Prevention Mechanism on DDOS Attacks by using Multilevel Filtering of Distributed Firewalls

Sagar Pande
Computer Science & Engineering, SGBAU,
Gangotri Colony near Tapovan Gate,
Amravati, Maharashtra, India.
sagarpande30@gmail.com

Prof. Ajay B. Gadicha
Information Technology, SGBAU,
Kathora Road,
Amravati, Maharashtra, India
ajjugadicha@gmail.com

Abstract— In the past decade, it has been found that DDoS has proved to be the most dangerous attack. IP spoofing is one of the kinds of DDoS attack which is emerging as a big threat in today's world of technology. The Proposed Framework is a unique technique composed of distributed firewalls and hop count based filtering, it can be used to prevent such kind of DDoS attack. At The primary level, distributed firewalls filters the IP addresses which can be either Internet or Intranet. Along with this it also provide various other advantages such as reducing the dependency of network topology. At secondary level, hop count and TTL based filtering provides more secure level of filtration. In this paper, we have proposed a new framework which reduces the limitations of previous conventional techniques**.**

Keywords*-DDoS, TTL, Packet Filtering, Hop Count, CHCF, Distributed Firewall, DPHCF, IP Spoofing.*

*****

I. INTRODUCTION

Network Security is the most important parameter for ideal network. It covers a variety of computer networks, such as public, private or even combination of both, used everywhere conducting transactions and communications among businesses, government agencies and individuals. Generally to protect the information, hiding it from the illegitimate access and illegitimate changes make that information available only to the legitimate users. The available link bandwidth varies in accordance with the statistics of the input traffic.

The basic problem with these kind attacks is to distinguish between legitimate and illegitimate client packets. Attackers are making their attacks impossible to determine whether a packet belongs to legitimate client or an attacker. It is a large-scale, coordinated attack on the availability of services of a victim system or may be through many zombie computers on the Internet. The frequency of DDoS attacks that target to the internet is continuously increasing to slow down a victim server or even the entire sites. In DDoS, the attack is initiated from a large number of attackers known as "**botnets**" or "**zombie**". The motives and targets of DDoS attacks can greatly vary; one of the motives is that the target person or company *loses* ***a great deal of time and money.*** The DDoS attack is that they involve concerted efforts to saturate the victim machine (often a webserver) with a large volume of traffic, which causes the server unable to respond to authenticated user requests. Network and protocol implementation loopholes can also be used for launching such attacks. DDoS Attacks mainly affect Software Systems, Network Routers/Equipment/Servers and End-User PCs.

- **Objectives**

1. Dual filtering helps to detect flooding & IP-Spoofing Attack which can falsify the senders or receivers information by modifying the IP Addresses.
2. New Multi-Level Architecture makes it difficult for one DoS to take down an entire site and occupy the complete resources**.**
3. Generate notifications to all the distributed firewalls for further blocking of spoofed addresses.

II. LITERATURE REVIEW

Determining the type of attack required the analysis of its consequences as per the communication is needed. Two different approaches have been taken by the researcher: *router-based approach* and *host-based approach*. Compared to the router-based approach, the host-based approach has the advantage of being immediately deployable. The Conventional host-based approach secures Internet servers using sophisticated resource management schemes.

CHCF technique [2] a host side and conventional method has been proposed which is ineffective as it take long computation time. In HCF technique [4] author was unable to improve the packet filtering mechanism In [3] the author requires a key which need to be shared between adjacent routers which take large computational time and more memory space. PHCF technique [5] does not assure whether the unchecked packets are legitimate only. DPHCF-RTT technique [1] has been implemented on real-time environment for maximum number of intermediate nodes up to 30. Hence, this technique lacks in maximizing the number of intermediate nodes greater than 30.

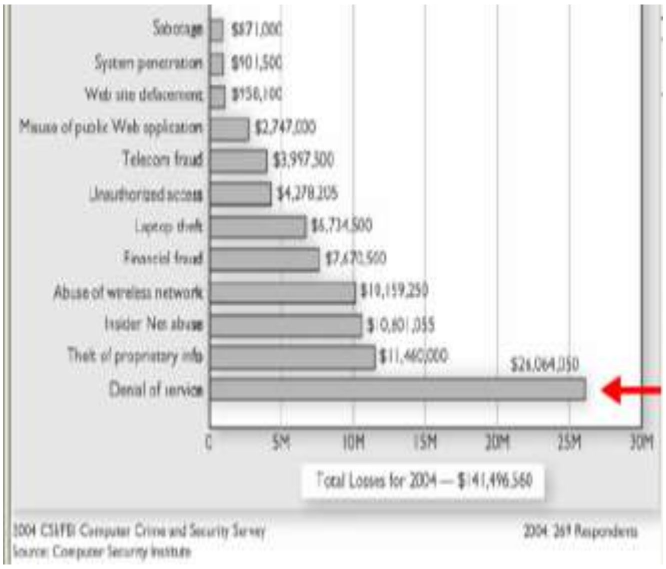


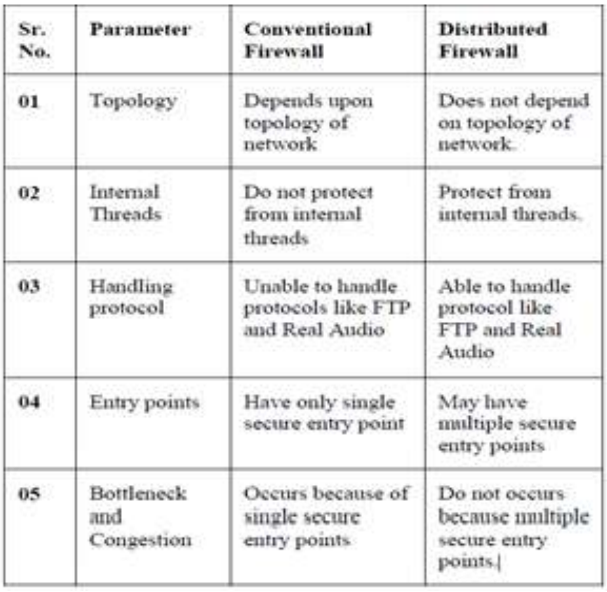
Fig.1: Computer Crime and Security Survey (2004)

After reviewing the literature, it is found that CHCF, PHCF, DPHCF-RTT techniques, which are used to filter the spoofed packets from the total packets, possess certain limitations pertaining to low detection rate of spoofed packets. Hence, there exists lot of scope to maximize the detection rate of spoofed packets. To support and make the existing filtering technique more powerful there was a need to provide filtering at firewalls.

A firewall is implemented in network and is operated by trusted or untrusted locations. It permits traffic from the trusted location to untrusted locations and it does not need any external configuration. The main purpose of firewall is maintaining the untrusted or non-requested users from accessing our computers [6]. A firewall may be a software or hardware and it is normally placed at the network with the range and safeguards the incoming and outgoing connections. Its main mechanism is to limit the traffic. The data packets are limited based on the some features such as source address, destination address, protocol (TCP/IP etc.), source port and the destination port. It prepares some set of rules and regulations to filter the data. It consists of the rules which deny or accept the network connections based on the details of the nodes which are going to connect [7] [8].

Conventional Firewall has number of limitation which makes it unsuitable for secure filtration due to this various research has been done to overcome these drawbacks. The author [9] has given comparisons between conventional and distributed firewall which is given in following table. Using this Information, a new framework is proposed which combines the benefits of both the techniques preventing the DDoS attacks.

Table 1: Comparison between Conventional and Distributed Firewalls [9]



Sr. No.	Parameter	Conventional Firewall	Distributed Firewall
01	Topology	Depends upon topology of network	Does not depend on topology of network.
02	Internal Threads	Do not protect from internal threads	Protect from internal threads.
03	Handling protocol	Unable to handle protocols like FTP and Real Audio	Able to handle protocol like FTP and Real Audio
04	Entry points	Have only single secure entry point	May have multiple secure entry points
05	Bottleneck and Congestion	Occurs because of single secure entry points	Do not occurs because multiple secure entry points.|

III. PROPOSED WORK

Traditional defense techniques focus on the network-layer DDoS attacks and use TCP and IP properties to discover attack signals arising. In this paper, the proposed framework is composed of multi-level filtering at firewalls. First level emphasis on filtering the IP addresses by using Distributed Firewall Based Inspection while at next level filtration is by done using Hop-Count & TTL based Inspection.

3.1. Distributed Firewall Based Inspection

Distributed firewalls are able to filter traffic from both the Internet and the Intranet. Distributed firewalls operate centrally which make distributed security practical. Unlike conventional firewalls, distributed firewalls are not placed in single location. They are installed throughout the network to all the distributed systems.

3.1.1. Distributed Firewalls are based on three main points.

- ***Policy Language & Distribution***

For assuring the integrity of the policy language during transfer, we need to use the policy distribution scheme. The policy language is used to create rules and regulations for each of the distributed firewalls. Various different tools can be used to assign the policy language to the firewalls. One of the famous tools for assigning policy language is KeyNote System.

- ***IPSEC***

To provide network-level encryption, we use IPSEC which secures network traffic and the transmission of policies. It helps the distributed firewall to authenticate each other based on the Encryption Mechanism.

- ***Centralized Control Server***

It is a core component of distributed firewalls. It reduces the cost & act as a single point of control over all the distributed firewalls.

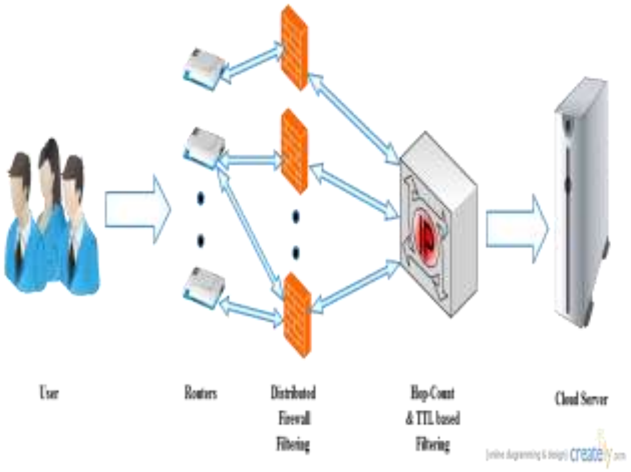

User
Routers
Distributed Firewall Filtering
Hop-Count & TTL based Filtering
Cloud Server
[online diagramming & design] creately.com

Fig 2: Multi-Level Filtration

3.1.2. Working of Distributed Firewalls

1. Install firewall on all network systems.
2. Write centralize policy by using policy language such as: Keynote.
3. Further compile the generated policy in a format to be transferred to each distributed firewalls.
4. Create certificates provided by IPSEC. These certificates uniquely identify the sender and don't depend on the network topology.
5. The firewall then evaluates the traffic based on the central policy and decides to allow or deny it.
6. The firewall then transfer logging information to a central location where it can be used for reporting.

3.1.3. Log Generation & Alerting Mechanism

Log Generation play very crucial role to discard the spoofed address. It consist of two parameters the Whitelist and the Blacklist. All the incoming IP address is store in one of the parameter. The IP address which is allowed to access is stored in the Whitelist whereas the one which need to be discarded are kept in the Blacklist. The Reason for such storage of both kinds of IP address is that it will help to reactively detect whenever another incoming spoofed request come from the same IP address. This helps to reduce our workload and saves our time as well as space from repeated operations. Alerting Mechanism is completely related to the Blacklist parameter as soon as the entry is made in the Blacklist, it alerts all the distributed firewalls to block that IP address and simultaneously discard that IP address from further communication. All the updated logs are generated here and forwarded to each and every firewall. Further, the log is also updated by the Hop- Count & TTL based Inspection, which is distributed to all the firewalls in the similar manner.

3.2. HOPCOUNT & TTL BASED INSPECTION

Central to HCI is the verification of the source IP address of each packet via hop-count & TTL based inspection. This is the second level of filtration which validates the IP address that come from Distributed Firewall Filtering. In this level we will filter the IP address on the basis of Hop Count & TTL value.

3.2.1 TTL based Hop Count Calculation

Since hop-count information is not directly stored in the IP header, one has to calculate it basis of the TTL field. TTL is an 8-bit field in the IP header, originally introduced to specify the maximum lifetime of each packet in the Internet. Following are the notation and formula for calculating Hop Count.

- **Notations**

  T0-- Initial TTL
  TF-- Final TTL
  HCC-- Hop Count Calculated
  HCS-- Stored Hop Count
  = -- Equal
  =! -- Not Equal
  || -- OR

- **Formula**

  HCC=T0-TF

- **Comparison**

  HCC=HCS || HCC=! HCS

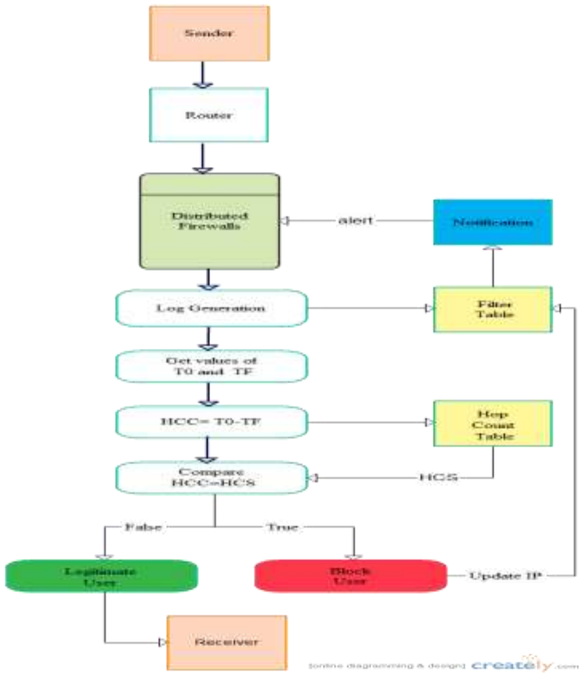


Fig 3: Internal working of HC and Firewall filtrations

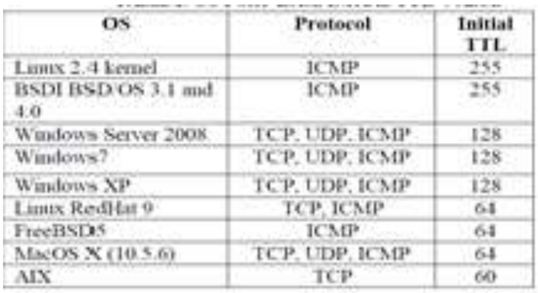
We will first gather the values of initial and final TTL values. The final TTL value is obtain from IP header. Then further the Hop Count is calculated by using the above formula. Further we will compare the values of both the HCC

& HCS and on the basis of this comparison we will update the value of log. The value of HCS is obtained from whitelist parameter of log table.

If the value of Hop count is HCC=HCS then the value of Whitelist parameter is kept as it is and if the value of Hop count is HCC=! HCS then the value of Blacklist parameter is updated creating the alert messages which are further forwarded to all distributed firewalls. By updating the log values at firewall level helps to avoid the repeated calculation for same IP addresses. This ultimately saves time and space and hence makes the filtration process work faster.

The following table represents the initial TTL values along with their respective operating Systems. We can easily determine the initial TTL value by selecting the smallest possible initial TTL value from the following table which is larger than its final TTL value.

Table 2: OS port base Initial TTL Values [10]



OS	Protocol	Initial TTL
Linux 2.4 kernel	ICMP	255
BSDI BSD/OS 3.1 and 4.0	ICMP	255
Windows Server 2008	TCP, UDP, ICMP	128
Windows7	TCP, UDP, ICMP	128
Windows XP	TCP, UDP, ICMP	128
Linux RedHat 9	TCP, ICMP	64
FreeBSD5	ICMP	64
MacOS X (10.5.6)	TCP, UDP, ICMP	64
AIX	TCP	60

3.2.2. Hop Count Table

The Hop Count table consist of two important parameters i.e. IP addresses and HCS value. Whenever the first time HC value is computed it is stored in HC table as HCS value along with their IP addresses. Next time, the value of HC is calculated and compared with the values of stored HCS. Based on their comparison IP addresses are allowed to communicate. If their values are consistently found as equal then it indicates that the request is not coming from legitimate user. Due to this reason the respective IP address must be blocked. Then value of IP address is updated in the filter table which will restrict these IP addresses from further communication.

IV. Conclusions

DDoS attacks are complex which causes serious problem on Internet .Affecting not only a victim but the victim's legitimate clients. DDoS defense approaches are numerous, so there is a need to learn how to combine the approaches to completely solve the problems. Proposed Framework is one such unique combination compose of two different defense mechanism .As networks continue to change and expand new tools are needed to keep them secure. Distributed firewalls take a new approach by securing every host on the network. They also have no trouble handling the changing topology of today's networks. Along with this Hop Count filtering provide a defense mechanism to mitigate IP-spoofing attack.

As the research is going on, new features will be added that will only increase their security and ease of use. During further research the approach will be to implement this framework by using NS2.

References

[1] Ritu Maheshwari, Dr. C. Rama Krishna and Mr. M. Sridhar Brahma--Defending Network System against IP Spoofing based Distributed DoS attacks using DPHCF-RTT Packet Filtering Technique, 978-1-4799-2900-9/14©2014 IEEE.

[2] A. Mukaddam, I. H. Elhajj, "Round Trip Time to Improve Hop Count Filtering," IEEE Symposium on Broadband Networks and Fast Internet, American University of Beirut, Lebanon, 66-72,28-29, May, 2012.

[3] B. Krishna Kumar, P.K. Kumar, R. Sukanesh, "Hop Count Based Packet Processing Approach to Counter DDoS Attacks," International Conference on Recent Trends in Information, Telecommunication and Computing, PET Engineering College, Thirunelvelli, India, pp. 271-273, March, 2010.

[4] H. Wang, C. Jin and K. G. Shin, Defense against Spoofed IP Traffic Using Hop-Count Filtering, IEEE/ACM Transaction of Networks, 10.1109/TNET.2006.890133, Volume. 15, No. 1, Feb 2007.

[5] B. R. Swain, B. Saboo, "Mitigating DDoS attack and Saving Computational Time using a Probabilistic approach and HCF method," IEEE International Conference on Advance Computing, NIT, Rourkela, 1170-1172,6-7, March 2009.

[6] Azzouna, Nadia Ben and Guillemin, Fabrice, Analysis of ADSL Trafficon an IP Backbone Link, IEEE Global Telecommunications Conference 2003, San Francisco, USA ,December 2003.

[7] Cho, Kenjiro, Fukuda, Kenshue, Esaki, Hiroshi and Kato, Akira, The Impact and Implications of the Growth inResidential User-to-User Traffic, ACM SIGCOMM 2006, Pisa, Italy, September 2006.

[8] Balachandran, Anand; Voelker, Geoffrey M.; Bahl, Paramvir and Ragan,P. Venkat, Characterizing user behavior andnetwork performance in a public wireless LAN, Proceedings of the 2002 ACM SIGMETRICS International Conference on Measurement and Modeling of Computer Systems, pp.195-205, 2002.

[9] Suraj J. Warade, Pritish A. Tijare, Swapnil. N. Sawalkar, Data Security in Local Network using Distributed Firewall: A Review, International Journal of Computer Applications (0975 – 8887) National Conference on Emerging Trends in Computer Technology (NCETCT-2014).

[10] Govind M Poddar, Nitesh Rastogi, UHCF: Updated Hop Count Filter Using TTL Probing and Varying Threshold for Spoofed Packet Separation, International Journal of Emerging Research in Management &Technology ISSN: 2278-9359 (Volume-3, Issue-4), April 2014.