CHAPTER 6
CONCLUSION AND FUTURE WORK

6.1 CONCLUSION

In MANETs, communication channel is accessible to both legitimate users and malicious attackers. Consequently, there is an increasing need for security solutions with extensive protection and desirable network performance. Three techniques, namely, Intrusion Detection System using classification mechanism, Trusted Dynamic Source Routing to Mitigate attacks and Optimal Swarm based trusted mechanism have been proposed in this thesis to identify and isolate faulty nodes in the network.

First, the classification accuracy of three popular algorithms Naïve Bayes, Random forest and CART is investigated in the proposed intrusion detection system analysis. Two different datasets are used in this work, one with few anomalous data (20%) and the other containing more anomalous data (60%). As MANET’s operate in power constrained environments, reducing the computational time is essential and hence only 65% of the attributes from training dataset are used. The classification accuracy obtained using the proposed approach is greater than 99.9%. It is also found that decision tree based algorithms are capable of identifying intrusions with more accuracy when compared to Naïve Bayesian method.
In this thesis, a trust based routing methodology which mitigates security threats by isolating malicious nodes is proposed. In this work, the behavior of DSR protocol with and without the black hole attack is investigated. As ad hoc networks are formed by cooperative dynamic nodes, i.e. nodes joining and leaving the network any time, it is difficult to maintain security mechanisms centrally. In this work, the DSR header is modified to carry an additional payload i.e. the computed trust values for every node in the network. The average number of hops is increased by 4.15% in the proposed trust based algorithm when compared to Dynamic Source Routing (DSR) protocol. The increased end-to-end delay is due to the control packet overhead in finding the route with trusted nodes. However, the throughput using the proposed trust based algorithm is in par with DSR.

Finally, an Ant Colony Optimization is proposed in this thesis to select the best path which has all intermediate nodes as trusted nodes. Simulations are conducted with on demand DSR routing and the proposed trust based Ant Colony Optimization (ACO) routing. Performance is evaluated by measuring packet delivery ratio, end-to-end delay and packet loss ratio. Results show that the proposed trust based ACO routing has 3.45% more packet delivery ratio and 1.75% less packet loss ratio when compared to the conventional DSR algorithm. However the proposed method incurs a little delay which is mainly due to verifying trust factor of all intermediate nodes in a path during data transmission.

6.2 FUTURE WORK

In this thesis, the proposed intrusion detection for three popular classification techniques is tested on a network with 50 nodes. Studying the
scalability issues by taking a larger network with more than 200 nodes is an interesting problem. The proposed trust based model uses Random Way Point (RWP) model for nodes with constant mobility speeds. This could be extended for different mobility models such as temporal dependency, spatial dependency and geographic restrictions. The DSR protocol is appropriately modified to include the trust based ACO algorithm to find optimal route between source and destination. Extending the proposed trust based ACO methodology to other protocols such as AODV and GRP is an interesting open problem. Similarly the proposed technique can be investigated for wormhole attack, grey hole attack and sybil attack. It would be interesting to study the proposed technique with other variances of wireless network such as VANET and Wireless Sensor Network.