ISSN: 2321-7782 (Online)

Volume 2, Issue 11, November 2014

International Journal of Advance Research in Computer Science and Management Studies

Research Article / Survey Paper / Case Study

Available online at: www.ijarcsms.com

A Review Paper On Proactive & Detection Strategy Designing For DRDoS Attack

Dipika Mahire[1]
Department of Computer Engineering,
G. H. Raisoni Collage of Engineering and
Management, Ahmednagar.
University of Pune, India

Amruta Amune[2]
Professor, Department of Computer Engineering,
G. H. Raisoni Collage of Engineering and
Management, Ahmednagar.
University of Pune, India

Abstract: : Nowadays , network security has become more important as attackers attacks the local networks .The Distributed Denial of service is one of the most famous attack which floods the victim(server)with the number of packets. so that, legitimate users can't access the service provided by the server. Detection of DDoS & DRDoS attack is somewhat difficult. But, there are many techniques available for detecting DDoS & DRDoS attack. Some of the techniques and papers we are reviewing here in this paper.

Keywords: DDOS attack, flash crowd, pushback, Identifier/Location Separation, TTL, DPM.

I. INTRODUCTION

Denial of Service (DoS) attacks is very common in the world of internet today [7][1]. They are difficult to detect because they do not target specific vulnerabilities of systems, but rather the very fact that the target is connected to the network. All known DDoS attacks make the use of the large number of hosts on the Internet that are vulnerable; the attacker break into such hosts, install slave programs, and at the right time instruct thousands of these slave programs to attack a particular destination. The attacker makes attack on the victim by sending large number of packets to the victim, and there is almost the victim can do nothing to protect itself. The Denial of service attack has 2 forms:

DDoS(Distributed Denial of Service)

DRDoS(Distributed Reflector Denial of Service)

At present, DDoS (Distributed Denial of Service) and DRDoS (Distributed Reflector Denial of Service), which invented from DoS, have already become famous in network attacks. In DDoS attack, the attacker controls some master zombies machines and large number of slave zombies machines; it sends attack commands to master zombies machines, then the master zombies instructs slave zombies machines to flood the victim, as shown in Fig. 1. & Fig .2

DDoS attack: A distributed denial of service attack (DDoS) (refer to fig 1) occurs when multiple machines flood the victim, usually the victims are web servers. In the DDoS attack the attacker searches for vulnerable system for attack called Zombie machine. Attacker instructs the vulnerable system(Zombie machine) to attack on the victim.

DR-DoS attacks : Distributed reflector denial of service (DRDoS) **(refer to** Figure 2) Illustrates another type of attack called a **distributed reflector denial of service** (DRDoS) attack, which hides the sources of attack(attacker) traffic by using third parties (routers or web servers) to send attack traffic to the victim. These innocent third parties are also called the reflectors. Any machine that replies to an incoming packet can become reflector.

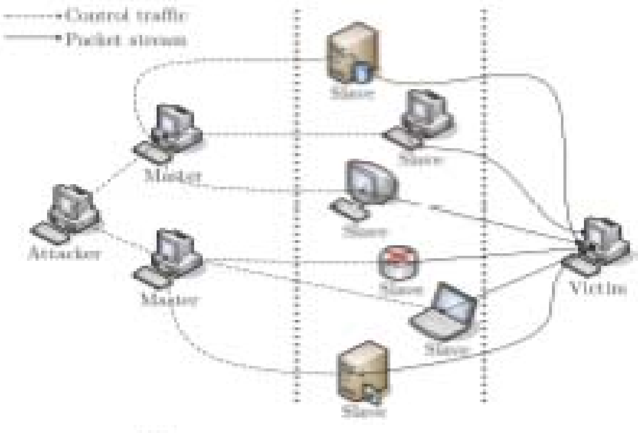


Fig. 1: Structure of DDoS attack

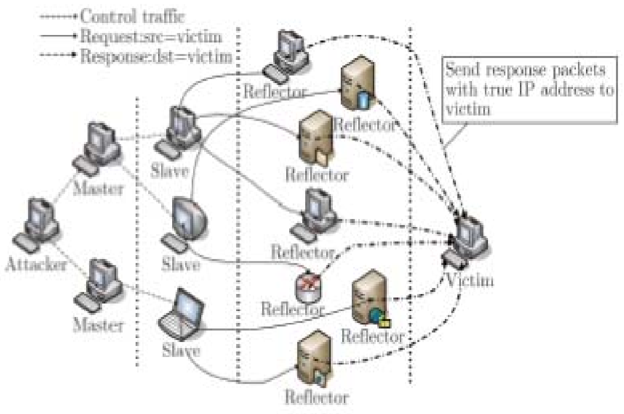
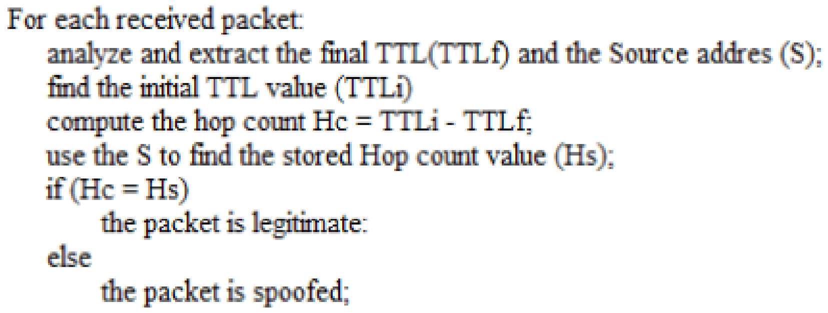


Fig. 2: Structure of DRDoS attack

II. Literature Survey

Hongbin Luo, Yi Lin and Hongke Zhang[5] has proposed the technique in which they have separated the identifier(represents identity), locator(represents *location).*While in today's world the IP address consist of both identity and location into it. So, If we separate the identifier from locator it helps to prevent DDoS attack [6]. In these technique only web servers which provides some service is registered into the Mapping system (MS) which maps the locator (location) from the identifier (identity). When the attacker searches for the vulnerable host for attack, it needs to send the packet to the hosts and to send the packets it should know both identifier and locator of the host. So, attacker can get only the identifier as it is publically available but it can't get the locator because normal clients are not registered into the MS.

Sneha S. Rana, T. M. Bansod proposed the technique which uses the Hop-count filtering technique to detect the IP spoofing.and also uses the traceback to get the source of attack.In hop-count filtering the final TTL value of IP packet header is compared with the initial TTL value. If the difference is not equal to already stored hop count value that means it is the not legitimate user. And traceback mechanism is used to find the source of attack.



```
For each received packet:
    analyze and extract the final TTL(TTLf) and the Source addres (S);
    find the initial TTL value (TTLi)
    compute the hop count Hc = TTLi - TTLf;
    use the S to find the stored Hop count value (Hs);
    if (Hc = Hs)
        the packet is legitimate:
    else
        the packet is spoofed;
```

Fig. 3 Algorithm for TTL based detection

Andrey Belenky and Nirwan Ansari has given a traceback[4] mechanism to detect the attack by using Dynamic packet Marking(DPM). Fig.3 Shows the scenario of DPM. Each incoming and outgoing packets are marked by the router. With some probability the address of the packet is marked in the router table. And this information is used to reconstruct the attackers path when the network experience the attack. The DPM(Dynamic packet marking)is easy to implement; It has low processing and no bandwidth overhead.

Dhruv A. Patel presented the technique in which he used HIP (Human Interaction Page) [7]which issues the graphical tests for the client, if client can't solve the puzzle put them into white list. Otherwise, allow the connection to the web server. If the client is already present in the white list rate limiter is applied to it to deny the access. This mechanism improve availability of web server for legal users .Fig 4 shows the flow of the system.

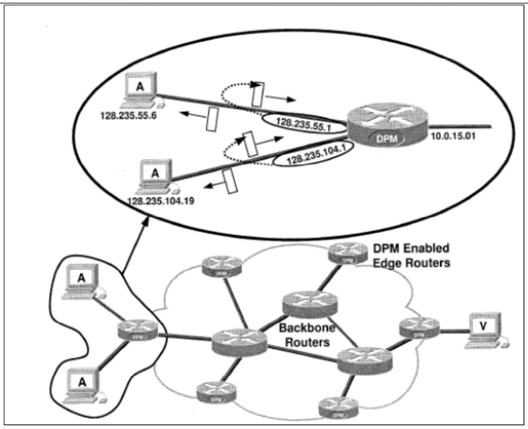


Fig 4.Deterministic Packet Marking

Saravanan Kumarasamy and Dr. R. Asokan presented the mechanism for defending against DDOS attack called Pushback. In which the intelligent router in ISP network identifies the attack traffic and sends pushback[3][8] message to the upstream routers. The upstream routers issues the graphical test to the client. And if the client can solve the puzzle then traffic from that particular client is taken as legitimate traffic else traffic from that client will be dropped. So, this technique minimizes the overhead of the intelligent router by sending the pushback messages to upstream routers. And remaining work is done by upstream routers. The only drawback of the mechanism is legitimate users also have to go through the puzzle test which wastes its time.

Srikanth Kandula Dina Katabi has proposed the mechanism called Kill-Bot which has two stages:1)Authentication 2)Admission control.So, in Killbot[2] first check the incoming packets source address if it is a zombie then it will be discarded.Otherwise,it admits the new client with probability $\alpha = f(load).$ and issues the puzzle for the client to check whether the client is zombie or not. If the client solves the puzzle it means it is legitimate client, so connection is accepted. otherwise the packet is droped by assuming it as zombie.Fig. 5 shows the kill-bot working.Even the legitimate client can't solve the puzzle in some attempts, it can try for particular threshold value ξ=32 And for this purpose the bloom filter is used. The bloom filter value incremented each time by one when the puzzle is issued for the client. The packet will be dropped when it reaches the threshold value by assuming it zombie.

Shui Yu, Theerasak Thapngam, Jianwen Liu, Su Wei and Wanlei Zhou has proposed the algorithm to discriminate DDoS flow from the flash crowd[12][13].In this algorithm the suspicious flows are sampled per time unit T by the cooperating router.After sampling is done the data is exchanged between the router and then router calculates the similarity flow using Sibson distance formula.If the calculated value is less than threshold then the flows are

DDoS attack flows, otherwise, the flash crowds.

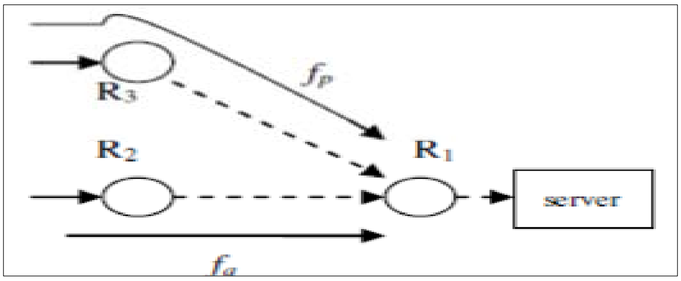


Fig 5.Sample network with two traffic flow

Hiroshi Tsunoda, Kohei Ohta, Atsunori Yamamoto, Nirwan Ansari[10] has proposed the simple response packet confirmation mechanism. In this the each request-respose pair is validated. The architecture for detection system consists of Translator, Comparator, Short-term buffer and long-term buffer. The fig 7. Shows the basic architecture of simple response packet confirmation mechanism.

The request-response relationship are of 2 types. One-One and One-Many relationship.The One-One response packets is called Clear response packets which are stored in short term buffer. while One-Many response packets are called Ambigous response packets which are stored in long term buffer. The original response packet is compared with the response packet generated by the translator.If the both response packets are same that means the packets are not attacking packets. And if it differs that means response packets are attack packets.

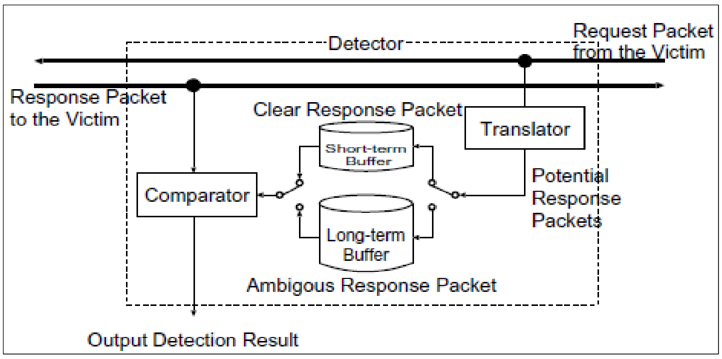


Fig. 6 Basic architecture of Simple Packet confirmation system

Xinyu Yang, Wenjing Yang has proposed the fuzzy association rule based DRDoS attack detection technique. It uses the DRDoS Attack Defensive Architecture based on Multi-Agent (D2AMA)algorithm[9]. Fig.8 shows the architecture of D2AMA. D2AMA consists of Brouter(border router), analyzer and control agent CA. The Brouter marks the traffic i.e. if it is the ingress router it marks the information from the incoming router and if it is the egress router it will mark the packet by its own address. So that the malicious packets or traffic can be identified easily.While the Association rule analyzer collects all the traffic information and by sending signals(alarm or No-alarm) it communicates with CA. The CA will then sends the commands to suspicious Brouter for dropping the packets.

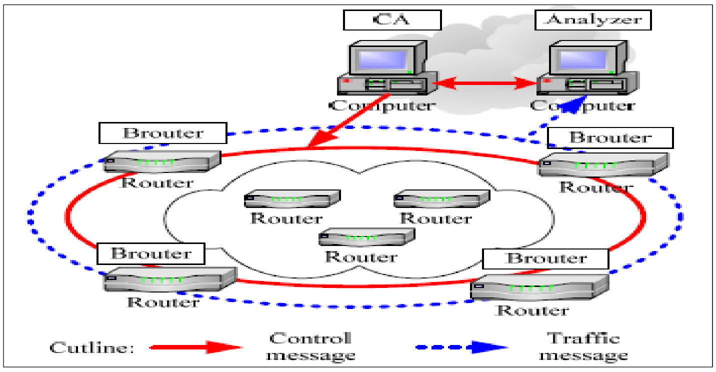


Fig 7.D2AMA

III. Conclusion

In this way we have studied the existing approaches for DDoS and DRDoS attack detetction. Today, DDOS attack has become more famous in the network. There were many techniques implemented to detect DDOS attack. So, as we have mentioned different techniques to detect DDOS attack.The Identifier/Locator separation scheme is also effective technique. But still it takes more time to locate the host. Most simpler technique is puzzle test. But the puzzle test is somewhat time consuming for legitimate clients. The traceback mechanism(DPM)is one of the best mechanism to detect the attacker of the suspicious traffic. DRDoS attacks may also defended using the given techniques. Fuzzy association rule algorithm and simple packet confirmation is effective techniques to detect DRDoS attack. But out of both the fuzzy association rule algorithm is more effective than other one. As it just check for limited request response packets.

References

1. Jelena Mirkovic,Sven Dietrich,David Dittrich,Peter Reiher, ―Internet Denial of Service:Attack and Defencse Mechanisms

2. NSDI '05: 2nd Symposium on Networked Systems Design & Implementation- Botz4Sale: Surviving Organized DDoS Attacks That Mimic Flash Crowds

3. John Ioannidis and Steven M. Bellovin, ―Implementing pushback: Router-based defense against DDoS attacks,‖ in *Proceedings of Network and Distributed System Security Symposium,* Suite 102, Reston, VA 20190, February 2002,The Internet Society.

4. Andrey Belenky and Nirwan Ansari, IP Traceback With Deterministic Packet Marking- IEEE COMMUNICATIONS LETTERS, VOL. 7, NO. 4, APRIL 2003

5. Hongbin Luo, Yi Lin, and Hongke Zhang-Preventing DDoS Attacks by Identifier/Locator Separation, IEEE

6. D. Farinacci et al., "Locator/ID Separation Protocol (LISP)," IETF RFC 6830, Jan. 2013.

7. Dhruv A. Patel, Prof. Hasmukh Patel-Detection and Mitigation of DDOS Attack against Web Server Volume 2, Issue 2| ISSN: 2321-9939

8. Saravanan kumarasamy, DR.R.Asokan- Distributed Denial Of Service (DDoS) Attacks Detection Mechanism, International Journal of Computer Science, Engineering and Information Technology,Vol.1,No.5,December 2011.

9. *Xinyu Yang, Wenjing Yang, Yi Shi, Yage Gong,* The Detection and Orientation Method to DRDoS Attack Based on Fuzzy Association Rules, Journal of Communication and Computer, ISSN1548-7709, USA

10. Hiroshi Tsunoda , Kohei Ohta , Atsunori Yamamoto , Nirwan Ansari , Yuji Waizumi , Yoshiaki Nemoto- Detecting DRDoS attacks by a simple response packet confirmation mechanism.

11. F. K. Ghalati, "Defending Against Distributed Denial of Service Attack Under Tunnel based Forwarding," Master Thesis, Aalto University, Aug. 2011.

12. G. Carl, G. Kesidis, R.R. Brooks, and S. Rai, "Denial-of-Service Attack Detection Techniques", *IEEE Internet Computing*, Vol. 10, No. 1, January 2006, pp. 82-89.

13. Y. Chen and K. Hwang, "Collaborative Change Detection of DDoS Attacks on Community and ISP Networks", *the IEEE International Symposium on Collaborative Technologies and Systems (CTS 2006)*, May 2006, pp. 401-410.

14. Subramani rao Sridhar rao. Denial of Service attacks and mitigation techniques: Real time implementation with detailed analysis.2011- SANS Institute InfoSec Reading Room.

15. Qijun Gu, Peng Liu. Denial of Service Attacks. Department of Computer Science Texas State University – San Marcos School of Information Sciences and Technology Pennsylvania State University Denial of Service Attacks Outline, 1–28.

16. International Journal of Advanced Research in Computer Engineering & Technology-IP Spoofing Attack Detection using Route Based Information, Volume 1, Issue 4, June 2012

AUTHOR(S) PROFILE

Miss. Dipika R. Mahire, Research Scholar, G. H. Raisoni Collage of Engineering and Management Ahmednagar, University of Pune, India. She received B.E. in Information Technology from K.C.E College of Engg. Jalgaon,India.

Prof. Amruta Amune received the B.E. and ME degrees in Computer Science and Engineering. Currently she is working as Assistant Professor at Computer Engineering Department in G. H. Raisoni Collage of Engineering and Management, Ahmednagar, India**.**