A Comparative Analysis of Various Deployment Based DDoS Defense Schemes

Karanbir Singh[1], Navdeep Kaur[2], and Deepa Nehra[3]

[1] Seth Jai Parkash Polytechnic, Damla, Yamuna Nagar, Haryana, India
karan_nehra@yahoo.co.in
[2] Chandigarh Engineering College, Landran, Mohali, Punjab, India
nrwsingh@yahoo.com
[3] Tilak Raj Chadha Institute of Management & Technology, Yamuna Nagar, Haryana, India
deepa.nehra@gmail.com

Abstract. Distributed denial of service attack is a major threat to the availability of internet services and resources. The current internet infrastructure is vulnerable to DDoS attacks and has no built in mechanism to defend against them. The main task of the defense system is to accurately detect and respond against DDoS attacks. A variety of DDoS defense solutions are available but having difficulties to choose among them. There are different places in the internet, where a defense system can be deployed. The various points in the internet where defense systems can be deployed are identified and discussed here. A comparative analysis of different defense schemes corresponding to deployment points are also carried out. The main aim of this review paper is to provide an individual or academia to insight into various possible deployments locations suitable for DDoS defense system. It helps them to choose an appropriate defense method and suitable deployment location.

Keywords: DDoS, Network Security, Distributed Defense, Deployment.

1 Introduction

A Denial of Service (DoS) attack is an attack with the aim of preventing normal users from using some network resource such as a website, web service, or computer system [1]. A Distributed Denial of Service (DDoS) attack is a large scale, coordinated attack launched through many compromised system on the internet to the availability of services of a given target system or network. In DDoS attack a large number of packets are sent by the attacker through multiple machines to a victim. The packets arrive on the victim are huge in quantity and it will quickly exhaust its resources like bandwidth, cpu time and buffers. The victim devotes its most of the time in handling the attack packets and cannot switch to the legitimate clients. Thus legitimate clients are dispossessed of victim resources as long as the attack last. These attacks are widely imposed a serious threat to the internet services.

One of the first major DDoS attacks was waged against Yahoo.com in February 2000, keeping it off from the internet for nearly 2 hours, costing it significant loss of

K. Singh, A.K. Awasthi, and R. Mishra (Eds.): QSHINE 2013, LNICST 115, pp. 606–616, 2013.

advertising revenue [2]. Recently, attackers perform a variety of DDoS attacks against many companies providing anti-spam services [3]. These attacks force them to shut down their services. Reports by law enforcement agencies indicates that the percentage of organizations that experienced virus disasters has grown geometrically every year over the last decade, with 92 percent of organizations reporting such incidents during 2003. DDoS attacks are one of the overall costly security incident for organizations. A lot of works have been done to combat against DDoS attacks. An excellent review of existing DDoS defense techniques is available in [6-12].

The organization of rest of the paper is as follows. Section 2 provides an insight into various deployment locations where defense system can be implemented. In section 3 we review and characterize some existing DDoS defense system on the basis of deployment. Section 4 compares them to evaluate their performance on the basis of some key points like detection, response, deployment, robustness and implementation. Section 5 suggests the best way to defend against DDoS Attacks by using performance evaluation. This work provides an individual to select an appropriate deployment for the defense method and point out the various deficiencies in the existing methods.

2 DDoS Defense Locations

DDoS attacks can be originated from any machine on the internet, which is geographically placed at any location. The network from where the attack stream originates is called source network. Then this attack stream is forwarded by many routers through the intermediate network and then later converged to a single machine in victim network. So, the networks responsible for the happening of DDoS attacks are source network (from where the attack originates), Intermediate network (responsible for forwarding the attack traffic to the target) and the victim network (where victim machine receives the burnt of attacks). So the three different locations are source network, intermediate network or victim network, which can host the DDoS defense system [13]. The figure 1 represents a simplified network divided into three parts as mentioned above. The edge router connects source/victim networks to the intermediate network (normally operated by ISP's). The intermediate network contains many ISP's, interconnected with each other through core routers. This figure will be used to illustrate various defensive locations. Here, the nodes at the left side are attackers and the node at the right side is the target of the DDoS attack. The figure given below illustrates that the defense system can be deployed at source network, intermediate network, victim network or distributed at all three locations.

The different deployment based DDoS defense schemes are effective in their respective area but suffers from some disadvantages. The table 1 gives their relative advantages and disadvantages.

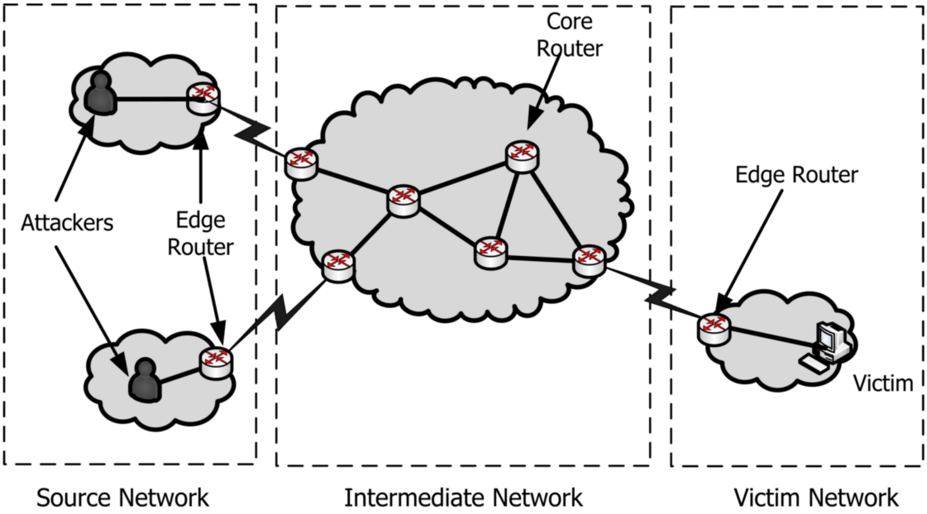

Fig. 1. Network illustrating different locations for DDoS deployment

Table 1. Comparison Between Different Deployment Locations

Deployment Point	Advantages	Disadvantages
Source Network	Good point to detect when attack happen	• Overwhelm with large no of attack packets. • Only protect individual target not the other edges.
Victim Network	Low volume of attack packets will flow in outgoing network	• Difficult to determine whether traffic is legitimate or attack. • Requires widespread deployment to all source networks.
Intermediate Network	Core router defenses are effective as all the traffic goes through them.	• Core router cannot devote sufficient resources for analyze individual packets. • Core routers could inflict massive collateral damage.
Distributed Network	More robust as the defense components are deployed on all above three locations	• To be effective it needs large scale deployment which is expensive and difficult

3 Review of Existing Defense Mechanisms

In this section, we review some existing DDoS defense methods. The methods are identified from the literature based upon their deployment in the network.

3.1 Source Based Defense

D-WARD [14] is a source-end DDoS defense system whose goal is to detect and constrain outgoing attacks at the source network. The system is installed at the source router and monitors the traffic passing through the router in both directions and correlates this observation to detect anomalies that can be a sign of DDoS attack. Upon detection, it selectively imposes a rate limit on the outgoing flow to the victim, attempting to detect and forward legitimate packets regardless of the limit. However, a major drawback is that it is only effective in actually stopping attacks if deployed at most attacking network.

Ingress Filtering [15] is a technique used to ensure that weather the incoming packets are coming from their original locations. Egress filtering is an outbound filter, which monitors and restricts the flow of outgoing traffic. A key requirement for ingress or egress filtering is information of the expected IP addresses at a particular port. For some networks with complex topologies, it is not always easy to obtain this information.

3.2 Victim Based Defense

Preferential filtering [16] is basically an IP traceback schemes to obtain the information concerning whether a network edge is infected (i.e. on the attacking path of an attacker) or clean (not on the attacking path). We observe that all the edges on the path of attacker are marked as “infected”, edges on the path of a legitimate client will normally be “clean”. This scheme filter out packets that are inscribed with the marks of “infected” edges, the scheme removes most of the DDoS traffic coming from attackers while putting little effect on legitimate traffic.

NetBouncer [23] is a client-legitimacy-based DDoS filtering. It tries to detect legitimate clients and only serve their packets. NetBouncer is deployed near the victim side and it is an inline defense device deployed in front of the possible choke point. A NetBouncer device maintains a large list of legitimate clients. If packets are received from a client (source) not on the legitimacy list, NetBouncer device will proceed to administer a variety of legitimacy tests to challenge the client to prove its legitimacy. The legitimacy of a client expires after a certain interval. NetBouncer can ensure good service to legitimate clients in the most of the cases and does not require modifications to clients or servers. However, some of the legitimate clients will not be validated. The use of only legitimate IP list has the potential problem that legitimate client identity can be misused for attacks.

3.3 Core Router Based Defense

Perimeter-based defense mechanisms [17] are used by Internet service providers (ISPs) to provide the anti-DDoS service to their customers. These methods completely depend on the edge routers of ISP to co-operatively identify the flooding sources and start rate-limit filters to block the attack traffic. This system does not need any support from ISP routers (outside or inside of the ISP), which not only makes it locally deployable, but also put less stress on the ISP core routers. This method requires widespread deployment and does not perform well in noncontiguous deployment.

Distributed Change-point Detection (DCD) [18] scheme detects DDoS flooding attacks by observing the propagation patterns of unexpected traffic changes at distributed network points. Once a sufficiently large CAT tree is constructed to exceed a preset threshold, an attack is declared. The system is deployed over multiple Autonomous Systems domains. The system detects traffic changes, checks flow propagation patterns, aggregates suspicious alerts, and merge CAT subtrees from collaborative servers into a global CAT tree. The system is built upon attack-transit routers, which works cooperatively together. Each ISP domain has a CAT server which aggregate the flooding alerts reported by the routers. CAT domain servers collaborate with each other to make the final decision.

Controller agent model [19] counteracts DDoS attacks within one ISP domain. In this model, agents represent the edge routers and controllers represent trusted entities owned by the ISP. Once a target detects an attack, it sends a request to the controller, asking all agents to mark all packets to the target after checking the marking field, the target can find out which agent (edge router) is the entry point for the attack traffic. The target then sends a refined request to the controller, asking some particular agents to filter attack traffic according to the attack signature provided by the target. The main limitation of this model is that it uses third party detection for detecting and characterizing attack traffic.

3.4 Distributed Defense

Local Aggregate-Based Congestion Control (Local ACC) [20] provides a self-contained solution in which detection and rate-limiting of DDoS attacks are done on a single router. Routers identify high-bandwidth traffic aggregates in their queue which are responsible for the majority of packet drops and responds by imposing a rate limit on each traffic aggregate. Pushback [21] extends local ACC with communication and coordination capabilities. If it is difficult for the congested router to control the aggregate, then it issues a rate limit request to its immediate upstream neighbors.

DefCOM [22] is a distributed cooperative system for DDoS defense. DefCOM builds a distributed peer-to-peer network of cooperative defense nodes which are scattered throughout the Internet. Defense nodes exchange information and control messages to detect attacks, and collectively respond to them while ensuring good service to legitimate traffic. DefCOM nodes can be classified into three categories, based on their functionality: Alert generator nodes that detect the attack and deliver an alarm to the rest of the peer network, Rate limiter nodes that rate limit a high volume of traffic destined for the victim, and Classifier nodes that perform selective rate-limiting.

Active Security System (ASSYST) [5] supports distributed response with non-contiguous deployment. All ASSYST nodes are essentially the equivalent of classifier nodes and are deployed only at edge networks. Active Security Protocol, which allows a set of active routers to interact in order to isolate the sources of a DDoS attack even in the case of address spoofing. Tuining and deployment of the Active Security System are perfectly suited to a Programmable Network environment.

4 Comparative Analysis of Different DDoS Defense Methods

The DDoS defense mechanisms discussed above are compared using some important performance metrics like attack detection, attack response, deployment location, robustness and implementation. Here firstly we will discuss these metrics and later use them to compare the DDoS defense system.

Attack Detection: DDoS detection is usually the first step in the mitigation of a DDoS attack. Any DDoS detection technique always attempts to detect an attack by observing anomalous changes in IP attributes or traffic volume because there do not exist clear DDoS attack signatures. The detection is main feature of a defense mechanism, because if we can detect an attack at its initial stage then it can be corrected by deploying a prevention or reaction countermeasure. This provides fast protection to the legitimate users against attacks. In addition, detection helps us to identify the attacker, which can later to be blocked at the source. The defense system which detects attacks quickly, with in time, with accuracy and minimal deployment costs are said to be efficient.

Attack Response: After a DDoS attack has been detected, response techniques attempt to control incoming traffic by packet filtering or rate limit techniques. Based on the studies done, packet filtering techniques can cause more damage to legitimate traffic than rate limit techniques, because it is difficult to distinguish DDoS traffic from normal traffic. Packet filtering task is usually done at the routers based on clearly defined attack signatures. However, DDoS attack traffic cannot be filtered out if it uses packets that request legitimate services [24]. Another common drawback of packet filtering is that it usually needs to be deployed widely in order to protect the victim. Rate limiting is used to control the traffic flow on a network interface. The traffic which is less than or equal to the specified rate is allow to send, whereas traffic which exceeds the rate is either dropped or delayed [25]. The effectiveness of rate limiting to defend DDoS attacks is defined in [26]. Rate limiting can be used as a fast, automatic reaction mechanism to mitigate an attack without any undue penalties for legitimate traffic [26]. In contrast, collateral damage for legitimate traffic is unavoidable in packet filtering because DDoS traffic cannot be easily distinguished from legitimate traffic [27].The goal of attack response is to improve the situation for legitimate users and mitigate the DDoS effect.

Deployment: Deployment of DDoS defense method is an important issue that must be considered. It tells us the place in the network where we can put our DDoS defense system. A practical DDoS defense solution should be easy to deploy in the sense that it minimally interferes with existing Internet protocols and settings. Also, the scale of deployment should be reasonable. Defenses which require local deployment are usually preferred over those which require global deployment. However, if a DDoS defense requires global deployment, then this deployment should be incrementally feasible.

Robustness: Robustness tells us the degree up to which the defense system can resist the attacks. When the defense system is deployed and known to the hackers, then there is possibility that the hacker can compromise the defense system and uses it to further attack on the protected network. Some of the defense systems are less vulnerable to attacks than others. Distributed defense is less vulnerable to DDoS attacks than isolated but still there is a possibility that distributed defense system fails as it can be targeted by the hacker. In case of distributed defense, the information exchanged between defense components are also vulnerable to hackers. So, it depends upon the defense system that how securely they exchange the information.

Implementation: DDoS defense systems are deployed at various locations in different schemes bears an implementation overhead. The defense systems follows different deployment strategies like their defense components are deployed at source/victim side or on different parts in the intermediate networks. DDoS defense sometimes require major changes (such as altering behavior of core routers, deploying new software on all machines in the Internet or changing fundamental Internet protocols) will never be implemented without far more convincing evidence that they would work if their price was paid. In particular, it will be more depressing if the defense system fails to respond to the majority of DDoS attacks even after doing major changes to the internet. This issue points out one serious advantage that target end systems have. They typically cost less to deploy, so if they do not work, less has been lost. Overall, we need to concentrate more on nature and behavior of these attacks and the characteristics of proposed defenses before we should accept anyone's.

The table 2 (divided into two parts) gives deployment based comparison between different DDoS defense mechanisms.

Table 2. Deployment Based Comparisons Between Different DDoS Defense Methods

Deployment Scheme	Scheme Name	Attack Detection	Attack Response
Source Based Defense	D-Ward	Abnormality in traffic	Rate Limiting
	Egress/Ingress filtering	IP Address validity	Rule based packet filtering
Victim Based Defense	Preferential Filtering	Attack traffic graph	Filtering packets with infected edges
	NetBouncer	Legitimacy test for clients	Packet filtering based of legitimacy test
Core Router Based Defense	Perimeter based defense	Traffic Aggregate	Rate Limit Filters
	Controller Agent Model	Signature Matching	Packet Filtering through agents
	Collaborative Change Detection	Change Aggregation tree (CAT)	Packet Filtering
Distributed Defense	ACC & Pushback	Congestion based	Rate limiting
	ASSYST	Packet Classifier Intrusion Detection	Packet Filtering Through Programmable Routers
	DefCom	Traffic Tree Discovery	Distributed rate limiting

Deployment Scheme	Scheme Name	Deployment Location	Robustness	Implementation
Source Based Defense	D-Ward	Source Network	Weak	Difficult
	Egress/Ingress filtering	Source Network	Weak	Difficult
Victim Based Defense	Preferential Filtering	Victim Network	Weak	Easy
	NetBouncer	Victim Network	Weak	Easy
Core Router Based Defense	Perimeter based defense	ISP Core network	Moderate	Moderate
	Controller Agent Model	ISP Core network	Moderate	moderate
	Collaborative Change Detection	ISP Core Network	Moderate	difficult
Distributed Defense	ACC & Pushback	Throughout the network	Strong	Difficult
	ASSYST	Throughout the network	Strong	Difficult
	DefCom	Throughout the network	Strong	Difficult

5 Performance Evaluations

There's a simple argument that which kind of DDoS defense solution is necessary to efficiently protect the network. Source based defense systems detect and filter the attack traffic at the early stages when the attack happens. This is effective, if deployment will cover maximum source networks. But practically it seems to be very difficult to cover all available source networks. Victim network is the best place to detect attack traffic due to its huge volume and easy deployment. But it suffers from high flood rate and itself vulnerable to DDoS attacks. Core routers in the intermediate network are the best places for attack detection and filtration but it require entire coverage, because no single location can capture all attacks. The individual packet scanning also creates additional overhead for the routers. All these schemes perform well in their respective area but we cannot rate anyone best suitable for an individual. All these schemes also have some drawbacks. So we need a defense system which can put their defense components at the following locations.

- Near the target, this is a good position to recognize attacks.
- Near the attackers, this is best place to differentiate between good and bad packets.
- In the center of the network, which achieve high defensive coverage with relatively few deployment points.

Distributed defense systems overcome the shortcomings of intermediate and source/victim end based defense systems. The distributed DDoS defense system spans its defensive components at the above mentioned three locations. Components of distributed defense system are deployed at various locations and cooperate with each other to defend the attacks. Distributed DDoS defense system is only solution to effectively control the flood of attack traffic. Hence, we can say that distributed solution provides effective protection against DDoS attacks than other kind of solutions.

6 Conclusion

This paper classified the various deployment based categories of DDoS defense systems. The categories identified are source, intermediate, victim and distributed networks. A comparison between these categories is identified. The existing defense methods falling under these categories are reviewed and their performance is evaluated on the basis of some metrics. After their performance evaluation the fact is discovered that not any individual location is best for the complete protection against DDoS attacks. We also suggested that we need a distributed defense in which defense components are placed on all the locations to effectively control attack flood. So in the end we make a conclusion that this classification is helpful for an individual in selecting an appropriate defense mechanism

References

1. Karig, D., Lee, R.: Remote Denial of Service Attacks and Countermeasures. Technical Report CEL2001-002, Department of Electrical Engineering, Princeton University (2001)
2. Yahoo on Trail of Site Hackers, `http://www.wired.com/techbiz/media/news/2000/02/34221`
3. Spam block lists bombed to oblivion, `http://www.msnbc.msn.com/id/3088113`
4. Sachdeva, M., Singh, G., Kumar, K.: A Comprehensive Survey of Distributed Defense Techniques Against DDoS Attacks. International Journal of Computer Science and Network Security 9(12) (2009)
5. Canonico, R., Cotroneo, D., Peluso, L., Romano, S., Ventre, G.: Programming Routers to Improve Network Security. In: Proc. of the OPENSIG 2001 Workshop, Next Generation Network Programming (2001)
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. Defenses against distributed denial of service attacks, `http://www.garykessler.net/library/ddos.html`
8. Lin, S., Chieuh, T.: A Survey on Solutions to Distributed Denial of Service Attacks. RPE Technical Report (September 2006)
9. Chen, L., Longstaff, T., Carley, K.: Characterization of Defense Mechanisms Against Distributed Denial of Service Attacks. Computers & Security, 665–678 (2004)
10. Abliz, M.: Internet denial of service attacks and defense mechanisms. University of Pittsburgh Technical Report, No. TR-11-178 (2011)
11. Sachdeva, M., Singh, G., Kumar, K.: Deployment of Distributed Defense Against DDoS attacks in ISP domain. International Journal of Computer Applications 15(2) (2011)
12. Fadlallah, A., Serhrouchni, A.: Denial of service attacks and defense schemes analysis and taxonomy. In: 3rd International Conference: Sciences of Electronics Technologies of Information and Telecomm., TUNISIA (March 2005)
13. Mirkovic, J., Dietrich, S., Dittrich, D.: Internet Denial of Service: Attack and Defense Mechanisms. Prentice Hall (December 2004)
14. Mirkovic, J., Prier, G., Reiher, P.: Source-end DDoS Defense. In: Proceedings of Network Computing and Applications Symposium NCA (2003)
15. Cert advisory ca-2000-01 Denial-of-Service Developments, `http://www.cert.org/advisories/CA-2000-01.html`
16. Sung, M., Xu, J.: IP Traceback-Based Intelligent Packet Filtering: A Novel Technique for Detecting Against Internet DDoS Attacks. In: Proc. of 10th IEEE International Conference on Network Protocols (2002)
17. Chen, S., Song, Q.: Perimeter-Based Defense against High Bandwidth DDoS Attacks. IEEE Transactions on Parallel and Distributed Systems 16(6) (2005)
18. Chen, Y., Hwang, K., Ku, W.: Collaborative Detection of DDoS Attacks over Multiple Network Domains. IEEE Transactions on Parallel and Distributed Systems 18(12) (2007)
19. Tupakula, U., Varadharajan, V.: A Controller Agent Model to Counteract DoS Attacks in Multiple Domains. In: Proc. of Integrated Network Management, IFIP/IEEE 8th International Symposium (2003)
20. Mahajan, R., Bellovin, S., Floyd, S., Ioannidis, J., Paxson, V., Shenker, S.: Controlling High Bandwidth Aggregates in the Network. ACM Computer Communications Review 32(3) (2002)
21. Ioannidis, J., Bellovin, S.: Pushback: Router-Based Defense against DDoS Attacks. In: Proc. of NDSS (February 2002)

22. Mirkovic, J., Robinson, M., Reiher, P., Oikonomou, G.: A Framework for Collaborative DDoS Defense. In: Proc. of the 22nd Annual Computer Security Applications Conference, Miami, Florida, USA, pp. 33–42 (December 2006)
23. Thomas, R., Mark, B., Johnson, T.: Net bouncer: Client-Legitimacy-Based High Performance DDoS Filtering. In: Proc. of the DARPA Information Survivability Conference and Exposition. IEEE (2003)
24. Xiang, Y., Zhou, W., Chowdhury, M.: A Survey of Active and Passive Defence Mechanisms against DDoS Attacks. Technical Report, TR C04/02, School of Information Technology, Deakin University, Australia (March 2004)
25. Evans, J., Filsfils, C.: Deploying IP and MPLS QoS for multiservice networks. Theory and Practice. Morgan Kaufmann (2007)
26. Molsa, J.: Effectiveness of Rate-Limiting in Mitigating Flooding DoS Attacks. In: Proc. of the Third IASTED International Conference on Communications, Internet, and Information Technology, pp. 155–160 (2004)
27. Sterne, D., Djahandari, K., Wilson, B., Babson, B., Schnackenberg, D., Holliday, H., Reid, T.: Autonomic Response to Distributed Denial of Service Attacks. In: Lee, W., Mé, L., Wespi, A. (eds.) RAID 2001. LNCS, vol. 2212, p. 134. Springer, Heidelberg (2001)