DDoS Prevention Techniques

Gökhan Dalkılıç
Dokuz Eylül University
106 PUBLICATIONS **798** CITATIONS

Mehmet Hilal Ozcanhan
Dokuz Eylül University
62 PUBLICATIONS **192** CITATIONS

Distributed Denial of Service Prevention Techniques

Oğuz Yarımtepe
Computer Engineering Department
Dokuz Eylül University
İzmir, Turkey
oguzyarimtepe@gmail.com

Gökhan Dalkılıç, Mehmet Hilal Özcanhan
Computer Engineering Department
Dokuz Eylül University
Izmir, Turkey
dalkilic@cs.deu.edu.tr, hozcanhan @cs.deu.edu.tr

***Abstract*—Distributed Denial of Service (DDoS) attacks keep their threatening power over the Internet world. The attackers focus on application levels and they are able to attack with higher bandwidths. It is important to know the nature of Distributed Denial of Service attacks to develop new prevention techniques. As in the other fields of security, it is an important subject to develop proactive prevention methods. This paper cover the recently published prevention methods. In addition, it focuses on the new era that is the cloud systems and how they are protected against DDoS attacks.**

Keywords— DoS; DDoS; DDoS attacks; DDoS prevention; cloud security

I. Introduction

Denial of Service (DoS) attacks are service mitigation attacks that aim to interrupt the communication between a machine and the user [1]. Starting from late eighties, DoS tools became easy to use to perform attacks that resulted an increase in DoS attacks, especially at the early 2000s. By flooding the target, it is aimed to consume computational resources such as CPU, RAM or bandwidth. The result is unavailability at the services [2]. Nowadays, DoS attacks are being used for distributed mitigation that is called Distributed DoS (DDoS) attacks. The aim is still the same, disrupting the legitimate user. Enormous amount of packet floods make the services unavailable for legitimate users [3].

One of the first DDoS attacks is detected as ping floods in 1989; ping.c source code lets the users to use the -f (flood) parameter [4]. It was in February 2000, 15 year old “Mafiaboy”, Michael Calce launched DDoS attacks on multiple sites, including Yahoo, Fifa, Amazon, eBay and CNN [5, 6]. Attack volumes are increased with the increase at the speed of the Internet. In 2001, it is started to be seen as Gbps attacks; a 3 Gbps attack is occurred to Efnet [4]. The scope of DDoS attack is expanded to root DNS servers, 13 of them, are subjected to serious DDoS attack. It is reported that the type of the attack was “Smurf” and the volume of the attack was 900 Mbps [6]. In 2005, attackers realized that DDoS attacks can be used as a money source for them. Jaxx.de which is a Hamburg based gambling site was forced to pay 40,000 euros for stopping an ongoing DDoS on the site [4]. In 2008, Anonymous group appeared in the DDoS scene with its hactivist move against the Scientologists for their try to remove a Tom Cruise video from Youtube. Anonymous group used LOIC, which is an open source tool, to take down some popular web sites. While approaching to 2010, the motivation behind the DDoS attacks is changed from money to political events and ideological issues. Wikileaks encountered with a serious attack. Stuxnet worm is detected in June 2010, which brings the cyber terrorism to the front. After 2012, it is started to be observed custom tools and application level attacks. Banks in the U.S, like Izz ad-Din al-Qassam, are affected by DDoS attacks. At the end of the 2013, it is recorded that two cyber-attacks are exceeded the 150 Gbps barrier [5]. In 2014, 111 attacks over 100 Gbps occurred [4].

Nowadays, botnets or zombie machines are becoming the new threats. These are infected distributed machines communicating via master servers or distributedly, using protocols like Internet Relay Chat (IRC), Hypertext Transfer Protocol (HTTP), Instant Messaging (IM) or Peer to Peer (P2P), for attacking a target. Besides DDoS attacks, botnets are also used for spamming, malwares, espionage and hosting malicious applications & activities. Botnets still remain as a large-scale problem of the Internet [7]. As stated in [8], the main problem with DDoS is its distributed structure. There are many zombie machines geographically distributed and even their attack is small, the overall attack becomes a huge one. The second problem is the spoofed IPs that they use.

Below is a recent screenshot from the digitalattackmap.com site that displays the world wide DDoS attacks. The web site displays the real-time attacks collected with the collaboration of Google and Arbour Networks. The attacks can be from one country to another or inside the country. There are also attacks with unknown destination or sources. The volume of the attacks vary from 1Gbps to 25 Gbps. Some attacks are TCP connection attacks aiming to consume the connection pool at infrastructure devices like load-balancers, firewalls and application server. Some are volumentric attacks that aim to consume bandwidth. Some can be seen as application level attacks that are targeting application servers with even low traffic rate.

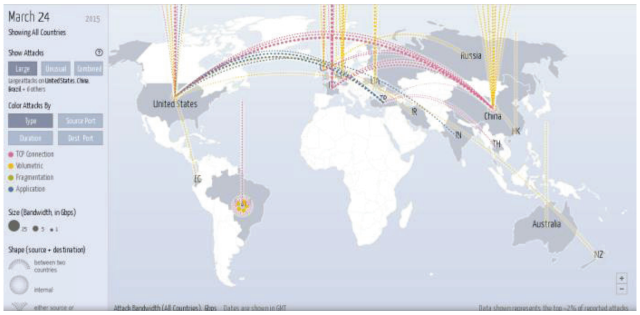

Fig. 1 Digital Attack Map

In section 2, attack types are explained. Section 3 is about the prevention methods. Section 4 details the attacks on cloud systems, and the last section is the conclusion.

II. DDoS Attack Types

According to the security reports [10], recent DDoS attacks target DNS and web applications. Layer 3 & 4 attacks cover nearly 75% of the attacks. More than half of them are SYN flood and HTTP Get attacks [11]. Akamai report supports the increase of the attacks to the web applications; it is stated as there is a significant increase at the attacks targeting port 80 and 443 [9]. Since the tendency at the DDoS attacks are floods, DNS and web applications, we analyze the attack types related to them.

A. Network/transport-level Flood Attacks

Flood attacks are categorized into two main categories as network/transport-level and application level attacks [12]. And also, network attacks are divided into four categories.

1. First one covers the spoofed and non-spoofed attacks, like UDP, ICMP and DNS floods. Since UDP is sessionless, UDP flooding aims flooding random ports of the remote host with numerous UDP packets. As a result of this attack, the host repeatedly checks for the application listening on that port and replies with ICMP Destination Unreachable. The attack consumes the host resources and may result in inaccessibility [13]. ICMP attacks act like UDP flooding by sending ICMP Echo Request (ping) packets as fast as possible; they are aimed to consume both inbound and outbound traffic.

2. Second type of network attacks is the usage of the protocol weaknesses that is basically TCP stack attacks like TCP SYN flood, TCP SYN-ACK, RST/FIN flood, etc. attacks. At the TCP SYN-ACK attack, the aim is to fill the target's backlog queue. When a SYN packet is received, a SYN-ACK is responded from the target side. Until SYN-ACK packet is responded by the client side, a half open connection is alive for 75 seconds. For half open connections, operating system maintains a backlog queue. When the attacker spoofed the IP address and starts sending SYN packets, there won't be SYN ACK responses for the real sender to complete the three way hand shake with ACK packet. This type of attack will cause the backlog queue to fill and new connection requests will be dropped [14].

3. Third one covers the smurf and fragle attacks that are using the answers of the protocol (e.g. ICMP) requests sent to the victim from different machines and causing the victim's resources consumed.

4. The last one works like smurf attacks, but uses the power of the returned answer's size. They are known as amplification attacks and generated by using small requests, but the resulting responses are big.

B. Application-level Flood Attacks

DNS and WEB attacks are application level attacks. They are generally amplification attacks or flood attacks. More details are covered under the related title.

1) DNS Attacks: Main problem with DNS is its use of UDP packets that pioneers extreme vulnerability to spoofing. DNS queries and responses use UDP packets that validate the source address [15]. Recursive name servers are used with the spoofed IP addresses to generate high volume responses to several networks, e.g. a 50 bytes request leads to 500 bytes response. This attack causes exhaustion both at the DNS server and victim side. The outbound bandwidth of the amplifying DNS server and the inbound bandwidth of the victim server are consumed. Amplification gives an attacker the power to consume a victim's bandwidth even the victim's bandwidth is 10 times bigger than the attacker's bandwidth [15]. It is reported that 10Gbps attack is generated by using 140,000 exploited name servers [16]. An amplification factor (AF) is defined as:

$$AF = \text{size of (response)} / \text{size of (request)} \qquad (1)$$

It is stated that the more AF, the more bandwidth and resource consumption at the target side. The attacker sends a query for valid record to a recursive name server with a spoofed IP address that belongs to the attacked network. The response is sent to the target network from the intermediate name server. Repeating the process with some amount of other recursive name servers, will cause the resource consumption.

2) Web Attacks: Web attacks are either HTTP GET/POST attack types or slow request/response attacks. HTTP GET flood attacks are hard to detect via Intrusion Detection System (IDS), since the IDS works on packet signatures. A bandwidth controller is required against HTTP GET attacks [17]. With the HTTP GET/POST attacks, large volume of valid requests is generated towards the victim's web server. They work on a non-spoofed basis. This attack type has some variations like sending multiple requests within a single HTTP session and creating multiple requests by a single packet in a single session.

One of the well-known types of the slow attacks is Slowloris attack. The aim is to send partial HTTP requests by sending subsequent headers at regular intervals for keeping the sockets from closing. Similar to Slowloris, HTTP fragmentation attack is used for holding up the HTTP connection for a long time. Then the attacker starts sending small HTTP traffic to the server in small fragments as slowly as possible causing the server to wait for data. Similar to HTTP GET attack, slow post attack occurs when the attacker sends a complete HTTP header including “content-length”, but the real data is sent as slow as possible for posting.

III. Prevention Methods

Prevention methods have been published so far with different perspectives. Classification methods are given in papers like [18] and [19]. In [18], prevention is categorized as the activity deployed or the location of deployment. Activity deployment category includes the actions that are taken against DDoS attacks. It also includes intrusion prevention techniques like disabling unused services, applying security patches to the host machines and changing the victim’s IP addresses. Intrusion detection systems like anomaly or misuse detection systems are also in this category. The location of the DDoS prevention mechanism can be either close to the victim’s network or to the attacker’s side or an inter-mediate solution. Work [19] mentioned about general techniques that can be applied commonly. These include, disabling unused services and IP broadcasting, installing the latest security patches as in [18], defining firewall rules and using an IP pool to dynamically switch the server IP addresses. Another approach is presented in [12]. According to this paper, DDoS prevention methods can be classified into two categories as classification based on the deployment location and based on the point of time when DDoS defense mechanism will react.

A. Source-based Mechanisms

Source-based mechanisms are deployed as much close as possible to the attacker side. Edge routers at the source local network or the access routers, connecting sources' edge routers, of an Autonomous System (AS) are the deployment points.

One of the deployment locations of DDoS defense mechanism is the source that is known as the attacker. The closer the defense mechanism to the source, the more efficient defense is applied. One defense mechanism at the edge routers is defined as Network Egress and Ingress Filtering (NEIF) that is applied by ISPs to the edge routers. The aim is to protect against the attacks from spoofed IP addresses and also prohibit their own network from participating DDoS attacks [20]. Although ingress filtering reduces DDoS attacks due to IP spoofing, it does not provide a solution to the usage of the spoofed legitimate addresses. IP ranges that are used as legal ones will not be filtered. On the other hand, egress filtering is an outbound filtering that is restricting only the defined IP addresses reaching to the outside network. The side effect of the egress filtering is the waste of resources. Related works with NEIF can be divided into two, either traffic aggregate (MULTOPS [22] and ACC-Pushback [21]) or individual flow based (D-WARD [23] and RED-PD [20]).

MULTOPS assumes that there is a proportion between incoming and outgoing traffic. A significant difference between coming and leaving traffic means that there is an attack going on. MULTOPS uses dynamic tree structure to keep packet rates and IP addresses which makes it vulnerable to memory consumption. At cooperative pushback mechanism, congested router asks its neighbors to rate-limit the traffic that depends on the idea that, the neighbors sending the traffic are more likely to be carrying the attack traffic.

D-WARD is a source-end defense mechanism. It is installed at the exit router of the end network and monitors inbound and outbound traffic. A profiling of the traffic is done periodically and attacks are defined by the flow models. D-WARD reacts the attacks by rate limiting the outgoing traffic to the victim. Since the profiling requires CPU power, it also consumes memory space. Attackers may behave like in the normal profiled flow attributes to skip D-WARD protection. RED-PD uses the packet drop history at the router. Because of the congestion, the dropped packets belonging to the flows are assumed to be the high-bandwidth ones and are dropped.

Another rate-limiter solution is MANAnet Reverse Firewall [25]. It works like traditional firewall, but the direction of the prevention is from inside to the outside world. It stops DDoS attacks between the networks it separates. The aim is to stop zombie machines attacking around. The reverse firewall requires manual guidance, so the configuration cannot be changed at runtime dynamically.

B. Destination-based Mechanisms

Another deployment location is the destination that is known as the victim. At this method, detection and prevention are done at the victim’s side. One of the methods is IP tracebacking [26]. IP tracebacking is used to detect IP spoofing where source IP validation is required. Either packet marking or link testing is used. Packet marking relies on the routers on the way to the victim to mark the packets with their identities, so that victim can identify the source [27]. Link testing generally starts from the router close to the victim and iteratively tests the upstream router until the source is reached. Traceback methods have serious problems. One of them is guaranteeing the number of routers that will contribute to the tracebacking. Second, most of the traceback functionality requires heavy computational power, network or management overheads [28].

History-based IP filtering relies on the IP address database (IAD). This database is generated by looking at the most frequent IP addresses appeared at the target side. During a DDoS attack, only the IP addresses in the source IP database are accepted. Since it is not required to work on the whole Internet, it is robust. On the other hand, if the attacker learns any IP address that belongs to the previous connections and also in the IAD, then it will be ineffective [29].

Instead of source IP database, another idea is also keeping the hops of the source IP addresses. This filtering technique is named as hop based IP filtering [30]. When an attack is alarmed, the IPs and their hops are fetched to detect the spoofed IP addresses. As with the history based method, hops can be copied with the valid IP addresses in the database that will cause a legitimate connection from an attacker.

Instead of keeping the database at the target side, Path Identifier (PI) suggests to mark the packets with the same fingerprint. According to the PI approach, each packet travelling the same path has the same identifier. Because of the limited space on the packets for identification, same path identification may represent different paths [31].

SYN floods are another threat for the victim side. They can be prevented via SYN Cookie usage. It is one of the techniques for SYN flood attacks. It is a technique to reconstruct the three way handshake between client and server when the appropriate ACK is returned. The server avoids dropping connections when the SYN queue fills up. The server keeps sending back SYN + ACK responses to the client and discard the SYN entry. When the appropriate ACK receives, the server is able to reconstruct the SYN queue entry.

C. Defence Mechanisms Against Application-level Attacks

Except from deployment location of the prevention, another important category includes the application level DDoS attack preventions. One of the most attacked targets is DNS. To prevent DNS amplification attacks, DNS Amplification Attacks Detector (DAAD) is proposed. DAAD processes captured network traffic on-the-fly by using Iptraf tool and saves it to the database. The DNS messages are categorized as request and response. For every response, a request is looked for at the database. If none found, it is marked as suspicious. When the suspicious number exceeds a threshold, an alarm is created [32]. For HTTP attacks, rate limiting is proposed. DDoS Shield uses statistical approach to detect suspicious sessions. According to the suspicion assignment, DDoS-resilient scheduler applies rate limiting [33]. Instead of using statistical methods, anomaly based approach is applied for HTTP attacks also. Semi-markov model is used with the entropy of the document to detect application layer attacks [34]. Another approach is to monitor user behavior to determine whether he is malicious or not. User's features like request volume, instant and long-term behaviors are monitored. For different behaved users, Defense to resist against Tilt-DDoS attacks, denoted as DAT, provide differentiated services to them [35].

IV. Attacks on Cloud Systems

With the rapid development of the cloud builders and their open structure, commercial firms are getting into cloud business and serving on the cloud platform for their customers. Redhat, Dell, HP, Intel, Paypal and many others are starting to develop their own cloud structures. They are also contributing to the development of the open source cloud tools like OpenStack or Cloudstack. With the increase of the investments at the cloud services, it is expected that the usage of cloud systems will also increase.

Cloud systems are in the scope of attackers while the big investors like Google, eBay, Amazon and IBM are publishing their services on the cloud. Google announced its Compute Platform, eBay joined the cloud environment by cooperating with Microsoft for its Azure platform and at the same time started to deploy OpenStack for research and development. Amazon is known with its Compute Cloud (EC2) platform and IBM has been serving its own cloud solution. Not only attackers, but also customers of these firms are under attack with the rented professionals who use the system's vulnerabilities to take down the cloud systems. A sample case occurred for Bitbucket.com where they keep their systems in EC2 [36].

Research on DDoS attacks and defense mechanisms in the cloud are at the early stages [37]. The cloud security covers many aspects like attack mitigation techniques against DDoS [38], economical DDoS attacks in the cloud [39], DDoS defense as cloud service [40] and security architecture against DDoS attacks [41].

One of the proposed mitigation techniques is using swarm network. Transparent and Intelligent Fast-Flux Swarm Network is DDoS prevention technique that is using Intelligent Water Drop (IWD) mechanism. Fast-Flux Swarm network is built onto fast-flux domain name servers and decentralized swarm nodes. A fast-flux service is used to provide multiple IP addresses to the attacker. IWD algorithm is used to determine the nodes that will relay messages between the client and the server. In traditional approach, requests are routed from client to the server through routers. In the swarm network approach, a layer is added that all incoming traffic will be registered to the swarm and forwarded to the server. The response will be sent back to the swarm which will be forwarded to the client at the end [38]. Since there is no obvious bottleneck at the network, it is hard for the attacker to take down the network. There are some limitations though. Each connection is bound to a particular route for a particular client and server at the swarm network. It does not allow SSL connections and fast changes that result in inactive name servers [42].

Another prevention method is announced as a network method and as a transparent solution that is Cloud Based Attack Defense (CLAD). All traffic that is routed to the protected server is forwarded to at least one CLAD entry point. Network layer attack defense is applied at the entry point to the CLAD. By using firewall techniques, unwanted or malicious packets are dropped. Admission control is also applied to limit the concurrent connections to the same server. The number of the concurrent connections can be varying depending on the load of the protected server. Authentication is also proposed to distinguish legitimate clients from malicious ones. A new challenging model is suggested for the improper charge of the malicious traffic instead of the maximum quota definition by the cloud service provider. To prevent the client from consuming resources, a congestion control mechanism is also added to the CLAD system [40]. CLAD focuses on HTTP traffic.

Although there are tools like Agobot, Mstream and Trinoo, most attackers are using less complicated tools for Extensible Markup Language (XML)-based Denial of Service (X-DoS) and HTTP-based Denial of Service (H-DoS) attacks because of their simple implementation [43]. For protecting H-DoS and X-DoS attacks, Service-oriented traceback architecture (SOTA) and Cloud TraceBack (CTB) are proposed [44]. SOTA is a web security service application that applies a Service-Oriented Architecture (SOA) approach to traceback methodology. It is used for identifying forged messages and used for protecting against X-DoS. CTB is placed at the edge router and all service requests are first sent to it for marking. In the attack situation, the client requests a web site from CTB, which is forwarded to the requested server. The attack client will then create a Simple Object Access Protocol (SOAP) request which will be answered by SOTA and a mark will be added within the header. This marked message is sent to the server where it is asked for extracting the mark to the client side which is used for filtering out the attack traffic [44].

As a defense strategy, IDS is also suggested for cloud environments. They are good for analyzing the actions of the attacker for the known signature types like smurf, SYN or other attack types. They work signature based and good for misuse detection, but for abnormal traffic and new type of attacks, they should not be preferred. One proposed method is to deploy the IDSes on each host machine. Snort is used as the IDS on each Virtual Machine (VM) and the collected data is analyzed by using Dempster-Shafer Theory (DST) [45]. It is an extension of Bayesian model that is a powerful method in statistical inference, diagnostics, risk analysis and decision analysis. The proposed work states that IDS data can be used to detect DDoS attacks.

Another Snort related work proposed as a distributed establishment is named as Firecol [29]. Firecol is a collaborative system that works on ISP level. A virtual ring is created between the ISPs when the attack is high. Although the system is based on Snort, it is proposed to extend the Snort rules to prevent other types of DDoS attacks.

IDS approach can be applied for known flood attack types like SYN. For spoofed attacks, spoofed IP detection techniques like Hop-Count Filtering (HCF) and IP-to-hop-count (IP2HC) are proposed. The HCF counts the number of hops depending on the value of Time to Live (TTL) [46]. Another version of HCF is IP2HC which creates a hash table between the source IP addresses and stores hop count of each IP address. Stored hop is determined from TTL value marked by checking the SYN flag status, the packet is marked as suspicious or not [47].

Detection methods can be combined with prevention methods to build a more powerful protection. In [48], DDoS detection using flow patterns are combined with the layered firewall structure to prevent DDoS attacks. It is proposed that by looking at the flow attributes (e.g. average number of flows per packets) coming from the router, some flooding attacks can be detected, also by using the IP and port information of these flows, a firewall can be used to filter the traffic.

V. Conclusion

While the signature based detection and prevention methods increase, there are also anomaly based approaches. For zero-day attacks, anomaly based preventions are supported with machine learning techniques. Both machine learning and data mining techniques have future study areas in the cloud computing. Especially at the botnet detection and prevention, data mining techniques are seemed to be a potential working area. By combining them with source based, destination based or web based preventions, hybrid methods can be more effective when also combined with the scaling functionality of the cloud itself.

Scaling property is one of the popular side at the cloud environments that can be used for DDoS prevention. By continuously increase the sources that are either at the traffic entries or at the routing side, the number of the preventers are increased. Since the data at the DDoS traffic is huge, distributed computing can be used to understand the attack sources. After the detection of the DDoS, dynamic resources can be created according the techniques chosen above.

As a future work, routing algorithms, dynamic resource creation and their usages are planned to be studied.

References

[1] F-Secure, “Denial of service (DoS)”, https://www.f-secure.com/en/web/labs_global/denial-of-service, 2014.

[2] CERT, “Denial of service attacks”, http://www.cert.org/tech_tips/denial_of_service.html, 2001.

[3] S. Tripathi, B. Gupta, A. Almomani, A. Mishra, and S. Veluru, “Hadoop based defense solution to handle distributed denial of service ddos attacks”, Journal of Information Security, vol. 4, pp. 150–164, June 2013.

[4] Defense.net, “DDoS attack timeline”, http://www.defense.net/ddos-attack-timeline.html, 2015.

[5] S. Hoffman, “DDoS: A brief history”, http://blog.fortinet.com/ddos-a-brief-history, 2013.

[6] A. Networks, “DDoS: from nuisance to menace”, http://www.arbornetworks.com/corporate/blog/4676-a-decade-of-ddos, 2012.

[7] N. Hachem, Y. Ben Mustapha, G. G. Granadillo, and H. Debar, “Botnets: Lifecycle and taxonomy,” in Conf. on Network and Information Systems Security, pp. 1–8, 2011.

[8] D. Mahajan and M. Sachdeva, “DSoS attack prevention and mitigation techniques - a review,” Int. Journal of Computer Applications, vol. 67, no.19, pp. 975–8887, April 2013.

[9] Akamai, “The state of the internet 2nd quarter report”, http://www.akamai.com/dl/documents/akamai_soti_q213.pdf?WT.mc_id=soti_Q213, 2013.

[10] P. Institute, “2013 cost of cyber crime study: United States”, http://media.scmagazine.com/documents/54/2013_us_ccc_report_final_6-1_13455.pdf.

[11] Prolexic, “Prolexic quarterly global ddos attack report”, http://www.valleytalk.org/wp-content/uploads/2013/07/Prolexic_Quarterly_Global_DDoS_Attack_Report_Q213_071313.pdf, 2013.

[12] S. Zargar, J. Joshi, and D. Tipper, “A survey of defense mechanisms against distributed denial of service (ddos) flooding attacks,” IEEE Communications Surveys & Tutorials, vol. 15, no. 4, pp. 2046–2069, 2013.

[13] Incapsula, “Distributed denial of service attacks”, http://www.incapsula.com/ddos/ddos-attacks, 2013

[14] M. Kumar, A. Panwar, and A. Jain, “An analysis of tcp syn flooding attack and defense mechanism,” Int. Journal of Engineering Research & Technology, vol. 1, no: 5, July 2012.

[15] F. Guo, J. Chen, and T. Chiueh “Spoof detection for preventing dos attacks against dns servers,” in 26th IEEE Int. Conf. on Distributed Computing Systems, 2006, pp. 37–44.

[16] R. Vaughn, and G. Evron, “Dns amplification attacks, a preliminary release,” http://vanilla47.com/PDFs/DNS-BIND-Docs/DNS Amplification Attacks.pdf, 2006

[17] T. Yatagai, T. Isahora and I. Sasase, “Detection of HTTP-GET flood attack based on analysis of page access behavior,” in IEEE Pacific Rim Conference on Communications, Computers and Signal Processing, 2007, pp. 232–235.

[18] C. Douligeris and A. Mitrokotsa, “DDoS attacks and defense mechanisms: a classification,” in 3rd IEEE Int. Symposium on Signal Processing and Information Technology, pp. 190–193, December 2003.

[19] B. B. Gupta, R. C. Joshi and M. Misra, “Distributed denial of service prevention techniques,” Int. Journal of Computer and Electrical Engineering, vol. 2, pp. 1793–8163, April 2010.