ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

Detection Prevention and Tracing Source of IP Spoofing Using HPS Technique

Meghana N M

PG student, CNE, Dept. of IS&E, National Institute of Engineering, Mysuru, India

ABSTRACT: It is very difficult to overcome from DDoS attack if attacker changes the source address in IP packets and send it to target system. Since each packets having different Source IP address it is difficult to detect an attack, find original source of attacker and to avoid the attack. In this paper we present a technique which includes efficient mechanisms to detect attack, to detect source of attacker and to avoid the attack.

KEYWORDS: Computer Network Security, IP traceback, Distributed denial of service, IP Spoofing, Multi-dimensional sketch, Hellinger distance

I.INTRODUCTION

In Distributed Denial of service attack there is a flood of messages to the particular target machine and it forces it to shut down, thereby interrupting the service to the actual users.
There is mainly two types DDoS attack
1. Network-centric attack: Here attacker denying the service by utilizing network bandwidth.
2.Application-layer attack: Here attacker overloads a service with multiple numbers of application calls.

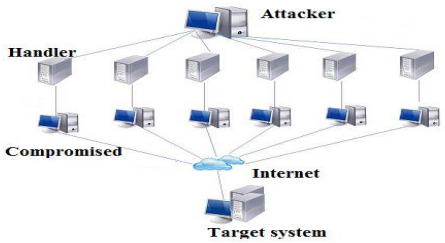

Figure 1: DDoS attack

DDoS is hard to detect avoid because these DDoS is implemented with IP Spoofing as shown in figure 1. In case of IP Spoofing source address of IP packet is changed. So it will become difficult to detect attack because each time source IP addresses changing. Here we make use of efficient multidimensional sketch method to detect attack and to detect original source of attacker we uses the passive IP traceback mechanism also to avoid this IP spoofed DDoS attack we use mechanism to temporarily block ISP .
In this paper we explained these three mechanisms and show the simulation result.

II. RELATED WORK

[1] Here author Stephen M. Specht et.al explained in detail about taxonomies and countermeasures of DDoS attack. They explained in detail about bandwidth depletion attack and resource depletion attack and also explained mechanisms for Prevent Secondary Victims, Detect and Neutralize Handlers, Detect or Prevent Potential Attacks and Mitigating the Effects of DDoS Attacks.
[2] Here author Wei Wang et.al presents a method to detect intrusion using some of network traffic key attributes and they prove the effectiveness of detecting intrusion only by considering 10 network traffic attributes and these traffic attributes are selected based on filter based attribute selection, wrapper based attribute selection and here they uses

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

separate new program to identify attack with 10 traffic attributes this program will convert tcpdump traffic into connection records.

[3] Jin Tang et.al presents a technique that will provide a efficient method to detect low rate flooding and detect flooding caused by multi attribute manner. Here author uses sketch data distribution and HD based detection for more flexible and efficient solution and here estimation freeze mechanism shows ability to maintain information about normal behavior under attack and this method is not applicable for large range of DDoS attack.

[4] Here author Syedasaleha Yasmeen et.al presents a sketch based design for recognizing flooding attack. Here author develop a scheme to detect and preventing the IP flooding attack. Hear author combine Sketch method along with Hellinger Distance algorithm.

[5] Here author Kejie Lu et.al presents a robust and efficient method to detect distributed denial of service attack. Here they presents a framework for exploiting spatial and temporal correlation of DDoS traffic. To detect the DDoS attack signal processing and machine learning technique are used. But in this method new real users dropped when detecting the DDos attack.

[7] Here author Stefan Savage et.al discuss about denial of service attack and presents a traceback mechanism which is based on probabilistic packet marking . This approach allow victim to identify attacker traffic path without taking support from Internet service provider. But here author not completely discuss about distributed attack and attack origin detection methods.

III. PROPOSED SYSTEM

In order to detect the attack and finding original source of attack and blocking DDoS attack 3 different methods have been used those are multi dimension sketch design for detecting attack and passive IP traceback mechanism to find original source of attack and temporary ISP blocking to prevent from DDoS attack.

1. *Detect DDoS attack*

It is very difficult to detect the DDoS attack because these attacks are implemented by spoofing the source IP address of packet. So in order to detect this attack we make use the novel three-dimensional sketch design[9] with the Hellinger distance (HD) detection technique. Sketch is used to determine constant size network traffic summary. And HD method is used find difference between two distributions. And when this HD value exceeds threshold value then we declare that attack has been occurred. This method will provide high detection accuracy in low rate flooding also.

2. *Finding original source of attack*

Since Source address of each IP Packets have been changed it is very difficult to detect the source of attack. There are many different methods[8] are there to detect original source of attack but there is deployment difficulty in each of this method. So in order to overcome from this here we make use of passive IP traceback mechanism[10] this mechanism uses path back scatter messages and uses only publicly available information to find out actual source of attack. And here we use Loop free assumption and Valley-free assumption to find out accurate location.

3. *Preventing DDoS attack*

If Distributed denial of service is caused from single Source then it can be easily prevent by blocking all IP packets from that particular IP address. But this method of preventing is not applicable here because attacker spoofs the source IP address so it is not possible to block all packets from all IP address. So here we temporarily block particular ISP on which all spoofed packets are arriving.

IV. SYSTEM ARCHTECTURE

To detect the DDoS attack HD detection method has been used here attacker sends spoofed traffic to receiver through router at receiver we run HD detection technique to detect attack as shown in Figure 2. Once attack has been detected this will inform receiver about the attack.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

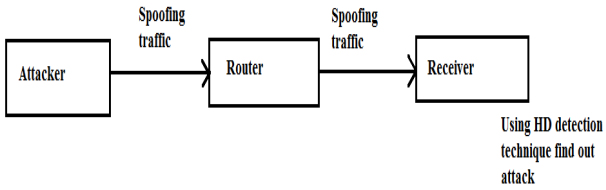

Figure 2: Attack detection

Once conformed about attack next step is to identify the original source of attacker. To find out source we are using the path backscatter messages.

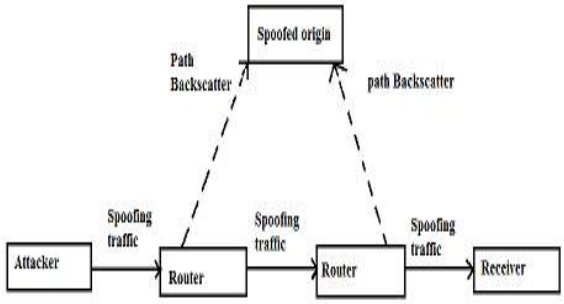

Figure 3: Path backscatter generation and collection

As figure 3 shows the path backscatter messages generated by router are send to source IP address in original packet. That is here host whose address are forged will get all pack backscatter messages.

V. SIMULATION RESULTS

When multiple number of ftp packets arriving for a particular system it due to heavy traffic denying the services of the system so first system have to identify whether is fake ftp packet or real ftp packet if it is fake ftp packet as shown in figure 4 then have to find out whether it is an attack or normal messages.

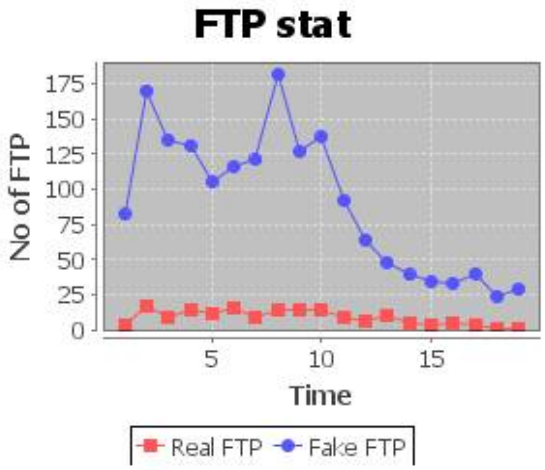

Figure 4: graph to find out number of real ftp and fake ftp

To find out attack above mentioned detecting DDoS attack method has been used. Here a threshold is fixed if traffic is greater than that of the threshold value then it give notice that attack has been accrued if not no action will take place.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

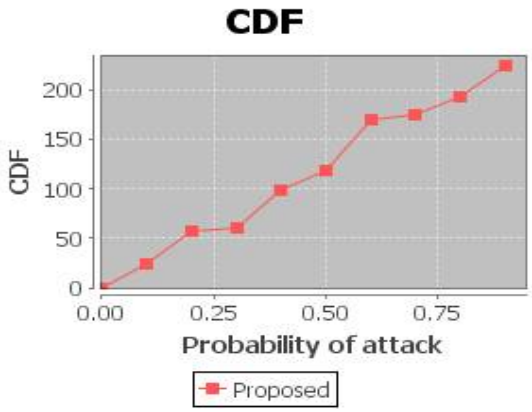

Figure 5: CDF graph

Above graph figure 5 represents CDF of accurate location of attack based on loop free assumption. This probability of location of attacker is based on random tuple.

VI. CONCLUSION

Since it is very difficult to detect and avoiding DDoS attack in network here we discuss a efficient method which include three different methods to detect the attack, find source of attacker, and to avoid the attack. And this method uses only generally available information to find out actual source of attack hence cost of adopting this method is less. And here we prove it with simulation results.

REFERENCES

[1] Stephen M. Specht, Ruby B. Lee "Distributed Denial of Service: Taxonomies of Attacks, Tools and Countermeasures"
[2] Wei Wang, Sylvain Gombault, Thomas Guyet , "Towards fast detecting intrusions: using key attributes of network traffic"
[3] Jin Tang, Yu Cheng and Yong Hao, "Detection and Prevention of SIP Flooding Attacks in Voice over IP Networks" 2012 Proceedings IEEE INFOCOM
[4] Syedasaleha Yasmeen, Amena Sayeed, Khadarbi Shaik," Sketch Based Designs for Recognising Flooding Attacks"IJSETR August 2015
[5] Kejie Lu , Dapeng Wu , Jieyan Fan , Sinisa Todorovic , Antonio Nucci,"Robust and efficient detection of DDoS attacks for large-scale internet" Science direct Computer Networks 51 (2007) 5036–5056.
[6] H. Wang, C. Jin, and K. G. Shin, "Defense against spoofed IP traffic using hop-count filtering," IEEE/ACM Trans. Netw., vol. 15, no. 1, pp. 40–53, Feb. 2007.
[7] David Moore, Geoffrey M. Voelker and Stefan Savage "Inferring Internet Denial-of-Service Activity"
[8] K. Arun Kumar , K. Sai Ashritha "Analysis of Various IP Traceback Techniques - A Survey" International Journal of Computer Applications (0975 – 8887) Volume 77– No.13, September 2013.
[9] Jin Tang, Yu Cheng, Yong Hao, and Wei Song "SIP Flooding Attack Detection with a Multi-Dimensional Sketch Design" Ieee Transactions On Dependable And Secure Computing, Vol. 11, No. 6, November/December 2014
[10] G. Yao, J. Bi, and Z. Zhou, "Passive IP traceback: Capturing the origin of anonymous traffic through network telescopes," in *Proc.* ACM SIGCOMM Conf. (SIGCOMM), 2010, pp. 413–414. [Online]. Available: http://doi.acm.org/10.1145/1851182.1851237