A Novel Direction Ratio Sampling Algorithm (DRSA) Approach for Multi Directional Geographical Traceback

Karthik.S kkarthikraja@yahoo.com
Research Scholar, Professor and Head,
Department of Computer Science Engineering
SNS College of Technology,
Coimbatore-641035, Tamil Nadu, India.
Telephone: +91-422-2669118, Mobile: +91-9842720118
.

Dr.V.P.Arunachalam vp_arun@yahoo.com
Principal and Research Supervisor,
SNS College of Technology,
Coimbatore-641035, Tamil Nadu, India.

Dr.T.Ravichandran dr.t.ravichandran@gmail.com
Principal and Joint Supervisor,
Hindustan Institute of Technology
Coimbatore-641032, Tamil Nadu, India.

Abstract

An important and challenging problem is that of tracing DOS/DDOS attack source. Among many IP Traceback schemes, a recent development is DGT (Directed Geographical Traceback). Though multidirectional two dimensional DGT schemes are available, ξξξin the real scenario, three dimensional, Multidirectional DGT has potential applications. The direction ratio algorithm[DRA] has the limitation of the impossibility of ensuring sufficient unused space in the packet header for the complete DRL (Direction Ratio List) especially when the length of the path is not known apriori. In this paper that limitation is overcome using DRSA(Direction Ratio Sampling Algorithm) which works well for Three dimensional, Multi-Directional, Geographical IP traceback. This approach enables the attack path reconstruction easily possible. In conclusion, DRSA is a robust scheme of attack path reconstruction in geographical traceback.

Keywords: DOS (Distributed Denial of Service), DGT (Directional Geographical Traceback), 3DMDGT (Three dimensional, Multi-Directional Geographical Traceback), DRA (Direction Ratio Algorithm), DRSA (Direction Ratio Sampling Algorithm).

1. INTRODUCTION

DOS attacks [14],[17] represent a growing threat to the internet infrastructure, by denying regular internet services from being accessed by legitimate users. IP traceback is the process of identifying the actual source(s) of attack packets[12], So that the attackers can be held accountable as also in mitigating them, either by isolating the attack sources or by filtering packets for away from the victim[18],[19], Several IP traceback schemes have been proposed to solve this problem.

DGT (Directed Geographical Traceback) scheme exploits the potential of the geographical topology of the internet for traceback. Z.hao gave a limited two dimensional, 8 directional DGT scheme. This was generalized by Rajiv etc.,[2], to 2n ($n \geq 4$) directions, though only in 2 dimensions. Considering the spherical / Ellipsoidal topology of the earth, it is clear that the internet path is 3 dimensional in nature. In this paper, 3 dimensional, Multidirectional, Geographical Traceback, through DRSA (Direction Ratio Sampling Algorithm) is proposed.

2. NORMALISED COORDINATES

Taking the geographical topology of the earth (on which all the routers are) either as the sphere

$$\xi^2 + \eta^2 + \Im^2 = a^2 \qquad (1)$$

or as the ellipsoid

$$\xi^2/a^2 + \eta^2/b^2 + \Im^2/c^2 = 1 \qquad (2)$$

then the transformation

$$ax = \xi,\ ay = \eta,\ az = \Im \qquad (3)$$

or

$$ax = \xi,\ by = \eta,\ cz = \Im \qquad (4)$$

makes (2.1), (2.2) into the unit sphere

$$x^2 + y^2 + z^2 = 1 \qquad (5)$$

for all the points on Note that(2.5), except for the points (±1,0,0), (0, ±1,0), and (0,0, ±1), we have

$$|x|, |y|, |z| < 1 \qquad (6)$$

satisfying (2.5). Thus routers R_i are at points (x_i , y_i , z_i) where

$$x_i^2 + y_i^2 + z_i^2 = 1 \qquad (7)$$

for all i. We assume that the routers are numbered serially and that the length of any internet path seldom exceeds 32 hops and hence a 10 bit field in the packet header can accommodate the last 3 digits of the router serial number, throughout its journey. All other assumptions regarding attack packets are the same as in [6].

Direction Ratios

In the dimensional space, the direction indicators[15] of a line are the direction cosines (d.c) (Cos α, Cos β , Cos r) where α, β, r are the angles which the line makes with the rectangular coordinate axes ox, oy, oz respectively. It can be shown that

$Cos2\alpha + Cos2\beta + Cos2r = 1$ (8)

For any d.c ,Since Cosθ in general is a cumbersome fraction/irrational, we use direction ratios (DR) of a line, which are proportional to d.c ; denoted by (a, b, c) where

(a, b, c) Є Z (9)

and gcd (a, b, c) = 1 (10)

(Z is the set of all integers). Though DR (a, b, c) do not, in general, satisfy

$a^2 + b^2 + c^2 = 1$ (11)

they can be made into d.c (a/r , b/r , c/r) where

$r = \sqrt{a^2 + b^2 + c^2}$ (12)

For any router R□, we can get a neighborhood direction set of DR (ai, bi ,ci)of neighbor routers Ri by taking

|ai|, |bi|, |ci| Є N (13)

Satisfying (10). (Where N, the set of naturals.) We can show that DR (n),for n Є N, the number of neighborhood direction from router R0 satisfy

(2n-1)3 < DR (n) < (2n+1)3 (14)

In fact DR(1) = 13 and DR(2) = 49 and they are listed in table 1 & 2.

Table 1: Elements of DR (1), The 13 DR are listed below,

i:	1	2	3	4	5	6
Elements of DR*(1)	(1,0,0)	(0,1,0)	(0,0,1)	(0,1,0)	(0,1,1)	(1,1,0)

i:	7	8	9	10	11	12	13
Elements of DR*(1)	(0,-1,1)	(-1,0,1)	(-1,1,0)	(1,1,1)	(-1,1,1)	(1,-1,1)	(1,1,-1)

Table 2 Elements of DR (2)

i:	1	2	3	4	5	6	7	8	9	10
DR*(2)	(1,0,0)	(0,1,0)	(0,0,1)	(0,1,1)	(1,0,1)	(1,1,0)	(0,-1,1)	(-1,0,1)	(-1,1,0)	(1,1,1)

i:	11	12	13	14	15	16	17	18	19	20
DR*(2)	(-1,1,1)	(1,-1,1)	(1,1-1)	(0,1,2)	(0,2,1)	(0,-1,2)	(0,-2,1)	(1,0,2)	(2,0,1)	(-1,0,2)

i:	21	22	23	24	25	26	27	28	29	30
DR*(2)	(-2,0,1)	(1,2,0)	(2,1,0)	(-1,2,0)	(-2,1,0)	(1,1,2)	(1,2,1)	(2,1,1)	(-1,1,2)	(1,-1,2

i:	31	32	33	34	35	36	37	38	39	40
DR*(2)	(1,1,-2)	(-1,2,1)	(1,-2,1)	(1,2,-1)	(-2,1,1)	(2,-1,1)	(2,1,-1)	(2,2,1)	(2,1,2)	(1,2,2)

i:	41	42	43	44	45	46	47	48	49
DR*(2)	(-2,2,1)	(2,-2,1)	(2,2,-1)	(-2,1,2)	(2,-1,2)	(2,1,-2)	(-1,2,2)	(1,-2,2)	(1,2,-2)

*-Direction ratios

One-to-One Correspondence between DR at a Router R0 and its Neighbor Routers Theorem

Given router R0 at (x0,y0,z0),and set of direction ratios DR(n) for some n Є N then, for each ratio di=(ai ,bi ,ci) Є DR(n),there is a unique neighbour router Ri at (xi,yi,zi) on the unit sphere is given by

$$xi = x0 + rai , \quad yi = y0 + rbi , \quad z i= z0 + rci \qquad (4.1)$$

$$\text{where } r = - \left(\frac{2(aix0+biy0+ciz0)}{ai2+bi2+ci2} \right) \qquad (4.2)$$

for i = 1,2,..........

Proof

Any point (x, y, z) on the line through router R0(x0 ,y0 ,z0) in the direction di with direction ratios(ai ,bi ,ci) is

$$x = x0+ rai , \quad y = y0+rbi , \quad z = z0 + rci \qquad (4.3)$$

and its on $x2 + y2 + z2 = 1$ (4.4)

and this value of r is unique for each i. Hence there is one-to-one correspondence between elements of DR(n) at R0 and its neighbour routers.

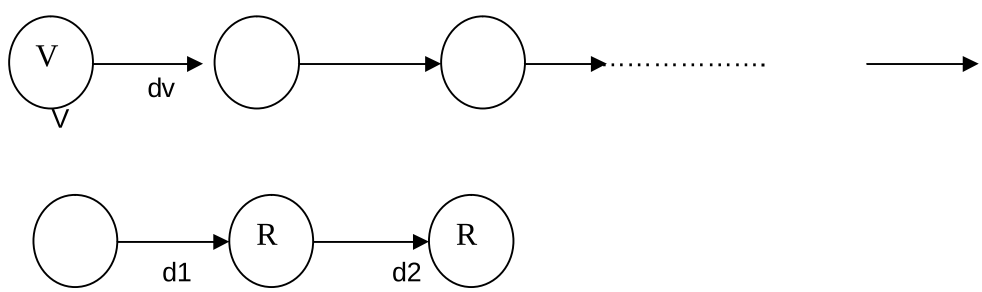
Materials and Methods

This is a theoretical paper on IP traceback problem using geographical information in three dimension in a multi-direction environment. The materials are a host of Routers Ri at points (xi,yi , zi) for i=1 to n on the earth x2+y2+z2=1. Also the internet attack packets in flight are materials whose flight path is to reconstructed for mitigating DOS/DDOS attacks.

The methods used in DRSA are random sampling methods, where, after sufficient number of samples are drawn, one can construct the path of the attack packets and trace the attack source.

DRA (Direction ratio algorithm)

In this algorithm of traceback,for every packet w arriving from the attacker at router R,we appened the DR dj=(aj ,bj ,cj) of the next destination in the packet header of w. Finally from the suffixes d0, d1, d2...........dv of w, at the victim router V,we reconstruct the path as in Fig.



Flow diagram of DRA

This is possible due to the unique (1-1) correspondence between dj (from any router from R) and its neighbors Rj.

The limitation of this DRA (direction ratio appending algorithm)is the impossibility of ensuring sufficient space in the packet header for appending the DR of every edge of the attack path.

This problem is addressed using DRSA (direction ratio sampling algorithm).

3. DRSA TRACEBACK PROCEDURE

We require an address field R, a direction ratio field DR[16], and a distance field S, in the packet header to implement this algorithm.

Assuming that the IP header has (16 + 8 + 1) = 25 bits, for DRSA, we can allot 10 bits each. For the address field, and DR Field and 5 bits for the distance field. This is acceptable since, routers are numbered serially; the 10 digit field can accommodate the last 3 digits of the serial number and is sufficient for R mod (1000). Since a 9 bit field is enough for the 4, 9 direction set of DR (2), 10 bits aare sufficient for the DR field. Since any IP path never exceeds 32 hops, a 5 bit distance field is taken at in Fig 2.

10	10	5
R mod (1000)	(a, b, c)	s
R Field (RF)	DR Field (DRF)	Distance Field (SF)

Fig 2: IP Header format for DRSA

Here is Ri: router at (xi, yi, zi) with a given serial number Dj = (aj, bj, cj) = an element of DR (2) indicating the direction ratio of the next router Rj (from Ri). Note that Ri (Rj) = Rj (the router from Ri in the direction Dj is the unique Rj since Dj is in (1 – 1) correspondence with Rj from a given Ri)

4. DRSA (DIRECTION RATIO SAMPLING ALGORITHM)

The marking procedure at a router Ri of every packet w from the attacker is as follows:

Let x be a random number in (0, 1) and p is a chosen probability level. If $x < p$, then if the packet is unmarked, then write Ri mod (1000) in RF, Dj in DRF, 0 in SF. Otherwise (if the packet is already marked) or ($x \geq p$) then only increment the distance field SF.

After sufficient number of samples are dream, then using the property Ri (Dj) = Rj and the distance field count, the attack path can be reconstructed. The victim uses the DR (along with R) sampled in these packets to create a graph leading back to the source (s) of attack.

5. CONSLUSION & FUTURE WORK

If we constrain p to be identical at each router, then the probability of receiving a marked packet from a router d hops array is p (1-p) d-1 and this function is monotonic in the distance from the victim. Because the probability of receiving a sample is geometrically smaller, the further away it is from the victim, the time for this algorithm to converge is dominated by the time to receive a sample from the further router.

We conservatively assume that samples from all of the d routers (in the path from A toV) appear with the same likelihood as the furthest router. Since these probabilities are disjoint, the probability that a given packet will deliver a sample from some router is at least dp (1-p)d-1 by addition law for disjoint events. As per the well known Coupon Collector problem [3], the number of trials required to select one of each of d equiprobable items. From (6.1) we can show that E(X) is optimal if p = 1/d (ie dE / dp = 0, d2E / d2p > 0 for p = 1/d).

For example, if p=1/d, where d= attack path length, then the victim can typically reconstruct the path after receiving E(x) = dd Ind / (d-1)d-1 packets for d=10; $E(x) \leq 75$ and hence a victim can typically reconstruct the path after receiving 75 packets from the attacker.

This same algorithm can efficiently discern multiple attacks. When attackers from different sources produce disjoint edges in the tree structure of reconstruction[13]. The number of packets needed to reconstruct each path is independent of other paths.

The limitations imposed by restricting the number of DR to /DR (2)/=49 at every stage and using R (mod 1000) instead of the full serial number of router R are marginal in nature. We need more space in the packet header to use elements of DR (3) and the full representation of the R serial number. In conclusion DRSA is a robust scheme of 3 dimensional, multi-directional, geographical IP trace back.

Acknowledgment

The author 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.

6. REFERENCES

1. Z.Gao and N.Ansari., 'Directed Geographical Traceback'., IEEE transcations., IEEE paper 221-224,2005.
2. Karthik.S. Dr.V.P.Arunachalam , Dr. T. Ravichandran, "Multi Directional Geographical Traceback "International Journal of Computer Science, 4 (8): 646-651, 2008
3. W.Filler., 'An Introduction to Probability thoery and its applications (2nd edition)., Vol I, Wiley and sons.1966
4. S Derring ; Internet protocol; Version 6(ipv6); RFC 2460; 1998
5. Computer Security Institute & Federal Bureau of investigation, CSI publication,1999 Stefan Savage etc;
6. Practical Network Support for Ip traceback', SIGCOMM 2000; Sweden.2000.
7. Rajivkannan.A, Dr.K.Duraiswamy, etc; 'Three dimensional, Multidirectional geographical traceback'; Journal of Cryptology , Springer , New York (Under Communication).
8. V.Padmanabhan etc; "Determining the geographic location of internet hosts";ACM SIGMETRICS'01; Cambridge, MA; pp 324-325, 2001,.
9. V.Padmanabhan etc; "An investigation of geographic mapping techniques for internet hosts"; ACMSIGCOMM '01, San Diego; CA; pp 173-185 , 2001..
10. P.Ferguson etc; "Network ingress Filtering Defeating DOS attacks which employ IP source address sparfing"; RFC 2267; 1998.
11. Stanford-chen.S; etc; "Holding Intruders accountable on the Internet".IEEE proceedings of symposium on security and privacy. pp 39-49; Oakland.CA ,1995.
12. Karthik.S. Dr.V.P.Arunachalam , Dr. T. Ravichandran, "A Comparative Study of Various IP Trace back Strategies and Simulation of IP Trace back" Asian Journal of Information Security pp 454-458, 2008.
13. Karthik.S. Dr.V.P.Arunachalam , Dr. T. Ravichandran "An Investigation about the Simulation of IP Traceback and Various IP Traceback Strategies" International Journal of Computer Science and Network Security, pp240-245, Vol.8, No.12, 2008.
14. Karthik.S. Dr.V.P.Arunachalam , Dr. T. Ravichandran "Analyzing Interaction between Denial of Service (DoS) Attacks and Threats" International Journal of Soft Computing, Page 68-75; 2009.
15. Karthik.S. Dr.V.P.Arunachalam , Dr. T. Ravichandran "Simulation of IP Traceback and Various IP Traceback Strategies for multi directional geographical traceback" International Journal of Intelligent Information Processing, Serials Publications, pp.123-132, 2009.
16. Karthik.S. Dr.V.P.Arunachalam , Dr. T. Ravichandran "An Investigation of 2n Direction Geographical Traceback Using Simulation of IP Traceback Strategies" CiiT International Journal of Networking and Communication Engineering,pp 110-114, 2009.
17. Rashid Hafeez Khokhar, Md Asri Ngadi , Satria Mandala "A Review of Current Routing Attacks in Mobile Ad Hoc Networks " International Journal of Computer Science and Security, volume (2) issue (3), pp 18-29, 2008.
18. Meera Gandhi, S.K.Srivatsa "Detecting and preventing attacks using network intrusion detection systems" International Journal of Computer Science and Security, Volume (2) : Issue (1), pp 49-58,2008.

19. Karan Singh, R. S. Yadav, Ranvijay "A Review Paper On Ad Hoc Network Security "International Journal of Computer Science and Security, Volume (1): Issue (1), pp 52-69, 2007.