On the (in)effectiveness of Probabilistic Marking for IP Traceback under DDoS Attacks

Vamsi Paruchuri[1], Arjan Durresi[2], and Raj Jain[3]
[1]University of Central Arkansas, [2]Louisiana State University, [3]Washington University in St. Louis

***Abstract*—Distributed denial-of-service attacks (DDoS) pose an immense threat to the Internet. The most studied solution is to let routers probabilistically mark packets with partial path information during packet forwarding, which is referred as Probabilistic Packet Marking (PPM). After receiving enough number of packets, the victim would be able to reconstruct the attack graph based on the information in the packet markings.**

Because of probabilistic marking, a large fraction of the packets reach the victim unmarked by any router, thus carrying the spoofed markings set by the attacker. In this paper, we study the effect of simple attacker strategies to spoof the markings to impede victim's capacity to traceback. We show that random marking is sufficient to impede the victim from tracing the attackers. A simple enhancement based on IP path length distribution makes it harder for the victim. We also study the challenges related to the attack graph reconstruction process and collecting the attack packets for traceback. We hope that this analysis would help researchers to adapt the current PPM techniques accordingly to thwart the DDoS attacks.

I. Introduction

Distributed denial-of-service attacks (DDoS) [23, 24] pose an immense threat to the Internet, and consequently many defense mechanisms have been proposed to combat them. Attackers constantly modify their tools to bypass these security systems, and researchers in turn modify their approaches to handle new attacks. DDoS attacks are very difficult to trace because the only hint a victim has as to the source of a given packet is the source address, which can be easily forged

A number of recent studies have been carried to solve the IP traceback problem. The technique of Probabilistic Packet Marking, first proposed in [6], is a promising approach to overcome this problem. This technique uses the fact that a large number of packets are sent in such attacks. Each packet arriving at the router with PPM capability, it is probabilistically marked with the IP address. After receiving enough number of packets, the victim would be able to reconstruct the attack graph based on the information in the packet markings. Several probabilistic marking techniques have been proposed [7, 8, 9, 13, 17, 31-35].

Although, these schemes are innovative for traceback, the probabilistic nature prevents them to provide a complete solution to the problem of DDoS attacks. Along with *spoofing* the source address in the attack packets, the attacker can also *spoof* the marking field in the packets. Because of probabilistic marking, a large fraction of the *spoofed* packets reach the victim unmarked. Surprisingly, the proposed PPM schemes discount *spoofed* markings received by the victim. Two major issues ignored by the proposed schemes are:

- Differentiating between legitimate (marked) packets from spoofed packets is non-trivial and in most instances impossible.
- It is not possible for the victim to compute the number of attack packets sent by a specific compromised node in a DDoS attack.

By intelligently *spoofing* packets, the attacker can hide his identity by inserting fake edges in the attack packets [19]. For this purpose, the attacker needs topology information. However, many DDoS attacks are launched from compromised systems. Thus, it might be very hard to make the compromised nodes obtain topology information and use to it intelligently *spoof* the packets.

In this paper, we study how an attacker could efficiently spoof the packets so as to mislead the victim and hence hide his identity, even without the knowledge of network topology. We initially focus on a simple method, in which the attacker sets the packet marking field randomly but still be able to achieve his objective. We also show that by utilizing the path length distribution, the attacker is able to achieve higher anonymity.

We also study the reconstruction process and the number of packets needed to reconstruct in realistic scenarios. We show that deciding how to collect the attack packets and how long the reconstruction process should be executed is a non-trivial challenge that *has not been* previously addressed.

The rest of the paper is organized as follows: We discuss several traceback schemes including PPM techniques and analysis in Section II. Section III presents network model, assumptions and some attacker strategies. In Section IV, we perform analysis of the impact of the simple attacker strategies on reconstruction procedure. Section V deals with the challenges, regarding attack graph reconstruction, which have not been addressed before. Finally, we present concluding remarks in Section VI.

II. Related Work

Researchers have proposed various schemes to address the IP traceback problem. The most obvious countermeasure against DDoS attacks certainly is ingress filtering [1], based on source address. The next step is victim pushback, where a site that believes to be under attack can send back messages installing filters at upstream routers [2, 3]. Due to the current lack of incentives for ISPs to provide such a service, the above techniques are not expected to become widely deployed anytime soon. The IETF working group proposed that each router periodically selects a packet and "append" authenticated traceback information to this packet [4], by creating a second packet tailgating the original packet.

Snoeren et al. [5] propose storing a hash of each packet along with information about where it arrived from in a memory efficient fashion. This approach needs complete (or at least very dense) deployment and the overhead on the routers is too huge. A graph coloring approach to the traceback problem employing packet marking is proposed in [16].

A. Probabilistic Marking Schemes:

The most studied traceback solution is to let routers probabilistically mark packets with partial path information during packet forwarding, first proposed in [6]. Song et al. [7] show that the approach [6] has a very high computation overhead for the victim to reconstruct the attack paths, and that the scheme is ineffective under distributed DoS attacks. Song et al. [7] improve on [6] by predetermining the network topology. This map also allows for a more efficient encoding of edges and thus resulting in fewer chunks to reconstruct paths and in greatly improving the efficiency and accuracy of the protocol.

Dean et al. [8] propose that the routers algebraically encode the path or edge information iteratively using Horner's rule. This scheme is susceptible to a GOSSIB attack [30]. Also, the number of packets required to reconstruct path is high.

FIT [9] seems to be the most efficient and scalable, requiring fewer packets to traceback and producing low false positives even in presence of thousands of attackers. FIT achieves these strong properties mainly because of the new mechanism for conveying the distance between a marking router and victim which uses only a single bit.

Several improvements have been proposed to improve the performance of PPM techniques [13, 31-35]. In [17], two probabilistic AS marking techniques were proposed. The approach has low network and router overhead since it traces the origin AS of the attack unlike the earlier schemes that try to trace the attack originating router(s). Tradeoffs in PPM schemes for IP Traceback are studied in [18].

B. *Effectiveness of Probabilistic Techniques*

In [19], the problem of spoofing is considered and a detailed analysis is performed on the effectiveness of packet marking proposed in [6]. According to [19], PPM is vulnerable to spoofing of the marking field, which can impede traceback by the victim. By choosing an appropriate attack volume and by spoofing the attack packets, the attacker can insert uncertainty in the traceback procedure. It is shown that, by choosing an optimal value of marking probability, the uncertainty factor can be limited to 1~2, provided the number of packets is lager. It is also shown that the performance is deteriorates significantly even in small cases of DDoS. Effectiveness of Advanced Marking Scheme [7] is studied in [21]. Similar work [20] extends the above analysis and show that Adjusted Probabilistic Packet Marking [13] is also susceptible to similar attacks. In fact, all probabilistic marking schemes suffer from spoofing since more than 50% of packets arrive unmarked at victim.

The studies [19, 20, 21] deal with sophisticated attacks wherein the attacker uses the topology information to deceive the victim to traceback to some other node(s). On the other hand, we show that simple attacks that do not even need network topology are sufficient to deceive the victim.

III. Probabilistic Packet Marking and Spoofing

In this Section, we initially present the network model and notation we use in this paper. We then state the assumptions regarding the attackers and the victim. Finally, we present different simple spoofing strategies that could be executed by the attacker to impede victim's ability to traceback.

A. *Network Model and Notation*

The network is given as a directed graph $G = (V, E)$ where V is the set of nodes and E is the set of edges. Let $S \subset V$ denote the set of *attackers* and let $v \in V \setminus S$ denote the *victim*. We use G_A and G_R to represent the actual attack graph and reconstructed attack graph, respectively. Thus, G_A is a tree rooted at the victim and the attackers being the leaves. Let S_A and S_R represent the set of routers that belong to G_A and G_R, respectively i.e., $S_A = \{R_A / R_A \in G_A\}, S_R = \{R_R / R_R \in G_R\}$

G	The Internet represented as a directed graph with V and E being set of nodes and edges
G_A	The actual attack graph
G_R	The reconstructed attack graph by the victim through the underlying PPM mechanism
N	Number of attackers in the DDoS attack
Pkt	Number of packets victim needs to receive from an attacker to reconstruct the attack path to the attacker
k	Number of fragments router/edge information is encoded into
b_{frag}	Size of each fragment in bits; $b_{frag} = 15 – \log_2 k$
n_{path}	Number of unique fragments needed for single IP address path reconstruction
M	The number of values a fragment could take; $M=2^{bfrag}$
p	Marking Probability; $p = 0.04$
r_d	Number of routers at hop distance d from victim v in the graph G
r_{da}	Number of routers at hop distance d from victim v in the attack graph G_A
p_{legit}	Probability that a packet received by the victim is marked by at least one router and thus carries *legitimate* marking
p_{spoof}	Probability that a packet received by the victim is not marked by any router and thus carries *spoofed* marking; p_{spoof} = 1 - p_{legit}

Figure 1. Notation used in this paper.

The metrics used to evaluate the performance of a traceback mechanism have been: the number of false positives (FP) and that of false negatives (FN). A router is said to be a false negative if it belongs to the attack graph but not to the reconstructed attack graph. Thus, $FN = |S_A - S_R|$. A router is said to be a false positive if it belongs to the reconstructed attack graph but not to the actual attack graph, i.e., $FP = |S_R - S_A|$. Figure 1 shows the notation we use in this paper.

B. *Assumptions*

Apart from the assumptions made by previous works, we make following additional assumptions that we believe are realistic:

- An attacker can *spoof* a packet however he or she wants to.
- The packet rates at the attackers do not need to be equal. This is either due to differing link speeds of the compromised hosts or due to deliberate choices by the attackers.
- Victim cannot differentiate between a *legitimate* router marking and *spoofed* attacker marking.
- Victim cannot determine if two spoofed packets originated from same attack source or different attack sources.

C. *Probabilistic Marking*

Each packet is assumed to have a *marking field* where identity of a link $(v, v') \in E$ traversed by the packet can be inscribed. Traditionally, the *marking field* is allocated 16 bits of IP header space. For details and related issues, we refer the reader to Savage's work [6]. Optimal value for the marking probability is shown to be $1/d$, where d is the length of the path [6, 7]. Since, most of the IP path lengths are less than 25 hops, the marking probability is set to 1/25. If a packet was already marked by a previous router, a new mark will replace/overwrite the old one.

The evaluation presented in this paper applies to all probabilistic marking techniques. Nevertheless, for illustration purpose, we assume a FIT [9] like mechanism mainly due to the following reason: FIT proposes a novel method that uses only 1-bit and the TTL field to compute the distance to the marking router. Thus, among all schemes, FIT allocates a maximum of 15-bits for encoding path information. This in turn results in lower false positives and faster reconstruction.

To reduce the number of false positives, authors in [7, 9] propose to split (encode) link (IP) information into multiple fragments. Then, the packets are probabilistically marked each time with one of these fragments and the corresponding fragment number. Let k be the total number of fragments the information is split into and the fragment size be b_{frag}. For reconstruction, the victim needs to receive at least n_{path} distinct fragments from a router.

D. Spoofing the Marking field

Because of the probabilistic nature of marking techniques, some packets might arrive at the victim without being marked by the intermediate routers. Therefore, the attacker could intelligently *spoof* the marking field hoping that it would reach the victim without being overwritten and impede victim's ability to identify true attack path. In this section, we present several strategies that an attacker could adapt to *spoof* the marking field:

1) *Simple Spoofing (SS):* In this scenario, the attacker sets the marking field to same value. Thus, the marked packets can be discerned from the spoofed packets. One example where this occurs is when the attacker keeps sending the duplicate of same packet multiple times. The victim could then simply consider only the packets/markings that are different from this. In practice, this assumption might not be valid. Still, we consider this case to obtain the baseline comparison and moreover, this seems to be the case considered for analysis by several authors to evaluate the performance of their papers.

2) *Random Spoofing (RS):* In this scenario, the attacker generates each packet randomly. Thus, marking field is set randomly. Hence, at the victim, the marking field of each unmarked packet would be a random number, but the victim cannot differentiate it from a router marking. The network topology information is not utilized in this case. We note that random marking sets the distance field randomly between 0 and 31, because of the design of the PPM techniques.

3) *Enhanced Random Spoofing (ERS): W*hile almost all the IP paths are shorter than 32 hops, most of the paths are shorter than 20 hops [26, 27]. None of the paths are shorter than 5 hops and less than 1% are longer than 24 hops. In fact, more than 80% of IP paths have path lengths between 10 and 20; 60% of IP paths can be attributed six different path lengths. In other words, more than 80% of nodes that the victim can reach are at a distance between 10 and 20. Thus, to be more effective, the attacker could set the marking field so that it seems to have originated/marked by a router at a hop distance between 10 and 20. We note that, here the attacker only utilizes IP path length distribution but does not need network topology.

4) *Topology Aware Spoofing (TS):* In this scenario, the attacker takes a sophisticated approach and makes the best use of the Internet topology to confuse the victim to a larger extent. Several tools [26, 27] are available to easily obtain the IP topology. Previous works [19, 20, 21] show ways, by which the attacker could utilize the topology information to severely impede victim's ability to reconstruct the actual attack graph.

In this paper, we consider attacker spoofing methods that do not utilize topology information. The compromised hosts might not have the capabilities to process the huge topology datasets. Moreover, topology based techniques have been previously studied [19, 20, 21] and we focus on the impact of the other simple spoofing methods in impeding the victim's ability to traceback.

IV. Analysis of DDoS Attacks with Random Spoofing

In this section, we first estimate the number of *spoofed* packets that reach the victim. We analyze the impact of these spoofed packets on the number of false positives with different spoofing strategies. Finally, we compliment the mathematical analysis with experimental results using representative Internet topologies.

A. Number of Spoofed packets at the Victim

Let N be the total number of attackers and let P*kt* be the number of packets need to be received by the victim from any given attacker so as to reconstruct the attack path to that victim. Then, $(1\text{-}p)^h$ is the probability that a packet sent by an attacker at a hop distance h from the victim is not marked by any router, where p is the marking probability and is typically around 1/25. For instance, for h = 15, a packet is not marked with a probability over 0.542.

Thus, effectively $N{*}Pkt$ packets would have to be collected by the victim for path reconstruction. Among these, the number of packets that are not marked by any router is lower bounded by $N{*}Pkt{*}(1\text{-}p)^{25}$. This lower bound is obtained based on the assumption that most IP paths are of length less than 25 hops. Figure 2 shows the probability that a packet received by the victim is *marked* or *spoofed* as a function of the attacker's distance from the victim for p=0.04.

For illustration purposes, we consider two datasets from Skitter data [26] – *cdg-rssac* to represent datasets whose average path length is low (around 13.5 hops) and *cam* to represent datasets with higher path lengths (around 18). From the distribution, one could obtain the probability P_i that an attacker is at a distance i from the victim. Thus, the expected number of spoofed packets arriving at the victim can be computed by using the distribution of number of routers in various paths and can be expressed as

$$E\left[Pkt_{spoof}\right] = \sum_{i=1}^{32} P_i \left(1-p\right)^i \qquad (1)$$

For *cdg-rssac* data, E[Pkt_{spoof}] is approximately 0.583 and for *cam* data it is around 0.495 for a marking probability at each router, p=0.04. From here on, for simplicity and illustration purpose, we assume that the probability that a packet arrives with a legitimate router marking as p_{legit} = 0.5 and that the packet's marking field is spoofed with a probability p_{spoof} = 0.5. In other words, according to conservative evaluation, around 50% of the packets received by the victim are *spoofed.*

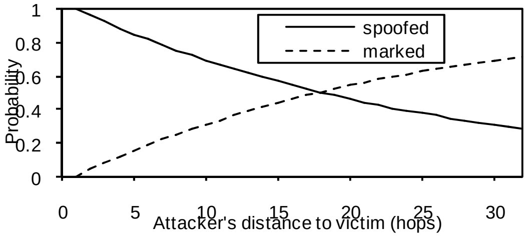


Figure 2. Probability that a packet received is *marked* or *spoofed* as a function of the attacker's distance from the victim.

B. Simple Spoofing – Performance Evaluation

In this section, we first compute the number of packets needed to reconstruct the attack graph in Simple Spoofing scenario. Then, we estimate the number of false positives. We note that in this scenario, since all spoofed markings from a given attacker are identical, the number of different spoofed markings is at most N. Moreover, the *spoofed* packets could be filtered out since they outnumber (50%) legitimate markings.

Assume r_d routers are at distance d from the victim in the graph G. Hash fragment size is b_{frag} and let r_{da} be the number of routers on the attack path at distance d from the victim in the attack graph G_A. n_{path} is the number of distinct fragments needed to reconstruct an IP address. The probability of receiving j distinct hash fragments from a set of k total fragments after receiving y randomly selected fragments is [26]

$$P_f\left[j,k,y\right]=\binom{k}{k-j}\sum_{v=0}^{k}(-1)^v\binom{j}{v}\left(1-\frac{k-j+v}{k}\right)^j \qquad (2)$$

Probability of receiving a fragment from a router at distance i hops from the victim, given marking probability p, is

$$p_m = p.(1-p)^{i-1} \qquad (3)$$

From equations (2) and (3), we could determine the number of packets needed to be received from a given path to reconstruct the path with certain probability. For FIT, it is shown in [9] that for 4/3* scheme, 400 packets would result in negligible false negative rates even in presence of 1000 attackers. For 4/4 and 8/5 schemes, the number of packets is around 700 and 800. The probability that a specific fragment of a router not on the attack matches that fragment of a router on the attack path is

$$p_{fm-ss}=1-\left(1-\frac{1}{2^{b_{frag}}}\right)^{r_{da}} \qquad (4)$$

The above equation is derived from the observation that $1/2^{b_{frag}}$ is the probability that a specific fragment of a router, r_x, not on the attack path (r_x ε G–G_A) *matches* the fragment of a router, r_a, on the attack path (r_a ε G_A). Since, at least n_{path} markings per router are required to add it to the attack path, the probability that a router will be a false positive is

$$P_{fp-ss}=\sum_{j=n_{path}}^{k}\binom{k}{j}p_{fm}{}^{j}\left(1-p_{fm}\right)^{k-j} \qquad (5)$$

The above expression is also the expected number of false positive IP addresses per router to be reconstructed. Table 1 lists some expected values for different α/β schemes in presence of multiple attackers. The 4/4 scheme is definitely more efficient resulting in very low false positives, but it requires more packets than the 4/3 scheme. Between, 4/3 and 8/5 schemes, 8/5 scheme is marginally better in small attack scenarios (<500 attackers), while 4/3 scheme is better in larger attack scenarios (>500 attackers). For evaluation purpose, we choose 4/4 and 8/5 schemes, as both require similar number of packets for reconstruction. Moreover, we would like to study the impact of fragment size on the performance – in 4/4 and 4/3 schemes b_{frag} is 13 bits, while in 8/5 scheme b_{frag} is 12 bits (as it requires 3 bits to encode fragment number compared to 2 bits for 4/3 and 4/4 schemes).

TABLE 1: EXPECTED NUMBER OF FALSE POSITIVES PER ROUTER FOR DIFFERENT α/β SCHEMES.

Number of attackers	α/β scheme		
	3/4	4/4	8/5
10	$7.3 \text{ X } 10^{-9}$	$2.21 \text{ X } 10^{-12}$	$4.8 \text{ X } 10^{-12}$
100	$7.1\text{X } 10^{-6}$	$2.17 \text{ X } 10^{-8}$	$4.3 \text{ X } 10^{-7}$
500	$7.9 \text{ X } 10^{-4}$	$1.23 \text{ X } 10^{-5}$	$8.3 \text{ X } 10^{-4}$
1000	$5.5 \text{ X } 10^{-3}$	$1.69 \text{ X } 10^{-4}$	0.01477
2000	0.034	0.0022	0.1533

C. Random Spoofing

In this scenario, the spoofed packets carry markings that were randomly generated. The reconstruction process would assume that a router at a distance d has marked the packet. Under random spoofing, d would be randomly distributed between 0 and 31. Thus, if $N*Pkt$ were collected for reconstruction process, around $N*Pkt*p_{legit}$ packets would carry actual router markings while $N_{spoof}=N*Pkt*p_{spoof}/32$ packets would appear to carry markings from a router at a given distance d ($0<d<31$).

We consider FIT like marking scheme, where 15 bits are allocated for hash fragment and the hash number. Thus, $M = 2^{15}$ markings are possible. For each $1 \le i \le M$, let x_i be the random variable such that $x_i=1$, if the i^{th} marking is carried by at least one of the $N*Pkt$ packets received by the victim. So, the total number of markings that are received at least once is $\sum_{i=1}^{M} x_i$ and our objective is to find the expected value of this.

For a given x_i, the event $x_i=1$ could result due to either of following reasons:

- At least one of the N_{spoof} packets carries i^{th} marking originating at a given distance d. The probability of this event is

$$P_{spoof}\left(x_i,N_{spoof}\right)=1-\left(1-\frac{1}{M}\right)^{N_{spoof}} \qquad (6)$$

- At least one of R_A^j routers decides to mark with i. The probability of this event is

$$P_{marked}\left(x_i,R_A^j\right)=1-\left(1-\frac{1}{M}\right)^{k*R_A^j} \qquad (7)$$

Detailed derivation of (6) and (7) is presented in [35]. Finally, the marking i is not received only if none of the spoofed packets carry i and none of the routers mark with i. Thus, the probability of the event $x_i = 1$ can be computed as

$$P\left(x_i=1\right)=1-\left[1-P_{spoof}\left(x_i,N_{spoof}\right)\right]\left[1-P_{marked}\left(x_i,R_A^j\right)\right] \qquad (8)$$

This is also the expected value of x_i. Since each x_i has the same expected value over all $1 \le i \le M$, the expected number of distinct markings that appear to originate at distance d is

$$M_d = M*P(x_i = 1) \qquad (9)$$

D. Enhanced Random Spoofing

In this scenario, the attacker utilizes the observation that more than 80% of routers are at a hop distance between 8 and 17†. Thus, the attacker marks the packets so that the victim thinks the packet has been marked by a router at a distance between 8 to 17 hops away from the victim. As we illustrate, this simple enhancement in marking significantly impedes the victim's ability to trace the attackers. Expected number of distinct markings received in this scenario could be computed similar to (8) and (9) except that

$$N_{spoof}=\begin{cases}N*Pkt*p_{spoof}/10, & if\ 8 \le d \le 17\\ 0 & else\end{cases}$$

Figure 3 presents the ratio of number of distinct markings to M received by victim in all three attacker spoofing scenarios. Simple Spoofing (SS) scenario could also be considered the case in which router markings could be distinguished from spoofed markings. We note that in the Enhanced Spoofing (ERS) scenario, the victim receives about ten times the markings in SS scenario. Thus, spoofed markings far outnumber legitimate router markings. Even with Random Spoofing (RS), the victim receives about four times the marking in SS scenario. We further note that in ERS scenario, the victim already receives about 40%

* The notation α/β scheme represents a scheme where n_{path} = β and number of hash fragments is k = α.

† The exact range depends on the graph under consideration, though most of the graphs have very similar ranges. For illustration, we use the range 8-17.

of all markings with just 200 attackers. The impact of these spoofed markings on the reconstruction procedure is evaluated in next section.

E. Spoofing and False Positives

Let M_d be the number of distinct markings received by the victim with the distance field set to *d*. The probability that a specific fragment of a router not on the attack matches that fragment of a router on the attack path can be computed similar to the SS scenario (eq. (4) and can be expressed as

$$p_{fm-rs} = 1-\left(1-\frac{1}{2^{b_{frag}}}\right)^{M_d} \tag{10}$$

Since, at least n_{path} markings per router are required to add it to the attack path, the probability that a router is a false positive is

$$P_{fp-rs} = \sum_{j=n_{path}}^{k} \binom{k}{j} p_{fm}{}^{j} \left(1-p_{fm}\right)^{k-j} \tag{11}$$

P_{fp-rs} is the expected number of false positive IP addresses per router to be reconstructed. Similar expression could be derived for ERS scenario.

Figure 4 presents the estimated number of false positives per router for all three spoofing scenarios. With 4/4 scheme (Figure 4.a), SS is very efficient with very low probability (~0.002) even in presence of 2000 attackers. But, even Random Spoofing results in around 6% probability in presence of 1000 attackers. ERS significantly increases false positives resulting in 12% and 40% false positives in presence of 500 and 1000 attackers, respectively. With 5/8 scheme (Figure 4.b), RS and ERS deteriorate the performance of PPM techniques more significantly yielding around 37% and 96% false positive probability in presence of just 500 attackers as compared to 0.8% probability with Simple Spoofing. We further note that, a DDoS attack comprising just 200 attackers results in a probability over 50% with ERS.

F. Performance analysis

We performed experimental evaluation using representative Internet topologies provided by CAIDA's Skitter map [26]. The f-root Skitter map we use has 174409 hosts. Over 83% of hosts are between 8 and 17 hops away from the f-root Skitter monitor, while around 90% of hosts are between 8 and 18 hops away.

In our experiments, a given number of attackers all send *x* packets to the victim. For each path reconstruction experiment, we assume that the victim has a complete map of the upstream router tree. Due to lack of space we provide just a summary of results. Interested readers could refer to [35] for further details.

The experimental results strongly support our previous analysis in Section IV. For the 4/4 scenario, ERS results in 251 and 18,869 false positives in presence of 100 and 500 attackers, respectively. Corresponding false positives with SS are 1 and 78. In presence of 1000 attackers, more than 36% of the routers are falsely counted as attack path routers with ERS. Even with RS, there are 1840 false positives in presence of just 500 attackers. The performance of 8/5 scheme is worse. ERS results in close to 9000 attackers with just 100 attackers. Moreover, with 500 attackers, the reconstructed attack graph consists of more than 80% of whole network. Even with RS, 500 attackers result in 37.5% of the routers to be false positives.

We also observe that increasing n_{path} hardly has any impact on the performance. The intuition behind this as follows: Higher n_{path} requires the victim to collect more packets to ensure receiving enough legitimate markings. Thus, the victim ends up receiving more *spoofed* markings, in turn resulting more false positives. Similarly, increasing the number of fragments does not improve the performance though it increases reconstruction complexity. In fact, more fragments implies smaller fragment size which significantly increases false positive rate.

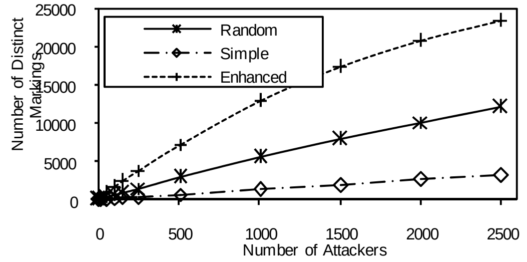
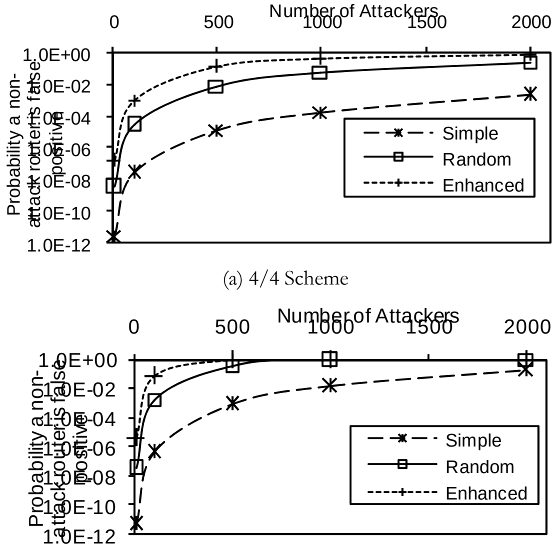


Figure 3. Number of distinct markings received by the victim. A packet marking could be a *legitimate router* marking or a *spoofed* marking; the victim cannot differentiate legitimate and spoofed markings.



(a) 4/4 Scheme

(b) 8/5 Scheme

Figure 4. Probability that a router is false positive with 4/4 and 8/5 schemes.

V. Challenges with Attack Graph Reconstruction

An important metric, to evaluate the performance of a traceback mechanism, is the number of packets to be received by the victim from a given attacker so that path reconstruction to that attacker could be possible. Let *P* be the number of packets the victim needs to receive from each attacker to ensure presence of at least n_{path} distinct marking from each router on the attack path with very high probability.

The next important question would be how to know when enough packets are received. For instance, if there is only one attacker, then it is straight forward – count number of attack packets and once the victim receives over *P* packets, the victim could reconstruct the attack path. Before extending the argument for multiple attacker scenarios, we make following observations:

- The victim cannot distinguish between marked packets from spoofed packets.
- The victim cannot identify if some two packets have arrived from same attacker or from two different attackers.

Now consider a simple scenario where there are only two attackers, A_1 and A_2. For illustration purpose, we assume *P* packets from each attacker are enough to complete path reconstruction. Here, we consider various criteria from victim's point of view to know when the reconstruction process is complete:

i. **Number of packets received from each receiver:** For this to be successful, the receiver should be able to identify whether it received *P* packets from each attacker. Since the victim cannot distinguish the attack flows, this is impractical.

ii. **Total number of packets:** It is not sufficient to end reconstruction after receiving 2**P* packets since the attackers could be transmitting at different rates. More importantly, the victim is not aware of the number of present attackers.

iii. **False negatives:** An important criterion to evaluate the performance of a traceback mechanism is the number of *false negatives*. Since the objective of traceback mechanism is to reconstruct the attack graph and the actual attack graph is not known, it would not be able to specify when to stop reconstruction.

iv. **Absence of additional attack routers:** The victim could continuously reconstruct until no new fragments are received, thus adding no further routers to the attack graph. But, even in the simple attack case where the attacker randomly generates the marking, effectively new fragments stop arriving at the victim only when all possible fragments have arrived. This only leads to the attack graph being equivalent to the IP graph!

v. **Rate of attack graph construction:** Another criterion to stop collecting packets might be to check if the number of new markings being received falls below some threshold. But, again since the attacker keeps sending randomly spoofed markings and each attacker could send at different rates, this criterion again only comes into effect only after almost all possible markings are received. This would result in the whole network to be part of attack graph!

VI. Conclusion

Several Probabilistic Packet Marking (PPM) techniques have been proposed for tracing the sources of a DDoS attack. While PPM techniques have the advantages of efficiency and implementability over deterministic packet marking and router based logging/messaging, they have potential drawbacks that attackers may impede traceback by spoofing both marking field and IP address of packets. This paper analyzes simple attacker strategies to spoof marking fields. We show that random spoofing is sufficient to mask attackers' identities. With knowledge of path length distribution, the attacker could achieve more anonymity. We also discuss challenges for reconstructing attack graph and collecting appropriate packets for that purpose. We show that, under marking field spoofing, it is non-trivial to collect packets and reconstruct attack graph. We think that the analysis presented in this paper would facilitate researches in extending/adapting PPM techniques to still efficiently traceback to the attack sources.

References

[1] P. Ferguson and D. Senie, "RFC 2827: Network Ingress filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing," May 2000.

[2] R. Mahajan, et. al, "Controlling high bandwidth aggregates in the network," Computer Communication Review, July 2002.

[3] J. Ioannidis and S. M. Bellovin, "Implementing pushback: Router based defense against DDoS attacks," in Proceedings of Network and Distributed System Security Symposium, Feb 2002.

[4] S. M. Bellovin, "ICMP Traceback Messages", Internet Draft, 2001.

[5] A. C. Snoeren, "Hash-based IP traceback," in SIGCOMM, Aug 2001.

[6] S. Savage, D. Wetherall, A. Karlin, and T. Anderson, "Practical network support for IP traceback," in Proceedings of SIGCOMM, August 2000.

[7] D. X. Song and A. Perrig, "Advanced and Authenticated Marking Schemes for IP Traceback," in Proceedings IEEE INFOCOM, 2001.

[8] D. Dean, M. Franklin, and A. Stubblefield, "An Algebraic Approach to IP Traceback," in Proc. 8th Network and Distributed System Security Symposium, 2001.

[9] A. Yaar, A. Perrig, and D. Song, "FIT: Fast Internet Traceback", in Proceedings IEEE INFOCOM, 2005.

[10] A. Yaar, A. Perrig, and D. Song. "Pi: A Path Identification Mechanism to Defend against DDoS Attacks", in IEEE Symposium on Security and Privacy, May 2003.

[11] A. Yaar, A. Perrig and D. Song, "StackPi: A new defensive mechanism against IP spoofing and DDoS attacks", IEEE JSAC, October 2006.

[12] A. Belenky and N. Ansari, "Tracing Multiple Attackers with Deterministic Packet Marking (DPM)," Proc. IEEE Pacific Rim Conf on Communications, Computers and Signal Processing 2003.

[13] T. Peng, C. Leckie, and R. Kotagiri, "Adjusted Probabilistic Packet Marking for IP Traceback", Proc. Conf. Networking, May 2002.

[14] A. Belenky and N. Ansari, "IP Traceback With Deterministic Packet Marking", IEEE Communication Letters, vol. 7, no. 4, Apr. 2003.

[15] A. Belenky and N. Ansari, "Accommodating Fragmentation in Deterministic Packet Markingfor IP Traceback", *IEEE GLOBECOM'03*

[16] M. Muthuprasanna and G. Manimaran, M. Manzor, and V. Kumar, "Coloring the Internet: IP Traceback," in Proc. IEEE ICPADS, Jul'06.

[17] V. Paruchuri, A. Durresi, R. Kannan, and S. S. Iyengar, "Authenticated Autonomous System Traceback," in IEEE Proc of AINA, 2004.

[18] M. Adler, "Tradeoffs in probabilistic packet marking for IP traceback," Proc. 34th ACM Symposium- Theory of Computing (STOC), 2002.

[19] K. Park and H. Lee, "On the Effectiveness of Probabilistic Packet Marking for IP Trace-back under Denial of Service Attack," in Proceedings of IEEE INFOCOM, 2001.

[20] B Rizvi and E Fernandez, "Analysis of Adjusted Probabilistic Packet Marking," In Proceedings of IEEE IP Operations and Management, '03.

[21] B Rizvi, E Fernandez, "Effectiveness of Advanced and Authenticated Packet Marking Scheme for Traceback of Denial of Service Attacks", in ITCC'04, Volume 2, April 2004.

[22] A Hussain, J Heidemann, and C Papadopoulos. A Framework for Classifying Denial of Service Attacks. In ACM SIGCOMM, Aug, 2003.

[23] J. Mirkovic, J. Martin, and P. Reiher, "A Taxonomy of DDoS Attacks and DDoS Defense Mechanisms," ACM SIGCOMM Computer Comm. Rev., vol. 34, no. 2, 2004, pp. 39–53.

[24] L Feinstein et al., "Statistical Approaches to DDoS Attack Detection and Response," Proc. DARPA Information Survivability Conf. and Exposition, vol. 1, 2003, IEEE CS Press, pp. 303–314.

[25] M. Walfish, M. Vutukuru, H. Balakrishnan, D. Karger, and S. Shenker, "DDoS Defense by Offense", in Proceedings of ACM SIGCOMM, September 2006.

[26] W. Feller, An Introduction to Probability Theory and Its Applications, Vol. 2, 1st ed. New York: Wiley, 1966.

[27] Skitter, CAIDA tools, www.caida.org/tools/measurement/skitter/.

[28] "University of Oregon Route Views Project," http://www.routeviews.org/.

[29] T. Peng, C. Leckie, and K. Ramamohanarao, "Adjusted probabilistic packet marking for IP traceback," in NETWORKING '02: Proceedings of the Second International IFIP-TC6 Networking Conference, 2002.

[30] M. Waldvogel, "Gossib vs. IP traceback rumors," in Proceedings of 18th Annual Computer Security Applications Conference, Dec'2002.

[31] B. Duwairi, A. Chakrabarti, and G. Manimaran, "An Efficient Packet Marking Scheme for IP Traceback", in Proc. of Networking 2004.

[32] M. Muthuprasanna and G. Manimaran, "Space-Time encoding scheme for DDoS attack traceback," in Proc. IEEE Globecom, Nov. 2005.

[33] D. Basheer and G. Manimaran, A novel packet marking scheme for IP traceback," in Proc. 10th IEEE ICPDS, July 2004.

[34] Q Dong, S Banerjee, M Adler, K Hirata,, "Efficient probabilistic packet marking", 13th IEEE ICNP, Nov 2005.

[35] V. Paruchuri and A. Durresi, "Study of Probabilistic Marking for IP Traceback under DDoS Attacks," CIS-LSU Technical Report, 2007, http://www.csc.lsu.edu/~durresi/reports/ppm-study07.pdf