An IP Traceback Scheme Integrating DPM and PPM

Fan Min, Jun-yan Zhang, and Guo-wie Yang

College of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu 610051, China
{minfan, xindyzhang, gwyang}@uestc.edu.cn

Abstract. IP traceback technology is an important means combating Denial of Service (DoS) attacks in Internet. This paper proposes a new IP traceback scheme constituting two parts: the first part is constructing a traceback tree by integrating Deterministic Packet Marking and Probabilistic Packet Marking, and the second part is getting attack routes by analyzing this traceback tree. Basing on performance analysis, we point out that our scheme is both efficient and robust against mark field spoofing.

Keywords: Denial of Service, IP spoofing, IP traceback, Deterministic Packet Marking, Probabilistic Packet Marking

1 Introduction

A "Denial-of-Service" (DoS) attack is characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service [1]. The attackers may use one or more of these ways to achieve their aims: a, bring down the machine providing the service; b, flood the link between the user and the service provider; c, utilize resources available at server using bogus requests [2]. Distributed Denial of service (DDoS) attacks constitutes one of the single greatest threats facing businesses involved in electronic commerce [3].

DoS attackers usually hide their actual address by IP forging, especially IP source address spoofing. Ingress / Egress filtering is effective method against IP forging. In ingress filtering, a router does not allow a packet into the network, if it has a source IP address of a node inside the network. On enabling egress filtering, a router sends packets to Internet only if the source address of the packet is that of a node within that network [4]. If ingress filtering is installed, spoofed IP address has to be in the same network part in order to pass through the router. Egress filtering is a complement of ingress filtering. The principal problem with ingress filtering is that its effectiveness depends on widespread, if not universal, deployment. A secondary problem is that even if ingress filtering were universally deployed at the customer-to-ISP level, attackers could still forge addresses from the hundreds or thousands of hosts within a valid customer network [5].

IP traceback is an important method finding actual addresses of IP forging attackers, also called anonymous attackers. If attack source could be found, attacking packet from corresponding computer can be abandoned, and attack could be prevented, legal issues could also be involved for corresponding person.

J. Zhou, M. Yung, Y. Han (Eds.): ACNS 2003, LNCS 2846, pp. 76–85, 2003.

2 Relative Works

Packet marking [5-8] is a new IP tracing back scheme in recent years, it can be further classified into Deterministic Packet Marking (DPM) and Probabilistic Packet Marking (PPM).

2.1 DPM

Using IP Record Router option [10] in IP packet, each router in the network will write its own IP address into option field of the IP packet. And destination host can get full route of correspond packet by simply investigating this field. This scheme is called DPM.

Shortcomings of DPM include: a, increases packet length dramatically. For about 20 hops the packet size will increase by 80 bytes (IPv4). An overhead of 80 bytes for every packet (about 500 bytes) is unacceptable [6]; b, since the length of the path is not known a priori, it is impossible to ensure that there is sufficient unused space in the packet for the complete list [5]; c, increases router operation.

2.2 PPM

PPM [6-8] is a scheme trying to make up shortcomings of DPM, it is supposed to deal with type b and c attack in Section 1. It is further classified into:

1. *Node Sampling*. A single static "node" field is reserved in the packet header—large enough to hold a single router address (i.e., 32 bits for IPv4). Upon receiving a packet, each router chooses to write its address in the node field with some probability p [5].
2. *Edge Sampling*. Reserve two static address-sized fields, *start* and *end*, in each packet to represent the routers at each end of a link, as well as an additional small field to represent the distance of an edge sample from the victim [5]. Upon receiving a packet, each router chooses to write its address in the *start* field with some probability p, and the *end* field is written by the next router if *start* field is written by the previous router. Distance from the edge to destination can be easily gotten through adding up [8].

In IPv4, 72 bits is needed for two address-sized fields and a distance field. Savage [5] uses coding method to compress it into 16 bits and put into *ID* field of IP header. Complexity is incurred by coding. In the following context, PPM all refer to node sampling.

Advantages of PPM over DPM includes: a, only one address-size field is needed; b, packet size does not change on the flight; c, a router only mark a packet with probability p, incurring less operation.

Disadvantages of PPM includes: a, getting a full path from victim to attacker is a rather slow progress; b, for DDoS attacks, this method may fail [5].

3 Integrated Marking and Tracing Scheme

In this section we present an integrated marking and tracing scheme based on DPM and PPM.

3.1 Assumptions

Let A denote attacking host, A is not unique; let V denote victim, V is unique; let T1 and T2 denote two types of ICMP packets, they all have *IP Record Router option* set.

Our scheme relies on the following assumptions. In most cases, these assumptions hold true.

[Assumption 1] Source address and marking field of attacking packets are spoofed.

Source address spoofing is the fundamental reason of IP traceback. Attackers usually choose spoofing IP source address except DDoS with very good distribution. Marking field spoofing can effectively impede traceback by the victim [8].

[Assumption 2] Routing does not change in a short period.

Theoretically network topology can change at any time. But changes of important network elements such as routers do not happen frequently. In short period (e.g. a few minutes), the probability of routing change is very small.

[Assumption 3] Let NS denote maximal packet sending speed of ordinary host to V; let P denote packet sending speed of any single A to V; let K denote attack volume factor; and $P > NS \cdot K$.

In order to make attack effective, for situation that number of A is not large, attackers may set $K > 100$.

[Assumption 4] V is unable to distinguish whether or not a packet is attack packet simply by data in the packet.

3.2 Scheme Description

Our scheme constitutes three closely related algorithms.

Any router runs Algorithm 1 upon receiving a packet:

1. If current packet is ordinary packet, and the destination address is not this router, fill IP address of this router into *node* field of this packet with probability p, and forward it; /*The same as PPM*/
2. If this packet is T1 packet, and the destination is not this router, write IP address into option field of this packet and forward it; /*The same as DPM*/
3. If this packet is T1 packet, and the destination is this router,

3.1 If the *Key* in the *Key* field is not generated by this router recently, exchange source and destination addresses of this packet, write IP address into option field of this packet and send it out;

3.2 If the *Key* in the *Key* field is generated by this router recently, store it for further use.

Algorithm 1. Marking algorithm run by routers.

When V discovers that packet arrival rate excesses a given bound, it concludes that it is under attack, and runs Algorithm 2.

1. Stop service;
2. Generate a key *Key*;
3. In time Δt, for each arrival packet, generate a T1 packet, copy the mark field of the arrival packet into destination address of the ICMP packet, copy *Key* into corresponding field, send it out;
4. Run Algorithm 3, analyze arrival T1 packets containing *Key*;
5. According to the analysis result, send T2 packets to routers nearest to A, and these routers will abandon packets whose destination is V.

Algorithm 2. Trace algorithm run by V

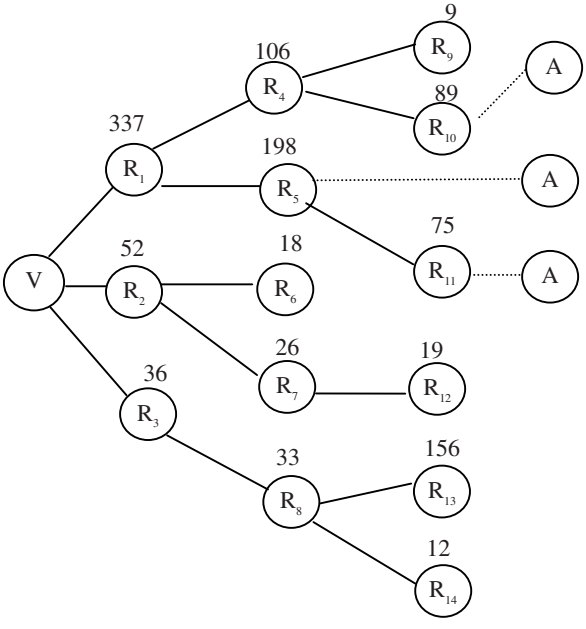

Fig. 1. An example of network topology

Upon receiving T1 packets from routers, V gets a series paths from which a tree taking V as root is constructed. Fig. 1 is an example of such tree, A is not included.

In Fig. 1, data above each node (called marking number) represents T1 packets received by V with corresponding node as source in Δt. Next we describe T1 packet analysis algorithm using Fig. 1.

1. According to node level with ascending order: let *MP* denote marking number of current node, let *C* denote its children number; let MC_i denote marking number of

children subject to $MC_1 \geq MC_2 \geq ... \geq MC_C$. If $MP < \sum_{i=1}^{C} MC_i$, decrease MC_1, MC_2, ..., MC_C until $MP = \sum_{i=1}^{C} MC_i$. In fig. 1, marking number of R_{13} should be changed to 21. For another example, suppose node N's marking number is 56, marking numbers of its four children is 132, 77, 15 and 9, these numbers should be changed to 16, 16, 15 and 9 respectively.

2. According to node level with descending order: if marking number of a node is smaller than $1/\alpha$ of that of its brother, delete sub-tree rooted at this node. We call α *safe speed factor 1*, and it's reasonable to let $\alpha \in [5, 10]$. If $\alpha = 5$, in fig. 1 R_9 should be deleted;
3. According to node level with descending order: if a node is already a leaf, and its marking number is less than $1/\beta$ of average marking number of the same level. We call β *safe speed factor 2*, it's reasonable to let $\beta \in [2, 3]$. If $\beta = 2$, in Fig. 1 R_{12}, R_{13}, R_{14}, R_6, R_7, R_8, R_2, R_3 should be deleted with corresponding order;
4. The remaining leaves are adjacent with A. In Fig. 1 they are R_{10} and R_{11};
5. According to node level with decreasing order: if a node has marking number greater than double of its children marking number sum, this node is also adjacent with A. In Fig. 1 it is R_5.

Algorithm 3. T1 packet analysis algorithm run by V.

3.3 Scheme Explanation

In essence, this scheme is an integration of PPM and DPM, in ordinary cases PPM is occupied, while routers use DPM on demand of V after DoS attack is detected.

Next we explain Algorithm 3 in detail. Let N denote node in context; because node has a unique address, let *N* denote address of N; let *d* denote hop count from N to V.

1. According to assumption 4, only packet sending speed from N to V can be collected to judge if N is adjacent with A;
2. From Algorithm 1 we can see that for IP packet from the same source, upon receiving it in V, the probability of the marking field be N is $p \cdot (1-p)^{d-1}$, be a child of N is $p \cdot (1-p)^d$. So we have

$$MP \cdot (1-p) = \sum_{i=1}^{C} MC_i \tag{1}$$

Obviously $0 < p < 1$, we have

$$MP \geq \sum_{i=1}^{C} MC_i \tag{2}$$

So only two kinds of reasons may lead to $\sum_{i=1}^{C} MC_i > MP$: a, because of uncertainty of probability. In this situation, a little modification of a few relatively large marking numbers does not influence result of the scheme; b, A forged a large amount of packets using some children of N as source address, and the most suspicious ones are those who have large marking numbers. So step 1 can greatly eliminate marking field spoofing.

3. Step 2, 3 are based on Assumption 4;
4. A router can receive attack packet directly or indirectly, which is the very basis of step 5.

3.4 Performance Analysis

Let T_L denote time from detecting attack to locate routers nearest to A. It constitutes three parts: I, time for collecting enough attack packet, Δt; II, time from sending T1 packets to receiving them; III, time needed running Algorithm 3. Next we analyze these three parts one by one:

I. Let A_i denote a specific attacker. To confirm that N is nearest to A_i, V needs a number of packets with marking field N. Let R_N denote packets needed for analysis, R_A denote packet from A_i, we have

$$R_N = R_A \cdot p\,(1-p)^{d-1} \tag{3}$$

Let packet generating speed of A_i be P, we have

$$\Delta t = \frac{R_A}{P} = \frac{R_N}{P \cdot p\,(1-p)^{d-1}} \tag{4}$$

R_N is related with accuracy of allocating A_i, R_N is determined by V. Routers can set p to minimize Δt. Let

$$f(p) = p\,(1-p)^{d-1} \tag{5}$$

$$f'(p) = (1-p-d\cdot p+p)(1-p)^{d-2} = (1-d\cdot p)(1-p)^{d-2} \tag{6}$$

Clearly when

$$p = \frac{1}{d} \tag{7}$$

$f(p)$ is maximized, and Δt is minimized.

In Internet environment, $d = 20$ is a widely used setting [8]. Under this condition we should set $p = 0.05$, if we further set $R_N = 50$, then

$$\Delta t = \frac{2650}{P} \tag{8}$$

Specifically, Δt = 5.3 (seconds) while P = 500 (packets / second); Δt = 88.3 (seconds) while P = 30 (packets / second).

If V can cache recently received packets, Δt can decrease accordingly.

II. The second part is related with channel speed. In most cases, it should be less than 1 second. Moreover, this time is overlapped with the first part.

III. Algorithm 4 only involves single loop, the time complexity is

$$O(ND) \tag{9}$$

ND is the number of routers sending back T1 packet to V. Run time of Algorithm 4 should also be less than 1 second.

In summary, T_L is mainly decided by Δt, while the latter is mainly decided by P. When number of A is relatively small, to make attack more effective, P is relatively large, and T_L can be under 10 seconds; when number of A is relatively large (well distributed DDoS), P is relatively small, and T_L may be tens of seconds or more. Another important problem incurred by small P is that K can also be small (e.g., less than 10), and our scheme can not distinguish between attack packets and ordinary packets.

3.5 Influence of Spoofed Marking Field

In PPM, the probability of receiving a marked packet from the farthest router is $f(p)$ (see Equation (5)), and the probability of receiving a packet never marked (potentially being spoofed by the attacker) is

$$g(p) = (1-p)^d \tag{10}$$

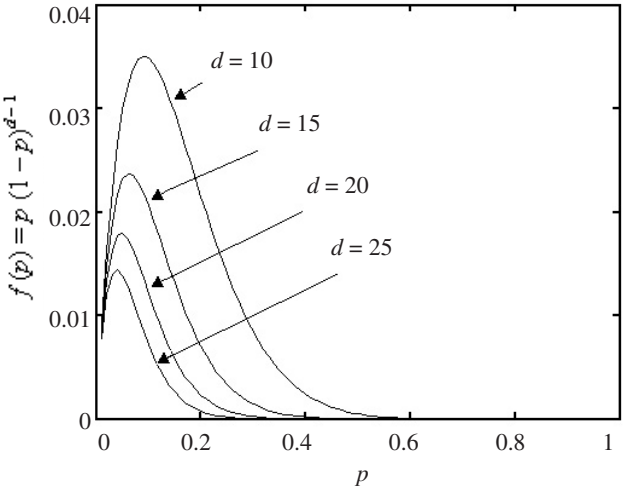

Fig. 2. Probability of receiving packets marked by the farthest router

For effectiveness, we want to maximize $f(p)$, which in turn requires $p=1/d$ (see Equation (7) and Fig. 2). While for robustness, we want to minimize $g(p)$, which in turn requires $p = 1$ (See Fig. 3).

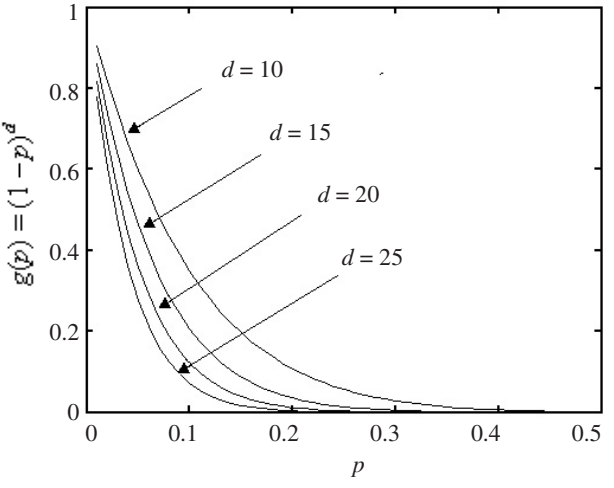

Fig. 3. Probability of receiving packets never marked

For example, if $d = 20$, and let $p = 1/d$, then $f(p) = 0.01887$, which is maximized; but $g(p) = 0.3585$, which means that a large proportion of attack packets would arrive at victim with forged mark address unchanged, and effectiveness of PPM would be significantly threatened.

In order that mark field spoofing has no essential influence, we should set $g(p) > f(p)$, which in turn requires $p > 0.5$. But this is inefficient. For example, let $d = 20$, $p = 0.51$, then $f(p) = 6.627\times10^{-7}$, $g(p) = 6.336 \times10^{-7}$, and $1 / f(p) \approx 1.5\times10^{6}$ packets are needed to get a marked packet from the furthest router.

Our scheme uses T1 packets instead of PPM packets for path reconstruction. In order to interference our scheme, attacker must deliberately spoof marking field as follows: a, use router IP (or else no corresponding T1 packet would return to V); b, router addresses or spoofed packet should comply with equation (2). These two conditions require that attackers have good knowledge about networks topology around V, which is very hard to achieve.

Accordingly, robustness of our scheme is not influenced by $g(p)$.We can set $p = 1/d$ to maximize $f(p)$, and only $1 / f(p) = 1 / 0.01887 \approx 53$ packets are needed to get a full path from the furthest router when $d = 20$.

3.6 Advantages of Our Scheme

Main advantages of our scheme include:

1. Effectiveness against DDoS with relatively large K;
2. Rapid reaction. In most cases less than tens of seconds;

3. Still valid after attack stops. Only Δt time is needed to collect enough attack packets;
4. More economy than DPM. Use DPM only for T1 packets under attack;
5. More robust than PPM, and can effectively eliminate influence of marking field spoofing;
6. No need of human interfering. All operation can be done by routers and V automatically;
7. T1 packet has little data. Added up router addresses would not excess IP packet length bound;
8. Because of *Key* (though the use of key is very simple), it's hard for attacker to spoof T1 packets. Besides, spoof T1 packet (or T2 packet) is a dangerous operation for attackers because full path is recorded.

4 Discussions

On constructing a traceback tree, V may send out a large number of T1 packets, many of which having identical destination addresses. From Assumption 2 and Algorithm 1 we can see that if the initial T1 packets are identical, the returned T1 packets are also identical. For example, in Fig. 1 V received 89 T1 packets from R_{10}, all recording the whole path from V to R_{10} and R_{10} to V. This is a waste of network resources. For example, in Fig. 1 a total of 1166 T1 packets are transferred.

We can revise Algorithm 2 (step 3) to send out only a few (more than one to ensure that one of them can fulfill the task) T1 packets per marking address, and at the same time calculate number of packets having the same marking address, in this way the traceback tree can also be successfully constructed, and bandwidth and router operation is largely saved. For example, in Fig. 1 if V sends 2 T1 packets per marking address, only $2 \times 14 = 28$ T1 packets should be transferred.

T2 packets are vital for networks behavior. In addition to DMP, stronger security mechanisms such as authentication are needed for secure transferring of T2 packets.

5 Conclusions

In this paper, we integrate DPM and PPM and get a new IP traceback scheme. Performance of our scheme is analyzed. Our scheme has advantages such as rapid reaction, robustness, and can efficiently combat DoS attacks. It can get even better performance if Assumption 4 does not hold true.

References

1. "Denial of Service Attacks", CERT Coordination Center, Oct 1997. Available at http://www.cert.org/tech_tips/ denial_of_service. html

2. K. J. Houle, G. M. Weaver, N. Long, R. Thomas, "Trends in Denial of Service Attack Technology", CERT Coordination Center, October 2001.
3. L. Garber, “Denial-of-service attacks rip the Internet,” Computer, pp. 12–17, Apr. 2000.
4. P. Ferguson and D. Senie, “Network ingress filtering: Defeating denial-of-service attacks which employ IP source address spoofing”, RFC 2827, 2000.
4. "Denial Of Service Attacks – A Survey", CERT Coordination Center, Draft. Work in progress.
5. S. Savage, D. Wetherall, A. Karlin and T. Anderson, “Practical Network Support for IP Trace-back,” Proc. 2000 ACM SIGCOMM, vol. 30, no. 4, ACM Press, New York, Aug. 2000, pp. 295–306.
6. H. Burch and B. Cheswick, “Tracing anonymous packets to their approximate source,” in Proc. 2000 USENIX LISA Conf., Dec. 2000, pp. 319–327.
7. T. Baba and S. Matsuda, “Tracing Network Attacks to Their Sources” IEEE Internet Computing March · April 2002, pp. 20–26.
8. K. Park and H. Lee, “On the Effectiveness of Probabilistic Packet Marking for IP Traceback under Denial of Service Attack” Proc. IEEE INFOCOM '01, 2001.
9. S. Bellovin, M. Leech, and T. Taylor, "ICMP Traceback Messages", Internet draft, work in progress, Jan. 2003; available online at http://www.ietf.org/internet-drafts/draft-ietf-itrace-03.txt (expires July 2003).
10. J. Postel, “Internet protocol,”, RFC 791, 1981.
11. Alex C. Snoeren, Craig Partridge, Luis A. Sanchez, et. al., “Hash-Based IP Traceback”, Proc. 2000 ACM SIGCOMM
12. D. Dean, M. Franklin, and A. Stubblefield, “An algebraic approach to IP traceback”, Network and Distributed System Security Symposium, NDSS '01
13. Minho Sung, Jun Xu , “IP Traceback-Based Intelligent Packet Filtering: A Novel Technique for Defending against Internet DDoS Attacks”, 10th IEEE International Conference on Network Protocols (ICNP'02) November 12–15, 2002