Efficient Probabilistic Packet Marking for AS Traceback

Abdullah Yasin Nur
Department of Computer Science
University of New Orleans
New Orleans, LA, USA 70148
Email: ayn@cs.uno.edu

***Abstract*—Distributed Denial of Service (DDoS) attacks are among the most perilous attack types in the Internet. In addition to the significant harms for the victim site, intermediate Autonomous Systems (AS) are also unintended victims in DDoS attacks. The main goal of a DDoS defense mechanism is to reduce the attack's effect as close as possible to their sources to prevent malicious traffic in the Internet. In this work, we proposed an AS traceback scheme to infer AS level forward paths from attacker sites to a victim site. We utilize the 16-bit IP ID field and 6-bit from the ToS field in the IPv4 protocol. In our method, only the ingress routers of ASes probabilistically mark the packet with their AS numbers. We propose an encoding technique to reduce the number of required packets significantly. The destination site can construct the path after receiving enough packets. Our results show that a victim site can construct the forward path from an attacker site after receiving 10.14 packets on the average. Compared to the other techniques, our approach requires fewer packets to construct the paths from attacker sites to a victim site.**

***Index Terms*—Denial of Service attack, DoS, DDoS, AS Traceback, IP Traceback**

I. Introduction

The Internet is the main communication medium, and the significant increase in online dependency for people worldwide brings additional challenges. It is designed to forward packets with minimal intervention, including malicious packets. Cyberattacks target computer systems with a purpose of disrupting or disabling services, stealing or altering data, or make unauthorized use of any assets. The economical, social, and political impacts of the cyberattacks have significantly increased. In a recent report from FBI Cyber Division [1], the number of cyberattacks that occurred in 2020 is $791,790$, whereas the numbers were $467,361$ in 2019. In the same report, the total losses in 2020 are reported as \$4.2 Billion. Additionally, Interpol reports that the rate of cyberattacks in 2020 reached an alarming rate to target major corporations, governments, and critical infrastructure [2].

Denial-of-Service (DoS) attack is one of the most harmful cyberattack types where an attacker aims to exhaust the target's system by flooding traffic until the target is inaccessible to intended users. Distributed Denial of Service (DDoS) attack is a more severe type of DoS attack where many hosts orchestrate a synchronized attack to a target. In 2020, Amazon reported a world record DDoS attack sustaining a 2.3 Tbps to their Amazon Web Services (AWS).

The current protocols in the Internet do not help a destination host to track incoming packets other than the source IP address. In packet switching network, the traditional forwarding in routers works as checking the destination IP address and forwarding the packets accordingly without worrying about the source IP address. Therefore, the source IP address can be easily forged, which is called IP spoofing. In case the victim site blocks the IP address of an attacker, it may block an incorrect host. Additionally, blocking the attack traffic at the destination is not a valid solution since the attack traffic uses the bandwidth of incoming links and creates congestion. Also, intermediate Autonomous Systems (AS) which carry the attack traffic are under attack and become unintentional victims. The ultimate goal of the DDoS defense mechanisms is to track the attacker and stop the attack as close as the attack site.

Inferring the path between an attacker and the victim site is called IP traceback. IP traceback techniques focus on the Interface level path between two hosts. One of the IP traceback variations is called AS traceback, where the victim site infers the AS level path from the attacker. Tracing AS path instead of Interface path has significant advantages, including reducing the number of required packets, fewer false positives and false negatives, and less overhead to routers. Additionally, the ASes are responsible for taking the filtering decisions within their internal network. Therefore, finding the attacker AS is adequate to stop the attacker.

Each AS in the Internet is assigned a 32-bit unique Autonomous System Number (ASN). In this work, we take advantage of these unique numbers to track the AS path between two end hosts. We utilize the 16-bit IP ID field and 6-bit Type-of-Service field in the IPv4 packet header. In our method, the border router, which is the first router that belongs to a different AS in the path, probabilistically appends its corresponding ASN into the header of a packet. After receiving enough packets, the victim site is able to infer the AS level path from attackers. Additionally, we present an encoding technique for marking the ASN to reduce the number of required packets significantly.

We conducted several experiments using a real-world dataset to demonstrate the efficiency of our approach under DoS and DDoS attacks. Our results show that a victim site can

978-0-7381-1316-6/21/$31.00 ©2021 IEEE

construct the AS level forward path from an attacker site after receiving 10.14 packets on the average. Our dataset contains a minimum of 1 and a maximum of 11 AS hop distances between two end hosts. Our experiments show that the victim can construct the path with 1 packet for AS hop distance 1 and 51.29 packets on the average for AS path 11. Next, we test our method for DDoS attack case. Our results show that the victim site successfully traces the attackers without any scalability problem.

In addition, we compared our results to other Probabilistic Packet Marking (PPM) schemes for AS Traceback: PPM fixed probability (PPM-fixed) [4] and the PPM dynamic probability (PPM-dynamic) [3]. Our results show that PPM-fixed needs 22.98 to 96.99 packets and PPM-dynamic needs between 3.53 and 63.74 packets on the average to construct AS level forward paths for varying hop distances. Our method requires 1 to 27.31 packets on the average for the same AS paths. Both methods can track a maximum of 8 AS hop distance, whereas our method can track up to 16 AS hop distance. Our maximum packet count is 51.29 for 11 AS hop length, which is still less than both methods' required packet numbers for 8 hop distance. The overall averages are 10.14, 27.26, and 46.04 for our approach, PPM-dynamic, and PPM-fixed, respectively, regardless of the hop distance.

The rest of the paper is organized as follows. In Section II, we present the related work. We explain the details of our approach in Section III. Section IV demonstrates our experimental results. Finally, we conclude the paper in Section V.

II. Related Work

Due to the severe effects of the DoS type attacks, researchers studied the problem and suggested several defense mechanisms [5]. The main focuses of the defense mechanisms can be categorized as attack detection, attack reaction, and attack source identification. Attack detection techniques analyze the incoming packets and identify attacks in case of an anomaly in the observed traffic [6]. The aim of attack reaction techniques is to mitigate the impact of attacks by applying resource management [7]. The last category is attack source identification, where the victim site aims to detect the attacker's position even if the attacker spoofs its IP address [9]. This paper falls into the last category, where we aim to detect the forward path between attackers and the victim site.

The IP protocol does not provide for the authentication of the source IP address, which creates a significant vulnerability where the adversaries can falsify the packet's origin by IP spoofing. Discovering the origin of a packet from the destination site is called IP traceback. One of the earliest works in IP traceback can be credited to Savage et al. [8]. In their influential work, they propose Fragment Marking Scheme (FMS), where routers probabilistically mark the 16-bit IP ID field of an IP packet, and the victim reconstructs the IP addresses of routers on the path using marked packets. Song and Perrig [11] discussed the computation overhead and high number of false positives of the FMS in DDoS attacks. They propose Advanced and Authenticated Marking Schemes (AMS) to reduce the number of required packets. Yaar et al. [12] improve AMS by using more space for encoding to reduce the number of required packets for constructing the forward paths. In our previous work [9], we propose RRTrace, which is a probabilistic packet marking scheme to infer forward paths from attackers to a victim by exploiting the Record Route feature of the IP protocol.

IP traceback is helpful to obtain the entire Interface Level path. However, ASes are responsible for taking the filtering decisions within their internal network. Tracing AS path instead of Interface path has significant advantages, including reducing the number of required packets, fewer false positives and false negatives, and less overhead to routers. Parachuri et al. [13] propose one of the earliest works in AS traceback. The proposed method uses the 16-bit IP-ID field to hold the ASN and 3-bit to mark the AS distance in the IP packet header. Their method tracks 16-bit ASNs, which is currently outdated by RFC 4893 that introduced 32-bit AS numbers in 2007. Alenezi and Reed [3] propose a method that utilizes 25 bits in the IP header. They adjust the packet marking probability dynamically by checking Border Gateway Protocol (BGP) table to obtain AS hop distance between the destination and the current router, which decides to write or skip rewriting the packet.

In this work, we propose AS Traceback method to infer the forwarding path between attackers and the victim site, and an encoding technique to reduce the number of packets. Different from the previous works, our technique reduces the bandwidth usage significantly, increases the maximum number of traceable ASes, and reduces the router overhead.

III. Methodology

This section demonstrates the packet marking scheme to infer the forward AS paths from attackers towards a victim site. We propose a probabilistic packet marking to infer the AS level path between attackers and the victim site. ASes in the Internet are assigned a unique AS number (ASN). Our method uses these unique ASNs to infer the forward AS level path. In the proposed technique, each AS Border Routers (ASBR) probabilistically inserts their ASN value into the packet's IP header. ASBRs are the ingress-routers of ASes, which are the first routers that receive the traffic from the previous AS. In the method, intermediate routers do not write the packet header. Instead of collecting all routers' information, receiving ASNs on the path reduces the number of required packets to infer the forward path between attackers and victim significantly.

We modify 22-bits in the IPv4 header, which are usually unused fields in the current Internet (16-bit IP-ID field, 6-bits Type-of-Service field) presented in Figure 1. We use 4-bit to track the distance of the AS that marks the packet. Our experiments show that the AS distance between two end hosts is between 1 to 12, with an average of 4.16. Therefore, 4-bit gives us enough room to track 16 AS hop length, which is adequate to track all cases in the Internet.

We use 1-bit flag for ASN encoding. ASN used to be a 16-bit unsigned integer. Due to the significant increase in the

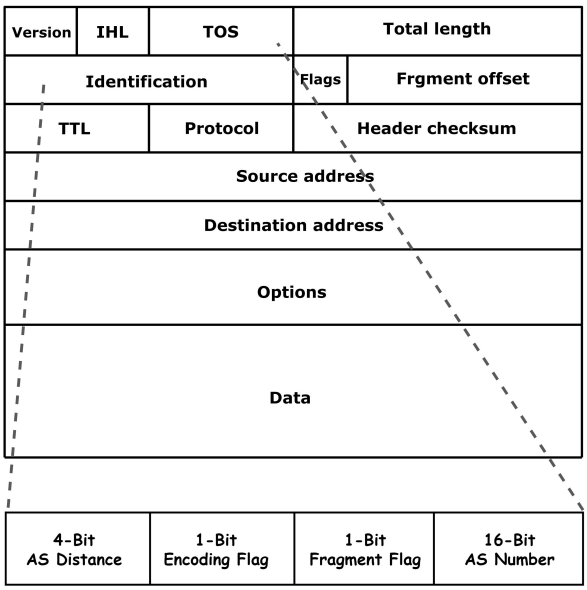

Fig. 1: Used bits in IPv4 Header

Algorithm 1 Rewrite / Skip-Rewrite Algorithm at ASBRs

Input: ASN ▷ AS Number of the current AS
1: **if** Router decides to rewrite **then**
2: **if** ASN is smaller than 65536 **then** ▷ ASN is in 16-bit range
3: set ASN encoding flag 0
4: set fragmentation flag 0
5: insert ASN into the packet header
6: **else** ▷ ASN is in 32-bit range
7: set ASN encoding flag 1
8: get ASN first or last 16-bit
9: **if** ASN first 16-bit **then**
10: set fragmentation flag 0
11: assign first ASN 16-bit into the packet header
12: **else**
13: set fragmentation flag 1
14: assign last ASN 16-bit into the packet header
15: **end if**
16: **end if**
17: **else** ▷ router decides to skip rewriting
18: do Nothing
19: **end if**
20: $ASDistance = ASDistance + 1$

Internet usage, the 32-bit version replaced the 16-bit version in 2007 [14, 15]. Right now, all ASNs are considered 32-bits [16]. In our previous work [10], we observe that 16-bit is enough to cover most of the tier-1 and tier-2 ASes' ASNs. These tier 1 and 2 ISPs are earlier ISPs that keep their 16-bit ASN by extending it by padding zeros and making the ASN 32-bit. Therefore, we use a simple encoding technique. In case an ASN can be represented by 16-bit, the encoding flag is 0; otherwise, the flag bit is set to 1 representing 32-bit ASN. Additionally, we use 1-bit fragmentation flag to represent 32-bit ASes. Since we use 16-bit to store AS Numbers in the header, we need two fragments for 32-bit ASNs. In case the flag bit is 1, the victim site needs to receive fragment 0 and fragment 1 to infer the ASN of that specific intermediate AS.

A. Packet Marking Technique

In this part, we explain our algorithms for packet marking at the intermediate border routers of ASes (ASBR). Algorithm 1 presents the encoding pseudocode executed by border routers of the ASes. The algorithm expects the ASN to be reported by the router. Line 1 checks the size of the ASN. Remember that the range of 16-bit is from 0 to $65,535$. Therefore, if an ASN is less than $65,536$, the algorithm executes line 2, which is the 16-bit ASN case. Line 3 sets the encoding flag to 0, which presents the 16-bit case. Since we do not need fragmentation, line 4 sets the flag as 0. Line 5 inserts the 16-bit ASN into the packet header. In case the ASN is greater than $65,535$, line 7 updates the encoding flag, which represents the 32-bit case. The router probabilistically decides to insert the first 16-bit or the last 16-bit of the ASN into the packet header. In case of the first 16-bit, line 10 updates the fragmentation flag as 0. On the other hand, line 13 sets the fragmentation flag as 1 in case of the last 16-bit of the ASN insertion. If ASBR decides to skip rewriting, it does not change any bits except the AS distance. No matter the ASBR rewrite or skip rewriting, it increases the AS Distance by 1.

B. Probabilistic Model

Assume that a border router of an AS (ASBR) writes the packet with a probability p and skip rewriting with a probability $(1-p)$. In the case of 16-bit ASN, ASBR writes the ASN with a probability of p directly without fragmentation. On the other hand, if the ASN is 32-bit, ASBR writes the ASN first fragment (first 16-bit) with a probability of $0.5p$ and the second fragment (last 16-bit) with $0.5p$.

EssentialPckt is defined as the packets that the victim needs to receive to rebuild the forward path correctly. Therefore, the victim site must receive all *EssentialPckt* and concatenate them in the correct order to build the forward path. Given that the AS level hop distance from the attacker to the victim site is h, where $h > 1$, the minimum total number of the required *EssentialPckts* is h where all ASNs are 16-bit (1 packet from each ASBR). On the other hand, the maximum total number of the required *EssentialPckts* is $2h$ where all ASNs are 32-bit (2 packets from each ASBR).

In case the k^{th} ASBR decides to rewrite the packet, the previous write or skip rewriting probabilities do not change the outcome since ASBR overwrites it. However, to receive k^{th} ASN, the remaining ASBRs need to skip rewriting the packet. Hence, the probability of receiving the k^{th} *EssentialPckt* (k AS level hop distance from the victim), $P\{k\}$, is

$$P\{k\} = p \times (1-p)^{h-k} \tag{1}$$

where h is the AS level hop distance between an attacker to the victim site.

C. Expected Number of Packets

In this part, we present the expected number of packets needed to construct a forward path between two hosts at

the destination. We modify the classical Coupon Collector's Problem [17], which is a "collect all coupons to win" contest. Assume that there is k different type of coupons that needed to be collected in order to win. Each coupon has the same probability of being drawn, and a person draws a new coupon each time with replacement. The Coupon Collector's Problem examines the average number of the required draws to collect each type of coupon at least once. In our problem, the victim site needs to receive at least one instance of each *EssentialPckt* from an attacker to construct the forward path. Therefore, each *EssentialPckt* corresponds to a coupon in this case.

Let h be the number of hops between a source and a destination. Then, the total number of distinct *EssentialPckt*s is $h \leq m \leq 2h$. Let $P\{k\}$ given in Equation 1 be the probability of receiving the k^{th} *EssentialPckt*. Regardless of the order of *EssentialPckts*, assume that $i-1$ *EssentialPckt*s have already been collected at least once. Then, the probability of receiving a new *EssentialPckt* that was not collected before is $p_i = [m-(i-1)] \times P\{k\}$. To put in other words, p_i is the probability of receiving the i^{th} unobserved *EssentialPckt* after observing $i-1$ *EssentialPckts* regardless of the order.

Let T_i be a random variable denoting the number of the packets to be received in order to get the i^{th} new *EssentialPckt*, given that $i-1$ *EssentialPckt*s have already been collected. The probability mass function of T_i is $P\{T_i = t\} = p_i \times (1-p_i)^{t-1}$. The expected value of $E[T_i]$ (Equation 2) gives us the average number of packets to observe a new *EssentialPckt*, given that $i-1$ *EssentialPckt*s have already been collected.

$$\begin{aligned} E[T_i] &= \sum_{t=1}^{\infty} t \times p_i \times (1-p_i)^{t-1} \\ &= p_i \times \sum_{t=1}^{\infty} t \times (1-p_i)^{t-1} \\ &= p_i \times \frac{\partial}{\partial(1-p_i)}[\sum_{t=1}^{\infty}(1-p_i)^t] \\ &= p_i \times \frac{\partial}{\partial(1-p_i)}[\frac{1-p_i}{p_i}] \\ &= p_i \times \frac{1}{p_i^2} \\ &= \frac{1}{p_i} \end{aligned} \tag{2}$$

where the final step is calculated by differentiating and integrating the right hand side of Equation 2 with respect to $1-p_i$.

Finally, $T = \sum_{i=1}^{m} T_i$ is the total number of received packets to collect all *EssentialPckt*s at least once. That is, $E[T]$ (Equation 3) is the total number of packets required to construct a complete forward path using all *EssentialPckt*s.

$$\begin{aligned} E[T] &= \sum_{i=1}^{k} E[T_i] \\ &= \sum_{i=1}^{k} \frac{1}{p_i} \end{aligned} \tag{3}$$

D. Packet Overhead

In the proposed method, we exploit an additional 22-bit (16-bit IP ID and 6-bit in ToS fields) of the IPv4 header. Assume that V is the IP traffic volume in bytes per second and L is the average IP packet length in bytes. The number of packets per second is defined in equation 4.

$$n = \frac{V}{L} \tag{4}$$

$$V' = (L + 2.75) \times n \tag{5}$$

$$TO = \frac{V' - V}{V} \tag{6}$$

$$TO = \frac{2.75}{L} \tag{7}$$

Holding n fixed, let V' be the traffic volume when we use an additional 2.75 bytes (22-bit) to construct forward paths. The new traffic volume under our scheme is presented in equation 5. It is reported that the IP packet length changes between 40 to 1500 bytes depending on the communication protocols and applications with a strong mode around 1300 bytes [18]. Assuming the packet length is 1300 bytes, our approach introduces $\approx 0.21\%$ additional traffic overhead (TO) as represented in equation 7.

IV. Experimental results

In this section, we empirically demonstrate the efficiency of our algorithm using a real-world dataset. We used the CAIDA IPv4 Prefix-Probing Traceroute Dataset [19] consisting of $20,377,233$ path traces. The minimum, maximum, and average Interface level hop lengths in our dataset are 1, 31, and 15.43, respectively. We used the RouteViews prefix to AS mapping dataset obtained from CAIDA [20]. In order to generate an AS Level Internet topology, we mapped IP addresses reported in the traceroute dataset to their corresponding ASes. The dataset consists of $39,148$ different ASes. The minimum, maximum, and average AS level hop lengths in our dataset are 1, 11, and 4.16, respectively.

Figure 2 presents the minimum and maximum average expected number of packets per AS hop distance. As we discussed in subsection III-B, in case all ASNs in the path are 16-bit, the victim site requires at least one packet from each AS on the path. On the other hand, the victim site needs at least two packets (first and last fragments) from ASes with 32-bit ASNs. Therefore, all 16-bit ASN case is the lower bound and all 32-bit ASN case is the upper bound for the expected number of packets per AS hop distance to construct the forward path.

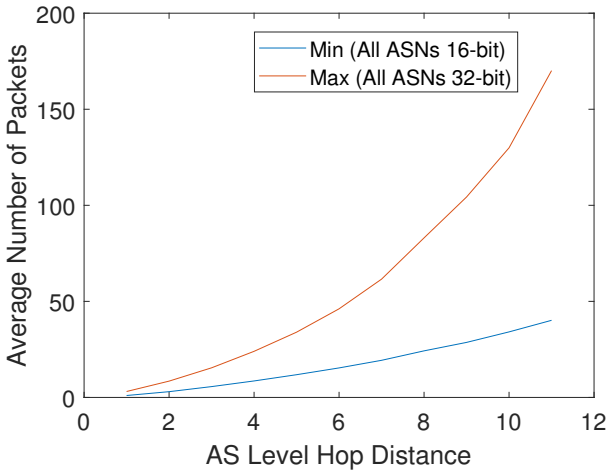

Fig. 2: Min and Max Expected Number of Packets

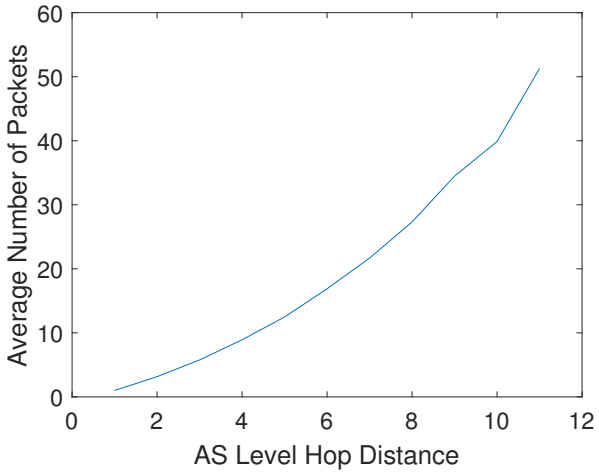

Fig. 3: Average number of packets needed to construct a path from an attacker toward a victim site with respect to the hop distance

We conducted two experiments for DoS and DDoS attack cases. In the DoS case, we analyze all AS paths in our dataset. We assume that the first AS is the attacker and the last AS is the victim. Next, we ran our Matlab procedure that emulates the approach presented in Section III. We calculated the number of required packets to construct the AS level forward-paths graph from the attacker toward the victim AS. To reduce the probabilistic bias, we repeated this experiment 5000 times.

Figure 3 shows the average number of packets needed to construct a forward path with respect to the AS level hop distances between the attacker and victim sites. Our method is able to construct the forward path with a minimum of 1 packet and a maximum of 51.29 packets on the average. The overall average regardless of the hop distance is 10.14.

In our next experiment, we emulated DDoS attacks for 100, 1000, 2000, 3000, 4000, and 5000 randomly chosen attackers.

TABLE I: Average number of packets w.r.t. number of attacker sites in DDoS

Number of Attacker Sites	Average Number of Packets
100	10.13
1000	10.17
2000	10.21
3000	10.29
4000	10.07
5000	10.18

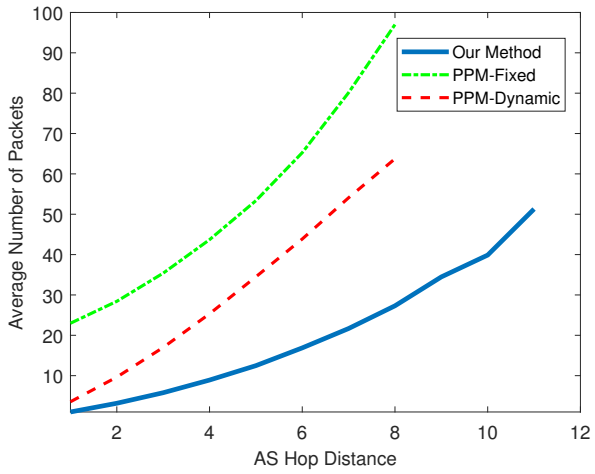

Fig. 4: Comparison between previously suggested methods and our method

We repeated the attack scenario 1000 times for each attack count case to reduce the bias. Table I presents the required average number of packets per attacker site to build a complete forward-paths graph for DDoS attacks. The numbers clearly show the scalability of the proposed method. Even though the number of attackers increases, the victim site tracks each attacker around 10 packets on the average.

In the following, we compare our work with the Probabilistic Packet Marking (PPM) based AS traceback methods [3, 4]. These types of methods apply the traditional PPM IP traceback [8] technique to AS level. We compare our method with PPM fixed probability [4] and dynamic probability [3] for packet marking. We implemented the method in [4] using a fixed probability $p = 0.092$, as suggested in the paper. Also, we implemented the method in [3] where the marking probability is calculated dynamically based on the distance between attackers and the victim. The distance field in both works is represented by 3 bits which gives the maximum number of traceable AS count as 8.

Figure 4 shows that PPM-dynamic needs 3.53 to 63.74 packets, and PPM-fixed needs 22.98 to 96.99 packets on the average to construct AS level forward paths for varying hop distances. On the other hand, our method requires 1 to 27.31

packets on the average for the same AS paths. Additionally, our method is able to trace more than 8 AS hop lengths, whereas PPM-fixed and PPM-dynamic are unable to trace more than 8. Our maximum packet count is 51.29 for 11 AS hop distance, which is still less than both methods' required packet numbers for 8 hop distance. The overall averages are 10.14, 27.26, and 46.04 for our approach, PPM-dynamic, and PPM-fixed, respectively, regardless of the hop distance. The PPM-fixed method uses 16-bit, PPM-dynamic uses 25-bit in the IP packet header, and we use 22-bit in the IP header.

V. Conclusions

Distributed Denial of Service attacks are one of the most perilous attack types in the Internet. In order to prevent malicious attack traffic in the Internet, deploying filtering as close as to the attack source is crucial. In this work, we proposed an AS traceback scheme to infer AS level forward paths from attacker sites to a victim site. We utilize the 16-bit IP ID field and 6-bit from the ToS field in the IPv4 protocol. In our method, only the ingress routers of ASes probabilistically mark the packet with their AS numbers. We propose an encoding technique to reduce the number of required packets significantly. The destination site can construct the path after receiving enough packets.

Our results show that a victim site can construct the forward path from an attacker site after receiving 10.14 packets on the average for DoS attacks. The victim site needs between 1 and 51.29 packets on the average to construct forward paths of varying hop distances. Compared to the other techniques, our approach requires less many packets to construct the paths from attacker sites to a victim site. Additionally, we show the scalability of our method against DDoS attacks.

References

[1] FBI Internet Crime Report 2020 - https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

[2] Interpol Report on Cyberattacks - August 2020 - https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19

[3] M. Alenezi and M. J. Reed, "Traceback of DoS over Autonomous Systems", International Journal of Network Security and Its Applications 5.2 (2013): 131

[4] M. Okada, Y. Katsuno, A. Kanaoka, and E. Okamoto, "32-bit AS Number Based IP Traceback", Fifth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, IEEE, 2011

[5] S. T. Zargar, J. Joshi, and D. Tipper, "A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks." IEEE Communications Surveys & Tutorials, 2013

[6] M. T. Gil and M. Poletto, "MULTOPS: A Data-Structure for Bandwidth Attack Detection", USENIX Security Symposium, 2001

[7] A. Y. Nur, "Combating DDoS Attacks with Fair Rate Throttling", IEEE International Systems Conference (SYSCON), 2021

[8] S. Savage, D. Wetherall, A. Karlin, and T. Anderson, "Network Support for IP Traceback", IEEE/ACM Transactions on Networking 9.3 (2001): 226-237

[9] A. Y. Nur and M. E. Tozal, "Record Route IP Traceback: Combating DoS Attacks and the Variants", Computers & Security 72 (2018): 13-25

[10] D. Song and A. Perrig, "Advanced and Authenticated Marking Schemes for IP traceback", IEEE INFOCOM, April 2001.

[11] A. Yaar, A. Perrig, and D. Song, "FIT: Fast Internet Traceback," IEEE INFOCOM, March 2005.

[12] V. Paruchuri, A. Durresi, R. Kannan, and S. S. Iyengar, "Authenticated Autonomous System Traceback", 18th International Conference on Advanced Information Networking and Applications, IEEE, 2004

[13] A. Y. Nur and M. E. Tozal. "Single Packet AS Traceback against DoS Attacks", IEEE SYSCON, 2021

[14] RFC 4893 - https://tools.ietf.org/html/rfc4893

[15] RFC 6793 - https://tools.ietf.org/html/rfc6793

[16] ARIN - Autonomous System Numbers - https://www.arin.net/resources/guide/asn/

[17] H. von Schelling, "Coupon collecting for unequal probabilities," American Mathematical Monthly, 61:306-311, 1954.

[18] E. Garsva, N. Paulauskas, and G. Grazulevicius, "Packet size distribution tendencies in computer network flows", IEEE Open Conference of Electrical, Electronic and Information Sciences, 2015

[19] The CAIDA IPv4 Prefix-Probing Traceroute Dataset - 2020/02/02, https://www.ImpactCyberTrust.org, DOI 10.23721/107/1354205

[20] Routeviews Prefix to AS mappings Dataset for IPv4 and IPv6 - 2020/02/02, https://www.caida.org/data/routing/routeviews-prefix2as.xml