Australian Journal of Basic and Applied Sciences, 7(7): 732-741, 2013
ISSN 1991-8178

Ant System Algorithm Based Ip Traceback Method to Detect Denial of Service Attack on Data Network

[1]N. Arumugam and [2]Dr.C. Venkatesh

[1]Research Scholar, Anna University, Chennai.
[2]Dean, Faculty of engineering, EBET Group of Institutions, Kankayam, India, Member IEEE.

Abstract: Resource sharing is the prime criteria of internet where anybody sends any information to anyone without a prerequisite. Currently many numbers of online applications are performed through internet. As per the design architecture Internet has no centralized governance in either technological implementation or policies for access and its usage. Hence internet do not performs any security verification of the originality of each data packets. The lack of such verification opens the door for a variety of network security vulnerabilities like denial-of-service (DoS) attacks, man-in-the-middle attacks etc. One of the major threats to the Internet is DoS attack which is achieved by source IP address spoofing. To detect the origin of the attack a number of detection techniques are proposed by the research community. One of the proactive approaches is the traceback technique used to identify the origin of the attack. Among different traceback technique this article proposed an ant system based traceback technique where pheromone intensity is the metric considered for the detection of the DoS attack origin. The simulation results confirmed that the proposed method can successfully find out the DoS attack origin.

Key words: IP spoofing, IP trace back, Ant algorithm, hop count, pheromone intensity, flow level.

INTRODUCTION

Internet is a global system of interconnected computer networks that works on the standard Internet Protocol Suite (TCP/IP) to serve billions of users worldwide. It is a network of networks that consists of millions of private, public, academic, business, and government networks, of local to global scope, that are linked by a broad array of electronic and optical networking technologies. The Internet carries a vast range of information resources and services, such as the inter-linked hypertext documents of the World Wide Web (WWW) and the infrastructure to support electronic mail. The phenomenal growth of the Internet owes much to the simplicity of its design principles, which allow to widely interconnecting heterogeneous systems. However, the penalty of this success has been poor security. The design architecture of Internet permits anybody to send any request to anyone without being authenticated, while the receiver has to process any information that arrives to a provided service. Due to this lack of authentication attackers can create a fake identity, and send malicious traffic on internet. Therefore any systems connected to the Internet are potential targets for attacks since the openness of the Internet makes them accessible to attack traffic.

Since internet does not have any form of control for a server to dictate how much traffic it wants to receive and from whom. During the routing process routers in the Internet do not perform any security verification of the source IP address contained in the packets. The lack of such verification opens the door for a variety of network security vulnerabilities like man-in-the-middle attacks, Denial-of-Service (DoS) and Distributed-Denial-of-Service (DDoS) attacks, in the mean time economic and social impact of internet has grown to considerable proportions. One of the major threats to the Internet is source IP address spoofing. In current Internet communication world, validity of the source of IP packet is an important issue. Thus the problems of IP spoofing is definitely alarm the legitimate users of the Internet. According to a study conducted by CSI Computer Crime and Security Survey 2010, the impact of Denial-of-Service (DoS) attacks is around 19.8%. Thus it is mandatory to detect and diffuse the DoS attack.

Literature Review:

More than a decade a number of network attack detection techniques have been developed and applied in detection of DoS network attacks. Most of the approaches required to modify the network infrastructure either encoding the router's information into the specific fields of the IP header or storing a representative amount of the packet content at the routers for the attack detection purpose. And also they require all the routers, along the DoS attacking path, to support the detection mechanism. Alex C. Snoeren *et al* proposed a hash-based IP traceback technique which generates audit trails for traffic within the network, and can trace the origin of a *single* IP packet delivered by the network (Alex C. Snoeren ,Craig Partridge, *et al*,2001).Probabilistic packet marking (PPM) is another technique where each packet is marked with partial path information at routers. Each

Corresponding Author: N. Arumugam, Research Scholar, Anna University, Chennai.

router marks their IP address onto the packet with the probability along the way the packet traversed. When DDOS attack is detected, the victim can reconstruct the whole path after collecting certain amount of packet by using the information of the mark, despite the source address in the IP header. One of the demerits of this method is its computation overhead discussed in (Savage.S, Wetherall.D, *et al*, 2001). The limitation of PPM was modified and reduces the computational overhead to an acceptable level were discussed in (D. Q. Li, P. R. Su, and D. G. Feng, 2004). M. M. Viana *et al* combine PPM and the concept of winding number. Their work shows that they are able to correctly trace the attacker's router IP address using integral equation discussed in (M. M. Viana, R. Rios, *et al*, 2009). Deterministic Packet Marking (DPM) is a new approach for IP traceback which is scalable and simple to implement, and introduces no bandwidth and practically no processing overhead. It is backward compatible with equipment which does not implement it. The approach is capable of tracing back attacks, which are composed of just a few packets. In addition, a service provider can implement this scheme without revealing its internal network topology (A.Belenky and N. Ansari, 2003). On Deterministic Packet Marking is another approach to IP Traceback based on marking all packets at ingress interfaces discussed in (Andrey Belenky, Nirwan Ansari, 2006).Flexible Deterministic Packet Marking (FDPM) provides a defense system with the ability to find out the real sources of attacked packets that traverse through the network. FDPM provides innovative features to trace the source of IP packets and can obtain better tracing capability than others. In particular, FDPM adopts a flexible mark length strategy to make it compatible to different network environments. It is also adaptively changes it's marking rate according to the load of the participating router by a flexible flow-based marking scheme (Y. Xiang, W. Zhou, and M. Guo, 2009). Path identification (Pi) DDoS defense scheme is a deterministic packet marking scheme that allows a DDoS victim to filter out attack packets on a per packet basis with high accuracy after only a few attack packets are receive. Enhancement of the idea called the StackPi marking, a new packet marking scheme based on Pi, and new filtering mechanisms. This scheme almost completely eliminates the effect of a few legacy routers on a path, and performs 2-4 times better than the original Pi scheme in a sparse deployment of Pi-enabled routers (A. Yaar, A. Perrig, and D. Song, 2006). Another attack mitigation scheme which adopts divides and conquers strategy. Attack diagnosis combines the concepts of pushback and packet marking. Its architecture is in line with the ideal DDoS attack countermeasure paradigm. Attack detection is performed near the victim host and packet filtering is executed close to the attack sources. Attack diagnosis is a reactive defense mechanism that is activated by a victim host after an attack is detected. By instructing its upstream routers to mark packets deterministically, the victim can trace back one attack source. Attack diagnosis enabled router close to the source to filter the attack packets. This process isolates one attacker and throttles it, which is repeated until the attack is mitigated (R. Chen, J. M. Park, and R. Marchany, 2007). Lih-Chyau Wuu *et al* proposed an IP traceback method based on the Chinese Remainder Theorem, where routers with the proposed method can interoperate seamlessly with legacy routers and be incrementally deployable. In the proposed method a victim does not need to maintain the network topology while it reconstructs attacking paths (Lih-Chyau Wuu, Tzong-Jye Liu *et al*, 2011).

MATERIALS AND METHODS

This section describes a DoS attack detection method based on Ant System Based IP Traceback Technique **(ASBITT)** to identify the origin of the attack. In an ant system, the ants are able to find the best path between their nest and a food source. Ants are communicated indirectly by dropping a chemical type of hormones called pheromones. Among different paths ants are use the shortest path to reach the food source. This shortest path is identified by referring the pheromone intensity. The following section narrates the behavior of ant and the packet flows in the network to detect the origin of DoS attack.

Behavior of Ants:

Ants are social creature living within a colony. The number of ants in a single colony may vary from tens to tens of millions. The activities of ants are very nature and optimal in transporting food, overcoming obstacles, building ant hills, and other operations. The social behavior of ants is based on self-organization, which is a set of dynamic mechanisms ensuring that the system can achieve its global aim through low-level interactions between its elements. A key feature of this interaction is that the system elements use only local information. Self-organization is achieved by the interaction of four components such as multiple renewals, randomness, positive feedback and negative feedback (Salah Zidi, Salah Maouche, Slim Hammadi, 2006).

According to the ethologyists report it was understood that ants could establish shortest route paths from their colony to feeding sources and back. It was found that the medium used to communicate information among individuals ants regarding paths selection based on pheromone trails. Pheromone is a special type of chemical that is deposited as trail by ants when they move. Thus a moving ant lays some pheromone (in varying quantities) on the ground and marking the path by a trail of this substance. While an isolated ant moves essentially at random, an ant encountering a previously laid trail can detect it and decide with high probability to follow it, thus reinforcing the trail with its own pheromone. The collective behavior that emerges is a form of autocatalytic behavior where more numbers of ants following the same route based on trail of pheromone. The process is thus characterized by a positive feedback loop, where the probability with which an ant chooses a path increases with the number of ants that previously chose the same path.

The above theory is demonstrated with an experimental setup shown in fig.1a. The ants are walking from their colony to food source and vice versa, where A represents their colony and E as food source. Suddenly an obstacle represent as BD appears hence the path is cut off. So at position B the ants are walking from A to E (or at position D those walking in the opposite direction) have to decide whether to turn right or left as in fig.1b. The choice is influenced by the intensity of the pheromone trails left by preceding ants.

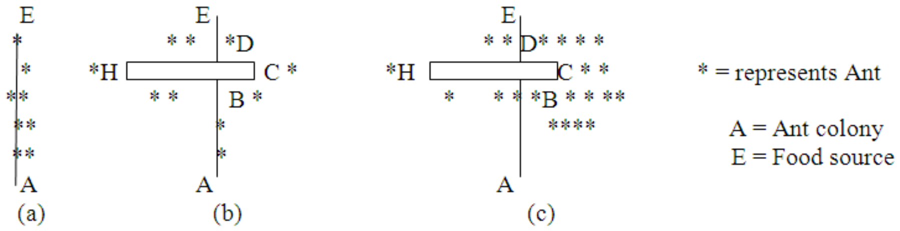

Fig. 1: Ant's behavior.

A higher level of pheromone on the right path gives an ant a stronger stimulus and thus a higher probability to turn right. The first ant reaching point B (or D) has the same probability to turn right or left (as there was no previous pheromone on the two alternative paths). Because path BCD is shorter than BHD, the first ant following it will reach D before the first ant following path BHD fig.1ca. The result is that an ant returning from E to D will find a stronger trail on path DCB, caused by the half of all the ants that by chance decided to approach the obstacle via DCBA and by the already arrived ones coming via BCD. And hence they will prefer (in probability) path DCB to path DHB. As a consequence, the number of ants following path BCD per unit of time will be higher than the number of ants following BHD. This causes the quantity of pheromone on the shorter path to grow faster than on the longer one, and therefore the probability with which any single ant chooses the path to follow is quickly biased towards the shorter one. The final result is that very quickly all ants will choose the shorter path. From this experimental setup it is conclude that at a given point an ant has to choose among different paths, those which were heavily chosen by preceding ants are chosen with higher probability. And also high trail levels are synonymous with shortest paths. This type of ant behavior is utilized to find the attack origin in the network (Marco Dorigo,Vittorio Maniezzo *et al*, 1996).

ANT Algorithm:

Normally ants are prefers shortest route to reach their food from their colony. The ant system algorithm utilized the natural behavior of ants such as the quick convergence and heuristic. Utilizing these characteristics this paper proposed a method to find the IP traceback based DoS attacks on the network (Gu Hsin Lai, Chia-Mei Chen *et al*, 2008). IP traceback is the ability to trace IP packets from source to destination and is a significant step toward identifying the source of DoS attack. Let us consider a network topology where IP traceback is a technique of finding the origin with a minimal length among the adjacent nodes. Assume that the length of the path between nodes i and j is d_{ij}. This length is expressed and calculated by Euclidean distance method as:

$$d_{ij} = \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2} \tag{1}$$

For an instance consider the network as a graph (N, E) where N is the set of nodes and E is the set of edges between nodes. Let b_i (t), is the number of ants at node i at time t where i=1,............., n and $m = \sum_{i=1}^{n} b_i(t)$ be the total number of ants. Each ant is an agent and they can choose the next possible node to move with a probability. The probability is a function of the node distance and of the amount of trail present on the connecting edge. The ant can make legal tours at the same time transitions to already visited nodes are not allowed until a traceback is completed which is controlled by a tabu list. When ants completes a traceback, it lays a substance called trail on each edge (i, j) visited. Let τ_{ij} (t) be the intensity of trail on edge (i, j) at time t. In the next move at time t each ant chooses the next node. According to the ant system algorithm, an iteration means m moves carried out by the m ants in the interval (t, t+1), then every n iterations of the algorithm each ant has completed one cycle. Up on completion of one cycle the trail intensity is updated as:

$$.\ \tau_{ij}(t+n) = \rho . \tau_{ij}(t) + \Delta\tau_{ij} \tag{2}$$

$$\Delta\tau_{ij} = \sum_{k=1}^{m} \Delta\tau_{ij}^{k} \tag{3}$$

where ρ is a coefficient such that (1 - ρ) represents the *evaporation* of trail between time t and t+n, and $\Delta\tau_{ij}{}^{k}$ is the quantity per unit of length of trail substance (pheromone in real ants) laid on edge (i,j).
Similarly by the kth ant between time t and t+n is given by:

$$\tau_{ij}^{k} = \begin{cases} \frac{Q}{L_k} \; if\ k^{th}\ ant\ uses\ edge\ (i,j)\ in\ its\ tour\ (between\ time\ t\ and\ t+n) \\ 0 \quad otherwise \end{cases} \tag{4}$$

where Q is a constant and L_k is the tour length of the kth ant. To avoid unlimited accumulation of pheromone trail the coefficient ρ must be set to a value < 1. And also set the initial value of intensity trail to a small positive value. In order to satisfy the constraint that an ant visits all the nodes with all possible paths, it is associate with each ant with a data structure called the *tabu list*, that saves the nodes already visited up to time t and forbids the ant to visit them again before n iterations have been completed. When ants reach its food, the tabu list is used to compute the ant's current solution (i.e., the distance of the path followed by the ant). The tabu list is then emptied and the ant is free again to choose. Thus $tabu_k$ is dynamically growing vector which contains the list of the kth ant, $tabu_k$ the set obtained from the elements of $tabu_{\mathbf{k}}$, and $tabu_{\mathbf{k}}(s)$ the sth element of the list (i.e., the sth node visited by the kth ant in the current tour). The parameter *visibility* η_{ij} the quantity obtained as $\eta_{ij}=1/d_{ij}$, is not modified during the running of the ant algorithm AS, as opposed to the trail which instead changes according to the previous formula (1).
The transition probability of ant moves from node i to node j for the kth ant as:

$$p_{ij}^{k}(t) = \begin{cases} \dfrac{[\tau_{ij}(t)]^{\alpha}.[\eta_{ij}]^{\beta}}{\sum_{k\epsilon allowed_k}[\tau_{ij}(t)]^{\alpha}.[\eta_{ij}]^{\beta}} \; if\ j\ \epsilon\ allowed\ _k \\ 0 \qquad otherwise \end{cases} \tag{5}$$

where $allowed_{\mathbf{k}} = \{N - tabu_k\}$ and where α and β are parameters that controls the intensity of pheromone trail and visibility. Therefore the transition probability is a trade-off between visibility and trail intensity at time t (Marco Dorigo and Thomas Stutzle, 2010).

Ant Algorithm Approach for IP Traceback:

From the earlier discussion of ant-system algorithm, at time zero an initialization phase takes place during which ants are positioned on different nodes and initial values τ_{ij} for trail intensity are set on edges. The first element of each ant's tabu list is set to be equal to its starting node. Thereafter every ant moves from node i to node j choosing the node to move to with a probability that is a function of two desirability measures. Thus the trail $\tau_{ij}(t)$, gives information about how many ants in the past have chosen that same edge (i,j) and the visibility η_{ij}, says the closer between the nodes. Obviously, setting α= 0, the trail level is no longer considered, and a stochastic greedy algorithm with multiple starting points is obtained. After n iterations all ants have completed a tour, and their tabu lists will be full; at this point for each ant k the value of L_k is computed and the values $\Delta\tau_{ij}{}^{k}$ are updated according to formula (3). Hence the shortest path found by the ants is saved and all the tabu lists are emptied. This process is iterated until the tour counter reaches the maximum (user- defined) number of cycles NC_{MAX}, or all ants make the same tour. This last case denotes a situation in which the algorithm stops searching for alternative solutions

The pseudo code of the proposed IP traceback algorithm is described in fig.2. According to the algorithm when the ants arrived at the edge node the probability of their next move is determined based on the flow information of the neighbor nodes. While exploring the network, the each ant keeps track of the path and the number of DoS flows. The above procedure is repeated tracing back to the upstream nodes until the ant completes its cycle. The intensity of pheromone trail is revised after all the ants complete their tour from the victim to a boundary node. The path information obtained by each ant is also calculated. The change of pheromone results in positive feedback is the more ants are following the same path, the more attractive that path becomes attack path. Each time when all ants complete one cycle, the intensity of pheromone on each path will be recalculated. From the algorithm it is understood that higher value of pheromone intensity path is indirectly an attack path.

```
Step1:  Initialize:
                    Set t: =0 //t is the time counter
                    Set NC: =0 //NC is the cycles counter
                    For every node (i, j) set an initial value   $\tau_{ij}(t) = c$   for trail intensity and
                    $\Delta\tau_{ij}(t) = 0$
Step2: Place the m ants on the node i
                    Set s: =1 //s is the tabu list index
                    For k: =1 to m do
                  Place the starting node of the k-th ant in tabuk(s) Step 3: Repeat until ant arrives the
edge node
                  //this step will   be repeated (n-1) times//
                   Set s: =s+1
                   For k: =1 to m do
                   Choose the node j to move to, with probability   $p_{ij}^{k}(t)$   given by
equation (4)
                  // at time t the $k^{th}$ ant is on node i=tabuk(s-1)//
                   Move the $k^{th}$ ant to the node j
                    Insert node j in **tabu$_k$**(s)
Step 4: For k: =1 to m do     //for each ant
                      Move the $k^{th}$ ant from **tabu$_k$** (n) to **tabu$_k$** (1)
                Compute the length $L_k$   //length of each ant's path
                Update the shortest path found
                       For every node (i, j)
                       For k: =1 to m do
.
$\Delta\tau_{ij}^{k} = \begin{cases} \frac{Q}{L_k} & if\ (i,j) \in tour\ described\ by\ tabu_k \\ 0 & otherwise \end{cases}$

$\Delta\tau_{ij}^{k} := \Delta\tau_{ij} + \Delta\tau_{ij}^{k};$
Step 5: For every node (i, j) compute $\tau_{ij}$ (t+n)
                       $\tau_{ij}$ (t+n) =$\rho.\tau_{ij}$ (t) + $\Delta\tau_{ij}$
                      Set t: =t+n
                      Set NC: =NC+1
                      For every node (i,j)
                      Set $\Delta\tau_{ij}$:=0
Step 6: //Most possible attack path
                       If (NC < $NC_{MAX}$)    // NC number of iteration
                            then      Empty all tabu lists
                        Goto step 2
                    else
               Display the possible attack path
               Stop
```

Fig. 2: The pseudo code of the proposed IP traceback method.

RESULTS AND DISCUSSION

The performance analysis of the proposed ASBITT algorithm for the detection of the attack source, a series of experiments was performed through the network simulator NS-2 using a PC with an Intel Dual core CPU 3.0G, DDR2 1G of RAM and the MS Windows XP operating system. Fig.3 show an experimental topology setup constructed with 9 numbers of nodes. The simulation parameters such as the simulation duration, experimental topology size, traffic type, number of nodes and the routing algorithm are list out in table 1.

For the analysis it is assumed that out of 9 numbers of nodes, node 1 is treated as an attacker node and the node 9 is a victim node. During the network operation naturally the victim node may receive frequent request from the attacker. To traceback the origin of the attacker all possible paths are identified by implementing ant system algorithm.

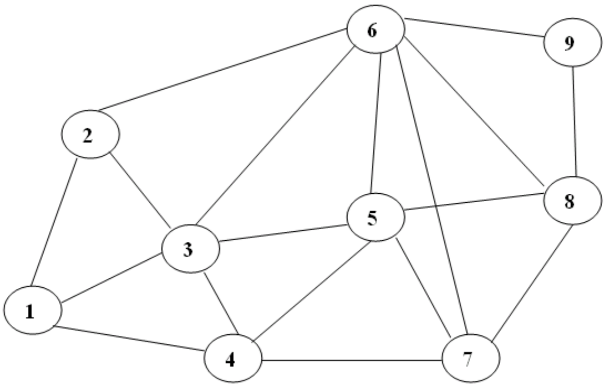

Fig. 3: Experimental topology with 9 nodes.

Table 1: Simulation Parameters.

S.No.	Parameters	Value
1	Simulation duration	100 seconds
2	Topology	1000m * 1000 m
5	Traffic type	CBR (UDP)
6	Data payload	512 bytes
7	Routing Algorithm	ANT
8	Number of nodes	9

As per the natural behavior of ant, majority of the ants choose the shortest path to reach the food source. During the first iteration the explorer ants are prepare the shortest path to reach the food source. As per the algorithm this path is identified by the intensity of the pheromone values. Table 2 shows the details of possible path with pheromone intensity of the first iteration. The experimental result implicates that maximum numbers of data packets are flooded on the shortest path 1->3->6->9. Fig.4 shows the graphical representation of the scenario discussed. Hence it is easy to desire the victim and attacker node. At the same time in the data network each packet is travelled individually and also follows different routes to its destination. Thus to find out the exact origin of the attacker the same procedure is repeated for more number of times. For the analysis purpose this article repeated the experimental procedure for 6 times. The obtained experimental values are tabulated from table 2 -7. Consequently the graphical representations of the each iteration are also shown in the fig. 4-9.

Table 2: Details of possible path with pheromone intensity of each path.

	S.No	Attack Source	Victim Node	Path Node	Hop Count	Pheromone Intensity
Iteration #1	1.	1	9	1->4->7->8->9	4	1.6
	2.	1	9	1->4->5->8->9	4	1.31
	3.	1	9	1->3->5->8->9	4	1.11
	4.	1	9	1->4->3->5->8->9	5	0.69
	5.	1	9	1->3->6->9	3	2.03
	6.	1	9	1->2->6->9	3	1.62
	7.	1	9	1->3->5->7->8->9	5	0.59
	8.	1	9	1->3->4->5->6->9	5	0.23
	9.	1	9	1->4->7->6->8->9	5	0.8
	10.	1	9	1->3->5->7->8->9	5	1.1

Table 3: Details of possible path with pheromone intensity of each path.

	S.No	Attack Source	Victim Node	Path Node	Hop Count	Pheromone Intensity
Iteration #2	1.	1	9	1->4->7->8->9	4	1.41
	2.	1	9	1->4->5->8->9	4	1.52
	3.	1	9	1->3->5->8->9	4	1.32
	4.	1	9	1->4->3->5->8->9	5	1.01
	5.	1	9	1->3->6->9	3	1.87
	6.	1	9	1->2->6->9	3	1.54
	7.	1	9	1->3->5->7->8->9	5	0.55
	8.	1	9	1->3->4->5->6->9	5	0.51
	9.	1	9	1->4->7->6->8->9	5	0.8
	10.	1	9	1->3->5->7->8->9	5	1.1

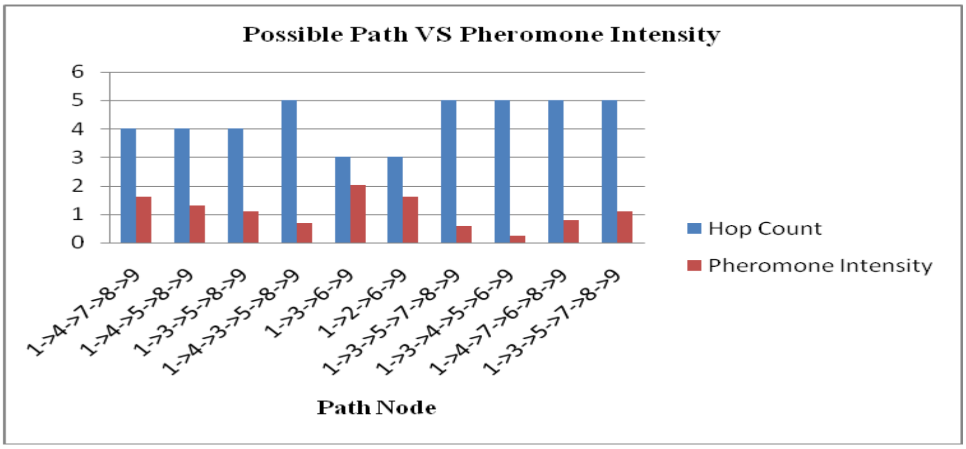

Fig. 4: Possible path with their pheromone intensity.

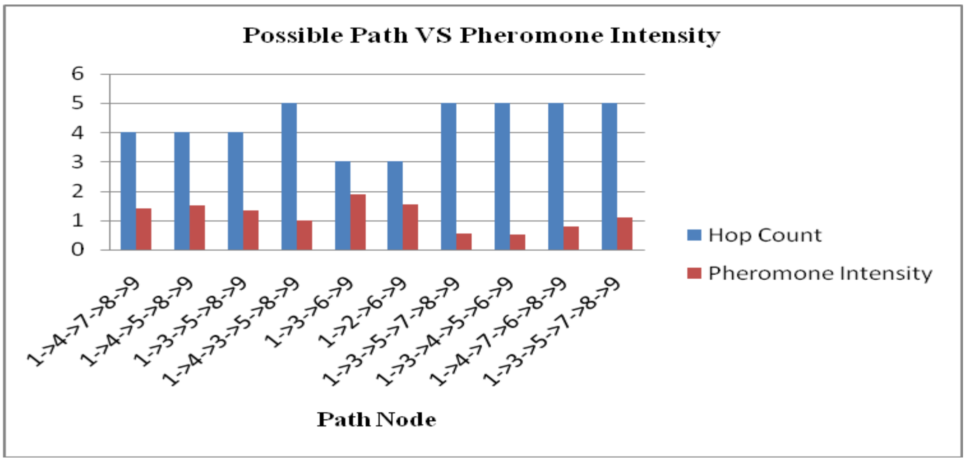

Fig. 5: Possible path with their pheromone intensity.

Table 4: Details of possible path with pheromone intensity of each path.

	S.No	Attack Source	Victim Node	Path Node	Hop Count	Pheromone Intensity
Iteration #3	1.	1	9	1->4->7->8->9	4	1.26
	2.	1	9	1->4->5->8->9	4	1.29
	3.	1	9	1->3->5->8->9	4	1.27
	4.	1	9	1->4->3->5->8->9	5	1.04
	5.	1	9	1->3->6->9	3	1.88
	6.	1	9	1->2->6->9	3	1.83
	7.	1	9	1->3->5->7->8->9	5	0.82
	8.	1	9	1->3->4->5->6->9	5	0.36
	9.	1	9	1->4->7->6->8->9	5	0.97
	10.	1	9	1->3->5->7->8->9	5	1.23

Table 5: Details of possible path with pheromone intensity of each path.

	S.No	Attack Source	Victim Node	Path Node	Hop Count	Pheromone Intensity
Iteration #4	1.	1	9	1->4->7->8->9	4	1.49
	2.	1	9	1->4->5->8->9	4	1.6
	3.	1	9	1->3->5->8->9	4	1.41
	4.	1	9	1->4->3->5->8->9	5	1.1
	5.	1	9	1->3->6->9	3	1.93
	6.	1	9	1->2->6->9	3	2.02
	7.	1	9	1->3->5->7->8->9	5	0.78
	8.	1	9	1->3->4->5->6->9	5	0.82
	9.	1	9	1->4->7->6->8->9	5	0.82
	10.	1	9	1->3->5->7->8->9	5	1.72

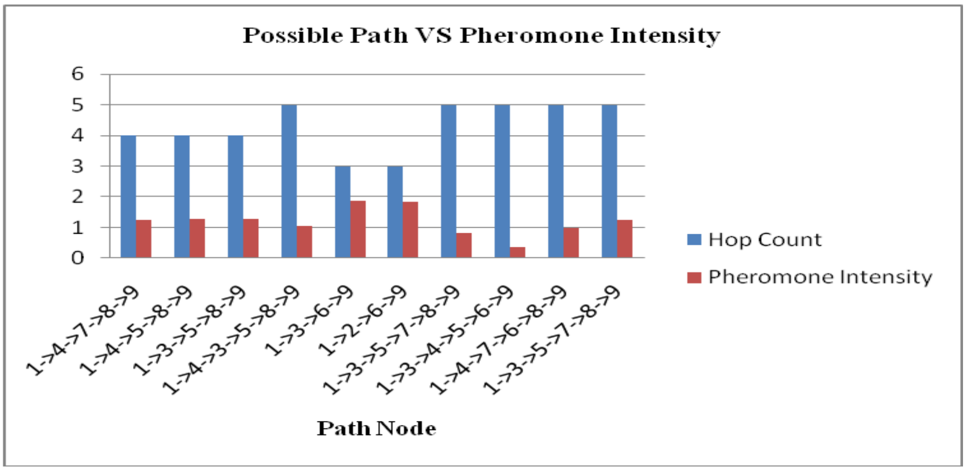

Fig. 6: Possible path with their pheromone intensity.

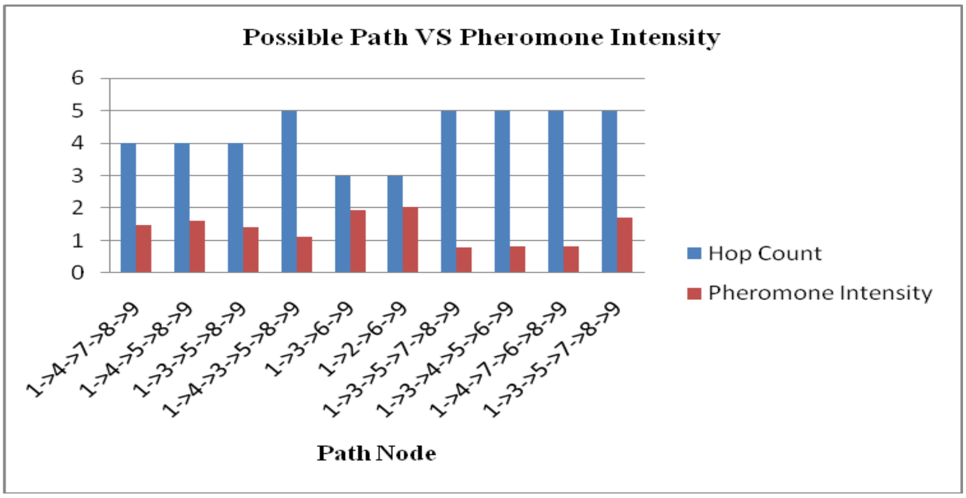

Fig .7: Possible path with their pheromone intensity.

Table 6: Details of possible path with pheromone intensity of each path.

	S.No	Attack Source	Victim Node	Path Node	Hop Count	Pheromone Intensity
Iteration #5	1.	1	9	1->4->7->8->9	4	1.91
	2.	1	9	1->4->5->8->9	4	1.54
	3.	1	9	1->3->5->8->9	4	1.56
	4.	1	9	1->4->3->5->8->9	5	1.19
	5.	1	9	1->3->6->9	3	2.14
	6.	1	9	1->2->6->9	3	2.29
	7.	1	9	1->3->5->7->8->9	5	1.11
	8.	1	9	1->3->4->5->6->9	5	0.96
	9.	1	9	1->4->7->6->8->9	5	0.94
	10.	1	9	1->3->5->7->8->9	5	1.81

Table 7: Details of possible path with pheromone intensity of each path.

	S.No	Attack Source	Victim Node	Path Node	Hop Count	Pheromone Intensity
Iteration #6	1.	1	9	1->4->7->8->9	4	1.89
	2.	1	9	1->4->5->8->9	4	1.92
	3.	1	9	1->3->5->8->9	4	1.5
	4.	1	9	1->4->3->5->8->9	5	1.59
	5.	1	9	1->3->6->9	3	2.42
	6.	1	9	1->2->6->9	3	2.41
	7.	1	9	1->3->5->7->8->9	5	1.3
	8.	1	9	1->3->4->5->6->9	5	1
	9.	1	9	1->4->7->6->8->9	5	1.4
	10.	1	9	1->3->5->7->8->9	5	1.98

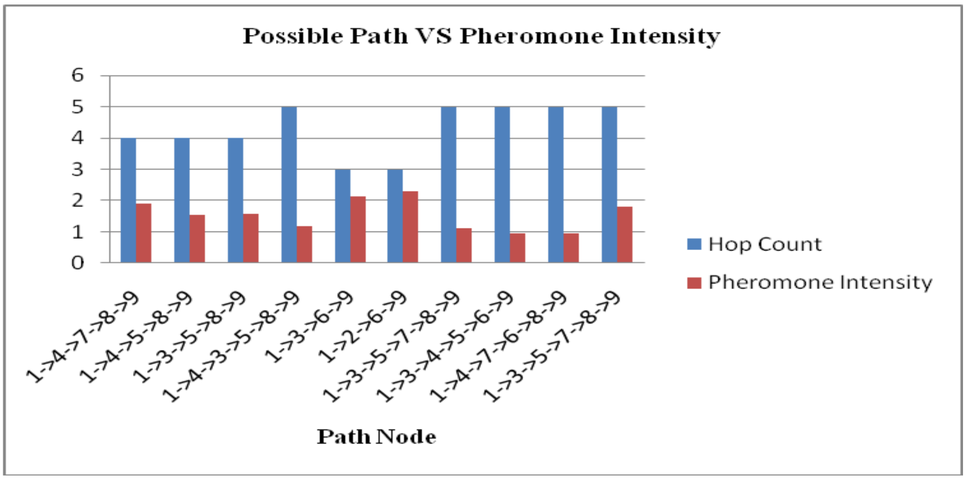

Fig. 8: Possible path with their pheromone intensity.

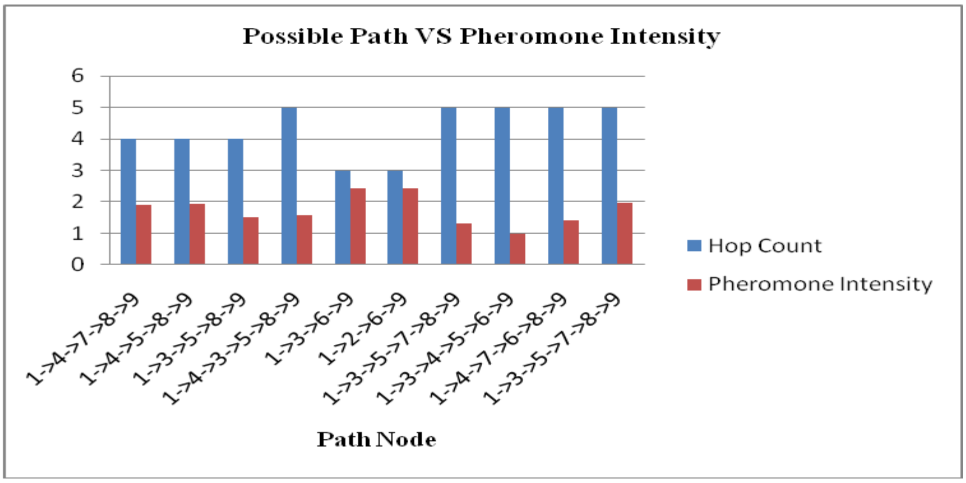

Fig. 9: Possible path with their pheromone intensity.

From the above said experimental values it is confirmed that the maximum contribution of pheromone intensity lies only in the path 1->3->6->9. Hence it is concludes that node 1 is the attacker and node 9 is the victim node. Table 8 shows the consolidated representation of 6 iteration values of all possible paths with their pheromone intensity value. Similarly fig.10 shows the graphical representation of the 6 iteration.

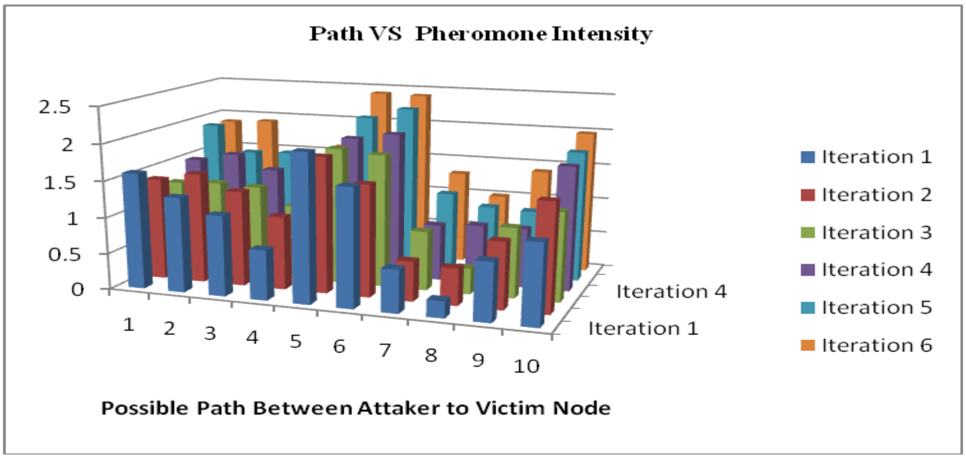

Fig. 10: Possible path with their pheromone intensity.

Table 8: Details of possible path with pheromone intensity of each path.

S.No	Path Node	Hop Count	Pheromone Intensity					
			Iteration #1	Iteration #2	Iteration #3	Iteration #4	Iteration #5	Iteration #6
1.	1->4->7->8->9	4	1.6	1.41	1.86	2	1.91	1.89
2.	1->4->5->8->9	4	1.31	1.52	1.79	1.6	1.54	1.92
3.	1->3->5->8->9	4	1.11	1.32	1.27	1.41	1.56	1.5
4.	1->4->3->5->8->9	5	0.69	1.01	1.04	1.1	1.19	1.59
5.	1->3->6->9	3	2.03	1.87	1.88	1.93	2.14	2.42
6.	1->2->6->9	3	1.62	1.54	1.73	2.02	2.29	2.41
7.	1->3->5->7->8->9	5	0.59	0.55	0.82	0.78	1.11	1.3
8.	1->3->4->5->6->9	5	0.23	0.51	0.36	0.82	0.96	1
9.	1->4->7->6->8->9	5	0.8	0.92	0.97	0.82	0.94	1.4
10.	1->3->5->7->8->9	5	1.1	1.49	1.23	1.72	1.81	1.98

Conclusion:

DoS attack becomes one of the major threats in internet and simply denies the access of the legitimate users. Normally it is deployed with IP address spoofing and hence it very tough to identify the source of the attack. The proposed **ASBITT** is an IP traceback based technique implemented to find the origin of the attack. This technique is developed with the concepts of ant system algorithm. According to the ant algorithm more numbers of ants are routed to reach the food source by shortest path. Once the shortest path is identified it is easy to point out the origin of the attack. The proposed method is verified and evaluated through simulation. Simulation results are also confirmed this concept by showing maximum pheromone intensity in a shortest path between the victim and attacker. To enhance the detection procedure more numbers of iteration are also performed. Hence, this paper concludes that the proposed solution is an efficient method to find out the DoS attack origin in the networks.

REFERENCES

Alex C. Snoeren, Craig Partridge *et al.*, 2001. “Hash-Based IP Traceback”, BBN Technologies, *SIGCOMM’01*, August 27-31, 2001, San Diego, California, USA.

Andrey Belenky, Nirwan Ansari, 2006. “On deterministic packet marking,” Elsevier.

Belenky, A. and N. Ansari, 2003. "IP traceback with deterministic packet marking," *IEEE Communications Letters,* 7: 162-164.

Chen, R., J.M. Park and R. Marchany, 2007. "A divide-and-conquer strategy for thwarting distributed denial-of- service attacks," *IEEE Transactions on Parallel and Distributed Systems*, 18: 577-588.

Gu Hsin Lai, Chia-Mei Chen *et al*, 2008. National Sun Yat-Sen University, Taiwan “ Ant-based IP traceback”, Elsevier, Expert Systems with Applications, 34.

Li, D.Q., P.R. Su and D.G. Feng, 2004. "Notes on packet marking for IP traceback," Ruan Jian Xue Bao/Journal of Software, 15: 250-258.

Lih-Chyau Wuu, Tzong-Jye Liu *et al*, 2011. “IP Traceback Based on Chinese Remainder Theorem”, Journal of Information Science and Engineering, 27: 1985-1999.

Marco Dorigo and Thomas Stutzle, 2010. “Ant Colony Optimization: Overview and Recent Advances”, Springer Science +Business Media, LLC.

Marco Dorigo, Vittorio Maniezzo *et al*, 1996. “The Ant System”, IEEE Transactions on Systems, Man, and Cybernetics-Part B, 26(1): 1-13.

Salah Zidi, Salah Maouche, Slim Hammadi, 2006. “Ant Colony with Dynamic Local Search for the Time Scheduling of Transport Networks”, International Journal of Computers, Communications & Control, I(4): 110-125.

Savage, S., D. Wetherall, A. Karlin, T. Anderson, 2001. “Network support for IP traceback”,IEEE/ACM Transactions on Networking, 9(3): 226-237.

Viana, M.M., R. Rios, R.M. De Castro Andrade and J.N. De Souza, 2009. "An innovative approach to identify the IP address in denial-of-service (DoS) attacks based on Cauchy's integral theorem," *International Journal of Network Management,* 19: 339-354.

Xiang, Y., W. Zhou and M. Guo, 2009. "Flexible deterministic packet marking: An IP traceback system to find the real source of attacks," *IEEE Transactions on Parallel and Distributed Systems*, 20: 567-580.

Yaar, A., A. Perrig and D. Song, 2006. "StackPi: New packet marking and filtering mechanisms for DDoS and IP spoofing defense," *IEEE Journal on Selected Areas in Communications,* 24: 1853-1863.