STF-DM: A Sparsely Tagged Fragmentation with Dynamic Marking an IP Traceback Approach

Hasmukh Patel[1] and Devesh Jinwala[2]
[1]Computer Engineering Department, Gujarat Technological University, India
[2]Computer Engineering Department, Sardar Vallabhbhai National Institute of Technology, India

Abstract: *Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks are serious threats to the Internet. The frequency of DoS and DDoS attacks is increasing day by day. Automated tools are also available that enable non-technical people to implement such attacks easily. Hence, it is not only important to prevent such attacks, but also need to trace back the attackers. Tracing back the sources of the attacks, which is known as an IP traceback problem is a hard problem because of the stateless nature of the Internet and spoofed Internet Protocol (IP) packets.Various approaches have been proposed for IP traceback. Probabilistic Packet Marking (PPM) approach incurs the minimum network and management overhead. Hence, we focus on PPM approach. Sparsely-Tagged Fragmentation Marking Scheme (S-TFMS), a PPM based approach, requires low overhead at the victim and achieve zero false-positives. However, it requires a large number of packets to recover the IP addresses. In this paper, we propose a Sparsely-Tagged Fragmentation Marking approach with dynamic marking probability. Our approach requires less number of packets than required by S-TFMS. Further, to reduce the number of packets required by victim, we extend our basic approach with the new marking format. Our extended approach requires less than one-tenth time number of packets than those in S-TFMS approach to recover the IP addresses. Our approaches recover the IP address quickly with zero false-positives in the presence of multiple attackers. We show mathematical as well as experimental analysis of our approaches.*

Keywords: *DDoS attack, IP traceback, probabilistic packet marking, dynamic marking, sparsely tagged marking.*

Received September 8, 2014; accepted October 20, 2015

1. Introduction

The Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks are major threats on the Internet today. The use of web services for various kinds of tasks like banking, shopping, booking tickets, email, etc. has been increasing. The targets of DDoS attacks can be the e-governance systems, private infrastructure for businesses or service providers. The recent 300 Gbps attacks on the Spamhaus, an anti-spam group, remind the seriousness of DoS/DDoS attacks. As a result of such attacks, the victim either loses important information or may be forced to close down its services. Automated tools [5] are also available that enable even non-technical people to implement such attacks easily. Hence, it is not only important to prevent such attacks, but also need to trace back the attackers/sources of attack.

The Internet infrastructure is so designed that it cannot trace the sender of the packet. Hence, the Internet infrastructure is vulnerable to DoS/DDoS attacks. In addition to that, attacker can spoof the source Internet Protocol (IP) address of packet to prevent trackback [17]. Therefore, to trace back the sources of packets is difficult. This problem is known as IP traceback problem.

Probabilistic Packet Marking (PPM) [20] is one of the approaches to resolve the IP traceback problem. PPM works efficiently when there is a single attack path. In case of multiple attack paths or multiple attackers, PPM suffers from the combinatorial explosion problem to recover the IP addresses of the routers at the victim and false-positives that prevent PPM deployment on the Internet. To deploy the PPM for the Internet, PPM must improve the following parameters.

1. Number of packets to recover the IP addresses at the victim (nPkts).
2. Number of combinations to resolve offset collision (nCmbs).
3. False-Positives (FPs).
4. Authentication of marking at the victim (Auth).

Various approaches have been proposed to improve the performance of the PPM scheme. We classify all the approaches into two categories. First category improves the PPM by reducing the number of packets required to recover the IP addresses at the victim (nPkts). It includes approaches based on dynamic marking probability [9, 10, 13, 16, 24] and logging at key routers [12, 14, 21]. Second category of approaches reduces the number of combinations (nCmbs) required at the victim to recover the IP addresses. It includes tag based approaches [10, 11] and uses of an additional data structure at the victim [7, 22, 25].

Tag based PPM approaches suffer from false-positives when the number of routers grow on the attack path. Sparsely-Tagged Fragmentation Marking Scheme (S-TFMS) [11] has low computational overhead at the victim and achieves zero false-positives. In S-TFMS, router marks the packets sparsely to resolve the combinatorial explosion problem at the victim. The victim can start the recovery process at any time whenever it detects the attacks. In case of tag collision, received marking with the same offset and tag are ignored to prevent false-positive. Therefore, S-TFMS requires a large number of packets to recover the IP addresses. In addition, S-TFMS do not authenticate the marking; hence, an attacker can spoof the marking to delay the recovery process.

Dynamic marking probability reduces the number of packets required and the number of unmarked packets reaches the victim. Therefore, we propose a Sparsely Tagged Fragmentation with Dynamic Marking approach (STF-DM1). Our approach is more efficient than S-TFMS. Our approach has low overhead and zero false-positives as the S-TFMS [11], yet our approach needs less number of packets to recover the IP addresses than required by S-TFMS. Further, to reduce the number of packets required by the victim, we extend our basic approach with the new marking format (STF-DM2). Our approaches recover the IP addresses with less number of packets than required by S-TFMS and zero false-positives in the presence of multiple attackers.

The rest of the paper is organized as follow. Section 2 covers the related work. Section 3 introduces our approaches STF-DM1 and STF-DM2. Section 4 presents the theoretical analysis of our approaches. We compare and analyze the performance of our approaches with the existing approach S-TFMS [11] in section 5. Section 6 concludes the work and discusses future work.

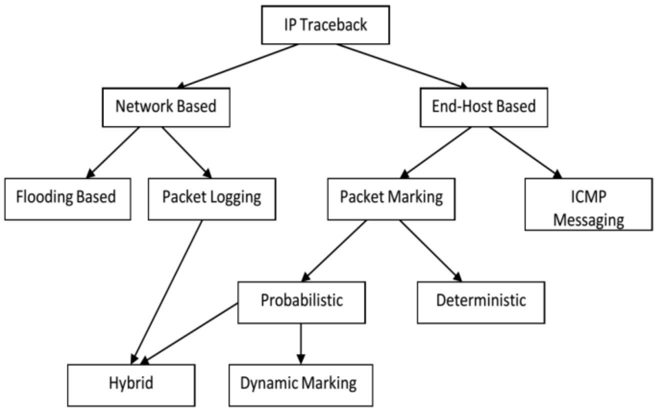

Figure 1. Classification of IP traceback schemes.

2. Related Work

In this section, we discuss the work related to IP Traceback. In Figure 1, we show the categories of IP Traceback approaches.

IP traceback approaches are broadly classified into network based [4, 6, 12, 14, 21, 23] and end-host based approaches [3, 7, 10, 13, 16, 19, 20, 22, 25]. In ingress filtering approach [6], the router is configured to prevent the packet with illegal address from the network on ingress port. However, Ingress filtering does not guarantee to prevent the IP spoofing. The attacker can still spoof source IP address of packet using the IP address from the legal range of network IP address. Input debugging approach [23] uses the feature available in router to find out the port on which the same signature packets are coming from the upstream router link. The operator has to communicate to the upstream router ISP to apply the same technique. The same is repeated to discover the path to the attacker. Controlled flooding approach [4] overcomes the disadvantages of input debugging, a manual communication by operator to inform about the port and attack signature. Controlled flooding assumes that the victim has an upstream router map. Log based approach [12, 14, 21] creates a log at key routers and uses mining technique to search for path whenever require. In [14], author uses routing path of packet to reconstruct attack paths. It requires less storage than log based approaches. In Internet Control Message Protocol (ICMP) traceback messages [3, 19] approach, the idea is to send a separate copy of the packet using ICMP packet containing the information about neighbour routers and packet information to the victim. The victim can use these packets later on if DoS attacks encountered. The frequency of ICMP packets should be very low to reduce the network overhead and storage requirement at the victim.

The principle of PPM scheme is also similar to ICMP traceback message to send the location of the router in the packet. However, PPM does not use separate packets, but uses the IP identification field of the IP header to send the location of router [20].

The PPM approach has low overhead compared to other IP traceback approaches. It does not require manual coordination among operator. As the size of the IP identification field is 16 bits only, router divides the IP address into several chunks and each chunk is marked into separate packet. The marking contains one of the chunks, offset of the selected chunk, and the distance from the victim. The victim combines the chunks from the received packets from the same router and constructs the IP address. In case of the single attack path, the victim uses the distance field of packet marking to resolve the offset collision. However, in case of multiple attackers and multiple attack paths, the victim may receive multiple packets with the same distance and offset fields in packet marking. The victim needs to combine the fragments and perform tests to verify correctness of IP address.

To improve the PPM scheme many techniques have been proposed. The dynamic marking probability gives equal opportunity to all the routers to send their marking to the victim. In [10], author proposed a method to adjust the packet marking probability using the distance of the router from the victim. The approach proposed in [13] uses the number of hops travelled by the packet from source to calculate the marking probability. In [16], the author uses the Time To Live (TTL) value of the packet and some constant t_p to adjust the marking probability.

In [7, 22, 25], authors propose a technique to trace the attacker using an upstream router map. In [22], packets are marked using 11-bits hash value of IP address and the distance value. The victim reconstructs the attack path using an upstream router map. In [25], author uses an upstream router map and node marking to reconstruct the attack path. In [7], packet is marked with a unique identification number generated using an Autonomous System (AS) number and id of router. The victim recovers IP of the router from unique id and an upstream router map. The IP traceback with an upstream router map are efficient; however, maintaining a data structure like an upstream router map is costly.

Tagging is a way to reduce the number of combinations required at the victim while reconstructing IP addresses. The tag is an identifier of the router. The victim uses tag to resolve the collision occurred (offset and distance fields have the same value) while combining the IP fragments. In [10], author uses 4-bits tag to resolve the collision. In [11], author proposed a sparsely tagged marking approach that uses tag to reduce the collision. The recovery algorithm ignores the marking whenever tag collision occurs, therefore approach does not require any trial and error to recover IP addresses; hence, it has zero false positives.

Belenky and Ansari [1, 2] have proposed Deterministic Packet Marking (DPM) technique. The idea is to mark the IP address of the ingress edge router in all the outgoing packets. DPM is simple and easy to implement. It has a little overhead on routers and the victim, but it requires universal implementation, and also suffers from false-positives. The authors in [26, 27, 28] proposed a hybrid approach, that uses the packet marking and logging both to improve the performance of the PPM. Sattari *et al*. [18] have proposed a network coding based PPM approach, that marks the packet with linear combination of router ID. The approaches proposed in [8, 22] authenticate the marking.

3. STF-DM:Sparsely-Tagged Fragmentation with Dynamic Packet Marking

In this section, we describe our approaches STF-DM1 and STF-DM2. We integrate dynamic marking based on TTL value of packet with S-TFMS [11] that reduces the number of packets required at the victim to recover the IP addresses. We also describe STF-DM2 that is extension of our basic approach STF-DM1 with a new marking format.

Our assumptions for STF-DM1 and STF-DM2 are as follow:

Related to attacker:

1. Multiple attackers may join.
2. Attackers may have knowledge of trackback implementation.
3. Attackers send large number of packets.
4. Victim has installed intrusion detection system to detect the attacks.

Related to network:

1. The routes of packets are fairly stable.
2. Routers have limited resources.
3. Routers are not compromised.

3.1. Sparsely-Tagged Fragmentation with Dynamic Marking Approach 1 (STF-DM1)

We observe that the S-TFMS uses fixed marking probability at all the routers. We may raise the marking probability in order to reduce the number of packets required at the victim. However, in this case, the nearer routers overwrite the marking from the farther routers and hence raise in marking probability favours the nearer routers to the victim. Hence, large numbers of packets are required to recover the IP addresses of the farther routers. With a goal to reduce the number of packets required at the victim to recover the IP addresses, we use a dynamic packet marking probability. The marking algorithm calculates marking probability based on TTL value of packet [16]. As the TTL value of the packet decrements hop by hop, the marking probability also decreases from farther router to the victim. Hence, the marking probability at the farther routers is higher compared to the nearer routers to the victim. The router closest to the attacker marks the packet with the highest and the router nearest to the victim marks the packet with the lowest marking probability. The dynamic marking probability also reduces the number of unmarked packets that reach the victim.

Algorithm 1: Marking algorithm for STF-DM1

```
STF-DM Marking Algorithm
for each packet P do
if (status = = 0) then
        x ⟵ a random number between [0, 1)
        if (TTL < 32) then
        q ⟵ 1/ (tp – TTL)
        else
        q ⟵ 1
        endif
        if (x <= q) then
        status ⟵ 1, offset ⟵ 0
        endif
endif
```

```
if (status = = 1) then
        if (offset = = 8) then
        status ⟵ 0
        else
P.offset ⟵ offset
        P.fragment ⟵ fragment (offset)
   P.tag ⟵ tag of the router
offset ⟵ offset + 1
        endif
endif
P.distance ⟵ P.distance + 1
End for
```

Like all the PPM approaches, our approach comprises of two algorithms. The first is the packet marking algorithm and the second is an IP recovery algorithm. Router executes the marking algorithm to mark the IP fragment into packet's IP fragmentation field of the IP header. The victim executes the IP recovery algorithm to combine the IP fragments from the marked packets to recover the IP addresses when victim suspects the attacks.

Marking Algorithm: In Algorithm 1, we show the marking algorithm that is executed by all the routers to mark the packets. The marking format consists of 5-bits for distance, 3-bits for offset, 4-bits for IP fragment and 4-bits for the tag. The tag is a hash of an IP address.

Initially the status of each router is set to zero (non-marking state). The status of the router is set to one (marking state) if the randomly chosen number x is less than marking probability q. Router marks the eight packets in sequence in marking state. In non-marking state, the router increments the distance field of the packet marking by one. The value of tp=N, where N is the total number of routers involved in attacks.

Recovery Algorithm: In Algorithm 2, we show the recovery algorithm. The victim runs the recovery algorithm to recover the IP addresses of the routers. The algorithm reads each packet from the buffer. The victim maintains the expected offset per distance and tag. Victim maintains two tables, pre-final and final table. The pre-final table stores the received IP fragments per tag and distance. If the offset of the marking is equal to the expected offset for the distance and tag of the marking, then the fragment is copied into the pre-final table. When all the eight fragments of the particular tag are received, the algorithm moves the row containing all the fragments from the pre-final table to the final table. The final table maintains entries containing recovered IP address. The recovery algorithm uses distance and tag fields to resolve the offset collision. Tag resolves offset collision of markings from the same distance. The recovery algorithm increases the value of the expected offset of the tag by 1 for each correct fragment received. If the offset of marking is not equal to the expected offset of the tag and distance, victim ignores the marking and expected offset of the tag and distance is set to zero.

The marking algorithm and recovery algorithm execute for each packet. Time required to perform the operations per packet is constant. Hence, the time complexity of the both algorithms is O (n).

3.2. Sparsely-Tagged Fragmentation with New Marking Format (STF-DM2)

The performance of STF-DM1 is better than S-TFMS. STF-DM1 needs to collect 8 fragments from each router to recover the IP address. In addition to that, when more than 16 (2^4) routers from the same distance share their marking period, 4 bits tag is not enough to resolve the collision. We observe that if collision is reduced, the number of packets required at the victim can be reduced. There are two ways to reduce the collision, one is to increase the number of bits to represent the tag in marking and another is to reduce the number of packets required to collect from each router. We design new marking format in order to increase the number of bits to represent the tag and further to reduce the number of packets required by adopting the 1-bit distance representation from Fast Internet Traceback (FIT) [25]. The marking format is as shown in Figure 2. The marking format has 8 bits to store the fragment of an IP address of the router. Hence, the victim needs to collect 4 packets from each router to reconstruct its IP address. We use 2 bits offset to index the 4 possible fragments of an IP address. We store the tag of the router into remaining 5 bits.

Algorithm 2: Recovery algorithm executes by victim in STF-DM1

```
STF-DM Recovery Algorithm
for each distance do
    for each tag do
        expected-offset [distance] [tag] ⟵ 0
    endfor
endfor
for each packet P do
P ⟵ read the packet from the buffer
if (P.offset = = expected-offset [P.distance] [P.tag]) then
    pre-final-table [P.distance] [P.tag] [P.offset] ⟵
    P.fragment
    expected-offset [P.distance] [P.tag] ⟵ expected-offset
    [P.distance] [P.tag] + 1
    if (all 8 fragments recovered) then
        move 8 fragments to final IP table
    endif
else
    skip the packet P
    Reset the entry in the pre-final-table
    expected-offset [P.distance][ P.tag] ⟵ 0
endif
endfor
```

Distance	Offset	Fragment	Tag
1 bit	2 bits	8 bits	5 bits

Figure 2. Marking format of STF-DM2 for 16 bits IP identification field of the IP header.

Marking Algorithm: The marking algorithm uses new marking format to mark the packet. The marking algorithm is the same as it is shown in Algorithm 1 except router marks 4 packets in sequence instead of 8 packets. The 1-bit distance in marking is sixth bit of TTL value and first five bits are set by global constantc.

P.distance ⟵ $TTL_{[5]}$

$TTL_{[4\text{-}0]}$⟵c

The interested reader may further refer FIT [25] for more details of 1-bit distance calculation.

Recovery Algorithm: The recovery algorithm is the same as it is shown in Algorithm 2 except victim requires collecting 4 packets from each router to reconstruct the IP address. The victim calculates the distance from the marking router from 1-bit distance field using d = (1-bit from marking | c - $TTL_{[5\text{-}0]}$) mod 64. The performance of this approach is better than STF-DM1, the approach discussed in section 3.1. Distance of the marking router from the victim is calculated using TTL value, hence STF-DM2 can handle legacy routers.

4. Theoretical Analysis

In this section, we first derive the equation to determine the expected number of packets required to recover the IP addresses for the STF-DM1 approach. Then after, we extend the derived equation for the STF-DM2 approach.

The marking algorithm calculates the marking probability based on TTL value of the packet, Hence the marking probability is decreasing from the farthest router to the victim. All the routers at the same distance from the source mark the packets with the same marking probability.

Table 1. Notation in analysis.

P_{md} -	Marking probability at distance d
P_d -	Proportion of marked packets
T_{pd} -	Total packets required for routers at distance d
N_d -	Number of routers at distance d
T_P -	Total packets required at the victim
N -	Total number of routers involved in attack
l -	Maximum path length

The marking algorithm calculates the marking probability at each router dynamically. Hence, the reaching probability (probability to reach the marked packet to the victim) of marking from each router is $r_p = \frac{1}{t_p + d\text{-}TTL_{init}}$, where t_p is a constant and d is a distance of router from source. Hence, the event determining IP of the router is identically distributed event. In Table 1, we show the notation we use in analysis.

We derive $T_{pd} = -\frac{8}{p_d a_d}\log(1\text{-}ep)$, where $p_d = \frac{8}{\frac{1}{p_{md}}+7}$ is marking probability at distance d and $a_d = e^{-2p_d(N_d-1)/16}$ is probability to recover the IP address of the router. N_d is the number of routers involved in an attack at distance d. The ep is expected proportion of IP determined routers. The interested reader may further refer STFM [11] for the detailed proof of equations.

For STF-DM1, total number of packets required is the sum of packets required for all the routers at the same distance from the victim to the farthest router. Hence, the total number of packets required is $T_p = \sum_{d=1}^{l} -\frac{8}{p_d a_d}\log(1\text{-}ep)$.

For STF-DM2, the recovery algorithm needs only 4 packets from each router to recover the IP address. Hence, the proportion of marked packets by the router at distance d is $p_d = \frac{4}{\frac{1}{p_{md}}+3}$. The probability to recover the IP of the router at distance d is $a_d = e^{-2p_d(N_d-1)/32}$ and the equation for total number of packets required is $T_p = \sum_{d=1}^{l} -\frac{4}{p_d a_d}\log(1\text{-}ep)$. Total number of routers in attacks is $N = \sum_{d=1}^{l} N_d$.

In Figure 3, we show the theoretical comparison of STF-DM1 and STF-DM2 with S-TFMS for the number of packets required to recover the 95% of IP addresses for different values of N. For marking probability $p_{md} = \frac{1}{0.25N}$, total packets have a minimum value.

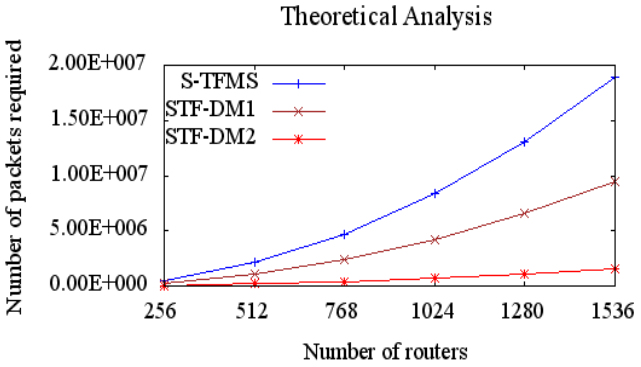

Figure 3. Theoretical - number of packets required to recover 95% of IP addresses.

5. Performance Results and Analysis

In this section, we discuss performance comparison of our approaches with S-TFMS [11]. We consider the number of packets required to recover the 95% of IP addresses for analysis and comparison with S-TFMS. We simulate our approaches and observe the performance for the number of packets needed to recover the IP addresses.

Table 2. Simulation parameters.

Parameter	Value
Model	waxman
m – Number of links per new node	2
Preferential connectivity	On
Node placement	Random
Growth type	Random

We use Boston university Representative Internet Topology generator (BRITE) [15] and network simulator with version 2.34 (NS-2.34) to simulate our approaches. We use parameters shown in Table 2 to generate the topology to perform the simulation.

We generated topology of 5000 nodes. We imported the generated topology into NS2. We randomly selected routers involved in attacks. We simulated for 256, 512, 768, 1024 and 1536 routers involved in attacks. The result shown in Figure 4 is average of 10 experiments for each value of N. We also generated topology for number of routers 256, 512, 768, 1024 and 1536. We simulated by randomly selecting N-1 routers as attacker and remaining router as victim. The results are similar as shown in Figure 4.

5.1. Analysis

In Figure 4, we show the number of packets required to recover 95% IP address at victim using our approaches and S-TFMS. The STF-DM1 approach requires less than half of the number of packets required by S-TFMS. The STF-DM2 approach requires less than one-tenth time the number of packets required by S-TFMS. Hence, our approaches require less number of packets than required by S-TFMS to recover 95% of IP addresses. Dynamic marking probability gives equal opportunity to all routers to send marking to victim. Hence, the number of packets required from farther routers and nearer routers is almost same. One of the reasons that STF-DM2 needs less number of packets compared to those required by STF-DM1 is the tag size of 5-bits instead of tag size of 4-bits in STF-DM1. The analysis based on simulation shown in Figure 4 matches with theoretical analysis shown in Figure 3.

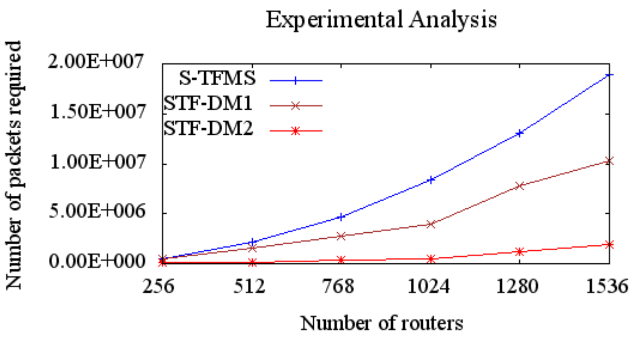

Figure 4. Simulation - number of packets required to recover 95% IP addresses.

5.2. Dynamic Marking Probability

In our approaches, we use dynamic marking probability that assigns higher probability to the routers that are farther away and lower probability to the nearer routers to the victim. Dynamic marking probability gives equal opportunity to all the routers; hence, packets from each router reach the victim early and IP recovery takes less time and less number of packets compared to constant marking probability. S-TFMS [11] uses constant marking probability; hence, it favours the nearer routers compared to the farther routers. Therefore, victim requires to collect more packets from the farther routers compared to the nearer routers. In Figure 5, we show the marking probability used for S-TFMS and STF- DM1 and STF-DM2 for N = 512.

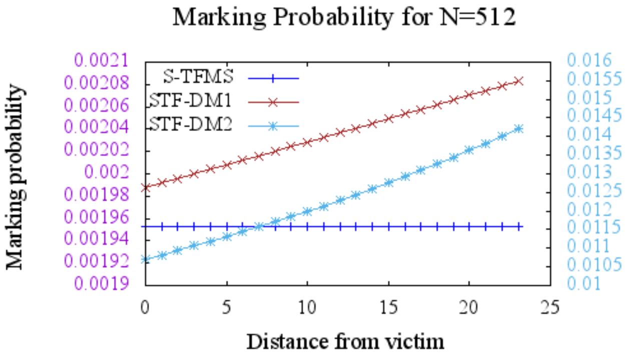

Figure 5. Marking probability for N=512

6. Conclusions and Future Work

DDoS is one of the growing attacks on the Internet. PPM is one of the effective approaches to resolve the IP traceback problem. None of the proposed PPM approaches optimizes all the parameters like number of packets requirement, high overhead at victim to recover IP addresses, false-positives and marking authentication. We propose an approach based on a sparsely-tagged fragmentation marking with dynamic marking probability. Further, to reduce the number of packets required by victim, we extend our basic approach STF-DM1 with a new marking format. Our approaches use a tag field to resolve the collision of the marking received from the routers at the same distance. We have simulated our proposed approaches and results are compared with S-TFMS. Our approach STF-DM1 requires less than half the number of packets to recover IP addresses required by S-TFMS. STF-DM2 requires less than one-tenth time the number of packets required by S-TFMS.

Majority of PPM approaches suffer from a large number of unmarked packets that reach to the victim or they need upstream router map. The low marking probability generates even more number of unmarked packets that reach to the victim. An attacker may take the advantage and can spoof the marking to misguide the victim while recovering the IP addresses; hence, recovery algorithm produces high false positives. In future, we plan to integrate authentication of the marking at victim to prevent compromise routers to spoof the marking.

References

[1] Belenky A. and Ansari N., "IP Traceback with Deterministic Packet Marking," *IEEE Communications Letters*, vol. 7, no. 4, pp. 162-164, 2003.

[2] Belenky A. and Ansari N., "On Deterministic Packet Marking," *Computer Networks*, vol. 51, no. 10, pp. 2677-2700, 2007.

[3] Bellovin M., Leech M., and Taylor T., ICMP traceback messages, Available: https://tools.ietf.org/html/draft-ietf-itrace-04, Last Visited, 2003.

[4] Burch H. and Cheswick B., "Tracing Anonymous Packets to Their Approximate Source," *in Proceedings of the 14th USENIX Conference on System Administration*, New Orleans, pp. 319-327, 2000.

[5] Criscuolo P., *Distributed Denial of Service: Trinoo, Tribe Flood Network, Tribe Flood Network 2000, and Stacheldraht*, Lawrence Livermore National Laboratory, 2000.

[6] Ferguson P., *Network Ingress Filtering: Defeating Denial of Service Attacks which Employ IP Source Address Spoofing*, RFC-2827, 2000.

[7] Gong C. and Sarac K., "Toward a More Practical Marking Scheme for IP Traceback," *in Proceedings of 3rd International Conference on Broadband Communications, Networks and Systems*, San Jose, pp. 1-10, 2006.

[8] Goodrich M., "Efficient Packet Marking for Large-Scale IP Traceback," *in Proceedings of the 9th ACM Conference on Computer and Communications Security*, New York, pp. 117-126, 2002.

[9] Iwamoto K., Soshi M., and Satoh T., "An Efficient and Adaptive IP Traceback Scheme," *in Proceedings of IEEE 7th International Conference on Service-Oriented Computing and Applications*, Matsue, pp. 235-240, 2014.

[10] Kim K., Hwang, J., Kim B., and Kim S., "Tagged Fragment Marking Scheme with Distance-Weighted Sampling for a Fast IP Traceback," *in Proceedings of Web Technologies and Applications*, Xi'an, pp. 442-452, 2003.

[11] Kim K., Kim J., and Hwang J., "IP Traceback with Sparsely-Tagged Fragment Marking Scheme under Massively Multiple Attack Paths," *Cluster Computing*, vol. 16, no. 2, pp. 229-239, 2013.

[12] Korkmaz T., Gong C., Sarac K., and Dykes S., "Single Packet IP Traceback in AS-Level Partial Deployment Scenario," *International Journal of Security and Networks*, vol. 2, no. 1, pp. 95-108, 2007.

[13] Liu J., Lee Z., and Chung Y., "Dynamic Probabilistic Packet Marking for Efficient IP Traceback," *Computer Networks*, vol. 51, no. 3, pp. 866-882, 2007.

[14] Lu N., Wang Y., Su S., and Yang F., "A Novel Path-Based Approach for Single-Packet IP Traceback," *Security and Communication Networks*, vol. 7, no. 2, pp. 309-321, 2014.

[15] Medina A., Lakhina A., Matta I., and Byers J., "BRITE: An Approach to Universal Topology Generation," *in Proceedings of 9th International Symposium on Modeling, Analysis and Simulation of Computer and Telecommunication Systems*, Cincinnati, pp. 346-353, 2001.

[16] Paruchuri V., Durresi A., and Chellappan S., "TTL based Packet Marking for IP Traceback," *in Proceedings of IEEE GLOBECOM Global Telecommunications Conference*, New Orleans, pp. 1-5, 2008.

[17] Sachdeva M., Singh G., Kumar K., and Singh K., "DDoS Incidents and Their Impact: A Review," *The International Arab Journal of Information Technology*, vol. 7, no. 1, pp. 14-20, 2010.

[18] Sattari P., Gjoka M., and Markopoulou A., "A Network Coding Approach to IP Traceback," *in Proceedings of IEEE International Symposium on Network Coding*, Toronto, pp. 1-6, 2010.

[19] Saurabh S. and Sairam A., "ICMP Based IP Traceback with Negligible Overhead for Highly Distributed Reflector Attack using Bloom Filters," *Computer Communications*, vol. 42, pp. 60-69, 2014.

[20] Savage S., Wetherall D., Karlin A., and Anderson T., "Practical Network Support for IP Traceback," *in Proceedings of the Conference on Applications, Technologies, Architectures, and Protocols for Computer Communication*, Stockholm, pp. 295-306, 2000.

[21] Snoeren A., Partridge C., Sanchez L., Jones C., Tchakountio F., Schwartz B., and Strayer W., "Single-Packet IP Traceback," *IEEE/ACM Transactions on Networking*, vol. 10, no. 6, pp. 721-734, 2002.

[22] Song D. and Perrig A., "Advanced and Authenticated Marking Schemes for IP Traceback," *in Proceedings of INFOCOM, 20th Annual Joint Conference of the IEEE Computer and Communications Societies*, Anchorage, pp. 878-886, 2001.

[23] Stone R., "CenterTrack: An IP Overlay Network for Tracking DoS Floods," *In USENIX Security Symposium*, vol. 21, pp. 114, 2000.

[24] Tian H., Bi J., and Jiang X., "An Adaptive Probabilistic Marking Scheme for Fast and

Secure Traceback," *Networking Science*, vol. 2, no. 1-2, pp. 42-51, 2013.

[25] Yaar A., Perrig A., and Song D., "FIT: Fast Internet Traceback," *in Proceedings of INFOCOM, 24th Annual Joint Conference of the IEEE Computer and Communications Societies*, Miami, pp. 1395-1406, 2005.

[26] Yan D., Wang Y., Su S., and Yang F., "A Precise and Practical IP Traceback Technique Based on Packet Marking and Logging," *Journal of Information Science and Engineering*, vol. 28, no. 3, pp. 453-470, 2012.

[27] Yang M. and Yang M., "RIHT: a Novel Hybrid IP Traceback Scheme," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 2, pp. 789-797, 2012.

[28] Yang M., "Storage-Efficient 16-Bit Hybrid IP Traceback with Single Packet," *The Scientific World Journal*, vol. 2014, pp. 1-14, 2014.

Devesh Jinwala has been working as a Professor in Computer Engineering at the Department of Computer Engineering, S V National Institute of Technology, Surat, India since 1991. His principal research areas of interest are broadly Security, Cryptography, Algorithms and Software Engineering. Specifically his work focuses on Security and Privacy Issues in Resource-constrained environments (Wireless Sensor Networks) and in Data Mining, Attribute-based Encryption techniques, Requirements Specification, and Ontologies in Software Engineering. He has been/is the principal Investigator of several sponsored research projects funded by ISRO, GUJCOST, Govt of Gujarat and DiETY-MCIT-Govt of India.

Hasmukh Patel has been working as an Assistant Professor in Computer Engineering Department at Gujarat Power Engineering and Research Institute, Mewad (India). His major areas of interests are security protocols verification and Network Security.