CHAPTER IX
SUMMARY AND FUTURE DIRECTIONS

9.1. CONTRIBUTIONS

In this thesis, swarm based Intrusion detection and defense mechanism is performed for the various routing and MAC layer attacks in MANET. This work is evaluated under the MANET environment using the performance metrics such as throughput, packet delivery ratio, end to end delay, energy consumption, packets drop, detection accuracy and percentage of false detection. The conclusion of the evaluation is given below.

In chapter three, the swarm based intrusion detection (SDIDS) is developed for the various routing attacks by creating n nodes in the MANET environment. The source node selects the active nodes from these n nodes by employing the forward ants (FAs) and backwards ants (BAs). These FAs and BAs are responsible for calculating the parameters namely residual energy, residual bandwidth, connectivity criteria and trust value. Then the source node selects the active nodes in the selected route with the highest residual energy, highest residual bandwidth and highest trust value. Because they should live longer to monitor the neighboring nodes. Then these active nodes monitor their neighboring nodes such that the trust value of these neighboring nodes should be above the minimum threshold value. If it is not so, those nodes are identified as the malicious nodes. For each identified malicious node, an alert message is given to the source node by the corresponding active node. Hereafter these malicious nodes are not involved in the data transmission. The performance of SDIDS is compared with already existing DTMF and found that SDIDS performance is better than DTMF.

In Chapter four, the Swarm based defense mechanism (SBDT) is performed to filter the malicious nodes in the path selection process. For this proactive secret key sharing, certificate renewal process and certificate revocation scheme are employed to filter the identified malicious nodes. After a specified time period t, every node involved in the data transmission applies for the certificate renewal process. Only for the
valid nodes certificates are renewed whereas for the malicious nodes, the certificates are not renewed and are added in the certificate revocation list (CRL). The nodes that are in the CRL are also broadcast to all the valid nodes in the MANET environment so that every valid node will omit these revoked nodes in the path selection for data transmission. By this technique only valid nodes take part in the communication and are regularly renewed as the valid nodes and all the identified malicious nodes are placed in the CRL. Then the performance of SBDT is compared with the already existing CAPMAN and found that SBDT is better than CAPMAN.

In Chapter five, the swarm based intrusion detection (SBDT-NB) is performed for the routing and MAC layer attacks using neighbors monitoring scheme in MANET. Here the swarm agents are employed to find the mean value of the nodes using the time of receiving RREQ and RREP packets. Then the source node verifies whether the mean value of any node is greater than the minimum route discovery threshold value. If it is so then that node is identified as the malicious node; Otherwise the node is identified as the valid node. It is how the node state1 is determined by the routing layer. This is used for identifying the routing layer attacks. To identify the MAC layer attacks, four parameters are used namely number of neighbors identified by the MAC layer, number of neighbors identified by the routing layer, the number of recent MAC receptions and the number of recent routing protocol receptions. It is how the node state2 is determined by the MAC layer. If either node state1 is malicious or the node state2 is malicious, then that node is not involved in the path selection. The source node uses these two node state estimation techniques to construct the reliable path to the destination. The performance of SBDT-NB is also compared with CACD and found that SBDT-NB is better than CACD.

Then the swarm based intrusion detection (SBDT-CL) is also performed for the routing and MAC layer attacks in MANET using the RTS/CTS scheme in MANET. Here also the swarm agents are employed to find the mean value of the nodes using the time of receiving RREQ and RREP packets. Then the source node verifies whether the mean value of
any node is greater than the minimum route discovery threshold value. If it is so then that node is identified as the malicious node. Otherwise the node is identified as the valid node. It is how the node state1 is determined by the routing layer. This is used for identifying the routing layer attacks. To identify the MAC layer attacks it uses the RTS/CTS scheme. Here every node involved in the path verifies whether the response for the RTS is received within the maximum back off timer value or not. If it is received within the maximum back off timer value then the node is identified as the valid node. Otherwise it is identified as the malicious node. It is how the node state2 is determined by the MAC layer. If either node state1 is malicious or the node state2 is malicious, then that node is not involved in the path selection. The source node uses these two node state estimation techniques to construct the reliable path to the destination. Then the performance of SBDT-CL is also compared with CACD and found that SBDT-CL is better than CACD.

In chapter six, two swarm based intrusion detection systems are compared and evaluated against the various performance metrics namely throughput, packet delivery ratio, packets drop and energy consumption. In the first swarm based intrusion detection technique (SDIDS1), Forward ants (FAs) and backward ants (BAs) are employed to select the active nodes. For this FAs and BAs calculate the residual energy, residual bandwidth, connectivity and trust value. The nodes with the highest residual energy, residual bandwidth and trust value are selected as the active nodes. Now these active nodes monitor their neighbor nodes to identify the malicious nodes. If the active node finds that its neighbor node is having the trust value which is below the minimum trust threshold, then that node is identified as the malicious node. In the second swarm based intrusion detection technique (SDIDS2), two phases are employed to identify the malicious nodes. In the first phase of SDIDS2, during the route discovery time, forward and backward ants are employed to identify the mean value of the nodes. Then the source node verifies whether the mean value of any node is below the minimum route discovery threshold value. If it is not so, then the node state1 of the node is set to be malicious. In the second phase of SDIDS2, FAs and BAs are employed to calculate the trust value of the nodes. If the trust value of
nodes is below the minimum trust threshold, then the nodestate2 of the node is set to be malicious. In SDIDS2, the nodes are used for the path selection only if both its notestate1 and nodestate2 are valid. The performance of SDIDS1 is also compared with SDIDS2 and found that SDIDS2 is better than SDIDS1.

In chapter seven, the performance of Swarm based Intrusion detection system is also verified under various mobility conditions namely low mobility, medium mobility and high mobility. For this, three (Swarm based Intrusion detection) SBDTs are created namely SBDT-LOW-MOBILITY, SBDT-MEDIUM-mobility and SBDT-HIGH-MOBILITY. In all the three SBDTs, the nodes with the highest trust value, residual bandwidth and residual energy are selected as active nodes using the swarm agents. Every active node examines its neighbor nodes within its radio transmission range and gathers the trust value from all monitored nodes. The active nodes will always be changing as per the trust thresholds. Upon collaborative exchange of the trust values of the monitored nodes among the active nodes, if the active node finds any node below a minimum trust threshold, then the node is marked as malicious. When the source node receives an alert message about the malicious node, a defense technique is deployed to filter the corresponding malicious node from the network. By simulation results, it is shown that the SBDT-HIGH-MOBILITY is producing better results while varying the nodes and SBDT-LOW-MOBILITY is producing better results while varying the attackers. From this it is found that the mobility condition also plays a major role during the swarm based intrusion detection.

In chapter eight, the performance of Swarm based Intrusion detection system is also verified under various mobility models in MANET. The various mobility models used are Random waypoint mobility model, Random walk mobility model and Random direction mobility models. Here the nodes with highest trust value and residual bandwidth are selected as active nodes using the swarm agents. Every active node examines its neighbor nodes within its radio transmission range and gathers the trust value from all monitored nodes. The active nodes will always be changing
as per the trust thresholds. Upon collaborative exchange of the trust values of the monitored nodes among the active nodes, if the active node finds any node below a minimum trust threshold, then the node is marked as malicious. When the source node receives alert message about the malicious node, a defense technique is deployed to filter the corresponding malicious node from the network. By simulation results, it is shown that the Swarm based intrusion detection using random direction mobility model is producing better results, while varying the attackers and speed. So the mobility model also plays a major role during the intrusion detection.

9.2. FUTURE SCOPE

In this thesis, we have restricted ourselves to the design of swarm based intrusion detection system using Ant Colony Optimization (ACO) alone. We have not dealt with other forms of swarm based intrusion detection such as PSO, etc. In future we can compare the performance of ACO based intrusion detection with PSO based intrusion detection.

We have also restricted ourselves to the swarm based intrusion detection technique using distributed nature. In future we can also extend the swarm based intrusion detection using hierarchical nature or cluster based nature. Then we can compare the distributed swarm based intrusion detection technique with the cluster based swarm based intrusion detection technique and hierarchical based swarm based intrusion detection technique.

We have restricted ourselves to identify the routing attacks during route discovery and data transmission phase. In Future, we can design the swarm based intrusion detection for the route maintenance phase also.

Moreover, we have restricted ourselves to the routing and MAC layer attacks. In future we can also extend the intrusion detection operation to other layers such as physical layer, transport layer and application layer.
AUTHOR’S PUBLICATIONS / COMMUNICATIONS

INTERNATIONAL JOURNALS


COMMUNICATED TO INTERNATIONAL JOURNALS
1) G.Indirani, Dr.K.Selvakumar, “Swarm based detection and defense technique for cross-layer attacks in MANET”, Wireless Networks [Under Review].

INTERNATIONAL CONFERENCES


2) G.Indirani, Dr.K.Selvakumar and V.Sivagamasundari, “Intrusion detection and defense mechanism for Packet replication attack over MANET using Swarm Intelligence”, PRIME 2013, Periyar University,2013, Salem.

3) G.Indirani, Dr.K.Selvakumar and V.Sivagamasundari, “Intrusion detection and defense mechanism for route cache poisoning attack over MANET using Swarm Intelligence”, ICCIAMR 2013, Vels University, Chennai.

NATIONAL CONFERENCES

1) G.Indirani, Dr.K.Selvakumar and R.Mohanapriya, “Intrusion detection and defense mechanism for wormhole attack over MANET using Swarm Intelligence”, NCCT, University College of Engineering, Villupuram, 2013.