Journal of Computer Science 4 (8): 646-651, 2008
ISSN 1549-3636

Multi Directional Geographical Traceback with n Directions Generalization

[1]S. Karthik, [2]V.P. Arunachalam and [3]T. Ravichandran
[1,2] SNS College of Technology, Sathy Main Road, Coimbatore-641035, Tamil Nadu, India
[3]Hindustan Institute of Technology, Coimbatore-641032, Tamil Nadu, India

Abstract: Problem Statement: Denial of Service/Distributed Denial of Service (DoS/DDoS) attacks deny regular, internet services from being accessed by legitimate users, either by blocking the services completely, or by disturbing it completely, so as to cause customer baulking. **Approach:** Several traceback schemes were available to mitigate these attacks. Directional geographical traceback8 (DGT8), directional geographical trackback scheme, with 8 directions was one of them. Having a limited set of 8 directions, DGT8 may not work for routers with more than 8 interfaces. In this study, we had proposed Multi-DGT (DGT-16), a 16 directional geographical traceback scheme having all the advantages of DGT. The 16 directions, though not having exactly equal interface, had nearly equal measures and were identified using a novel scheme of Segment Direction Ratios (SDR). **Results:** The scheme of DGT16 SDR in directions D1-D16 in quadrant I-IV and DGT32 SDR in directions D1-D9 in quadrant I were examined. **Conclusion:** The implementation of DGT16, when a packet arrives at the victim, the geographical location of the attack router can be obtained from the data in the SDR subfields, regardless of the source IP address which may be incorrect or compromised.

Key words: DoS, DDoS, Directed Geographical Traceback (DGT), IP traceback, Segment Direction Ratio (SDR)

INTRODUCTION

A Denial of Services attack (DoS) is an attempt to prevent legitimate users of a service, from using that service. DoS attacks are essentially, resource overloading attacks and either crash the communication system of the host with the rest of the Network or degrade the host's service rendering it unavailable for legitimate users. A DDoS attack, in general, consumes the target's resources, so that it cannot provide service. The resource is either an internal host resource on the target system or data transmission capacity in the local network.

IP traceback is the process of identifying the actual sources of attack packets. This has the benefit of holding attacker accountable for abusing the internet. It helps in mitigating DoS attacks by isolating identified attack sources. To abort these attacks, many IP traceback schemes[1,6] have been advocated.

Broadly they can be categorized into 3 groups: those which reconstruct the entire attack path the attack packets have traversed[2-4], such as Probability Packet Marking (PPM); those which focus only on the sources of attack packets, irrespective of the path taken[5], such as Deterministic Packet Marking (DPM) and the third is the Directed Geographical Traceback (DGT) and geographical mapping techniques[1,7].

The DGT Scheme of[1] possesses many desirable features such as fast convergence, light weight, good scalability and attack mitigation capability.

The DGT Scheme of[1] considers only 8 directions and may not work well for Routers that have more than 8 interfaces. In this study, we are generalizing the DGT scheme to 16 interfaces of nearly equal measures.

By the novel scheme of Segment Direction Ratios (SDR), the 16 directions are identified by their SDR and every Router need know only the SDR of its immediate neighbors.

The rest of this study is organized as follows. The traceback mechanisms are discussed in IP Traceback. The description of Segment Direction Ratios (SDR) is introduced in Concept of SDR. The SDR of scheme DGT 16 are presented together with the assumptions of DGT is explained in DGT16 procedure. Storage formalities are discussed in Encoding Requirements of Materials and Methods. Finally Comparison of DGT16 with other traceback schemes, Qualitative comparison with other schemes and the limitations of DGT 16 are described. Generalization to DGT 2^n is discussed in results and discussion followed by the conclusion.

Corresponding Author: S. Karthik, Department of Computer Science and Engineering, SNS College of Technology, Sathy Main Road, Coimbatore-641035, Tamil Nadu, India Tel: +91-422-2669118/+91-9842720118

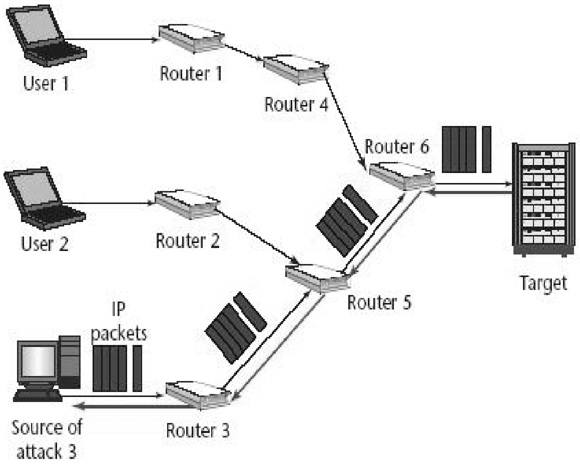

Fig. 1: Link testing or hop-by-hop testing

IP traceback: IP traceback is the process of identifying the source machines/nodes that generate the attack traffic and detecting the path traversed by the malicious DDoS traffic. Traceback primarily depends on packet marking (augmenting packets with partial path information) and packet logging techniques (storing packet digest/signature at intermediate routers). Savage *et al*.[10] IP traceback is complicated by various factors which include the distributed anonymous nature of DDoS attacks, stateless nature of the Internet, destination oriented IP routing and the millions of hosts connected to the Internet. The traceback mechanisms fall into four main categories:

- Link testing-hop-by-hop tracing
- Messaging (ICMP based trace back)
- Logging
- Packet marking

Link testing or hop-by-hop tracing: As shown in Fig. 1 Method tests the network link between routers to determine the origin of the attacker's traffic. Method starts from router closest to the victim and tests the incoming links to determine which link caries the malicious packets. Process is repeated on upstream routers until source node is identified. Drawback: attack should remain active until trace is completed. Link testing approaches:

- Input debugging
- Controlled flooding

Messaging (ICMP based traceback): ICMP messages are generated by the router and sent along with the network traffic to the victim/destination machine. These messages contain partial path information, including information about where the packet came from, where it was sent and its authentication as Shown in Fig. 2. This information is used by the victim to trace the path of a packet to its originating source node.

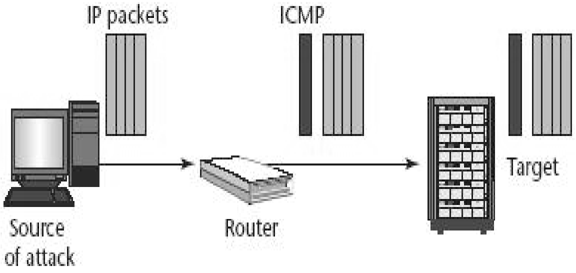

Fig. 2: ICMP based traceback messaging

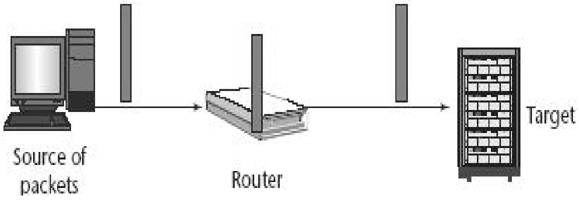

Fig. 3: Logging

Logging: As packets traverse the network towards the destination victim, they are logged at the key routers. This information is analyzed using data mining techniques to extract information about the traffic sources as shown in Fig. 3.

Packet marking: In packet marking method traceback data is inserted into the IP packet by the routers on the path to the destination node. Packet marking information stored in identification field of IP header. Types of packet marking are PPM-Probabilistic packet marking and DPM-Deterministic packet marking

Probabilistic packet marking: As Shown in Fig. 4 Focuses on reconstructing the entire attack path the malicious packets have traversed. Routers put stamps into packets with a fixed probability and victim reconstructs attack path from these stamps.

Packets are marked with partial path information as they arrive at the routers. This approach exploits the observation that attacks generally comprise large number of p. while each marked packet represents only partial path it has traversed, by combining a modest number of packets a victim can reconstruct the entire path.

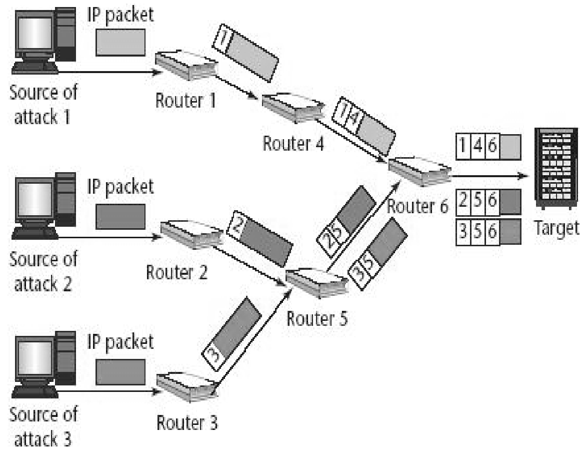

Fig. 4: Packet marking

Advantages:

- Victim can locate the approximate source of attack traffic without the assistance of outside network operators
- This determination can also be done even after the attack has stopped

Deterministic packet marking: Focuses only on the sources of the malicious packets, no matter which path the malicious packets take to attack the victim Each packet is marked when it enters the network. This mark remains unchanged as long as the packet traverses the network. Incoming packet is marked by the interface closest to the source of the packet on an edge ingress router. Marking is done deterministically.

MATERIALS AND METHODS

The concept of SDR: We assume a two dimensional square grid with Routers at selected grid points[1]. The edge between 2 routers is thus a line in two dimensions whose directions are specified by its direction cosines (Cosα, Cosβ), where α, β are the angles made by the edge with positive E and N directions (Fig. 5). Direction cosines satisfy Cos2 α + Cos2 β = 1, always.

Since most Cosθ values are cumbersome rationals and irrationals in [-1, 1], the concept of direction ratios (d.r) was introduced. Direction ratios (d.r) are proportional quantities to Direction cosines (d.c); are integers, denoted by (a,b) where in general a2 + b2 ≠ 1. From direction ratio (a, b) we can get the directional cosine (cosα, cosβ) as (a/r, b/r) where $r = \sqrt{a^2 + b^2}$. In Fig. 5, the direction ratios of the line are (2, 1), from which we can recover the dc as (2/√5, 1/√5).

By segment, we mean the edge between 2 adjacent routers, with coordinates (x1, y1), (x2, y2) with suitable origin Oand OE, ON as axes of reference.

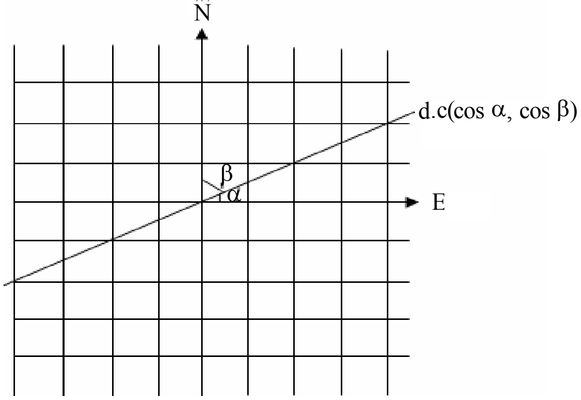

Fig. 5: Square grid where an edge line has d.c (Cos α, Cos β)

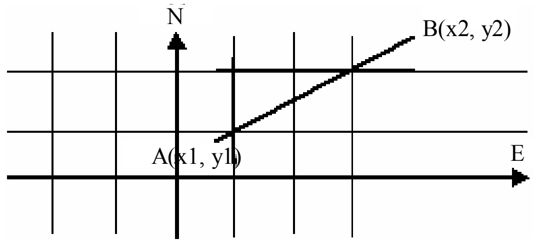

Fig. 6: For edge AB between routers at A, B with SDR (x2-x1, y2-y1) = (2, 1)

The coordinates are in units of the grid size. If AB is the edge joining 2 routers A, B with coordinates of A (x1, y1) and B(x2, y2) then SDR (Segment Direction Ratio) of AB are defined as (x2-x1, y2-y1) where |x2-x1|, |y2-y1| ≤ 2 and co primes (Fig. 6). In general for DGT of 2n directions we handle SDR with |x2-x1|,|y2-y1| ≤ (n-2)and co primes for n ≥ 3.

It is easy to see that (x2-x1), (y2-y1) are only the grid steps to be taken in ±OE, ±ON directions (depending on the sign of SDR), to reach B from A. They are the projections of the edge AB on OE, ON with appropriate sign attached.

Figure 7, shows the 16 directions D1, to D16 (where D1 = OE, D5: = ON directions) with their SDR in bits.

The SDR of DGT 16 are given as ordered 2 bits with appropriate sign. It is easily verified that for such SDR (a, b); (a,-b), (-a, b), (-a, -b) are also SDR.

The assumptions of DGT2n for n≥4 are the same as in DGT8. The following basic assumptions are standard:

- Any number of packets can be generated by an attacker
- Attackers are aware of trace attempts on them

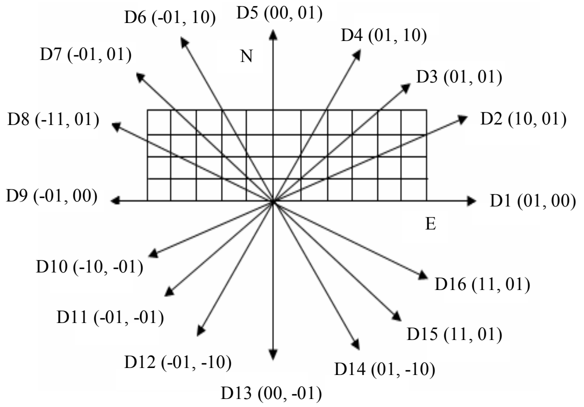

Fig. 7: DGT 16 SDR

- The routing behavior may be unstable
- Circuits routing is not there
- A router knows the SDR of its neighboring routers in one of the 2n directions (n≥4). Specifically for n = 4, in the 16 directions D1-D16

Most of these assumptions are common to traceback schemes of one type or the other.

DGT16 procedure: When a packet arrives at router Ri and is destined for router Rj where the direction Dij, is one of D1-D16 the only task that Ri, has to perform is to add the ordered SDR values of Dij, to the corresponding ordered subfields in the IP header and subtract 1 from the TTL value.

Thus for the implementation of DGT16, we require 2 subfields in the IP header, to keep track of the cumulative grid step movements, from router to router, through their SDR.

In this way, when a packet arrives at the victim, the geographical location of the attack router can be obtained from the data in the SDR subfields, regardless of the source IP address which may be incorrect or compromised.

Encoding requirements: Assuming that the length of internet paths seldom exceed 32 hops, the cumulative SDR value cannot exceed in magnitude, the integer 64, for DGT16. Hence 2 (1+7) = 16 bits are needed in the IP header for the CSDR totals.

To calculate the total number of hops between the attack router and the victim router, as the difference of initial TTL value and the final TTL value, we need to store the initial TTL value in the IP header.

Assuming that the IP header has (16+8+1) 25 bits, for DGT 16, we use the 8 bit segment for storage of initial TTL value.

Location of the attacker and the hop count enables the victim to process the traceback.

Comparison of DGT 16 with other traceback schemes:

Comparison with DGT 8: DGT16 and DGT8 being like schemes, offer equivalent advantages with respect to computational burden, scalability and mitigation capability of the attack, except for the fact that 16 directions are available now, with nil or negligible additional computations.

.

Specifically DGT2n restricts SDR of **Qualitative comparison with other schemes like PPM and SPIE:** DGT, PPM and SPIE being different types of trackback schemes only qualitative comparison is possible[1]. The inferences are same as those reported in[1] with respect to computational, scalability and capability parameters.

Limitations of DGT16: A limitation of DGT16 is the inequality (though marginal) among the interfaces. This is the cost we have to pay to satisfy the integer requirements of the SDR and generalization to DGT2n.

RESULTS

The concept of SDR allows us to extend the DGT 16-DGT2n for n>4, without any restriction, in an elegant manner.

The only additional requirement that arises is the increased CSDR upper limits and consequently more bits in the neededsegment joining grid points A (x1, y1) and B (x2, y2) to the constraint of |x2-x1|, |y2-y1| being co primes and satisfying.IP header, for the 2 subfields, are

|x2-x1|, |y2-y1 |≤n -2, (n≥3) and imparts a corresponding increased requirement for the two CSDR maximum totals for an optimal 32 hop situation.

The SDR of the DGT32 scheme are given below. These SDR with first or second or both components changed in sign give the SDR of the remaining directions, in quadrants II, IV and III respectively (Fig. 8).

Ultimately the number n of scheme DGT 2^n, depends solely on the IP header bit capacity as is evident from the Table 1.

Table 1: DGT 2n specifications

n	2n	SDR bit length	Max step moves	Max CSDR value	IP header CSDR length
3	8	1	1	32	2 (1+6)
4	16	2	2	64	2 (1+7)
5	32	2	3	96	2 (1+7)
6	64	4	4	128	2 (1+8)

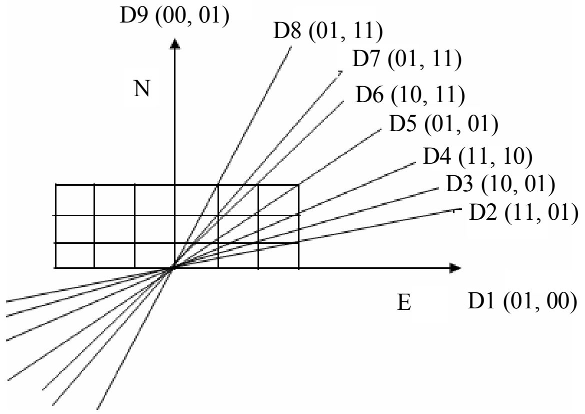

Fig. 8: DGT32 SDR in the directions D1-D9 in quadrant I

DISCUSSION

The Internet has transformed from an information repository to a vital channel for conducting business. Unfortunately, with this positive change has come an increased frequency in malicious attacks[8]. All the proposed traceback schemes have their own specific advantages and disadvantages. Currently, no single solution could fulfill all the requirements outlined for an effective trace-back method[9]. For any of these IP traceback solutions to be effective, they would need to be deployed across corporate and administrative boundaries in a substantial portion of the Internet infrastructure. This in itself seems to be one of the biggest obstacles to a unified approach to IP traceback. Also, some measures are ineffective against DDoS attacks, are resource intensive, cause network overhead and cannot be used for post-attack analysis.

CONCLUSION

One conclusion we can draw from this is that unless IP traceback measures are deployed all over the Internet, they are only effective for controlled networks than for the Internet. The researchers are working towards to extend this multidirectional geometrical two dimensional traceback scheme to three dimensions.

ACKNOWLEDGEMENT

The researcher would like to thank Dr. S.N. Subbramanian, Director cum Secretary, Dr. S. Rajalakshmi, Correspondent, SNS College of Technology, Coimbatore for their motivation and constant encouragement. The author would like to thank Dr.V.P.Arunachalam, Principal cum Research Supervisor and Dr. T. Ravichandran, Joint Supervisor for critical review of this manuscript and for his valuable input and fruitful discussions. Also, he takes privilege in extending gratitude to his family members and friends who rendered their support throughout this research work.

REFERENCES

1. Zhiqiang Gao and Nirwan Ansari, 2005. Directed geographical traceback. Proceeding of the 3rd International Conference on Information Technology: Research and Education, June 27-30, IEEE Xplore Press, USA., pp: 221-224. DOI: 10.1109/ITRE.2005.1503108.
2. Savage, S., A. Karlin, T. Anderson and D. Wetherall, 2001. Network support for IP traceback. IEEE/ACM Trans. Network., 9: 226-237. DOI: 10.1109/90.929847.
3. Songand, D.X. and A. Perrig, 2001. Advanced and authenticated marking schemes for IP traceback. Proceedings of the IEEE 20th Annual Joint Conference on Computer and Communications Societies, Apr. 22-26, Anchorage, AK., USA., pp: 878-886. DOI: 10.1109/INFCOM.2001.916279.
4. Yaar, A., A. Perrig and D. Song, 2005. FTT: Fast internet trackback. Proceedings of the 24th Annual Joint Conference on Computer and Communications Societies, Mar. 13-17, IEEE Xplore Press, USA., pp: 1395-1406. DOI: 10.1109/INFCOM.2005.1498364.
5. Basheer Al-Duwairi and Manimaran Govindarasu, 2006. Novel hybrid schemes employing packet marking and bagging for IP Traceback. IEEE Trans. Parall. Distribut. Syst., 17: 403-418. DOI: 10.1109/TPDS.2006.63.
6. Al-Duwairi, B. and T.E. Daniels, 2004. Topology based packet marking. Proceedings of the 13th International Conference on Computer Communications and Networks, Oct. 11-13, Chicago, IL., pp: 146-151. DOI: 10.1109/ICCCN.2004.1401609.
7. Padmanaban, V. and L. Subramanian, 2001. An investigation of geographic mapping technologies for internet hosts. Proceedings of the 2001 Conference on Applications, Technologies, Architectures and Protocols for Computer Communication, 2001, ACM Press, New York, USA., pp: 173-185. http://portal.acm.org/citation.cfm?id=383073.
8. Cisco, 2008. Strategies to Protect Against Distributed Denial of Service Attacks. http://www.cisco.com/en/US/tech/tk59/technologies_white_paper09186a0080174a5b.shtml.

9. Meadows, C., 1999. A formal framework and evaluation method for network denial of service. Proceedings of the 12th IEEE Workshop on Computer Security Foundations, June 28-30, IEEE Computer Society, Washington, DC., USA., pp: 4-4. http://portal.acm.org/citation.cfm?id=795127.

10. Savage, S., D. Wetherall, A. Karlin and T. Anderson, 2000. Practical network support for IP traceback. ACM SIGCOMM Comput. Commun. Rev., 30: 295-306. http://portal.acm.org/citation.cfm?id=347057.347560.