Asian Journal of Information Technology 5(7): 691-695, 2006

Comprehensive Mitigation Mechanism Against DDoS Attack-A Comparative Study

S. Meenakshi
Department of Information Technology, Sathyabama Institute of Science and Technology, Chennai, S.K. Srivatsa, MIT, Chennai, India

Abstract: Distributed Denial of Service (DDoS) attacks are a relatively new type of attack on the availability of Internet services and resources. A Denial of service attack is with the purpose of preventing legitimate users from using victim system resources. DDoS is a large scale coordinated attack on the availability of services of a victim system (or) network resource. Large-scale distributed nature of Internet makes DDoS attack stealthy and difficult to counter. As attack traffic is indistinguishable from normal traffic, it would be desirable to develop comprehensive DDoS solution. As various attack tools become widely available, automated anti-DDoS systems become increasingly important. This study proposes taxonomy of various mitigation mechanisms against DDoS attack. We studied the different mitigation mechanisms like IP-Traceback,Change point monitoring method and perimeter based defense. Finally we drafted a taxonomy which helps to understand the advantages and drawbacks of various mitigation mechanisms and scope of the DDoS problem.

Key words: Denial-of-service, change point monitoring, perimeter based defense

INTRODUCTION

Business organizations and other users depend on the information stored and transferred in the Internet. With the Internet emerging as a backbone of commercial communications infrastructure, it has increasingly become the target of attacks from a broad range of sources[1] Enterprise networks disseminate information and transfer business critical data from customers to business organizations and vice versa. Thus, organizations and their customers heavily depend on their network.

Denial-of-service pose significant problems to these networks. A Denial of service(DoS) attack is an attack with the purpose of preventing legitimate users from using victim computing system(OR) network resource[2]. A Distributed Denial of Service(DDoS) attack is a large scale coordinated attack on the availability of services of a victim system(or) network resource, launched indirectly through many compromised computers on the Internet[2].

According to the CIAC(Computer Incident Advisory capability), the first DDoS attack occurred in 1999[2,3]. In February 2000, one of the major DDoS attack was waged against Yahoo. com[2]. This attack kept Yahoo off the Internet for about 2 hours and cost Yahoo a significant loss in advertising revenue. Another recent DDoS attack occurred on October 20,2002 against 13 root servers that provide the Domain Name System (DNS) service to Internet users around the world. If all 13 servers were to go down, there would be disastrous problems accessing the World Wide Web[2]. It caused 7 of the 13 root servers to shutdown, demonstrating the vulnerability of the Internet to DDoS attacks[2]. If unchecked, more powerful DDoS attacks could potentially cripple the Internet services in minutes[2].

VARIOUS DOS MITIGATION MECHANISMS

The table gives the different mitigation methods against DoS attacks and their drawback.

For all the approaches mentioned in the Table 1, although deployment can be carried out incrementally, the effectiveness of preventing DoS comes only after the filters (or) software are widely deployed across the Internet[6]. Most of the models focus on tracking on locations of the attackers but after the attack little is done to mitigate.

CLASSIFICATION OF DDoS MITIGATION MECHANISMS

There are number of countermeasures against DoS attacks. In general the countermeasures of DoS attacks can be classified[8] into three different categories:

- Prevention
- Detection
- Post-attack forensic

Table 1: Gives the different mitigation methods against DoS attacks and their drawback.

Mitigation method	Method of implementation	Draw back
IP-Trace back[4]	This function must be implemented on the routers to mark the packets[4]	•The mitigation is outside the defense line to marks the packets before they reach the line[4].
Aggregate-based	Congested router starts with local rate limit. Then congestion control[5] progressively pushes the rate limit to some neighbor routers and further out. , forming a dynamic rate-limit tree. All the routers in the tree measure the traffic arrival rates, which are propagated upstream toward the congested router, allowing it to know the total arrival rate and decide whether to continue rate limiting[5]	•Expensive to maintain.
Anti address	This requires the routers of stub networks to inspect spoofing[6] outbound packets and discard these packets whose source addresses do not belong to the stub networks	•Thesemethods apply incremental deployment and prevents DDoS after deployment.
Route-based distributed packet filtering[6]	The router has to drop the packet if the packet is received from a link that is not on any routing path from the packet's source to the packet's destination[6].	
SYN-dog[6]	It is software agent installed at leaf routers connecting to stub networks. The agent detects SYN flooding[6].	
Secured Overlay System(SOS)[7,6]	This is designed for emergency services.	•Only authenticated traffic can enter [7]the overlay network[. •Not suitable for general purpose public server[7].

Why detection is very important:

- Even though we classify the mitigation mechanisms against attack into three types, detecting DDoS attacks in real time is the first step of combating DoS attacks[8].
- An automated and fast detection helps in prevention against DDoS. Upon timely detection of DoS attack, more sophisticated defense mechanisms will be triggered to shield the victim server (or) link bandwidth from DoS traffic[8].
- IP-trace back mechanisms used to single out[8,4] flooding sources is expensive. Instead we can design detection mechanism with little overhead to withstand any flooding attacks.

Change point monitoring method[8]: Normal traffic models are based on flow rates. So, it is difficult to obtain general model. This change point monitoring method is based on protocol behavior instead of traffic rates[8]. Internet applications demonstrate a unique request vs. reply protocol behavior. Thus reliable data delivery leads to the inherent data versus acknowledgement protocol behavior. There exists a strong correlation between requests and corresponding replies and DoS attacks easily destroy this correlation. on parametric cumulative sum method is used to detect the cumulative effect of the deviation from normal protocol behavior caused by a DoS attack[8].

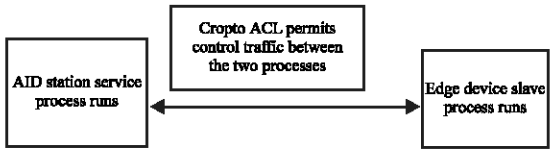

Fig. 1: A crypto access control mechanism

Anti-dos service(aid-rp2p)-random peer to peer network[6]: This provides an anti-DoS service called AID[6] for general purpose TCP-based public servers. It has a random peer to peer network that connects the registered client network with registered servers even when they are under DoS attack. A centrally managed service eliminates the requirement of an Internet-wide deployment.

AID service[6] is implemented as a distributed overlay system consisting of geographically dispersed AID stations for service registration and anti-Does operations. AID stations are owned by trusted entities. AID stations communicate among themselves via secure communication channels. Figure. 1 shows the secure IPSec tunnel implementation.

A client network register to a nearby AID station. As part of registration, a network device is installed at the edge of the client network to support secure Virtual private network. The registration establishes IPSec tunnel with the AID station. All tunnels together form aan exclusive overlay network between registered clients and the registered servers. This overlay network will be activated when a registered server is under attack. An IPSec tunnel has two end points, one at the AID station and the other at the edge device of the client(or) server. A crypto access control is defined at both tunnel end points. It specifies what traffic should be put through the tunnel. When a server is under attack, it will signal it's AID station, which propagates the information via the overlay network to the AID stations. Each AID station instructs it's slave processes to modify the crypto ACLs to admit a portion of traffic for the server into the tunnels. Figure 2 shows the protection steps taken by the AID station after receiving the tunneled traffic.

Perimeter based defense against DDoS attack[5]: This allows Internet Service Provider (ISP) to provide an

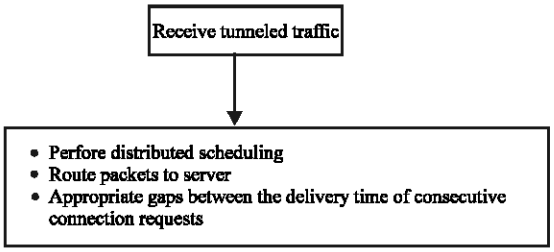

Fig. 2: Steps taken after tunneling

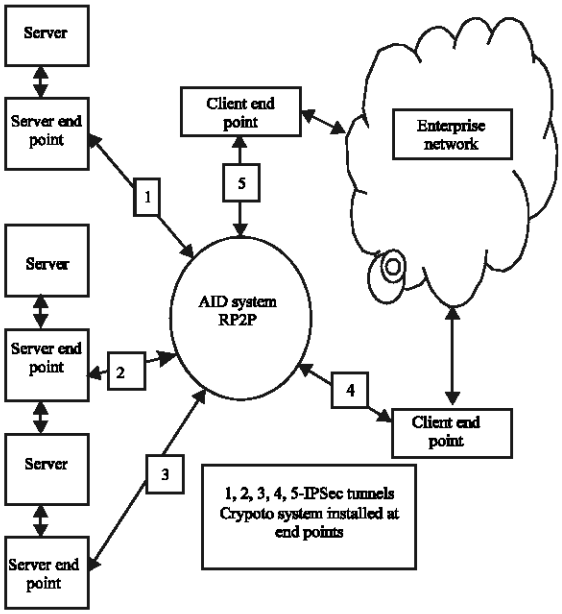

Fig. 3: Architecture of anti-does service(AID-RP2P)-random peer to peer network

anti-DDoS service to it's customers. Most business organizations ,institutions and homes access the Internet via ISPs. An ISP network interconnects it's customer networks and routes the IP traffic between them. An ISP network has two types of routers.

Edge router[5]: It has at least one direct connection to a customer network.

Core router[5]: It doesn't have any direct connections to any customer networks. They route traffic between edge routers.

The goal of high bandwidth DDoS attack is to send a large amount of traffic to exhaust a target resource . So, that legitimate users cannot access the resource. The resource may be link bandwidth, buffer space or any other processing resource. The affending traffic can be characterized as an aggregate of packets.

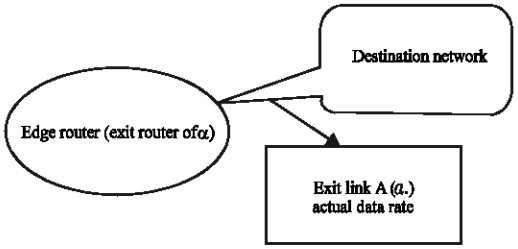

Fig. 4: Exit link of A(α)

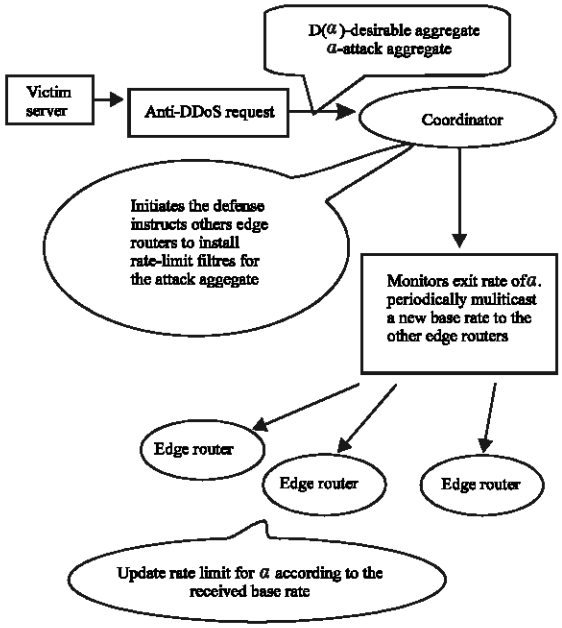

Fig. 5: Defense perimeter by the coordinator using multicast

The attack traffic is often indistinguishable from the legitimate traffic, which makes it difficult to block the attack traffic while letting the legitimate traffic through. Perimeter based defense[5] has two tasks:

- Identify the attack traffic[5].
- To identify the flooding sources and install appropriate rate-limit filters on the edge routers connecting to the flooding sources[5].

Attack aggregate is not the collection of attack packets[5], but a traffic aggregate that contains the "attack" packets as well as legitimate packets. The work focuses on assuming that the attack aggregate and the desirable rate for the aggregate are known, the problem is how to bring the total traffic volume to the desirable level.

Terminology[5]

- Consideer an aggregate α.
- A packet belonging to α. Is called an α. packet.

FINDINGS AFTER THE COMPARATIVE STUDY OF PERIMETER BASED DEFENSE[5] AND IP-TRACE BACK[4]

Criteria selected for comparison	Method	Findings after the comparative study	Reason
Line of defense[4,5]	IP-trace back	Not self complete	The routers on the line of defense perform packet filtering, but it requires support from inside the perimeter and outside the perimeter. Inside the perimeter the victim constructs the attack graph, identifies the infected edges and informs the packet filtering routers about these edges. Outside the perimeter the Internet routers must support IP-trace back[4].
	Perimeter based defense	Self complete	It does not need any assistance from outside and inside[5].
Location of defense[4,5]	IP-trace back	The defense is not at the earliest location	In all the routers of the path the trace back is done[4].
	Perimeter ba--sed defense	The perimeter is the earliest location of defense.	In order to reach a customer network of an ISP, any attack traffic must enter the first by passing an edge router[5].
Criteria selected for comparison	Method	Findings after the comparative study	Reason
Resource consumption[4,5]	IP-trace back	More resources are consumed by the attack	The attack is not stopped before it enters the ISP[4].
	Perimeter ba--sed defense	Minimizes the resources consumed by the attack	The attack is stopped before it enters the ISP[5]
Separation of attack traffic and legitimate traffic	IP-trace back	The more attack traffic mixes with the legitimate traffic	The attack traffic is not far away from the victim[4]
	Perimeter ba--sed defense	Reduces the collateral damage of blocking legitimate traffic	Blocking is performed at the furthest possible locations. The further away the attack traffic is from the victim, the less is mixed with the legitimate traffic[5]

- Arrival rate of α. At an edge router is defined as total size of α. packets received by the router from outside the ISP.
- The acceptance rate is defined as the total size of α. Packets thata are forwarded by the router into the ISP network per unit of time.

Figure 4 shows the exit link for A(α).

Defense perimeter based on multicast[5]: Edge routers of an ISP form a designated multicast group[5]. The address of the system is local to the ISP. Fig. 5 shows how during DDoS attack, the edge router connecting to the victim network is responsible of coordinating the defense (Coordinator)[5].

The process is repeated until the exit rate converges to the desirable rate.

CONCLUSION

A number of conclusions can be drawn from understanding DDoS attacks and several mitigation mechanisms against them. DDoS attacks are advanced methods of attacking a network system . Solutions and security measures must be developed to prevent theses types of attacks. A more comprehensive solution that can defend against known attacks is necessary.

The present AID[6] system is developed for TCP traffic. It can be developed for protecting UDP traffic also[6]. Similarly the compromise of the IPSec tunnel end points must be resisted[6]. The same IPSec tunneling can be extended within the system also. The perimeter based defense can be extended when there are compromised hosts[5]. Cooperation of neighboring ISPs in change point monitoring method must be implemented[8].

REFERENCES

1. John haggerty, Memmber, IEEE, Qi Shi, Member IEEE and Madjid Merabti, 2005. Member, IEEE, Early detection and prevention of Denial-of service attacks: Anovel mechanism with propagated Traced-back attack blocking. IEEE J. Selected Areas in Communications.
2. Stephen, M. specht, 2004. Electrical engineering, Princeton University, Ruby B. Lee, Electrical engineering, Princeton University, Distributed Denial of service: Taxonomies of attacks, tools and countermeasures. Proceedings of 17th Intl. conference on parallel and distributed computing system, 2004. International Workshop on Security in Parallel and Distributed System, pp: 543-550.
3. Valer Bocon, 2004. Developments in Does research and mitigation technologies. Transactions on Automatic Control and Computer Science, pp: 49-63.

4. Minho Sung and jun Xu, 2003. Member, IEEE, IP trace back-based intelligent packet filtering: A novel technique for defending against Internet DdoS attacks. IEEE Transactions on Parallel and Distributed Systems.
5. Shigang Chen, 2005. Member, IEEE and Qingguo Song, Perimeter-Based Defense against High Bandwidth DDoS Attacks. IEEE Transactions on Parallel and Distributed Systems.
6. Shigang Chen and Randy Chow, Department of Computer and Information science and Engineering, University Of Florida, Gainesville, FL 32611, USA, A New Perspective In Defending Against DDoS.
7. Angelos Stavrou, L. Debra Cook, G. William Morein, D. Angelos Keromytis,Vishal Misra and Dan Rubenstein, Department of Computer science, Columbia University in the city of New york, WebSOS: An overlay-based system for protecting web servers from denial of service attacks, Elsevier Science.
8. Haining Wang, Member, IEEE, Danlu Zhang, Member, IEEE and Kang G. Shin, 2004. Fellow, IEEE, Change Point Monitoring for the Detection of Dos Attacks.