Volume 4, Issue 7, July 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

A Protective Model of Distributed Denial-of-Service in Internet For Lack of Variations

[1]**Mohd Imran** (M-Tech, CSE)
Tula's Institute, The Engineering
& Management College
India

[2]**Mr.Shashi Bhushan** (Asst Prof)
Tula's Institute, The Engineering
& Management College
India

[3]**Ms. Anuja Sharma** (M.Tech ,CS)
BM College of Technology
& Management
India

Abstract: Now a day's Internet is essential part of our life but due to Distributed Denial-of-Service (DDoS) attacks it's have some critical problems. Distributed Denial of Service (DDoS) attacks have emerged as a popular means of causing mass targeted service disruptions, often for extended periods of time. The memory less feature of the Internet routing mechanisms makes it extremely hard to trace back to the source of these attacks. As a result, there is no effective and efficient method to deal with this issue so far. Since the increasing popularity of web-based applications has led to several critical services being provided over the Internet, it is imperative to monitor the network traffic so as to prevent malicious attackers from depleting the resources of the network and denying services to legitimate users. In this paper, we propose a novel trace back method for DDoS attacks that is based on entropy variations between normal and DDoS attack traffic, which is fundamentally different from commonly used packet marking techniques. To cater to different scenarios, the detection algorithm has various modules with varying level of computational and memory overheads for their execution. In comparison to the existing DDoS trace back methods, the proposed strategy possesses a number of advantages—it is memory non intensive, efficiently scalable, robust against packet pollution, and independent of attack traffic patterns.

Keywords: Distributed Denial of Service (DDoS), Traffic Flow, Buffer, Poisson Arrival, Queuing Model, PTraceback, and Prevention.

I. INTRODUCTION

A revolution came into the world of computer and communication with the advent of Internet. Today, Internet has become increasingly important to current society. It is changing our way of communication, business mode, and even everyday life [1]. Almost all the traditional services such as banking, power, medicine, education and defense are extended to Internet now. The impact of Internet on society can be seen from the fig. 1 which shows exponential increase in number of hosts interconnected through Internet [2]. Internet usage is growing at an exponential rate as organizations, governments and citizens continue to increase their reliance on this technology. Unfortunately with an increase in number of host, count of attacks on Internet has also increased incredibly fast. According to [3], a mere 171 vulnerabilities were reported in 1995, which boomed to 7236 in 2007. Already, the number for the same for merely the third quarter of 2008 has gone up to 6058. Apart from these, a large number of vulnerabilities go unreported every year. In particular, today DoS attack is one of the most common and major threat to the Internet. In DoS attack, goal of the attacker is to tie up chosen key resources at the victim, usually by sending a high volume of seemingly legitimate traffic requesting some services from the victim. It reveals big loopholes not only in specific applications, but also in the entire TCP/IP protocol suite. DoS attack is considered to take place only when access to a computer or network resource is intentionally blocked or degraded as a result of malicious action taken by another user [4]. A DDoS attacker uses many machines to launch a coordinated DOS attack against one or more targets [5]. It is launched indirectly through many compromised computing systems by sending a stream of useless aggregate traffic meant to explode victim resources. As a side effect, they frequently create network congestion on the way from a source to the target, thus disrupting normal Internet operation. The number of DDoS attack has been alarmingly increasing for the last few years [6]. Many of today's DDoS attacks are carried out by organized criminals targeting financial institutions, e-commerce, gambling sites etc [7]. A classification of a wide range of DDoS attacks found in the wild is presented in [4, 8] that Internet providers and users need to be aware of. Usually, it can be launched in two forms [9]. The first form is to exploit software vulnerabilities of a target by sending malformed packets and crash the system. The second form is to use massive volumes of legitimate looking but garbled packets to clogs up computational or communication resources on the target machine so that it cannot serve its legitimates users. The resources consumed by attacks include network bandwidth, disk space, CPU time, data structures, network connections, etc. While it is possible to protect the first form of attack by patching known vulnerabilities, the second form of attack cannot be so easily prevented. The targets can be attacked simply because they are connected to the public Internet.

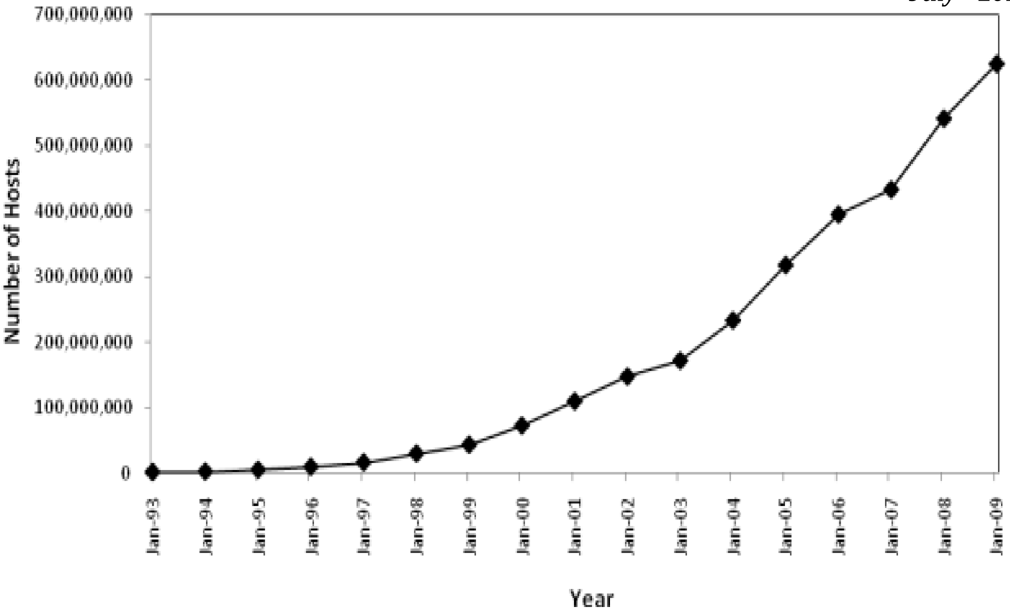

Fig. 1 Internet Domain Survey Host Count

Manuscript received April 1, 2009. This work was supported in part by the Ministry of Human Resource Development, Government of India. B. B. Gupta is with the Department of Electronics & Computer Engg., Indian Institute of Technology, Roorkee, 247667 India. (phone: +91-9927713132; e-mail: bbgupta@ieee.org). R. C. Joshi is with the Department of Electronics & Computer Engg., Indian Institute of Technology, Roorkee, 247667 India. Manoj Misra is with the Department of Electronics & Computer Engg., Indian Institute of Technology, Roorkee, 247667 India.

It has been a major threat to the Internet since year 2000, and a recent survey [1] on the largest 70 Internet operators in the world demonstrated that DDoS attacks are increasing dramatically, and individual attacks are more strong and sophisticated.

Furthermore, the survey also found that the peak of 40 gigabit DDoS attacks nearly doubled in 2008 compared with the previous year. The key reason behind this phenomena is that the network security community does not have effective and efficient traceback methods to locate attackers as it is easy for attackers to disguise themselves by taking advantages of the vulnerabilities of the World Wide Web, such as the dynamic, stateless, and anonymous nature of the Internet [2], [3]. IP trace back means the capability of identifying the actual source of any packet sent across the Internet. Because of the vulnerability of the original design of the Internet, we may not be able to find the actual hackers at present. In fact, IP trace back schemes are considered successful if they can identify the zombies from which the DDoS attack packets entered the Internet. Research on DDoS detection [4], [5], [6], [7], [8], [9], mitigation [10], [11],[12], and filtering [13], [14], [15], [16], [17], [18] has been conducted pervasively. However, the efforts on IP trace back are limited.

II. DDOS OVERVIEW

A Distributed Denial of Service attack is commonly characterized as an event in which a legitimate user or organization is deprived of certain services, like web, email or network connectivity, that they would normally expect to have. DDoS is basically a resource overloading problem. The resource can be bandwidth, memory, CPU cycles, file descriptors, buffers etc. The attackers bombard scare resource either by flood of packets or a single logic packet which can activate a series of processes to exhaust the limited resource [20]. In the Fig. 2 simplified Distributed DoS attack scenario is illustrated. The figure shows that attacker uses three zombie's to generate high volume of malicious traffic to flood the victim over the Internet thus rendering legitimate user unable to access the service. **Fig. 2** Illustration of the DDoS attack scenario Extremely sophisticated, user friendly, automated and powerful DDoS toolkits are available for attacking any victim, so expertise is not necessarily required that attract naive users to perform DDoS attacks. Although DoS attacking strategies differ in time, studies show that attackers mainly target the following resources to cause damage on victim [8, 21].

A. Network bandwidth resources

This is related with the capacity of the network links connecting servers to the wider Internet or connectivity between the clients and their Internet Service Providers (ISP). Most of the time, the bandwidth of client's internal network is less than its connectivity with the external network. Thus the traffic that comes from the Internet to the client may consume the entire bandwidth of the client's network. As a result, a legitimate request will not be able to get service from the targeted network. In a DoS attack, the vast majority of traffic directed at the target network is malicious; generated either directly or indirectly by an attacker. These attacks prevented 13,000 Bank of America ATM from providing withdrawn services and paralyzed such large ISPs as Freetel, SK Telecom, and KoreaTelecom on January 25, 2003.

I) System memory resources: An attack targeting system memory resources typically aims to crash its network handling software rather than consuming bandwidth with large volume of traffic. Specific packets are sent to confuse the operating system or other resources of the victim's machine. These include temporary buffer used to store arriving packets, tables of open connections, and similar memory data structures. Another system resource attack uses packets whose structures trigger a bug in the network software, overloading the target machine or disabling its communication mechanism or making a host crash, freeze or reboot which means the system can no longer communicate over the network until the software is reloaded.

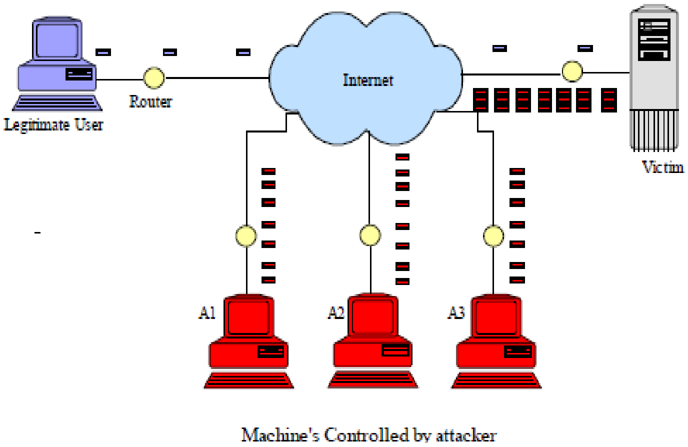

Fig. 2 Illustration of the DDoS attack scenario

II) System CPU resources/ Computational Capacity: An attack targeting system's CPU resources typically aims to employ a sequence of queries to execute complex commands and then overwhelmed the CPU. The Internet key Exchange protocol (IKE) is the current IETF standard for key establishment and SA parameter negotiation of IPsec. However, IKE's aggregate mode is still very susceptible to DoS attacks against both computational and memory resources because the server has to create states for SA and compute Diffie-Hellman exponential generation [22].

III. CLASSIFICATION OF DDOS PREVENTION MECHANISM

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. Attack prevention schemes are not enough to stop DDoS attacks because there are always vulnerable to novel and mixed attack types for which signatures and patches are not exist in the database.

Techniques for preventing against DDoS can be broadly divided into two categories: (i) General Techniques, which are some common preventive measures [31] i.e. system protection, replication of resources etc. that individual servers and ISPs should follow so they do not become part of DDoS attack process. (ii) Filtering Techniques, which include ingress filtering, egress filtering, router based packet filtering, history based IP filtering, SAVE protocol etc.

A. General Techniques

I) Disabling unused services: The less there are applications and open ports in hosts, the less there are chance to exploit vulnerabilities by attackers. Therefore, if network services are not needed or unused, the services should be disabled to prevent attacks, e.g. UDP echo, character generation services [31].

II) Install latest security patches: Today, many DDoS attacks exploit vulnerabilities in target system. So removing known security holes by installing all relevant latest security patches prevents re-exploitation of vulnerabilities in the target system [31].

III) Disabling IP broadcast: Defense against attacks that use intermediate broadcasting nodes e.g. ICMP flood attacks, Smurf attacks etc. will be successful only if host computers and all the neighboring networks disable IP broadcast [32].

IV) Firewalls: Firewalls can effectively prevent users from launching simple flooding type attacks from machines behind the firewall. Firewalls have simple rules such as to allow or deny protocols, ports or IP addresses. But some complex attack e.g. if there is an attack on port 80 (web service), firewalls cannot prevent that attack because they cannot distinguish good traffic from DoS attack traffic [24, 25].

V) Global defense infrastructure: A global deployable defense infrastructure can prevent from many DDoS attacks by installing filtering rules in the most important routers of the Internet. As Internet is administered by various autonomous systems according their own local security policies, such type of global defense architecture is possible only in theory [31].

VI) IP hopping: DDoS attacks can be prevented by changing location or IP address of the active server proactively within a pool of homogeneous servers or with a pre-specified set of IP address ranges [31]. The victim computer's IP address is invalidated by changing it with a new one. Once the IP addresses change is completed all internet routers will be informed and edge routers will drop the attacking packets. Although this action leaves the computer vulnerable because the attacker can launch the attack at the new IP address, this option is practical for DDoS attacks that are based on IP addresses. On the other hand, attackers can make this technique useless by adding a domain name service tracing function to the DDoS attack tools.

B. Filtering Techniques

I) Ingress/Egress filtering : Ingress Filtering, proposed by Ferguson et al. [33], is a restrictive mechanism to drop traffic with IP addresses that do not match a domain prefix connected to the ingress router. Egress filtering is an outbound filter, which ensures that only assigned or allocated IP address space leaves the network. A key requirement for ingress or egress filtering is knowledge of the expected IP addresses at a particular port. For some networks with complicated topologies, it is not easy to obtain this knowledge.

One technique known as reverse path filtering [34] can help to build this knowledge. This technique works as follows. Generally, a router always knows which networks are reachable via any of its interfaces. By looking up source addresses of the incoming traffic, it is possible to check whether the return path to that address would flow out the same interface as the packet arrived upon. If they do, these packets are allowed. Otherwise, they are dropped.

Unfortunately, this technique cannot operate effectively in real networks where asymmetric Internet routes are not uncommon. More importantly, both ingress and egress filtering can be applied not only to IP addresses, but also protocol type, port number, or any other criteria of importance. Both ingress and egress filtering provide some opportunities to throttle the attack power of DoS attacks. However, it is difficult to deploy ingress/egress filtering universally. If the attacker carefully chooses a network without ingress/egress filtering to launch a spoofed DoS attack, the attack can go undetected. Moreover, if an attack spoofs IP addresses from within the subnet, the attack can go undetected as well. Nowadays DDoS attacks do not need to use source address spoofing to be effective. By exploiting a large number of compromised hosts, attackers do not need to use spoofing to take advantage of protocol vulnerabilities or to hide their locations. For example, each legitimate HTTP Web page request from 10,000 compromised hosts can bypass any ingress/egress filtering, but in combination they can constitute a powerful attack. Hence, ingress and egress filtering are ineffective to stop DDoS attacks.

II) Router based packet filtering: Route based filtering, proposed by Park and Lee [35], extends ingress filtering and uses the route information to filter out spoofed IP packets. It is based on the principle that for each link in the core of the Internet, there is only a limited set of source addresses from which traffic on the link could have originated.

If an unexpected source address appears in an IP packet on a link, then it is assumed that the source address has been spoofed, and hence the packet can be filtered. RPF uses information about the BGP routing topology to filter traffic with spoofed source addresses. Simulation results show that a significant fraction of spoofed IP addresses can be filtered if RPF is implemented in at least 18% of ASs in the Internet. However, there are several limitations of this scheme. The first limitation relates to the implementation of RPF in practice.

III) History based IP filtering: Generally, the set of source IP addresses that is seen during normal operation tends to remain stable. In contrast, during DoS attacks, most of the source IP addresses have not been seen before. Peng et al. relies on the above idea and use IP address database (IAD) to keep frequent source IP addresses. During an attack, if the source address of a packet is not in IAD, the packet is dropped. Hash based/Bloom filter techniques are used for fast searching of IP in IAD. This scheme is robust, and does not need the cooperation of the whole Internet community [36].

However, history based packet filtering scheme is ineffective when the attacks come from real IP addresses. In addition, it requires an offline database to keep track of IP addresses. Therefore, Cost of storage and information sharing is very high.

IV. FEATURE BASED DETECTION METHODS

A common methodology for anomaly detection is to identify normal patterns of the study objects, and an action out of the normal patterns is treated as an anomaly. This method has been widely applied in various security detection. We note that this strategy inherits false negative and false positive by its nature.

A. Profile Based Detection

A common strategy to disguise attack sources is IP spoofing. In order to fight against source IP spoofing, a hop-count filter is an effective method. Wang, Jin and Shin [2] found that a hacker cannot falsify the number of hops an IP packet takes to reach its destination although he can forge any field in the IP header. Moreover, a receiver can infer the hop-count information based on the Time-to-Live field of the IP header. At the same time, it is easy for a Internet server to establish a table of IP address and their related hop-counts for its legitimate clients, which is called IP-to-hop-count (IP2HC) mapping table. Based on this table, defenders can therefore discriminate spoofed IPs from legitimate IPs

B. Low Rate DDoS Attack Detection

Low rate DDoS attack is also called shrew DDoS attack, which features with a low attack rate, and it is hard to detect it [28]. Due to the mechanism of low rate DDoS attacks, they inherent a specific characteristic: they submit attack packets periodically. Based on this feature, Chen and Hwang [1] proposed a spectral analysis method to detect this kind of low rate attacks.

V. CONCLUSIONS AND FUTURE SCOPE

DoS attack causes either disruption or degradation on victim's shared resources, as a result preventing legitimate users from their access right on those resources. DoS attack may target on a specific component of computer, entire computer system, certain networking infrastructure, or even entire Internet infrastructure. Attacks can be either by exploits the natural weakness of a system, which is known as logical attacks or overloading the victim with high volume of traffic, which is called flooding attacks. A distributed form of DoS attack called DDoS attack, which is generated by many compromised machines to coordinately hit a victim. DDoS attacks are adversarial and constantly evolving. Once a particular kind of attack is successfully countered, a slight variation is designed that bypasses the defense and still performs an effective attack.

In this paper, we covered an overview of the DDoS problem, available DDoS attack tools, defense challenges and principles, and a classification of available DDoS prevention mechanisms. This provides better understanding of the problem and enables a security administrator to effectively equip his arsenal with proper prevention mechanisms for fighting against DDoS threat. The current prevention mechanisms reviewed in this paper are clearly far from adequate to protect Internet from DDoS attack. The main problem is that there are still many insecure machines over the Internet that can be compromised to launch large-scale coordinated DDoS attack. One promising direction is to develop a comprehensive solution that encompasses several defense activities to trap variety of DDoS attack. If one level of defense fails, the others still have the possibility to defend against attack. A successful intrusion requires all defense level to fail.

REFERENCES

[1] Leiner, B. M., Cerf, V. G., et. al. (2003). A Brief History of the Internet. Internet Society. http://www.isoc.org.

[2] The ISC Internet Domain Survey. https://www.isc.org/solutions/ survey.

[3] Leiner, B. M., Cerf, V. G., et. al. (2003). A Brief History of the Internet. Internet Society. http://www.isoc.org.

[4] The ISC Internet Domain Survey. https://www.isc.org/solutions/ survey.

[5] CERT statistics. Available at: http://www.cert.org/stats/cert_stats. html.

[6] C. Douligeris, A. Mitrokotsa, "DDoS attacks and defense mechanisms: classification and state-of-the-art," Computer Networks, Volume 44, Issue 5, pp. 643-666, April 2004.

[7] C. Douligeris, A. Mitrokotsa, "DDoS attacks and defense mechanisms: classification," in Proceedings of the 3rd IEEE International Symposium on Signal Processing and Information
Technology (ISSPIT 03), Darmstadt, Germany, pp. 190-193, Dec. 14-17, 2003.

[8] D. Moore, C. Shannon, D. J. Brown, G. Voelker, S. Savage. "Inferring Internet Denial-of-Service Activity", ACM Transactions on Computer Systems, 24 (2), pp 115-139, 2006.

[9] Juniper Network, "Combating Bots and Mitigating DDoS Attacks (Solution brief)", Juniper Networks, Inc, 2006.

[10] J. Mirkovic, P. Reiher, "A Taxonomy of DDoS Attack and DDoS defense Mechanisms," ACM SIGCOMM Computer Communications Review, Volume 34, Issue 2, pp. 39-53, April 2004.

[11] J. Molsa, "Mitigating denial of service attacks: A tutorial," Journal of computer security, 13, pp. 807-837, IOS Press, 2005.

[12] L. Garber, "Denial-of-service attacks rip the Internet," IEEE Computer, Volume 33, Issue 4, pp. 12–17, Apr. 2000.

[13] D. Dittrich, "The DoS Project's Trinoo Distributed Denial of Service attack tool," University of Washington, October 21, 1999. Available at: http://staff.washington.edu/dittrich/misc/ trinoo.analysis.txt.

[14] D. Dittrich, "The Tribe Flood Network Distributed Denial of Service attack tool," University of Washington, October 21, 1999. Available at: http://staff.washington.edu/dittrich/misc/tfn.analysis.txt.

[15] J. Barlow, W. Thrower, "TFN2K- An Analysis," Axent Security Team. February 10, 2000. Available at: http://security.royans.net/info/posts/bugtraq_ddos2.shtml.

[16] D. Dittrich, "The Stacheldraht Distributed Denial of Service attack tool," University of Washington, December 1999. Available at: http://staff.washington.edu/dittrich/misc/stacheldraht.analysis.txt.

[17] S. Dietrich, N. Long, D. Dittrich, "Analyzing Distributed Denial of Service tools: The Shaft Case," in Proceedings of the 14th Systems Administration Conference (LISA 2000), New Orleans, LA, USA, pp. 329-339, December 3–8, 2000.

[18] D. Dittrich, G. Weaver, S. Dietrich, and N. Long, "The "Mstream" distributed denial of service attack too," May 2000. Available at: http://staff.washington.edu/dittrich/misc/mstream.analysis.txt.

[19] Bysin, "Knight.c sourcecode," PacketStormSecurity.nl, July 11, 2001. Available at: http://packetstormsecurity.nl/distributed/ knight.c.

[20] B. Hancock, "Trinity v3, a DDoS tool," hits the streets, Computers Security 19(7), pp. 574, 2000.

[21] M. Marchesseau, „Trinity-Distributed Denial of Service Attack Tool," 11 Sept, 2000. Available at:

http://www.giac.org/ certified_professionals/practicals/gsec/0123.php.

[22] K. Kumar, R.C. Joshi and K. Singh, "An Integrated Approach for Defending against Distributed Denial-of-Service (DDoS) Attacks", iriss, 2006, IIT Madras.

[23] B. Wang, H. Schulzrinne, "Analysis of Denial-of-Service Attacks on Denial-of-Service Defensive Measures", GLOBECOM 2003, pp. 1339-43

[24] S. Bellovin, M. Blaze, R. Canetti, J. Ioannidis, A.D. Keromytis, O. Reingold, "Efficient, DoS-resistant, secure key exchange for Internet protocols," In Proceedings of the 2001 Security Protocols International Workshop, April 2001, Cambridge, England.

[25] S Hazelhurst, "Algorithms for Analysing Firewall and Router Access Lists", In proceddings of workshop on dependable IP systems and plateforms (ICDSN), 2000.

[26] R. Oppliger, "Internet Security: firewall and beyond," Communications of the ACM, Volume 40, Issue 5, pp. 92-102, 1997.

[27] McAfee, "Personal Firewall". Available at: http://www.mcafee.com/ myapps/ firewall/ov_firewall.asp.

[28] Debar H, Dacier M, Wespi A, "Towards a taxonomy of intrusion detection systems", Computer Networks, Vol. 31, 1999.

[29] Bai, Y. Kobayashi, H., "Intrusion Detection System: Technology and Development", in the Proceedings of the 17th International Conference on Advanced Information Networking and Applications (AINA), pp. 710-715, march, 2003.

[30] K. Kumar, R.C. Joshi and K. Singh, "An Integrated Approach
for Defending against Distributed Denial-of-Service (DDoS) Attacks," IRISS, 2006, IIT Madras. Available at: www.cs.iitm.ernet.in/~iriss06/ iitr_krishan.pdf.

[31] M. Robinson, J. Mirkovic, M. Schnaider, S Michel, and P. Reiher, "Challenges and principles of DDoS defense," SIGCOMM, 2003.

[32] U.K.Tupakula, V.Varadharajan "A Practical Method to Counteract Denial of Service Attacks", Proceedings of the Twenty-Sixth Australasian Conference on Computer Science, ACSC2003, Springer Verlag, Australia. (Feb 2003).

[33] X. Geng, A.B. Whinston, Defeating Distributed Denial of Service attacks, IEEE IT Professional 2 (4) (2000) 36–42.

[34] Felix Lau, Rubin H. Stuart, Smith H. Michael, and et al., "Distributed Denial of Service Attacks," in Proceedings of 2000 IEEE International Conference on Systems, Man, and Cybernetics, Nashville, TN, Vol.3, pp.2275-2280, 2000.

[35] P. Ferguson, and D. Senie, "Network ingress filtering: Defeating denial of ser-vice attacks which employ IP source address spoofing," RFC 2267, the Internet Engineering Task Force (IETF), 1998.

[36] Baker, F. "Requirements for IP version 4 routers," RFC 1812, Internet Engineering Task Force (IETF).Go online to www.ietf.org.

[37] K. Park, and H. Lee, "On the effectiveness of router-based packet filtering for distributed DoS attack prevention in power-law Internets," Proceedings of the ACM SIGCOMM Conference, 2001, pp. 15-26, 2001.

[38] T. Peng, C. Leckie, K. Ramamohanarao, "Protection from Distributed Denial of Service attack using history-based IP filtering," in Proceedings of IEEE International Conference on Communications (ICC 2003), Anchorage, AL, USA, Volume 1, pp. 482-486, 2003.