International Journal of Advance Research in Science and Engineering
Vol. No.4, Special Issue (01), August 2015
www.ijarse.com
IJARSE
ISSN 2319 - 8354

SWAPNILs PACKET MARKING AND TRACEBACKING (SPMT) TECHNIQUE FOR EFFICIENT IP TRACEBACK

Mr. Swapnil M. Sanap

Master of Engineering, Dept. Of Information Technology STES's S.K.N College of Engineering, Pune, Maharashtra, (India)

ABSTRACT

There are many existing packet marking techniques [1] like probabilistic packet marking (PPM) [1][2][3[4], deterministic packet marking (DPM) [1][5][6], router-based approach (RBA)[7][8], and the like. In order for traceback mechanism to be competent in tracing, the mechanism should require minimum number of packets from the attacker to perform IP Traceback. A mechanism which takes minimum or few or less packets and avoids all the possible overheads on packet, router, and/or network is needed for an efficient traceback of the origin of the attack, and the mechanism must also provide a solution to mitigate the DoS and/or DDoS attacks on the network [1]. In this paper an efficient packet marking technique called swapnil's packet marking and tracebacking (SPMT) technique that requires number of packets equal to the hop distance between the attack initiator and the destination (server), which is less than 31 [11] [12] is proposed. Using simulation technique we demonstrate that the proposed SPMT algorithm executes in better way than the existing packet marking techniques in view of packets required for successful traceback and in mitigating the DoS and/or DDoS attacks on the network. Further, the proposed SPMT algorithm does not generate any kind of overhead at the intermediate nodes of the network.

Keywords: Internet, Security, IP Protocol, IP Spoofing, IP Traceback, Denial-Of-Service (Dos) Attack, Packet Marking, Packet Tracing, Packet Filtering.

I. INTRODUCTİON

The DoS and DDoS attacks on the networks are increasing and the result in the performance of network is decreasing. Most of the existing packet marking techniques (for IP traceback) requires many packets to traceback the source. They also have drawbacks such as packet header overload, network overhead, router overhead, etc. Hence in order for traceback mechanism to be competent in tracing, the mechanism should require minimum number of packets from the attacker to perform IP Traceback [1].

Thus, a mechanism which takes few or less packets and avoids all the possible overheads on packet, router, and/or network is needed for an efficient traceback of the origin of the attack. Further, the techniques must also provide a solution to mitigate the DoS and/or DDoS attacked on the network [1].

In this paper, we propose an efficient packet marking technique called swapnil's packet marking and tracebacking (SPMT) technique that requires number of packets almost equal to the hop distance between the

attack initiator and the destination (server), which is less than 31 [11][12]. The existing tracebacking techniques take many packets for tracebacking and some of them take even thousand packets for tracebacking. The proposed SPMT may work on complicated DoS / DDoS attacks that may involve multiple attackers in it. Further, this proposed SPMT may be utilized by other existing tracebacking techniques as well so as to reduce the number of packets required for the construction of the path during tracebacking.

II. SWAPNIL'S PACKET MARKING AND TRACEBACKING (SPMT) TECHNIQUE

The existing packet marking techniques needs many packets for the path reconstruction. For example, PPM technique *[1][2][3][4]*, used for a complete and a successful trace back, the edge sampling [9] technique involved in it requires almost 75 packets. In this existing technique, 16 bit IP identification (Id) field is used for marking. Also, as a well know concept, a single packet does not carry all the information/data and hence the marking node / router fragments the marks and send it in multiple packets.

In the attack situation, even though the victim/destination may receive enormous number of packets, for doing a single traceback to the attacker, the attacker may have triggered the attack by less number of attacks. Hence, a technique that will take less or fewer number of packets form tracebacking is considered as most efficient and reliable technique for tracebacking.

In this paper we propose an efficient packet marking technique called swapnil's packet marking and tracebacking (SPMT) technique that requires number of packets equal to the hop distance between the attack initiator and the destination (server). The proposed SPMT technique uses time-to-live (TTL) value and the identification filed (ID) value of a packet to schedule the marking of the packet. The SPMT algorithm may be implemented at the routers available in the network and hence, the algorithm decides which router will mark the packet. The proposed algorithm uses the TTL value to find the hop distance or the count and the ID field of the packet to value generated by the source of packet to mark the packet.

In SPMT we have used the TTL value of the packet to find the hop count at the router. We use the IP ID field value of packet and hop count of the packet to decide if the router would mark the packet.

SPMT Marking Algorithm at router R

Input: Packet w; Output: w: start; w: end; w: distance

```
1:    for each packet p do
2:     if ((w: ID%31) + 1) = w:hop then
3:    w: start   IP(router)
4:    w: distance   0
5:    else
6:    if w: distance = 0 then
7:    w: end   IP(Router)
8:    end if
9:     increment w: distance
10:   end if
11:   end for
```

As the algorithm is adapted to perform modulo arithmetic with 31, the result will always be between v Є {0, 1, ….. 30}, and hence v + 1 Є {1, ….. 31}. It may be understood that the value v can be equal to the hop count at only one of the routers in the path for a given IP ID value of packet.

From RFC 791 [10], the IP ID field is assigned values normally in three main ways.

1) Sequential- Each session on machine has its own IP ID assignment counter. In this all packets are marked with ID field value by the sender.

2) Sequential Jump - All the communication sessions going on the machine has same counter for IP ID field assignment.

3) Random - IP ID field is assigned randomly. In randomly generated ID values, ID%31 will have a result which would be uniformly distributed. It means that all the routers will have equal probability of marking the packet which would be equal to 1 to 31.

III. PATH RECONSTRUCTION IN THE SPMT TECHNIQUE

In the path reconstruction, a separate algorithm is proposed, in which the system under attack collects the malicious packets and thereby constructs a tree using the packet mark data. If the distance field of the packet is 0 then an edge is added with root as victim otherwise edges in tree are inserted with end point of edge being start and end node given in packet mark and it is inserted at distance w.distance. The complete reconstruction algorithm is provided below:

ALGORITHM:

Input: Packet w

Output: Path from victim to attacker

1: Let T be a tree rooted at v

2: Let edges in T be tuples (start, end, distance)

3: for each packet w from attacker do

4: if w.distance = 0 then

5: T.insertEdge(w.start,v,0) (edge is inserted with end nodes being victim and start node if the distance field of the packet is zero.)

6: else

7: T.insertEdge(w.start,w.end,w.distance) (edges are inserted in tree T if distance field is non zero.)

8: end if

9: end for

10: remove any edge (x,y,d) with d!= distance from x to v in T (some pruning takes place and all edges(x; y; d) are removed where distance of x 6= d from victim)

11: extract path (Ri;…….;Rj) by enumerating acyclic paths in T (acyclic paths are extracted forming the attack paths)

IV. RESULTS OF SIMULATION

In this section, we try to analyze how SPMT perform with the different hop values. We simulate our algorithm in NS-2 simulator having Network animator as front end and TCL as back end scripting language. We have

written small code to simulate PPM, and SPMT. The Parameters analyzed / calculated for the successful implementation of the propose Packet Marking Algorithm.

Table I. Time vs. Throughput and Normalized Routing Overhead

Time (sec)	SPMT Algorithm		PPM Algorithm	
	Throughput	Normalized Routing Overhead	Throughput	Normalized Routing Overhead
0.01	775245	9.29894	365689	19.7134
0.02	285267	25.271	182823	39.4315
0.03	190178	37.9064	121867	59.1543
0.04	142655	50.5341	91433.3	78.8439
0.05	114159	63.1481	73155.4	98.543

Throughput is increased as time passes. Better performance for SPMT algorithm than PPM algorithm is seen. Normalized Routing Overhead is decreased with time effectively with SPMT algorithm than PPM algorithm. The throughput is measured as data packets per second or data packets per time slot, and the unit is packet/second. The Normalized Routing Overhead is measured as the total the number of transmitted routing packets (hop-wise) to the number of data packets received by the destination nodes. The Normalized Routing Overhead is measured as data packets per second or data packets per time slot, and the unit is packet/second. The Normalized Routing Overhead is calculated by using a formula: Normalized Routing Overhead = Control overhead / No of packets received by a node.

Table II. Time vs. Packet Delivery ration and Dropping ratio.

Time (sec)	SPMT Algorithm		PPM Algorithm	
	Dropping Ratio	Packet Delivery Ratio	Dropping Ratio	Packet Delivery Ratio
0.01	0	100	52.8292	47.1708
0.02	26.4145	73.5855	52.8403	47.1597
0.03	26.4145	73.5855	52.8459	47.1541
0.04	26.4198	73.5802	52.8396	47.1604
0.05	26.4055	73.5945	52.8393	47.1607

Dropping ratio is less using SPMT algorithm as compared to PPM Algorithm. The Packet Delivery ratio is more in SPMT algorithm as compared to the PPM Algorithm. The packet delivery ratio is the ratio of the number of delivered data packet to a end point (destination). This explains the level of delivered data to the destination. The packet delivery ratio is calculated by packet delivery ratio = (total number of packets received by a node / total number of packets sent by a node)*100

The dropping ratio is a packet loss during transmission till delivery of packets from source to destination. The packet dropping ratio is calculated by packet dropping ratio = (((total number of packets sent by a node) – (total number of packets received by a node) / (total number of packets sent by a node)*100)

Table III. Time vs. Packet Delivery ration and Dropping ratio.

Hop(s)	SPMT Algorithm		PPM Algorithm	
	No. of Packets required	Probability	No. of Packets required	Probability
1	834	1	835	1
2	5482	0.5	835	0.5
3	9301	0.333333	9301	0.333333
4	5482	0.25	834	0.25
5	10132	0.2	834	0.2
6	5482	0.166667	10132	0.166667
7	10132	0.142857	833	0.142857
8	10132	0.125	831	0.125
9	832	0.111111	831	0.111111
10	832	0.1	833	0.1
11	10132	0.0909091	10132	0.0909091

The below motioned table is used to show the average number of packets required for a successful traceback to the source for threshold values 20, 25 and 31. The number of packets sent from source to destination in this simulation is 25, 50, 60, 75 and 100. The below mentioned result was obtained:

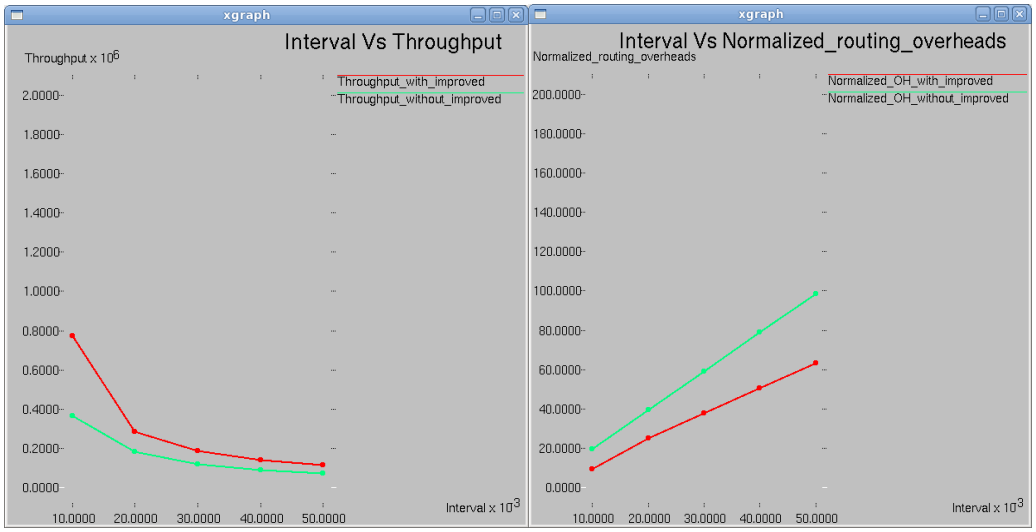
Threshold Value	**20**				
Packet Sent	25	50	60	75	100
Packet Received	25	50	60	75	100
Marked Packet	21	31	41	58	73
Unmarked Packets	4	19	19	17	27
Tracing Possible	NO	NO	NO	NO	YES

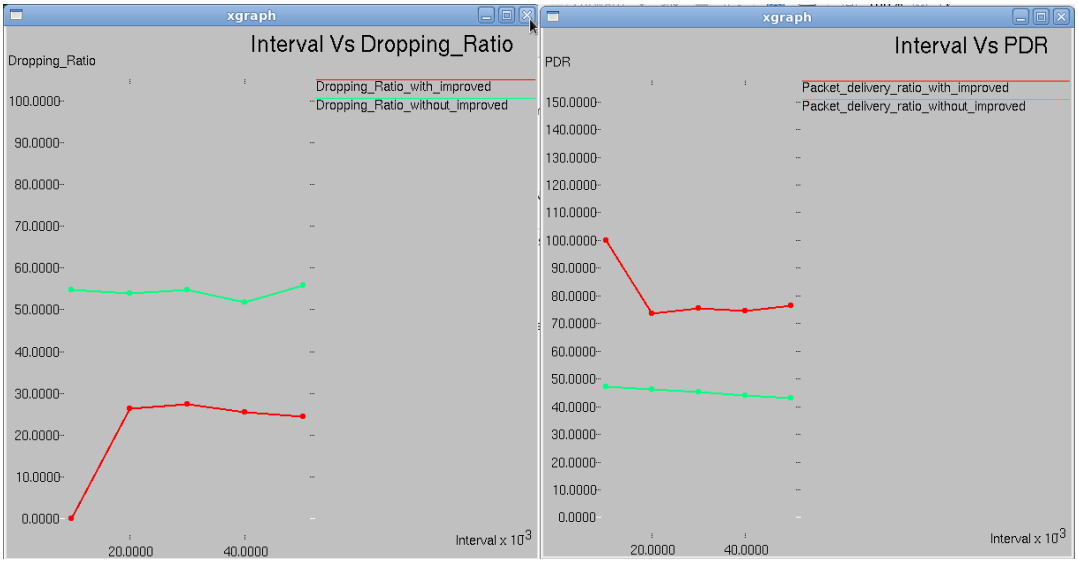
Threshold Value	**25**				
Packet Sent	25	50	60	75	100
Packet Received	25	50	60	75	100
Marked Packet	13	37	39	53	61
Unmarked Packets	12	13	21	22	39
Tracing Possible	NO	NO	NO	YES	YES

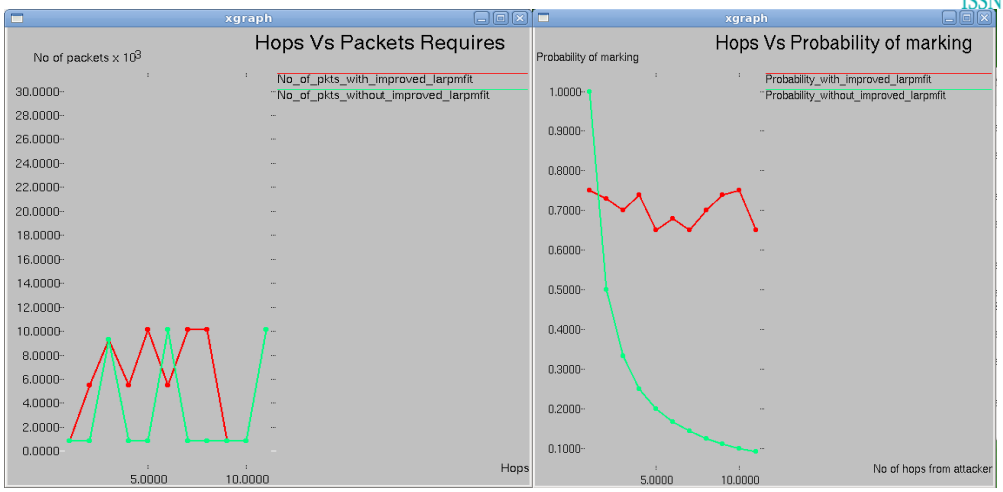
Threshold Value	**31**				
Packet Sent	25	50	60	75	100
Packet Received	25	50	60	75	100
Marked Packet	15	33	38	43	57
Unmarked Packets	10	17	22	32	43
Tracing Possible	NO	NO	YES	YES	YES

From the results in Table above it is seen that traceback is possible for different set of packets with threshold values of 20, 25 and 31 using the SPMT algorithm. It can also be observed from the results in Table that on an average about 65-75% of the packets received at the destination are marked. This proves the marking efficiency of the algorithm.

V. GRAPHICAL RESULTS OF SIMULATION







VI. CONCLUSION

The DoS and DDoS attacks on the networks are increasing and the result in the performance of network is decreasing. Most of the existing packet marking techniques (for IP traceback) requires many packets to traceback the source. They also have drawbacks such as packet header overload, network overhead, router overhead, etc. Hence in order for traceback mechanism to be efficient in tracing, it should take minimum number of packets from the attacker to perform IP Traceback.

Thus, a mechanism (SPMT) that takes few or less packets and avoids all the possible overheads on packet, router, and/or network is proposed for an efficient traceback of the origin of the attack. Further, the techniques also provide a solution to mitigate the DoS and/or DDoS attacked on the network.

REFERENCES

[1] Swapnil M. Sanap, and Pranav Pawar; March 2015 “Overview of ip tracebacking using packet marking techniques”, ICACEA, 2015, IEEE transaction.

[2] Savage, Stefan; D. Wetherall, A. Karlin, and T. Anderson (2000), "ACM SIGCOMM", Stockholm, Sweden. Retrieved 2008-11-18.

[3] Shui Yu; 2014 “Attack Source Traceback”, Springer Briefs in Computer Science, PP 55-75.

[4] Song, Dawn; A. Perrig (2001) “"Advanced and Authenticated Marking. Schemes**for** IP Traceback"” INFOCOM 2001. pp. 878–886. Retrieved 2008-11-23.

[5] Belenky, Andrey; Nirwan Ansari (2007), "On deterministic packet marking". Computer Networks: the International Journal of Computer and Telecommunications Networking 51 (10): 2677–2700. doi:10.1016/j.comnet.2006.11.020.

[6] Shokri, Reza; A. Varshovi; H. Mohammadi; N. Yazdani; B. Sadeghian (September 13–15, 2006), “ DDPM: Dynamic Deterministic Packet Marking for IP Traceback”, IEEE International Conference on Networks, Singapore. pp. 1–6.

[7] Snoreren, Alex C.; C. Partridge; L. A. Sanchez; C. E. Jones; F. Tchakountio; B. Schwartz; S. T. Kent; W. T. Strayer (2002), “Single-packet IP traceback”, IEEE/ACM Trans. Netw. 10 (6): 721–734. doi:10.1109/TNET.2002.804827

[8] Hazeyama, Hiroaki; Y. Kadobayashi, D. Miyamoto and M. Oe (June 26–29, 2006), "An Autonomous Architecture for Inter-Domain Traceback across the Borders of Network Operation", Proceedings of the 11th IEEE Symposium on Computers and Communications, Cagliari, Sardinia, Italy. pp. 378–385.

[9] A. Karlin. S.Savage, "Practical Network Support for IP Traceback:, ACM SIGCOMM, pages 295-306, 2000.

[10] J. Postel, Internet protocol, "Internet Protocol", RFC 791, Internet Engineering Task Force, Sept. 1981.

[11] C.Partridge A.C.Snoeren and C.E.Jones, "Hash-based IP Traceback", ACM SIGCOMM, 2001.

[12] A. Perrig A.Yaar and D. Song., against IP Spoofing and DDoS Attacks. Technical Report, CMU, 2003.