www.irbas.academyirmbr.com
International Review of Basic and Applied Sciences
November 2018
Vol. 6 Issue.11

DDoS Defence Mechanisms and Challenges

AMER TAJ
University of Engineering & Technology, Peshawar
Email: amertaj@uetpeshawar.edu.pk

Dr. SADEEQ JAN
University of Engineering & Technology, Peshawar
Email: sadeeqjan@uetpeshawar.edu.pk

MUHAMMAD IMRAN KHAN KHALIL
University of Engineering & Technology, Peshawar
Email: imrankhalil@uetpeshawar.edu.pk

Abstract

Hyper Text Transfer Protocol (HTTP) is the standard protocol used for communication on the Internet. The simplistic client-server paradigm of HTTP attracts various forms of DDoS attacks. One such attack is the slow HTTP DDoS attack, which exploits the packet structure of HTTP request to disrupt the services at a given server. These attacks are hard to detect due to their comparable traffic patterns to that of the normal network traffic. This paper identifies prevalent techniques to detect and mitigate Slow HTTP DDoS attacks that are prevalent in literature. We highlight the main features of the detection techniques and present some challenges at the end for further research in the field.

Keywords: *Defense, Mechanism, Challenges.*

Introduction

Hyper Text Transfer Protocol (HTTP) is a fundamental protocol that defines the actions a web server and a browser must take to transmit/receive over the World Wide Web (WWW). HTTP defines message formats, methods such as GET, POST, PUT, DELETE etc., and various processing attributes (Lee, Fielding, & Frystyk, 1996). HTTP is at the application layer of the protocol stack and it works as a request/response protocol. A client sends requests (HTTP requests) for the resources and the server responds (HTTP response) by providing the requested resources. A server is usually capable of receiving multiple requests from multiple clients; each request received on a different connection. After sending a HTTP response, a server closes the connection. This simplistic design of HTTP attracts various forms of attacks on the web servers. According to (Mirkovic & Reiher, 2004), among the major type of DDoS attacks, HTTP DDoS are one of the most frequent attacks that target web applications, as shown in Figure 1.1.

For instance, Distributed Denial of Service (DDoS) attack compromises multiple distributed systems to launch an attack on a target system such as a web server (Mirkovic & Reiher, 2004). The aim of such attacks is to exhaust the limited resources (i.e., connections) at a server One of the characteristics of DDoS is its asymmetrical traffic pattern i.e., inflated traffic rate at the target system. Therefore, application level detection mechanisms are deployed at potential targets to monitor traffic patterns and to block the DDoS attack as and when it happens (Zargar, Joshi, & Tipper, 2013).

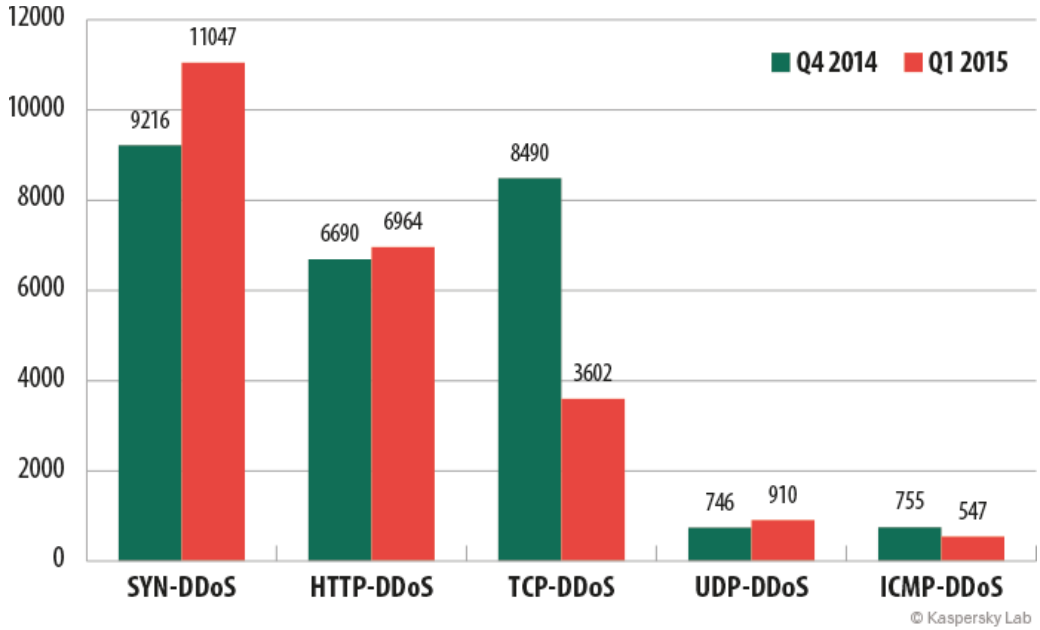

Figure 1.1: Statistics of the most common DDoS attacks in 2014-15

In literature various approaches exist that address the DDoS attack prevention. These approaches can be deployed near the source of the attack, at the destination, at the network routers etc. For instance, Speak Up (Walfish, Vutukuru, Balakrishnan, Karger, & Shenker, 2006) is an intuitive approach that encourages the users to increase transmit rate. Only the legitimate users respond by increasing transmit rate. This is because malicious users have a higher transmit rate during the attack. Therefore, response to the speak up approach identifies malicious users.

However, although there exists a plethora of detection mechanisms for the HTTP DDoS detection, little is known about the effective mechanisms to detect a more sophisticated slow HTTP DDoS attack (Cambiaso, Papaleo, & Aiello, 2015) (Cambiaso, Papaleo, & Aiello, 2012). This attack exploits the processing attributes of HTTP. Observe that, every HTTP request message has a sequence of empty lines at the end of the message that helps the server to confirm a completed HTTP request. In this attack, the attacker sends HTTP requests without appending the sequence of empty lines at the end of the message. As a result, the server waits for the completion of HTTP requests. This also means that the connection resources are kept alive and genuine HTTP requests are denied access to the resources. Eventually, with increasing number of distributed compromised systems, the services at the target system become unavailable.

Problem Statement

The detection of Slow HTTP DDoS attacks has received little attention in literature. Unlike DDoS attacks, wherein the attackers proliferate the transmission rate of HTTP requests, the slow HTTP attacks have comparable traffic patterns to that of the normal traffic. This feature makes detection of Slow HTTP DDoS attack a challenging task. This implies that existing DDoS detection mechanisms cannot be readily applied for the detection of Slow HTTP DDoS attacks. It is also worth mentioning that detection of the slow HTTP attack is difficult to detect within the network because network devices do not work at the application layer. It follows that the detection of Slow HTTP DDoS attack at the destination is more desirable.

In the following sections, we look at some of the defense strategies that exist in literature.

Techniques to Detect and Mitigate DDoS Attacks

In literature, the DDoS detection approaches can be divided into four different categories i.e., 1) Source-based Mechanisms, 2) Destination-based Mechanisms, 3) Network-based Mechanisms, and 4) Hybrid Mechanisms.

Source-based Mechanisms

These mechanisms are deployed very close to source of attack which helps to save other network clients from creating a chain reaction of DDOS flooding attacks. These mechanisms can either be implemented at the access routers of the Autonomous System that connects the edge routers of the source or can also be deployed directly at the border routers of the source network (Criscuolo, 2000). To protect SBMs from DDOS flooding attacks many SBMs developed.

Egress/Ingress Filtering

At the sources border routers (Ferguson & Senie, 2000). At present IP protocol allows many hosts at source to make changes in source IP addresses in packets. Packets with imitated IP addresses create a problem in detecting the DDOS flooding attacks. Dupes cannot differentiate a legitimate packet from attack packet using source addresses (Kent & Atkinson, 1998). IPSec protocol can handle this situation by authentication of the IP packets for their source addresses. However, due to its heavy overhead it is not in use by most of the ISPs (Kent & Atkinson, 1998). These mechanisms are developed to detect the imitated IP addresses packets from the source border routers based on authentic IP address range. However, the imitated IP addresses cannot be detected if it comes under the authentic addresses range. For example, if host A of network J sends out the packet with host B source address. This is an authentic address in J network and filtering will never sense the imitated packet. Moreover, filtering for mobile IP users their packets will have to go through tunneling to avoid the filtering mechanisms. Although attackers can still attack using botnets using genuine IP addresses.

D-WARD

Mirkovic, Prier & Reiher, (2002): scheme is used to detect the DDOS flooding attack by monitoring the inbound and outbound traffic of a source network and compare it with the predefined traffic models that show normal flow. This mechanism tries to stop the attack traffic from the edge of source network. Moreover, attack packets are recognized and filtered in case if they do not match the normal flow model. For example, in transmission control protocol every packet is acknowledged by the destination point. The numbers of packets send and received by TCP protocol is calculated and its ratio is predefined in normal flow traffic. D-WARD can be responsible to generate filtering rules at the source which cause systems to consume more space and CPU cycles as compared to some Network based mechanisms. Moreover, attackers who control the traffic within a normal range can easily bypass D-WARD (Mirkovic, Prier & Reihe, 1998).

MANAnets Reverse Firewall

This mechanism works opposite to the conventional firewall and protect the system from other network packets. To protect the external network from flooding attacks and control the rate of forwarding packets is done through reverse firewall. New packets must be allowed to be send for the new conversation that are not thee reply packets, but they must be in low rate. The most important disadvantage of a reverse firewall is that it is controlled manually by the administrator, so its configuration cannot be changed dynamically according to the situation created. On top of all it is of no benefit for source network as it protects the outside not the within network (John & Sivakumar, 2009).

Hop Count Filtering

Wang, Jin & Shin, (2007) is a destination-based detection mechanism. When the target system is not under attack, the server records the source logical addresses (IPs) and their corresponding hop counts. During the attack, the attacked node inspects the hop counts of incoming packets for inconsistencies. Subsequently, blocking the spoofed packets.

Destination-based Mechanisms (DBMs)

DBMs detect and response through destination of attach commonly called victims. Different types of DBMS work from the border or access routers of the autonomous system lies. Some of the important DBMs are as follows:

IP Traceback

John & Sivakumar, (2009)*:* This mechanism molded packets from original source instead imitated logical addresses. There are various mechanisms proposed of this kind and all of them can be categorize into two (Chen, Park, & Marchany, 2006): Packet marking and Link testing. In Packet marking routers in the path to victim mark packets so the victim identify the attacking traffic and differentiate it with the authorized packets (Duwairi & Manimaran, 2006)(Savage, Wetherall, Karlin & Anderson, 2000) This need to store entire path in IP identification field which requires some coding schemes. However sometimes these mechanisms unable to mark properly so untrue positive rates are still high in these mechanisms and considering legitimate packets. The LTMs (Link Testing Mechanisms) is the next category in which traceback processing starts from the closest router to the node that has been attacked and tests its upstream links finding the link which is used to carry attacker's traffic. Almost all traceback mechanisms have some challenges like number of routers that supports traceback. Attackers can also create traceback messages and send to victim, so some form of confirmation is required. Moreover traceback mechanisms have heavy computational and network overheads (Burch & Cheswick, 2000) (Glave, 1998).

Management Information Base (Joao & Cabrera, 2001): This mechanism helps victim nodes for identification of DDOS attack. ICMP, UDP and TCP packets are mapped which create abnormalities to the statistical patterns which can be easily caught if MIB is deployed properly during DDOS attack (Jalili & Imani, 2005) (Li, Liu & Long, 2004). MIB is in initial stages of deployment in real network environment so its efficiency is still in evaluation stage.

Packet marking and filtering mechanisms (Peng, Leckie & Ramamohanarao, 2003)*:* These mechanisms focus on the marking of authentication of packets at every router with the path to destination which helps victim border routers to identify the attack routers and filter them from legitimate traffic (Wang, Jin & Shin, 2007) (Yaar, Perrig & Song, 2003). Various destination-based packet filtering mechanisms are proposed so far.

History based IP filtering (Peng, Leckie & Ramamohanarao, 2003)*:* by implementing this procedure a victim can filter a flooding attack traffic according to the values they maintained in database during normal trafficking. Usually a target destination keeps track of IP addresses that visits frequently and during attack target destination admits only those packets whose source IP address is in IP database.

Hop count filtering (HCF) (Wang, Jin & Shin, 2007): In HCF mechanism hops count information and the source IP address information are stored at the destination side in a table form in peace time. When the attack is occurred, a destination analyzes the incoming packets logical addresses and their corresponding hops that help target host to differentiate between the spoofed and legitimate packets.

Network-based Mechanisms

These mechanisms are usually deployed on Autonomous System routers. These mechanisms detect attack traffic and give response at intermediate networks (Chan, 2006). Here are some of the NBMs against DDOS attack are:

Route based packet filtering (Park & Lee, 2001): This mechanism is the extension of ingress filtering. All the traffic on the links of network are commonly generated from a source addresses. So whenever a new or unexpected source address appears on a link it is considered to be imitated source address and that packet can be filtered from legitimate traffic. This mechanism will fail when attackers use a genuine IP address as a source address.

Detecting and filtering malicious routers (Mizrak, Savage & Marzullo, 2008): Routers in networks are mostly targeted as they can be used strategically to empower DDOS attack. Several specialized protocols are proposed to detect malicious routers involved in traffic forwarding between genuine routers. For example, watchers (Bradley, Cheung, Puketza, Mukherjee, & Olsson, 1998) detect malicious routers by misrouting, absorbing and discarding packets. It uses the conservation of flow mechanism to analyze the traffic flow between neighbors and endpoints. Watchers can only detect those routers who has been compromised but it cannot respond to malicious host in a network (Hughes, Aura, & Bishop, 2000).

Bayesian Inference Model

It has been employed to find the trustworthiness of an access router with regards to forwarding packets without changing their source IP addresses. In this mechanism the trust values are examined by a judge (router) that samples all traffic being forwarded by the access routers (Gonzalez, Anwar & Joshi, 2011). Implementing trust calculations and decision making between the routers in order to detect malicious routers trying to forward packets within a network.

Hybrid Mechanisms

In majority of the DDOS defense mechanisms, detection and response is mostly done centrally either by each deployment point e.g., source based or destination-based mechanism, or by some accountable points within the group of deployment points like in NBMs. Therefore, we call these defense mechanisms as centralized defense mechanisms. In opposition to those hybrid defense mechanisms is distributed defense mechanism as its component is employed on different locations and the deployment points have cooperation between each other to detect an attack which was not present in centralized mechanisms. For example, that detection was occurred at victim side and its response will be distributed on other nodes of network to avoid more damage. Some of the hybrid distributed defense mechanism is as follow:

Hybrid Packet Marking and throttling/filtering Mechanisms

All the previously discussed detection and filtering mechanisms shows that the detection unit and filtering unit is placed at same place. Where in hybrid packet marking and filtering the detection module is usually place at victim site and filtering is done near attack source. In some of these mechanisms a router throttle (filter) is installed at upstream router several hops away as to lower the forwarding rate of packets destined to the victim address. These mechanisms only lower the rate of flow of malevolent packets not the valid traffic.

COSSACK

Papadopoulos, Lindell, Mehringer, Hussain & Govindan, (2002) this defense mechanism is deployed on all the border routers of the edge networks and with the core software installed called watch dog. This defense

mechanism is based on some assumptions. 1) The border routers are implementing ingress/egress filtering mechanisms. 2) Border routers can provide good defense against IP spoofing using the ingress/egress filtering. The final assumption is the capability of border routers to strain packets based on signature and connection availability between watchdogs. However, COSSACK is unable to defend attacks from standard networks who do not implement COSSACK.

Active Internet Traffic Filtering (AITF) as a filter-based datagram mechanism (Argyraki & Cheriton, 2009)*:* All the capability-based mechanisms allow the receiver to stop accepting all traffic except the traffic that is originated from the established network layer connections. Alternatively, a datagram (AITF) mechanism allows all traffic and denies the access to those packets which have been identified undesirable. AITF enable the receiver to contact the attacking source and ask them to stop sending the packets. The attacking source is on radar by its own ISP which ensures their compliances. When the receiver is popular access point than each ISP hosting misbehaving source must follow AITF mechanism otherwise will lose all the compliances from receiver. AITF has several problems as well like it is depended on routers which are in the center of the network and performs the real filtering. It also depends on various old route records to determine the packets originality and authenticity.

Research Directions

1. The rise of Internet of Things (IoTs) (Shah, S. A. A., Ahmed & Ahmed, Ejaz et. al, 2018), there will be more devices capable of communication that ever. While this opens up plethora of business opportunities and novel applications, it also raises concerns about security. In particular, IoT devices have potential to be turned into botnets and launch DDoS attacks such as Slow HTTP DDoS. This calls for novel proposals to secure IoT paradigm before its widespread adoption.
2. Software Defined Networks (SDNs) are one of the building blocks of 5G enabled communications (Shah et. al, 2018). With a single controller to look after all the switches in the forwarding plane, SDN is a perfect candidate for DDoS. A successful attack on the controller could halt the forwarding behavior in the forwarding plane. Currently, there are lack of proposals to protect the controller against the Slow HTTP DDoS.

Conclusions

This paper has presented the prevalent techniques in the literature to protect systems from the DDoS attacks and Slow HTTP DDoS attacks. We have highlighted the key categories of detection techniques and presented the key features of various techniques. The destination based detection mechanisms allow the attack to reach the target before it is detected. The source based defense mechanisms are the most difficult to propose due to the difficulty of identifying source of attacks. The network based attacks presents a unique challenge of suspicious traffic identification at the network devices. It follows that the most effective techniques are the hybrid approaches that can be designed to maximize the chances of detection.

Acknowledgment

This work is supported by HEC funded project “National Center in Cyber Security-UETP” University of Engineering & Technology, Peshawar, Pakistan.

References

Abdelsayed S., Glimsholt D., Leckie C., Ryan S., and Shami S. (2003). An efficient filter for denial-of-service bandwidth attacks, in Proc. of the 46th IEEE Global Telecommunications Conference (GLOBECOM03), 1353-1357.

Al–Duwairi B., and Manimaran G. (2006). Novel Hybrid Schemes Employing Packet Marking and Logging for IP Traceback, IEEE Trans. Parallel and Distributed Systems, 17(5) 403- 418.

Al–Duwairi B., and Manimaran G. (2006). Novel Hybrid Schemes Employing Packet Marking and Logging for IP Traceback, IEEE Trans. Parallel Distrib. Syst., 17(5), 403- 418.

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

Berners-Lee, T., Fielding, R., & Frystyk, H. (1996). Hypertext transfer protocol--HTTP/1.0 (No. RFC 1945).

Bradley K. A., Cheung S., Puketza N., Mukherjee B., and Olsson R. A. (1998). Detecting Disruptive Routers: A Distributed Network Monitoring Approach, in Proc. 1998 IEEE Symposium on Security and Privacy.

Burch H., and Cheswick B. (2000). Tracing anonymous packets to their approximate source, in Proc. USENIX Large Installation Systems Administration Conference, pages 319–327, New Orleans, USA.

Cambiaso, E., Papaleo, G., & Aiello, M. (2012). Taxonomy of slow DoS attacks to web applications. In International Conference on Security in Computer Networks and Distributed Systems. Springer, Berlin, Heidelberg, 195-204.

Chan E. Y. K. (2006). Intrusion Detection Routers: Design, Implementation and Evaluation Using an Experimental Testbed, IEEE J. Sel. Areas Commun., 24(10), 1889 - 1900.

Chen R., Park J. M., and Marchany R. (2006). RIM: Router interface marking for IP traceback, in IEEE Global Telecommunications Conference (GLOBECOM'06).

Chen R., Park J. M., and Marchany R. (2006). RIM: Router interface marking for IP traceback, in IEEE Global Telecommunications Conference (GLOBECOM'06).

Criscuolo P. J. (2000). Distributed Denial of Service, Tribe Flood Network 2000, and Stacheldraht CIAC-2319, Department of Energy Computer Incident Advisory Capability (CIAC), UCRL-ID-136939, Rev. 1., Lawrence Livermore National Laboratory.

Farina, P., Cambiaso, E., Papaleo, G., & Aiello, M. (2015). Understanding ddos attacks from mobile devices. In Future Internet of Things and Cloud (FiCloud) 3rd International Conference IEEE, 614-619.

Ferguson P., and Senie D. (2000). Network Ingress Filtering: Defeating Denial of Service Attacks that employ IP source address spoofing, Internet RFC 2827.

Gil T. M., and Poleto M. (2001). MULTOPS: a data-structure for bandwidth attack detection, in Proc. of 10th Usenix Security Symposium, Washington, DC, 23-38.

Glave J. (1998). Smurfing cripples ISPs, in Wired TechnologyNews, [online] http://www.wired.com/news/news/technology/story/9506.html

Gonzalez J. M., Anwar M., and Joshi J. B. D. (2011). A trust-based approach against IP-spoofing attacks, in Proc. IEEE PST, 63-70.

Hughes J. R., Aura T., and Bishop M. (2000). Using Conservation of Flow as a Security Mechanism in Network Protocols, in Proc. 2000 IEEE Symposium on Security and Privacy.

Jalili R., and ImaniMehr F. (2005). Detection of Distributed Denial of Service Attacks Using Statistical Pre-Prossesor and Unsupervised Neural Network, ISPEC,Springer-Verlag Berlin Heidelberg, 192-203.

Joao B., and Cabrera D. (2001) Proactive Detection of Distributed Denial of Service Attacks Using MIB Traffic Variables — A Feasibility Study, Integrated Network Management Proceedings, 609-622.

John A., and Sivakumar T. (2009). DDoS: Survey of Traceback Methods, International Journal of Recent Trends in Engineering ACEEE (Association of Computer Electronics & Electrical Engineers), 1(2).

Kent S., and Atkinson R. (1998). IP Authentication Header, IETF, RFC 2402.

Kent S., and Atkinson R. (1998). Security Architecture for the Internet Protocol, IETF, RFC 2401.

Li M., Liu J., and Long D. (2004). Probability Principle of Reliable Approach to detect signs of DDOSFlood Attacks, PDCAT, Springer-Verlag Berlin Heidelberg, 596-599.

Mananet, Reverse Firewall, [online] http://www.cs3–inc.com/pubs/Reverse FireWall.eps

Mirkovic J., Prier G., and Reihe P. (2003). Source-End DDoS Defense, in Proc. 2nd IEEE International Symposium on Network Computing and Applications.

Mirkovic J., Prier G., and Reiher P. (2002). Attacking DDoS at the Source, in Proc. 10th IEEE International Conference on Network Protocols (ICNP '02), Washington DC, USA.

Mirkovic, J., & Reiher, P. (2004). A taxonomy of DDoS attack and DDoS defense mechanisms. ACM SIGCOMM Computer Communication Review, 34(2), 39-53.

Mizrak A. T., Savage S., and Marzullo K. (2008). Detecting compromised routers via packet forwarding behavior, IEEE Network, 34-39.

Papadopoulos C., Lindell R., Mehringer J., Hussain A., and Govindan R. (2003). Cossack: Coordinated Suppression of Simultaneous Attacks, in Proc. DARPA Information Survivability Conference and Exposition, 1(4), 12-13.

Park K., and Lee H. (2001). On the effectiveness of probabilistic packet marking for IP traceback under denial of service attack, in Proc. IEEE INFOCOM 2001, 338-347.

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

Peng T., Leckie C., and Ramamohanarao K. (2003). Protection from distributed denial of service attacks using history-based IP filtering, ICC '03. 1(3), 482- 486.

Savage S., Wetherall D., Karlin A., and Anderson T. (2000). Practical Network Support for IP Traceback, Technical report, Department of Computer Science and Engineering, University of Washington.

Savage S., Wetherall D., Karlin A., and Anderson T. (2000). Practical Network Support for IP Traceback, Technical report, Department of Computer Science and Engineering, University of Washington.

Shah, S. A. A., Ahmed, E., Imran, M., & Zeadally, S. (2018). 5g for vehicular communications. IEEE Communications Magazine, 56(1), 111-117.

Shah, S. A. A., Ahmed, E., Rodrigues, J. J., Ali, I., & Noor, R. M. (2018). Shapely Value Perspective on Adapting Transmit Power for Periodic Vehicular Communications. IEEE Transactions on Intelligent Transportation Systems, 19(3), 977-986.

Walfish M., Vutukuru M., Balakrishnan H., Karger D., and Shenker S. (2006). DDoS defense by offense, SIGCOMM Computer Communications Review, 36(4), 303-314.

Wang H., Jin C., and Shin K. G. (2007) Defense Against Spoofed IP Traffic Using Hop-Count Filtering, IEEE/ACM Trans. On Networking, 15(1), 40-53.

Wang H., Jin C., and Shin K. G. (2007). Defense Against Spoofed IP Traffic Using Hop-Count Filtering, IEEE/ACM Trans. Netw., 15(1), 40-53.

Yaar A., Perrig A., and Song D. (2003). Pi: A Path Identification Mechanism to Defend against DDoS Attacks, in IEEE Symposium on Security and Privacy, 93-99.

Zargar, S. T., Joshi, J., & Tipper, D. (2013). A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks. IEEE communications surveys & tutorials, 15(4), 2046-2069.