Available online at www.sciencedirect.com

ScienceDirect

Computer Networks 51 (2007) 732–750

Computer Networks

www.elsevier.com/locate/comnet

A practical and robust inter-domain marking scheme for IP traceback

Zhiqiang Gao, Nirwan Ansari *

Advanced Networking Laboratory, Department of Electrical and Computer Engineering, New Jersey Institute of Technology, Newark, NJ 07102, United States

Received 5 May 2005; received in revised form 29 March 2006; accepted 1 June 2006
Available online 5 July 2006

Responsible Editor: P. Van Mieghem

Abstract

A practical and robust inter-domain marking scheme for IP traceback is proposed. We first identify six drawbacks of Probabilistic Packet Marking (*PPM*), and then contrive a synergic scheme to address all of them. To relieve the victim from the daunting computational overhead, we derive the optimal marking probability with respect to the number of packets required for path reconstruction, and explore two different approaches to enhance PPM. In so doing, computational burden and spoofed marking inscribed by the attacker are thwarted. Next, we study the issue of bogus marking incurred by subverted routers. By coupling the marking and routing information, a downstream router can examine the correctness of the marking provided by upstream routers, thus eliminating the spurious marking embedded by subverted routers. Our coarse-grained marking tactic (marking at the AS level rather than hop-by-hop) brings two additional benefits: our scheme can effectively suppress false positives, and partial deployment of our scheme may achieve the similar effect as global deployment in the power-law Internet. Finally, we evaluate and analyze the performance of our proposal on empirical Internet measurement data. Results show that as many as 90.67% of marked packets required for path reconstruction may be reduced on average while false positives are greatly suppressed and robustness is significantly enhanced.

Keywords: Distributed denial of service (DDoS); Probabilistic packet marking (PPM); IP traceback; Network security

1. Introduction

The ubiquitous Internet significantly alters our way of living. Daily activities (e.g., online-banking, stock trading and teleconferencing) increasingly rely on the performance of the Internet. Military communications and financial transactions in the Internet render security a big concern. Broadly speaking, confidentiality, integrity, and availability are the three aspects of network security. A recent study shows that most previous works on network security focus on confidentiality, some on integrity, and few on availability [1].

The advent of the lethal Denial of Service (*DoS*) attack and its advanced variant, the Distributed DoS (*DDoS*) attack quickly changes the landscape.

[*] Corresponding author. Tel./fax: +1 973 596 3670.
E-mail addresses: zg4@njit.edu (Z. Gao), Nirwan.Ansari@njit.edu (N. Ansari).

1389-1286/$ - see front matter © 2006 Elsevier B.V. All rights reserved.
doi:10.1016/j.comnet.2006.06.003

The detrimental impact of DoS/DDoS attacks has been demonstrated again and again. Even high-profiled sites can be easily overwhelmed by the attacks. A tip-of-the-iceberg victim list includes Yahoo, CNN, Ebay, Amazon (in February 2000), Domain Name Service (DNS) root servers (in October 2002), and SCO (in December 2003). Previous research on tackling DoS/DDoS may be categorized into four groups, i.e., intrusion prevention, intrusion detection, intrusion mitigation, and intrusion response [2,3]. This paper focuses on IP traceback, which belongs to the fourth group.

IP traceback is to trace attack flows from the target (called the victim) back to disparate sources. To devise a sound scheme for IP traceback is a big challenge for several reasons. First, to elude possible penalties and achieve better attack effects, the attacker assaults the victim from hundreds of zombies (subverted hosts) rather than from his/her own machine. Second, attack traffic from many zombies will aggregate at the victim. Therefore, it is very hard, if not impossible, for the victim to distinguish the malicious traffic from the normal one. There are a variety of DoS/DDoS attacks [2–4]. From the perspective of protocols used, most attacks are based on TCP (e.g., SYN Flood, RST Flood, PUSH+ ACK, and mstream), some on UDP (e.g., Trinoo and Fraggle), and few on ICMP (e.g., Smurf). Furthermore, some attacks are comprised of combinations of TCP, UDP and ICMP traffic (e.g., TFN, Stacheldraht, and Shaft). In terms of the attack rate, a vast majority of attacks are flood-based, some attacks may adjust their rates according to the response of the target systems, and a new and more sophisticated attack is low-rated [5]. Third, to deter the effort of tracing, attack packets routinely carry phony source IP addresses.

In this paper, we propose a novel marking scheme for IP traceback at the Autonomous System (AS) level, referred to as AS-based Edge Marking (*ASEM*). Legacy IP traceback schemes use IP address information of each router to reconstruct the attack paths, hop-by-hop [6–9]. Yaar et al. [10] first introduced the concept of path identification and they presented a new scheme, Pi. In their point of view, a path identifier does not have to be the IP address information. Using this idea, we here advocate a coarse-grained path identification at the AS level. Similar to the conventional Probabilistic Packet Marking (PPM) [6], routers along the attack paths mark packets according to a certain probability. The differences between ASEM and PPM are listed below. (1) Only the ingress edge routers of each AS conduct marking. (2) All routers are prohibited from re-marking packets already marked by any upstream router. (3) The marking information is the AS number (*ASN*) rather than the IP address of each traversed router.

Our contributions are sixfold. First, ASEM greatly relieves the victim from the overwhelming computational burden. We define a metric—the number of marked packets required for path reconstruction–to evaluate disparate traceback schemes. Using this metric as the guideline, we explore two different approaches to mitigate the computational overhead. Second, these improvements not only reduce the number of packets needed for reconstruction, but also completely eradicate the threat of spoofed marking inscribed by the attacker. Third, ASEM can address spoofed marking incurred by subverted routers by allowing ingress edge routers in downstream ASs to examine the correctness of the marking information from their adjacent ingress edge routers in upstream ASs. Fourth, false positives are effectively suppressed. Fifth, ASEM outperforms PPM in that it can handle large-scale DDoS attacks. Finally, the power-law Internet renders ASEM effective even under partial deployment [11]. With the above merits, ASEM can be deployed in practice.

The rest of this paper is structured as follows. Section 2 briefs the related work on IP traceback. Section 3 revisits and analyzes legacy PPM, whose shortcomings serve as our motivation. Section 4 outlines our design. We derive the optimal marking probability and explore two different approaches to mitigate computational burden in Section 5, and study the robust marking strategy in Section 6. Section 7 further extends the marking information to contain large-scale DDoS attacks. We present in detail our marking and verification algorithms in Section 8. Performance analysis and computational results are showed in Section 9. We finally summarize our work in Section 10.

2. Related works

Inspired by the ingenious work of Savage et al. [6], the research on IP traceback has taken off. In [6], Savage et al. presented the well-known PPM scheme. Since then, variants of PPM have been proposed [7,9,12–17]. Song et al. [7] proposed an advanced and authenticated scheme that significantly enhanced PPM. However, the assumption that the victim needs to be cognizant of the upstream router map is "big". To address this problem, an enhanced version was recently proposed by Yaar et al. [12]. Goodrich [9] proposed to use linkage information to tackle large-scale DDoS attacks. Sung and Xu [13] first proposed a mechanism that combines tracing and defending. Tseng et al. [14] proposed to use counters at routers to compensate those upstream routers whose marking information are overridden by downstream routers. Aljifri et al. [15] proposed an efficient scheme based on IP header compression. From the perspective of service providers, Wei and Ansari [16] proposed a variable probability marking method. Similar ideas can be found in [17]. An analysis of adjusted PPM is given in [18]. Adler [19] studied tradeoffs in PPM between the number of bits for marking and the number of marked packets for reconstruction. Park and Lee [20] studied the effectiveness of PPM and drew several important conclusions.

Bellovin et al. [8] proposed iTrace, which is similar to PPM. They used ICMP messages to determine the full paths from the attack sources to the victim. Mankin et al. [21] improved iTrace with "intention-driven" marking. Wang et al. [22,23] proposed a new ICMP message which may be used to address reflective DDoS attacks.

Different from PPM, Dean et al. [24] presented an interesting idea by using the algebraic approach to find the full attack path. Chen and Lee [25] further extended Dean's scheme to contain reflective DoS attacks.

All the above schemes were designed for flood-based DoS/DDoS attacks. To locate the single-packet attack, Snoeren et al. [26] proposed to employ bloom-filters to log some information of all traversed packets, but the scheme does not scale well since it is very difficult to coordinate among different administrative domains. Similar problem exists in CenterTrack, an overlay network traceback scheme [27]. Based on SPIE [26], Li et al. [28] introduced a new scheme to relieve the storage burden of routers by sampling.

Instead of the recovery of the full paths, Belenky and Ansari [29,30] proposed to only record the IP addresses of ingress edge routers. Their scheme, Deterministic Packet Marking (*DPM*), is simple and easy to implement, and has a little overhead on routers and the victim.

As secure marking is concerned, Waldvogel [31] found that forged marking information intentionally inscribed by the attacker could confuse the victim and impede tracing and reconstruction. Song and Perrig [7] proposed to use authentication to handle spurious marking. A similar idea can be found in [32]. The difference between [7] and [32] is that the latter conducts traceback at the AS level, which is similar to ASEM. The difference between [32] and ASEM include: (1) the marking mechanism, (2) the method to achieve secure marking, and (3) the effectiveness to large-scale DDoS attacks.

Other works on traceback includes [33–36]. Burch and Cheswick [33] proposed a traceback method using "link-testing". Paxson [34] first analyzed the reflector-based DDoS attacks. Evaluations of different IP traceback schemes can be found in [35,36].

3. Revisiting PPM

Among all previous works, PPM is a promising one which possesses several attractive features such as low router overhead, support of incremental deployment, and "post-mortem" tracing. Up to date, many variants of PPM have been developed [7,9,12–17]. Our work here is also based on PPM.

3.1. Basic PPM

PPM was first introduced by Burch and Cheswick [33], and cleverly developed by Savage et al. [6] later. The basic idea of PPM is simple. Suppose that one attack flow from an attack source to the victim traverses routers $R_1, R_2, \ldots, R_d$ in order (see Fig. 1 where $d = 3$). Denote p as the marking probability of each router. For router R_i $(1 \leqslant i \leqslant d)$, with respect to the victim, the probability of a packet marked by R_i is $p(1-p)^{d-i}$, which is different from p[14,20]. The reason is that subsequent routers may "re-mark" packets already marked by previous ones, thus overriding marking information of previous routers. The closer a router is to the victim, the more likely its marking survives. Therefore, the first router is the "weakest" part of the whole path [20].

To handle DDoS attacks, the edge-sampling method was proposed. The detailed marking procedure at each router is depicted in Fig. 2, in which the attack traverses routers R_1, R_2, and R_3. Each router makes the decision whether to mark the current packet or not independently. At router R_1, the upper box shows the case that R_1 marks packets, and the unmarked case is presented in the bottom

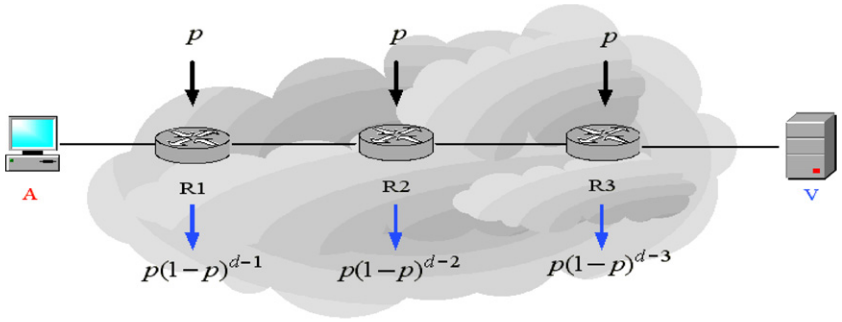

Fig. 1. Marking probability with respect to the victim, where $d = 3$.

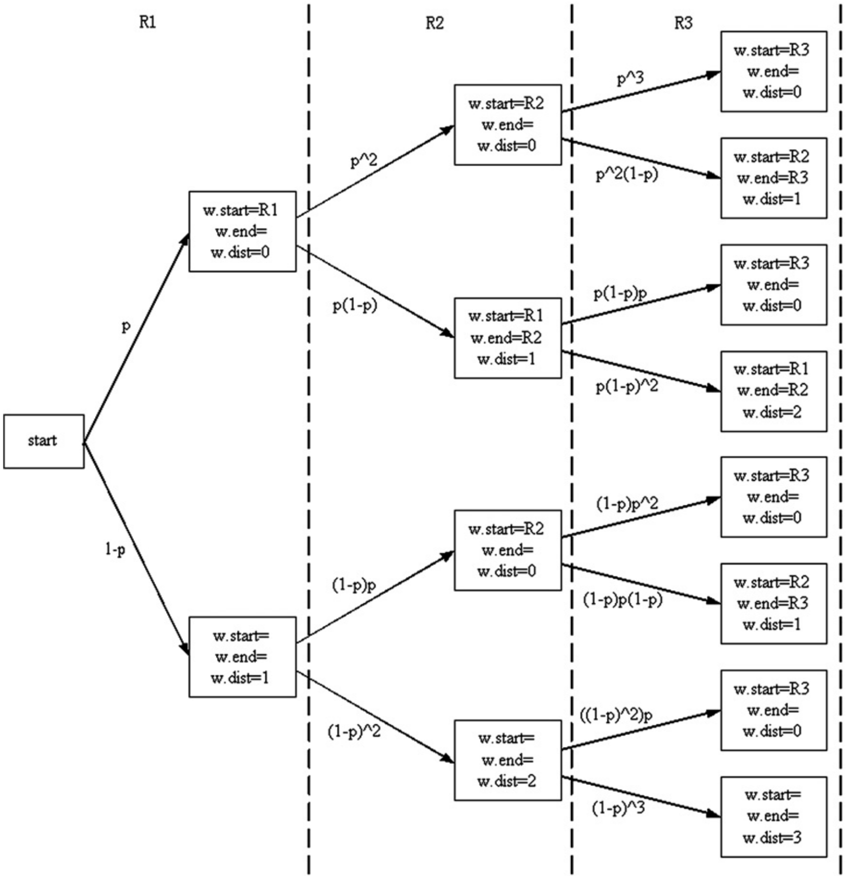

Fig. 2. PPM marking procedure, where w.start records the information of a router R which marks packet w, w.end stores the information of the downstream neighbor router of R (the other endpoint of an edge), and w.dist stands for the distance between R and the victim.

box. The probability of each case is also shown. At router R_2, four cases may arise. The upper two boxes show the scenario that packets have been marked by router R_1. Of these two boxes, the upper one stands for the scenario that router R_2 "re-marks" these packets while the bottom one does not. Similarly, the bottom two boxes represent those packets that have not been marked by router R_1. Of these two boxes, the upper box represents that packets have been marked by R_2, while the bottom one not marked by R_2. Using the similar procedure, the final result (what the victim receives) can be easily obtained. In Fig. 2, "$\wedge x$" represents that x is an exponent. Here, we do not attempt to calculate the final result of the probability for each case to clarify the marking and "re-marking" procedure. For instance, the probability of $p(1-p)p$ stands for the case that router R_1 marks the packets, and router R_2 does not while R_3 re-marks these packets. Note that though 2 cases may arise at router R_1, 4 cases at R_2, and 8 cases at R_3, the marking results may be the same. For example, the boxes 1, 3, 5, and 7 at router R_3 own the same marking information that can be combined.

After having combined the results with the same marking information, the victim will see four different marks. The victim first locates the closest router, $R_{3,}$ by looking at the packet whose dist field has a value of 0. Next, from the packets with dist = 1, it can locate R_2. To save space, a new field called addr is used instead of the start field and end field shown in Fig. 2, and its content is the result of executing the exclusive or (XOR) operation over the start and end fields. From the first step, we obtain the value of R_3; from the second step, we determine the value of $(R_2 \oplus R_3)$ [6]. Since $R_3 \oplus (R_2 \oplus R_3) = R_2$, R_2 may be located by using XOR. The procedure is repeated until the farthest router is reached.

3.2. Analysis of PPM

The above path reconstruction procedure works well if the victim is under a DoS attack (i.e., a single attack source). However, more common scenarios today are large-scale DDoS attacks where hundreds or thousands of attack sources are concerted to assault the victim synchronously. Under these cases, PPM has the following deficiencies.

1. *Heavy computational load for path reconstruction*. When there are 25 attack sources, path reconstruction will take days and thousands of false positives may be generated [7]. Currently, a DDoS attack may orchestrate thousands of zombies. As a result, the victim will never be able to complete the path reconstruction procedure. The daunting computational burden is caused by combinatorial explosion, which is originated from the insufficient number of bits for marking.
2. *High false positives*. One source of false positives is limited marking bits. The IP address is composed of 32 bits while the length of the ID field where the marking is stored is only 16 bits. Another is rooted in the reconstruction algorithm. When there exist a large number of attack paths, the victim may be confused because many routers along different paths may be at the same distance to the victim.
3. *Spoofed marking*. The attacker may inscribe spurious marking in such a way that the victim receives more packets with forged marking information than those with the correct one [20,31]. As a result, the victim will have little opportunity to discover the attack paths.
4. *Subverted routers*. Few measures have been taken to defend against malfunctioned or subverted routers. Some subverted routers may be triggered by misconfigurations, and others may be resulted from internal vulnerabilities [37]. Note that subverted routers may also generate spoofed marking. Up to now, few schemes may contain this issue.
5. *Unawareness of the path length*[1] *in advance*. When a router decides to mark a packet, it has no idea of the path length, d. Therefore, it is incapable of setting p to the optimal value $1/d$ [6]. One possible choice is to use the recommended value, e.g., 0.04 [6]. If there are many attack paths with disparate lengths, simply using a predetermined marking probability for all paths may seriously degrade the performance.
6. *Ineffectiveness to address large-scale DDoS attacks* [7,20]. Two steps are required for path reconstruction in PPM. One is the recovery of the 32-bit IP address of each router from several packets. Another is the recovery of the whole path. In PPM, 8 packets marked by the same router need to be identified and combined to resume the IP address of that router. Since there exists no hint except the distance field, it is difficult for the victim to identify which marked packets are from the same router when many routers are located at the same distance from the victim. Similarly, the victim cannot identify packets that are launched from the same attack source and traverse the same path because no clue is provided in PPM, thus seriously hampering the recovery of that path.

[1] In this paper, path length is defined as the number of routers eligible to conduct marking in between the attack sources and the victim. In PPM, all routers along an attack path can mark packets passing by, and therefore all routers along the path are eligible. In ASEM, only ingress edge routers of each AS are allowed (eligible) to perform marking and the path length in our scheme is at the AS level rather than hop-by-hop as in PPM.

3.3. Motivations

The aforementioned six problems motivate our work. We observe that Problems 1 and 2 are related. Normally, a scheme that can significantly alleviate the computational burden is very helpful to suppress false positives. These two problems may thus be handled together. We enhance PPM from two perspectives, and rigorously prove that our marking scheme is optimal. In our framework, we define a marking scheme as "optimal" if the number of packets required for path reconstruction is minimized. Note that the goal of IP traceback is to reconstruct the attack paths so that the attack sources may be located. Therefore, we believe that using the number of packets required for path reconstruction as the metric of evaluation is reasonable. To handle Problem 3, one shall ensure that all packets reaching the victim have been marked somewhere while they traverse the network. In PPM, the probability of intact (unmarked) packets is $(1-p)^d$. Given a typical value of $p = 0.04$ and $d = 25$, this probability may be as high as 36.04%. If Problem 3 is solved and thus all packets are marked, the correctness of the marking information can be guaranteed as long as there is no compromised router. To address Problem 4, we propose to embed routing information in the marking. Our idea is that if a router is aware of the expected marking information of its neighboring routers, then it may examine the correctness of the marking from its neighbors. Actually, each router does know much information of its neighbors for the purpose of routing. This is similar to route-based filtering [11]. One difference is that route-based filtering assumes that a router knows the global routing information while here a router needs only to be aware of the BGP routing information of its domain. The BGP routing protocol makes it easy for a router to be aware of the path length, and therefore Problem 5 is not an issue in ASEM. We will explain this nice feature in Section 4. Similar to [9,30], we include linkage information in marking to tackle Problem 6.

4. Overview

4.1. Background

Before proceeding to depict the whole picture of ASEM, we introduce some background.

Internet hierarchy is well known but rarely used in IP traceback. The Autonomous System is an important component of the Internet hierarchy. Normally, an AS is regulated by one entity, which can enforce a consistent routing policy inside the whole administrative domain. Among different ASs, the administrative policy may be distinct dramatically.

BGP is the de facto standard for inter-AS routing while the intra-AS routing frequently uses OSPF, IS-IS, RIP, and IGRP [38–40]. Multiple ASs depend on BGP to exchange the route reachable information, and the task is conducted by a few routers called *BGP Speakers*. There are three nice characteristics of AS. The first characteristic is that an AS path is much shorter than the corresponding IP path [41]. For instance, as shown in Fig. 3, the attack path from A1 takes 8 hops, and the one from A2 takes 7 hops to V while the AS paths are 3 "hop"s away. The second nice property of ASs is that routing at the AS level is much more stable than at the IP level [42]. Finally, one important attribute in the BGP routing message is called ASPATH, which provides the ordered list of the ASs needed to traverse before reaching a given destination. As shown in Fig. 4, suppose that the BGP speaker inside AS 12654 receives two routing information for prefix 135.207.0.0/16, one is from AS 1129 with the ASPATH attribute "1129 1755 1239 7018 6341" and another is from AS 3549 with ASPATH attribute "3549 7018 6341" [40]. Since the latter is shorter, the BGP speaker in AS 12654 may keep it in its routing table. This implies that (1) the address prefix 135.207.0.0/16 is located inside AS 6341; (2) for packets with destination address in the range of (135.207.0.0, 135.207.255.255), they will traverse to AS 7018 via AS 3549, and to AS 6341 via AS 7018 (We here assume that there is not any other prefix inside this range. That is, no prefix such as 135.207.1.0/24 exists in the same BGP routing table).

Note that the above three features can be exploited by an IP traceback scheme. The first means less "hop" counts from the source to the destination, inferring less number of marked packets required for path reconstruction. To recover an attack path, the victim *only* needs to receive several marked packets in ASEM, which significantly outperforms other PPM schemes [6,7,9,12–17,32]. The second simplifies path reconstruction because fewer possible paths are needed to be considered, and thus the victim is relieved from the problem of combinatorial explosion. The third can be used for marking verification if the ASPATH attribute is used for

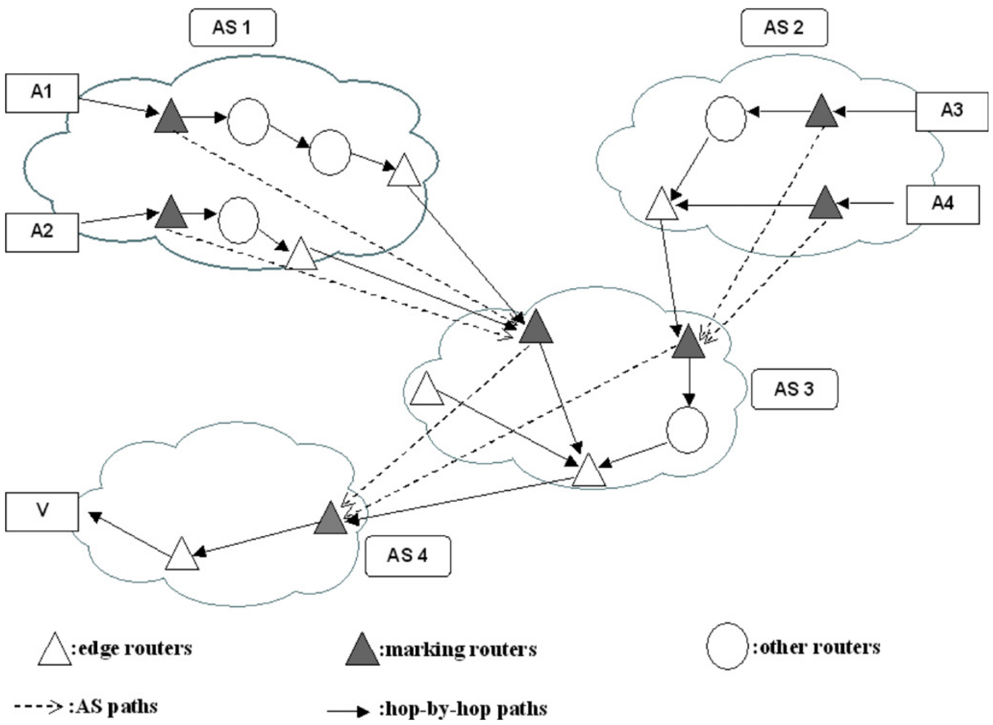

Fig. 3. AS path *vs.* hop-by-hop path.

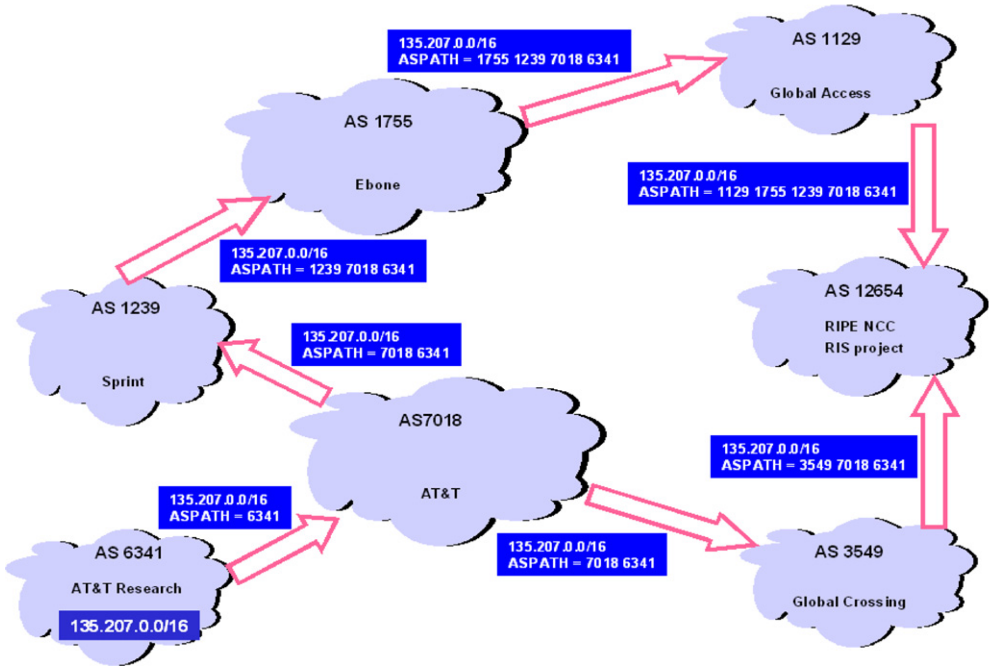

Fig. 4. Prefix originated ASPATH attribute [40].

marking. Suppose a flow of packets are bombarding at a host 135.207.x.y, the marking at AS 12654 is then “3549 7018 6341”, and the marking at AS 3549 is “7018 6341”. It is easy for AS 3549 to determine whether the marking from its upstream neighbor AS 12654 is correct or not because the only difference of these two markings is the ASN of the current AS. Since we only use 16 bits to record the ASPATH attribute, some transformation is required. Further details are provided in Section 6.2.

4.2. Assumptions

In order to outline the framework of our design, the following assumptions are made:

1. The attacker may create any packet.
2. The attacker may know the tracing scheme.
3. The attack is at least composed of tens of packets.
4. Only a few routers, if any, may be subverted. Compromised routers are not adjacent.
5. Every ingress edge router of an AS shares the BGP routing information of its domain.
6. The AS path is rather stable.
7. The length of any AS path is limited.

The first two assumptions represent the fact that the attacker may have the root privilege over the zombies, and may generate any packet he/she wants, including spoofed marking intentionally. The third one indicates that ASEM is contrived for flood-based attacks, the dominant DoS/DDoS attack pattern [2–4]. Different from previous works, we address the challenge of spoofed marking from both the attacker and compromised routers. We further assume that compromised routers are not adjacent. Considering the technical hurdle to subvert a router, our assumption is acceptable. The fifth one is critical to our design. We assume that all ingress edge routers in each AS share the BGP routing table of the BGP speaker in the same domain. This assumption requires some additional memory on each ingress edge router to store the BGP routing table. However, this requirement is not a big issue because the total number of ASs is only about 20,000 [43]. In ASEM, when an ingress edge router receives a packet, it uses the BGP routing table to conduct marking and marking examination. The last two assumptions are supported by the Internet measurement [41,42,44,45]. The dominant AS path lengths are 3–5, with an average value of 4. Our proposal assumes that an AS path length is not greater than 8, which is satisfied by about 99.5% of all AS paths [41,44,45].

4.3. Overview of our proposal

We propose that the ingress edge routers of each AS, referred to as *marking routers*, inscribe some marking information in traversed packets according to a certain probability. Note that in each AS only the marking routers conduct marking and/or marking examination, and all other routers will not. The marking information consists of four parts, 32 bits in total. The first part is 16-bit long, called AS_PATH, storing the transformed ASPATH information. We will explain in detail how to store the whole ASPATH attribute in 16 bits in Section 6.2. The second part is a flag, called FLAG, that tells the downstream marking router whether the current packet has been marked or not. The third one is comprised of 3 bits, which records the length[2] of the ASPATH attribute. The length information can be used to determine the optimal marking probability, as well as for marking verification. The fourth component is called HASHIP, a hash function of the IP address of the first marking router along a path. HASHIP is used as linkage information so that the victim can readily identify packets from the same sources and thus path reconstruction is significantly facilitated and the rate of false positives is reduced. Note that the procedure of path reconstruction has already been greatly simplified because the first step, recovering the 32-bit IP address of each router, is unnecessary in ASEM. More importantly, HASHIP can be used to distinguish disparate attack sources, making it easy to tackle large-scale DDoS that are dominant in today's Internet. Furthermore, with the help of HASHIP, the victim can block attack traffic proactively rather than depending on the response of its ISPs. This is impossible for PPM because the marking information of one router has to be segmented and transmitted in several packets.

Using routing information as marking allows the downstream marking router to examine the correctness of the marking from its upstream neighbors. If spoofed marking is found, the downstream marking router may filter or drop those packets with spoofed marking. More details can be found in Section 6.2. To handle falsified marking injected by the attacker, we enforce the policy of NO "re-marking". That is,

[2] In ASEM, we disregard padding in calculating the length of the ASPATH attribute. That is, suppose an ASPATH is "110 2 2 2 2 317" (padding AS 2), its length is still 3, same as the length of the ASPATH "110 2 317".

all subsequent marking routers cannot re-mark any packet that has been marked by any upstream marking routers. By integrating these two approaches and using the derived optimal marking probability, we minimize the number of packets required for path reconstruction and at the same time significantly enhance robustness and greatly suppress false positives.

5. Reducing the computational burden

The computational burden lies mainly on the procedure of path reconstruction. Reducing the total number of marked packets required for path reconstruction is therefore critical. We first attempt to find the optimal marking probability, then to enhance the marking mechanism, and finally to study the possibility of "reducing" the path length.

Denote k as the number of attack paths to the victim v. For path j ($1 \leqslant j \leqslant k$), the number of routers between the attack source and v is d_j. Let $p_j^i(m)$ be the marking probability of router i ($1 \leqslant i \leqslant d_j$) along path j, and $p_j^i(v)$ be the marking probability of router i along path j perceived by v. $p_j^i(v)$ may be different from $p_j^i(m)$, e.g., for PPM $p_j^i(m) = p$ and $p_j^i(v) = p(1-p)^{d_j - i}$ [14,20]. Denote N_j as the number of packets traversing along path j, and M_j^i as the number of packets marked by the ith router along path j and received by v. In other words, those packets initially marked by the ith router but are remarked by any subsequent router are not counted into M_j^i. Denote M_j as the number of packets marked by any router along path j and received by v. Clearly, the expectations of M_j^i and M_j are

$$E[M_j^i] = N_j p_j^i(v), \tag{1}$$

and

$$E[M_j] = E\left[\sum_{i=1}^{d_j} M_j^i\right] = \sum_{i=1}^{d_j} E[M_j^i] = N_j \sum_{i=1}^{d_j} p_j^i(v), \tag{2}$$

respectively.

Since PPM and ASEM mark packets probabilistically, M_j^i and M_j are random variables. Thus it is difficult to directly compare the number of marked packets under PPM and ASEM. However, we can compare their performance given the same number of attack packets and the same attack path. Two metrics that we use are : the expectation of the total number of marked packets, $E[M_j]$, and the probability that the victim receives at least one marked packet from each router, $P\{M_j^1 \geqslant 1; M_j^2 \geqslant 1; \cdots; M_j^{d_j} \geqslant 1\}$.

5.1. The number of marked packets for path reconstruction

5.1.1. The expected values of the total number of marked packets along path j

In PPM, $p_j^i(v) = p(1-p)^{d_j - i}$. From (2) we obtain

$$E[M_j] = N_j \sum_{i=1}^{d_j} p_j^i(v) = N_j(1 - (1-p)^{d_j}). \tag{3}$$

The design of ASEM ensures that all packets are marked somewhere along a path so that all spoofed markings from the attacker are overwritten. Therefore, spoofed marking from the attacker is not an issue for ASEM. Since

$$\sum_{i=1}^{d_j} p_j^i(v) = 1, \tag{4}$$

for ASEM,

$$E[M_j] = N_j \sum_{i=1}^{d_j} p_j^i(v) = N_j. \tag{5}$$

That is, given the same number of attack packets and the same path, on average, the victim can obtain more marked packets in ASEM than in PPM. Subsequently, the victim can more likely reconstruct the attack path in ASEM than in PPM.

5.1.2. Probability of receiving at least one marked packet from each router

In PPM, since each router conducts marking independently, therefore

$$P\{M_j^1 \geqslant 1; M_j^2 \geqslant 1; \cdots; M_j^{d_j} \geqslant 1\} = P\{M_j^1 \geqslant 1\} P\{M_j^2 \geqslant 1\} \cdots P\{M_j^{d_j} \geqslant 1\}. \tag{6}$$

That is,

$$P\{M_j^1 \geqslant 1; M_j^2 \geqslant 1; \cdots; M_j^{d_j} \geqslant 1\} = \prod_{i=1}^{d_j} (1 - P\{M_j^i = 0\}) = \prod_{i=1}^{d_j} (1 - [1 - p_j^i(v)]^{N_j}). \tag{7}$$

Since $p_j^1(v) < p_j^2(v) < \cdots < p_i^{d_j-1}(v)$,

$$1 - [1 - p_j^1(v)]^{N_j} < 1 - [1 - p_j^2(v)]^{N_j} < \cdots < 1 - [1 - p_j^{d_j}(v)]^{N_j}. \tag{8}$$

Combining with (7), we obtain

$$\begin{aligned} P\{M_j^1 \geqslant 1; M_j^2 \geqslant 1; \cdots; M_j^{d_j} \geqslant 1\} &< (1 - [1 - p_j^{d_j}(v)]^{N_j})^{d_j} \\ &= (1 - [1 - p]^{N_j})^{d_j}. \end{aligned} \tag{9}$$

Inequality (9) holds for any p $(0 < p < 1)$. On the other hand, the maximum value of (7) can be obtained by taking the derivative of (7) with respect to p, resulting in

$$p = \frac{1}{d_j}. \tag{10}$$

Thus, the maximum value of (7) can be reached if (10) is satisfied.

Unlike PPM, the marking probability of each router with respect to the victim is the same in ASEM, i.e.,

$$p_j^i(v) = \frac{1}{d_j}. \tag{11}$$

Following the similar derivation, for ASEM,

$$\begin{aligned} P\{M_j^1 \geqslant 1; M_j^2 \geqslant 1; \cdots; M_j^{d_j} \geqslant 1\} &= \prod_{i=1}^{d_j}(1 - [1 - p_j^i(v)]^{N_j}) \\ &= \left(1 - \left[1 - \frac{1}{d_j}\right]^{N_j}\right)^{d_j}. \end{aligned} \tag{12}$$

From Inequality (9), (10) and (12), we can draw the conclusion that given the same number of attack packets and the same path, the probability for the victim to receive at least one marked packet from each router is greater in ASEM than that in PPM.

5.2. Estimating the number of attack packets required for path reconstruction

In the last subsection, we study the number of marked packets and the probability for the victim to receive at least one marked packet from each router in ASEM and PPM, given the number of attack packets. Here, we further study the number of attack packets required for successful path reconstruction.

We assume that the path reconstruction can be completed as long as the victim receives at least one marked packet from each router. In this subsection, to simplify our analysis, when we discuss the number of marked packets, we refer to their expected values. Similar simplification can be found in most previous traceback schemes, such as [6,7,14,20].

$$\text{Given } M_j^i = N_j p_j^i(v) \geqslant 1, \quad \forall i\ (1 \leqslant i \leqslant d_j), \tag{13}$$

in PPM, since $p_j^i(v)$ is a monotonically increasing function of i (i.e., $p_j^1(v) < p_j^2(v) < \cdots < p_i^{d_j-1}(v)$), (13) can be simplified to

$$N_j \geqslant \frac{1}{p_j^1(v)}. \tag{14}$$

That is,

$$N_j \geqslant \frac{1}{p(1-p)^{d_j-1}}. \tag{15}$$

For PPM, the minimum value of N_j can be obtained by taking the derivative of (15) with respect to p, thus resulting in $p = \frac{1}{d_j}$.

In this case, N_j for PPM can be as low as

$$N_j \geqslant \frac{(d_j)^{d_j}}{(d_j - 1)^{d_j-1}}. \tag{16}$$

Unlike PPM, the marking probability with respect to the victim is the same at each router in ASEM. Combining (4) with Inequality (13), it is easy to see that N_j can reach its minimum as long as (11) holds. In this case,

$$N_j \geqslant d_j. \tag{17}$$

In fact, (11) always holds in ASEM, and therefore, ASEM always uses the optimal marking probability.

Since Inequality

$$\frac{(d_j)^{d_j}}{(d_j - 1)^{d_j-1}} > d_j \tag{18}$$

always holds, theoretically, the minimum number of attack packets required for path reconstruction in ASEM is less than that in PPM even both use the optimal marking probability.

5.3. Further discussion on the optimal marking probability

The last two subsections study the path reconstruction from the perspective of the victim v.

Now, we consider the issue from the perspective of each router along the attack path. Two questions arise naturally. (1) What would the marking probability ($p_j^i(m)$) at each router be in order to obtain the optimal $p_j^i(v)$? (2) Can the derived optimal marking probability be practically implemented at each router?

For PPM, the marking probability ($p_j^i(m)$) at each router is the same: $p_j^i(m) = p, \forall i (1 \leqslant i \leqslant d_j)$. Furthermore, if each router can know in some way the path length (d_j) ahead of time, the router can set the marking probability to the optimal value. If this is the case, the number of packets required for path reconstruction can be reduced to the value shown in (16). However, since PPM works at the IP level, no feasible method exists in the current Internet to provide the path length for each router in advance. Therefore, the derived optimal marking probability is infeasible for PPM from the practical perspective.

For ASEM, the marking probability ($p_j^i(m)$) at each router is not the same. Each router determines its marking probability according to its distance to the victim. For path j, the ith router sets its marking probability to be $p_j^i(m) = \frac{1}{(d_j - i + 1)}$, where $(d_j - i + 1)$ is the distance (path length) between the current router and v. This is feasible because the ASPATH attribute provides the exact length information (more details can be found in Section 6.2). For the first router, the marking probability is $1/d_j$; for the second router, the marking probability is $1/(d_j - 1)$; etc. However, since the policy of NO "re-marking" is imposed in ASEM, what the first router has marked cannot be re-marked by subsequent routers. Therefore, only $\left(1 - \frac{1}{d_j}\right) N_j$ packets (average number) are available for the second router to mark. With respect to the victim,

$$p_j^2(v) = \frac{1}{(d_j - 2) + 1} \times \left(1 - \frac{1}{d_j}\right) = \frac{1}{d_j}. \tag{19}$$

Similarly,

$$\begin{aligned} p_j^i(v) &= \frac{1}{(d_j - i) + 1} \times \left(1 - \sum_{s=1}^{i-1} p_j^s(v)\right) \\ &= \frac{1}{(d_j - i) + 1} \times \left(1 - \frac{i-1}{d_j}\right) = \frac{1}{d_j}. \end{aligned} \tag{20}$$

That is, each router in ASEM always marks packets using the optimal marking probability. Thus, the computational burden is minimized. Table 1 lists the average number of marked and intact (unmarked) packets at each router in legacy PPM and ASEM. For simplicity, we use S to stand for N_j, and p to stand for $p_j^i(v)$.

In summary, with respect to the computational burden, ASEM distinguishes from PPM in two aspects. First, the derived optimal marking probability is feasible and practically used in ASEM while it is impractical for PPM to use the optimal marking probability because of its unawareness of the whole path length. Second, even assume that all routers in PPM always use the optimal marking probability, Inequality (18) shows that ASEM still requires less number of packets for path reconstruction.

5.4. Decreasing path length

Considering (17), N_j in ASEM may be further reduced by decreasing the value of d_j. Suppose that only d'_j of d_j ($d'_j < d_j$) routers are used to recover the attack path. The smaller d'_j, the smaller N_j

$$N_j \geqslant d'_j, \quad d'_j < d_j. \tag{21}$$

We use the AS path, which is much shorter, instead of the hop-by-hop IP path. Since only marking routers along a path conduct marking, this is equivalent to a shorter path length with respect to path reconstruction. Note that the most important information for IP traceback is the information of the first router along a path. Though ASEM is

Table 1
Marking procedure at each marking router for PPM and ASEM

Schemes	Classifications	After the first router	After the second router	…	After the last router
PPM	# of marked packets	Sp	$S(2p - p^2)$	…	$S(1 - (1 - p)^d)$
	# of intact packets	$S(1 - p)$	$S(1 - p)^2$	…	$S(1 - p)^d$
	# of packets can still be marked	S	S	…	S
ASEM	# of marked packets	Sp	$2Sp$	…	S
	# of intact packets	$S(1 - p)$	$S(1 - 2p)$	…	0
	# of packets can still be marked	$S(1 - p)$	$S(1 - 2p)$	…	0

based on the AS level, it also records the information of the first router along a path, and therefore ASEM can trace attack sources efficiently.

6. Robust marking

A good marking scheme shall balance between efficiency and robustness. Section 5 investigates the issue of optimal marking. Here, we address the issue of bogus marking from the attacker and/or subverted routers.

6.1. Spoofed marking embedded by the attacker

The attacker may effectively deter tracing by inscribing forged marking [20,31]. In traditional PPM [6], with respect to v, the possibility that packets marked by the farthest router is $p(1-p)^{d_j-1}$ along path j. Let q_j be the probability that a packet has never been marked by any router along path j

$$q_j = (1-p)^{d_j}. \qquad (22)$$

Clearly, if $p < 0.5$, $q_j > p_j^1(v) = p(1-p)^{d_j-1}$. That is, the attacker may confuse v by filling bogus information on the unmarked packets so that v cannot locate the farthest router of each path. Even worse, the negative impact of spoofed marking is not limited to the farthest routers, i.e., the routers closest to the attack sources. For the average path length of 15, the optimal marking probability is $p = 0.0667$. Thus, $q_j = 0.3553$. Note that even for the closest router to v, $p_j^{15}(v) = 0.0667 < q_j$, letting alone any other farther routers (recall that $p_j^i(v)$ is a monotonically increasing function of i in PPM). This example shows how easy it is to disguise the victim v if the attacker embeds bogus marking information in PPM. However, with our NO "re-marking" strategy and the derived optimal marking probability $p = 1/((d_j - i) + 1)$, this is not an issue any longer in ASEM because q_j becomes 0.

6.2. Spoofed marking caused by subverted routers

Another source of bogus marking is the subverted routers. Up to now, few works explored this problem. Refs. [7,32] proposed to use authentication to ensure secure marking; here we attempt to tackle this problem by a simpler method.

The feature of BGP routing allows a downstream marking router R_b of AS_b to examine the correctness of the marking embedded by its adjacent upstream marking router R_a of AS_a because the ASPATH attribute of R_a shall be the concatenation of the ASN of R_b and the ASPATH attribute of R_b [38,40]. Note that here AS_b is a neighbor of AS_a. If a mismatch is found, the downstream marking routers can filter or drop those packets with spoofed marking. For example, assume that a path from the source *src* to the destination *dst* traverses AS_a, AS_b, AS_c, AS_d, AS_e at the AS level. The ASPATH attributes for each AS mentioned above to *dst* are "$AS_bAS_cAS_dAS_e$", "$AS_cAS_dAS_e$", "AS_dAS_e", "AS_e", "•", respectively. We use "•" to denote the last AS because the destination *dst* is inside AS_e and then only IGP routing protocol rather than EGP routing protocol (such as BGP) is used. Note that $ASPATH(AS_a) = \boldsymbol{Concatenate}(AS_b, ASPATH(AS_b))$. Subsequently, if the ASPATH attribute is used as the marking information at each AS, the marking router at AS_b can then check the correctness of the marking information from the marking router of its upstream neighbor AS_a. Since only 16 bits are used to store the ASPATH attribute in our scheme, we use XOR operation to the ASN of the current AS and all of the ASN in the ASPATH attribute and record the final result in AS_PATH. At AS_a, the marking information for *dst* is $AS_a \oplus AS_b \oplus AS_c \oplus AS_d \oplus AS_e$, where $\oplus$ is the exclusive or operator; at AS_b, the marking information for *dst* is $AS_b \oplus AS_c \oplus AS_d \oplus AS_e$. We then have $\text{AS\_PATH}(AS_a) = AS_a \oplus \text{AS\_PATH}(AS_b)$. This relationship holds for all neighbors.

7. Effectiveness to large-scale DDoS attacks

PPM is ineffective to large-scale DDoS attacks [7,20]. This is originated from the insufficient number of bits for marking in the IP header. As mentioned earlier, two steps are required for path reconstruction in PPM. One is the recovery of the complete IP address of each router, and another is the recovery of each full path. The performance of the first step may be seriously degraded because many routers may have the same distances to the victim and there exists no hint for packets from the same router to combine into a complete IP address. Similarly, no clue for packets from the same sources is presented for the victim to reconstruct a path effectively.

Goodrich [9] presented the idea of using "linkage" information to identify packets from the same router, and the same method can be found in [30]. We employ this idea in ASEM. Note that *only* one step is required for path reconstruction in ASEM, and that *only* packets with the same linkage may be combined into a full path.

We propose to use the next 16 bits of the ID field (3-bit Fragment Flag field+13-bit Fragment Offset field) in the IP header to store the linkage information. These two fields were originally designed to handle fragmented traffic that is very rare in today's Internet (about 0.25% of all traffic) [6]. To ensure the success of reassembling at the destination, all fragments must bear the same ID. We argue that keeping the Fragment Flags and Fragment Offset fields unchanged is meaningless when the ID field has been used for marking in IP traceback. As mentioned earlier, the "No re-marking" flag occupies the 1st bit of the Fragment Flag field, which is the reserved bit with the default value of 0. The next 3 bits is used to record the length of the AS path. We propose to use a hash function to map the 32-bit IP address of the first router to 12-bit hash value, called HASHIP. Using this field as the guide, ASEM is very effective in determining the packets from the same sources. In so doing, ASEM may tackle large-scale DDoS attacks that are dominant today.

The following are the merits of using the HASHIP field:

1. Using HASHIP as the guide, the path reconstruction procedure is significantly simplified because blind combinations of nodes to form a path is effectively avoided.
2. The HASHIP field alone may be used as the identifier for the victim to block attack traffic, which is infeasible for PPM (and most other schemes) because the marking information of a router in PPM is segmented and transmitted in several packets.
3. With the help of HASHIP and AS_PATH, ASEM may be used to tackle large-scale DDoS attacks. AS_PATH may be used to differentiate attack flows traversing different ASs; HASHIP is used to distinguish attack flows launched from different sources at the same AS, thus facilitating ASEM to address large-scale DDoS attacks.
4. After determining the AS path that the attack packets have traversed, the system administrator of the first AS along the attack path can identify the ingress edge router from which attack packets emitted as long as the number of the ingress edge routers in the AS is less than 4096 ($2 \wedge 12$, we here suppose that an ideal hash function is used). For PPM, even the victim can reconstruct the IP address of the ingress edge router along a path, it still requires the system administrator of the corresponding AS to take action because the victim is not entitled to manage that router. Therefore, telling the corresponding system administrator the full IP address of the ingress edge router or HASHIP is equivalent because the system administrator can keep a lookup table to determine the IP address from the HASHIP value.

8. Marking algorithms

Our marking and path reconstruction algorithm is very similar to that of PPM. One difference is that the linkage information in ASEM avoids blind combination in the recovery of each attack path, thus making path reconstruction fast and efficient. Here, we present the marking algorithm only because our marking algorithm performs an additional job, marking verification.

The marking algorithms are further divided into the one for the first marking router (shown in Fig. 5), and another for other marking routers (shown in Fig. 6). If a marking router receives a packet from the same AS, it is the first marking router. On the contrary, if a marking router gets packets from other AS, it is not the first marking router. For the first marking router, it is important to check the value of the FLAG field because a sophisticated attacker may pre-set this field to 1 to block any further marking. For all other marking router, they need to check the AS_PATH field to address forged marking.

9. Performance analysis

9.1. Computational burden

We compare the computational burden of ASEM with that of PPM from two aspects, with and without considering practical path length distribution.

9.1.1. Performance comparison under different path lengths without considering real path length distribution

In PPM, routers are not cognizant of each path length ahead of time. To simplify our analysis, we assume that PPM will use the recommended marking probability, 0.04 [6]. We first present the effectiveness of each single improvement that we propose, and

Marking procedure at the first ingress edge router R

```
For each packet $w$
    If $w$.FALG='1'                        //the attacker may spoof the flag intentionally
        $w$.FALG='0'
    write hash($R$) into $w$.HASHIP
    Let $dst$ be the destination IP address of $w$
    Lookup the BGP routing table of $R$ to get the ASPATH attribute, $ASPATH_R(dst)$
    $p1$=1/(len($ASPATH_R(dst)$)+1)          //the optimal marking prob. of R
    Let $x$ be a random number from [0,1)
    If $x$<$p1$                              //mark the packet
        Write ASN($R$) into $w$.AS_PATH    //initiate w.AS_PATH with the current ASN
        For each item $u$ in $ASPATH_R(dst)$
            Write XOR($w$.AS_PATH,$u$) into $w$.AS_PATH
        Write len($ASPATH_R(dst)$) into $w$.LEN
        Write '1' into $w$.FLAG
    Forward $w$
```

Fig. 5. Marking at the first edge router.

Marking and marking verification procedure at other ingress edge router S

```
For each packet $w$ from neighbor AS $T$
    Let $dst$ be the destination IP address of $w$
    Lookup the BGP routing table of $S$ to get the ASPATH attribute, $ASPATH_S(dst)$
    current_mark=ASN($S$)
    For each item $u$ in $ASPATH_S(dst)$
        current_mark=XOR(current_mark, $u$)
    len2=len($ASPATH_S(dst)$)
    $p2$=1/(len2+1)                            //the optimal marking prob. of S
    If $w$.FALG='1'                            //w has been marked
        If $w$.LEN=len2+1 and $w$.AS_PATH$\neq$XOR(ASN(T), current_mark)
                                               //spoofed marking from neighbor T
                Drop $w$
    Else
        Le  $x$ be a random number from [0,1)
        If $x$<$p2$                            //mark the packet
            Write current_mark into $w$.AS_PATH
            Write len($ASPATH_S(dst)$) into $w$.LEN
            Write '1' into $w$.FLAG
        Forward $w$
```

Fig. 6. Marking and verification algorithms at other routers.

then show the synergic effect. Note that N_j shown in Figs. 7–9 and Tables 2 and 3 is rounded up to the nearest larger integer, i.e., $\lceil N_j \rceil$.

9.1.1.1. Optimal marking probability. Our first improvement is achieved by using the optimal marking probability (shown in (11)).

The value of N_j with PPM can be obtained by substituting $p = 0.04$ into (15). For our improvement 1 (see Section 5.2), the value of N_j is computed by using (17). The result is shown in Fig. 7.

9.1.1.2. Shorter path length. Fig. 8 demonstrates the advantage of our second improvement (see Section 5.3) over PPM. Note that ASEM and PPM work at different granularity. Even for the same path, the value of path length is different for PPM and our approach because ASEM works at the AS level and only marking routers along each path are allowed to perform marking. Thus, ASEM has a "shorter" path length. According to the recent Internet measurement [41], on average the path length at the IP level is about 3 times the corresponding path length at the AS level. Hence, for simplicity, we only consider those IP paths with path length $6, 9, 12, \ldots, 30$, corresponding to path length of $2, 3, 4, \ldots, 10$ at the AS level. The simplification will be used whenever a comparison involves our improvement 2.

9.1.1.3. Putting everything together. Integrating both improvements into one scheme, the final result is

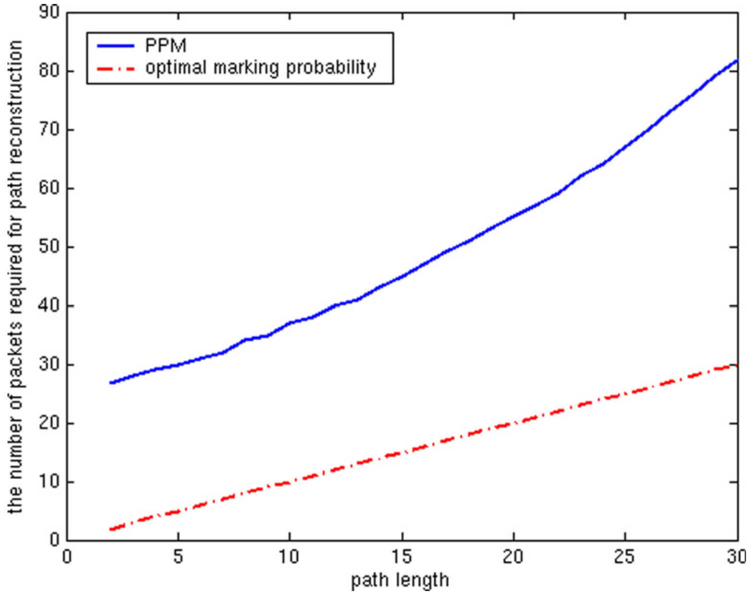

Fig. 7. N_j for PPM *vs*. our improvement 1.

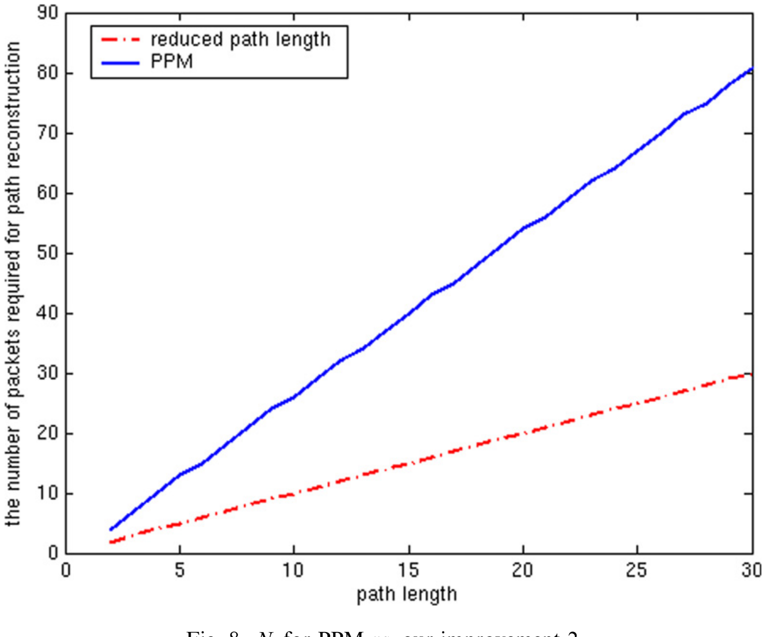

Fig. 8. N_j for PPM *vs*. our improvement 2.

shown in Fig. 9. Obviously, ASEM outperforms PPM significantly.

9.1.2. Performance comparison considering real path length distribution

In this subsection, we take the practical path length distribution into account. In so doing, we hope to provide a more accurate picture of the performance of ASEM.

We have two datasets. One is from the Skitter project of CAIDA [47], and another is the Internet Mapping data from Lumeta [46]. We simply average the number of paths from both datasets for each path length, and use the result as our dataset. Since a vast majority of IP path lengths fall in the range of $(6, 30)$ inclusively, we discard all paths whose lengths are out of this range. We choose a total of 9804 paths from the rest of our dataset. Among

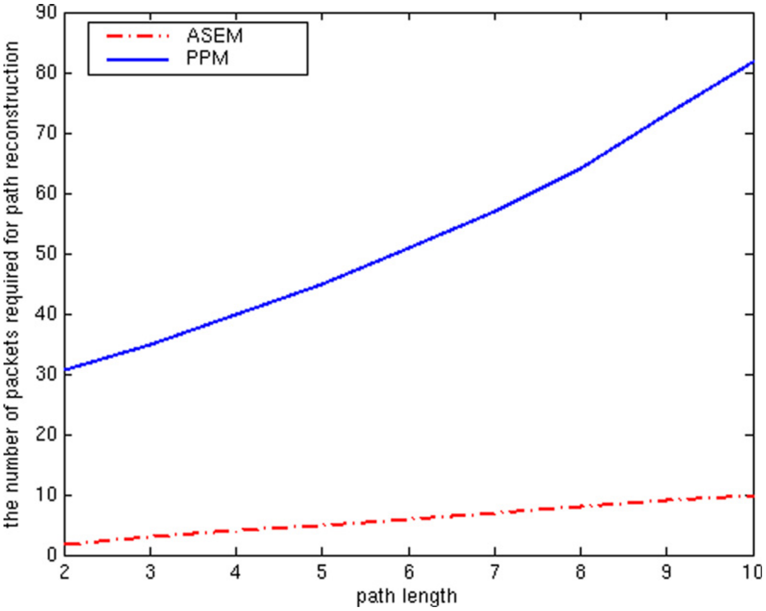

Fig. 9. N_j for PPM *vs.* ASEM (integrating 2 improvements).

the 9804 paths, 3448 paths, which have IP path lengths of $6, 9, 12, \ldots,$ or 30, will be used for comparisons involving our improvement 2.

To reconstruct all 9804 paths (denoted as set S_1), we consider two related parameters: the total number of packets required to reconstruct all paths, N; and the average number of packets required to reconstruct a path, n. Similarly, for the selected 3448 paths (denoted as set S_2), N' and n' are used to represent the total number of packets required to reconstruct all paths and a path on average, respectively.

N, N', n, and n' are computed according to (23)–(26), respectively. The results are shown in Tables 2 and 3

$$N = \sum_{j \in S_1} N_j, \tag{23}$$

$$N' = \sum_{j \in S_2} N_j, \tag{24}$$

$$n = \frac{N}{9804}, \tag{25}$$

$$n' = \frac{N'}{3448}. \tag{26}$$

Table 2
N and n under PPM, our improvement 1

	PPM	Improvement 1
Total (N)	672,996	156,687
Average (n)	68	16

Table 3
N' and n' under PPM, our improvement 2, and both improvements

	PPM	Improvement 2	Improvements 1 and 2
Total (N')	223,667	30,986	20,511
Average (n')	65	9	6

In Table 2, as explained before, we use only those IP paths whose lengths are multiples of 3 and in the range of (6, 30) inclusive. Note that our approximation does not seem to affect the result much. Considering PPM, on average, the numbers of marked packets required for reconstructing a path from 9804 paths and 3448 paths are 68 and 65, respectively. These two values are very close (the difference is only 4.41%). With ASEM, a saving of **90.67%** on average of the total number of packets required for reconstructing a path may be achieved.

9.2. Robustness

ASEM can address spoofed marking from the attacker and subverted routers.

For PPM, the possibility that a packet reaches the victim untouched (i.e., unmarked) is $(1-p)^{d_j}$ along path j. To totally confuse the victim, the following inequality shall be satisfied,

$$q_j = (1-p)^{d_j} \geqslant \sum_{1}^{d_j} p_j^i(v). \tag{27}$$

In this case,

$$p \leqslant 1 - 2^{(-1/d_j)}. \tag{28}$$

For the average path length of 15 [46,47], (28) holds if $p \leqslant 0.04516$. Therefore, using the recommended value $p = 0.04$ [6] will seriously impede reconstruction and invoke high false positives. In ASEM, on the contrary, $q_j = 0$. In other words, even all packets mounted by the attacker are inscribed with spurious marking, such bogus marking information will be totally overridden by correct marking information from routers as packets traverse along the attack path. Therefore, with this improvement, we eradicate spoofed marking from the attacker while optimizing N_j.

For subverted routers, ASEM thwarts their adverse impacts by examining the correctness of marking information. In comparison with proposals using authentication [7,32], ASEM introduces far less overhead.

9.3. False positives

9.3.1. Less marking bits

One reason for high false positives is the insufficient marking bits. In PPM, the victim has to combine packets with 8 fragments to determine a 32-bit IP address while this step is not necessary in ASEM. Furthermore, the marking information for one router in ASEM is 16-bit, only half of that required in PPM. Therefore, false positives incurred by combinatorial explosion are mitigated significantly by both factors.

9.3.2. Linkage information

The linkage information in ASEM can effectively avoid blind combinations in path reconstruction. This is very important especially in large-scale DDoS attacks, the dominant attack pattern today. The 12-bit linkage information can be used as a guide in path reconstruction.

9.3.3. Reduced path lengths

Note also the "avalanche" effect of false positives caused by routers closer to the victim. During path reconstruction, if a router R that is h hops away from the victim is added to the attack path by mistake, then this will affect locating routers $h+1$ hops away. The smaller h, the higher false positives. In general, the decrement in path length can reduce false positives exponentially, thus favoring our proposed scheme.

10. Conclusions

In this paper, we have proposed a robust and optimal marking scheme for IP traceback. First, we provide a metric for the optimization of path reconstruction. Note that path reconstruction is the fundamental goal of packet marking. Using this metric as the guideline, two improvements have been presented. By integrating both improvements, ASEM possesses the following benefits: (1) Optimal marking probability. We have derived the optimal marking probability, and presented a *practical* implementation. In comparison with legacy PPM, as many as 90.67% of marked packets can be reduced on average. (2) Robust marking. ASEM can handle not only spoofed marking by the attacker, but also the phony marking incurred by subverted routers. (3) Effectiveness to handle large-scale DDoS attacks which is dominant in today's Internet. (4) Reduced false positives. High false positives are effectively suppressed due to the above improvements. (5) Partial Deployment. The power-law Internet facilitates effective partial deployment of ASEM.

Acknowledgements

The authors would like to express their gratitude to the insight and constructive comments of the reviewers that have helped improve the quality of this paper. This work was supported in part by the New Jersey Commission on Science and Technology via the NJ Center for Wireless Networks and Internet Security.

References

[1] R. Anderson, J.H. Lee, Jikzi – a new framework for security policy, trusted publishing and electronic commerce, Computer Communications 23 (17) (2000) 1621–1626.

[2] C. Douligeris, A. Mitrokotsa, DDoS attacks and defense mechanisms: classification and state-of-the-art, Computer Networks 44 (5) (2004) 643–666.

[3] J. Mirkovic, P. Reiher, A taxonomy of DDoS attack and DDoS defense mechanisms, ACM Computer Communications Review 34 (2) (2004) 39–53.

[4] A. Hussain, J. Heidemann, C. Papadopoulos, A framework for classifying denial of service attacks, in: ACM SIGCOMM'03, 2003, pp. 99–110.

[5] A. Kuzmanovic, E. knightly, Low-rate TCP-targeted denial of service attacks the shrew vs. the mice and elephants, in: ACM SIGCOMM 2003, 2003, pp. 75–86.

[6] S. Savage, D. Wetherall, A. Karlin, T. Anderson, Network Support for IP Traceback, IEEE/ACM Transactions on Networking 9 (3) (2001) 226–237.

[7] D. Song, A. Perrig, Advanced and Authenticated Marking Schemes for IP traceback, in: IEEE INFOCOM'01, 2001, pp. 878–886.

[8] S.M. Bellovin, ICMP Traceback Messages, IETF Draft, 2000. Available from: <http://www.ietf.org/proceedings/02mar/i-d/draft-ietf-itrace-01.txt>.

[9] M. Goodrich, Efficient packet marking for large-scale IP traceback, in: 9th ACM Conference on Computer and Communications Security, 2002, pp. 117–126.

[10] A. Yaar, A. Perrig, D. Song, Pi: a path identification mechanism to defend against ddos attacks, in: IEEE Symposium on Privacy and Security, 2003, pp. 93–107.

[11] K. Park, H. Lee, On the effectiveness of route-based packet filtering for distributed DoS attack prevention in power-law Internets, in: ACM SIGCOMM 2001, 2001, pp. 15–25.

[12] A. Yaar, A. Perrig, D. Song, FIT: fast Internet traceback, in: IEEE INFOCOM 2005, 2005.

[13] M. Sung, J. Xu, IP traceback-based intelligent packet filtering: a novel technique for defending against Internet DDoS attacks, IEEE Transactions on Parallel and Distributed Systems 14 (9) (2003) 861–872.

[14] Y. Tseng, H. Chen, W. Hsieh, Probabilistic packet marking with non-preemptive compensation, IEEE Communications Letters 8 (6) (2004) 359–361.

[15] H. Aljifri, M. Smets, A. Pons, IP traceback using header compression, Computer and Security 22 (2) (2003) 136–151.

[16] D. Wei, N. Ansari, Implementing IP traceback in the Internet – an ISP perspective, in: Proceedings of 3rd Annual IEEE Workshop on Information Assurance, 2002, pp. 326–332.

[17] T. Peng, C. Leckie, R. Kotagiri, Adjusted probabilistic packet marking for IP traceback, in: Proceedings of Networking, 2002.

[18] B. Rizvi, E. Fernandez-Gaucherand, Analysis of adjusted probabilistic packet marking, in: IP Operations & Management (IPOM 2003), 2003, pp. 9–13.

[19] M. Adler, Tradeoffs in probabilistic packet marking for IP traceback, in: Annual ACM Symposium on Theory of Computing'02, 2002, pp. 407–418.

[20] K. Park, H. Lee, On the effectiveness of probabilistic packet marking for IP traceback under denial of service attack, in: IEEE INFOCOM 2001, 2001, pp. 338–347.

[21] A. Mankin, D. Massey, C. Wu, S. Wu, L. Zhang, On design and evaluation of 'intention-driven' ICMP traceback, in: Proceedings of Computer Communications and Network, 2001, pp. 159–165.

[22] B. Wang, H. Schulzrinne, Multifunctioal ICMP messages for e-commerce, in: 2004 IEEE International Conference on e-Technology, e-Commerce and e-Service, 2004, pp. 325–332.

[23] B. Wang, H. Schulzrinne, An IP traceback mechanism for reflective DoS attacks, in: 2004 Canadian Conference on Electrical and Computer Engineering, 2004, pp. 901–904.

[24] D. Dean, M. Franklin, A. Stubblefiled, An algebraic approach to IP traceback, ACM Transactions on Information System Security 5 (2) (2002) 119–137.

[25] Z. Chen, M. Lee, An IP traceback technique against denial-of-service attacks, in: 19th Annual Computer Security Applications conference (ACSAC 2003), 2003, pp. 96–105.

[26] A.C. Snoeren, C. Partridge, L. Sanchez, C. Jones, F. Tchakountio, B. Schwartz, et al., Single packet IP traceback, IEEE/ACM Transactions on Networking 10 (6) (2002) 721–734.

[27] R. Stone, CenterTrack: an IP overlay network for tracing DoS floods, in: USENIX Security Symposium, 2000, pp. 199–212.

[28] J. Li, M. Sung, J. Xu, L. Li, Large-scale IP traceback in high-speed Internet: practical techniques and theoretical foundation, in: 2004 IEEE Symposium on Security and Privacy, 2004, pp. 115–129.

[29] A. Belenky, N. Ansari, IP traceback with deterministic packet marking, IEEE Communications Letters 7 (4) (2003) 162–164.

[30] A. Belenky, N. Ansari, Tracing multiple attackers with deterministic packet marking (DPM), in: Proceedings of the 2003 IEEE Pacific Rim Conference on Communications, Computers and Signal Processing (PACRIM'03), 2003, pp. 49–52.

[31] M. Waldvogel, GOSSIB vs. IP traceback rumors, in: Computer Security Applications Conference 2002, 2002, pp. 5–13.

[32] V. Paruchuri, A. Durresi, R. Kannan, S. Lyengar, Authenticated autonomous system traceback, in: 18th International Conference on Advanced Information Networking and Applications (AINA 2004), 2004, pp. 406–413.

[33] H. Burch, B. Cheswick, Tracing anonymous packets to their approximate source, in: USENIX LISA Conference, 2000, pp. 319–327.

[34] V. Paxson, An analysis of using reflectors for distributed denial-of-service attacks, ACM Computer Communications Review 31 (3) (2001) 38–47.

[35] A. Belenky, N. Ansari, On IP traceback, IEEE Communications Magazine 41 (7) (2003) 142–153.

[36] Y. Sawai, M. Oe, K. Iida, Y. Kadobayashi, performance evaluation of inter-domain IP traceback, in: 10th International Conference on Communications (ICT 2001), 2003, pp. 583–588.

[37] CERT, Cisco IOS Interface Blocked by IPv4 Packet. Available from: <http://www.cert.org/advisories/ca-2003-15.html>.

[38] Y. Rekhter, T. Li, A Border Gateway Protocol 4, RFC 1771, 1995.

[39] L. Gao, J. Rexford, Stable Internet routing without global coordination, IEEE/ACM Transactions on Networking 9 (12) (2001) 681–692.

[40] T. Griffin, The stable paths problem as a model of BGP routing. Available from: <http://web.njit.edu/~ott/Griffin.ppt>.

[41] B. Huffaker, M. Fomenkov, D.J. Plummer, D. Moore, K. Claffy, Distance Metrics in the Internet. Available from: <http://www.caida.org/outreach/papers/2002/distance/distance.pdf>.

[42] V. Paxson, End-to-end routing behavior in the Internet, IEEE/ACM Transactions on Networking 5 (5) (1997) 601–615.

[43] G. Huston, Growth of BGP routing table (94-present). Available from: <http://bgp.potaroo.net/>.

[44] M. Fayed, P. Krapivsky, J. Byers, M. Crovella, D. Finkel, S. Redner, On the size distribution of autonomous systems, Technical Report, Boston University, 2003.

[45] National Laboratory for Applied Network Research, AS Path Length. Available from: <http://moat.nlanr.net/ASPL>.

[46] Internet Mapping Project. Available from: <http://research.lumeta.com/ches/map/>.

[47] CAIDA, Skitter. Available from: <http://www.caida.org/tools/measurement/skitter/>.

Zhiqiang Gao received the B.S. degree in Computer Science from Zhejiang University, China, and the M.S. degree from the Chinese Academy of Sciences. He is pursuing his doctorate in Computer Engineering at New Jersey Institute of Technology (NJIT), focusing on IP traceback, DoS/DDoS defense, and wireless security. He was one of the four recipients of the Spring Semester 2005 Cisco Systems Information Assurance Scholarship.

Nirwan Ansari received the B.S.E.E. degree (summa cum laude) from the New Jersey Institute of Technology (NJIT), Newark, NJ, in 1982, the M.S.E.E. degree from the University of Michigan, Ann Arbor, MI, in 1983, and the Ph.D. degree from Purdue University, West Lafayette, IN, in 1988.

He joined the Department of Electrical and Computer Engineering, NJIT, as an Assistant Professor in 1988, and has been a Full Professor since 1997. He authored *Computational Intelligence for Optimization* (Kluwer, 1997) with E.S.H. Hou and translated into Chinese in 2000, and co-edited *Neural Networks in Telecommunications* (Kluwer, 1994) with B. Yuhas. He is a Senior Technical Editor of the *IEEE Communications Magazine*, and also serves on the editorial board of *Computer Communications*, the *ETRI Journal*, and the *Journal of Computing and Information Technology*. His current research focuses on various aspects of broadband networks and multimedia communications. He has also contributed approximately 100 refereed journal articles, plus numerous conference papers and book chapters.

He initiated (as the General Chair) the First IEEE International Conference on Information Technology: Research and Education (ITRE2003), was instrumental, while serving as its Chapter Chair, in rejuvenating the North Jersey Chapter of the IEEE Communications Society which received the 1996 Chapter of the Year Award and a 2003 Chapter Achievement Award, served as Chair of the IEEE North Jersey Section and in the IEEE Region 1 Board of Governors during 2001–2002, and has been serving in various IEEE committees including as TPC Chair/Vice-chair of several conferences. He was the 1998 recipient of the NJIT Excellence Teaching Award in Graduate Instruction, and a 1999 IEEE Region 1 Award. He is frequently invited to deliver keynote addresses, tutorials, and talks. He has been selected as an IEEE Communications Society Distinguished Lecturer (2006–2007).