the analysis made so far it is observed that the sourced end solution prevents spoofing and the high rate flooding attack effectively and the victim end solution prevents most of the low rate attacks. The performance of our multilayer technique shown in Fig. 12 - Fig.15 indicates better mitigation with low false positive and low false negative.

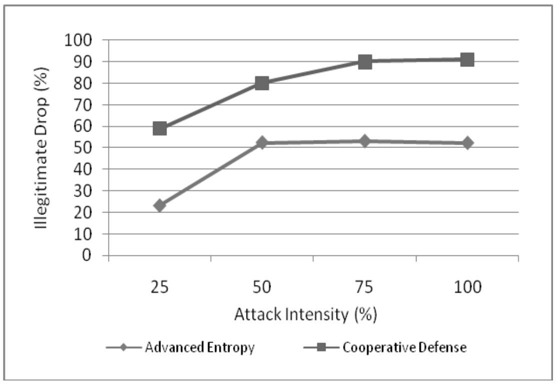


Fig. 12. Illegitimate drop

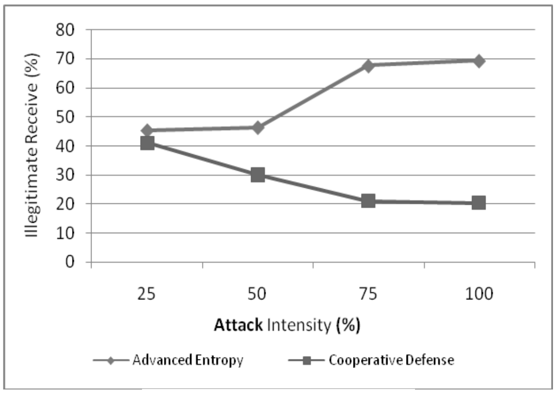


Fig. 13. False positives

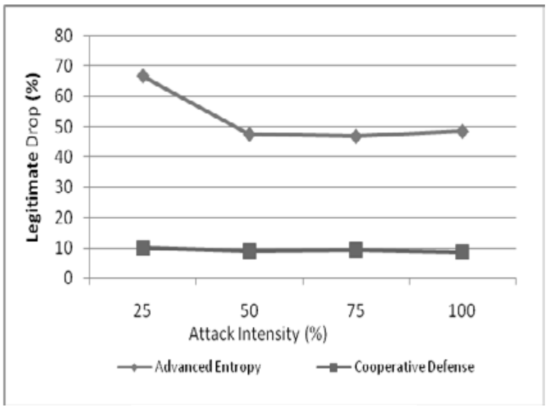


Fig. 14. False Negatives

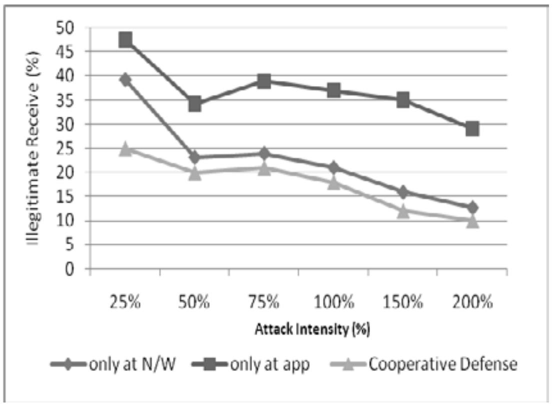


Fig. 15. Comparing Multilayer Mitigation with Single Layer Mitigation

6 Conclusion

There has been considerable research work to defend against DoS attack, but each one is capable of mitigating one or the other forms of DoS attack. Almost all approaches relay on single layer mitigation strategy deployed either at source end or at the victim end. To overcome the limitations of the single layer approach, we integrate a multilayer cooperative defense mechanism. We employed the comprehensive approach at the source end and the self similarity approach at the victim end. The performance analysis reveals that a cooperative mechanism is the better solution than the source end or victim end solution. The work can be further extended to a cross layer mitigation mechanism that can enrich the cooperative mitigation mechanism.

References:

[1] 15th Annual 2010/2011 Computer Crime and Security Survey, *Computer Security Institute*, 2011.

[2] LIU, Xiao-ming, Gong CHENG, Qi LI, and Miao ZHANG. A comparative study on flood DoS and low-rate DoS attacks, *The Journal of China Universities of Posts and Telecommunications*, Vol. 19, 2012, pp. 116-121.

[3] T. Peng, C. Leckie, K. Ramamohanarao, Survey of network-based defense mechanisms countering the DoS and DDoS problems, *ACM Computing Surveys*, Vol. 39, No. 1, 2007.

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

[5] 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.

[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] 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.

[12] 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.

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

[18] 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.

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

[20] http://en.wikipedia.org/wiki/Pearson_product-moment_correlation_coefficient

[21] The CAIDA UCSD "DDoS Attack 2007" Dataset from http://www.caida.org/data/passive/ddos-20070804_dataset.xml

[22] FIFA World Cup 1998 dataset from http://ita.ee.lbl.gov/html/contrib/WorldCup.html