A Marking/Traceback System for Detecting the Source of Dos/Ddos Attacks

Malliga Subramanian, Kogilavani, P.S.Nandhini

***Abstract:** Distributed Denial of Service (DDoS) attack is a significant threat in today's world. Attackers hide their identity by spoofing and defending. To quickly detect a spoofed Internet Protocol (IP) during a DDoS attack the number of time-to-live hops in the network can be evaluated. While using time-to-live, if the routers gets compromised it may lead to the wrong detection of spoofed IP when both the source and attacker are at same distance. To identify an attacker, this system proposes an enhanced packet marking and traceback algorithm for IP traceback that helps the traceback of the spoofed packet to its source. A number of IP traceback techniques exist, but they have limitations like the number of packets required or storage and computational overheads incurred at routers. The technique proposed reduces marking and storage overhead..*

***Keywords:** IP Spoofing, DoS/DDoS, IP Traceback, Packet Marking, Storage Overhead.*

I. INTRODUCTION

Spoofing is the creation of TCP / IP packets with a forged source IP address. To forward packets over the Internet, routers use the destination IP address, but ignore the source address and it is never authenticated. This motivates attackers to exploit spoofing to attack Denial of Service (DoS) or Distributed DoS (DDoS).A DoS / DDoS attack is an explicit attempt made by attackers to prevent the legitimate users from getting the service. Because the DoS / DDoS attackers use spoofing, finding the source of such attacks and defending against them is very difficult.

There are two kinds of attacks on DoS / DDoS: flooding attacks and exploits of software. It is not always necessary to flood a victim with these attacks. However, a single well - focused packet of attacks can detrimentalize a target system.

Researchers have made enormous efforts to address these attacks. Such an effort is the technique of IP traceback. It is a technique that determines the real origin of the packet and establishes protective mechanisms to prevent spoofing attacks. IP traceback is used to identify flooding as well as single packet attacks.

Revised Manuscript Received on December 30, 2019.
* Correspondence Author

S. Malliga*, Professor, Department of Science and Engineering, Kongu Engineering College, Perundurai, Erode, Tamil Nadu, India Email: mallinishanth72@gmail.com

S.V.Kogilavani, Associate Professor, Department of Science and Engineering, Kongu Engineering College, Perundurai, Erode, Tamil Nadu, India, kogilavani@kongu.ac.in

P.S.Nandhini Assistant Professor, Department of Science and Engineering, Kongu Engineering College, Perundurai, Erode, Tamil Nadu, India, nandhini.cse@kongu.ac.in

IP traceback techniques can be broadly classified into two types: in-band and out-of-band approaches. In - band approaches use IP packets to enable traceback and out - of - band approaches use a separate trace packet such as an ICMP packet.

It is possible to classify IP traceback schemes into link testing, logging, marking or hybrid methods. Link testing and packet marking – based traceback schemes require a huge number of packets are required to reconstruct the path of the attack. Packet marking requires the routers along the path to mark the packets they forward with their identification information. These markings are either probabilistic (PPM) or deterministic (DPM) markings. Such marked packets are then used to reconstruct the packets path. Packet logging allows the routers to store the packets they are forwarding and these packets are used during traceback to reconstruct the path.

For DDoS attacks, source tracking techniques are classified into origin-based, relay-based, and destinatio-based approaches. The origin-based detection technique is generally egress filtering method.. The relay-based detection techniques include controlled flooding, IP traceback, Spoofing Prevention Method (SPM), and Stack Push Identification (StackPI), which identify the fake source by tracking DDoS traffic. The destination-based detection technique consists of unicast Reverse Path Forwarding (uRPF), bogon filtering, Transmission Control Protocol (TCP) interception, and Hop Count Filtering (HCF).

This article proposes a method for detecting a spoofed IP from the DDoS shelter at source to provide simultaneous protection against multiple target DDoS attacks and also uses marking and traceback (ESPITRI) approach. Spoofed IP can be detected quickly by calculating the number of normal Time-To- Live (TTL) hops from the reference table.

II. RELATED WORK

Several attempts have been made to reduce the effect of IP spoofing. One approach, ingress filtering [1], blocks packets on the routers when the packets have illegitimate IP addresses. But, this scheme needs enormous power and knowledge to filter each of the incoming packets. This approach works well on border routers, while the success rate in transit networks is dependent on other upstream Internet service providers (ISPs). In addition, legitimate user table and look-up time are increasing exponentially as the network grows, which impairs high-speed links.

This work leads to some complications on existing services that use source address spoofing, such as mobile IP(MIP) and some satellite hybrid architectures;

Router interface-based approaches use interface router numbers rather than IP addresses to trace the attacker back. The RIM (Router Interface Marking), proposed by Chen et al[2], is a packet marking approach that marks packets probabilistically; So, it requires more packets and leads to false positives when the number of attackers increases. Malliga and Tamilarasi[3] have proposed Modulo / Reverse Modulo Technique (MRT), a hybrid scheme that uses router interfaces. Using the router interface, MRT performs mathematical calculations and marks the resulting value. This process continues to the victim. During trace back, the reverse calculations are performed to identify the upstream links. MRT uses a 32-bit marking field and requires routers to store when the marking field overflows.

Malliga and Tamilarasi[4] proposed another hybrid scheme called MORE (MOdulo and REverse modulo), in which the field size of the marking is reduced to 16 bits but more log tables may be required based on the degree of the routers. Both MRT and MORE index the log by packet digest, which requires logging every packet that passes the same path. MRT and MORE use single packet to track back the attacker, but a comprehensive search is required for trace-back process. They can also produce false positives due to collisions in the log table. M-H Yang and M-C Yang[5] recently proposed RIHT, a hybrid trace-back scheme that uses the router interface. In RIHT, the mathematical calculations performed in MRT are appropriately modified and replaced the log table with a hash table to reduce the search time. RIHT has been shown to be superior to any other hybrid scheme in terms of storage requirements, computational time and accuracy. Although trace-back time is minimized by eliminating the comprehensive search with MRT and MORE, the logging time in RIHT is more due to hash table collisions. Kamaldeep et al. [6] proposed a trace-back scheme that reduced logging time of RIHT. However, it consumes more time for double hashing.

SPITRI [7] is an ICMP traceback scheme. At first, in SPITRI, the egress router generates an ICMP packet with the probability ‘P’ and sends it towards the destination. While forwarding the packets, the intermediate routers update the path information in the received ICMP traceback packet using the ID assigned to the incoming link. Equation (1) is used to update the path information.

$$Pathinfo_{new} = \frac{1}{Pathinfo+2} + ID + 1 \qquad (1)$$

In Equation (1), *‘Pathinfo$_{new}$‘* is the path information to be recorded at a router, ‘P*athinfo*’ is the path information received from the upstream router. *‘ID’* is number assigned to the incoming link. This formula was derived in such a way that value of path information has a collective (i.e.cummulative) effect of all the incoming interfaces through which the packet traversed to reach the destination. Hence, *Pathinfo* is used to retrieve the complete list of upstream Interface Ids so that the attacker could be reached. During traceback, every router uses Equation (2) and Equation (3) to find the incoming link and the path information it received from its upstream router.

$$ID = floor(Pathinfo) - 1 \qquad (2)$$

$$Pathinfo_{old} = \frac{1}{Pathinfo - floor(Pathinfo)} - 2 \qquad (3)$$

In Equation (2), ‘Pathinfo$_{old}$’ is the path information retrieved from the upstream router during the marking process. These equations are repeatedly applied by routers to find their upstream routers. To stop the traceback process, TTL is used. From Equations (1), (2) and (3), we can understand that these equations perform a few arithmetic operations like adding and subtracting two, adding and subtracting one. While analyzing SPITRI with some numerical examples, it is found that these arithmetic operations are highly redundant. The number of clock cycles required for integer addition and subtraction depends on the processor. For instance, Intel core 2 duo processor expends one clock cycle for addition and subtraction. Even though, addition and subtraction require a one clock cycle, when a router marks more number of packets, it has to spend huge clock cycles. This causes additional overhead on the routers. Also, the size of path information element in the ICMP traceback packet is at least 512 bits. The content of the traceback packet is stored in router and it contains at least the 20 byte IP header of the traced packet. This is used to correlate the ICMP packet with the original packet being traced. It is found that the path information of size 512 bits is also redundant. A maximum of 16 bits path information is sufficient to enable traceback. Another limitation is that it can trace only the flooding attacks and it could not trace a single attack packet asthe ICMP packet is sent with a probability,. These limitations are addressed in the proposed approach.

III. RESEARCH METHOD

A. Enhanced SPITRI

3.1.1 Marking

ESPITRI allows each packet that flows through the router to be marked, here again, the markings made by the routers give the cumulative effect of the packet's complete path. The routers use the incoming link or interface by which the packets enter the routers to mark each packet. Each router keeps a table mapping each of its link's hardware address to a unique ID from 0 onwards. It finds the ID associated with the incoming link when a router marks and marks the packet. ESPITRI eliminates redundant operations. This addition requires one clock cycle on most processors, the number of clock cycles would be considerably very high if a large number of packets are marked. The given Equation (4) reduces the clock cycle.

$$Markinfo_{new} = \frac{1}{Markinfo} + ID \qquad (4)$$

‘Markinfo’ is the marking information that arrives at a router. ‘Markinfonew’ is the newly computed marking information by R.

3.1.2. Marking Algorithm

1. Begin
2. Let R = {Ri} be a set of routers in the path and ID be their interfaces through which the traceback message entered the router, Markinfo$_{new}$ be the newly computed path information element of ESPITRI message, Markinfo be the current path information.

```
3. At each router Ri
   i. If Ri is border router, then the router marks the ID
      associated with the incoming link and marks the packet
   ii. ID=No.of interfaces Markinfonew = ID
   iii. else
   iv. ID=No.of interfaces
   v. Markinfonew =(1/ Markinfo )+ID
           a. End If
           b. Markinfo = Markinfonew
           c. Forward ESPITRI message to next router.
           d. Go to Step i.
           e. End
```

After marking algorithm is implemented, to check whether the packets are spoofed or not TTL is used.

B. TTL Based DDoS Attack

Time to live (TTL) is a mechanism that limits the lifetime of packet in a network.TTL is used as counter. Once limit is reached, the packet will be discarded. It prevents a data packet from indefinite circulation.

The abnormal number of hops at the destination is applied to determine and block the fake traffic. The number of hops is detected from the TCP packets. A DDoS shelter at the destination uses the TCP packets to detect the attacking traffic and conducts a statistical analysis to determine whether it is falsified. The DDoS shelter can quickly block the relevant IP traffic if found to be counterfeited.

To block counterfeit traffic, a method for detecting the abnormal number of hops in the DDoS shelter is applied. When the original TTL value is deducted from the destination, the number of total hops can be detected for each router.TTL value is deceased by one on passing each router. Table 1 shows the initial TTL value for different types of operating systems.

Table 1. Initial TTL value of each OS

Operating Systems	TTL
Linux .6	64
Windows 2000	128
Windows XP	128
Windows7,Vista and Server 8	128
MAC	64

When the TCP packets pass through the routers, the TTL value in each packet is reduced by one and an abnormal number of hops at the destination is detected using the normal Internet path statistical information.

On an average, the upper limit on number of hops over a normal Internet path will not exceed 30. In general, the number of traffic hops is less than 30. Thus, if the destination's TTL value is 93, the initial TTL value shall be within 93 + 30.

For instance, if the starting TTL value is 128 and the final TTL value is 103, it is estimated that the total number of hops passed is 128 − 103 = 25 hops. The hop number found is then compared with the Table 1.

Method for detecting spoofed IP

The step - by - step detection procedure for a spoofed IP is given below:

1. Check the type of OS and get the initial TTL value.
2. Get the TCP packet's final TTL hop count (T_f).
3. Infer the TCP packet initial TTL hop count (T_i).
4. Add a constant value to T_f and assign to T_s.
5. Compute hop count: $H_c = T_i - T_f$
6. If H_c is larger than T_s, then the IP address must be faked and perform traceback.

In TTL, traceback has to be performed whether the packet is spoofed or not. The TTL value may be same if the attacker and the source IP's are at same distance. To verify whether the packet is sent by the source, traceback is used.

C. Traceback

When the victim detects that the received packet is an attack packet, the process of traceback or path reconstruction is brought into play. The victim is now using the packet's marking or path information to trace the packet's path. Because the markings are made to create a cumulative path effect, they are used to allow traceback. First, the victim is sending the packet to their first hop router. Upon receiving the requested traceback packet, the router finds the incoming interface that allows the tracked packet to be tracked into it using the victim's marking information and also finds markings that it received from its upstream router when the packet was previously sent through it. After identifying these two details, the router uses the identified interface to forward the request for traceback to its upstream router. To determine the marking information, every router uses Equation (5) and (6).

$$ID = floor(Markinfo) \tag{5}$$

$$Markinfo_{new} = 1/(Markinfo - ID\ ) \tag{6}$$

Traceback algorithm

```
Begin

Let ID be Upstream Interface ID through which the packet
came in, Markinfo be the current path information value
received and Markinfo_new be the newly computed path
information value
For every router,
{
    ID = floor(Markinfo)
    Markinfo_new= 1/(Markinfo -ID)
    Markinfo = Markinfo_new
    Print the Upstream Interface ID
    Forward the packet via ID with Markinfo to the
    upstream router
     }
End
```

IV. RESULTS AND ANALYSIS

To understand the performance, we test ESPITRI with TTL and compared SPITRI. The time taken to perform the marking process for SPITRI and ESPITRI with TTL differs.

Table 2 and 3 illustrate the working of Marking and Traceback algorithm. Table 4 shows the comparison results.

Table 2. Illustration of marking process

Router ID	Number of interfaces in the router	Interface through the packets come in (average case)	Marking information	
			Received	Computed

N169668	175	87	87	87.01
N10994	84	42	87.01	42.01
N105646	44	22	42.01	22.02
N172198	568	284	22.02	284.05
N166846	38	19	284.05	19.01

Table 3. Illustration of Traceback process

Router ID	No. of interfaces in the router	Interface through the packets come in (average case)	Marking information	
			Received	Computed
N166846	38	19	19.01	284.05
N172198	568	284	284.05	22.02
N105646	44	22	22.02	42.01
N10994	84	42	42.01	87.01
N169668	175	87	87.01	87

In Table 4, marking and traceback timings were compared. For 10,000 packets, the existing system gives 0.01000 seconds as a marking time and 0.007000 seconds as the traceback time whereas in the proposed system the time differs for marking and traceback as 0.007000 and 0.005000. The time difference between the existing and the proposed work gives the percentage gain of 30% for marking and 28.57% for traceback. Likewise, several number of packets have been tested and the percentage gain results are obtained.

V. CONCLUSION

This work carefully considered the DoS / DDoS attack problems and suggested an hybrid approach to detect the source of these attacks. The source of the proposed ESPITRI is SPITRI, an ICMP traceback system. SPITRI was analyzed carefully and its problems were identified. The solutions to these problems have led to ESPITRI's development along with TTL.

ESPITRI eliminates SPITRI's redundant arithmetic operations. This reduces the marking and storage overhead of ESPITRI during the process of marking and traceback. Since every IP packet is marked, once an IP packet is detected as an attack packet based on TTL , the traceback process is initiated. When no router is consulted during traceback, ESPITRI provides 100% traceback accuracy

Table 4.Marking and Traceback overhead

No. of Packets	Existing System (SPITRI) (in sec)		Proposed System (Enhanced SPITRI with TTL) (in sec)		Percentage of improvement (Proposed system)	
	Marking	Traceback	Marking	Traceback	Marking	Traceback
10,000	0.010000	0.007000	0.007000	0.005000	30%	28.57%
20,000	0.011000	0.010000	0.007000	0.009000	36.36%	10%
30,000	0.009000	0.012000	0.003000	0.010000	66.67%	16.67%
50,000	0.020000	0.017000	0.009000	0.016000	55%	5.88%
1,00,000	0.033000	0.029000	0.023000	0.027000	39%	6.9%
2,00,000	0.058000	0.035000	0.042000	0.036000	24%	8.5%
3,00,000	0.089000	0.072000	0.061000	0.063000	54%	8.75%

REFERENCES

1. P. Ferguson, D. Senie, "Network ingress filtering: defeating denial of service at-tacks which employ IP source address spoofing (BCP 38)", 2000. http://tools.ietf.org/html/rfc2827 (accessed 19 February 2018).
2. R. Chen, J.M. Park, R. Marchany, "RIM: Router interface marking for IP traceback", *IEEE Global Telecommunications Conference (GLOBECOM '06)*, San Fransisco, California, November 2006, pp 1–5
3. S. Malliga, A. Tamilarasi, "A proposal for new marking scheme with its performance evaluation for IP traceback", *WSEAS Trans. Computer research*. Vol. 3, (2008), pp. 259–272
4. S. Malliga, A. Tamilarasi, "A hybrid scheme using packet marking and logging for IP traceback", *Int.ernational Journal Internet Protocol Technology*. Vol 5, (2010), pp. 81–91.
5. M.H. Yang, M.C. Yang, "RIHT: a novel hybrid IP traceback scheme", IEEE Transaction .Information Forensics Security. Vol. 7, 2012, pp. 789–797.
6. M. Kamaldeep, M. Malik, M. Dutta, "Implementation of single-packet hybrid IP traceback for IPv4 and IPv6 networks", *IET Information. Security*. Vol. 12, (2018), pp. 1–6, doi:10.1049/iet-ifs.2015.0483.
7. M. Vijayalakshmi, and M. Shalinie, "Single Packet ICMP Traceback Technique using Router Interface". *Journal of Information Science and Engineering,* Vol. 30, No. 6, 2014, pp. 1673-1694

AUTHORS PROFILE

Dr. S.Malliga is working as a Professor in the Department of Computer Science and Engineering, Kongu Engineering College, Tamil Nadu, India. She obtained PhD in the year 2010 from Anna University, Chennai. Her research area inlcudes Computer Network and Security. She has done many consultancy projects including VoIP, Web site developement for many industries. She has also offered many training programmes urses on latest technology and trends. Currently she is guiding four research scholars. She has also guided many UG and PG projects. She has published 40 articles in international journals and presented more than 40 papers in national and international conferences in her research and other technical areas. Recentlty she is awarded with Summer Reseacrh Fellowship by Indian Academy of Sciences.

Dr. S.V.Kogilavani is associated with the Department of Computer Science and Engineering as an Associate Professor at Kongu Engineering College, Tamil Nadu, India. Her research interests include Information Retrieval and Summarization. She received her Ph.D from Anna Unviesity, Chennai in the year 2013. She has presented many papers in national and international conferences and published 15 papers in national and international journals. She is also awarded with Summer Reseacrh Fellowship by Indian Academy of Sciences

Ms.P.S.Nandhini Completed BE (IT) with first class distinction in Avinashilingam Institute for Home Science and Higher Education for Women, Coimbatore. Secured Gold Medal in ME (Computer and Communication Engineering) in Kongu Engineering College, Perundurai, Erode. Currently, pursuing PhD in (Internet of Things) under Anna University. Area of interest includes Wireless Networks, Wireless Sensor Networks and Internet of Things. Published papers in National and International Journals and Conferences. . Recentlty she is awarded with Summer Reseacrh Fellowship by Indian Academy of Sciences