CHAPTER 5

ANT ALGORITHM BASED NETWORK ATTACK
DETECTION ON DATA NETWORK

5.1 INTRODUCTION

The growth rate of the beneficiaries of Internet is increasing exponentially every day due to its simplicity and openness. It has experienced a tremendous growth in its size and complexity since its commercialization described by Lixin Gao (2001). Hence presently all commercial and social sectors are preferred internet for data transferring as it is easy to equip and execute the task quickly. As the token of these advantages Internet hosts are threatened by large-scale network based attacks by Abraham Yaar et al (2006). These attacks typically rely on compromising a large number of hosts to generate traffic to a single destination, the severity of network based attacks will likely increase as greater numbers of poorly secured hosts are connected to high-bandwidth Internet connections.

Thus it is mandatory for the service providers not only to protect the network resources from the network attackers but also for the assurance of secured transfer of data. By the implementation of an efficient network attack detection techniques the unauthorized access to resources server may be prevented described by Srinath et al (2010). There are different types of detection and prevention techniques are identified by the research communities. Among them filtering technique is a proactive method where an unauthorized user called as attacker are identified and prevented from the access of the server on the data network. The detection efficiency of the
filtering methods is good but the requirement of additional memory and time requirement for the request validation are inevitable.

Along with these constraints these detection techniques can prevent the attack request only they unable to identify the source of the attack. For the complete prevention of the attacker involvement the origin of the attacker must identified.

Traceback technique is one of the proactive methods used by many research communities for the identification of the attack origin. This traceback technique is used to identify the origins of the sequences IP packets when the source IP addresses of these packets are spoofed.

Since the late 1999, research on IP trace back has been rather active for the detection of network based attacks. Several approaches have been proposed to trace IP packets to their origins. In general there are two major categories of traceback techniques, the first one is to trace a single packet, and the other is to use a large number of packets for tracing the attacker. And also research communities are proposed different types of IP traceback techniques focus on tracking the location of the attackers Minho Sung and Jun Xu (2003).

As a successor, this thesis is also implementing an optimistic IP traceback technique called as an Ant system based IP traceback technique used to trace the attack sources based on the reaction of attack traffic. In this algorithm data flow is considered as a metric used for the traceback techniques. The following sections of this thesis will discuss the ant system based IP traceback method implemented for the detection of the origin of the attack.
5.2 TRACING TECHNIQUES FOR SOURCE IP VERIFICATION

In general, routers in the Internet do not perform any security verification of the requested user’s source IP address of each IP packet, the lack of such activities leads to the possibility of more numbers of network-based attacks. The lack of such verification opens the door for a variety of vulnerabilities, including denial-of-service (DoS) and man-in-the-middle attacks.

As the supportive for the above said vulnerabilities, today’s Internet is not fully equipped with proper defense mechanisms against network-based attacks. Stefan Savage et al (2001). Detection of these attacks is essential for the effective utilization of internet resources. Variety of detection and defense mechanism are discussed by the research community. In the earlier work this study discussed a filtering scheme where incoming request is validated before it reaches the protected server without using any cryptographic methodology. The detection rate this method is found good with compensating more validation time. To improve the identification of the attack source this thesis proposed an ant system based IP traceback method which to be discussed in the following section.

Since the late 1999 research on IP trace back has been active to detection of network-based attacks. Several approaches have been proposed to trace IP packets to their origins. IP traceback is usually performed at the network layer, with the help of routers and gateways. The trace back techniques can trace packet paths and help in identifying the perpetrators of the attacks with a high probability.
An algebraic approach to IP traceback is discussed by Drew Dean et al (2002). It provides a new solution to the problem of determining the path for a packet traversed over the Internet during a denial of service attack. It is an algebraic marking scheme for IP traceback, which is based on the mathematical theory of Linear Algebra and coding theory. Packet marking based IP traceback method proposed by Goodrich et al (2001). Savage, S. (2000) quoted the support which is provided by the internet for IP traceback. Similarly Snoeren (2001) discussed the hash based technique used for the IP traceback technique.

In continuation with hash based technique Sanchez (2001) discussed hardware support for hash based IP traceback technique. Li et al (2004) proposed an IP traceback method discussed the concepts of practical techniques used for high speed internet. Stone et al (2000) explained an IP overlay network based method which used to track the DoS flood. Another marking based technique for the traceback method called Advanced and authenticated marking scheme for IP traceback is proposed by Song and Perrig (2001). The effectiveness of marking scheme used for IP traceback proposed and implemented as the effectiveness of probabilistic packet marking for IP traceback by Park and Lee (2001) proposed a traceback method against DoS attacks using the concepts of both path identification and traceback concepts. Prevention of the attacker involvement is possible by the detection of its origin, to achieve this, the victim can trace the attackers back within the path tree and perform rapid packet filtering using the marking in each packet. Using the above discussed traceback concepts this thesis implementing and tested an ant system based traceback techniques for the detection of the attack source. The following section will describe the proposed the ant system based traceback techniques.
5.3 ANT SYSTEM BASED IP TRACEBACK TECHNIQUE (ASBITT)

Identification and prevention of network attack at the origin is mandatory for the secure transfer of data on the data network. Implementation of any attack defense mechanism may simply prevent the attacks but the involvements of attacks are not completely eliminated. Unless the source of the attack identified the complete attack prevention is not possible. In data network traceback is one of technique used to find the attack source. Thus detection of the attack source is possible by the implementation of an efficient traceback technique.

Among the variety of traceback technique this thesis employed an Ant System Based IP Traceback Technique (ASBITT) used to identify the origin of the attack. This traceback approach used the flow level information for the identification of attack origin. In the ant system based IP traceback, the natural behavior of ants uses for the traceback techniques. As per the natural behaviors, the ants are able to find the best path (shortest path) between their nest and a food source. While searching for food, the first ant called as explorer ant searching for food. Once the food is identified, it starts back to their colony with the shortest path. While going back to its colony the explorer ant lays some chemical like substance called as a pheromone. These chemicals like substance will help the other ants to reach the food source.

As per the natural behavior, ants are used the shortest path to reach the food source. This shortest path is identified by the subsequent ants by referring the pheromone substance laid by explorer ant explained by Marco Dorigo et al (1996). The following section narrates the behavior of ants and the packet flows in the network to detect the origin of network attack.
5.3.1 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 et al (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 individual ants regarding paths selection based on pheromone trails. Pheromone is a special type of chemical that is deposited as a trail of 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 formed of autocatalytic behavior were more numbers of ants following the same route based on the 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 Figure 5.1. The ants are walking from their colony to the food source and vice versa, where A represents their colony and E as a food source. Figure 5.1a shows the movement of ants on a single path without any disturbances. Assume that a sudden movement of an obstacle denoted as BD appears across the ant’s movements hence the ant movement path is cut off. Now the ants have to take diversion either left or right of the obstacle so that it can reach the food court. So at the point B there are two possible paths for the ants to reach the food source. Some of ants take a left diversion to reach E via B, H, D and E similarly few ants are taking a right diversion to reach the food source E. The probabilities of ant’s movement either left movement or a right movement is based on the pheromone intensity value laid by the explorer ants. The choice is influenced by the intensity of the pheromone trails left by preceding ants.

Figure 5.1 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. Initially, the explorer ant reaching at the point B (or D) has the same probability to turn right or left (as there was no previous pheromone on the two alternative paths). Since path BCD is shorter than BHD, the ant used the path BCD will reach the food court before the other ant which is used path BHD as in the
Figure 5.1c. 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 most of ants prefer the path DCB than 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 shortest 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 shortest path. From this experimental setup it is concluded that at a given point an explorer ant has to choose a path (normally a shortest path) 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 shortest path among different path in the network quoted by Marco Dorigo et al (1996) and Ping Wang et al (2001).

5.3.2 ANT Algorithm

Normally ants are preferred 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. Keeping this ants behavior in mind this thesis proposed a simple and proactive method named as an ant system based IP traceback implements to find the source of the attacks on the network.

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 used to finding the origin with a minimal length among the adjacent nodes.
In mathematics the distance between two points are calculated as follows. Assume that the length of the path between nodes \( i \) and \( j \) is \( d_{ij} \). This length is expressed and calculated by the Euclidean distance method as:

\[
d_{ij} = \sqrt{(X_i - X_j)^2 + (Y_i - Y_j)^2}
\] (5.1)

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 \( i = 1, 2, \ldots, n \).

Then the total numbers of ants are represented as: \( \sum_i^N b_i(t) \)

Hence 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 \( \tau_{ij}(t) \) be the intensity of trail on the 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:

\[
\tau_{ij}(t + n) = \rho \tau_{ij}(t) + \Delta \tau_{ij}
\] (5.2)
Where $\rho$ is a coefficient such that $(1 - \rho)$ represents the evaporation of trail between time $t$ and $t+n$ is given by,

$$\Delta \tau_{ij} = \sum_{k=1}^{m} \Delta \tau_{ij}^k$$  \hspace{1cm} (5.3)$$

$\Delta \tau_{ij}^k$ is the quantity per unit of length of trail substance (pheromone in real ants) laid on edge $(i, j)$.

Similarly by the $k^{th}$ ant between time $t$ and $t+n$ is given by:

$$\Delta \tau_{ij}^k = \begin{cases} 
\frac{Q}{L_k} & \text{if } k^{th} \text{ ant uses edge } (i,j) \text{ in its tour} \text{ (between time } t \text{ and } t+n) \\
0 & \text{otherwise}
\end{cases}$$  \hspace{1cm} (5.4)$$

Where \( Q \) is a constant

\( L_k \) is the tour length of the $k^{th}$ ant.

To avoid unlimited accumulation of pheromone trail the coefficient $\rho$ 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 associated with each ant with a data structure called the tabu list, that saved 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 $k^{th}$ ant, tabu$_k$ the set obtained from the elements of tabu$_k$, and tabu$_k$(s) the $s^{th}$ element of the list (i.e., the $s^{th}$ node visited by the $k^{th}$ ant in the current tour). The parameter
visibility $\eta_{ij}$, 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 Equation (5.1).

The transition probability of ant moves from node $i$ to node $j$ for the $k^{th}$ ant as:

$$p_{ij}^k(t) = \begin{cases} \frac{[\tau_{ij}(t)]^\alpha [\eta_{ij}]^\beta}{\sum_{k \in \text{allowed}_k} [\tau_{ik}(t)]^\alpha [\eta_{ik}]^\beta} & \text{if } j \in \text{allowed}_k \\ 0 & \text{otherwise} \end{cases} \quad (5.5)$$

Where $\text{allowed}_k = \{N - \text{tabu}_k\}$

$\alpha$ and $\beta$ 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 $t$ defined by Marco Dorigo and Thomas Stutzle (2010). Thus this concept may apply to other optimization problems like the asymmetric traveling salesman, the quadratic assignment and the job-shop scheduling.

### 5.3.3 Ant System based Traceback Technique

As per the earlier discussion of ant behavior, at time zero an initialization phase takes place during which ants are positioned on different nodes and initial value $\tau_{ij}(0)$ 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 next node to move with a probability that is a function (as in equation 5.5) of two desirability measures. Thus the trail $\tau_{ij}(t)$, gives information about how many ants in the past have
chosen that same edge \((i,j)\) with the visibility \(\eta_{ij}\), says the closer between the nodes. Obviously, setting \(\alpha = 0\), 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 \(\Delta \tau^k_{ij}\) are updated according to Equation (5.3). 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 \(NC_{\text{MAX}}\), 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 ant based IP traceback algorithm is described in Figure 5.2. 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 an 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 the pheromone intensity path is indirectly an attack path quoted by Ping Wang et al (2011).
Step #1: 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
\[ \Delta \tau_{ij} = 0 \]
Place the m ants on the n nodes

Step #2: Set s=1 where s is the tabu list index
For k = 1 to m do
Place the starting town of the k\textsuperscript{th} ant in tabu\textsubscript{k}(s)

Step #3: Repeat until tabu list is full
Set s=s+1
For k= 1 to m do
Choose the town j to move to with probability
\[ p_{ij}^k(t) \] Given by equation (5.5)
At time t the k\textsuperscript{th} ant is on town i=tabu\textsubscript{k}(s-1)
Move the k\textsuperscript{th} ant to the town j
Insert town j in tabu\textsubscript{k}(s)

Step #4: for k= 1 to m do
Move the kth ant from tabu\textsubscript{k}(n) to tabu\textsubscript{k}(1)
Compute the length L\textsubscript{k} of the tour described by the k\textsuperscript{th} ant
Update the shortest tour found
For every edge (i,j)
For k=1 to m do
\[ \Delta \tau_{ij}^k = \begin{cases} \frac{Q}{L_k} & \text{if } (i,j) \epsilon \text{ tour described by } \text{tabu}_k \\ 0 & \text{otherwise} \end{cases} \]
\[ \Delta \tau_{ij} = \Delta \tau_{ij} + \Delta \tau_{ij}^k \]
Figure 5.2 (Continued)

Step #5: For every edge (i, j) compute $\tau_{ij}(t+n)$

According to the equation $\tau_{ij}(t+n) = \rho \tau_{ij}(t) + \Delta \tau_{ij}$

Set $t = t+n$

Set NC=NC+1

For every edge (i, j) set $\Delta \tau_{ij} = 0$

Step#6: if (NC<NC_MAX)

Then

Empty all tabu lists

Go to step 2

Else

List out shortest tour path

Stop

Figure 5.2 The pseudo code of the proposed ant based IP traceback algorithm

5.4 IMPLEMENTATION AND EVALUATION

The performance of the proposed ASBITT algorithm for the detection of the attack source is analyzed by a series of experiments were conducted 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. Experiment is performed using the experimental topology setup shown in figure 3.8 constructed with 9 numbers of nodes. The details of the simulation parameters such as the simulation duration, experimental topology size, traffic type, number of nodes and the routing algorithm used are listed out in the Table 5.1.
In 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. Under normal network data transfer operation, data packets are flowing as usual hence each node receives a packet as per the user’s requirement. This scenario has changed by the involvement of the attacker by flooding of more numbers of requests; the victim node may receive more numbers of requests. Hence under abnormal network operation (after the involvement of attacker) naturally the victim node may receive frequent requests from the attacker.

Under this scenario the source of the attack is to be identified by the implementation of the traceback technique. In this experimental setup an ant system algorithm is used to traceback the origin of the attacker and finally all possible paths are identified.

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

As per the natural behavior of ant, the majority of the ants choose the shortest path to reach their food source. During the first iteration the
explorer ant finds out the shortest path to reach the food source. While searching the path these ants laid a chemical like substance called as a pheromone. Frequent users of path have more pheromone intensity. Experimental results are listed out in the Table 5.2 it shows the details of possible path with the pheromone intensity of each path for the first iteration output.

The experimental result implicates that maximum numbers of data packets are flooded on the shortest path 1->3->6->9. Figure shows the graphical representation of the scenario discussed. Since more requests are flooded by the attacker from their origin, more numbers of the packets are reaching the victim. Since the experimental setup executed the ant system algorithm more ants are used the shortest path (1->3->6->9) to reach the victim. From the obtained result it is easy to find the victim and attacker node.

As per the design architecture of data network, data packets are changes its routes dynamically through different data network based on the changes in the network path. Thus the network routing methodology in the data network each packet is travelled individually and use different route path to reach the destination. Hence to find out the exact shortest path and the origin of the attack request the same procedure is repeated for more number of times.

In the ant colony algorithms, the identification of the best solution is achieved by increase the number of iterations. Since the pheromone intensity values are updated for the each and every iteration, to find out the maximum pheromone intensity values, the same experimental setup is repeated for more numbers of times. In this experimental analysis the iteration procedure is repeated for 6 numbers of times. The obtained experimental values are tabulated in the table 5.2 which shows the consolidated
representation of 6 iteration values of all possible paths with their pheromone intensity value. From the obtained values the attacker source is identified easily. Thus from the obtained experimental results it is confirmed that the maximum contribution of pheromone intensity lies only in the path 1->3->6->9. Since more numbers of ants are used the same path it is concluded that node 1 is the attacker and node 9 is the victim node. Similarly Figure 5.3 shows the graphical representation of all six numbers of iterations. The snap chart of simulation output all iterations results are consolidated and it is shown in the Figure 5.4.

Table 5.2  Details of possible path with pheromone intensity of each path for Iterations 1- 6

<table>
<thead>
<tr>
<th>S.No</th>
<th>Path Node</th>
<th>Hop Count</th>
<th>Pheromone Intensity</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>Iteration 1</td>
</tr>
<tr>
<td>1.</td>
<td>1-&gt;4-&gt;7-&gt;8-&gt;9</td>
<td>4</td>
<td>1.6</td>
</tr>
<tr>
<td>2.</td>
<td>1-&gt;4-&gt;5-&gt;8-&gt;9</td>
<td>4</td>
<td>1.31</td>
</tr>
<tr>
<td>3.</td>
<td>1-&gt;3-&gt;5-&gt;8-&gt;9</td>
<td>4</td>
<td>1.11</td>
</tr>
<tr>
<td>4.</td>
<td>1-&gt;4-&gt;3-&gt;5-&gt;8-&gt;9</td>
<td>5</td>
<td>0.69</td>
</tr>
<tr>
<td>5.</td>
<td>1-&gt;3-&gt;6-&gt;9</td>
<td>3</td>
<td>2.03</td>
</tr>
<tr>
<td>6.</td>
<td>1-&gt;2-&gt;6-&gt;9</td>
<td>3</td>
<td>1.62</td>
</tr>
<tr>
<td>7.</td>
<td>1-&gt;3-&gt;5-&gt;7-&gt;8-&gt;9</td>
<td>5</td>
<td>0.59</td>
</tr>
<tr>
<td>8.</td>
<td>1-&gt;3-&gt;4-&gt;5-&gt;6-&gt;9</td>
<td>5</td>
<td>0.23</td>
</tr>
<tr>
<td>9.</td>
<td>1-&gt;4-&gt;7-&gt;6-&gt;8-&gt;9</td>
<td>5</td>
<td>0.8</td>
</tr>
<tr>
<td>10.</td>
<td>1-&gt;3-&gt;5-&gt;7-&gt;8-&gt;9</td>
<td>5</td>
<td>1.1</td>
</tr>
</tbody>
</table>
Figure 5.3 Possible path with their pheromone intensity – Iteration #1-6

Figure 5.4 Possible path with their pheromone intensity - snap chart
5.5 SUMMARY

Network 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. This chapter explained the concepts of 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 the 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 setup.

Simulation results are also confirm this concept by showing the 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 thesis concludes that the proposed solution is an efficient method to find out the DoS attack origin in the networks. The proposed method identified the origin of the attacker by considering both the shortest path and with their intensity of the pheromone values. From the experimental result it is found that it is a simple and effective technique for the identification of the source of the attack.