Integrated Intelligent Research (IIR)
International Journal of Web Technology
Volume: 05 Issue: 01, June 2016, Pages: 81-83
ISSN: 2278-2389

Study on Various Marking Techniques for IP Traceback

C. Kavitha, K.Chitti Babu, S.Vaishnavi
Assistant Professor, CSE Department, R.M.K College of Engineering and Technology, Puduvoyal
Email: kavitha4cse@gmail.com, mailtocbabu@gmail.com, vaishnaviseva@gmail.com

Abstract - Attacks on the internet are a growing threat. Various means of malicious acts usually origin from an anonymous source which will steals, alters, compromise trustworthiness or destroys a specified victim by hacking into a susceptible target system. One challenge in defending against this Distributed Denial of Service attacks is that, source IP addresses are spoofed by attackers in order to evade traceability and bypass access controls. IP Traceback method is a solution for attributing cyber Attacks. It is also useful for accounting user traffic as well as network diagnosis. Although there are many IP traceback methods are proposed, the majority of research efforts decade in this area. Marking-based traceback (MBT) is a traceback approach which will find the traceback message delivery problem. This is very important to the successful completion of a Traceback which has been adequately studied in this paper. To address this issue, various Marking techniques for IP traceback have been presented.

Keywords - IP Traceback; Marking Techniques; Cyber Attacks; DDOS attacks; message content decoding.

I. INTRODUCTION

The Internet provides a wealth of value and information to its users, but this accessibility makes it vulnerable to well-equipped users intent on disrupting the flow of information. The Internet protocol (IP) specifies a header field in all IP packets that contains the source IP address. This would seem to allow for identifying every IP packet's origin. IP traceback is a common solution to identify the sources of attacks and also the paths followed by these attack packets. It can mitigate the attack effects and enable forensic investigations of network attacks [12]. Although IP traceback approaches are motivated by many adversarial applications, they can also be used for a wide range of non-adversarial network analysis applications, such as traffic accounting analysis, fault diagnosis analysis, network bottleneck identification and path validation analysis[6][8][10].

The key needs for IP trace back strategies include: Existing network protocols must be compatible, Network traffic overhead must be insignificant, It support for progressive implementation, It should even be compatible with existing routers and network infrastructure While a number of IP traceback techniques have been proposed, marking-based Traceback (MBT) approach has received respectable attention. The basic idea of Marking Based Technique is that routers convey their traceback messages (e.g., the identity information) to the end-hosts by marking on passing packets. Existing analysis efforts in Marking Based Technique are devoted to two key problems. The primary issue is that the traceback decision making at individual routers. The second analysis issue is that the message content encoding, that determines the data a router marks in the IP header. In this paper, Comparison of all various Marking techniques has been extensively studied.

II. RELATED WORK

Q. Dong, S. Banerjee, M. Adler, and K. Hirata [10] propose an Efficient Probabilistic Packet Marking. Probabilistic packet marking technique is a general technique in which routers uses to reveal local network information to end-hosts. Such internal information is probabilistically set by the routers in packet headers of regular IP packets to destinations. They investigate the two representative examples such as the internet bottlenecks and IP traceback demonstrate its effectiveness. Their proposed scheme imposes a single-bit overhead in the packet headers. It significantly reduces the no. of IP packets which is required to convey the relevant information that is compared to the best known scheme. Vahid Aghaei-Foroushani and A. Nur Zincir-Heywood [4] propose a Probabilistic Flow Marking for IP Traceback (PFM) technique. DDOS are one of the security issues we faces on the Internet today. The source of the attacks are difficult to counter. To hide their original source, they often use spoofed source IP addresses. They presents a new IP traceback scheme, which is called as Probabilistic Flow Marking (PFM). The main goal in this paper is to trace the anonymous flooding attacks which held on the network then back toward their original source.

Ahmad Fadlallah, Ahmed Serhrouchni, Youcef Begriche, Farid Naït-Abdesselam[9] propose a Hybrid Messaging-Based technique for IP traceback. In this paper, they propose a new traceback scheme which mixes these two techniques in order to achieve the efficiency. The hybrid messaging technique uses packet marking mainly to include signaling information in IP packets which are forwarded. In complementary signaling part, out-of-band messaging is used in the case of random spoofed IP packets. The evaluation of the proposed work is against the various performance bottleneck. Ming-Hour Yang and Ming-Chien Yang [7] propose a RIHT which is a Novel Hybrid IP traceback Scheme. They propose a hybrid IP traceback technique with an efficient packet logging which aims to have a fixed storage for each router in the packet logging. This does not require to refresh the logged tracking information. Also in attack path reconstruction, there is no need to achieve zero false positive and false negative rates in attack-path reconstruction.

III. COMPARISON OF VARIOUS MARKING BASED APPROACHES

There are various marking based approaches for IP traceback. We discuss only some important latest techniques among them.

International Journal of Web Technology
Volume: 05 Issue: 01, June 2016, Pages: 81-83
ISSN: 2278-2389

A. Opportunistic Piggyback Marking (OPM)

This technique differentiates itself from the existing work. It decouples the traceback message content encoding as well as the delivery functions in marking based approaches, and achieves expedited and robust traceback message delivery by exploiting piggyback marking opportunities.

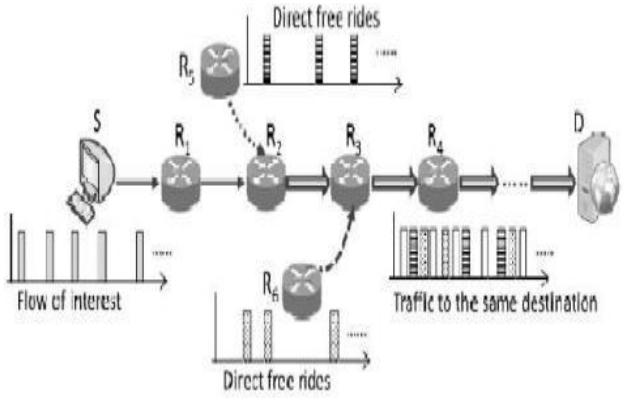

Fig 1: Direct Piggyback Marking

Fig. 1 shows an opportunistic piggyback marking scheme. In this case, the flow of interest is forwarded from Source S to Destination D through intermediate routers {R1, R2, R3, R4,..}. Besides the traffic from Source to Destination, R5 and R6 forwards packets to the destination D. Along the network path assume all routers that are traceback-enabled routers, and are thus involved in the packet marking operation. From Fig. 3, we observe that external-flows paths are forwarded from R5 or R6 that carry these message fragments directly to Destination. The traceback messages which are delay in delivery are opportunistically reduced by exploiting external traffic flows.

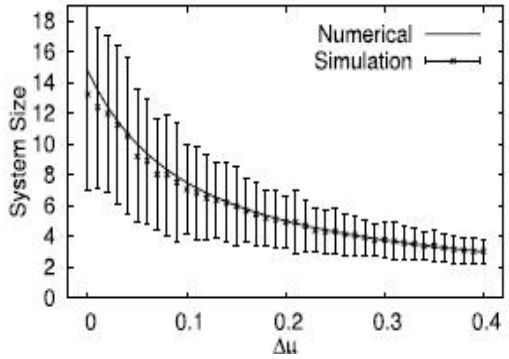

Fig 1.1(a): Average System Size

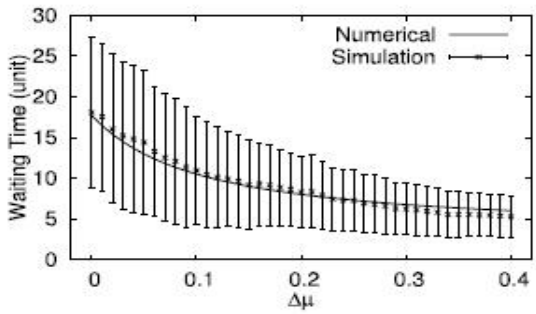

Fig 1.1(b): Average waiting time.

Fig. 1(a) and Fig. 1(b) is the average steady-state of system size and also the waiting time against the piggyback marking opportunity scheme, respectively. This evaluates the performance of piggyback marking approach.

B. Efficient Probabilistic Packet Marking (EPPM)

This technique is a probabilistic packet marking technique with a potential application. This technique locates the Internet bottlenecks and IP traceback which are investigated as two representative examples mainly to demonstrate its effectiveness

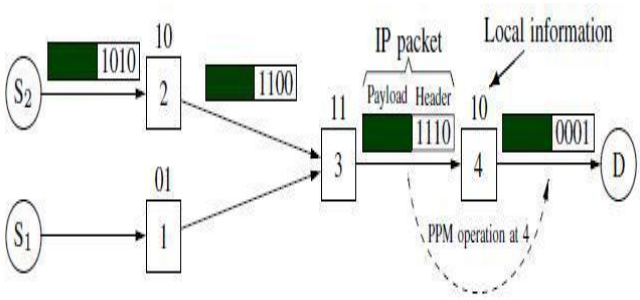

Fig 2: An example of probabilistic packet marking

The Fig 2 considers the traffic flow on an Internet path from the source S2 to the destination D along the path from S2 to 1, 1 to 3, 3 to 4, and 4 to D. All the routers in the path have some local information which needs to be communicated to the destination R.

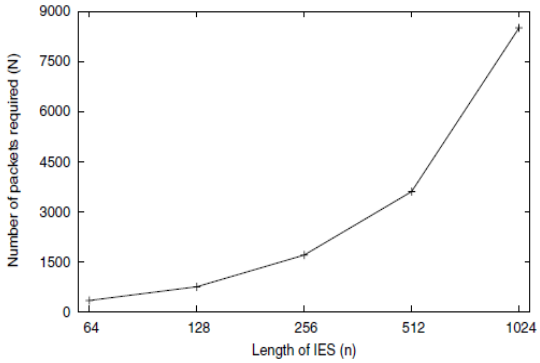

Fig 3: EPPM technique Tradeoff

Many different Probabilistic Packet Marking techniques are differed in their number of PPM bits which are allocated. In each intermediate router, the transformation is applied and the no. of IP packets are required to convey the local information to the destination with the decode information held at the destination. The two general measures based on probabilistic packet marking efficiency are: the no. of PPM bits that are required in packet header and the no. packets that are required to convey local network information to the destination.

C. Probabilistic Flow Marking (PFM)

Fingerprint in the packets are randomly embedded by PFM technique. This enables PFM technique to identify the traffic origin which traverses through the internet based on the flow, despite of the source IP address spoofing. Three real life Internet data sets using Probabilistic Flow Marking technique from the CAIDA archives has been evaluated. The evaluation results show that when compared to the previous IP traceback schemes, no. of marked packets required to traceback are significantly decreased by PFM and represents a performance and deployability. There is also Deterministic Flow Marking technique which embeds the source identity data for every flow to the first packets, whereas PFM marks only some of the

International Journal of Web Technology
Volume: 05 Issue: 01, June 2016, Pages: 81-83
ISSN: 2278-2389

flows which are chosen randomly. Identifications of the origin of the traffic are encoded by Probabilistic Flow Marking scheme and then partial information are embedded into the forwarded packets which are randomly chosen few that are destined to the target on the edge router. Later the origin of the traffic can be inferred by the victim target by combining a low no. of marked packets.

IV. CONCLUSION

In this paper, we have presented a complete study on various marking techniques for IP traceback. This survey provides an overview of the evolution of existing IP traceback method using various Marking based approaches. This study shows that the main focus on traceback scheme has moved from the quick traceback from the target to the quick detection of attack before the victim/target is affected.

References

[1] Long Cheng, Dinil Mon Divakaran, Wee Yong Lim, and Vrizlynn L. L. Thing, "Opportunistic Piggyback Marking for IP Traceback", IEEE Transactions On Information Forensics And Security, Vol. 11, No. 2, February 2016.
[2] H. Zhang, J. Reich, and J. Rexford, "Packet traceback for software defined networks,"Dept. Comput. Sci.,Princeton University, Princeton, NJ, USA, Tech. Rep. TR-978-15, 2015.
[3] The CAIDA UCSD DDoS Attack 2007 Dataset, http://www.caida.org/data, accessed Oct. 2015.
[4] Vahid Aghaei-Foroushani and A. Nur Zincir-Heywood ,"A Probabilistic Flow Marking for IP Traceback (PFM).", International Workshop on Reliable Networks Design and Modeling (RNDM), Oct. 2015
[5] Y. Xiang, K. Li, and W. Zhou, "Low-rate DDoS attacks detection and traceback by using new information metrics," IEEE Trans. Inf. Forensics Security, vol. 6, no. 2, pp. 426–437, Jun. 2011.
[6] T. H.-J. Kim,C. Basescu, L. Jia, S.B. Lee, Y.-C. Hu, and A.Perrig,"Lightweight source authentication and path validation," in Proc. SIGCOMM, 2014, pp. 271–282.
[7] Ming-Hour Yang and Ming-Chien Yang, "RIHT: A Novel Hybrid IP Traceback Scheme", IEEE Transactions on Information Forensics And Security, Vol. 7, No. 2, April 2012.
[8] L. Lu, M. C. Chan, and E.-C.Chang, "A general model of probabilistic packet marking for IP traceback," in Proc. ASIACCS, 2008, pp. 179–188.
[9] Ahmad Fadlallah, Ahmed Serhrouchni, Youcef Begriche, Farid Naït-Abdesselam,"Hybrid Messaging-Based Scheme for IP Traceback", International Conference on Information and Communication Technologies: From Theory to Applications, 2008.
[10] Q. Dong, S. Banerjee, M. Adler, and K. Hirata, "Efficient probabilistic packet marking," in Proc. ICNP, Nov. 2005, pp. 367–377.
[11] B. Al-Duwairi and M. Govindarasu, "Novel hybrid schemes employing packet marking and logging for IP traceback," IEEE Trans. Parallel Distrib. Syst., vol. 17, no. 5, pp. 403–418, May 2006.
[12] H. Aljifri, "IP traceback: A new denial-of-service deterrent?" IEEE Security Privacy, vol. 1, no. 3, pp. 24–31, May/Jun. 2003.