ISSN:0975-9646

A Survey on Packet Marking and Logging

Ruby Jain, Prof. Akanksha Meshram
Radharaman Institute of Technology & Science, Bhopal

***ABSTRACT*: A hybrid model of packet marking and logging for the IP trace back for the node that wants to attack any node in the network. The main idea is to detect the DOS attacks in the network by employing the IP of the attacker node. Packet logging scheme used to record packet state information in a router log, for reconstruct the attack path and get the attack source. Pre shared key exchange applied between the router and the sender for authentication. This paper provides a brief survey of different packet marking technique for the filtering of any unwanted anomalies in the network. Here in this paper a survey of different packet marking and logging is given and also IP trackback of the packets is presented.**

***Keywords*— Packet logging, Authentication, packet marking, internet trace back**.

1. INTRODUCTION

Attacks that use supply address spoofing represent a growing threat to the net infrastructure. Denial of Service (DoS) attacks and additional difficult version called Distributed Denial of Service (DDoS) is that the commonest to require advantage of supply address spoofing. These attacks deny regular web services from being accessed by legitimate users either by blocking service utterly or by distressing it specified users become not curious about the service any longer (for example inflicting important delay in accessing associate airline reservation net site). In such attacks, the most objective is to overpower the victim whereas concealing attacker's identity. Today's web has witnessed many incidents that make sure the devastating impact of such attacks [1].

In order to defend web against DoS intrusion, an efficient method is to find the supply and eliminate the attack going down. Sadly, attributable to the anonymous access and non-state characteristics of web, there's no record regarding the transmission path of packets. Therefore, we tend to cannot get the packet supply simple from the supply address of the packet dependably.

In current cyber intrusion, Denial of Service and a few later forms become one in all the foremost threatening varieties. It was absolutely reported that DDoS traffic within the web increase variety of times in eight years from many Mega-bytes in year 2002 to a hundred of Giga-bytes in year 2010. According to Worldwide Infrastructure Security Report 2010 from Arbor Networks, many celebrated web firms, together with Yahoo, Amazon and CNN were brought down for hours [2].

The main idea behind packet logging is that routers record the state information of their forwarding packets locally. When the victim node experience with intrusion, it can refer the log-tables recorded via query in the routers and makes matching with the attack packet. In the recursive process, it can achieve the complete path in the end. The most representative method is SPIE (Source Path Isolation Engine). The two types have their own features: PPM incurs little overhead when routers mark packets in a low marking rate, although the victim desires a huge amount of packets to reconstruct the path to the source. It is more suitable for flooding DoS trace back, and does not have the capability to trace a single packet. Although SPIE (Source Path Isolation Engine) extorts the grasps of packets and stores them in a space-efficient data structures known as bloom filter, which decreases the storage overhead and makes the packet logging scheme realistic. It can track small packets flows, yet a single packet. Nevertheless, it is yet a challenging task for its practicality due to its remaining high storage overhead. Hence, it is striking to recommend an effective IP trace back mechanism with the combination of the two trace back techniques, which is called a hybrid IP Trace back scheme [3].

A. Hybrid Internet Trace back

At present, Hybrid Internet Trace back (HIT) offered by Gong Chao [3] is the most representative way. HIT make use of the main idea of packet logging, and traces packet digests in each other router. The marking of routers do not record digests, but can be used to write their ID information into IP header. It is proficient to decrease the huge storage overhead of SPIE. Conversely, there are various drawbacks of HIT. Initially, it may return inaccurate path even the false source; then it still has a great demand for storage, which would limits its practicality [4].

B. Packet Logging Scheme

Introduced an idea to record packet state information in a router log, so as to reconstruct the attack path and get the attack source. This method can trace not only the flooding attack with a huge amount of packets, but also the single packet attack. It was thought to be impractical for its huge storage requirement. In order to reduce the storage overhead of log-based technology, log information requires a space-efficient manner. SPIE is proposed with the packet logging idea, so it has the capability to track a single packet. In SPIE, routers do not store the whole packet, but the digest with bloom filter, which is famous for its space-efficiency. In this way, the condition of storage requirement has been greatly improved (down to 0.5% of the total link capacity per unit time) [5].

C. Packet Marking Scheme

Unlike packet logging scheme, in packet marking scheme, routers do not record packets digests, but note their ID information into IP header. When the victim gets sufficient packets, it can reconstruct the full attack path. Savage et al. [6] proposed the classic probabilistic packet

marking (PPM) method. PPM makes use of the Identification field as the marking space and stores the link information. It divides the IP address into eight fragments block of 4 bits 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 block, and the last 5 bits are sufficient 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 selects a arbitrary fragment of its IP address, and records the fragment offset with the distance field set to 0. The benefit of PPM is that it desires no storage overhead for each router. But the weaknesses are also noticeable. The victim requires a large number of packets to reconstruct the attack path, and PPM does not have the ability to trace a single packet [6].

D. Probabilistic Packet Marking Schemes

Probabilistic Packet Marking (PPM) is one stream of the packet marking methods. The assumption of PPM is that packets are much more frequent than the standard packets. It identifies the packets with path information in a probabilistic manner and enables the victim to reconstruct the attack path by using the marked packets. PPM codifies the information in infrequently used 16-bit Fragment ID field in the IP header. To decrease the data stored in 16 bits the algorithm of compressed edge fragment sampling is used. Although PPM is simple and can support incremental exploitation, it has numerous shortcomings that can critically prevent it from being widely used.

E. Deterministic Packet Marking Schemes

Another stream of packet marking methods, which does not make use of the existing probabilistic assumption and stores the source address in the marking field, in the category called the deterministic approaches, such as Deterministic Packet Marking (DPM).The DPM scheme was modified to reduce false positive rates by adding redundant information into the marking fields. Dissimilar PPM, deterministic approaches only keep the first ingress edge router's information in the marks. Additionally, they track marks in a deterministic manner (but not a probabilistic manner as in PPM).

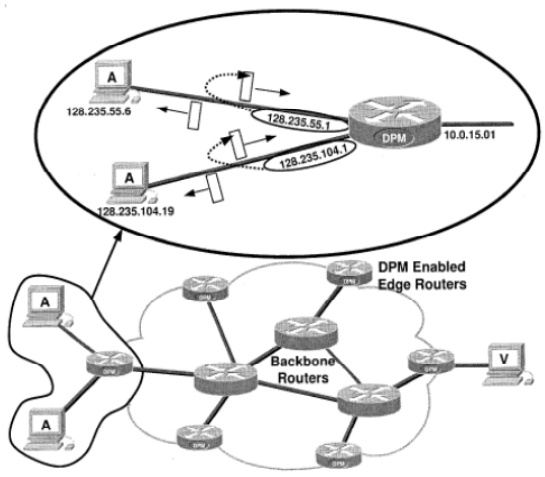

Figure 1: Deterministic packet marking (DPM).

2. Background And Motivation

Firstly focus on the attack track back problem before discussing backgrounds. Let Ri1, Ri2,….,Rin be the ordered list of routers between attacker (Ai) and victim (V) shown in figure 1. This ordered list of routers defines the attack path for Ai. This call each of these routers involved in forwarding malformed packets to the victim of attack, as an Attack Router. For any such attack router Rij in the list, all routers between Rij and the victim are called the Predecessor List of Rij, while all routers between the attacker and Rij are called Successor List of Rij. The main objective of attack trace back problem is to identify the attack router connected directly to Ai (i.e., router Ri1 which has an empty successor list). In this view, it is correspondent to identifying the end point of a link list starting at the victim, where every element in the list represents an intermediate router along the path from victim to attacker as Multiple attackers' case corresponds to a tree of link lists rooted at the victim (V), where each leaf represents a link list end point.

The main suppositions completed in this are similar to those made in and with an exception that we do not necessarily assume that each attack source has to send numerous packets [7].

The forthcoming threats imposed by Denial of Service attacks call for efficient and fast trace back schemes that enjoy the following features [1]:

1. Providing accurate information about routers near the attack source rather than those near the victim.
2. Recognition and exclusion of false information injected by the attacker.
3. Avoiding the use of large amount of attack packets to construct the attack path or attack tree.
4. Low processing and storage overhead at intermediate routers.
5. Efficient collection of marking information stored at intermediate routers (if any).

3. Related Work

B. Al-Duwairi,, and G. Manimaran gives the concept about Tracing DoS attacks that make use of source address spoofing is an important and challenging problem and there are different scheme used ,The first scheme, called Distributed Link-List Trackback (DLLT), and for propagating marking The second method known as Probabilistic Pipelined Packet Marking (PPPM) that uses the concept of a "pipeline" for propagating marking information and at the destination end small amount of resources to be allocated at intermediate routers for packet logging purposes [1].

In 2012 by Dong Yan et al [4] proposed their work in the field of Packet Marking and Logging. Tracing malicious packets back to their source is important to defend the Internet. There are two major kinds of IP trace back techniques, which have been proposed as packet marking and packet logging. In packet marking, it incurs little transparency. In packet logging, its needed storage space to record packet digests information and his capability to trace even a single packet. Consequently, it is a new idea to draw on both advantages to obtain the

intrusion source and propose a precise IP trace back approach with low storage overhead that is used to improve accuracy and realism greatly. [4].

In the field of Packet Marking R. Sravani, and J. Swami Naik in 2011 present a practical IP trackback system called Flexible Deterministic Packet Marking (FDPM) which provides a defense system with the ability to find out the real sources of attacking packets and finally In case of FDPM, the marks in packets do not increase their size; therefore, no additional bandwidth is consumed and overload prevention capability, FDPM can maintain the trackback process when the router is heavily loaded, whereas most current trackback schemes do not have this overload prevention capability [9].

In 2012 by Shih-Hao Peng et al [10] introduced A Probabilistic Packet Marking scheme and propose the LT Code IP Trace back scheme to reconstruct the attack graph and find the source of attacker and finally LTCIP is a reliable IP Trace back method that can discover the source of DDoS attack and avoid the attack [10].

Introduce an efficient Ip traceback in packet marking algo. In 2010 by Y.Bhavani and P.Niranjan Reddy propose a technique that efficiently encodes the packets than the Savage probabilistic packet marking algorithm and reconstruction of the attack graph and to conclude, our Efficient Probabilistic Packet Marking is an effective means of improving the reliability of original probabilistic packet marking [11].

Jeevaa Katiravan, C. Chellappan, and N. Duraipandian, in 2011 introduce the It Security concept there are different types of cyber crime is major threat such as surrounding hacking, copyright infringement etc and also problems of privacy when confidential information is lost or intercepted. So here over comes this problem by using a pre shared key method. This solution proves that even if attacker node changes its IP address but it can't change the pre shared key exchanged between it and egress router which is used for authentication [12].

Andrey Belenky and Nirwan Ansari proposed a new technique of packet marking and logging. The technique uses the concept of deterministic packet marking scheme where the probability of each of the packet is detected on the basis of which the packet needs trace back or not is decided [13]. Although there are any packet marking techniques are used, so here in this paper the previous packet marking technique based on probabilistic packet marking limitations has been removed and the solution is implemented in this paper.

According to Chao Gong and Kamil Sarac, a new packet marking technique has been implemented based on IP trace back [14]. The technique implemented here not only increases the efficiency of the IP trace back but also the accuracy. It implements a new technique of storing whole information of router into a single header of the packet so as to reduce the computation overhead.

Michael T. Goodrich proposed a new technique of packet marking based on probabilistic packet marking for large-scale trace back of packets [15]. Here in this technique randomize and link using the check sum of chords and message is fragment which is used to find the probability of the packets.

WANG Xiao-jing and WANG Xiao-yin has proposed a new technique of packet marking and IP Traceback using deterministic based packet marking . Here in this paper the technique is used for the prevention of Denial of Service and Distributed Denial of service attacks. The technique used here in this paper is based fragmentation of the packet and then deterministic probability of each packet is determined such that the attacks possible can be reduced [16].

A new approach of IP traceback using algebraic approach is proposed in [17]. Here in this paper a proposed solution of IP traceback is given based on the algebraic solution of the packets that are transferred through the network. Here the concept of algebraic coding theory is applied on the packet and hence a probability of the packet is determined based on which the IP traceback of the packets is possible.

Kihong Park and Heejo Lee proposed a new technique of probabilistic based packet logging and packet marking for the Denial of service attacks [18]. Here in this paper the attack possible in the network is analyzed and finds the spoofed packet in the network so that the chances of DOS attack has been reduced. Here each and every packet has been spoofed and then the probability of each packet is detected so that the packets cannot get traceback but the chances of attack possible can be minimized.

Tatsuya Baba and Shigeyuki Matsuda have survey the source of the packet from where it gets traced back [19]. Here in this paper the network can be traced and find the different sources of attacks possible in the network is detected. Here the concept of packet tracer is used for the detection of packet source attacks.

Bilal Rizvi and Emmanuel Fernández-Gaucherand also focus on the detection of the denial of service attacks possible in the network [20]. Here in this paper the effectiveness of the packet marking the traceback of the packet is proposed and using the concept of packet logging using probability of the packets the attack can be detected. Here in the proposed technique they take the perspective of the attacker and analyze the effects of inserting fake edges against AAPM.

Alex C. Snoeren has proposed a new and efficient way of IP traceback using the concept of hash values [21]. Here in the proposed technique a new of identifying the traceback since it is very difficult to identify which packet needs to be marked or not, hence a new technique of finding the hash value of every packet is marked and the detection takes place.

4. PROBLEM IDENTIFICATION OF EXISTING WORK

Although there are many efficient techniques used to identify the DOS attacks in the network. Hybrid trace back for the packet marking and the packet logging is one of the efficient techniques to trace back the IP address. But this technique is not used in the distributed or if the architecture of the network gets changed. The technique can't retrieve sufficient information from the packets.

5. PROPOSED WORK

1. First of all create a homogenous or heterogeneous network.

2. Apply pre shared key exchange between the router and the sender using:
   Assumption:
   Sender node has already registered with the router and got the pre-shared key.
   Process:
   1. Sender node sends a request to egress for sending data packets to destination node using the function sendPacket (req).
   2. Egress Router now will send challenge response acknowledgement to sender node chaAck ().
   3. Now Sender node will send the new packet encrypted with pre-shared key to the ingress router. This packet need to be a tcp/syn packet making sure that further authentication of packets is not required in that session for the same node. sendPacketv (TCP/SYN(msg)).
   4. Now egress router will use the compare (Hcs,Hcr). Where Hcs is the sender msg and Hcr is the msg created by ingress router.
   5 .If comparisons are true then call the function forward (msg) to forward the packets
   else
   reject (req) , reject the request

3. Then apply the following algorithm for the packet marking as shown:
   IR (Marking Info. Of _Attack Packets)
   Pass I
   1) *for* each subset of routers that marked certain packet (P).
   a) *if* (P end-list router is not in the table)
      i) add new entry for P end-list router
      ii) add P remaining routers to the predecessor list of P end-list router
   b) *else* add P remaining routers to the predecessor list of P end-list router
   Pass II
   1) *for* each end-list router E Rx in the table
   a) *if* (E Rx appears in the predecessor list of any other end-list router E Ry)
   i) append predecessor list of E Rx _ to the predecessor list of ERy.
   Ii) remove ERx and its predecessor list from the table.

6. CONCLUSION

Here in this paper a survey of the different techniques implemented for the packet marking and logging of the packets has been overviewed and also the IP trace back of the packets is shown. We also give brief idea about pre shared key exchange that is mainly used for authentication between sender and router. On behave of review we can formulize our work.

REFERENCES

[1] B. Al-Duwairi,, and G. Manimaran, **"**Novel Hybrid Schemes Employing Packet Marking and Logging for IP Traceback Bashee", IEEE Transactions on Parallel and Distributed Systems, Volume 17, Issue 5, pp. 403-418, May 2006.

[2]. Arbor Networks Inc., "2010 worldwide infrastructure security report," [EB/OL], http: //www.arbornetworks.com/report.

[3]. C. Gong and K. Sarac, "A more practical approach for single-packet IP traceback using packet logging and marking," IEEE Transactions on Parallel and Distributed Systems, Vol. 19 , pp. 1310-1324, 2008.

[4] Dong yan, Yulong Wang, Sen Su and Fangchun Yang. "A Precise and Practical IP Traceback Technique based on packet marking and logging", published journal of information science and engineering 28, 453-470, 2012.

[5]. A. Snoeren, et al., "Single-packet IP traceback," IEEE/ACM Transactions on Networking, Vol. 10, pp. 721-734, 2002.

[6] S. Savage, D. Wetherall, A. Karlin, and T. Anderson, "Network support for IP traceback," IEEE/ACM Transactions on Networking, Vol. 9, pp. 226-237. 2001.

[7]. D. Song and A. Perrig, "Advanced and authenticated marking schemes for IP trace back", in Proceedings of IEEE Twentieth Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOMM – 2001), pp. 878 – 886, April 2001.

[8]. Dong Yan, Yulong Wang, Sen Su And Fangchun Yang "A Precise and Practical IP Traceback Technique Based on Packet Marking and Logging", Journal Of Information Science And Engineering 28, pp. 453-470 , 2012.

[9]. R. Sravani, J. Swami Naik "A Study on Flexible Deterministic Packet Marking: An IP Traceback System", International Journal of Advanced Engineering Sciences And Technologies, ISSN: 2230-7818, Vol No. 9, Issue No. 1, pp. 01 – 07, 2011.

[10]. Shih-Hao Peng, Kai-Di Chang, Jiann-Liang Chen, I-Long Lin, and Han-Chieh Chao "A Probabilistic Packet Marking scheme with LT Code for IP Traceback", International Journal of Future Computer and Communication, Vol. 1, No. 1, June 2012.

[11].Y.Bhavani, P.Niranjan Reddy." An Efficient Ip Traceback Through Packet Marking Algorithm", International Journal of Network Security & Its Applications (IJNSA), Vol.2, No.3, July 2010.

[12]. Jeevaa Katiravan, C. Chellappan, N. Duraipandian," Improved IP Trace Back Using Pre-Shared Key Authentication Mechanism**"** European Journal of Scientific Research ISSN 1450-216X Vol.50 No.1 , pp.99-109, 2011.

[13] Andrey Belenky and Nirwan Ansari," IP Traceback With Deterministic Packet Marking",IEEE 2003.

[14] Chao Gong and Kamil Sarac," Toward a Practical Packet Marking Approach for IP Traceback", 2006.

[15] Michael T. Goodrich," Probabilistic Packet Marking for Large-Scale IP Traceback",IEEE 2007.

[16] WANG Xiao-jing, WANG Xiao-yin," Topology-assisted deterministic packet marking for IP traceback", ELSEVIER 2010.

[17] Drew Dean, Matt Franklin, Adam Stubblefield," An Algebraic Approach to IP Traceback", 2001.

[18] Kihong Park Heejo Lee," On the Effectiveness of Probabilistic Packet Marking for IP Traceback under Denial of Service Attack", 2001.

[19] Tatsuya Baba and Shigeyuki Matsuda," Tracing Network Attacks to Their Sources",IEEE 2002.

[20] Bilal Rizvi and Emmanuel Fernández-Gaucherand," Effectiveness of Advanced and Authenticated Packet Marking Scheme for Traceback of Denial of Service Attacks", IEEE 2004.

[21] Alex C. Snoeren, Craig Partridge, Luis A. Sanchez, Christine E. Jones," Hash-Based IP Traceback",ACM 2001.