International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

A Survey on Novel Flow Marking IP Traceback Schemes

S. M. Chaware[1], Shubhangi R. Sardar[2]

[1]Pune University, Maharashtra, India

[2]PG Student, Computer Engineering, Pune University, Maharashtra, India

Abstract: ***In recent years, communication and data stored over the World Wide Web (www) increased enormously. At the same time attacks over internet have increased. As a result, lots of researches have been done on securing the internet infrastructure. Due to trusting nature of IP, the source address of a packet is never authenticated. This leads to the need of some technique to find the source of transmitted packet. IP traceback has become widely used technique for these researches .In previous IP traceback methods, finding exact source of attack and reconstructing the attack path was two major issues. Deterministic Flow Marking (DFM) provides an innovative approach to overcome these issues. It traces the origin of spoofed source IP Address of attacker node and provides an optional authentication approach for the victim. In this paper, a wide survey has been carried out to identify and classify the existing IP traceback schemes.***

Keywords: DDoS Attack, IP Traceback, Packet Marking

1. Introduction

In the field of communication and data storage over the internet, security has been the key center of many researchers over the years. The Denial of Service (DoS) and Distributed Denial of Service (DDoS) are attacks which has changed the perspective of network security. By these types of attacks even high performance capacity servers can be crushed. Due to the trusting nature of IP, the source address of a packet is never authenticated therefore it is difficult for the victim to identify the source of DoS/DDoS attack. This leads to the need of some technique to find the source of the transmitted packet. Therefore different IP traceback approaches have been studied and evaluated [14]. The two main drawbacks with the studied approaches are: First, due to the considerable computational overhead, it's inefficient to use hop-by-hop path reconstruction. It takes lot of time to collect the samples of the traveled path. Secondly, changes are needed to be done in the core routing structure, for the path reconstruction. This is not profitable at all. Accordingly, the existing approaches can be classified by different viewpoints [13][17].

A new deterministic packet marking approach, called DDPM, was proposed [9]. Its prime focus was on the DoS and DDoS attack. They successfully found the source of DoS and DDoS attack by deploying only edge routers in the internet. The base for this algorithm was the dynamic marking, which will be done at the edge routers or nearest routers from the victim node. The drawback of the algorithm was space overhead. But recently, the routers are equipped with large amount of physical memory. This makes the drawback ignorable. The paper also provided the authenticated marking system. This practice only uses one cryptographic MAC (Message Authentication Code) calculation per marking, which is orders of magnitude more competent to compute and can be adapted so it only requires

the 16-bit overloaded IP identification field for storage. The identification data needs to be passed to the destination for each current. The recognition data is separated into some fragments. Therefore, the mark contains the identification data and some bits required to identify a fragment. It also identifies marked and unmarked packets in a flow. Each destination maintains a table matching the flow ID and possible mark fragments. When a packet belong to an unseen flow arrives at the target, the target creates a new table entry in the reconstruction table. Then, it will extract the marking bits of this flow from the marked packets, and writes them in the corresponding fields. After all fragments corresponding to a flow reach the target, the starting node for the given flow becomes recognizable to the target. Using DFM (Deterministic Flow Marking), the target is able to differentiate the traffic of different nodes behind an edge router.

In authentication marking method [5], both parties share a secret key. The source appends the message with MAC (Message Authentication Code) of message using the key. Receiver can check the validity of MAC. This method also provides the router authentication, but it is impractical as each router needs to share the secret key with every potential victim. Therefore, the need of mechanism to authenticate the flow marking was aroused. Source can send signatures along with the marking data to the targets. Because a compromised router does not identify the secret keys of edge routers, it cannot forge flow markings. When the destination gets the signed flow, it uses the dispatcher's public key to validate the sender. If both parties agree, the destination knows that the author of the mark was in possession of the edge router's private key, and that the mark is in fact valid, or else it would reject the flow.

Besides these, [15] Deterministic Flow Marking (DFM) scheme was introduced for large distributed attacks

to the source node located in the LAN behind the edge routers. The deterministic method is chosen over the probabilistic method is due to the higher traceback accuracy. Same is the reason for the usage of deterministic marking for advanced security services. DFM also provided a method to authenticate the marking information to solve the issue of mark spoofing by forged routers. One advantage of the proposed authenticated flow marking method is that it is optional for the destination to extract and validate the signature for every flow while it does not get attacking flows. In circumstances when the victim is under attack, it may use the signature to authenticate the mark to find the attacker node. Therefore the target is not enforced to always consume its CPU and memory resources to verify Elliptic Curve Digital Signature Algorithm (ECDSA) signature as explained [6].

2. Literature Survey

Many traceback approaches have been proposed yet. According to [13][17][15] the traceback approaches are classified in diverse categories. They are Basic Principle, Processing Mode, and Location.

2.1 Basic Principle

If classified with Basic principle, the offered traceback methods are discriminated into Marking and Logging groups. In marking methods [12], the traveling packets are added with particular information by some or all routers in the path. Using this information, even if the IP is spoofed, the attacker can be traced down. In logging method [11], the routers keep some information associated to the travelling packet. This information can be later on used to traceback to the sender node from which the packet has been originated. Requirement of large amount of memory and CPU usage at routers of the attacked path creates a basic problem for logging method, as it stores information about each and every packet passed through the router [4].

2.2 Processing Mode

Based on the processing mode, traceback schemes are distinguished in two groups, deterministic and probabilistic. In deterministic method, the packet should be practiced at source as well as at target, despite of marking or logging. Though this method provides superior accuracy, it requires more dispensation overhead at both source and the target, in assessment to the probabilistic method. Probabilistic methods are somewhat analogous to the deterministic methods, only the required processing time and bandwidth is comparatively less. Most of the existing traceback methods are probabilistic.

2.3 Location

From the aspect of classification by locations, presented traceback methods can be divided into two groups. One that send traceback information through the edge routers next to the source, called source group. Second, in the network through some or all routers in the assault path called network group. Most of the present traceback methods belong to the network group. The basic purpose of the group is to identify attack path entirely or moderately [3][16]. These methods require inclusion of all routers and highly consume resources such as processing time and memory. While, source group method aims at identifying the attack source and not the attack path [1][7].

Light, scalable, secure DPM is suitable for many types of attacks [7]. A simple modification was needed to the basic approach to handle the situation for the fact that attacker can keep changing the IP source address during the attack. Although the marks in DPM cannot be spoofed, the fact that frequent spoofing of IP source address with diverse values by the attacker, may decrease the DPM's effectiveness. The destination could make to rely on the marks, which cannot be spoofed to solve this problem. The destination can verify that two halves of the ingress address do belongs to the same ingress address, without relying on the source address of the packet, by using a globally known hash function. This solution does require sending additional marks with hash value. However, the number of packets needed to reconstruct the ingress address will be increased.

Deterministic Edge Router Marking (DERM) for defense against DDOS attack was proposed to highlight reconstruction approach [10]. The reconstruction was done by user in two phases. Namely, a filtering phase and an attacker identification phase. The filtering phase involved a setting of flag in the table supported on marks, in arriving packets for identification of attacking traffic and usage of these marks to filter the attack traffic. The attacker identification phase involved noting down of the IP address of ingress packet and to check them against the filter table entries. The number of packets required for the identification of an attacker is also small.

3. IP Traceback Approaches

3.1 Probabilistic Packet Marking (PPM)

Based on approaches of IP traceback scheme discussed above PPM comes under Basic Principle: Marking, Processing Mode: Probabilistic, Location: Network Group. Figure 1 illustrates the PPM approach for IP traceback
.

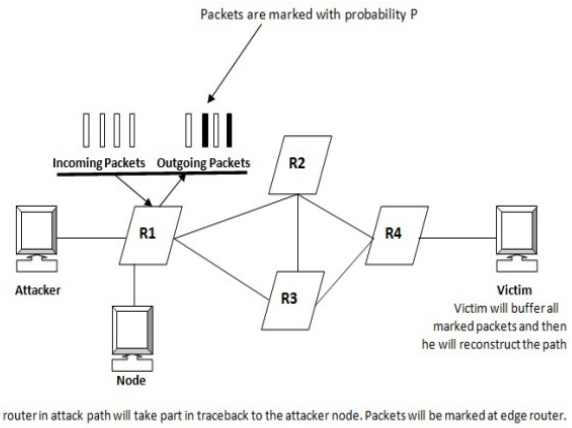

Figure 1: PPM approach for IP Traceback

In PPM [12], it is assumed that attacking packets are much more frequent than normal packets. It marks the packets

probabilistically with some path information and allows the victim to rebuild the path based on marked packets. But packets are marked randomly based on some probability therefore it is difficult to reconstruct the path. It requires high computational work when there are many sources. Many sources could result in false positive rate [5]. To overcome this problem, advance and authenticated PPM was proposed [5], which was able to trace more resources at one time and solved the problem of spoofed marking. To reduce the problem of reconstruction [12] another approach is presented [16] which reduced computational time and false positive rate.

3.2 Deterministic Packet Marking (DPM)

Based on approaches of IP traceback scheme discussed above DPM comes under Basic Principle: Marking, Processing Mode: Deterministic at packet level, Location: Source Group. Figure 2 illustrates the DPM approach for IP traceback.

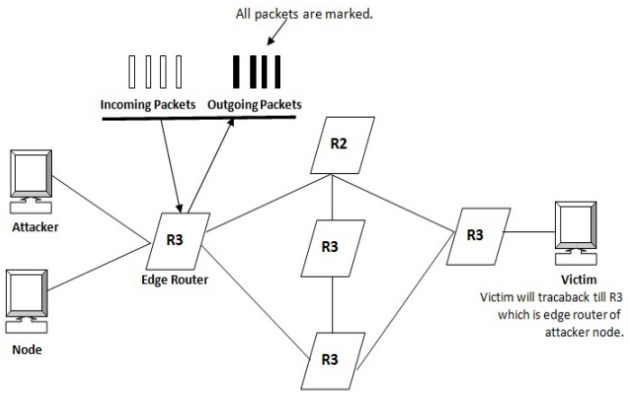

Figure 2: DPM approach for IP Traceback

By "Deterministic Packet Marking", the reference is made to the fact that, on a DPM enabled router, every packet traversed is marked. It means that every packet that goes through a router is inscribed with some added information about the router interface. The method is based on two key assumptions: First, any given packet may be generated by the Attacker and second, routers have limited CPU and memory.

The prime focus was on security against the anonymous attacks[1]. In this approach, the identity of attacker(s) is not instantly available for the victim. Because the source IP address is spoofed. Therefore, a solid technique to traceback the correct IP was needed and the deterministic packet marking was initially proposed [1]. The deterministic packet marking (DPM) technique is based on marking packets with the fractional address information of ingress interface lonely. The victim is able to recuperate the entire address information after getting some packets from a particular attacking host or hosts. The entire path is not really needed for the traceback, as it would be different for different packets because, the route is randomly followed by different packets. This approach is scalable, easy to implement, also it introduces no large bandwidth and creates no additional processing overhead on the network equipments, like routers. It can trace thousands of attackers simultaneously during a Distributed Denial of Service (DDOS) attack. Almost all processing is done at the victim side. Internet Service Providers (ISPs) involvement in these processes is very limited. Minimum changes are needed to be done to the infrastructure and minimal operations are required to install the DPM. The desired quality of any traceback scheme is not to reveal the internal topology of provider's network, which is achieved by the DPM.

3.3 Deterministic Flow Marking (DFM)

Based on approaches of IP traceback scheme discussed above DPM comes under Basic Principle: Marking, Processing Mode: Deterministic at flow level, Location: Source Group. Figure 3 illustrates the DFM approach for IP traceback.

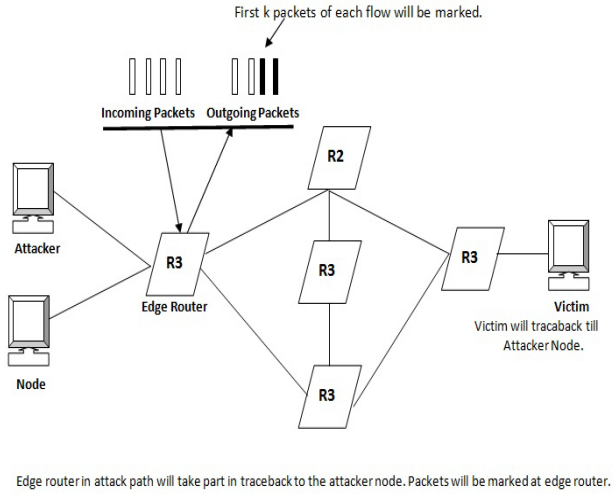

Figure 3: DFM approach for IP Traceback

Deterministic Flow Marking (DFM) approach [15], allows the victim to traceback the origin of an incorrect or spoofed source IP address up to the attacker node, even if the attack has been originated from a network behind a NAT or a proxy server. This scheme has low processing and memory overhead at the victim machines and edge routers. Additionally, DFM provides an optional authentication, so that a compromised router cannot forge markings of other uncompromised routers.

3.3.1 Authenticated Flow Marking

Although, victim can reach the exact attacker node [14], marking bits can also be changed and victim will not be able to find the attacker node. In this case authentication method is required.

In an authentication marking method suggested [5], a secret key is shared by the participating parties, source and destination. When a message is send by the source to the destination, the Message Authentication Code (MAC) of message is appended to the message by source. When the message arrives at the destination, it can check the legitimacy of MAC. The secret key can be time varying to guard against replay issue.

A Digital Signature Algorithm is needed for the authentication process in DFM. The simplest algorithm was RSA algorithm. But there are two major drawbacks of the

RSA algorithm: first, it is very expensive to compute. And second, the memory overhead is large. So, Elliptic Curve Digital Signature Algorithm (ECDSA) is used for digital signing [2]. The elliptic curve analogue of the Digital Signature Algorithm (DSA) is the Elliptic Curve Digital Signature Algorithm (ECDSA).

3.3.2 ECDSA algorithm

The prime reason for the popularity of ECDSA [2] algorithm is that, there is no sub exponential algorithm have been developed to solve the elliptic curve discrete logarithm problem on specifically chosen elliptic curve. Hence, ECDSA takes the full exponential time to solve the problem, while other best algorithm developed for solving the fundamental integer factorization for RSA and discrete logarithm problem in DSA; both of them take sub exponential time. A highly secured key is generated by the implementation. And as small key size is used in the elliptic curve, thus it consumes lesser bandwidth.

As compared to competitive systems like, RSA and DSA, ECDSA uses significantly smaller parameters, but with the security of equivalent level [8]. Having smaller key has some benefits, which includes faster computation time and reduction in storage space, processing power and bandwidth as well. Due to this features, ECDSA is ideal for constrained environments like pagers, PDAs, smart cards and cellular phones.

4. Comparison Parameters

Base on some parameters, comparison of processing modes PPM, DPM and DFM is summarized in following Table 1.

Table1: Comparison of IP Traceback Approaches.

Parameters	*PPM*	*DPM*	*DFM*
Computational Overhead	Moderate	Low	Very Low
Maximum Traceback Ability	Edge Router	Upto ingress interface of edge router	Upto attacker node
Flow Marking	No	No	Yes
No. of packets marked at ingress interface of edge router	Random number of packets	Each packet of every flow	Few packets of every flow
Minimum Packets required to Trace IP	More than DPM	More than DFM	Minimum 4

5. Conclusion and Future Work

With increasing number of internet users, issue of tracing the source of Denial of Service (DoS) attack is reviewed. In this paper, a wide survey has been carried out to identify and classify the existing IP traceback schemes. Selecting the best method for packet marking is the key point in tracing the source IP. Challenges of previous IP traceback methods was, reconstructing the attack path efficiently and tracing exact attacker node hidden by a NAT or proxy server. These challenges are overcome by DFM IP traceback approach. In addition it provides optional authentication method. DFM provides higher traceback accuracy and authentication, but victim resources in attach path are consumed even before the traceback is completed. Therefore, a need arises to provide a mechanism to preserve the resources in attach path even before the IP traceback. To accomplish this, attack detection, prevention and traceback with novel approch can reinforce complete security platform to preserve the resources in attack path even before traceback..

References

[1] Ansari, Belenky, N. “Deterministic Packet Marking”, New Jersey Institute of Technology, 2005.
[2] Aqeel Khalique, Kuldip Singh, Sandeep Sood, “Implementation of Elliptic Curve Digital Signature Algorithm”, Indian Institute of Technology, Roorkee, 2010.
[3] A. Yaar, A. Perrig, D. Song, “Pi: A Path Identification Mechanism to Defend Against DDOS Attacks” Proc. Symposium on Security and Privacy, 2003.
[4] B. Gong., K. Sarac, “IP Traceback based on Packet Marking and Packet Logging”, University of Texas at Dallas, 2005.
[5] D. X. Song, A. Perrig, “Advanced and Authenticated Marking Schemes for IP Traceback,” INFOCOM, 2001.
[6] D. Johnson, A. Menezes and S. Vanstone, “The Elliptic Curve Digital Signature Algorithm (ECDSA)”, Certicom Corporation, 2009.
[7] M. T. Goodrich, “Efficient Packet Marking for Large-Scale IP Trace back,” Proc. Ninth ACM Conference of Computer and Communication Security, 2002.
[8] National Security Agency/ Central Security Service (NSA/CSS), the Case for Elliptic Curve Cryptography.
[9] R. Shokri, A. Varshovi, H. Mohammadi, N. Yazdani, B. Sadeghian, “DDPM: Dynamic Deterministic Packet Marking for IP Traceback”, 2006.
[10] S. K. Rayanchu, G. Barua, “Tracing Attackers with Deterministic Edge Router Marking”, 2005.
[11] S. Matsuda et al., “Design and Implementation of Unauthorized Access Tracing System,” SAINT 2002.
[12] S. Savage, D. Wetherall, A. Karlin and T. Anderson, “Network Support for IP Traceback,” IEEE/ACM Transactions on Networking, 2001.
[13] T. Subbulakshmi, I. A. A. Guru and S. M. Shalinie, “Attack Source Identification at Router Level in Real Time using marking Algorithm Deployed in Programmable Routers”, ICRTIT, 2011.
[14] V. Aghaei-Foroushani and N. Zincir-Heywood, “Deterministic and Authenticated Flow Marking for IP Traceback”, The 27th IEEE International Conference on Advanced Information Networking and Applications (AINA-2013), March 2013.
[15] V. Kuznetsov, H. SandStrom, A, Simkin, “An Evaluation of Different IP traceback Approaches”, Information and Communications technology, 2002.
[16] Y. Tseng, H. Chen and W. Hsieh, “Probabilistic Packet Marking with Non-Preemptive Compensation,” IEEE Communications Letters, vol. 8, no. 6, pp. 359–361, JUN 2004.
[17] Z. Gao, N. Ansari, “Tracing Cyber Attacks from the Practical Perspective”, IEEE Communications Magazine, 2005.