Multi Positional Track And Multi Management Ip Traceback Using Angle Based Reckoning Sampling Process (Arsp)

V.SHYAMALADEVI
Associate Professor
Department of MCA,
KSRCT,Tiruchengode
Tamilnadu, India

Dr. R. UMARANI
Associate Professor
Department of MCA
Saradha Womens College, Salem
Tamilnadu, India

Abstract - **Distributed Denial of Service (DDoS) is a major issue for the availability of internet services. The vast number of insecure machines available in the Internet provides a fertile ground for attackers to compromise them and create attack zombies. Attack , mitigation and traceback of perpetrators is extremely difficult due to a large number of attacking machines, the use of source-address spoofing or modifying IP address and the similarity between legitimate and attack traffic. IP traceback has been proposed where one attempts to reconstruct the entire attack path, the attack packets have traversed or focusing only on the source of attack packets, no matter which path they take for assault. IP Traceback (IPT) based on the geographical information, rather than the traditional IP address information, has come to vogue. In this paper Multi positional view and Multi management IP Traceback mechanism for defense against Distributed Denial of Service attacks", has been addressed. This paper proposes a Multi dimensional representation with d(n) directions, where d(n) is the neighborhood direction ratio set generating function using the Angle based Reckoning Process (ARP) and also mitigates the Impossibility of ensuring adequate space in the packet header during its flight, by the Angle based Reckoning Sampling Process. To demonstrate the entire process and analytically simulate that the proposed mechanism react quickly blocking attack traffic while achieving high survival ratio for legitimate traffic.**

Keywords: **DDoS, Direction based Segment Ratio, ARP, ICMP, ARSP**

I. INTRODUCTION

An important and challenging problem is that of tracing DoS/DDoS attack source. IP traceback is the process of identifying the actual sources of attack, so that the attackers can be held accountable and mitigating the attacks, either by isolating the attack sources, or by filtering packets far away from the victim. The method of direction based segment ratio (DBSR) scheme to overcome the directional limitations of 2^3 DGT is proposed. A two dimensional square grid with routers at selected grid points is made. Figure 1.1 focus 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 which the line of the routers makes with axes of reference OE, ON where E is the east and N is the north direction.

$\text{Cos}^2\, \alpha + \text{Cos}^2\, \beta = 1$

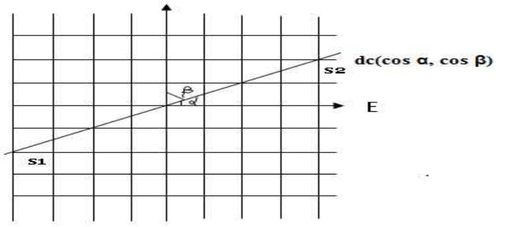


Figure 1.1 Router edge Ra Rb direction

cosines Cos α, Cos β)

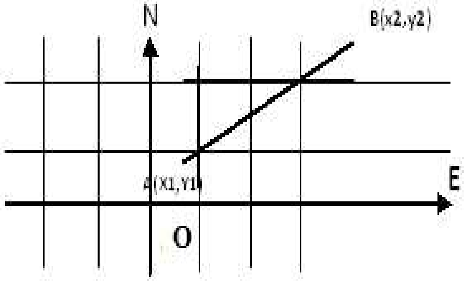


Figure 1.2 edge between routers A and B with DBSR = (x2- x1, y2- y1)

Figure 1.2 segment it can be found that the edge AB between 2 adjacent routers, with coordinate A (x_1, y_1) and B (x_2, y_2) with respect to OE, ON axes of reference. The coordinates are in units of the grid size. Direction based segment ratio (DBSR) of AB is (x_2- x_1, y_2- y_1) where | x_2- x_1 |, | y_2- y_1| ≤ 2 and co-primes. It is easy to see that (x_2- x_1, y_2- y_1) are only the grid steps to be taken in the ±OE, ±ON directions to reach B from A. They are the projections of the edge AB on OE, ON with appropriate sign attached.For the choice of | x_2- x_1 |, | y_2- y_1| ≤ 2 there are 16 directions possible called D_1 to D_{32} where D_1, D_5, D_9, D_{13} directions are respectively OE, ON, OW and OS directions. Table 1.1 also gives the summary of the DBSR bits of the 32 directions D_1 to D32.

Table 1.1 Direction 32 DBSR in decimal and binary forms

Direction	D_1	D_2	D_3	D_4	D_5	D_6
D	(0,1)	(3,1)	(2,1)	(3,2)	(1,1)	(2,3)
B	(00,01)	(11,01)	(10,01)	(11,10)	(01,01)	(10,11)
Direction	D_7	D_8	D_9	D_{10}	D_{11}	D_{12}
D	(2,1)	(1,3)	(0,1)	(-1,3)	(-2,1)	(-2,3)
B	(10,01)	(01,00)	(00,01)	(-01,11)	(-10,01)	(-10,11)
Direction	D_{13}	D_{14}	D_{15}	D_{16}	D_{17}	D_{18}
D	(-1,1)	(-3,2)	(-2,1)	(-3,1)	(0,-1)	(-1,-3)
B	(-01,01)	(-11,10)	(-10,01)	(-11,01)	(00,-01)	(-01,-11)
Direction	D_{19}	D_{20}	D_{21}	D_{22}	D_{23}	D_{24}
D	(-2,-1)	(-2,-3)	(-1,-1)	(-3,-2)	(-2,-1)	(-3,-1)
B	(-10,-01)	(-10,-11)	(-01,-01)	(-11,-01)	(-11,-01)	(-11,-01)
Direction	D_{25}	D_{26}	D_{27}	D_{28}	D_{29}	D_{30}
D	(0,-1)	(1,-3)	(2,-1)	(2,-3)	(1,-1)	(3,-2)
B	(00,-01)	(01,-11)	(10,-01)	(10,-11)	(01,-01)	(11,-10)
Direction	D_{31}	D_{32}				
D	(2,-1)	(3,-1)				
B	(11,-01)	(11,-01)				

A. Differential interface limitation

A limitation of DGT 32 is the inequality (though marginal) among the interfaces. But, this is the cost one has to pay to satisfy the integer requirements of the DBSR and for generalization to 2^n DGT. 2^n DGT scheme and its generalization below remove only the directional limitations. The dimensional limitations still exist. Specifically 2^n DGT restricts DBSR of segment joining A (x_1, y_1) and B (x_2, y_2) to the constraint $| x_2 - x_1 |, | y_2 - y_1| \leq n-2$ and co-primes. Ultimately the number n of the scheme DGT 2^n depends on the IP header bit capacity as is evident from Table 1.2. Though the directional constraint of DGT is eliminated by the concept of DBSR, the dimensional constraint remains.

Table 1.2 2^n DGT specifications

n	2^n	DBSR bit length	Max step moves on grid	Max Count DBSR value	IP header Count DBSR length
3	8	1	1	32	two(1+6)
4	16	2	2	64	two(1+7)
5	32	3	3	96	two(1+7)
6	64	4	4	128	two(1+8)

II ARP (ANGLE BASED RECKONING PROCESS)

During a packet's flight, each router appends D_i, the direction ratio of the successor router R_i from it. As it reaches the victim, from the suffix of the packet w, the Direction Ratio List (DRL) is extracted so as to spot the attacker. The serious limitation of ARP is the impossibility of ensuring adequate unused space in the packet header during its flight. This problem cannot be eliminated. It can be addressed by modifying the algorithm used. The Angle based Reckoning Sampling Process (ARSP) was proposed for managing the deficiency in packet header space.

A. ARSP Traceback Basics

It requires an address field (R), a direction ratio field (DR) 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 MRSP, 10 bits each for the address field & the DR field and 5 bits for the distance field was allotted. This is acceptable since the routers are numbered serially. The 10 bit field can accommodate the last 3 digits of the serial number and is sufficient for RN (mod 1000) where RN is the router number. Also a 9 bits are sufficient for d(2) (=49) members, and 10 bits are sufficient for the DR field. Since any IP path never exceeds 32 hops, a 5 bit distance field is sufficient and the layout is shown in Figure 2.1.

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

Figure 2.1 IP header format for ARSP

Here RN is the router number of router R_i at (x_i, y_i, z_i) and D_j is the d.r (a_j, b_j, c_j) Є d(2) of the successor router R_j from R_i. Note that R_i (D_j) = R_j and by uniqueness theorem, there is One-to-One correspondence between D_j (from R_i) and successor R_j.

B. *Angle based Reckoning Sampling Process*

The marking procedure at a router R_i of every packet w from the attacker is as follows. Let x be a random number in (0, 1) and p, a chosen probability level. If $x < p$, then if the packet is unmarked, then write RN (mod 1000) of the router in the RF, D_i in DRF, and 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 drawn, then using the property R_i (D_j) = R_j and the distance field count, the attack path can be reconstructed. The victim uses the DRF, sampled data along with RF, in these packets to create a graph, leading to the source (s) of the attack.

III PERFORMANCE ANALYSIS

If they constrain p to be identical at each router, then the probability of receiving a marked packet, from a router d hops away is $p\ (1\text{-}p)^{d-1}$ and this function is monotonic in the distance variable d from the victim. Because the probability of receiving a sample is geometrically smaller, the farther away it is from the victim, the time of this algorithm to converge is dominated by the time to receive a sample from the furthest router. Let us assume that samples from all of the d routers, in the path from A to V, appear with the same likelihood as the furthest router. Since these probabilities are disjoint i.e. mutually exclusive, the probability that a given packet will deliver a sample from some router is at least $dp\ (1\text{-}p)^{d-1}$, by addition law of mutually exclusive events. The number of trials required to select one of each of d equiprobable victims, is d (ln(d)) + O(1) Therefore, the number of packets X, required by the victim to reconstruct a path of length d, has the bounded expectation,

$$E(x) \;=\; \frac{\ln(d)}{p(1-p)^{d-1}}$$

(2.1)From (2.1) it is known that E(x) is optimally minimum for

$$p=\frac{1}{d} \text{ Since } \frac{dE}{dp}=0 \text{ and } \frac{d^2E}{dp^2}>0 \text{ for } p=\frac{1}{d}p\ .$$

Thus min $(E(x))=\dfrac{d^2\ln(d)}{(d-1)^{d-1}}=k$

for $p=\frac{1}{d}$, where d is the attack path length and hence the victim can typically reconstruct the path after receiving k packets. For d =10, $k \leq 75$ and hence the victim can typically reconstruct the path after receiving 75 packets from the attacker. This same algorithm can discern efficiently, multiple attacks also. When attackers from different sources, produce disjoint edges in the tree structure of reconstruction, the number of packets needed to construct each path is independent of other paths. The limitations imposed by restricting the number of directions at a router to d(2) at every stage and using RN (mod 1000) instead of the full serial number of the router are marginal in nature. Hence ARSP is a robust scheme of Multi position viewed and Multi management IP Traceback.

IV DEPLOYMENT

The scale of a DDoS network is too large to be recreated in a simulation environment and hence an attack topology was designed to allow variations in a number of different dimensions. The number of attacking machines in a DDoS attack was varied between one to six attack nodes. The distance between the source attack machine and the targeted victim was varied from a minimum of three hops to a maximum of 12 hops with a Connection Delay of 1sec per hop. Intermediate routers in the network were set to default CISCO generic type and switches were of either manageable or auto configurable types. The Bandwidth was automatically configured by the packet tracer to its default value. Both Routing Information Protocol (RIP1) and ICMP were used as the Supportive protocol. The Topologies used in the depicted network involved star, mesh, hybrid, tree, ring and bus. The range of the Attack Level was categorized as low, medium and high depending on the volume of packet generated and sent to the victim machine.

A. *Simulation Topology 1*

Due to the large volume of packets and the scale of the network involved in a DDoS attack, it is highly difficult to simulate a complete DDoS attack scenario in any simulator. This article utilizes three different environments involving a simplified topology to demonstrate the effectiveness of the proposed mechanisms rather than a depiction of a complete DDoS attack. Figure 4.1 shows the first topology with one attack source machine and a victim with 3 generic intermediate routers and 2 manageable switches placed on a 16 directional and 2 dimensional grid environment. The star topology is used with a 3 hop distance from source to victim. The bandwidth was auto configured with a default connection delay of 1 sec/hop. As the packet is forwarded through the depicted network, the DGT enabled routers mark the packet with the traceback information in the ID field of the IP header of the packet. In Figure 4.1, If R14(Router 14), R16(Router 16) is the edge joining 2 routers R14, R16 with coordinates of R14(x1, y1) and R16(x2, y2) then SDR (Segment Direction Ratio) of R14, R16 are defined as (x2 - x1, y2 - y1) where $|x2-x1|, |y2-y1| \leq 2$ and co primes. In general for DGTof 2^n directions we handle SDR with $|x2-x1|, |y2-y1| \leq (n-2)$, and co primes for $n \geq 3$. It is easy to see that (x2 - x1), (y2 - y1) are only the grid steps to be taken in ± OE, ± ON directions, to reach R16 from R14. They are the projections of the edge R14, R16 on OE, ON with appropriate sign attached. Figure 4.2 shows the Second topology comprising an attack scenario with two simultaneous attack sources and a victim. 3 CISCO generic intermediate routers and 2 manageable switches were placed on a 16 directional and 2 dimensional grid environment. The star topology is used with a 3 hop distance from Source 1 (PC5) to Victim and a 4 hop distance from Source 2 (PC9) to Victim.

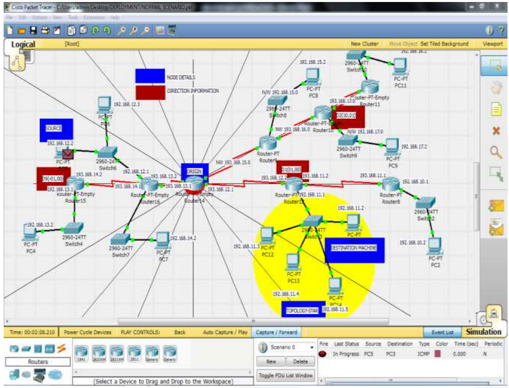


Figure 4.1 source machine and destination machine

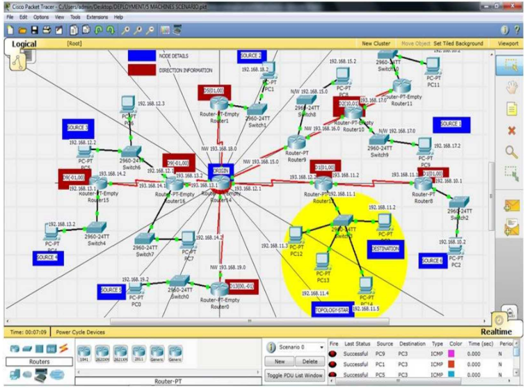
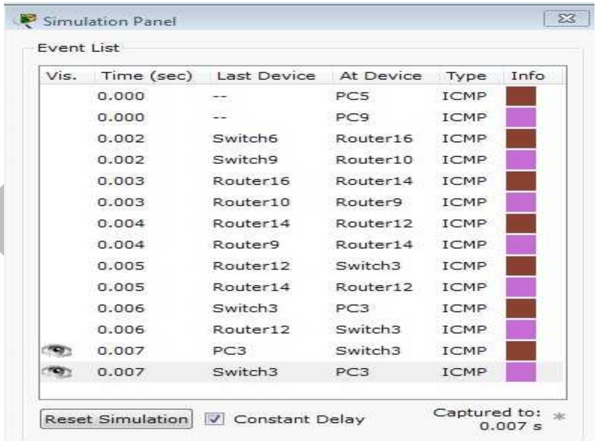


Figure 4.2 comprising an attack scenario with different simultaneous attack sources and a victim

The bandwidth was auto configured with a default connection delay of 1 sec/hop ICMP was again used as the support protocol to analyze the path traversed by the packet in the simulator. Figure 4.3 shows the details of two packets traversing from source machines PC5 and PC9 to victim machine PC3 determined using the ICMP support protocols.



Simulation Panel

Event List

Vis.	Time (sec)	Last Device	At Device	Type	Info
	0.000	--	PC5	ICMP	🟫
	0.000	--	PC9	ICMP	🟪
	0.002	Switch6	Router16	ICMP	🟫
	0.002	Switch9	Router10	ICMP	🟪
	0.003	Router16	Router14	ICMP	🟫
	0.003	Router10	Router9	ICMP	🟪
	0.004	Router14	Router12	ICMP	🟫
	0.004	Router9	Router14	ICMP	🟪
	0.005	Router12	Switch3	ICMP	🟫
	0.005	Router14	Router12	ICMP	🟪
	0.006	Switch3	PC3	ICMP	🟫
	0.006	Router12	Switch3	ICMP	🟪
👁	0.007	PC3	Switch3	ICMP	🟫
👁	0.007	Switch3	PC3	ICMP	🟪

Reset Simulation ☑ Constant Delay Captured to: 0.007 s

Figure 4.3 The packet details at victim for the next topology

Packet leaves Source machine 1 - PC 5 at 0.000s. Packet from Source machine 1 - PC 5 passes through Switch 6 at 0.001s and reaches Router 16 at 0.002s. From Router 16 the packet is forwarded to Router14 at 0.003s From Router 14 the packet is then forwarded to router12 at 0.004s. From Router 12 the packet finally reaches Switch 3 at 0.005s. From Switch 3 the packet finally reaches PC 3 at 0.006s. Similarly the packet from Source machine 2 - PC9 traverses through Switch9 to Switch3 with four intermediate hops at Router10, Router9, Router14 and Router12 and finally reaches PC3 at 0.007s from Switch3. Figure 6.10 also shows the start of the return packet from PC3 to PC5 being sent to Switch3 at 0.007s.

B. *Simulation Topology 2*

Figure 4.4 shows the Third topology comprising an attack scenario with six simultaneous attack sources - PC0, PC1, PC2, PC4, PC5 and PC9 and a victim PC3. Here eight CISCO generic intermediate routers and 12 Manageable switches were placed on a 16 directional and 2 dimensional grid environment. The star topology is used with different hop distances from source to victim. The bandwidth was auto configured with a default connection delay of 1 sec/hop. The simulation was run for 200 seconds with different attack rate (number of packets sent per second) for the six source machines. ICMP was used as the support protocol. Figure 4.5 shows six packets being sent from the six source machines and the packets reaching the switches at 0.001s. The complete simulation panel shown gives the details of the actual path traversed by the packet from source to destination. Figure 4.6 shows the details of the packets from 6 Source machines traversing the various components in the network and reaching the Victim machine PC3.

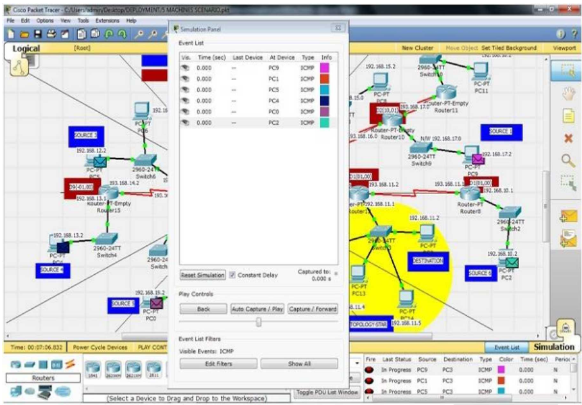
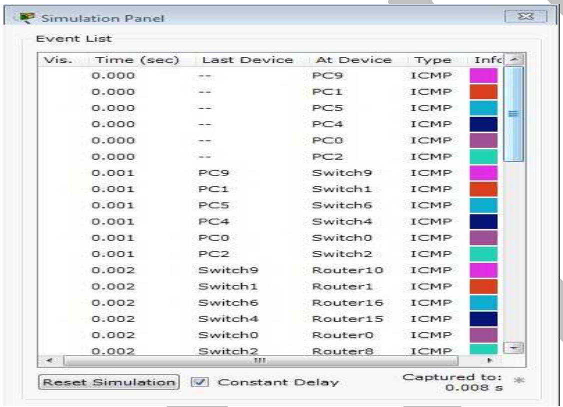


Figure 4.4 The third topology with 6 attack source machine and a victim



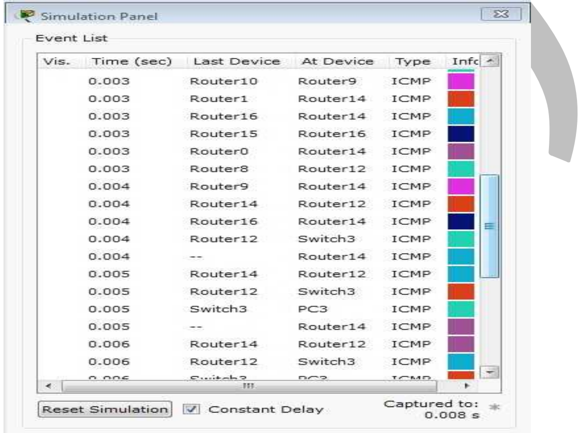
Simulation Panel

Event List

Vis.	Time (sec)	Last Device	At Device	Type	Infc
	0.000	--	PC9	ICMP	■
	0.000	--	PC1	ICMP	■
	0.000	--	PC5	ICMP	■
	0.000	--	PC4	ICMP	■
	0.000	--	PC0	ICMP	■
	0.000	--	PC2	ICMP	■
	0.001	PC9	Switch9	ICMP	■
	0.001	PC1	Switch1	ICMP	■
	0.001	PC5	Switch6	ICMP	■
	0.001	PC4	Switch4	ICMP	■
	0.001	PC0	Switch0	ICMP	■
	0.001	PC2	Switch2	ICMP	■
	0.002	Switch9	Router10	ICMP	■
	0.002	Switch1	Router1	ICMP	■
	0.002	Switch6	Router16	ICMP	■
	0.002	Switch4	Router15	ICMP	■
	0.002	Switch0	Router0	ICMP	■
	0.002	Switch2	Router8	ICMP	■

Reset Simulation ☑ Constant Delay Captured to: 0.008 s

Figure 4.5 The details of the packets sent from 6 Source machines



Simulation Panel

Event List

Vis.	Time (sec)	Last Device	At Device	Type	Infc
	0.003	Router10	Router9	ICMP	■
	0.003	Router1	Router14	ICMP	■
	0.003	Router16	Router14	ICMP	■
	0.003	Router15	Router16	ICMP	■
	0.003	Router0	Router14	ICMP	■
	0.003	Router8	Router12	ICMP	■
	0.004	Router9	Router14	ICMP	■
	0.004	Router14	Router12	ICMP	■
	0.004	Router16	Router14	ICMP	■
	0.004	Router12	Switch3	ICMP	■
	0.004	--	Router14	ICMP	■
	0.005	Router14	Router12	ICMP	■
	0.005	Router12	Switch3	ICMP	■
	0.005	Switch3	PC3	ICMP	■
	0.005	--	Router14	ICMP	■
	0.006	Router14	Router12	ICMP	■
	0.006	Router12	Switch3	ICMP	■
	0.006	Switch3	PC3	ICMP	■

Reset Simulation ☑ Constant Delay Captured to: 0.008 s

Figure 4.6 The details of the packets from 6 Source machines traversing the various components network and reaching the Victim machine PC3

V CONCLUSION AND FUTURE SCOPE

The SRP between any two points (x_1,y_1), (x_2,y_2) in two dimensions are defined as (x_2-x_1,y_2-y_1) where, for limited directions.$| x_2- x_1 |$,$| y_2- y_1| \leq 1$ and co primes, and for n directions.$| x_2- x_1 |$,$| y_2- y_1| \leq 2$ and co primes ,and for up to 2^n directions.
$| x_2- x_1 |$,$| y_2- y_1| \leq n-2$ and co primes where $n \leq N$ a set of natural numbers, for $n > N$. The importance of SRP lies in the fact that it can be generalized easily to higher order of direction. Also the two elements being in integers are represent able as bits which is vital for marking / processing purposes which enables the traceback. These properties are made N directional, limited dimensional traceback is possible. The DGT of maximum dimensions, the problem of paucity of adequate header space in packets is addressed using the statistical theory of random sampling. The fixed header space of 25 bits is assumed for every packet. Trifurcated into 10 + 10 + 5 to accommodate the R (mod 1000) for the serial number R of the router, the elements (a,b,c) of direction D_i and the hop count, all in bits. Of course, construction of the traceback path is possible only after sufficient numbers of samples are drawn. This is true for any "statistical method" which means that "the conclusions are true only when the random experiment is repeated a number of times".
The minimum number of packets needed for reconstruction of a path of d hops for a choice of $p=\frac{1}{d}$ is given by, $k=\frac{d^2\ln(d)}{(d-1)^{d-1}}$ which gives $k = 75$ for $d = 10$. The packet header space limitation has been overcome by superior management using Management Reckoning Sampling Process. Though this article has been successful in overcoming the directional and dimensional constraints and header space constraints, by the use of sampling theorem.

REFERENCES

[1] P. DU, S. Abe, Ip packet size entropy-based scheme for detection of dos/ddos attacks, IEICE Transactions on Information and Systems 5 (2008) 1274–1281.

[2] P. Du, A. Nakao, Routelite: one-hop path splicing with path migration, in: IEEE First International Conference on Future Information Networks (ICFIN), 2009.

[3] J. Lee, D. Kim, S. Lee, J. Park, DDoS attacks detection using GA based optimized traffic matrix, in: The 5th Int. Conf. on Innovative Mobile and Internet Services in Ubiquitous Computing, 2011, pp. 216–220.

[4] Arbor Networks, World Wide Infrastructure Security Report 2008, 2008.

[5] C.V. Zhou, S. Karunasekera, C. Leckie, Evaluation of a decentralized architecture for large scale collaborative intrusion detection, in: Proceedings of 10th IFIP/IEEE International Symposium on Integrated Network Management (IM), 2007, pp. 80–89.

[6] T. Gamer, M. Schöller, R. Bless, An extensible and flexible system for network anomaly detection, in: Proceedings of 1st International IFIP TC6 Conference on Autonomic Networking (AN), Lecture Notes in Computer Science, Springer, Paris, France, 2006, pp. 97–108.

[7] T. Gamer, Anomaly-based identification of large-scale attacks, in: Proceedings of IEEE Global Telecommunications Conference (GlobeCom), IEEE, Honolulu, HI, USA, 2009.

[8] C.V. Zhou, C. Leckie, S. Karunasekera, A survey of coordinated attacks and collaborative intrusion detection, Computer & Security 29 (1) (2010) 124–140.

[9] D. Sadok, E. Souto, E. Feitosa, J. Kelner, L. Westberg, RIP – a robust IP access architecture, Computers & Security 28 (6) (2009) 359–380.

[10] T. Gamer, M. Scharf, M. Scholler, Collaborative anomaly-based attack detection, Self-Organizing Systems 4725/2007 (2007) 280–287.

[11] C.V. Zhou, C. Leckie, S. Karunasekera, Decentralized multidimensional alert correlation for collaborative intrusion detection, Journal of Network and Computer Applications (2009) 1106–1123.

[12] T. Peng, C. Leckie, K. Ramamohanarao, Survey of network- based defense mechanisms countering the DoS and DDoS problems, ACM Computing Surveys39 (1) (2007) 1–42.

[13] Z. Duan, X. Yuan, J. Chandrashekar, Controlling IP Spoofing through Inter domain Packet Filters, in: IEEE Trans. on Dependable and Secure, Computing,5(1), January-March 2008, pp. 22–36.

[14] F. Yi, S. Yu, W. Zhou, J. Hai, A. Bonti, Source-based filtering algorithm against DDOS attacks, International Journal of Database Theory and Application 1 (1)zzz (December 2008) 9–20.

[15] H. Wang, C. Jin, K.G. Shin, Defense against spoofed IP traffic using hop-count filtering, in: IEEE/ACM Trans.s on Networking, vol. 15, No. 1, February 2007,pp. 40–53