International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 02 Issue: 08 | Nov-2015 www.irjet.net p-ISSN: 2395-0072

Extended Hybrid IP Traceback Scheme: E-RIHT

Mrs. Kavita Sunchu [1], Dr. Deshmukh P.K [2] , Prof. Dhainje P.B [3]

[1]M.E. Student, Computer Science and Engineering, Shriram Institute of technology, Maharashtra, India
[2]Dr. and Project guide, Computer Science and Engineering, Shriram Institute of technology, Maharashtra, India
[3]Professor, Computer Science and Engineering, Shriram Institute of technology, Maharashtra, India

---

Abstract - ***Internet is the major source of communication and retrieval of information, so there is the need of network security. The data transferred is most of the times confidential and should reach the destination without any tampering. People attack in the network using spoofing by hiding their IP addresses and start attacking on the systems. Lot of research has been carried out in this domain, various trace back schemes are developed to trace the source the attacks. Packet logging technique is used to trace the system; IP tracking till now is done only using single packet in packet logging. In this research we propose a new hybrid IP trace back with enhanced packet logging method providing sufficient storage for each router reducing the rate of refreshing logged track and gain zero false positive and negative rates in recognizing the path of the attacker. Packet marking field is also used to censor attack on upstream routers. The combination of hybrid IP trace and packet marking makes the tracing system more strong leading to identify the attacks. Here we have considered some basic experiments and compared the work other techniques and found our technique gives promising results.***

Key Words: *DoS/DDoS attack, hybrid IP traceback, IP spoofing, packet logging, packet marking,RIHT ,MORE.*

1. INTRODUCTION

Due to internet as major source the use internet becomes more. With the increasing availability and use the impact of attacks becomes more significant. For disrupt the service of a server, the sophisticated attackers may launch a distributed denial of service (DDoS) attack. There are basically two types of attacks are found i.e. flooding based attack and software exploit attack.

The major identification of flooding-based attacks is a huge amount of forged source packets to exhaust a victim's limited resources. Second type of DoS attack is software exploit attacks; Software exploit attacks include IP spoofing attack. The source IP address in a packet can be found when an attacker wants to hide himself from tracing. So, IP spoofing makes hosts hard to preserve against a DDoS attack [1]. For tracing the original source of flooding-based attack packets, we introduced a traceback scheme that marks routers' interface numbers and integrates packet logging with a hash table (RIHT) to deal with these logging and marking issues in IP traceback.

IP Spoofing is a type of software exploit attack. In order to find the real source of these attacks, some uses packet logging technique. Some uses packet marking along with packet logging, which is also called as hybrid IP trace back. In packet
logging, packet's information such as its digest or signature will be stored in intermediate router. If we use packet logging alone, it requires large number of packets to trace back the real source of attacks. Ultimately large amount of space is required by each router. Even these traceback schemes cannot avoid false positive and false negative problems.

There are basically two main types of IP traceback techniques have been introduced: packet marking [1] and packet logging [1]. In packet marking, the router keeps identification information by marking forwarded IP packets. Due to the space limitation in packet header, routers probabilistically decide to mark packets so that each marked packet carries only partial path information. The network path can be reconstructed by combining a reserved number of packets containing mark information. This type of approach is known as probabilistic packet marking (PPM) [3]. The PPM approach incurs little overhead at routers. But it can only trace the traffic composed of a number of packets because of its probabilistic nature.

The actual source of flooding-based attack packets is traced by the scheme that marks routers' interface numbers and integrates packet logging with a hash table (RIHT. Packet marking can categories in two parts, deterministic packet marking (DPM) and probabilistic packet marking (PPM). Belenky and Ansari [3], [4]

introduced Border routers' IP address on the passing packets by using DPM traceback schemes. But still IP header's identification field is not sufficient to store the complete IP address. Due to this, the border router partitioned its IP into several parts and calculates the digest of its IP.

In this paper, we are concentrating on Hybrid IP traceback schemes, which include both packet marking and packet logging as mentioned. In packet marking, the packet is marked with router's information such as degree, interface number and so on. It causes a little overhead on packet.

The entire work of this paper is divided into five different modules:

- Network topology Construction
- Path Selection
- Packet Sending
- Packet Marking and Logging
- Path Reconstruction

2. TRACEBACK METHODS CLASSIFICATION

We can classify IP traceback methods into two types:

2.1 Proactive traceback :

In proactive IP traceback methods, alternative actions will be taken. In proactive methods, mainly concentrate on attack detection and access control are. Technologies used for preventive actions are firewalls and intrusion detection system.

2.1.1 Firewalls

Firewalls are mostly used to protect the networks from attacks. In specific, those responses coming from web. Firewall access management is based on protocol type, source port number, destination port number, source IP address and destination IP address.

2.1.2 Intrusion Detection System

Intrusion Detection System admonishers network activities and system activities for security breaches like intrusion and misuse.

2.2 Reactive traceback :

In reactive traceback methods, the source of attack will be identified by applying various traceback techniques. In reactive traceback methods Packet marking, packet logging and Hybrid IP traceback approach are the possible solutions.

2.2.1 Packet Marking

In this scheme, each packet is marked with a value based on router's identification number or degree. Marking is nothing but inserting a value in the packet. This approach requires lot of packets to find the source of attack.

Advantages:

- Low cost
- Compatible with existing routers and infrastructure
- Very effective for DoS attacks
- No need of ISP co-operation

Disadvantages:

- We need to modify the protocol structure.
- Sometimes result can be false positive.
- IP traceback is possible only when victim receives minimum number of packets
- Not compatible with IPv6

2.2.2 Packet Logging

In this scheme, packet digest or signatures will be logged (stored) at key routers. Problem with this technique is, sample amount of storage is requires at key routers, which is overhead on the network.

Advantages:

- Packet logging is compatible with all existing protocols.
- Existing routers and infrastructure.

Disadvantages:

- Due to legal issues, we cannot share logging information among the ISPs.

2.2.2 Hybrid Ip Traceback (HIT)

In this scheme, we use both packet marking and packet logging. It has pros of both the schemes. By applying this scheme, we can find source of attack even by using single packet.

3. RELATED WORK

Cheswick and Burch [1] proposed link test scheme, which generates extra load on upstream links. This extra load will disturb the attack traffic by competing with it. So we can easily identify the attack traffic.

B. Al-Duwairi and M. Govindarasu [2] proposed hybrid IP traceback scheme, which is named as DLLT (Distributed Link List Technique). In DLLT, subnet of routers is involved for forwarding the packets through a

temporary link between routers DLL. packets are marked and logged based on probability. Advantage of DLLT is, we can get the attack path by using less number of packets. DLLT uses 34 bits for packet encoding which includes 32 bit IP address. Packet marking can be classified in to two types, Deterministic Packet Marking (DPM) and Probabilistic Packet Marking (PPM).

Belenky and Ansari [3, 4] introduced Deterministic Packet Marking traceback schemes; passing packets are marked with border router's IP address. Border router divides its IP address into chunks and calculates the digest of its IP. Then a random chunk and digest are marked in IP identification field. Destination uses this digest to assemble the different chunks.

C. Gong and K. Sarac [5] proposed HIT (Hybrid IP Trace back). In HIT, deterministic packet marking and packet logging are done at each and every router.

B. Al-Duwairi and M. Govindarasu [6] proposed PPPM (Probabilistic Pipelined Packet Marking), in which packets with similar destination IP address are grouped together. In this technique, path fragments are stored in packet marking field. Since it uses packet logging scheme, storage overhead is distributed on routers also. Ming-Hour Yang and Ming-Chien Yang [7] proposed RIHT (Routers Interface Hybrid Traceback) scheme. In this technique, packets are marked with router's upstream interface numbers to track the path. Packet logging is done at each and every router in a hash table data structure.

Snoeren *et al* [8] propose a system SPIE to digest the unchanged parts of a packet and used bloom filter to log the digest. However, this scheme requires large amount of storage space and has a false positive problem in the bloom filter.

For this reason, Zhang and Guan [9] propose TOPO to improve the efficiency and precision of SPIE, but TOPO still needs large storage capacity and absolutely it has a false positive problem because of the bloom filter. The hybrid IP traceback schemes are proposed to reduce the storage problem of logging-based traceback schemes.

Gong and Sarac [9] proposed a hybrid IP traceback scheme which is also called Hybrid IP Traceback (HIT) combining packet marking and packet logging. HIT uses packet marking to reduce the number of routers required for logging. Further researchers are proposed new schemes which reduces the storage requirement for router logging and to mitigate the number of routers required for logging, Modulo/Reverse modulo Technique (MRT) [15] and MOdulo/REverse modulo (MORE) [16]. Since these schemes use interface numbers of routers for marking, they assume a router set R = {R1, R2,….,Ri,….Rl} comprising l routers in a network and require all the routers support the respective traceback schemes. And, they use the degree of a router as a parameter in their marking schemes where the degree is the number of interfaces of the router, not including ports connected to local networks. Here we use D(Ri) to denote the degree of a router Ri. Besides, these schemes need to maintain an interface table on each router in advance. This table maps a unique number to each interface of a router along which the router is connected to another router. The interface numbers of a router Ri are between 0 and D(Ri)-1 . For discussion, we denote by UIr i (or UIi if there is no ambiguity) the upstream interface number of a Ri router in a route r. In what follows, we use routes and paths interchangeably. In the marking process, each router puts UIi into the marking field. Perhaps the simplest way to encode UIi is by fixed-length coding [8]. However, such an approach does not use a packet's marking field efficiently D(Ri) if is not a power of two.

Choi and Dai [9] propose a marking scheme using Huffman coding to reduce the bits required for marking on a packet. It encodes UIi by Huffman coding according to the traffic of each interface. Their analysis shows their scheme has superior performance when the traffic distribution for each interface is unequal.

Malliga and Tamilarasi proposed two traceback schemes, namely MRT [10] and MORE [11]. While MORE uses a 16-bit marking field and separates a log table into D(Ri) parts. MRT uses a 32-bit marking field; both of these uses mathematical methods for marking fields. In their marking schemes, the new marking field =marking field * D(Ri)+ UIi is calculated by the routers to which a packet is forwarded. In their path reconstruction, the old marking field= marking field/ D(Ri) is calculated by the routers to which a packet is traced back; the upstream interface number UIi =marking field% D(Ri)is also computed where % is the modulo operation, also the packet is sent back to the upstream router along the obtained upstream interface. According to the final test results in MRT and MORE, the average bits used for marking are lesser than those in Huffman coding.

4. RIHT

As we know MRT and MORE, RIHT marks interface numbers of routers on packets so as to trace the path of packets. While the marking field on each packet is restricted, our packet marking scheme can need to log the marking field into a hash table and store the table index on the packet. We replace this marking/logging process until the packet reaches its destination. After that, we can reverse such scheme to trace back to the origin of attack packets.

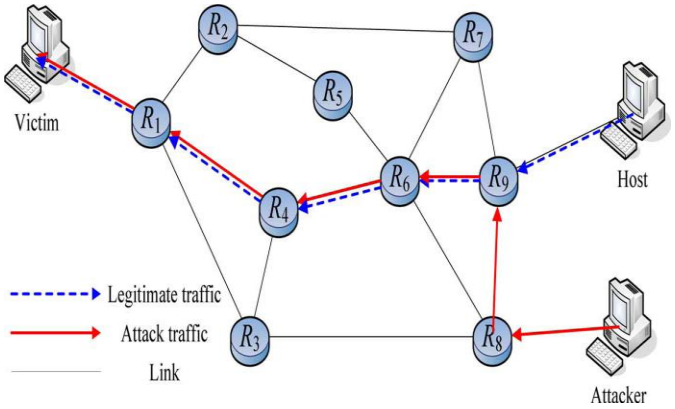

Fig-1: Network topology

Introduction to Network Topology

As shown in Fig-1 the network topology, in which a router is connected to a local network or other routers, or routers are connected to local network as well as router itself. A frame router receives packets from its local network. A core router receives packets from remaining routers.
The assumptions of our methods are as follows.
1) A router knows whether a packet comes from a router or a local network.
2) A router creates an interface table and numbers the upstream interfaces from 0 to D(Ri)-1 in advance.
3) The traffic route and network topology can be changed, but not often.
4) Such a traceback method is feasible on every router.

Bit offset	0-3	4-7	8-15	16-18	19-31
0	Version	Header length	TOS	Total length	
32	Identification field			Flag	Fragment offset
64	TTL		Protocol	Header checksum	
96	Source address				
128	Destination address				
160	Options				
160 or 196+	Payload (first 8bytes)				

Fig-2: Fields of an IP packet. We use the gray fields as marking field in RIHT.

4. PROPOSED SYSTEM

In this paper, proposed IP traceback scheme is named as Extended-RIHT which is similar to RIHT [8] with slight modifications. Extended-RIHT uses both packet marking and packet logging. In Extended-RIHT, packet marking and logging are done at border routers and core routers. In RIHT, 32-bits are used for packet marking field while Extended- RIHT uses 16-bits in IP packet.

UIi	Upstream Interface Number
P	Packet Received
H()	Hash Function
H'()	Secondary Hash Function
M	Hash Table Size
c1, c2	Constants
HT	hash table with M entries
HT[index]	p-mark value at Hash table Index specified
%	The modulo division operation
UIi	Upstream Interface Number

Fig-3: Notation Table

RIHT which uses quadratic probing to resolve collisions is known as hash based IP traceback scheme, in that occur during the calculation of index positions. Issue due to quadratic probing is secondary clustering, and the position calculated does not depend on key value, instead it is constant. In order to get rid of secondary clustering issue, we are using double hashing technique for collision resolution. The index position depends on key value in double hashing (In this we are using P.mark value, hence index value depends on P.mark value)

Algorithm for Packet Marking And Logging

Begin

1. Input: P.mark, UIi

2. Begin

3. marknew = P.mark × (D(Ri) + 1) + UIi +1

4. if marknew > 2Size of address then

a. index = h = H(P.mark)

b. i = 0

c. while not (HT[index] is empty or HT[index] is equal to (P.mark, UIi))

i. i++

ii. h'=H'(P.mark)

iii. index = (h + i × h') % m

d. end while

e. if HT[index] is empty then

i. HT [index]. Mark = P.mark

ii. HT[index].UI = UIi

f. end if

g. marknew = index × (D(Ri) + 1)

5. end if

6. P.mark = marknew

7. Forward the packet to the next router

End

In the above algorithm, P.mark value at each and every hop is calculated using Upstream Interface number and degree of that particular router. If P.mark value exceeds the limit, i.e., 2 power (size of address bits), then it will be stored in hash table. The index of hash table is calculated by applying hash function. If any collisions occur, double hashing technique is used to find the index position. After storing the value, based on the index of hash table, new mark value is calculated. New p. mark value is inserted in the packet and is sent to the next hop.

Algorithm for Path Reconstruction

In the below algorithm, first we need to calculate Upstream Interface number by applying the formula *UIi = markreq %(D (Ri) + 1) – 1 where* markreq is the p-mark value of the incoming packet. If UI= -1, we need to UI number from hash table, where the index of it is: *markreq / (D (Ri) + 1)* .Usually, this algorithm is invoked when the victim sends path reconstruction request. By applying this algorithm, we can find the real source of attack, or Attacker's nearest router.

Algorithm for Path Reconstruction

Begin

1. UIi = markreq %(D(Ri) + 1) – 1

2. if UIi = -1 then

a. index = markreq / (D(Ri)+ 1)

b. If not index = 0 then

i. UIi = HT[index].UI

ii. markold = HT[index].mark

iii. Send reconstruction request with markold to upstream router by UIi

c. else

d. This router is the nearest border router to the attacker

e. endif

3. else

a. markold = markreq / (D(Ri)+ 1)

b. Send path reconstruction request with markold to upstream router by UIi

4. endif

In the above algorithm, first we need to calculate Upstream Interface number by applying the formula *UIi = markreq %(D (Ri) + 1) – 1 where* markreq is the p-mark value of the incoming packet. If UI= -1, we need to UI number from hash table, where the index of it is: *markreq / (D (Ri) + 1)* .Usually, this algorithm is invoked when the victim sends path reconstruction request. By applying this algorithm, we can find the real source of attack, or attacker's nearest router.

5. COMPARISION OF VARIOUS HYBRID IP TRACEBACK SCHEMES

Extended-RIHT is better than RIHT, since it uses dynamic hashing instead of quadratic probing. Hence there won't be a problem of secondary clustering during collisions of hash table.

6. CONCLUSION

In this paper, we propose a new hybrid IP traceback scheme Extended RIHT (E-RIHT) for efficient packet logging which aiming to have a fixed storage in packet logging without the need to refresh the logging trackback information. And, the proposed scheme has achieves zero false positive and false negative rates in an attack-path reconstruction. Apart from these properties, our scheme can also introduce a marking field as a packet identification to filter malicious traffic and secure against DoS/DDoS attacks. Accordingly, with high accuracy, a low storage condition, and fast computation, E-RIHT can provide as a secure and efficient scheme for hybrid IP traceback.

7. RESULTS

In this we overcome fragmentation problem by using new version of E-RIHT which uses a 16-bit marking field to avoid the packet fragmentation. By following this scheme, we can achieve zero false positive and false negative feedback. Since we are using 16 bit marking field, Due to this storage overhead, marking overhead are reduced, to make calculations simple.

IP Traceback schemes	DLLT	PPPM	HIT	RIHT	Extended-RIHT
Required NO. of packets for traceback	Minimum number	Minimum number	One	One	One
Marking overhead	High	High	Low	Low	Low
Storage Overhead at router	High	High	Low	Low	Low
Traceback overhead	Medium	Medium	Medium	Low	Low
Size of Marking Field	34-bits	57-bits	32-bits	32-bits	16-bits

REFERENCES

[1] Burch H, Cheswick B. Tracing anonymous packets to their approximate source. Proc. USENIX LISA, New Orleans, LA, Dec. 2000; 319–327.

[2] Al-Duwari B, Govindarasu M. Novel hybrid schemes employing packet marking and logging for IP traceback. IEEE Trans. Parallel Distributed Syst. 2006; 17(5): 403–418.

[3] Belenky A, Ansari N. IP traceback with deterministic packet marking. IEEE Commun. Lett. 2003; 7(4): 162–164.

[4] Belenky A, Ansari N. Tracing multiple attackers with deterministic packet marking (DPM). Proc.IEEE PACRIM'03, Victoria, BC, Canada, Aug. 2003; 49–52.

[5] Gong C, Sarac K. A more practical approach for single-packet IP traceback using packet logging and Marking. IEEE Trans. Parallel Distributed Syst. 2008; 19(10): 1310–1324.

[6] Al-Duwariand B, Govindarasu M. Novel hybrid schemes employing packet marking and logging for IP traceback. IEEE Trans. Parallel Distributed Syst. 2006; 17(5): 403-418.

[7] Yang M-H, Yang M-C. RIHT: A Novel Hybrid IP Traceback Scheme. IEEE Transactions On Information Forensics And Security 2012; 7(2).

[8] A. C. Snoeren, C. Partridge, L. A. Sanchez, C. E. Jones, F. Tchakountio, B. Schwartz, S. T. Kent, and W. T. Strayer, "Single-packet IP traceback," IEEE/ACM Trans. Networking, vol. 10, no. 6, pp. 721– 734, Dec. 2002.

[9] C. Gong and K. Sarac, "Toward a practical packet marking approach for IP traceback," Int. J. Network Security, vol. 8, no. 3, pp. 271–281, Mar. 2009.

[9] K. H. Choi and H. K. Dai, "A marking scheme using Huffman codes for IP traceback," in Proc. 7th Int. Symp. Parallel Architectures, Algorithms Networks (SPAN'04), Hong Kong, China, May 2004, pp. 421–428.

[10] S. Malliga and A. Tamilarasi, "A proposal for new marking scheme with its performance evaluation for IP traceback,"WSEAS Trans. Computer Res., vol. 3, no. 4, pp. 259–272, Apr. 2008.

[11] S. Malliga and A. Tamilarasi, "A hybrid scheme using packet marking and logging for IP traceback," Int. J. Internet Protocol Technol., vol. 5, no. 1/2, pp. 81–91, Apr. 2010.

[12] W. John and S. Tafvelin, "Analysis of internet backbone traffic and header anomalies observed," in Proc. IMC '07: 7th ACM SIGCOMM Conf. Internet Measurement, San Diego, CA, Oct. 2007, pp. 111–116.

[13] W. John and T. Olovsson, "Detection of malicious traffic on backbone links via packet header analysis," Campus-Wide Inform. Syst., vol. 25, no. 5, pp. 342–358, 2008.

[14] F. Gont, "Security assessment of the internet protocol version 4," Internet Draft: Draft-Ietf-Opsec-Ip-Security-07.Txt, Apr. 2011

[15] I. Stocia and H. Zhang, "Providing guaranteed services without peer flow management," in Proc. ACM SIGCOMM'99, Boston, MA, Sep. 1999, pp. 81–94