Deployment of Distributed Defense against DDoS Attacks in ISP Domain

Monika Sachdeva
Assistant Professor
SBS College of Engg. & Technology, Ferozepur, Punjab, India.

Gurvinder Singh
Associate Professor
Guru Nanak Dev University, Amritsar, Punjab, India.

Krishan Kumar
Associate Professor.
SBS College of Engineering & Technology, Ferozepur, Punjab, India.

ABSTRACT
Distributed Denial of Service attacks pose a serious threat to the online applications like banking, trade, and e-commerce which are dependent on availability of Internet. Defending Internet from these attacks has become the need of the hour for sustainable development of any economy. Most of the research work in this area focuses on developing defense against these attacks without considering its practical deployment on the Internet. They evaluate the defense through simulation or experimenting in controlled environments. However a sincere thought is required to deploy these defense mechanisms in an incrementally acceptable way on the Internet. In this paper, the focus is on deployment aspect of defense system against DDoS attacks. The DDoS defense system in general is anatomized and need for distributed defense as compared to centralized defense has been highlighted. All possible defense locations on the Internet are critically analyzed for suitability of DDoS defense system deployment. A review of existing distributed defense schemes in terms of deployment is also carried out. Based on Internet structure, its working, and desired DDoS defense characteristics, ISP domain is chosen for deployment. However extending cooperation among ISPs and secure framework for communication among ISPs remain future concerns of our work.

General Terms
Network Security, Distributed Systems.

Keywords
DDoS, Centralized defense, Distributed Defense, Deployment, Detection, Response.

1. INTRODUCTION
In the present era, an increasing number of critical services like e-commerce, banking, trade, social activities and mail discussions are motivated to use the Internet for daily operations. Thus Internet has come up as a critical resource whose disruption induces financial implications or even dire consequences on humanity. Technically Internet design follows the end-to-end paradigm [1]. The end hosts deploy intelligence in terms of complex functionalities to achieve desired service guarantees, while the intermediate network which is full of resources provides the bare-minimum, best-effort service. Thus there is intelligence and resource asymmetry on the Internet. Such design opens several security issues that provide opportunities for various kinds of attacks on the Internet. Internet security includes aspects such as confidentiality, authentication, message integrity and non repudiation [2, 3]. One of the main aspects of Internet security is availability. DDoS attacks pose a big threat to availability of services on the Internet.

According to the WWW Security FAQ [4] a DoS attack can be described as an attack designed to render a computer or network incapable of providing normal services. Especially it is against the frequently visited web sites of a number of high-profile companies [3] or governments. In Distributed Denial of Service (DDoS) attacks scenario, the attacks become coordinated and come from multiple sources at the same time [5], thus are even more devastating. In order to launch a DDoS attack, the attacker first scan millions of machines for vulnerable service and other weakness, then gain access and compromise these zombies or slave machines. These infected machines can recruit more zombies. When the assault starts, the real attacker hides the identity and sends orders to zombies to perform the attacks. The attackers are not going to thieve, modify or remove the information exchanged on networks, but they attempt to impair a network service, thus to block legitimate users from accessing the service. As per CSI/FBI report, DDoS attacks have incurred 100 billion dollar loss from 2006 to 2009 [6].

A lot of work has been already done to combat DDoS attacks [7-16]. An excellent review of existing techniques is also available in [7-8]. However in the existing work, classification of DDoS defense techniques based on placement of component modules is not done, which is very essential to devise robust solutions. In this paper an effort has been made to identify appropriate locations on the Internet for placement of DDoS defense. It has been found that ISP domain is the best place for deploying DDoS defense as it has infrastructure as well as autonomous control, required to fight against DDoS attacks. The organization of rest of the paper is as follows:-

In section 2, possible locations for placement of DDoS defense are explored. Section 3 highlights characteristics of an ideal DDoS defense. In section 4, need of distributed defense is discussed. Moreover existing distributed defense techniques are critically reviewed in terms of locations of defense. In section 5, a practical DDoS deployment scenario is devised. Finally section 6 concludes the paper.

2. POSSIBLE LOCATIONS FOR PLACEMENT OF DDOS DEFENSE TECHNIQUES
A typical DDoS defense system consists of detection of attack, characterization of attack sources, and rate limiting filtering of attack traffic. The process of identifying that a network or

server is under attack after launch of attack is called detection. Characterization means differentiating attack traffic from legitimate traffic. Rate limiting and Filtration is used to mitigate DDoS traffic so that legitimate traffic should not suffer. The placement of DDoS defense logic at a particular point of the Internet is an important concern, as Internet has decentralized management [17].

On the Internet, DDoS attack streams originate from geographically distributed machines, are forwarded by core routers and converge at the victim network. There is interaction of three types of networks: source networks that unwittingly host attack machines, several intermediate networks that forward attack traffic to the victim, and the victim network that hosts the target. Figure 1 depicts this interaction [8]. Each of the involved networks i.e. source, intermediate, and victim can host DDoS defense systems. Here we have analyzed feasibility of DDoS defense deployed at each of these individual points.

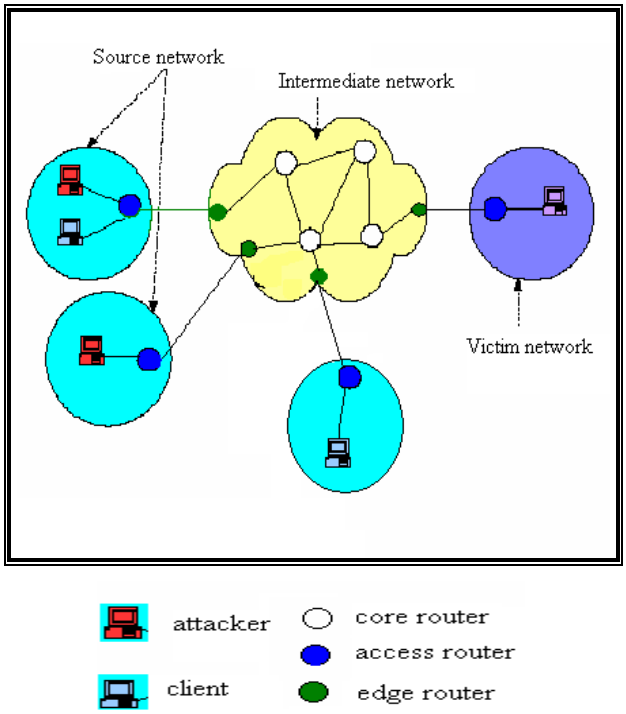

Figure 1: Points of DDoS defense

Historically, most of existing DDoS defending systems: resource accounting [18, 19, 20, 21, and 22] and protocol security mechanisms [23, 24, 25, and 26] have been designed to work on the victim side. DDoS attacks have maximum impact on the victim, so the motivation for DDoS defense deployment on the victim side is also justified. However, under a sustained high bandwidth DDoS attack, it is not possible to contain the attack at border gateway and/or firewall [27] in the victim side. The offending packets actually consume the finite bandwidth available on the connection to the ISP. Therefore, the legitimate packets are not able to even reach at the victim side. Hence, filtering on victim side has no meaning as it cannot protect legitimate traffic. Table 1 summarizes the advantages/disadvantages and technical challenges of victim network defense.

Prevention methods, such as Ingress/Egress Filtering [28] and repairing security holes [29], are implemented at source networks to stop origin of DDoS traffic. Absence of incentives, per packet filtering overheads, and security measures awareness stand in the way of DDoS defense deployed at the source network. D-WARD [7] is also a source-end defense scheme. It faces two hard challenges. First, in a highly distributed attack (i.e. isotropic DDoS attack), each source network is responsible for only a small fraction of the attack traffic, which is unlikely to generate anomalous statistics. Secondly, a witty DDoS attacker can also control the attack traffic from each source network to be within normal range because ultimately it is the aggregation of attack traffic and not individual source traffic which is going to inflict damage to the victim. Moreover, the biggest problem in source-end defense is requirement of global deployment which is impossible to achieve as Internet has no central control. Moreover motivation for source deployment is also low because it is unclear who would pay the expenses associated with this service. Table 1 summarizes the advantages/disadvantages and technical challenges of source network defense.

Many solutions, such as pushback [14], SOS [9], and traceback [30, 31, 32, 33, and 34] are deployed at the intermediate network i.e. in the core of Internet. They all put burden on core routers, which are meant for forwarding packets at high speeds as per Internet design. Besides, intermediate network is not owned by single administrative domain. So, establishing cooperation and trust relationships between different domains, such that requests originating from one domain will be honored by the other or the module to be installed in other domain will be allowed, are the concerns that have practically no answer. However DDoS defense mechanisms deployed at the intermediate network are more effective than a victim network based mechanisms since the attack traffic can be handled easily and origin of the attack can also be traced [35]. DDoS defense mechanisms provide infrastructural service to a large number of Internet hosts. Victims of DDoS attacks can contact the infrastructure and request the service, possibly providing adequate compensation. Table 1 compares the advantages/disadvantages and technical challenges of source, victim and intermediate network defense.

The technical challenges manifested in table 1 clearly highlight the gravity of the DDoS defense problem. Moreover viability of various DDoS defense modules with their vulnerability and relative deployment possibility are also explored in table 2 at all possible location.

Table 1: Comparison of various deployment locations

Deployment	Main features	Advantages	Disadvantages	Technical Challenges
Source Network [7][28][29][36]	Both detection component and defeating component are deployed at the source end of attacking	- Filter attack traffic before it reaches target. Limited collateral damage -Detects attacks as soon as possible -Avoid overall network congestion as Stops attack traffic from polluting the entire Internet, an ideal scenario -Computation requirements of this solution is low -Low vulnerability of this solution	-Very difficult to deploy as all networks cannot deploy unless enforced by legislation. -Lack of coordination -Less sensitive to catch attack signals -ISP's need to be financially motivated -Many deployment points needed for high efficacy	How to detect an attack at the source without traffic aggregation
Victim Network [18][19], [20],[21],[22] [37] [38]	Used to protect a set of host from being attacked	- Most suitable for victim as it has to suffer losses due to attacks -DDoS attacks are easily detected due to huge volume of traffic -Its deployment cost is low as it is to be deployed at victim network.	-Computationally expensive due to high volume of traffic -Sometimes defense itself is vulnerable to DDoS attack due to high volume of data -Filtering attack traffic is computationally expensive -Response is manual	-Protection of legitimate traffic -Generating automatic attack alerts
Intermediate network [8] [9] [10][14][31][32] [33]	A set of detection systems distributed in network	-Better infrastructure available for deploying detection sensors and filtering attack traffic	--Possible performance degradation -Interdomain politics of isolation -Attack detection is hard	-Communication between defense modules should be secured

Table 2: Viability of DDoS defense at different deployment locations

Deployment	Detection/ Characterization	Rate Limiting/ Filtering	Defense Vulnerability/ Robustness	Deployment difficulty
Source Network	Very difficult	Easy	Low	Highly difficult
Victim Network	Easy	Difficult	High	Very Easy
Intermediate Network	Difficult	Difficult	Medium	Difficult

3. CHARACTERISTICS OF AN IDEAL DDOS DEFENSE SYSTEM

In the previous section table 1 and table 2 clearly identified advantages/disadvantages, technical challenges and viability of DDoS defense at source, victim and intermediate network. Now the objective is to find characteristics of an ideal DDoS defense system so that a viable deployment location can be finalized. Following are the characteristics [8] of an ideal DDoS defense system:-

1. Deployment should be economical as far as possible.
2. Deployment should be practical.
3. There should be autonomous control for deployment.
4. Defense modules should be robust.
5. Computational complexity should be low.
6. Detection accuracy should be high
7. Collateral damage should be minimal.
8. Availability of High infrastructure against voluminous DDoS attacks

All possible deployment locations are compared based on ideal characteristics of a DDoS defense in table 3 given below:-

Table 3: Comparison of deployment locations based on ideal DDoS defense characteristics

	Source Network	Victim Network	Intermediate Network
Economical		✓	✓
Practical		✓	
Autonomous Control		✓	
Robustness	✓		✓
Low Computational complexity	✓		✓
High Detection Accuracy		✓	
Low Collateral Damage	✓		
High Infrastructure Availability			✓

As we can see from above table that, detection accuracy is high at the victim end but it is not robust, it will succumb to high volume of DDoS traffic. Collateral damage is low at the source end but it is not practical due to requirement of global deployment. In intermediate network, although high infrastructure is available but Response(eliminate attack traffic) is likely to inflict collateral damage, because core routers can only accommodate simple rate limiting requests and cannot dedicate memory or processor cycle to traffic profiling.

So it is evident that no single deployment point can achieve successful defense. Distributed Defense deployment is the best way to combat DDoS Attacks. It consists of multiple defense nodes (with semi functionality) deployed at various locations and organized as network. Traffic Monitoring, Traffic Analysis, and Traffic Filtering are the three main modules in any comprehensive DDoS solution. In next section, we will discuss need of Distributed DDoS defense and compare it with centralized DDoS defense.

4. DISTRIBUTED DEFENSE AND ITS DEPLOYMENT AGAINST DDOS ATTACKS

A comprehensive DDoS solution requires three effective modules namely traffic monitoring, traffic analysis, and attack traffic filtering [7-8]. In a centralized solution all the modules are deployed at same place whereas voluminous and distributed nature of DDoS traffic demands a distributed DDoS solution because centralized solutions cannot handle high overheads of monitoring, analyzing and filtering. Components of distributed defense system are deployed at different locations and cooperate with each other to defend from the attacks. Compared with the centralized defense systems, distributed defense systems can discover and fight the attacks with more resources and at more than one point of the Internet. It is very difficult for the centralized defense system to detect the attack at the beginning. When the attacks are full-fledged, it becomes more difficult for defense system to resist the flooding. Moreover centralized defense systems are themselves more vulnerable to be attacked by hackers. The centralized defense systems are mostly deployed on the victim network because of economic reasons. Thus such defense systems are irresponsible systems which could only detect the attacks but cannot generate automatic alert and are also not able to filter the attack traffic themselves.

Distributed defense systems overcome the shortcomings of centralized and isolated defense systems. Deployed on all around the Internet, distributed defense systems can detect the attacks before they are launched by inspecting the traffic on many edge networks in which the computers are compromised by hackers. The most important and attractive feature of the distributed defense system is that the components in the distributed defense system can cooperate with each other to fight against DDoS attacks.

The advantage of distributed over centralized defense has been recognized in [9-11] [39]. A comparison of centralized Vs distributed is given in table 4

Table 4: Centralized Vs Distributed defense

Centralized	***Distributed***
All the component modules are deployed at same place.	Whereas in distributed they are deployed at multiple places.
Highly Vulnerable and hence not robust against DDoS attacks.	Less Vulnerable and hence robust against DDoS attacks.
No cooperation and communication framework required.	Cooperation among various modules and proper communication framework required
Lesser resources are available for fighting against the attacks	More resources are available for fighting against the attacks
Mostly deployed at Victim site	Deployed at Victim-Core, Throughout the Internet and Victim-Source

Clearly distributed defense is the only workable solution to combat DDoS attacks. Some recently proposed defenses use collaborating source-end and victim-end nodes [10], while others deploy collaborating nodes at the victim and

core networks [13]. While they perform well against a variety of attacks, they do not completely handle the flooding DDoS threat. Specifically, source/victim defenses fail to handle large attacks launched from legacy networks, while victim/core defenses inflict high collateral damage to legitimate traffic. A few defenses combine defense nodes at all three locations [9] [11]. These defenses mechanism achieve higher effectiveness, but focus on a single approach to defense (e.g., a capability mechanism in [11], victim-hiding in [9]), which ultimately discourages integration with other defenses and wide deployment and hence are not practical. So a practical distributed defense mechanism which can have wide deployment is the need of the hour. Many distributed defense techniques are proposed in the literature. Distributed DDoS defense can be deployed at source, victim and intermediate, source/victim, and victim/intermediate networks. A Review of existing DDoS Defense techniques like ACC [14] [40], SOS [9], Controller-agent (CA) [41][42][43], Throttling (TT) [12], DiDDeM (DM) [16], MANANet (MN) [44], CROSSACK (CK) [10], IDIP [45], ASSYST (AT) [15], and DefCOM (DM) [13] in terms of deployment is presented below in table 5:

Table 5: Deployment locations for existing Distributed Defense Techniques against DDoS attacks

	Defense technique											
	ACC [40]	CA [41]	TT [12]	DM [13]	SOS [9]	MN [44]	CK [10]	IDIP [45]	AT [15]	DM [16]	D-DCFI [8]	Anjali et al. [46]
Source Network	✓				✓	✓	✓	✓	✓	✓		
Victim Network	✓		✓		✓		✓	✓	✓	✓		
Intermediate Network	✓							✓	✓	✓		
ISP Domain		✓									✓	✓
Multiple ISPs				✓								

5. Practical DDoS Defense Deployment

Distributed defense techniques are likely to be the proper solution for handling the DDoS threat [47]. However, they are infrastructural solutions i.e. they span multiple networks and administrative domains and represent major undertakings of many Internet participants. Such systems are difficult to deploy and maintain. Further, the required cooperation of defenses is hard to achieve due to distributed Internet management and strictly autonomous operation of administrative domains. Securing and authenticating the communication channels also incurs a high cost if the number of participants is large. In light of above said issues and Internet design vulnerabilities [1], a practical DDoS defense system deployment should have following important characteristics:

- Autonomous system i.e. whole defense location under one administrative control so that different defense nodes can collaborate in a secure manner.
- Large and infrastructure wise rich enough to handle high voluminous traffic from evenly distributed flood sources.
- Capability to evolve DDoS defense in incremental fashion.
- Sufficient financial motivation for value-added DDoS security service.

The Internet consists of thousands of Autonomous Systems (ASes) i.e., networks that are each owned and operated by a single institution. Usually each ISP operates one AS, though some ISPs may operate multiple ASes for business reasons (e.g. to provide more autonomy to administrators of an ISP's backbones in the United States and Europe) or historical reasons (e.g. a recent merger of two ISPs) [48]. An ISP has total autonomy to collaborate defense nodes in a secure manner. Enough infrastructures can be provided for DDoS defense to handle high volume at ingress points. Moreover, once agreement is reached between various ISPs then inter co-operation among ISPs is also possible [42, 49]. Accordingly, there is scope of incremental DDoS defense. If a provider's infrastructure is attacked (routers, DNS, etc.), all services to its customers fail, resulting in service level agreement (SLA) violations. Moreover,

ISPs normally host most of the services available on the Internet. The cost of DDoS protection is insurance against catastrophic failures that would cost the business orders of magnitude more in terms of both revenue and negative customer relations. However, Cost-avoidance is not the only motivation to implement a complete DDoS solution in ISP domain. For the users, DDoS protection can also be offered as a value-added service that creates new revenue streams and provides competitive differentiation for ISPs. In nutshell, ISP level DDoS defense is most practical and viable at this stage. Though, longer term objective "how to achieve inter ISPs cooperation" still remains as the biggest challenge.

6. Conclusion

The major contributions of the paper are as follows:-

- Relative advantages/disadvantages and technical challenges of deploying DDoS defense at source, victim, and intermediate network are highlighted.
- Characteristics of an ideal DDoS defense and practical DDoS defense deployment scenario are identified.
- A deep insight into need of distributed defense and its evolution are provided.
- Identification of appropriate locations and domain for deploying Distributed Defense against DDoS attacks are done.

Future Work

- There is need for secure framework for Distributed Defense against DDoS attacks.
- Cooperation development strategies among ISPs should be developed.
- Economic model for value-added DDoS security service is the need of hour.

REFERENCES

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

[2] McCumber, J. (1991). Information System Security: A Comprehensive Model. Proceedings of the 14th National Computer Security Conference. Baltimore. MD. USA.

[3] Kurose, J. and Ross, K. W. (2002). Computer Networking: A Top-Down Approach Featuring the Internet. pp 605-607. Second Edition, Addison Wesley.

[4] WWW Security FAQ. <http://www.w3.org/Security/Faq/wwwsf6.html>. Accessed 2007 Dec 9.

[5] Neumann, P. G. (2000). Denial-of-Service Attacks. Communications of the ACM 43(4): 136. Xx

[6] CERT. [Online]. Available: http://www.cert.org/advisories/CA-2000-01.html

[7] Mirkovic, J. (2003). D-WARD: Source-End Defense Against Distributed Denial-of-service Attacks, Ph.D. Thesis, University of California, Los Angeles

[8] Kumar, K.(2007). Protection from Distributed Denial of Service (DDoS) Attacks in ISP Domain, Ph.D. Thesis, Indian Indian Institute of Technology, Roorkee, India

[9] Keromytis, A. D., Misra, V. and Rubenstein, D. (2004). SOS: An Architecture For Mitigating DDoS Attacks. IEEE Journal on Selected Areas in Communication, Vol. 22, No.1, pp. 176-188.

[10] Papadopoulos, C., Lindell, R., J. Mehringer, Hussain, A. and Govindan,R.(2003). CROSSACK: Coordinated Suppression of Simultaneous Attacks. Proceedings of DISCEX, pp. 2-13, 2003.

[11] Yang, X., Wetherall, D. and Anderson, T. (2005). A DoS-limiting network architecture. Proceedings of ACM SIGCOMM, pp. 241-252.

[12] Yau, D. K. Y., Lui, J. C. S., Liang, F. and Yam, Y. (2005).Defending against distributed denial of service attacks with Max-Min fair server-centric router throttles. IEEE Transactions on Networking, Vol. 13. No. 1, pp. 29-42.

[13] Oikonomou, G., Mirkovic, J., Reiher, P. and Robinson, M.(2006).A Framework for a Collaborative DDoS Defense. Proceedings of the 22nd Annual Computer Security Applications Conference, pp. 33-42.

[14] Mahajan, R., Bellovin, S., Floyd, S., Paxson, V. and Shenker, S. (2002).Controlling high bandwidth aggregates in the network. ACM Computer Communications Review 32(3).

[15] .Canonico, R., Cotroneo, D., Peluso, L., Romano, S. P. and Ventre, G. (2001). Programming Routers to Improve Network Security. Proceedings of the OPENSIG 2001 Workshop Next Generation Network Programming.

[16] Haggerty, J., Shi, Q. and Merabti, M.(2005).Early Detection and Prevention of Denial-of-Service Attacks: A Novel Mechanism with Propagated Traced-Back Attack Blocking. IEEE Journal on Selected Areas in Communication. 23(10): 1994-2002

[17] Mirkovic, J., Robinson, M., Reiher, P. and Kuenning, G. "Alliance Formation for DDoS Defense," Proceedings of the New Security Paradigms Workshop, ACM SIGSAC, August 2003.

[18] Garg, A. and Reddy, A. L. N., "Mitigation of DoS attacks through QoS Regulation," In Proceedings of IWQOS workshop, 2002

[19] Juels A. and Brainard, J., "Client puzzles: A cryptographic countermeasure against connection depletion attacks," In Proceedings of the 1999 Networks and distributed system security symposium, pp. 134-149, March 1999.

[20] Lau, F, Rubin, S. H, Smith, M. H. and Trajkovic, L. "Distributed Denial of Service Attacks," In IEEE International Conference on Systems, Man, and Cybernetics, pp. 2275-2280, October 2000.

[21] Spatscheck O. and Petersen, L. L., "Defending Against Denial of Service Attacks in Scout," In Proceedings of the 3rd Symposium on Operating Systems Design and Implementation, pp. 59-72, February 1999.

[22] Zheng Y. L. and Leiwo, J., "A Method to Implement a Denial of Service Protection Base," In Information Security and Privacy, volume 1270 of LNCS, pp. 90-101, 1997.

[23] Meadows, C., "A formal framework and evaluation method for network denial of service," In Proceedings of the 12th IEEE Computer Security Foundations Workshop, pp. 4-13, June 1999.

[24] Schuba, C., Krsul, I., Kuhn, M., Spafford, G.. Sundaram, A. and Zamboni, D. , "Analysis of a denial of service attack on TCP," In Proceedings of the 1997 IEEE Symposium on Security and Privacy, pp. 208-223, May 1997.

[25] Leiwo, J., Nikander, P. and Aura, T., "Towards network denial of service resistant protocols," In Proceedings of the 15th International Information Security Conference, pp. 301-310, August 2000.

[26] Aura, T., Nikander, P. and Leiwo, J.,"DOS-Resistant Authentication with Client Puzzles," Lecture Notes in Computer Science, Vol. 2133/ 2001.

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

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

[29] Geng X. and Whinston, A. B., "Defeating Distributed Denial of Service attacks," IEEE IT Professional, pp. 36–42, 2002.

[30] Snoeren, A. C., Partridge, C., Sanchez, L. A., Jones, C. E., Tchakountio, F.,. Kent, S. T and Strayer, W. T., "Hash-Based IP Traceback," In Proceedings of ACM SIGCOMM 2001, pp. 3-14, August 2001.

[31] Dean, D., Franklin, M.and Stubblefield, A., "An Algebraic Approach to IP Traceback," ACM Trans. Info. and Sys. Sec., vol. 5, pp. 119-137, 2002.

[32] Song D., and Perrig, A., "Advanced and Authenticated Marking Schemes for IP Traceback," In IEEE INFOCOM, pp. 878-886, 2001.

[33] Bellovin, S., ICMP Traceback Messages, IETF draft, 2000 [online] Available at: http://www.research.att.com/smb/papers/draft-bellovin-itrace-00.txt.

[34] Savage, S., "Network Support for IP Traceback," IEEE/ACM Trans. Net., Vol. 9, pp. 226-237, 2001.

[35] Bradley, K. A., Cheung, S., Puketza, N., Mukherjee, B.and Olsson, R. A., "Detecting disruptive routers: A distributed network monitoring approach", in Proceedings of the 1998 IEEE Symposium on Security and Privacy, IEEE Press, New York, 1998, pp. 115-124.

[36] Fan, Y., Hassanein, H., and Martin, P., "Proactively defeating distributed denial of service attacks." in Canadian Conference on Electrical and Computer Engineering, 2003., vol. 2, May 2003, pp. 1047-1050

[37] Thomas, R., Mark, B., Johnson, T. and Croall, J., "NetBouncer: client-legitimacy based high-performance DDoS filltering," in Proceedings of the DARPA Information Survivability Conference and Exposition, vol. 1, April 2003, pp. 14-25.

[38] Kim, Y., Jo, J.-Y., Merat, F., Yang, M. and Jiang, Y., " Mitigating distributed denial-of-service attack with deterministic bit marking, International Journal of Information Technology, vol. 11, no. 2, 2005, pp. 62-82.

[39] Shi, W., Xiang, Y., and Zhou, W. (2005). Distributed Defense Against Distributed Denial-of-Service Attacks. Proceedings of ICA3PP 2005, LNCS 3719, pp. 357-362

[40] loannidis, J. and Bellovin, S. M.(2002).Implementing Pushback: Router-Based Defense against DDoS Attacks. Proceedings. of Network and Distributed System Security Symposium, Catamaran Resort Hotel San Diego, California.

[41] Tupakula, U. K. and Varadharajan, V. (2003). A practical method to counteract denial of service attacks. Proceedings of the 26th Australasian Computer Science Conference, Volume 16, pp. 275-284.

[42] Tupakula, U. K. and Varadharajan, V. (2003).A controller agent model to counteract DoS attacks in multiple domains. Proceedings of Integrated Network Management, IFIP/IEEE Eighth International Symposium. pp.113-116, 2003

[43] Tupakula, U. K. and Varadharajan, V. (2004).Tracing DDoS Floods: An Automated Approach. Journal of Network and Systems Management 12: 111-135.

[44] MANAnet DDoS White Papers, available at http://www.cs3-inc.com/mananet.html

[45] Schnackenberg, D., Djahandari, K. and Sterne, D. (2000). Infrastructure for Intrusion Detection and Response. Proceedings of the DARPA Information Survivability Conference and Exposition, pp. 3-11

[46] Sardana, A., Joshi, R. (2009). An auto-responsive honeypot architecture for dynamic resource allocation and QoS adaptation in DDoS attacked networks. Computer Communications. 32(12): 1384-1399

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

[48] Caesar M.and Rexford, J., "BGP routing policies in ISP networks,"

[49] Chen S.and Song, Q., "Perimeter-Based Defense against High Bandwidth DDoS Attacks," IEEE Transactions on Parallel and Distributed Systems, Vol. 16, No. 6, pp. 526-537, June 2005Bowman, M., Debray, S. K., and Peterson, L. L. 1993. Reasoning about naming systems. .