Detect DDoS Attack Using Border Gateways and Edge Routers

Sowmyadevi.K
PG Scoloar
Department of Computer science engineering
Coimbatore Institute of Engineering and Technology
Coimbatore, India

Jenitha vincy.T
Assistant Professor
Department of Computer science engineering
Coimbatore Institute of Engineering and Technology
Coimbatore, India

ABSTRACT
The system is design to implement an identification and classification algorithm for tracing DDoS attack and multicast attack information to a edge router using cyclical deterministic packet marking (CDPM) method. Edge router registry stores the received packet IP source address and mark the packet. An Identification and classification algorithm implemented on Border gateway. An algorithm based on received packet and path variation. Border gateways analyze the packet path and number of request received from particular source address. And classify the packet if attacker multicast the attack packet information to edge router and intermediate router or if legitimate packet the border gateway allow to use server. Finally edge router can update their registry and block the attacker IP source address from home network itself. In our proposed model we identify an attack source and multicast the information to an edge router.

Keywords

Edge router, gateway, legitimate user, multicasting, packet marking.

1. INTRODUCTION
One type of attack on computer systems is known as a Denial of Service (DoS) attack. A Denial of Service attack is designed to prevent legitimate users from using a system. Traditional Denial of Service attacks are done by exploiting a buffer overflow, exhausting system resources, or exploiting a system bug that results in a system that is no longer functional. In the summer of 1999, a new breed of attack has been developed called Distributed Denial of Service (DDoS) attack. Several educational and high capacity commercial sites have been affected by these Distributed Denial of Service attacks. A Distributed Denial of Service attack uses multiple machines operating in concert to attack a network or site.

There is very little that can be done if you are the target of a DDoS. The nature of these attacks cause so much extra network traffic that it is difficult for legitimate traffic to reach your site while blocking the forged attacking packets. The Internet anonymous access and non- state characteristics enable the aggressor to forge IP source addresses at random, which causes that victims cannot determine the source of attack. Therefore, it is necessary to study the IP traceback method with the aim of locating the attack source accurately and providing technical support to punish the aggressor. At present, researchers have already proposed various types of IP traceback methods, e.g. input debugging, hash-based IP traceback, and packet marking. However, these methods all have certain limitations in the application. They can only either trace some kinds of attacks or demand consuming large amounts of network resources.

2. ARCHITECTURE

2.1 DDoS Attack
In the network ,Common forms of DDoS attacks is the use of continuous flow rate of the impact of the big servers, causing a server overload handling large amount of garbage flow, and thus cannot handle normal requests [1]. The most essential characteristic is that the normal client-attack aircraft violated the standards of conducts, in no circumstances be allowed to the server, sending a large quantity of super-normal data. Thus, according to the essential characteristics of common network attacks through analysis and research, a new SOA-based active defense network architecture, design and implementation of the overlay network built on top of SOA based DDoS defense framework.

Server's actual location unknown, servers and related equipment over the Internet from the overlay network, overlay networks have two sets of nodes, it is a routing node, corresponding to the Internet on the arbitrary types of apparatuses and those serving node, its corresponding server on the Internet, SOA-based service interface to the outside. Any node within the network coverage of communications between all encrypted. Through the establishment of overlay, that it can effectively hide the location of the server, up to a certain purpose to protect the server. In this system the proved the strong versatility and a strong defense of DDoS attacks, and also this system can find attack source network and node it is used to block the traffic intrusion.This system high overload one, it is tough to develop and co ordinate the web application with web server or application server, it increases the developers overhead SOA is showing

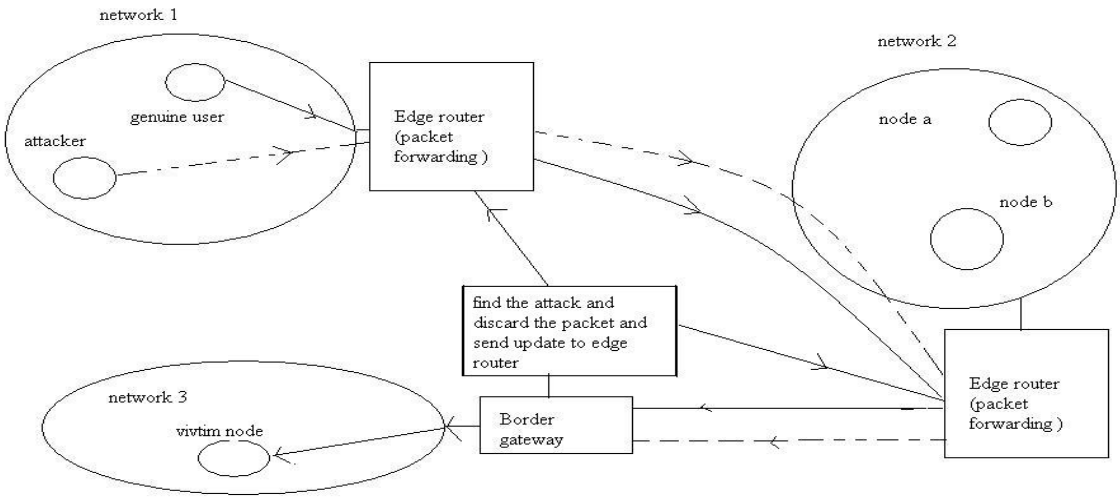

Fig**. 1. Detecting Single Packet DDoS Attack**

that it is a service-oriented framework for the new standards, due to the loose coupling of services and no state of nature, making communication much lower ends of the mutually dependent, it can a good to ensure communication privacy of both parties, and also it proved that is a effective against a large-scale DDoS attacks. This DDoS defense architecture built to achieve in the end stop the invasion of attack traffic source. Through the introduction of SOA and the overlay network, it makes loosely coupled framework and the outside world. And it achieve a universal nature of its underlying architecture, which based on this method of construction can be based encryption to protect the security certificate system architecture.

2.2 Help To Detect

Help to detect some special attacks. The new model brings the attack detection point to the source network of the attack, which makes detection of many attacks become more convenient. As the detection point and attack aircraft in the same network, so the detection point c detection point is easy to judge whether the source address of the data packet issued from its own network is forged, but to judge whether the source address is forged in the intermediate or target network is very difficult.

2.3 Effective Response

Some attacks can only be an effective response in the source network. For example, distributed denial service attacks, are issued from different edge networks, and through the core network convergence, ultimately achieving the target network. Whether in the intermediate or target network, because that the legitimate data packets and various attack packets have been gathered mixed together, so it is difficult to detect which packets are legitimate. In addition, whether the intermediate network's core routers or the victims, security tools in the target network does not have sufficient processing power to deal with these many complex packets. And even if the intermediate or target network can detect and distinguish these attack packets, but at this time they have consumed a lot of additional bandwidth, resulting in a very bad impact. So, to deal with this kind of distributed denial service attacks, to detect and defense them only in the source network is more effective and feasible.

2.4 Easily Accepted

The improved security model does not require a variety of security tools to conduct the number of interactions. So that, it is more easily to be replicated comparing with the distributed network security model needed large-scale deployment. Company, school, ISP and so on can select the desired security technology and products according to their actual situation. Combining with the features of current network security model, this proposed system is an improved network security model and analyzed its advantages: not only more effective response to such a distributed DDOS attacks, and because no request of strict collaboration between the defense node.

2.5 Cyclical Deterministic Packet Marking

The packets referred in this section belong to the flow from the source to the end host unless it is said otherwise. CDPM [2] should be able to handle both single sourced and multiple sourced attacks. Here end host receive a sequence of marked packets. The sequence of marked packets composes of n subsequences and *n* is the number of nodes in the path. The n subsequences of packets are numbered as Pn to P1. The Pi subsequence contains the information of the edge, which is i hops away from the end host. If this concept can be realized, the end host can easily and quickly build the path. To mark an edge, we will need to include the IP addresses of the two routers at its vertices. There are 64 bits in total. In the fragmentation field of the IP header is proposed as a candidate

for marking because it is rarely used in practice. It contains 16 bits. Thus, at least four packets are necessary to carry the IP addresses. However, we need to leave a portion of the fragmentation bits to label different parts of the IP addresses. The label is used during the reassembly of the two IP addresses.

The two addresses are joined and padded with a 0 bit. Then, we divide the data into five pieces of equal size of 13 bits and use 3 bits to label them accordingly. The label and a piece of the two addresses are fitted into the fragmentation field. In summary, five packets are required in CDPM to mark an edge. It should be noted that CDPM does not prohibit more sophisticated edge marking technique being deployed. It should be noted that using the optional field for marking is undesirable. It is said that about 1% of the traffic bandwidth are subject to fragmentation in the network.

Increasing the size of a packet in the network increases the risk of additional fragmentation. Also, when a router performs this edge marking function, it will place the addresses of itself (Ni) and the next router (Ni-1) in the packet headers. A mark will consume 5 packets and these five associated packets are referred to as a packet set. Next, we describe the details of the edge marking function in the routers along the path. When CDPM is activated in a router *Ni*, it enters the initial mode. That is, it attempts to synchronize with its predecessor (Ni+1). It examines packet headers to see if Ni+1 mark the packets. If such marking is not observed for a predefined number of packet sets, say max_hop, then Ni concludes that its predecessor is not trustworthy at this point and changes to the false sync mode and continues looking to synchronize with its predecessor. It, then, starts its own marking cycle. This cycle begins with continuous packet marking. Let the value in time-to-live field in the packet be packet.TTL. And, Ni places (Ni, Ni-1) information in packet headers for packet.TTL times. Then, this router turns to the initial mode and waits for (max_hop-packet.TTL) packet sets. In this waiting period, the router seeks to synchronize with the predecessor.

This system is advanced then probabilistic packet marking (PPM) and deterministic packet marking (DPM) because it can find the full path of the packet and any point of the network. The router goes through its decision tree for each received packet in order to identify the right actions. In general, the increase in computational cost is high and should be consider well spent in boosting the traceback performance. CDPM is a pioneer in considering packet loss and other realistic network conditions. We show that it exhibits extremely fast convergence time, a small fraction of that of the prevailing PPM based schemes. It incurs mild computational overhead in the routers while having comparable complexity in the end host. Unlike its DPM brethren, CDPM can be used to build a much complete path by the end host. It is also demonstrated that it is resilient against packet loss. In this paper [2], we made qualitative discussions on random activation, packet loss, and fragmentation.

3. IMPLEMENTATION DETAILS

3.1 Internet Topology Setup

In this module we will setup the internet topology. We will create five networks and these five networks will be interconnected. Each network has edge routers and intermediate routers. Different IP address and group configuration for each network.

3.2 Agent Border Gateway Creation

In this module we will create new Agent. It will act as a Border Gateway. It is an ordinary Router with extended features. It will check the path of the Packet using path re construction. And it will compare with Standard path and classify the packet. After classification it will mark the packet Multicast the information about attack packet to Edge Routers periodically.

3.3 Multicasting and Packet Marking

In this module Edge Router receive the attack packet information from Border Gateway. Based on the information (SA-DA Pair) Edge Router will mark the packet. After marking the packet based on the traffic, Router will decide whether to forward or discard the packet Information will multicast within the network.

3.4 Packet Filtering

In this module every Intermediate Routers doing the filtering work. It will check the network traffic and Queue length. Based on the Queue length and marked packet value. It will forward the packet to next hop or discard the packet. Packet classifications are attack, and legitimate.

4. IMPLEMENTATION RESULTS

Generated the traffic using hacker node and legitimate node and analyzed the results, implementation results showing that we can reduce the traffic due to communication messages between the gateways.

Fig. 2. Time vs received packets of legitimate and attack packets.

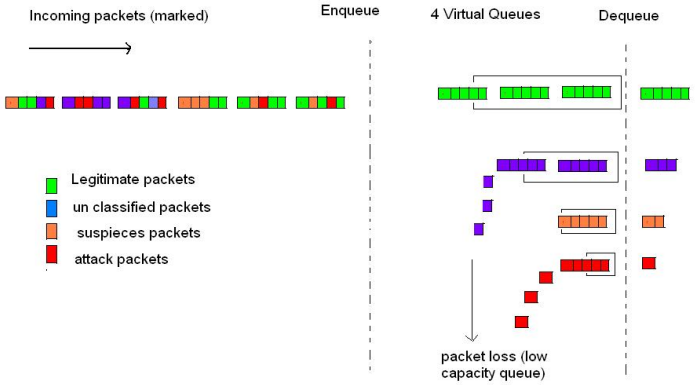

Fig. 3. Packet filtering

5. ALGORITHM

The Algorithm is used to identify and classify the attack packet as follows,

Algorithm for Identification and Classification

Step 1: Start the process

Step 2: Pink the request to a target server. Request sends to an edge router.

Step 3: Edge router store their IP address to an ER registry and mark the received packet.

And then sends to intermediate routers.

Step 4: Intermediate router find the packet mark, analyze the traffic order gateway and queue length. And sends to border gateway.

Step 5: Border gateway using identification and classification algorithm to classify the packets. They are attacked packets, legitimate packets.

Step 6: Identify an attacked packet then the border gateway multicast the message to an edge router and intermediate routers. An intermediate router received message based on priority. Edge routers verify their registry and then block that IP address.

Step 7: Identify legitimate packet then the border gateway allow the user to use server.

Step 8: Stop the process.

6. CONCLUSION

Cyclical Deterministic Packet Marking can trace back single packet attack, Denial of Service attack and Distributed Denial of Service attack. It allows incremental deployment: one new EBG can be known automatically by other EBGs through the

extended BGP. Finally, it multicasts the information to all edge routers. ++. Algorithm for coordinating the border gateways, and reduced the communication and traffic for coordination, our algorithm discarding the attack packets before reaching the victim's network. Simulation results show that CDPM is able to reconstruct the attack path as well as own good feasibility and little influence on the end-to-end delay of IP packet.

7. ACKNOWLEDGMENTS

Our thanks to the experts who have contributed towards development of the project.

8. REFERENCES

[1] Xiaoming Bi, Qiansheng Zheng (July 2010), 'Study on Network Safety Strategy Against DDoS Attack' IEEE International Conference on Advanced Management Science (ICAMS).

[2] Wei Yen, Chao-Cheng-Huang (Oct 2007), 'Cyclical Deterministic Packet Marking' IEEE International Conference on System, Man and Cybernetics(ISIC).

[3] S. Savage, D. Wetherall, A. Karlin, and T. Anderson (Jun 2001), 'Network Systems support for IP traceback' IEEE-Acm Transactions on Networking, vol. 9, pp. 226-237.

[4] D. X. Song and A. Perrig (2001), 'Advanced and Authenticated Marking Schemes for IP Traceback' in Proceedings - IEEE INFOCOM, pp. 878-886.

[5] A. Belenky and N. Ansari (Apr 2003), 'IP traceback with deterministic packetmarking' IEEE Communications Letters, vol. 7, pp. 162164..

[6] R. P. Laufer, P. B. Velloso, D. d. O. Cunha, I. M. Moraes, M. D. D. Bicudo, M. D. D. Moreira, and O. C. M. B. Duarte (2007), 'Towards Stateless Single-Packet IP Traceback' in 32nd IEEE Conference on Local Computer Networks, Washington, pp. 548-555.

[7] A. Castelucio, A. Ziviani, and R. M. Salles (2009), 'An AS-Level Overlay Network for IP Traceback' in IEEE Network. vol. 23, pp. 36-41.

[8] Yang-Seo Choi, Jin-Tae Oh, Jong-soo Jang, Jae-Cheol Ryou (Aug 2010), 'Integrated DDoS Attack Defense Infrastructure For Effective Attack Prevention' IEEE 2nd International Conference on Information Technology convergence and services (ITCS).

[9] Feng Qiaojuan,Wei Xinhong (2010), 'A New Research on DoS/DDoS Security Detection Model' IEEE 2nd International Conference on Computer Engineering and Technology, vol. 3.

[10] Y. Bavani, P. Niranjan Reddy (July 2010), 'An Efficient IP Traceback Through Packet Marking Algorithm' International Journal of Network Security and Its Application, vol 2, No.3.

[11] Baijian Yang, Prasant Mohapatra (June 2005), 'Edge Router Multicasting With MPLS Traffic Engineering' IEEE Communications Letters.

[12] Linfeng Zhang, Yong Guan (2005), 'TOPO: A Topology-aware Single Packet Attack Traceback Scheme' Department of Electrical and Computer Engineering, Iowa State University.

[13] Robert Stone (2003), 'CenterTrack: An IP Overlay Network for Tracking DoS Floods' UUNET Technologies, Inc.

[14] Javad Ebrahimi, Christina Fargouli (2010), 'Multicasting Algorithm For Deterministic Networks' on Computer and Communication Sciences.

[15] S. Savage, D. Wetherall, A. Karlin, and T. Anderson (Jun 2001), 'Network Systems support for IP traceback' IEEE-Acm Transactions on Networking, vol. 9, pp. 226-237.

[16] D. X. Song and A. Perrig (2001), 'Advanced and Authenticated Marking Schemes for IP Traceback' in Proceedings - IEEE INFOCOM, pp. 878-886.

AUTHOR PROFILE

Sowmyadevi Kanagasabapathy B.Tech., (M.E)., Currently pursuing Master of Engineering in Coimbatore Institute of Engineering and technology, Anna university Coimbatore. As completed B.Tech Information technology in Coimbatore Institute of Engineering and technology, Anna university chennai. Her research work is in the Data mining and Computer.