SOURCE IDENTIFICATION FOR ANONYMOUS ATTACKS WITH DETERMINISTIC PACKET MARKING

[1]Mrs. Nupur Rathod, [2]Mohit Patel, [3]Priya Patel
[1]Student, [2, 3]Assistance Prof, Department of Computer Engineering
Swaminarayan College of Engineering & Technology, Ahmedabad- Mehsana Highway, Gujarat - 382721

ABSTRACT

The Anonymous attack is one of the potential threats to the Internet, with the growth of the Internet and IOT, where all the object are going to connect with Internet, the scope of the anonymous attack will be tremendous. The denial of service attack is one of the anonymous attacks. Therefore it is need to identify the source/sources of the attacks and mitigate the attacks nearer to the sources. This paper discusses the deterministic packet marking for the spoofed packets along with identification of attacker.

Keywords *- DoS, DDoS,DPM ,IP Traceback*

I. INTRODUCTION

In this paper we are describe a tracing the attackers in a denial-of-service (DoS) attack is particularly difficult since attackers spoof or incorrect the source address. DoS attacks are among one of the hardest security problems to address because they are simple to implement, hard to prevent and difficult to trace. The network traffic of an attack should include information identifying the source. By targeting your computer and its connection, or the computers and network of the site you are trying to use, an attacker may be able to prevent you from accessing email, websites, online accounts, or other data or service that security on the affected computer. The most common and obvious type of DoS attack occurs when an attacker "floods" a network with information. The **DoS** attack typically uses one computer and one Internet connection to flood a targeted system or resource. The **DDoS**[1] attack uses multiple computers and Internet connections to flood the targeted resource.

The attacker tries to hide its identification by spoofing the IP address. We present a novel approach to IP Traceback [2], [3] . IP traceback is to locate the base of the IP packets and it is post mortem analysis, investigation into other kinds networks of attacker. It is complicated when IP address can be spoofed [4] or incorrect. Current IP traceback mechanisms can be mainly classified into many categories. These are Ingress Filtering , Logging, Link Testing, Packet Marking, ICMP Traceback, and Hybrid Tracing. These mechanisms mark the identification of the router in the IP packets. We are focusing on packet marking and the various marking mechanism like Probabilistic Packet Marking and Deterministic Packet Marking. In PPM, all routers mark the packet using some probability. The victim reconstructs the path back to the source using the bit encoding by each router. DPM mark the packet with fixed probability, it uses the identification of edge routers while marking the packets.

This paper describe as the tracing the incorrect or spoofed IP address by using deterministic packet marking.

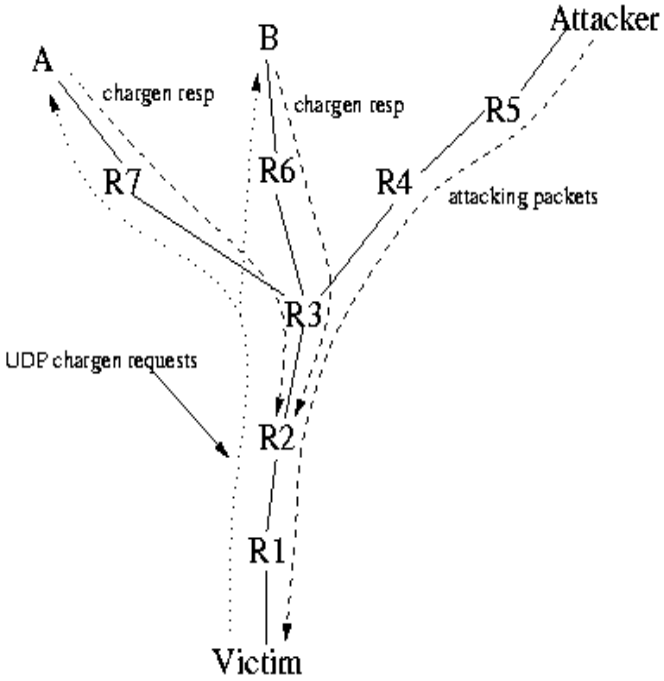

Fig 1 : Tracing Anonymous Packet [2]

In fig 1, we show the attack sources and victim. IP traceback problem involves identifying the actual source of a packet across the Internet. It is however, a tough and challenging problem due to the spoofing of source address of the packets by the attacker. The attackers, who in general enjoy their anonymity, can now be implecated by traceback for their malicious act. As the identity of an attacker could be exposed by traceback, the attacker would think twice before performing a DoS attack. Traceback also help[s in a better implementation of filtering rules as the counter-measures can be taken near the originating point of the attacks.

II. RELATED WORK AND EXISTING SCHEMES

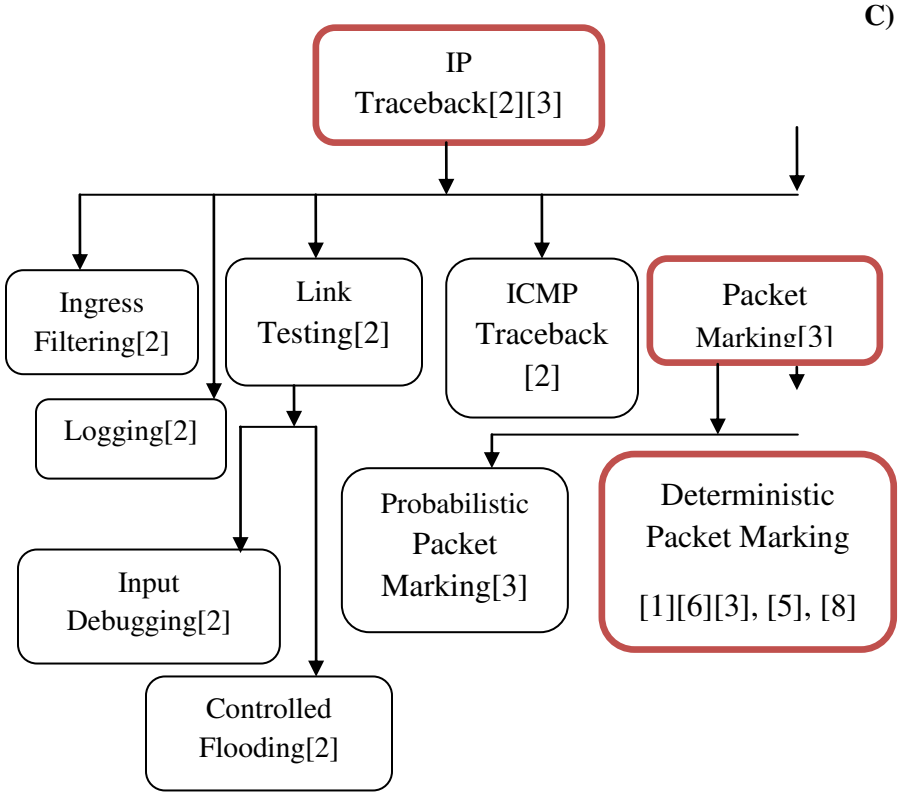

Fig 2: Classification of IP Traceback Schemes[1]–[3], [5], [6][7]–[9]

A) Ingress Filtering

Ingress filtering is a technique used to ensure that incoming packets are actually from the networks from which they claim to originate. This technique is often used in the denial-of-service attack, and this is a primary target of ingress filtering. Networks receive packets from other networks. Normally a packet will contain the IP address of the computer that originally sent it. This allows devices in the receiving network to know where it came from, allowing a reply to be routed back (amongst other things), except when IP addresses are used through a proxy or a spoofed IP address, which does not pinpoint a specific user within that pool of users.

B) Logging

This solution involves storing packet digests or signatures at intermediate routers. The drawbacks of this technique include significant amount of resources have to be reserved at intermediate routers and hence large overhead on the network, complexity, centralized management [10].

C) Link Testing

Most existing traceback techniques start from the router closest to the victim and interactively test its upstream links until they determine which one is used to carry the attacker's traffic. We describe two varieties of link testing schemes, input debugging and controlled flooding .

1) **Input Debugging:** Many routers include a feature called input debugging, which allows an operator to filter particular packets on some egress port and determine which ingress port they arrived on. This capability is used to implement a trace as follows.
2) **Controlled Flooding:** Link-testing traceback technique that does not require any support from network operators. We call this technique controlled flooding because it tests links by flooding them with large bursts of traffic and observing how this perturbs traffic from the attacker.

D) ICMP Message

Internet Control Message Protocol (ICMP) in would like of trace out full path of the attacks. Typically this scheme is for each router to come up with an ICMP traceback message or reach directed to the identical destination.

E) Packet Marking

Packet marking methods relies on the routers in the network to send their identities to the destinations either by encoding this information directly in rarely used bits of the IP Header, or by generating new packet to the same destination. There are two approaches of packet marking schemes.

1) Probabilistic Packet Marking: Probabilistic packet marking makes use of the Identification field as the marking space and stores the link information. It divides the IP address into eight fragments, 4 bits for each. This IP address fragment and the same offset fragment of the next router compose the edge fragment with 8 bits. The offset flag needs 3 bits for eight fragments, and the last 5 bits are enough to show the hop number. It is reported that few packets exceed 25 hops in the forwarding network. When a router decides to mark a packet, it chooses a random fragment of its IP address, and records the fragment offset with the distance field set to 0.
2) Deterministic Packet Marking: Deterministic Packet Marking scheme (DPM) is technique overcomes the disadvantages of PPM. Every packet passing through the first ingress edge router is only marked with the IP address of the router. The IP address is divided into two fragments (16 bits each) and each fragment is randomly recorded into each inflowing packet.

III. EXISTING PROBLEM WITH DPM

From the above literature survey, we identify the limitations of the existing approaches. They are as follows:

1. The Deterministic Packet Marking may produce high false-positives.
2. As the existing deterministic packet marking approach do not authenticate the marking at the victim, the compromised routers on the attack path could forge the marking of upstream routers. So it prevents the victim from detecting and determining the compromised router by analyzing the marking. Hence authentication marking need to be included here. The proposed approach use the hash function. The hash function cannot authenticate the marking.
   Improved deterministic packet marking algorithm may generate wrong traceback in case of compromised router.

IV. PROPOSED SOLUTION

Our goal in this research is to propose the IP traceback mechanism based on deterministic packet marking. The advantages of deterministic packet marking is that the edge router only marks the packet therefore it has less network overhead. Another important goal of our research is to authenticate the packet marking to prevent the forged marking and therefore the further false-positives. This would be based upon some authentication protocol that can satisfy above both security mechanisms. So, this work will enable the receiver to verify that the received data was actually originates from the authenticate node and not from any malicious node and was not changed within route.

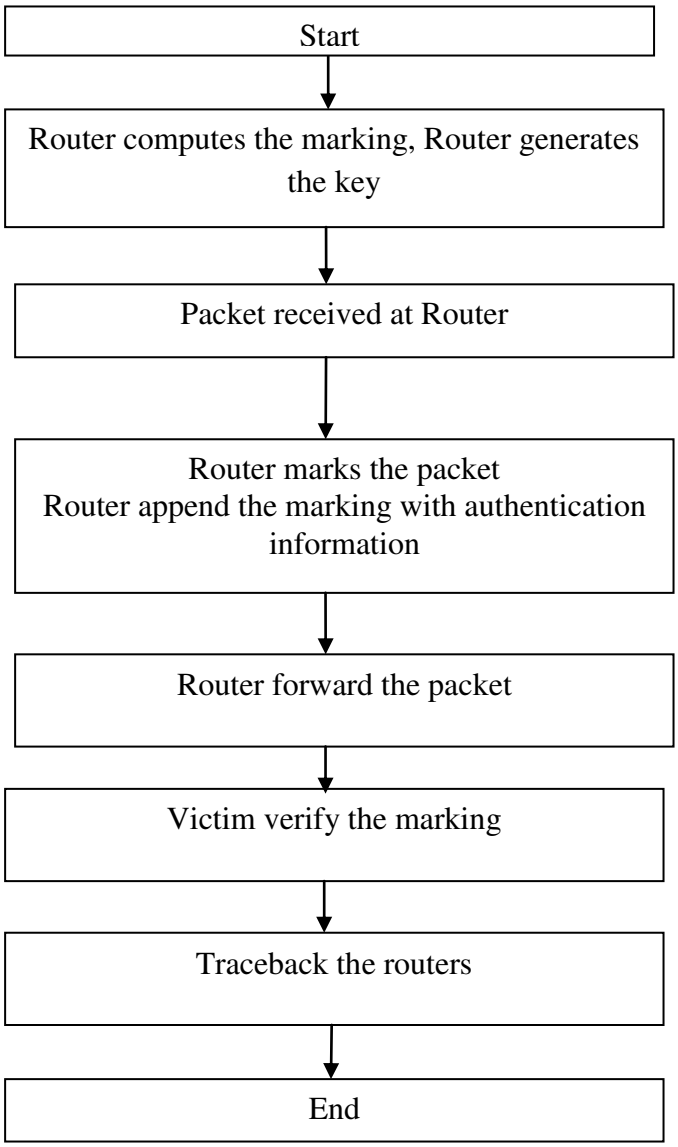

Fig 3: Flow chart of proposed algorithm

Proposed work is divided into two algorithms:

(1) Packet Marking
(2) Attacker router identification Algorithm

In the packet marking procedure, the edge router marks the packet with some information for authentication and the attacker router identification algorithm collect the marking and construct graph from this information.

(1) Packet Marking Algorithm

We are using 16 bits of fragmentation, 13 bits of fragmentation offset and 1 bit of reserved flag for the marking. The router needs to mark the 2 packets to send the address. The 13 bits fragmentation offset is used to mark the MAC of the IP address. The 1 bit reserved flag is used to indicate the IP address fragment index.

```
For each packet P
    Let r be a random number[0,1)
    if r<=0.50then
    mark 0 to P.flag
    write 0 to 15 of IP bit to P.Frag[0-15]
    write MAC(IP) to  P.fragOff[0-12]
    if r>0.50 then
   mark 1 to P.flag
   Write 16 to 31 bit to P.frag[0-15]
   Write MAC (IP) to P.FragOff[0-12]
```

(2) Attacker router identification Algorithm:

To identify the edge router, the victim combine the both half of the address and derive the IP address of the router. The index of IP address and MAC from the marking is used to merge the two halves of IP address correctly.

V. CONCLUSION AND FUTURE WORK

The attacks based on anonymous attacks are increasing tremendously. DoS attackers exploit flaws in protocols and systems to deny access of target Services. Today we need to design proper mechanisms to protect systems from such attacks, without the cooperation of ISPs (Internet Service Providers) it will be difficult to deploy any scheme.

IP traceback is today need as number of attacks based on IP Spoofing are increasingly. Many IP traceback has been prepared. However, they suffers from many limitations. Therefore in this work, we do research to propose IP traceback method that require less number of packets with reduced false-positives.

REFERENCES

[1] A. Belenky and N. Ansari, "Tracing multiple attackers with deterministic packet marking (DPM)," *2003 IEEE Pacific Rim Conf. Commun. Comput. Signal Process. (PACRIM 2003) (Cat. No.03CH37490)*, vol. 1, pp. 1000–1003, 2003.

[2] S. Savage, D. Wetherall, A. Karlin, and T. Anderson, "Network support for IP traceback," *IEEE/ACM Trans. Netw.*, vol. 9, no. 3, pp. 226–237, 2001.

[3] Piyush P., Jigneshkumar V Madhad, "Comparative Study of IP Trace back Techniques," *Reserch*, vol. 2, no. 2, pp. 42–47, 2016.

[4] M. Lavanya and P. K. Sahoo, "2016 IP spoofing and its Detection Technique," *Adv. Comput. Tech. Appl.*, vol. 4, no. 1, pp. 167–169, 2016.

[5] A. Parashar and R. Radhakrishnan, "Improved Deterministic Packet Marking Algorithm," *IEEE*, pp. 1–4, 2013.

[6] A. Parashar and R. Radhakrishnan, "Improved deterministic packet marking algorithm for IPv6 traceback," *2014 Int. Conf. Electron. Commun. Syst. ICECS 2014*, pp. 6–9, 2014.

[7] C. K. Singh, S. Koppu, and V. M. Viswanatham, "E-RIHT : Enhanced Hybrid IP Traceback Scheme with 16-bit marking field," vol. 5, no. 3, pp. 2594–2600, 2013.

[8] S. Yu, W. Zhou, S. Guo, and M. Guo, "A Feasible IP Traceback Framework through Dynamic Deterministic Packet Marking," *IEEE Trans. Comput.*, vol. 65, no. 5, pp. 1418–1427, 2016.

[9] V. Murugesan, M. Shalinie, and N. Neethimani, "A brief survey of IP traceback methodologies," *Acta Polytech. Hungarica*, vol. 11, no. 9, pp. 197–216, 2014.

[10] K. Singh, P. Singh, and K. Kumar, "A systematic review of IP traceback schemes for denial of service attacks," *Comput. Secur.*, vol. 56, pp. 111–139, 2015.

[11] M. H. Yang, "Storage-efficient 16-bit hybrid IP traceback with single packet," *Sci. World J.*, vol. 2014, 2014.