DDoS Prevention System Using Multi-Filtering Method

Ji-Ho Cho
Dept. of Computer Engineering
Hannam University
Dae-Jeon, South Korea
charismaup@nate.com

Jeong-Min Kim
Dept. of Computer Engineering
Hannam University
Dae-Jeon, South Korea
kjm9366@naver.com

Ji-Yong Shin
Dept. of Computer Engineering
Hannam University
Dae-Jeon, South Korea
shinpar90@naver.com

Geuk Lee*
Dept. of Computer Engineering
Hannam University
Dae-Jeon, South Korea
leegeuk@hnu.kr

Han Lee
Dept. of Computer Engineering
Hannam University
Dae-Jeon, South Korea
history1989@naver.com

Abstract— This paper proposes multi-filtering method to prevent DDoS attack. Several filtering methods are applied in two firewall architecture for effective DDoS prevention. In the first firewall, R-PA filtering algorithm and strict hop counter filtering method are applied by analyzing packet paths. In the second firewall, packets are examined to distinguish abnormal packets from normal packets. Security policy system monitors each user sessions and if the traffic is over the threshold value, the system blocks the session for an assigned time.

Keywords- DDoS; Double Firewall; Packet Filtering;

I. INTRODUCTION

Recently, infrastructure attacks have been rapidly increasing. Infrastructure attacks are a form of attacks that makes Internet infrastructures exhausted so that normal users cannot use the Internet. Examples of these attacks include DDoS (Distributed Denial of Service) attacks, slammer worms, and DNS cache poisoning[1][2][4]. The distributed denial of service attacks are a form of attacks that completely consume important resources such as web servers, routers, and DNS(Domain Name Server) servers so that normal users cannot use those resources. In the case of most distributed denial of service attack strategies, multiple distributed agents attack the target system simultaneously so that the resource of the target system is completely consumed[12].

Over the last three years, Distributed Denial of Service attack rates increased by approximately 20 times and in South Korea, DDoS attacks aiming at multiple web sites have been frequently occurring every year. The analysis and tracking of DDoS attacks become more difficult because DDoS attack is diversified and intellectualized. Accordingly, the importance of DDoS defenses has is gradually magnified and DDoS attack preventing methods through firewalls are also one of methods being studied.

Various patterns of DDoS attacks are expected to continuously appear hereafter. In this paper, a method for effective prevention and detection DDoS attacks is proposed. The proposed method uses two firewall and the first firewall analyze packets coming in from the outside for stricter packet filtering. The secondary firewall inspects the data of those packets that came through the primary firewall to distinguish between normal packets and abnormal packets and inspects whether the packets exceed the total traffic threshold. It also inspects the traffic of each users whether it exceeds the threshold allocated to the user.

II. RELATED WORKS

A. ACL(Access Control List)

ACL is the most common traffic control technology used in network systems. Although being capable of preventing abnormal traffic based on IP addresses, service ports, or contents, this method becomes a cause of performance decline by giving a lot of loads to network equipment if there is no special ASIC(Application-Specific Integrated Circuit) module[4]. In the case of organizations that manage many network systems, they have to make different scripts for each systems or have to logged in

individually and change their settings to update access control policies for those systems.

B. *Blackhole Routing*

This is a method in which the router blocks all traffic transmitted to the IP of the target server and sends those packets to a sort of dumping sites called blackhole. If packets transmitted to those IPs that have been registered in advance are set as Null 0, the packet going to the destinations IP will be blocked. This method is also called Null 0 routing or Null 0 filtering because it transmits those packets that are requested to be send to destination IPs to a virtual system named Null 0 instead of the destination IPs to remove the packets[6].

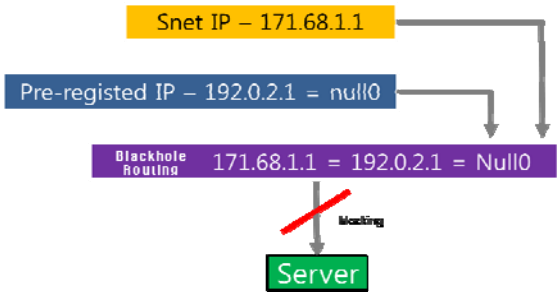

Figure 1. Blackhole routing

C. *DNS sinkhole*

This is a system that prevents malicious behavior such as personal information leak or DDoS attacks by blocking communications between C&C (Command and Control) server and computers infected by malicious bot. In cases where the domain names of C&C servers or download sites are known, this method controls answers to zombie PCs' DNS inquires to bypass to the DNS sinkhole server when the zombie PCs try to access the C&C servers to block attack commands. When zombie PCs inquire of the DNS server about the C&C server's address information, the sinkhole server address stored in the DNS server can be transmitted instead of the C&C server's address to prevent connection with the C&C server. Using DNS sinkholes, information of PCs infected by bots can be obtained and connection between the C&C server and bots can be effectively prevented as well as monitoring the actions of the bots.

DNS sinkholes bypass individual users' access to malicious domains to the sinkhole server.

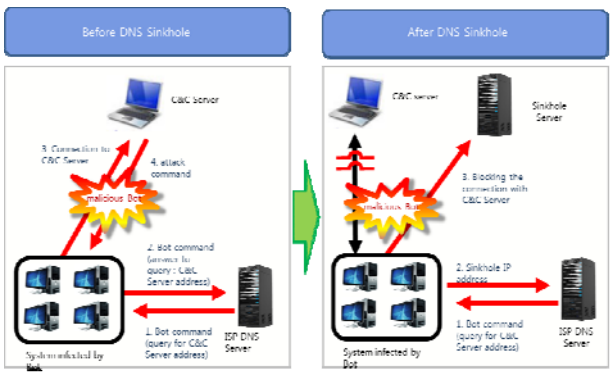

Figure 2. DNS sinkhole

D. *2.4 uRPF(unicast Reverse Path Forwarding)*

This is a technology that can prevent IP Spoofing attacks that use spoofed source IP addresses. It checks the source IP addresses of packets received to see if reverse paths to the source IPs exist. If the reverse path is exist, the source IP address is reliable.

When a packet is inserted in the router, it checks whether a reverse path to the input interface of the packet exists and allows the packets to pass in case where the reverse paths exists. If the reverse path does not exist, the packet will be removed as a spoofed source IP address[7].

Since DDoS attacks spoof their source addresses, uRPF can be a effective denial of service attack preventing method. However, this technology cannot be applied to asymmetric network structures with multiple routing paths and has a shortcoming that it has no solution but to preventing spoofing attack to deal with various DDoS attacks[6].

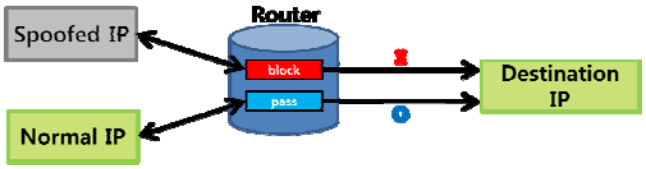

Figure 3. uRFP

E. *Problems of DDoS Prevention Systems*

1) *Strategy of current DDoS prevention systems*

Existing DDoS prevention systems are capable of defense against high traffic DDoS attacks on layers 3, 4, and 7 in OSI 7 layers. To detect high traffic DDoS attacks, security policies are set on the defense systems so that DDoS can be detected in cases where traffic exceeding the defined range occurs. The prevention systems are configured to detect Flooding attacks occurring in heavy scales through Traffic Rate Limit policies to recognize the traffic that exceeds the threshold value during the determined time and inspect the data part of all packets to check where the data are harmful. In addition, to reduce the load of analyzing all incoming packets, the frequencies of attacks from certain IPs are figured out and IP addresses that are classified as bad or zombie PCs are registered in the black list to drop packets from those IPs with a view to improving packet processing performance.

2) *Problem of Current DDoS Systems*

Current DDoS defense systems have been developed against heavy traffic DDoS attack and do not have measures to respond to low traffic DDoS attacks. It just removes packets from bad IPs or close the ports connected with them. In the case of high traffic DDoS attacks, randomly selected forged IPs are used in most cases. In this case, service requests from normal users who use those IPs are also blocked due to the black list registration of those IPs. In addition, if abnormal transmission caused by temporary network malfunction is determined as DDoS attack at layer 7, the relevant users cannot receive normal packets because of the same reason[3].

III. MULTIPLE FIREWALLS AND MULTI-FILTERING

A. *Multiple Firewall*

Double firewall is typical multiple firewall. In the case of double firewall, the Internet and internal networks are connected through screened gateways and screened sub networks are guarded with firewall systems.

Screening routers are placed between the Internet and screened sub networks, and between internal networks and screened sub networks and filter input/output packets using packet filtering rules. The Bastion Hosts placed in screened sub networks side and refuse packets that are not allowed to enter using a proxy server (application gateway). In this structure, access to screened sub networks can be made only through bastion hosts. Therefore, trespass to the screened sub network is not easily[11]. Trespassers can trespass on internal networks through the Internet only after re-configuring the Internet, screened sub networks, and internal network routing tables so that they can freely access internal networks. However, this is not easy because screening routers exist. Even when the bastion host has been invaded, the trespasser should trespass the screening router to access the screened sub network.

Figure 4. Double firewall

B. *System structure*

"Fig. 5" shows the double firewall structure used in this paper and the structure is already proposed[8]. NAT(Network Address Translation) is used to logically divide the inside and outside.

The first firewall works in two separate stages. First, it analyze packets using information on the paths through which the packets passed the router. Packets with spoofed source IP are removed if the hop count values of the IP is different from those of original source IP[8]. Second, it use R-PA(Router Path Analysis) packet filtering method which applying path names(Path Identification) to the existing packet filtering and it is a stricter packet filtering method[14].

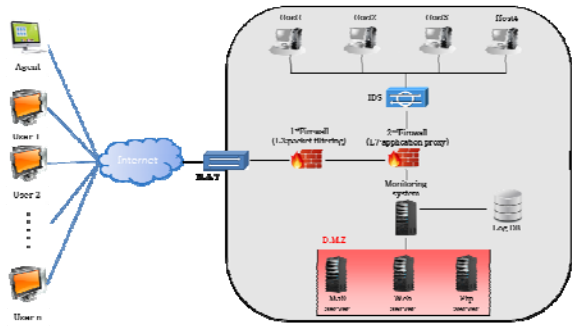

Figure 5. System structure

1) *Packet filtering using a hop counter*

Since spoofed IP packet has the hop count value of the original IP address when it arrived at the destination, the IP packet can be identified whether it is spoofed one or normal one.

In this structure, packets are filtered through router path analysis (see chapter 3.3.2) first and filtered again using TTL(Time to Live) values. To supplement the problem of delays in filtering processes because packet information for individual existing IPs should be obtained, the mean value calculated through statistical analysis based on previous TTL activities (TTLm) is used.

When the packets arrived, their Source IPs and final TTL values are extracted. Thereafter, information of the saved initial TTL values and mean TTL values is taken from the IP table. The hop count value of each packet is calculated with the initial TTL value in the table and the final TTL value of the packet. The calculated value is compared with the mean TTL value to decide whether the packet is a normal one or not. When the packet is passed, finally, the hop count value of the packet and the already stored hop counter value are compared with each other to decide whether the packet is a normal one[5][13]. In this case, a range of errors exists between the mean TTL value and the calculated hop count value of the packet. Error boundary is exist between the calculated hop count value of the input packet and the hop count value that is stored in the table already.

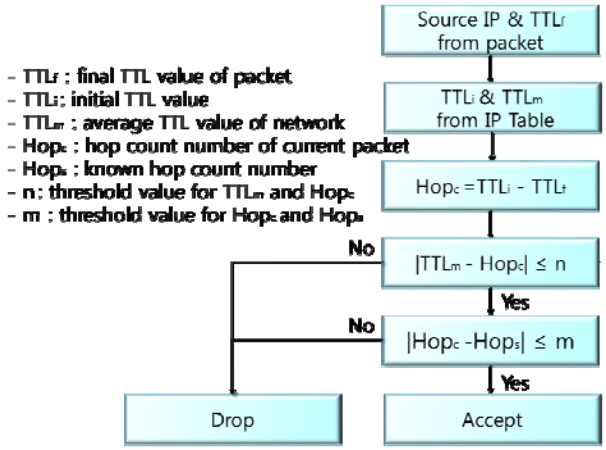

Figure 6. Hop counter filter

2) *Packet filtering using using path analysis*

a) *Routing Path analysis*

Packets that passed the router through the same path have the same path name value. Path name values are formed through packet marking when packets pass the router. When a packet arrives at the router, the router marks the last n bits of the IP at the bit string position of the 16 bit ID field of the packet. The bit string position to be marked is calculated using TTL(Time to Live) value. Because the values marked as such has different value according to the paths passed by packets, spoofed IPs can be identified based on their path name value. Using the path name value, the victim host(V) can make a black list of attacking packets to filter out attacking packets inserted into the victim host[14].

If the system consists of an attacker(A), a victim(V), and routers(R) as seen in “Fig.7”. By a basic marking method, routers mark the last n bits of their IP addresses at the IP Identification Fields of the inserted packets. To decide the position where the path name should be marked, 16 bits are divided into n sections(16/n) and the TTL values of packets are used as indexes (TTL mod [16/n]). Routers insert the last n bits of their IP addresses into the positions for marking. The victim uses these path name values to block attacking packets[9]. Since the path name method is designed with very simple, the method has advantages that it does not give overheads to the routers and that the victim can filter the packets immediately without help of upper routers.

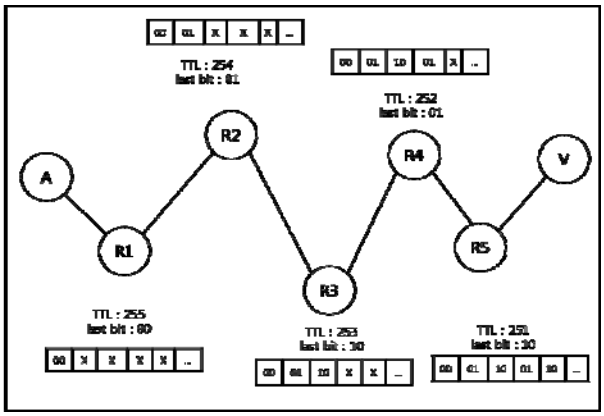

Figure 7. Routing path analysis

Attackers may change the initial TTL value to make the different path name marking value inserted from the same path. To deal with this trick, the victim host can inspect TTL values to find out the oldest marking position in the packet and can rotate the remaining values base on the position to obtain the inherent path name marking values from modified TTL values.

b) R-PA(Router Path Analysis) packet filtering method

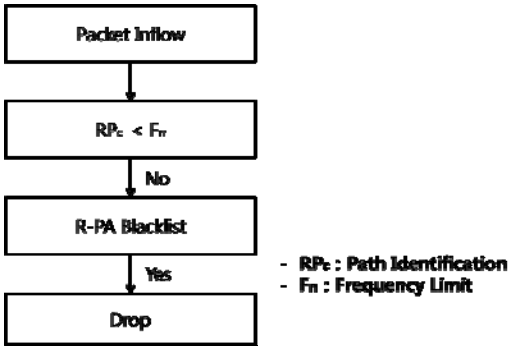

Figure 8. Router path analysis

This method is dividing all network paths into attacking paths and normal paths and filtering out those packets that come from the attacking paths. The criterion for distinguishing between attacking paths and normal paths is the amount of traffic. That is, detect those packets that include frequently occurring marking values. When a packet arrives, the frequencies of path name values are measured to find out frequently occurring marking values and if the value is higher than the threshold value determined by the administrator, the packet is removed[9][14].

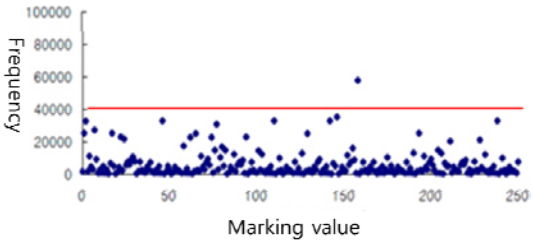

Figure 9. Marking frequency measurement

Suspected packets are added to the black list and removed to prevent them from coming in again later.

3) Second firewall and traffic monitoring

The second firewall is a layer 7 firewall that inspects packets that came through the first firewall and IDS (Intrusion Detection System) to classify packets. The packets are inspected to check if specific source IP traffics and specific session traffics are exceed the threshold value. Packets that came through the first firewall are inspected by IDS to determine whether the packets should be passed or should be removed according to the contents of packet data. Packets remaining after filtering through the first firewall and IDS are transmitted to the monitoring system. The monitoring system monitors system resources allocated to each users according to the security policy determined by the administrator and decides suspending, blocking, and permission in real time[13].

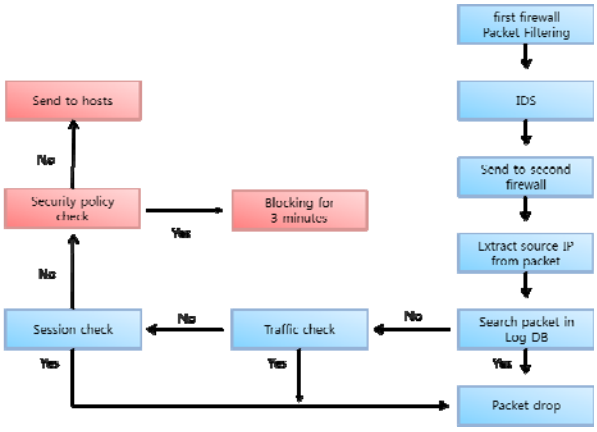

Figure 10. Traffic minitoring system

4) Security Policy

The security policy referred to the monitoring system is set through statistical analysis after determining the threshold value that can be handled by existing servers. The threshold value of session traffics and the number of sessions for each users are managed in the second firewall. Server down and illegal actions are prevented by applying the security policy to the user's activities and the server's activities[9][10].

Security policies for resource limits that fit the Users' roles and role class assigned and threshold values are set so that users can use resources that proper to their roles.

When a user conducts an action that deviates the determined security policy, the users is left under the interrupted status for three minutes first and if the same situation is repeated, the IP is blocked.

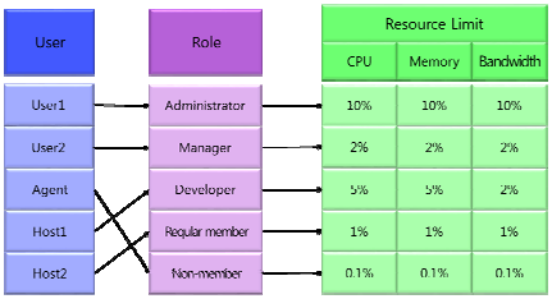

Figure 11. Security policy

IV. CONCLUSION

Before As the Internet has been developing rapidly, DDoS attacks also have been diversified by equipping new attack methods. Recently, as DDoS attack rates increase, more rigid responding systems than current defense systems are required. Current DDoS attack prevention methods set threshold values by collecting and analyzing traffics for a certain period of time. However, those DDoS attack detection methods cannot detect DDoS attacks at the beginning of attack so that the victims are damaged or the victim cannot respond effectively to the attacks even if the attacks are detected because the victim is already damaged.

In this paper, a DDoS prevention system is proposed that is reinforced by combing effective packet filtering methods on the double firewall. To determine the possibility of attacks by packets coming in from the outside, strict R-PA(Router Path Analysis) packet filtering method is installed in the first firewall. With this method, packet filtering processes can be improved and false detection ratios also can be reduced because delay problem of the hop count filtering method which need packet information for individual existing IPs is partially covered. In the second firewall, the data of packets that come through the first firewall are inspected to classify the packets into normal ones and abnormal ones. And it checks if packets exceed the traffic limit and if user session traffic exceeds the threshold value to determine whether the packets should be passed as normal ones or should be removed. System overloads can be reduced obviously by concurrent processing of internal and external packets separately at the same time using the first and second firewall.

ACKNOWLEDGMENT

This work was supported by 2015 Security Engineering Research Center, granted by the Korea Ministry of Trade, Industry & Energy and 2015 Hannam University Research Fund.

*Corresponding author

REFERENCES

[1] David Moore, and Slammer worm, “http://www.cs.berkeley.edu/~nweaver/sapphire/”

[2] Dong-Su Kim, “SYN flooding attack defense framework using ability tokens,” Seoul : Ajou University, 2005.

[3] Hyeong-Su Lee, “Respond System for Low Traffic DDoS Attack.,” Seoul : Soongsil University, 2011.

[4] Ji-Seon Lee, Min-Sun Lee, and Byeong-Su Lee, “Hacking and security master,” Seoul : Ehan Publishing, 2004.

[5] Ji-Yong Ahn, “Development of a Fast Packet Filtering Algorithm,” Seoul : Soongsil University, 2002.

[6] J.K.Lee, “Responding methods by type of DDoS attacks and by security equipment,” National Computing and Information Agency of Korea, 2010.

[7] Juan M. Estevez-Tapiador, Pedro Garcia-Teodoro and jesus E.Diaz-Verdejo, “Anomaly Detection Methods in Wired Network: a Survey and Taxonomy,” Computer Communication. vol. 27, pp. 1569-1584, October 2004

[8] Jung-Hyo Park, Hyun-Chul Kim, and Moon-Seog Jun, “Efficient detection and defense techniques of using two firewalls and a monitoring system for DDoS attacks” Proceedings of Korea Institute of Information Scientist and Engineers(D), vol. 36, no. 2, pp. 78-81, 2009.

[9] Kang-Sin Lee, “Dynamic Path Identification Method to Defend Against DDoS Attack,” Seoul : Korea University, 2005.

[10] Karanjit siyank, and Chris Hare, “Internet Filerwalls and Network Secureity,” New Rider, 1996.

[11] Se-Deok Jang, “TCP/IP wire/wireless networks,” Seoul : Daelim Publishing, 2005.

[12] Dong-Min Seo, “DDoS attacks - zombie attacks that paralyze servers,” http://it.donga.com/openstudy/4064/

[13] Wu-Seok Seo, Dae-Woo Park, and Mun-Seok Jeon, “A study on DDoS attack methods and defense using multi-firewall methods,” Proceedings of the Korean Society of Computer and Information. Vol. 18, no. 1, pp. 231-240, 2010.

[14] Yong-hoon Jeong, Man-pyo Hong, and Hong-jin Yeh, “An Efficient Implementation of Hop Count Filtering using Path Identification Mechanism,” Proceedings of Korea Institute of Information Scientist and Engineers(A), vol. 31, no. 1, pp. 322-324, 2004.