International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 4 Issue 5, July-August 2020 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

A Survey of DDOS Attacks and Solutions using Packet Filtering Mechanism

Usman Aijaz N

Department of Computer Science, Brindavan College of Engineering, Bangalore,
Visvesvaraya Technological University, Belgaum, Karnataka, India

ABSTRACT

Distributed Denial Of Service attack is the most significant and continuous threat in cyber security. It is one of the biggest security concerns for security professionals and has taken the attention of today's cyber world. This attack is an attempt by an attacker to flood the victim machine by generating a large volume of traffic using compromised machines. DDOS attacks can affect any device on any network and at the same time target different types of resources such as CPU, memory, and bandwidth, etc. The Decentralized nature of the internet helped the attacker to lunch this type of attack. The impact of a DDOS attack is huge like Money, time, clients and even reputation of the organization can be lost. Depending on the severity of an attack, resources could be offline for 24 hours, multiple days, or even a week. To prevent this attack, it is very important to filter the attack traffic not to enter the network. All filtering techniques are applied to the routers which ensure that only legitimate traffic can get access to a system. In this paper, we provide an overview of different types of DDOS attacks. we also cover different packet filtering techniques found in the literature along with their success and failure in DDOS prevention.

KEYWORDS: *Distributed denial-of-service, DDOS Attacks, Packet Filtering, Prevention Mechanism*

How to cite this paper: Usman Aijaz N "A Survey of DDOS Attacks and Solutions using Packet Filtering Mechanism" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-4 | Issue-5, August 2020, pp.755-759, URL: www.ijtsrd.com/papers/ijtsrd32938.pdf

IJTSRD32938

INTRODUCTION

Distributed Denial Of Service attack uses a large number of computers called bots and internet connection. The attacker uses bots to flood the target system or resources. Bots are collected from unprotected computers that are accessing the internet through a high-speed internet connection. Attackers place malicious software on these bots. These bots are then grouped to shape one big network called a Botnet. Bots in this Botnet are awaiting only a command from the attacker to launch DDOS attacks. Once if this attack is launched then it presents legitimate users from accessing a specific system or network resources.

DDOS attacks can be launched using these two ways

1. Vulnerability attack: The attacker send some malicious packets to the victim machine to confuse a protocol or an application running on it.
2. Network/Transport and Application flooding attack: Here the attackers interrupt legitimate user connectivity by exhausting network resources. In application-level flooding attack, the attacker disrupts the services of a legitimate client by exhausting server resources such as CPU, Memory, and Bandwidth [1].

Packet filtering is the process of controlling access to a network by examining the incoming and outgoing packets and allowing them to pass or drop based on the IP address of the source and destination. Packet filtering is both a tool and a technique that is used to accomplish a task either by using some instruments or methods. It works in the network layer of the OSI model or the IP layer of the TCP/IP model. All Internet traffic travels in the form of packets. A packet is a quantity of data of limited size. When larger amounts of continuous data need to be sent, it is broken up into several small packets for transmission. These are reassembled at the receiving end. A packet is a series of digital numbers that convey information such as data, acknowledgment, request, the source, and destination IP address and port Information about the protocol and Error checking information, etc. In packet filtering mechanism Depending on the packet and the filtering rule, the router can drop the packet, forward it, or send a message to the Source. The rules which determine which packets to be sent, and which not to be sent can be based on the source and destination IP address, source, and destination port number, or the protocol used. Packet filtering can also be done at the firewall level, providing an additional layer of security [2].

A. Motivation Of Attackers In Launching DDOS Attacks

DDOS attackers are usually encouraged by various motivations. We can categorize DDOS attacks based on the motivation of the attackers into five main categories [1]:

1. Financial or economical gain: These attacks are a foremost concern for companies, businesses, and organizations. Attackers of this category are usually the most technical and the most experienced attackers.

Attacks that are launched for financial gain are the most dangerous and hard-to-stop attacks.

2. Revenge: Attackers of this category are generally angry individuals of the organizations. with lower technical skills they carry out such attacks as a response to a perceived injustice.
3. Ideological belief: Attackers who belong to this category are encouraged by their ideological beliefs to attack their targets. This category is currently one of the major motivations for launching DDOS attacks.
4. Intellectual Challenge: Attackers of this category attack the targeted systems to learn how to launch various attacks. They are generally young hacking enthusiasts who want to show off their abilities. Attackers use different attack tools and botnets that are available for rent to launch a successful DDoS attack.
5. Cyber warfare: Attackers of this category usually belong to the military or terrorist organizations of a country. they are diplomatically motivated to attack a wide range of critical infrastructure in another country.

B. DDOS Attack Scope And Classification

DDOS flooding attacks can be classified into two categories based on the protocol level that is targeted[1].

1. Network /Transport level DDOS Flooding attacks.
2. Application-level DDOS Flooding attacks.

1. Network/transport-level DDoS flooding attacks:

These attacks have been launched using a protocol such as TCP, UDP, and ICMP and DNS. There are four types of attacks in this category [1] as shown in figure 1.

1.1. Flooding attacks: Attackers focus on disturbing authentic user's connectivity by exhausting the victim network's bandwidth [3]. These attacks exhaust the network by consuming all the resources until it shuts down. They were very effective in flooding the network bandwidth. This type of attack is harder to recognize because it looks like legitimate traffic.

1.2. Protocol exploitation flooding attacks: Attackers exploit the specific vulnerability of the victim's protocols to consume excess amounts of the victim's resources [3].

These vulnerabilities mainly come from two aspects. One is from protocol design procedure other is from the malicious use of a legitimate protocol process.

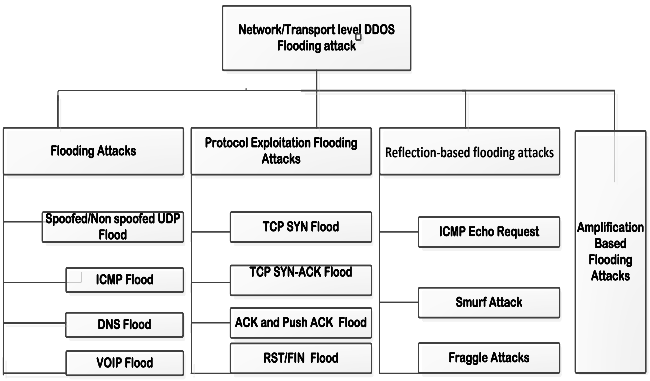
Network/Transport level DDOS Flooding attack
Flooding Attacks
Protocol Exploitation Flooding Attacks
Reflection-based flooding attacks
Amplification Based Flooding Attacks
Spoofed/Non spoofed UDP Flood
ICMP Flood
DNS Flood
VOIP Flood
TCP SYN Flood
TCP SYN-ACK Flood
ACK and Push ACK Flood
RST/FIN Flood
ICMP Echo Request
Smurf Attack
Fraggle Attacks

Fig 1 Network /Transport level DDOS flooding attacks

1.2.1. TCP SYN Flood attack: This attack exploits weaknesses in the TCP connection sequence which is 3 Way handshakes. The attacker pretenses as a DNS Client and spoofs the source IP address with a fake IP address, which will make the DNS server to send SYN-ACK packets to the fake destinations. The receivers of the SYN-ACK will simply drop them, as they have not initiated it[4].

These flooding attacks exhausts a victim's server by depleting its system resources (memory, CPU, etc.).These attacks result in performance degradation or complete server shutdown.

1.3. Reflection-based flooding attacks: Attackers usually send fake requests (e.g., ICMP echo request) instead of direct requests to the reflectors. Any server open to the Internet and running UDP-based services can be used as a reflector. these reflectors send their replies to the victim and exhaust victim's resources [5].

1.3.1. Smurf attacks: Attackers send ICMP echo request traffic with a spoofed source IP address of the target victim to several IP broadcast addresses.

Most hosts on an IP network will accept ICMP echo requests and reply to the victim machine., in this way the attacker target the victim machine[6].

1.3.2. Fraggle attacks: these attacks are similar to Smurf except styled. Do not use hard tabs, and limit use of hard returns to only one return at the end of a paragraph. Do not add any kind of pagination anywhere in the paper. Do not number text heads-the template will do that for you.

Finally, complete content and organizational editing before formatting. Please take note of the following items when proofreading spelling and grammar:

A. Abbreviations and Acronyms

Define abbreviations and acronyms the first time they are used in the text, even after they have been defined in the abstract. Abbreviations such as IEEE, SI, MKS, CGS, sc, dc, and rms do not have to be defined. Do not use abbreviations in the title or heads unless they are unavoidable.

that they use UDP echo packets instead of ICMP echoes. Fraggle attacks generate even more bad traffic and can create even more damaging effects than just a Smurf attack and TCP-SYN flood attack.

2. Application-level DDoS flooding attacks:

These attacks emphasis on disrupting authentic user's services by exhausting the server resources (e.g., Sockets, CPU, memory, disk/database bandwidth, and I/O bandwidth) [7]. Application-level DDoS attacks consume less bandwidth and are very analogous to benign traffic. There are two types of attacks in this category [5] as shown in figure 2.

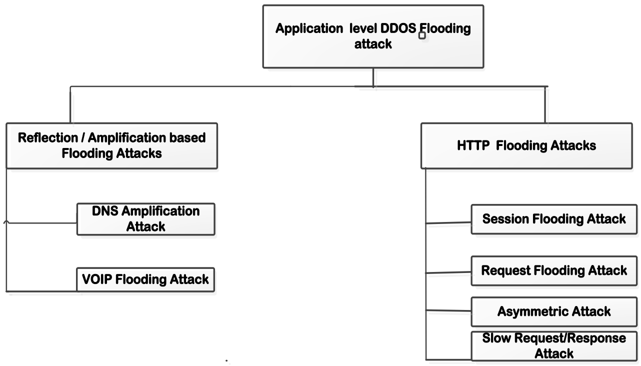

Fig 2: Application-level DDOS Flooding attacks.

2.1. Reflection/amplification-based flooding attacks: When a DNS query is sent to the DNS server, it will respond to the IP address from where the query originated. So if an attacker forges an IP address of the victim in the DNS query, the DNS server will send the response packet to the victim. The victim will mistake the response received as that of a response from an intermediary DNS server and drop them. When the victim starts receiving too many similar DNS response packets, the time taken for it to process and discard would be significantly higher and this adds to the network congested also, thereby making the victim go down. Also during this attack, the attacker remains hidden and cannot be traced. This kind of attack is called a DNS Reflection attack [5]

If the DNS request is constructed in such a way that it results in a larger response packet, then the victim has to go through the entire packet resulting in an amplification of the reflection attack. This phenomenon is called the amplification attack. Typically thousands of such requests are sent by the attacker in the name of the victim. When the recipients reply, all responses converge to the victim whose infrastructures are affected by the unexpected load and may go down.

VoIP flooding is another application-level attack example that employs the reflection technique [6]. This attack is a variation of an application-specific UDP flooding. Attackers usually send spoofed VoIP packets through Session initiation protocol at a very high packet rate and with a very large source IP range. VoIP flooding can overwhelm a network with packets with randomized or fixed Source IP addresses. If the source IP address has not been changed the VoIP flooding attack mimics traffic from large VoIP servers and can be very difficult to identify since it resembles legitimate traffic.

2.2. HTTP flooding attacks: There are four types of attacks in this category [8].

2.2.1. Session Flooding Attack: Resources of a server become exhausted when session request rates get higher than valid users. This malicious activity may result in a DDOS flooding attack, for instance, HTTP GET/POST flooding attack.

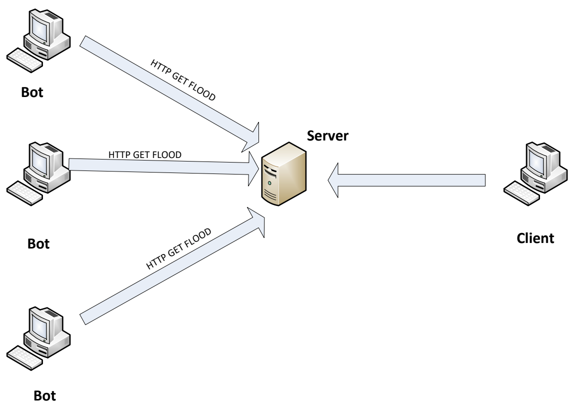

Fig 3: HTTP Flooding Attack.

2.2.2. Request Flooding Attack: This attack occurs when an attacker starts a vast number of requests in one session as shown in fig 3. This request is larger than the request of a valid user. The HTTP GET/POST session is an instance of an attack in this category that takes advantage of the HTTP 1.1 feature. The use of HTTP 1.1 also causes the attacker to bypass the defense mechanism of the session rate of several security systems.

Rai and Challa [9] claimed that the botnet is used for this attack. The botnet is designed to have a command-and-control structure that allows cyber impostors to issue a command to botnet machines. This attack can exhaust server resources as the botnet sends plenty of HTTP GET flood requests to a server.

2.2.3. Asymmetric Attack: this is a cyber-attack that uses a relatively small number of resources by an attacker to cause a significantly greater number of target resources to a malfunction or fail.

2.2.4. Slow Request/Response Attack: An attacker sends a high workload of requests to initiate attack as shown in fig 4 in the form of a session. The consequence of this attack introduces unreachability against a server. the attacker partially sends HTTP requests that grow quickly and repeatedly, update slowly, and never close. This continuous attack will make an available socket of a server to be full due to these requests. Another example of this attack is HTTP fragmentation, where the connection of HTTP is held for some time to bring down the server.

Rai and Challa [9] stated that the attack functions under a threshold limit to confuse the victim with malicious traffic that resembles legitimate traffic. The Slowloris attack is the example from this attack category, and it works by sending a large number of simultaneous HTTP requests, be it GET or POST, to a server. A server will continuously open separate connections as each HTTP request fails to complete its connection. The consequence of this attack denies users from gaining a connection to a server as the server concurrent connection is exhausted [1].

C. Packet Filtering Mechanisms Against DDOS Attacks

Prevention against DDoS attacks is the most desirable defense technique to fight against the DDoS attacks. As mentioned in the previous section, DDoS attacks put an immense threat to the resources of the victim (CPU, memory) as well as to the network bandwidth and infrastructure. Therefore, if an attack has been already launched and becomes successful, it may cause significant compromise to the victim's system. Thus, protection against DDoS attacks is more effective against DDoS attacks. since it ensures the prevention of the DDoS attack traffic as well as manages large attack loads before it may cause the attack to be successful.

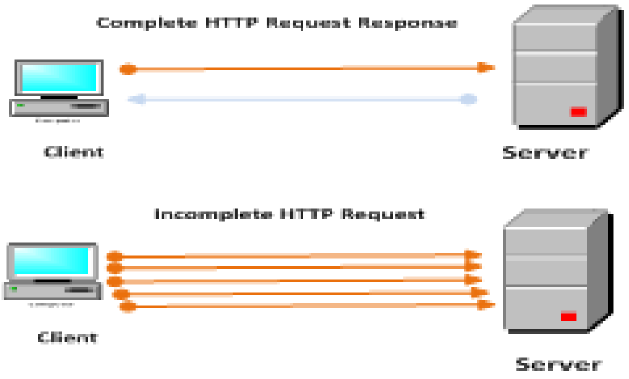

Fig 4: Slowloris DDOS Attack.

1. Ingress/egress filtering. A very popular and well-known filtering technique is the ingress/egress filtering. These techniques prevent traffic with spoofed IPs to enter into a network. Ingress filtering filters the malicious traffic intended to a local network and egress filtering rejects the malicious traffic leaving a local network. Ingress filtering defined in RFC 226768 allows those traffic to enter the network which matches with a predefined range of domain prefix of the network. Thus, if an attacker uses a spoofed IP address that does not match with the prefix, it is discarded in the routers. By blocking spoofed IPs this filtering techniques safeguard from a significant amount of DDoS attacks. However, it is not a suitable mechanism in the cases where the attacker uses the valid IP addresses of the Botnets as a source IP [10].

The success of these filtering depends on the Awareness of the range of probable IPs for different ports. This is not always possible to achieve for the complicated topologies used in different networks. Moreover, the filters in the routers cannot detect malicious traffic if an attacker uses spoofed IP addresses that fall into the valid address range.

2. History-based IP filtering: This method uses a pre-built legitimate IP address database. It has built based on the history of all the legitimate IP addresses that frequently appear at the target. During a bandwidth attack, the target only allows the packets whose source IP addresses belong to the IP address in the database. This technique helps destination hosts in resource management when their links to the upstream network become a bottleneck during a DDOS flooding attack [11].

However, any large-scale DDOS attack that simulates normal traffic behavior will defeat these filtering mechanisms.

3. Hop-count filtering. In this method, the time to live (TTL) value is used to count the number of hops. This hop counts are stored in a mapping table against each source IP address. Upon getting each packet, the number of hops required for this packet to reach the destination is calculated. This count is matched against the mapping table. A packet is identified as a spoofed packet if a mismatch is found in this comparison. If a packet is identified as a spoofed packet, the filter discards those packets as a prevention of an attack. The deployment of such a filtering technique is easier as it requires implementation in the victim's system [12].

However, it has a major drawback in the process of hop count. As this method counts the number of hops based on TTL, the number of false-positive is larger in this method. This is because the initial TTL value is usually different for different operating systems. the attacker can forge valid hop counts in their packets which allow the packets to pass the filter. Finally, for a flood of malicious packets, the system cannot perform the calculation and comparison and thus become the victim of the attack [12].

4. Route-based packet filtering: This mechanism extends the feature of ingress filtering to the routers at the core of the Internet. The traffic on each link in the core of the Internet commonly originates from a limited set of source IP addresses. if an unexpected source IP address appears in a packet on a link, then that packet will be filtered by assuming that the source address has been spoofed[13]. However, this mechanism is unsuccessful against DDoS attacks. if attackers use genuine IP addresses instead of spoofed ones that are not going to be filtered.

5. Active Internet Traffic Filtering (AITF): AITF is a hybrid DDOS defense mechanism that can block a million-flow attack within seconds. AITF allows a receiver to contact misbehaving sources. The receiver then asks them to stop sending packets. Each of the sources that have been asked to stop is policed by its ISP, which ensures their compliance [14].

Each ISP that hosts misbehaving sources must either support the AITF mechanism (i.e., accept to police its misbehaving clients) or risk losing all of its access to the complaining receiver.

AITF shows that the network-layer of the Internet can provide an effective, scalable, and incrementally deployable solution to bandwidth-flooding attacks.

AITF has several deployment problems since it relies on the routers, which are in the middle of the network to perform the actual filtering. It also depends on various IP route records to determine where packets come from [14].

6. StopIt]: is a hybrid filter-based DDoS defense mechanism. StopIt allows each receiver to install a network filter that will block the undesirable traffic it receives. It uses Passport as its secure source authentication system to prevent source address spoofing. Its design employs a novel closed-control and open-service architecture [15]. This will help to fight against strategic attacks that aim to
i) prevent filters from being installed and
ii) to provide thee StopIt service to any host on the Internet.
StopIt mechanism is also susceptible to the attacks in which attackers flood the routers and StopIt servers with filter requests and packet floods. To prevent these attacks, the StopIt framework must guarantee that a router or a StopIt server only receives StopIt requests from local nodes. In doing so, network administrators must manually configure the routers and StopIt requests with the list of hosts, routers, and other StopIt servers. Such manual configuration for hundreds of thousands of nodes is a burdensome task. Furthermore, StopIt needs complex verification/authentication mechanisms. It also needs misbehaving StopIt server detection mechanisms to be implemented in both hosts and routers. This requirement makes it a challenging mechanism to deploy and manage in practice [15].

7. Path identifier: Path identifier (Pi) method filters the attacker's packets based on the path identified by this identifier [36]. It is a deterministic method where each packet is marked with an identifier. The packets that travel the same path contain the same identifier. Thus, if the victim can identify a packet traveling from the attacker path, it can filter all the successive packets sent by the attacker [16].

However, this mechanism works fine, if half of the routers get involved to mark the packets. As it works with only a small-sized Identification field to distinguish the path, there remains the chance that different paths will show the same path information. Thus, it increases the chance of false-positive and false-negative results. Later, Yaar et al.[16] have proposed a better version of the Pi technique named StackPi. This method improves Pi's performance in terms of incremental deployment. Also, the improved filtering mechanism is capable of identifying malicious flows based on just a single packet.

8. PacketScore: It is a proactive filtering technique that uses Bayes' theorem to compute the conditional legitimate probability (CLP). This CLP is used to define the probability of a legitimate packet based on the baseline profile value and the attribute value of a packet. The packet filtering works based on this CLP value and a dynamic threshold. As the filtering takes into account the statistical analysis, this method works well for new attack signatures as well as non-spoofed attack traffics.

However, this method needs a huge volume of storage to deal with the growing number of attack attributes [17].

D. Conclusion And Future Work

In this paper, we have presented a comprehensive classification of various DDOS attacks along with different packet filtering mechanisms. While the filtering techniques discussed in this paper does absolutely nothing to protect against flooding attacks that originate from valid IP addresses. Most of these filtering techniques will prohibit an attacker within the originating network from launching an attack of this nature using forged source addresses that do not conform to filtering rules. All providers of Internet connectivity are urged to implement filtering described in this paper to forbid attackers from using forged source IP addresses. These IP addresses do not reside within a range of legitimately advertised prefixes. In other words, if an ISP is aggregating routing messages for several downstream networks, stringent traffic filtering should be used to prohibit traffic which claims to have originated from outside of these aggregated messages. An additional benefit of implementing this type of filtering is that it empowers the originator to be easily traced to its true source since the attacker would have to use a valid, and legitimately reachable, source address. The packet filtering techniques discussed in this paper offer better security but can never totally remove the threat of DDoS attacks. These techniques are always vulnerable to fresh attacks for which signatures and patches do not exist in the database. Although these techniques can be effective for controlled traffic loads, it needs to be further assessed in a real network environment. This research area could provide significant information and techniques that can be used in the identification and filtering of DDOS attacks.

REFERENCES:

[1] S. T. Zargar, J. Joshi, and D. Tipper, "A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks," *IEEE Communications Surveys and Tutorials*, vol. 15, no. 4, pp. 2046–2069, 2013.

[2] Mr. Amit Bhanot "Implementing network security policies: packet filtering mechanism "International Journal of Emerging Trends & Technology in Computer Science(IJETTCS) Volume 2, Issue 3, May–June 2013. ISSN 2278-6856.

[3] B. Todd, Distributed Denial of Service Attacks, Feb. 18,2000,[online]http://www.linuxsecurity.com/resource files/intrusion detection/ddos–whitepaper.html.

[4] U. Tariq, M. Hong, and K. Lhee, A Comprehensive Categorization of DDoS Attack and DDoS Defense Techniques, ADMA LNAI 4093, pp.1025-1036, 2006.

[5] RioRey, Inc. 2009-2012, RioRey Taxonomy of DDoS Attacks, RioRey Taxonomy Rev 2.3 2012, 2012. [online]http://www.riorey.com/xresources/2012/Rio Rey Taxonomy DDoS Attacks 2012.pdf

[6] S. M. Specht and R. B. Lee Distributed Denial of Service: Taxonomies of Attacks, Tools, and Countermeasures, in Proc. Of the 17th International Conference on Parallel and Distributed Computing Systems, pp.543-550, 2004.

[7] C. Douligeris, and A. Mitrokotsa, DDoS attacks and defense mechanisms: classification and state-of-the-art, Computer Networks, Vol.44, No. 5, pp. 643-666, April 2004

[8] J. Mirkovic and P. Reiher, "A taxonomy of DDoS attack and DDoS defense mechanisms," ACM SIGCOMM Computer Communications Review, vol. 34, no. 2, pp. 39-53, April 2004.

[9] A. Rai and R. K. Challa, "Survey on recent DDoS mitigation techniques and comparative analysis," in *Proceedings of 2016Second International Conference on Computational Intelligence & Communication Technology (CICT)*, pp. 96–101, Ghaziabad, India, February 2016.

[10] P. Ferguson, and D. Senie, Network Ingress Filtering: Defeating Denial of Service Attacks that employ IP source address spoofing, Internet RFC 2827, 2000 [11] List of root servers https://www.iana.org/domains/root/servers.

[11] T. Peng, C. Leckie, and K. Ramamohanarao, Protection from distributed denial of service attacks using history-based IP filtering, ICC '03. May, Vol.1, pp: 482- 486, 2003.

[12] H. Wang, C. Jin, and K. G. Shin, Defense Against Spoofed IP Traffic Using Hop-Count Filtering, IEEE/ACM Trans. On Networking, vol. 15, no. 1, pp.40-53, February 2007.

[13] K. Park, and H. Lee, On the Effectiveness of Route-Based Packet Filtering for Distributed DoS Attack Prevention in Power-Law Internets, in Proc. ACM SIGCOMM, August 2001.

[14] K. Argyraki, and D. R. Cheriton, Scalable network-layer defense against internet bandwidth-flooding attacks, in IEEE/ACM Trans. Netw., 17(4), pp. 1284-1297, August 2009

[15] X. Liu, X. Yang, and Y. Lu, To filter or to authorize: network layer DoS defense against multimillion-node botnets, in Proc. of the ACM SIGCOMM conference on Data communication (SIGCOMM '08), NY, USA, pp. 195-206, 2008.

[16] Yaar A, Perrig A, and Song D. Pi: a path identification mechanism to defend against DDoS attacks. In: Proceedings of the 2003 symposium on security and privacy, Berkeley, CA, 11–14 May 2003, pp.93–107. New York: IEEE.

[17] Kim Y, Lau WC, Chuah MC, et al. Packet Score: a statistics-based packet filtering scheme against distributed denial-of-service attacks. IEEE T Depend Secure 2006; 3(2): 141–155.