16- Directional Geographical Traceback (DGT16) with Generalization to $2^n$ (n>4) Directions

A. RAJIV KANNAN1*, J. RAJAVEL2**, Dr. K. DUARAIWAMY3***, Dr. K. THIYAGARAJAH4**** and V. SURESH5*****

Abstract

DoS / DDoS (Distributed Denial of Service) 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. Several traceback schemes are available to mitigate these attacks. DGT8, directional geographical traceback scheme [1], with 8 directions is one of them.

Having a limited set of 8 directions, DGT8 may not work for routers with more than 8 interfaces. In this paper, we propose DGT 16, a 16 directional geographical traceback scheme having all the advantages of DGT. The 16 directions, though not having exactly equal interface, have nearly equal measures, and are identified using a novel scheme of Segment Direction Ratios (SDR). The SDR concept and the associated marking scheme allow the victim to defend against DDoS attacks independent of its ISP and also the generalization to DGT$2^n$, having $2^n$ directions (n>4).

Index terms: - DoS, DDoS, DGT (Directed Geographical traceback), IP traceback, SDR (Segment Direction Ratio).

1. 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 paper, 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 paper is organized as follows. The concept of Segment Direction Ratios (SDR) is introduced in section II. The SDR of scheme DGT 16 are presented in section III, together with the assumptions of DGT. In section IV DGT16 procedure is explained. Storage formalities are discussed in section V. Qualitative comparison with other schemes and the limitations of DGT 16 constitute section VI. Generalization to DGT 2^n is discussed in VII. VIII constitute the Conclusion.

II. The Concept of SDR

As in [1], we assume a two dimensional square grid with Routers at selected grid points. The edge between 2 routers is thus a line in two dimensions whose directions are specified by its direction cosines (Cos α, Cos β), where α, β are the angles made by the edge with positive E and N directions (refer fig.1). Direction cosines satisfy Cos^2 α + Cos^2 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 a^2 + b^2 ≠ 1. From direction ratio (a, b) we can get the directional cosine (cos α, cos β) as (a/r, b/r) where r = \sqrt{a^2+b^2}. In fig1, the direction ratios of the line are (2, 1), from which we can recover the dc as (2/\sqrt{5}, 1/\sqrt{5}).

By segment, we mean the edge between 2 adjacent routers, with coordinates (x_1, y_1),(x_2,y_2) with suitable origin O, and OE, ON as axes of reference. The coordinates are in units of the grid size. If AB is the edge joining 2 routers A, B with coordinates of A (x_1, y_1) and B(x_2, y_2) then SDR (Segment Direction Ratio) of AB are defined as (x_2 – x_1, y_2–y_1) where |x_2-x_1|, |y_2-y_1| ≤ 2 and co primes. In general for DGT of 2^n directions we handle SDR with |x_2-x_1|,|y_2-y_1| ≤ (n-2), and co primes for n ≥ 3.

It is easy to see that (x_2-x_1, y_2–y_1) 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.

Section III

Fig 3, gives 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 DGT2^n for n≥4 are the same as in DGT8.

The following basic assumptions are standard.

a. Any number of packets can be generated by an attacker.
b. Attackers are aware of trace attempts on them.
c. The routing behavior may be unstable.
d. Circuits routing is not there.
e. A router knows the SDR of its neighboring routers in one of the $2^n$ directions ($n \geq 4$). Specifically for $n=4$, in the 16 directions D1 to D16.

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

IV. DGT16 Procedure

When a packet arrives at router $R_i$ and is destined for router $R_j$ where the direction $D_{ij}$, is one of D1 to D16 the only task that $R_i$, has to perform is to add the ordered SDR values of $D_{ij}$, 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.

<table>
<thead>
<tr>
<th>n</th>
<th>SDR bit length</th>
<th>Max step moves</th>
<th>Max CSDR value</th>
<th>IP Header CSDR Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>8</td>
<td>1</td>
<td>32</td>
<td>2 (1+6)</td>
</tr>
<tr>
<td>4</td>
<td>16</td>
<td>2</td>
<td>64</td>
<td>2 (1+7)</td>
</tr>
<tr>
<td>5</td>
<td>32</td>
<td>2</td>
<td>96</td>
<td>2 (1+7)</td>
</tr>
<tr>
<td>6</td>
<td>64</td>
<td>4</td>
<td>128</td>
<td>2 (1+8)</td>
</tr>
</tbody>
</table>

V. 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

VI. Comparison of DGT16 with other traceback schemes

a) 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.

b) Qualitative comparison with other schemes like PPM and SPIE

DGT, PPM and SPIE being different types of traceback schemes only qualitative comparison is possible [1],

The inferences are same as those reported in [1] with respect to computational, scalability and capability parameters.

c) 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 DGT2$^n$.

Table I. DGT $2^n$ Specifications

VII. Generalization to DGT2$^n$ ($n>4$)

The concept of SDR allows us to extend the DGT 16 to DGT2$^n$ 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 IP header, for the 2 subfields, are needed.

Specifically DGT2$^n$ restricts SDR of segment joining grid points A ($x_1,y_1$) and B ($x_2,y_2$) to the constraint of $|x_2-x_1|$, $|y_2-y_1|$ being co primes and satisfying.

$|x_2-x_1|$, $|y_2-y_1|$ $\leq$ n -2, (n $\geq$ 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.4 DGT32 SDR in the directions D1 to D9 in quadrant I](image)

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

VIII. Conclusion

The authors are working towards to extend this multidirectional geometrical two dimensional traceback scheme to three dimensions.

IX. References

of Computer Science and Engineering at K.S.Rangasamy College of Technology, Anna Univ. since 2006. His research interest includes Computer Networks and Network Security.

V.Suresh received the M.Sc. degree from Periyar Univ. in 2002. After working as a lecturer (from 2002 to 2006) at K.S.R. College of Engineering, Anna Univ., and he has been doing M.E (CSE), at K.S.R. College of Engineering affiliated to Anna University. His research interest includes Network Security, Operating Systems, DBMS, Image processing, Mobile Computing and Nano Technology.