International Journal of Latest Trends in Engineering and Technology
Special Issue NCRTCC 2017, pp.026-031
e-ISSN:2278-621X

AN APPROACH TO TRACEBACK THE IP PACKETS DYNAMICALLY IN DDOS ATTACK

A.Revathi[1], Mrs. J.Vijayalakshmi[2], Dr. C. R. Rene Robin[3]

Abstract—A goal of network security is to protect the network and its component parts from unauthorized access and misuse. Distributed Denial of Service (DDOS) attack is a critical threat to the Internet. An IP traceback is a technology to control internet crime. Dynamic Deterministic packet marking (DPM) which are used to find out the malicious users who produce the volume of traffic needed to deny a services to computer user. Based on this finding, we have a tendency to propose a completely unique Marking On Demand (MOD) traceback supported in the DPM mechanism. Similar to existing schemes, only the participated routers to put in a traffic monitor. Once a monitor notices a surge of suspicious network flows, it will request associate degree distinctive mark from a globally shared MOD, and mark the suspicious flows with the distinctive marks. The mode server records the knowledge of the marks and their connected requesting addresses. Once the DDOS attack is confirmed, the victim will get the attack sources by requesting the MOD server with the marks extracted from attack packets. In this paper, the suspicious packet is detected by threshold value. The confirmed DDoS attack is detected when it is greater than the experimented threshold value.

Keywords- cyber security, IP trace back, packet marking, scalability

I. INTRODUCTION

Network security consists of the policies and practices adopted to prevent and monitor unauthorized access and denial of a computer network and network-accessible resources. Network security involves authorized user for handling data in a network which is controlled by a network administrator. Users have a unique ID and password or other authenticated information for the purpose of access the information and program within the authority.

Distributed Denial of Service (DDOS) attack remains an open problem. Detection, mitigation and traceback are the research in this field. The detection performs attack source and traceback is a step to eliminate cyber attack and mitigation helps in minimization of potential impact of threat. The definition of DDOS attack source traceback is identifying a node on an attack path. Detection and traceback strategies are specific features of DDOS attack. The packet marking mechanism is categorized into two: probabilistic packet marking and deterministic packet marking. The basic idea is to inject marks into the unused space of IPv4 head to trace the source of the packet. DPM mechanism is better for traceback mechanism in comparison with PPM because of its accurate, low demand on storage and computing power.

Packet marking is a technique in which the routers in the intermediate network mark, either probabilistically (PPM) or deterministically (DPM) and the packets that pass through them. These marks are used to check whether the packet is from authorised person. The main idea of PPM is to mark the packets probabilistically as they traverse through the routers. A packet can carry only a partial data and after receiving the number of packets, the path can be reconstructed using the marking information. In DPM, a router would mark all the packets that pass through it. The idea is to write either upper or lower half of the IP address of the ingress edge into the packet with a random probability and a reserved bit indicates which portion of the address is placed in the ID field of the packet.

[1] *Dept. of Computer Applications, Sri Sairam Engg. College*
[2] *Dept. of Computer Applications, Sri Sairam Engg. College*
[3] *CSE Department, Jerusalem Engg.College*

An IP traceback method has following features:
a. Providing the information about the path traversed to traceback
b. Ability to perform single packet IP traceback
c. Support for backward compatibility: As the packets may undergo fragmentation and valid transformations when they move towards the destination, a traceback system should be able to run under such cases.

The DPM schemes suffer a critical disadvantage and scalability problem in practice. There are at least two million routers on the Internet, and the current DPM schemes covers only possible routers. Defenders can only trace 2,048 sources in the original DPM scheme in according to [2].

To perform traceback task, the DPM mechanism introduce a Marking on demand (MOD) scheme for dynamically assign making IDs which is done by related routers. The proposed framework, we set up a global mark distribution server (MOD server) for marking the suspicious packets. At every local router the DDoS attack detector is installed to monitor the network flow. Whenever a suspicious network flow overload, the detector requests unique IDs from the MOD server, and injects the assigned unique IDs to mark the suspicious flows. The MOD server has a database it stores information about time stamp, requesting IP address and assigned mark. Once an attack is confirmed, the unique marks can be extracted from the attack packets. We can search the MOD database to identify the IP addresses of the attack sources using the marks. In IPv4 packet head, there are some unused bits, which are usually 16, 17, 19 or 24 bits for different underlying protocols that is given[2].

II. Proposed System

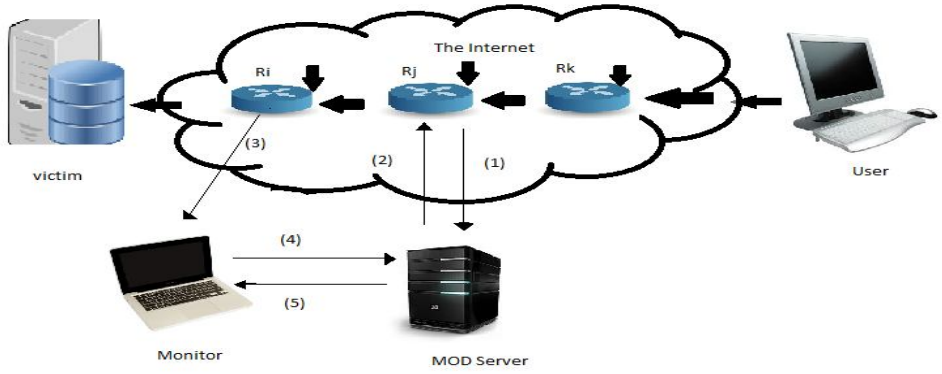

Fig.2. Marking on demand scheme for DDoS attack traceback.

From the above diagram Ri, Rj and Rk are routers which is used to detect the suspicious flow. The MOD server is used from making a unique mark for the suspicious flow. The router Rj senses the packet, if it is within the threshold value that packet is sent to the MOD server. The Marking is done in the unused space of IPv4 header of 16, 17, 19 or 24 bits. The given router defines the network layer packets that share the same destination address as a network flow or a flow. Then we call a DDoS attack flow as an attack flow. Due to the detection sensibility, the router Rk may not able to detect the possible attack and the router Rj may able to detect a surge of flows but cannot confirms the attack. Then the threshold value is greater than the experimental value, the DDoS attack is confirmed by the router Ri.

Once an attack has been confirmed, the router Ri will notify the MOD server regarding mark that is extracted from the marked packets. The MOD server can update its database to identify the earliest marking router on an attack path using the unique mark.

A detailed work flow of the traceback methods are:

1) When there is a suspicious surge of network flows, the detector (e.g., Rj) checks the marking space of the packets of the suspicious flows. If any packet is marked it ignores the packet. If it is not marked, then submits a request to the MOD server for a unique mark.

2) The MOD server identifies a unique mark to serve the request, and it stores the related information such as the mark, request source IP address, time stamp into its database.

3) The detector Rj uses the assigned mark to pad the suspicious passing flows at the available marking fields.

4) As the magnitude of attack flows gets sufficient, a downstream detector is able to identify the attack. The detector Ri will notify the MOD server about the attack with the unique marks. The MOD server will set this information in its database. Moreover, the detector will also notify the system monitor of the victim domain with the attack and its related unique marks.

5) When the monitor performs the traceback task, it queries the IP addresses related to the unique marks that it received.

6) The MOD server checks its database about the marks, and responds the request with the related IP addresses. The monitor knows the attack sources and related action could be taken to counter the attack.

III. EXPERIMENT AND RESULTS

The experiment and result of threshold value is calculated from the raw data. The traffic ratio is calculated by (no. of outgoing packets/ no. of incoming packets). This study is based on detecting the DDos attack[6].
An approach consists of keeping a table for monitoring TCP traffic ratios in order to detect attack traffic. During a DDoS attack, no acknowledgments will be sent because the victim will be overwhelmed. Our first intention consisted of monitoring each individual TCP connection by keeping a table of TCP traffic ratios in order to detect potential attack traffic. We monitor the total number of outgoing packets and incoming traffic regardless of which TCP connection the packets belonged to. By adopting this method, we are reducing the processing time by each packet. Once a DDoS attack is confirmed, the traffic ratio is higher than usual because the number of outgoing packets is greater than the number of incoming packets. By approaching this method, if the value of traffic ratio is within the threshold, we can avoid the false-positive numbers. Based on the raw data acquired to measure traffic ratios, the value of the threshold should be chosen from 1.5 to 2.5.

Threshold	Attack Rate[p/s]	Attack Duration [s]	Attack Detection [time,s]
2.0	100	30	-
1.5	100	30	11.423
1.3	100	30	8.4635

Table 1. Experiment Settings and Results [Average][6]

Finding the DDoS attack is not only based on threshold value, it also based on size of the data on the packet. The router1 may not able to detect any attack it just forward the packet to the next router. The router2 checks the packet, if there is any suspicious flow ariase it sent the packet to the MOD server for marking scheme.

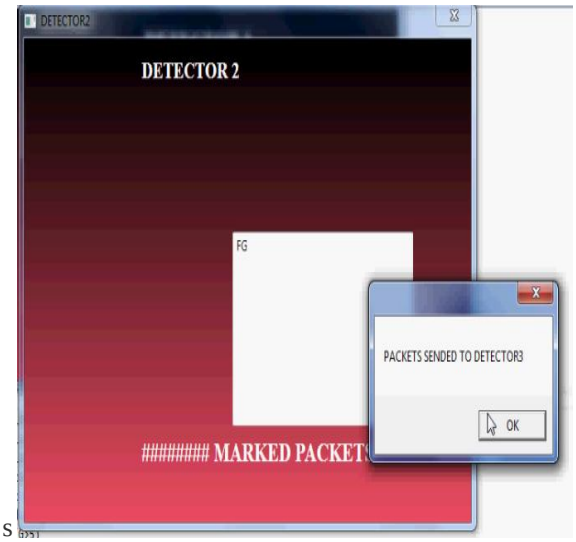

Fig. 2. Marked packet is forwarded to detector3

Dectector2 checks the size of the packet. The packet is considered as authenticated packet based on the size of the packet. So, the packet is Forwarded to detector3

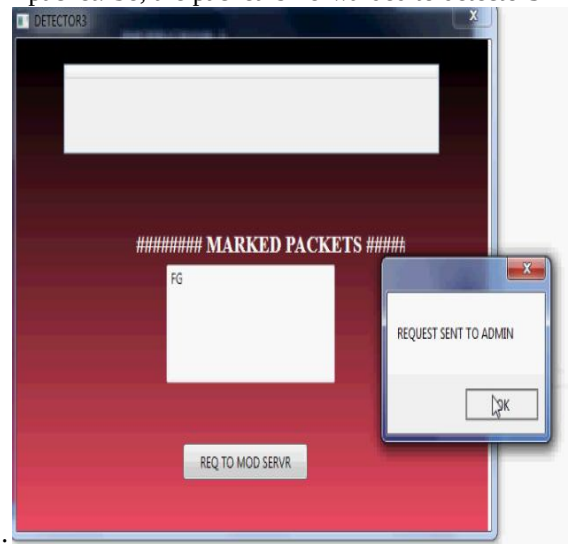

Fig.3. Packet forwarded to Admin

The detector3 confirmed it as an authenticated packet. So, there is no need for marking the packet. Then the packet is forwarded to admin for response to the user.

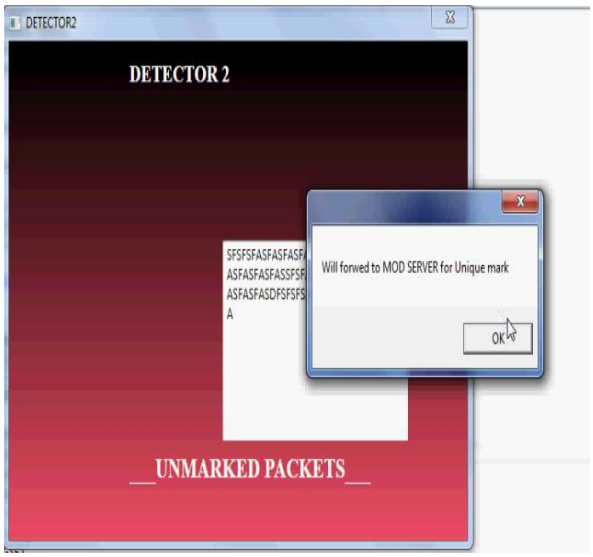

Fig.4. Packet forwarded to MOD server

If there is any suspious flow is detected in detector2, then it is forwarded to MOD server for unique mark.

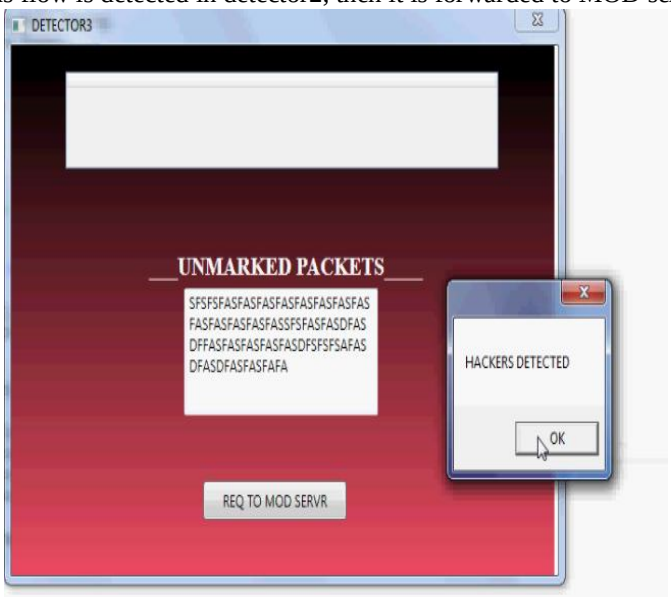

Fig.5. Hacker detected

After providing unique mark to the packet, it is forwarded to detector3. If the value of the threshold is increases, then we finalize it a packet from the hacker. Then the hacker is detected.

This is the unique mark set by the MOD server. The Above fig. shows the detectors packet marking technique, if the packet is mark the request will sent to the admin for further process if the pack is unmarke4d the MOD server will make unique mark to the particular request.

IV. CONCLUSION

In this paper, the author propose a marking scheme for traceback purpose and attack can be detected from the threshold value of experimental settings. In general, the proposed scheme fundamentally addresses the scalability problem of the existing DPM based traceback schemes. As a result, the router can traceback every attack source son the Internet, which is impossible for the previous traceback schemes.

In regards to future work, the First plan to extend the current work to improve the availability of the MOD server itself as it is a centralized system. Second, we expect to extend the proposed scheme to trace back to each every attack computer (but) by using multiple packets for marking coding. Thirdly, a thorough investigation on the MOD

system is desired, such as the false positive rate and false negative rate of the MOD scheme. Finally, a real system prototype is planned to examine the efficiency of the proposed scheme in practice in the near future.

REFERENCES

[1] S. Yu, W. Zhou, W. Jia, S. Guo, Y. Xiang, and F. Tang, "Discriminating DDoS attacks from flash crowds using flow correlation coefficient," IEEE Trans. Parallel Distrib. Syst., vol. 23, no. 6, pp. 794–805, Jun. 2012.

[2] Shui Yu, Wanlei Zhou, Song Guo, "A Feasible IP Traceback Framework through Dynamic Deterministic Packet Marking", IEEE Trans on computers, vol. 65, May 2016.

[3] Yadong Wang, Lianzhong Liu, Bo Sun,"A survey of defense mechanisms against application layer distributed denial of service attacks", IEEE international conference on 23rd sept. 2015.

[4]Yang Xiang, Wanlei Zhou, Minyi Guo," Flexible Deterministic Packet Marking: An IP Traceback System to Find the Real Source of Attacks",IEEE international conference 2008.

[5] S. Yu, W. Zhou, R. Doss, and W. Jia, "Traceback of DDoS attacks using entropy variations," IEEE Trans. Parallel Distrib. Syst., vol. 22, no. 3, pp. 412–425, Mar. 2011.

[6] Vicky Laurens and Abdulmotaleb El Saddik,"detecting distributed denial of service attack traffic at the agent machines", IEEE Trans. Parallel Distrib. Syst., vol.27, 2014

[7] S. Yu, W. Zhou, R. Doss, and W. Jia, "Traceback of DDoS attacks using entropy variations," IEEE Trans. Parallel Distrib. Syst., vol. 22, no. 3, pp. 412–425, Mar. 2011.

[8] Bao-Tung Wang; Schulzrinne, Henning, "An IP traceback mechanism for reflective DoS attacks," Electrical and Computer Engineering, 2004. Canadian Conference on, vol.2, no., pp.901, 904 Vol.2, 2-5 May 2004 doi: 10.1109/CCECE.2004.1345260

[9] https://www.slashgear.com/whats-a-ddos-attack-zombies-shopping-help-explain-it-all-11333110/

[10] https://www.incapsula.com/ddos/ddos-attacks/denial-of-service.html.