Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 49 (2015) 202 – 210

Procedia Computer Science

ICAC3'15

Understanding DDoS Attack & Its Effect In Cloud Environment

Rashmi V. Deshmukh[a], Kailas K. Devadkar[b]

[a]Sardar Patel Institute of Technology, University Of Mumbai, India
[b]Sardar Patel Institute of Technology, University Of Mumbai, India

Abstract

Cloud computing is blooming technology and adopted by many companies. But there are many issues and one of them is DDOS. It can effect organizations depending on cloud for their business. This paper explains DDoS attack, its effect in cloud computing and things needs to be considered while selecting defense mechanisms for DDoS.

Peer-review under responsibility of organizing committee of the 4th International Conference on Advances in Computing, Communication and Control (ICAC3'15)

Keywords: Cloud computing; Cloud Security; DDoS

1. Introduction

In 2009 NIST[3] defined Cloud Computing as "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction. Pay per usage, Virtualization, on demand access, flexibility and reduced hardware and maintenance cost are some of the factors contributing to popularity of cloud computing[1 2]. Platform as a Service (PaaS), Infrastructure as a Service (IaaS), and Software as a Service (SaaS) are service models of cloud computing. SaaS provides ability to run and use the software/ application without the need to install it on your own machine. IaaS makes use of virtualization technology to provide Infrastructure by sharing the hardware with many customers or tenants[3]. Virtualization plays a major part in cloud computing by making effective and systematic use of the available hardware. Recently Virtualization is used at various stages like networks, CPU, memory, storage etc. It increases the availability of system and also reduces cost and present a superior flexible system.

DDoS attack is major trouble to the availability. The attacker can greatly degrade the quality or fully breakdown the of victim's network connectivity. The attacker first compromises many agents or hosts and then uses these agents to launch the attack by deplete the target network. The main intention of a DDoS attack is to make the victim unable to use the resources. In most of the scenarios, targets could be web servers, CPU, Storage, and the other Network resources[4]. In cloud environment also DDoS can reduce the performance of cloud services significantly by damaging the virtual servers.

*

Peer-review under responsibility of organizing committee of the 4th International Conference on Advances in Computing, Communication and Control (ICAC3'15)
doi:10.1016/j.procs.2015.04.245

1.1. Understanding The Attack

DDoS attacks are launched by affecting the victim in following forms:

- Attacker can find some bug or weakness in the software implementation to disrupt the service.
- Some attacks deplete all the bandwidth or resources of the victims system.

Attackers scan the network to find the machines having some vulnerability and then these machines are used as agents by the attacker. These are called zombie machines. Spoofed IP's are used by zombie machines. The design of internet gives rise to many conditions causing denial of service attacks[4]. Some of these features will be explained in this section. Security in internet is dependent on hosts. Attackers compromise the security of hosts to launch DDoS attacks and they use spoofed IP addresses making it difficult to trace attack source. Further internet is full hosts. It gives attacker huge amount of options, out of which vulnerable hosts are chosen. Main target of DDoS attack are resources like bandwidth, CPU etc. and the resources are limited in network. If these resources are increased then impact of the attack can be lowered but still resources will be wasted leading to monetary loss.

1.2. DDoS Attacks In Past

DDoS attacks are initiated by a network of remotely controlled, well structured, and widely dispersed nodes called Zombies. The attacker launches the attack with the help of zombies. These zombies are called as secondary victims. The recent attacks in 2013 include the attack in China's websites, Bitcoin, largest cyber-attack by Cyber Bunker, NASDAQ trading market, Iranian Cyber-attacks on FBI and so. From the above survey most of the victims of DDoS attacks are distributed and shared. Apart from the list mentioned there are numerous anonymous tools emerging day by day. Table 1 lists the DDoS attacks occurred over years and how it evolved[5 6 7].

Table 1. DDoS attacks in past

Year	Details
1998	First DDoS tools were discovered. These tools were not used widely but point-to-point DoS attacks and Smurf amplification attacks continued.
1999	A trinoo network was used to flood a single system at the University of Minnessota, which made the network unusable for more than 2 days. And massive attack using Shaft was detected. The Data gathered during the attack was then analyzed in early 2000 by Sven Dietrich and presented in a paper at the USENIX LISA 2000 conference.
2000	15 year old boy Michael Calce (Mafiaboy) launched attack on Yahoo's website. He was then sentenced in juvenile detention center for 8 months. He also went forward to degrade the servers of CNN, eBay, Dell, and Amazon, showing how easy it was to damage such major websites.
2001	The attack size grows from Mbps to Gbps. Efnet was affected by a 3 Gbps DDoS attack.
2002	It was reported that 9 of the 13 root internet servers were under serious threat of DDoS attack. Congestion due to attack made few root name servers were not reachable from many parts of the global Internet, which made many valid queries unanswered.
2003	Mydoom was used to shut down the service of SCO group's website. Thousands of PC's were infected to send the data to target server.
2004	Authorize-IT and 2Checkout were Online payment processing firms attacked by DDoS in April targeted. It was later known that the attackers extorted and threatened to shut down there sites.
2005	In August of 2005, jaxx.de, a gambling site was under DDoS attack and to stop this attack, the attacker demanded 40,000 euros.
2006	A number of DDoS attacks targeted the blog of Michelle Malkin. The attacks started on Feb. 15, and continued till Feb. 23.
2007	In December 2007 during the riots in Russia, government sites suffered severe DDoS attacks. Access to IP addresses outside Estonia was removed by many of them for several days.
2008	In November 2008, the Conficker worm used vulnerabilities found in Microsoft OS. It uses vulnerable machine and other machines are unwillingly connected to it, to make a large botnet.
2009	On 4th July (Independence Day in the US) 27 websites of White House, Federal Trade Commission, Department of Transportation, and the Department of the Treasury were attacked. On 1st august, Blogging pages of many social networking sites (Twitter, Facebook etc.) were affected by DDoS attack, aimed at "Cyxymu" Georgian blogger.
2010	Operation Payback: DDoS attacks launched on websites of MasterCard, PayPal and Visa, as they decide to stop giving service to WikiLeaks.
2011	LulzSec hacktivist group attacked website of CIA (cia.gov).
2012	Many attacks at us banks involve use of itsoknoproblembro DDoS tool. Many such do-it-yourself toolkits are available.
2013	150 Gbps DDoS attacks are increasing.

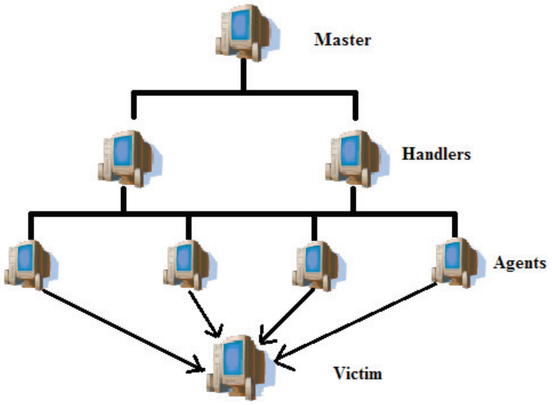

Fig. 1. Constituents of DDoS

1.3. DDoS Constituents

Recently, Botnets are been used widely to perform DDoS attacks. This section explains botnet architectures and the tools that have been used to launch DDoS flooding attacks. Many computers are used for launching a DDoS Attack. It makes use of client server technology. In general, DDoS attack comprises of Master, Handler, Agents and victim (as show in Fig. 1). The zombies (agents or bots) are the one used by the master to form a botnet. Larger the number of zombies, more disruptive the attack will be[8]. The Master communicates with agents via handlers. For Example, handlers can be programs installed on a set of compromised devices (e.g., network servers) that attackers communicate with to send commands. Attacker sends command and controls their agent through handlers. Bots are devices that have been compromised by the handlers.

The bots actually carry out the attack on the victim's system. Attacker uses many scanning techniques for finding a vulnerable machine[19].

Random Scan is a simplest strategy which randomly scans whole IPv4 address space as the worm doesn't know where the host is present. It effective only for IPv4 as address space space of IPv6 is too vast. Hitlist Scan has a list which contains IP address vulnerable hosts in the Internet. The scanning is done in this list. When it makes another machine a host, part of the initial hit list will be sent to that machine[20]. Route-based Scan reduces the search addresses BGP routing prefixes are used and this prefixes information can reduce the search space drastically[21]. In Divide-and-conquer Scan technique the scanning is done by different hosts on different part of address space hence saving the resources. Apart from these there are other strategies too like Permutation Scan, Local Preference Scan and Topological Scan. Once host is found after scanning, vulnerabilities of that host need to be found to gain its control. More information about these vulnerabilities is available on internet. For example Common Vulnerabilities and Exposures refer[22].

1.4. Classification

The variety of DDoS attacks are sprouting in the computing world. The major types include Bandwidth based and resource based attacks. Both types consume the entire bandwidth and resources of the network that's been exploited. Through the analysis made, taxonomy has been depicted in the Fig. 2. Depending upon the exploited vulnerability it can be further divided into different types.

Bandwidth Depletion Attacks:

This type of attack consumes the bandwidth of the victim or target system by flooding the unwanted traffic to prevent the legitimate traffic from reaching the victim network. Tools like Trinoo are usually used to perform these attacks. Bandwidth depletion attacks are categorized further as:

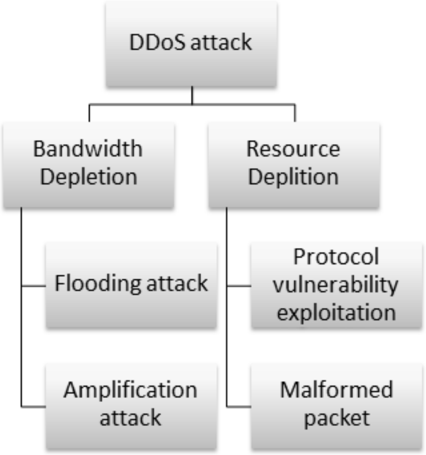

Fig. 2. Taxonomy of DDoS Attacks

- **Flood Attacks:** This attack is launched by an attacker sending huge volume of traffic to the victim with the help of zombies that clogs up the victim's network bandwidth with IP traffic. The victim system undergoes a saturated network bandwidth and slows down rapidly preventing the legitimate traffic to access the network. This is instigated by UDP (User Datagram packets) and ICMP (Internet Control Message Protocol) packets.
  An UDP flood attack is initiated by following steps:

  1. An attacker sends a large number of UDP packets to the victim system's random or specified ports with the help of zombies.
  2. On receiving the packets, the victim system looks the destination ports to identify the applications waiting on the port.
  3. When there is no application, it generates an ICMP packet with a message "destination unreachable".
  4. The return packets from the victim are sent to the spoofed address and not to the zombies.

  As a result the available bandwidth has been depleted without servicing the legitimate users. This impacts the connections and systems located near the victim. Other variations of this attack include Fragmentation, DNS flood attack, VoIP flood attack, Media data flood attack etc. An ICMP flood attack involves following steps:

  1. An attacker sends a large number of ICMP_ECHO_REPLY i.e. ping packets to the victim system with the help of zombies. This kind of packets requires a response message from the victim.
  2. The victim sends the responses to the packets received.
  3. Now the network is clogged with request response traffic. The spoofed IP address may be used in the ICMP packet.

  The bandwidth of the victim network connections is saturated and depleted rapidly without servicing the legitimate users. Fragmentation, DNS flood and Ping flood are the other variations of ICMP flood attacks.
- **Amplification attacks:** The attacker sends a large number of packets to a broadcast IP address. In turn causes the systems in the broadcast address range to send a reply to the victim system thereby resulting in a malicious traffic. This type of attack exploits the broadcast address feature found in most of the internetworking devices like routers. This kind of DDoS attack can be launched either the attacker directly or with the help of zombies. The well-known attacks of this kind are Smurf and Fraggle attacks.
  The Smurf attack is caused by following steps:

1. Attacker sends packets to a network device that supports broadcast addressing technique. The return address in these packets are forged or spoofed with victim's address.
2. ICMP_ECHO_RESPONSE packets are sent by the network amplifier to all the systems in the broadcast IP address range. This packet implies the receiver to respond with an ICMP_ECHO_REPLY.
3. An ICMP_ECHO_REPLY message from all the systems in the range reaches the victim.

The Fraggle attack is the variation of Smurf attacks where the UDP echo packets are sent to the ports that supports character generation. It has following steps:

1. Attacker sends UDP echo packets to a port that supports character generation. The return address in these packets are forged or spoofed with victim's address with the port supporting character generation thus creating an infinite loop.
2. This targets the port supporting character generation of all the systems reached by broadcast address.
3. All these systems in the range echoes back to the character generator port in the victim.
4. This process repeats since UDP echo packets are used.

This attack is worse than the smurf attacks. A variant of these attacks is the reflector attack, which involves a set of reflectors to accomplish the specified task. The reflector is intermediary hosts or devices that are used for launching the amplification attacks. The special feature of the reflector is it keeps responding to the packets it receives. So the attackers make use of these reflectors for the attacks that requires responses. In this case the return IP-address will be spoofed to the victim's system.

Resource Depletion Attacks: The DDoS Resource depletion attack is targeted to exhaust the victim system's resources, so that the legitimate users are not serviced. The following are the types of Resource depletion attacks:

- **Protocol Exploit Attacks**: The goal of these attacks is to consume the surplus quantity of resources from the victim by exploiting the specific feature of the protocol installed in the victim. TCP SYN attacks are the best example of this type. The other examples of Protocol exploit attacks are PUSH + ACK attack, authentication server attack and CGI request attack.
- **Malformed Packet Attacks:** The term malformed packet refers to the packet wrapped with malicious information or data. The attacker sends these packets to the victim to crash it. This can be performed in two ways:
  IP Address attack: The malformed packet is wrapped with same source and destination IP address thus creating chaos in the operating system of victim. By this way it rapidly slows down and crashes the victim.
  IP packet options attack: Each of the IP packets consists of the optional fields to carry additional information. This attack makes use of these fields to form the malformed packet. The optional fields are filled by setting all the quality of service bits to one. So the victim spends additional time to process this packet. This attack is more vulnerable when attacked by more than one zombie.

1.5. Defense Mechanism

Various countermeasures had been adopted and still emerging for mitigating against the DDoS attacks. Mostly DDoS attacks are influenced by an intruder attempting to make an unauthorized access in the victim system/network. The defense mechanisms are as shown in Fig. 3

Prevention Techniques

The best strategy against any attacks is to prevent the occurrence of the attacks. One such technique is using filters.

- Ingress filtering[15] - this process stops the incoming packets with a not legitimate source address. Routers are used for this purpose. This technique prevents the DDoS attack caused by IP address spoofing.
- Egress filtering[16] - an outbound filter is used in this technique. This technique allows the packets having valid IP address in the network- specified range to leave the network.

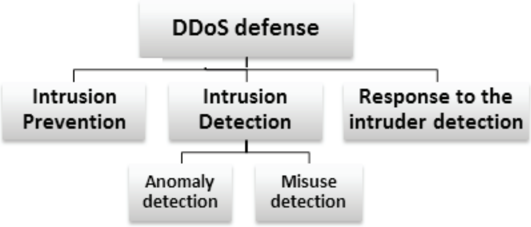

Fig. 3. DDoS defense mechanisms

- Route based distributed packet filtering - The filter uses the route information to capture/filter the IP address spoofed packets and prevents the attack. It is also used in IP trace back. But it requires global information about the network topology[17].
- Secure Overlay Services (SOS) - SOS is architecture with distributed feature that safeguards the victim system. It assumes an incoming packet to be valid if it is from the legitimate servers. Other packets are filtered by the overlay. A client must authenticate itself with replicated access points viz. SOAP to gain access to the overlay network[18].

The other prevention techniques includes disabling unused services, applying security patches, changing IP address, disabling IP broadcasts, load balancing and honeypots[14]. The intrusion prevention techniques do not completely remove the risk of DDoS attacks but provided a base or increased the security.

Detection Techniques

The intrusion detection system helps the victim to avoid the propagation of DDoS attacks and prevents it from crashing. The various methods in intrusion detection include:

- **Anomaly detection:** This method detects the attacks by recognizing the abnormal behaviors or anomalies in performance of the system. This is done by comparing current values with previously detected normal system's performance. This method identifies the false positives in the system behavior. Some of the Anomaly detection techniques studies include the following:
  NOMAD- a scalable network monitoring system that detects the network anomalies by analyzing the IP packet header information[24].
  Packet sampling and filtering technique with congestion[25]- A statistical analysis had been made from the subset of dropped packets and once an Anomaly is detected a signal is passed to the router to filter the malicious packets.
  D-WARD[23]- detects the DDoS attack at the first victim. It prevents the attack from spreading to the neighbors of victim. D-WARD is set up at the edge router to detect the incoming and outgoing network traffic.
  MULTOPS[26]- MULTOPS is a data structure designed for the purpose of detecting DDoS attacks. It works on the assumption that, if the IP addresses of the system participating in a DDoS attack is possible, then measures are taken to block only these particular addresses. It keeps tracks of detecting either attacking systems or systems under attack by functioning in attack oriented mode or victim oriented modes respectively. It's a multi-level tree that maintains the packet rate statistics at different aggregation levels. But it requires router reconfiguration and novel memory management schemes.
- **Misuse detection:** This method detects the DDoS attacks by maintaining the database of well-known signatures or patterns of exploits. Whenever one such pattern has been detected, DDoS attacks are reported. Various misuse detection techniques has been discussed in[6].

Response to detection

In case when DDoS attack is detected, the next thing to do is the attack should be blocked and attacker should be traced for finding out attacker's identity. This can be done in two days, firstly manually using ACL or automatically.

Certain methods used for tracing and identifying the attacker as as shown on table 2. Besides many techniques used to stop DDoS attacks but not all of the can be detected and prevented. All that can be done is to reduce the impact of the attack.

Table 2. Traceback Methods

Method	**Description**
ICMP traceback	The mechanism deals with forwarding low probability packets to each router and also sends an ICMP traceback message to destination. With major no of ICMP messages which used to identify attacker, faces issues like additional traffic, also the validation of these packets is difficult and moreover path detection overhead of information from route map.
IP traceback	This method traces back the attacker's path to find the origin of attack. In this technique the path of attacker is followed back to find its source. But this becomes difficult if source accountability in TCP/IP protocol is disabled and also internet is stateless[29].
Link-testing traceback	This mechanism tests each of incoming links to check the probability of it being an attack. This is done by flooding large traffic and testing if it causes any network disruption. But the precondition to do this would be system that will be able to flood traffic and information about topology of network[28].
Probabilistic packet marking	This technique overcomes drawbacks of link-testing traceback as it does not require previous knowledge of network topology, large traffic etc. This advantage also overheads the systems but there are many methods to avoid this overhead as proposed in[27].

1.6. DDOS Attack In Cloud Environment

As discussed in our paper[30], recently cloud computing has been greatly increased in both academic research and industry technology. DDoS are one of the security threats that challenge the availability. According to Cloud Security Alliance, DDoS is one of the top nine threats to cloud computing environment[13]. Out of many attacks in clod environment 14% are DoS attacks. Many popular websites like yahoo were affected by DDoS in early 2000. Website of grc.com was hit by huge DDoS in May, 2001. The company was dependent on internet for their production work and business was greatly impacted. Forrester Consulting was contracted by VeriSign in March 2009 to perform a study on DDoS threats and protection. The survey was performed among 400 respondents from the US and Europe[11]. 74% had experienced one or more DDoS attacks in their organizations. Out of this 74%, according 31% the attacks caused service disruption, according 43% attacks does not result into services disruption as shown in Fig. 4[30]. The survey of DoS attacks in cloud says that as the use of cloud increases the rate of DDoS attacks will also grow in a fast pace. In Cloud environment when the workload increases on a service, it will start providing computational power to withstand the additional load. Which means Cloud system works against the attacker, but to some extent it supports the attacker by enabling him to do most possible damage on availability of service, starting from single attack entry point.

Cloud service consists of other services provided on the same hardware servers, which may suffer by workload caused by flooding. Thus, if a service tries to run on the same server with another flooded service, this can affect its own availability. Another effect of a flooding is raising the bills for Cloud usage drastically. The problem is that there is no "upper limit" to the usage[12]. And one of the potential attacks to cloud environment is neighbor attacks i.e. VM can attack its neighbor in same physical infrastructures and thus prevent it from providing its services. These attacks can affect cloud performance and can cause financial losses and can cause harmful effect in other servers in same cloud infrastructure.

1.7. Factors for Selecting Defense Solution

While selecting DDoS solution many things need to be considered.

- Functional: The solution should be functional enough, which means it should be able to reduce impact of the attack irrespective of how powerful the attack is.
- Transpicuous: The solution must be easy to implement i.e. it should not require modifying the existing network and its infrastructure.
- Lightweight: Most importantly the solution should not overhead the system.

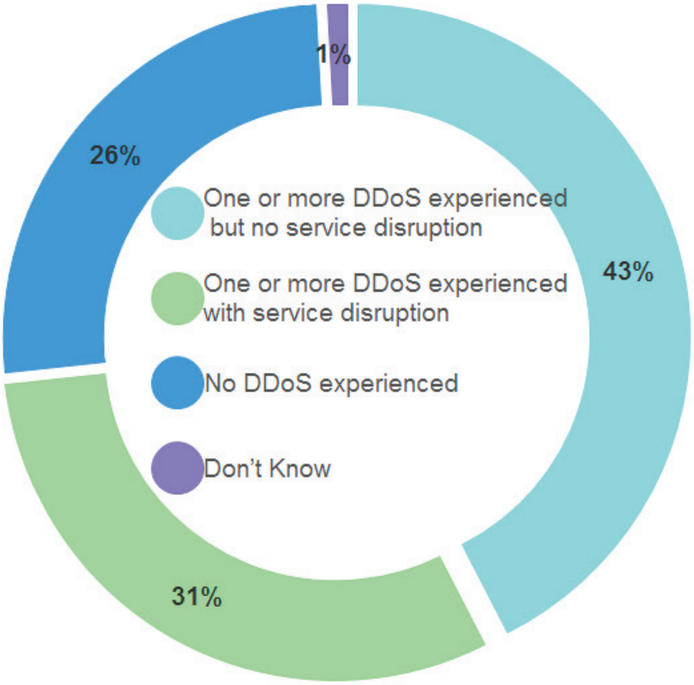

Fig. 4. DDoS experienced by organizations

- Precise: The solution selected should not give lots of false positive. Many methods need the traffic to be dropped or discarded and the solution must not drop genuine traffic.

2. Conclusion

As DDoS attacks are on rise in cloud computing. This paper provides a brief survey on DDoS attacks, then taxonomy of attacks, its types and various counter measures to mitigate the DDoS attacks. This survey confers DDoS detection, prevention and tolerance techniques. The paper concludes by providing some points to be considered while selecting DDoS defense solution.

References

1. P. Mell and T. Grance, "The NIST definition of cloud computing (draft)," NIST special publication, vol. 800, no. 145, p. 7, 2011.
2. Reference_Architecture_Doc_2011_NIST-CloudComputing.pdf.
3. T. Dillon, C. Wu, and E. Chang, "Cloud Computing: Issues and Challenges," in *24th IEEE International Conference on Advanced Information Networking and Applications (AINA)*, 2010, pp. 2733.
4. Denial of Service Attack, http://en.wikipedia.org/wiki/Denial-of-service_attack
5. DDoS attack tool timeline, http://staff.washington.edu/dittrich/talks/sec2000/timeline.html
6. History of DDoS, http://www.timetoast.com/timelines/history-of-ddos
7. DoS and DDoS Evolution, http://users.atw.hu/denialofservice/ch03lev1sec3.html
8. CERT Coordination Center, Overview of attack trends, Feb. 2002. http://www.cert.org/archive/pdf/attack_trends.pdf.
9. B. Grobauer, T. Walloschek, and E. Stocker, "Understanding Cloud Computing Vulnerabilities," *Security Privacy, IEEE*, vol. 9, no. 2, pp. 5057, Mar. 2011.
10. C. Douligeris and A. Mitrokotsa, DDoS attacks and defense mechanisms: Classification and state-of-the-art, *Computer Networks: the Int. J. Computer and Telecommunications Networking*, Vol. 44, No. 5, April 2004, pp. 643666.
11. CERT Advisory CA-1998-01, Smurf IP Denial-of-Service Attacks, January 5, 1998, Available: http://www.cert.org/advisories/CA-1998-01.html

12. Meiko Jensen, Jorg Schwenk, Nil Gruschka “On technical issues in cloud computing”, *IEEE International Conference on cloud computing*, 2009.
13. The Notorious Nine, Cloud Computing Top Threats in 2013, https://downloads.cloudsecurityalliance.org/initiatives/topthreats/TheNotoriousNineCloudComputingTopThreatsin2013.pdf
14. N. Weiler, Honeypots for Distributed Denial of Service, in *Proceedings of the Eleventh IEEE International Workshops Enabling Technologies: Infrastructure for Collaborative Enterprises 2002*, Pitsburgh, PA, USA, June 2002, pp. 109114.
15. P. Ferguson, D. Senie, Network ingress filtering: defeating Denial of Service attacks which employ IP source address spoofing, in: RFC 2827, 2001.
16. Global Incident analysis Center Special Notice Egress filtering, Available from http://www.sans.org/y2k/egress.htm.
17. K. Park, H. Lee, On the effectiveness of route-based packet filtering for Distributed DoS attack prevention in power law Internets, in: *Proceedings of the ACM SIGCOMM 01 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications, ACM Press*, New York, 2001, pp. 1526.
18. A. Keromytis, V. Misra, D. Rubenstein, SoS: secure overlay services, in: *Proceedings of the ACM SIGCOMM 02 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications, ACM Press*, New York, 2002, pp. 6172
19. C. Zou, D. Towsley, and W. Gong, the performance of internet worm scanning strategies, 2003.
20. V. Paxson S. Staniford and N. Weaver, How to own the internet in your spare time, in *11th Usenix Security Symposium*, San Francisco, August 2002.
21. V. Paxson S. Staniford and N. Weaver, How to own the internet in your spare time, in *11th Usenix Security Symposium*, San Francisco, August 2002.
22. C. Zou, D. Towsley, W. Gong, and S. Cai, Routing worm: A fast, selective attack worm based on ip address information, 2005. Common Vulnerabilities and Exposures, http://cve.mitre.org/cve/
23. J. Mirkovic, G. Prier, P. Reiher, Attacking DDoS at the source, in: *Proceedings of ICNP* 2002, Paris, France, 2002, pp. 312321
24. R.R. Talpade, G. Kim, S. Khurana, NOMAD: Traffic based network monitoring framework for anomaly detection, in: *Proceedings of the Fourth IEEE Symposium on Computers and Communications*, 1998.
25. Y. Huang, J.M. Pullen, Countering Denial of Service attacks using congestion triggered packet sampling and filtering, in: *Proceedings of the 10th International Conference on Computer Communiations and Networks*, 2001.
26. T.M. Gil, M. Poleto, MULTOPS: a data-structure for bandwidth attack detection, in: *Proceedings of 10th Usenix Security Symposium*, Washington, DC, August 1317, 2001, pp. 2338.
27. S. Savage, D. Wetherall, A. Karlin, T. Anderson, Network support for IP traceback, *IEEE/ACM Transaction on Networking* 9 (3) (2001) 226237.
28. H. Burch, H. Cheswick, Tracing anonymous packets to their approximate source, in:*Proceedings of USENIX LISA (New Orleans) Conference*, 2000, pp. 319327
29. S. Bellovin, The ICMP traceback message, Network Working Group, Internet Draft, March 2000, Available S. Bellovin, The ICMP traceback message, Network from ¡http://lasr.cs.ucla.edu/save/rfc/draft-bellovin-itrace-00.txt¿
30. Rashmi D. and Kailas D. mitigating ddos attack in cloud environment with packet filtering using iptables in *International Journal of Computer Engineering and Applications*, Volume VII, Issue II, August 14.