A Recent Survey on DDoS Attacks and Defense Mechanisms

A. Srivastava[1],[*] B.B. Gupta[1,2,] , A. Tyagi[1], Anupama Sharma[1], and Anupama Mishra[1]

[1] Department of Computer Science, Graphic Era University, Dehradun, India
gupta.brij@gmail.com
[2] Department of Electronics and Computer Engineering,
Indian Institute of Technology Roorkee, Roorkee, India

Abstract. Distributed Denial-of-service (DDoS) attack is one of the most dangerous threats that could cause devastating effects on the Internet. DDoS mainly started in 1998 but the influence of it was realized by the people only when the big organizations and corporations were hit by DDoS attacks in July 1999. Since then several DDoS attack tools such as Trinoo, Shaft, Tribe flood network (TFN), Tribe flood network 2000 (TFN2K) and Stacheldraht are identified and analyzed. All these tools could launch DDoS attacks from thousands of compromised host and take down virtually any connection, any network on the Internet by just a few command keystrokes. This survey paper deals with the introduction of DDoS attacks, DDoS attack history and incidents, DDoS attack strategy, DDoS attack tools, and classification of various attack and defense mechanisms. Finally, direction for future research work has been pointed out.

1 Introduction

Today, Distributed Denial of Service (DDoS) attacks have become a common threat to online businesses. With over 50,000 distinct attacks per week, DDoS attacks have become highly visible and costly form of cyber-crime, and are increasingly being proactively addressed by online businesses to avoid devastating costs of DDoS-related downtime [1,2,3]. Recent trends in the Internet [4, 5] show that the total amount of the DDoS attacks reached over 100 gigabit per second barrier. It also shows that the amount of DDoS attack traffic has been increasing in size year by year. A study conducted by Arbor networks [5] shows the year by year increase of the DDoS attack traffic on the Internet, from the year 2001 to 2010 as shown in Figure 1.

Denial of service attacks (DoS) deny services to legitimate users offered by the server or target machine. With time, DoS attack evolved to distributed denial of service attack where attacker compromises some other vulnerable machines on the Internet to coordinate attack at a single instant of time on the victim machine thus multiplying the effect of denial of service [6].

[*] Corresponding author.

D. Nagamalai, E. Renault, and M. Dhanushkodi (Eds.): PDCTA 2011, CCIS 203, pp. 570–580, 2011.

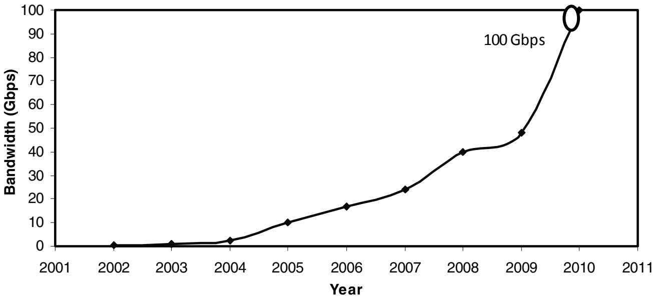

Fig. 1. Increase in DDoS attack traffic

Figure 2 shows the typical scenario under DDoS attack where legitimate users use only a bandwidth of 3 Mbps while the botnet can generate traffic of attack size ranging from 3-100Gbps. A Botnet of 20,000 [7] machines can bring down almost 90% of the Internet Websites.

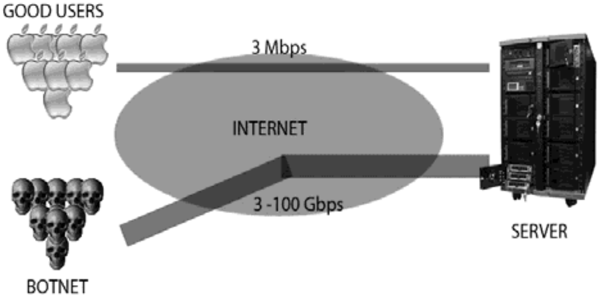

Fig. 2. Scenario under DDOS attack

Earlier, hackers used to have few machines and exploit some spoofing techniques to spoof multiple IP addresses. To the target machine, it would appear as if the attack is coming from multiple IP addresses. However now the time has changed and the hackers look for the vulnerable machines that lack security and use all those compromised machines to launch a real DDoS attack. They take the advantage of distributed system services offered by the operating systems like resource sharing, public folder sharing, accessibility, and so on. With increasing number of Internet users, DDoS attack has become the second most significant threat after virus infection to the Internet users [8].

In this paper, we will describe the DDoS problem, DDoS attack history and incidents, their classification along with the defense mechanisms to deal with them. In addition to this, paper also presents the challenges dealing with this problem and direction for further research work.

Rest of the paper is organized as follows: Second section deals with DDoS attacks history and recent incidents. Third section gives brief overview of DDoS attack.

Fourth section describes the components of DDoS attack and how it can be launched. Fifth section classifies describes the classification of DDoS attack mechanisms. Sixth section shows classification of the DDoS defense mechanisms. Seventh section describes the challenges in dealing with DDoS attacks. Finally, section eighth concludes the paper and states future scope for further research.

2 DDoS Attack History and Incidents

A revolution came into the world of computer and communication with the advent of Internet. Therefore, Internet has become increasingly important to the current society. It has changed our way of communication, business mode, and even everyday life [1]. The impact of Internet on society can be seen from figure 3 which shows exponential increase in number of hosts interconnected through Internet [9].

As, we can see from figure 3, there were only around 1 million Internet host in January 1993, which has increased to more than 775 million Internet hosts in October 2010. More and more users are connected to Internet and most of them are unaware about Internet Security. Poorly managed machines tend to be easier to compromise by attackers.

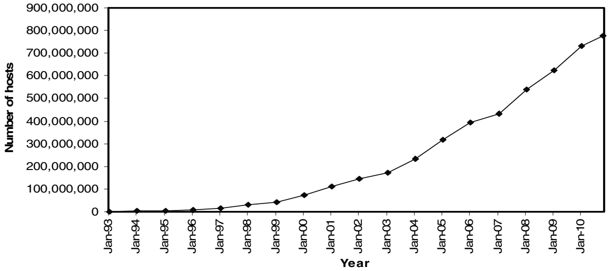

Fig. 3. Internet Domain Survey Host Count

According to this survey, the estimated Internet users are 1,966,514,816 for June 30, 2010. DDoS is one of the major threats to the Internet because of its ability to create a huge volume of unwanted traffic. The primary goal of these attacks is to prevent access to a particular resource like a Web site [11].

The first reported large-scale DDoS attack occurred in August, 1999, against the University of Minnesota. [12].This attack shut down the victim's network for more than two days. In the year 2000, a DDoS attack stopped several major commercial Web sites, including Yahoo and CNN, from performing their normal activities. Moore et al. [13] used backscatter analysis on three week-long datasets to assess the number, duration and focus of DDoS attacks, and to characterize their behavior. They found that more than 12,000 attacks had occurred against more than 5,000 distinct victim networks in February, 2001.

Initially these attacks were supposed to be a problem only with synchronous means of communication, which worked on IRC (Internet Relay chat) servers. So, these servers were initially banned from networks but, the attack on high profile websites such as Yahoo in 2000, wikileaks in 2009 and so on have proved these attacks to be a affecting whole of the Internet regardless of the means of communication [14]. Considering the attack on Yahoo in 2000, which pushed the site offline for about 3 hrs as the site received an unprecedented level of traffic of about 1GB/sec which was a huge amount to handle.

3 Overview of DDoS Attacks

As mentioned in [15], to create an effective DDoS attack, three steps are needed: Scanning, Propagation and Communication.

Scanning is the first step to exploit any system. The attacker first recruits the machines that have some vulnerability. Earlier this process was done manually by the attacker but now this process is automated. Some scanning strategies such as hit list scanning, topological scanning, permutation scanning, and local subnet scanning are popular or potential in deployment of DDoS attacks [6]. Attacker uses these techniques to continuously scan the vulnerable machines over the Internet and installs malicious scripts into them. So these machines become capable of recruiting other slaves or zombies under them too.

Propagation: While scanning deals with just looking for vulnerable machines, propagation deals with recruiting further machines with the help of already compromised machines which can be used further to generate a stream of packets towards the victim` s machine. Central source propagation model, back-chaining model and autonomous model are three main models of propagation [16].

Communication: The communication channel is important for coordinating an attack. Either Agent-Handler model or IRC model can be used to communicate with each other. In Agent-Handler Modal communication can be done by using TCP/ICMP/UDP protocol between attacker to handler, handler to agent and vice versa. In this model the communicators know each other` s identity. Internet Relay Chat (IRC) is a multi-user, on-line chatting system. In IRC (Internet Relay Chat) Model, the communicators cannot communicate directly so tracebacking is not easy that make it most widely used model by the attackers over a network.

4 DDoS Attack Strategy

Launching DDoS attack involves four components: attacker, control masters (or handlers), agents (or slaves or zombies), victim (or target machine). Attacker first scans millions of machines over the Internet for finding vulnerable machines whose security can be exploited easily. These machines are known as masters or handlers as these are directly under the control of attacker. The process of recruiting handlers is completely automated and is done through continuous scanning of remote machines looking for any security loopholes. The attacker installs malicious codes into these infected machines which then become capable of deploying further infected machines [17].

The machines deployed by handlers are directly under their control and are known as slaves or zombies. Attacker indirectly controls these machines through handlers. These handlers and zombies, on the signal of attacker are used to start a coordinated attack on target machine. This makes the target machine incapable of communicating or utilizing any of its resources. Attacker often uses IP spoofing in handlers and zombies to hide the identity of these machines. This leaves future scope for attacker of using the same machines for creating DDoS attack.

5 Classification DDoS Attack Mechanisms

We can classify DDoS attacks into two broad categories: flooding attacks and logical attacks [26]. Flooding attacks creates avalanche of transmitting packets at the victim side which makes the target machine incapable of handling request from the legitimate users.

In case of flooding attacks, the attacker keeps on sending request packets to the server at a particular rate. Due to increase in attack packets, the legitimate users decrease their flow of packets as per network Congestion control mechanism. Once the total request rate from the server becomes greater than the service rate of the server, the request packets starts getting buffered in the server and after some time the requests start dropping down. Finally, the time comes when whole of the bandwidth is exhausted by the attack packets only and the legitimate users are denied of the services, thus creating successful DDoS attack. In Logical or software attack, a small number of malformed packets are designed to exploit known software bugs on the target system. These attacks are relatively easy to counter either through the installation of software patches that eliminate the vulnerabilities or by adding specialized firewall rules to filter out malformed packets before they reach the target system [27].

A. Types of flooding attacks

i). *SYN flooding attack*: A normal TCP connection involves 3-way handshaking. In case of attack, the attacker uses spoofed IP addresses to send requests to a server. The server responds by sending the SYN/ACK signal waiting for the ACK signal from its client. But this time no reply comes since the IP is spoofed and the real client is unaware of the ACK signal that the server is expecting. This leaves the half open connections on the server side thus consuming its resources. Therefore, creating thousands and thousands of requests like this can force the server to crash or hang [28].

ii). *ICMP attack:* An attacker sends forged ICMP echo packets to broadcast addresses of vulnerable networks. All the systems on this network reply to the victim with ICMP ECHO replies. This rapidly exhausts the bandwidth available to the target, effectively denying its services to legitimate users [2, 29].

iii). *UDP Flood Attack:* A UDP flood attack is possible when an attacker sends a UDP packet to a random port on the victim system. The victim system will look for the application waiting on that port. When it realizes that there is no application that is waiting on the port, it generates an ICMP packet of destination unreachable to the forged source address. If flood of UDP packets are send to the victim machine, the system will surely go down [2].

B. Types of Logic Attack

i) *Ping of Death:* It's the use of ping command to exploit the fact that the maximum packet size that TCP/IP allows for being transmitted over the Internet is restricted to 65,536 octets. In this attack, the target system is pinged with a data packet that exceeds the maximum bytes allowed by TCP/IP. A simple command

C:\>ping 66000 hostname can force the system to hang or crash. Nowadays our host systems are safe from this type of attack because these attacks were prevalent in UNIX systems [2].

ii) *Teardrop Attack:* Whenever a packet is send over the Internet, it is broken down into fragments at the source system and reassembled at the destination system. An attacker sends two fragments that cannot be reassembled properly making use of a bug in the TCP/IP fragmentation re-assembly code of various operating systems by manipulating the offset value of packet and cause reboot or halt the victim system [2].

iii) *Land Attack*: An attacker sends a forged packet with the same source and destination IP address. Whenever victim system replies to that packet it actually sends that packet to itself, thus creating an infinite loop between the target system and target system itself thus causing the system to crash or reboot [2].

6 Classification of DDoS Defense Mechanisms

DDoS defense mechanisms can be classified as follows:
A. DDoS Attack Prevention: Attack prevention methods try to stop all well known signature based and broadcast based DDoS attacks from being launched in the first place or edge routers, keeps all the machines over Internet up to date with patches and fix security holes. Signature of the packets is matched with the existing database consisting of known attack patterns at each edge router [2]. To prevent the DDoS attack against target machine we have the following approaches:-

i) *Filtering* all packets entering and leaving the network protects the network from attacks conducted from neighboring networks, and prevents the network itself from being an unaware attacker. This measure requires installing ingress and egress packet filters on all routers. It is used to filter spoofed IP address but approaches to prevent it needs global implementation that is not practical [30, 31].

ii) *Firewall* can allow or deny protocols, ports or IP addresses but some complex attack like on port 80 cannot be handled by it because it is unable to distinguish between legitimate traffic and DDoS attack traffic. Only those attacks can be identified whose signatures are already there in the database. A slight variation from the original attack pattern can leave the attack undetected. Also new attacks cannot be detected [32].

iii) *Anti-DDoS HTTP Throttling:* Google has very cleverly devised a new mechanism that has made their new Google chrome browser to prevent DDoS attacks from being perpetrated, intentionally or accidentally, by web pages and extensions running within Chrome. It cannot stop someone from sending DDoS attacks to a server or website but, if a website is down because of DDoS or similar attacks, Chrome can stop it's users from sending requests (accessing) to that website for a while, thus reducing load on the server. The way this mechanism works is, once a few server errors (HTTP error codes 500 and greater) in a row have been detected for a given URL, Chrome assumes the server is either unavailable or overloaded due to a DDoS, and denies requests to the same URL for a short period of time. If, after this period of time, requests keep failing, this interval is again increased using an exponential factor, and so on and so forth until the maximum interval is reached. It's important to note that failures due to the throttling itself are not counted as failures that cause the back-off interval to be increased.

B. DDoS Detection: Attack detection aims to detect an ongoing attack as soon as possible without misclassifying and disrupting legitimate traffic. DDoS detection approaches can be classified as follows:

i) *Signature based detection:* Signature based approach employs a priori knowledge of attack signatures. The signatures are manually constructed by security experts analyzing previous attacks and used to match with incoming traffic to detect intrusions. SNORT [33] and Bro [34] are the two widely used signature based detection approaches. Signature based techniques are only effective in detecting traffic of known DDoS attacks whereas new attacks or even slight variations of old attacks go unnoticed.

ii) A*nomaly based detection:* Anomaly-based system uses a different philosophy. It treats any network connection violating the normal profile as an anomaly. A network anomaly is revealed if the incoming traffic pattern deviates from the normal profiles significantly [2]. Detecting DDoS attacks involves first knowing normal behavior of our system and then to find deviations from that behavior. Anomaly based techniques can detect novel attacks; however, it may result in higher false alarms.

C. DDoS Response:
After detecting an attack we must block the traffic from its source. Identification of source is difficult because their IP addresses are spoofed and thus difficult to trace back [2].

i) *Filtering* the malicious traffic can be done but it is really difficult to isolate the malicious packets and legitimate packets.
ii) *Rate throttling* is a measure which is used when there is high number of false positives in identifying the malicious packets. In this technique the rate of malicious traffic packets is reduced.
iii) *Passive traceback* [35-39] aims at tracking the real attacker causing the DDoS attack.

D. DDoS Attack Mitigation and Tolerance:
This aims at reducing the effect of the attack on victim machine during DDoS attack [2].

i) It can be done by using *load balancer* at the server side. Other methods can be implemented at routers like better queue management, traffic control scheduling.
ii) *Fault tolerance* is a well-developed research area whose designs are built-in in most critical infrastructures and applied in three levels: hardware, software and

system. The idea of fault tolerance is that by duplicating the network's services and diversifying its access points, the network can continue offering its services when flooding traffic congests one network link.

iii) *Quality of service* (QoS) describes the assurance of the ability of a network to deliver predictable results for certain types of applications or traffic. Many Intrusion tolerant QoS techniques and Intrusion tolerant QoS systems have been developed in order to mitigate DDoS attacks.

7 DDoS Defense Challenges and Discussion

In spite of numerous defense techniques and mechanism developed, the problem of DDoS is hardly tackled. As mentioned in [6, 40] there are various factors that are responsible for dealing with this problem:

i) The Internet security is highly interdependent; therefore, dealing with DDoS at victim side only doesn't solve the problem. If an attacker manages to exploit a legitimate machine which is authorized to communicate with victim machine, then that machine can be used to attack the victim because incoming traffic from the legitimate machine will be considered as normal traffic by the victim machine.

ii) Internet is not designed as a system to keep the track of incoming and outgoing traffic; it just designed to push packets from one hop to another.

iii) Need of a widespread and contiguous deployment of defense systems since Internet is widely distributed.

iv) Use of legitimate traffic models by attacker.

v) Internet service providers do not want to cooperate due to business purposes.

vi) Due to IP spoofing and encryption techniques between the attacker and agent machines, tracing the real attacker even after getting devastated by DDoS attack is not possible.

vii) The defense technique used may itself be able to slow down the request rate of legitimate users while filtering the traffic.

viii) The limited availability of resources is also one core reason.

We opt for a defense mechanism only after the attack has been launched. The work being carried out is mostly concentrated on developing defense mechanism [15] only after the attack is detected. We monitor the incoming traffic based on several performance metrics. But this defense mechanism mostly fails to detect the attack and the first signal of attack comes from the customer's report showing service unavailability. At that time, the victim is already under attack. Currently there are many challenges development effective DDoS defense mechanisms. These challenges include

(a) Large number of ignorant participants

(b) No common characteristics of DDoS streams

(c) Use of legitimate traffic models by attackers

(d) No administrative domain cooperation

(e) Use of automated tools

(f) Hidden identity of participants

(g) Persistent security holes on the Internet
(h) Lack of attack information, and
(i)Absence of standardized evaluation and testing approaches.

8 Conclusion and Future Work

DDoS attack has now become the number one threat to Internet in present scenarios. There is millions of dollars loss to the companies suffering from these attacks. The major challenge is to differentiate between the legitimate traffic and attack traffic. Since most of the attackers uses the legitimate attack models differentiating between the two becomes a trivial task. We know there is no one to govern over the Internet. The security of Internet is highly dependent on others. Internet needs to be more secure and users needs to be more aware about Internet security So to deploy a defense mechanism only at the victim's side alone is not going to solve this problem. We need to deploy defense techniques at every level, whether its edge router, core routers, ISP levels, etc. Moreover our effort should be more on dealing with these attacks before the actual damage has happened.

References

1. Leiner, B.M., Cerf, V.G.: A Brief History of the Internet, `http://www.isoc.org`
2. Gupta, B.B., Joshi, R.C., Misra, M.: Defending against Distributed Denial of Service Attacks: Issues and Challenges. Information Security Journal: A Global Perspective 18(5), 224–247 (2009)
3. Gupta, B.B., Misra, M., Joshi, R.C.: An ISP level Solution to Combat DDoS attacks using Combined Statistical Based Approach. International Journal of Information Assurance and Security (JIAS) 3(2), 102–110 (2008)
4. Mills, E.: Radio Free Europe DDOS attack latest by activists (May 2008), `http://news.cnet.com/8301-10784_3-9933746-7.html`, CNET News
5. Vamosi, R.: Study: DDoS attacks threaten ISP infrastructure (November 2008), `http://news.cnet.com/8301-1009_3-10093699-83.html` CNET News
6. Mirkovic, J., Reiher, P.: A taxonomy of DDoS attack and DDoS defense mechanisms. ACM SIGCOMM Computer Communications Review 34(2), 39–53 (2004)
7. Prolexic Technologies, DDOS problem, `http://www.prolexic.com/index.php/the-DDoS-problem/`
8. Gupta, B.B., Joshi, R.C., Misra, M.: Distributed Denial of Service Prevention Techniques. International Journal of Computer and Electrical Engineering (IJCEE) 2(2), 268–276 (2010) ISSN: 1793-8198
9. The ISC Internet Domain Survey, `https://www.isc.org/solutions/survey`
10. Internet World Stats, Internet User Statistics–The Big Picture: World Internet Users and Population Stats, `http://www.internetworldstats.com/stats.htm`
11. CERT Coordination Center, Denial of service attacks (March 2007), `http://www.cert.org/techtips/denialofservice.html`
12. Garber, L.: Denial-of-service attacks rip the Internet. IEEE Computer 33(4), 12–17 (2000)
13. Moore, D., Voelker, G.M., Savage, S.: Inferring Internet denial-of-service activity. In: Proceedings of the 10th USENIX Security Symposium (August 2001)

14. Sachdeva, M., Singh, G., Kumar, K., Singh, K.: DDoS Incidents and their Impact: A Review. The International Arab Journal of Information Technology 7(1), 14–20 (2010)
15. Xiang, Y., Zhou, W., Chowdhury, M.: A Survey of Active and Passive Defense Mechanisms against DDoS Attacks. Technical Report, TR C04/02, School of Information Technology, Deakin University, Australia (2004)
16. Houle, K.J., Weaver, G.M.: Trends in Denial of Service Attack Technology, CERT (October 2001), http://www.cert.org/archive/pdf/DoS_trends.pdf
17. Douligeris, C., Mitrokotsa, A.: DDoS attacks and defense mechanisms: classification and state of the art. Elsevier Science Direct Computer Networks 44, 643–666 (2004)
18. Dittrich, D.: The DoS Project's Trinoo Distributed Denial of Service attack tool, University of Washington (October 21, 1999), http://staff.washington.edu/dittrich/misc/trinoo.analysis.txt
19. Dittrich, D.: The Tribe Flood Network Distributed Denial of Service attack tool, University of Washington (October 21, 1999), http://staff.washington.edu/dittrich/misc/tfn.analysis.txt
20. Barlow, J., Thrower, W.: TFN2K- An Analysis," Axent Security Team (February 10, 2000), http://security.royans.net/info/posts/bugtraq_ddos2.shtml
21. Dittrich, D.:The Stacheldraht Distributed Denial of Service attack tool, University of Washington (December 1999), http://staff.washington.edu/dittrich/misc/stacheldraht.analysis.txt
22. Dittrich, D., Weaver, G., Dietrich, S., Long, N.: The Mstream distributed denial of service attack too (May 2000), http://staff.washington.edu/dittrich/misc/mstream.analysis.txt
23. Bysin: Knight.c sourcecode, PacketStormSecurity.nl (July 11, 2001), http://packetstormsecurity.nl/distributed/knight.c
24. Hancock, B.: "Trinity v3, a DDoS tool," hits the streets. Computers Security 19(7), 574 (2000)
25. Marchesseau, M.: Trinity-Distributed Denial of Service Attack Tool (September 11, 2000), http://www.giac.org/certified_professionals/practicals/gsec/0123.php
26. Gupta, B.B., Joshi, R.C., Misra, M.: Dynamic and Auto Responsive Solution for Distributed Denial-of-Service Attacks Detection in ISP Network. International Journal of Computer Theory and Engineering (IJCTE) 1(1), 71–80 (2009) ISSN: 1793-821X
27. Molsa, J.: Mitigating denial of service attacks: A tutorial. Journal of Computer Security 13, 807–837 (2005)
28. CERT, CERT Advisory CA-1996-21 TCP SYN Flooding and IP Spoofing Attacks (September 1996)
29. Azrina, R., Othman, R. (n.d.) Understanding the various types of denial of service attack, http://www.niser.org.my/resources/dos_attack.pdf
30. Park, K., Lee, H.: On the effectiveness of route-based packet filtering for distributed DoS attack prevention in power-law Internets. In: Proceedings of the ACM SIGCOMM 2001 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications, pp. 15–26. ACM Press, New York (2001)

31. Peng, T., Leckie, C., Ramamohanarao, K.: Protection from distributed denial of service attack using history-based IP filtering. In: Proceedings of IEEE International Conference on Communications (ICC 2003), Anchorage, AL, vol. 1, pp. 482–486 (2003)
32. McAfee (n.d.) Personal Firewall, http://www.mcafee.com/myapps/firewall/ov_firewall.asp
33. Roesch, M.: Snort-Lightweight Intrusion Detection for Networks. In: Proceedings of the USENIX Systems Administration Conference (LISA 1999), pp. 229–238 (November 1999)
34. Paxson, V.: Bro: A System for Detecting Network Intruders in Real-Time. International Journal of Computer and Telecommunication Networking 31(24), 2435–2463 (1999)
35. Stone, R.: CenterTrack: An IP Overlay Network for Tracking DoS Floods. In: 9th Usenix Security Symposium, pp. 199–212 (August 2000)
36. Burch, H., Cheswick, B.: Tracing Anonymous Packets to Their Approximate Source. In: Proceedings of the 14th Systems Administration Conference (LISA 2000), New Orleans, Louisiana, USA (December 2000)
37. Bellovin, S.M.: ICMP Traceback Messages, Internet Draft, Network Working Group (2000)
38. Mankin, A., Massey, D., Wu, C.-L., Felix Wu, S., Zhang, L.: On Design and Evaluation of Intention-Driven ICMP Traceback. In: Proceedings of Computer Communications and Networks (2001)
39. Wang, B., Schulzrinne, H.: A Denial-of-Service-Resistant IP Traceback Approach. In: 3rd New York Metro Area Networking Workshop, NYMAN 2003 (2003)
40. Kumar, K., Joshi, R.C., Singh, K.: An Integrated Approach for Defending against Distributed Denial-of- Service (DDoS) Attacks. In: Proceedings of IRISS-2006, IIT Madras (2006), http://www.cs.iitm.ernet.in/~iriss06/iitr_krishan.pdf