CHAPTER 6

CONCLUSION

MANET is a self organized network without depending on the pre-existing network infrastructure. It is an autonomous system, in which mobile nodes connected by wireless links are free to move randomly. MANETs are gaining great importance all over the world due to its dynamic nature and ease of deployment without any base station. In MANETs, MAC layer misbehavior is an important research domain to improve the security of the network.

In recent years, ad hoc networks mainly focus on achieving fairness and increasing spatial reuse through the distributed contention based shared algorithms. Misbehavior is one of the major problems in MANET implementation. It may seriously degrade the performance of the network. MAC layer uses a CSMA/CA mechanism to access the wireless channel. However, it is easily vulnerable to different types of attack due to the absence of centralized administrator.

There are several reports on the reduction of misbehavior in MANET. It is observed that various types of MAC protocols are demonstrated to ensure fairness in the network. Most of the MAC protocols are designed based on the trust of receiver or AP. This assumption cannot be true for all the time. Few protocols are designed to detect the misbehavior based on MAC protocol modification and hardware implementation. These
protocols require implementation cost. Hence, it is necessary to design a fair MAC protocol to improve the security and network performance.

6.1 CONTRIBUTION OF THIS RESEARCH WORK

In this work, three algorithms are developed to detect the malicious nodes and provide fair access to the channel. Through extensive simulation, it is shown that the proposed protocol perform very well in terms of throughput, packet delivery ratio and detection ratio achieved by means of fair access.

The following are the major contributions in this work:

A wide-range of the various MAC protocols was studied. This suggests that the MAC layer misbehavior through the modification of the IEEE 802.11 MAC protocol and the trust based detection were proved to be a good solution in order to detect and penalize the malicious nodes. Hence, it is mandatory to define any one of the node which is assumed to be trusted. This enables the researcher to attain the objectives in the different parameters.

In the first method, a new algorithm is proposed to detect the malicious nodes participating in the TO attack and the performance is evaluated. A TMDA is developed to detect both sender misbehavior and receiver misbehavior.

By using the TMDA algorithm, the throughput value is found to be increased, which indicates that the performance enhancement in the throughput is significant compared to IEEE 802.11 MAC protocol. It is also found that on applying the TMDA algorithm, the frame delivery ratio is increased linearly with the increasing number of nodes. The study on the
effect of delay with the number of nodes using TMDA algorithm showed insignificant effect compared to IEEE 802.11. However, the delay in TMDA is balanced due to the reduction of misbehaving nodes, which in turn increases the overall network performance. By measuring the TO$_{CTS}$ actual value using TMDA algorithm, this method makes the misbehavior detection easier by simple comparison.

This type of algorithm helps to minimize the number of misbehaving nodes participating in the network and also significant gains in terms of throughput, packet delivery ratio and correct detection ratio. It also decreases the delay considerably.

The second method also deals with the detection of TO attack using the particle swarm optimization. It is a stochastic population based heuristic search technique which imitates finding food principle of bird swarm. In PSO, each particle represents a potential solution within a search space. PSO has attracted many significant attentions from the researchers due to good performance, low computational cost and easy implementation. PSO maintains a swarm of candidate solutions referred to as particles. Its key concept is that, particles are flown hyper dimensional search space and each particle being accelerated towards the best optimum solution found by the particles neighborhood.

The ability of the particle swarm optimization algorithm is analyzed and proved that the performance of the throughput increases with decreasing the number of misbehaving nodes. The misbehavior percentage estimated using swarm size indicated that the large swarm size causes more complexity. The effect of inertia on the misbehavior percentage indicated that the smaller
inertia, the misbehavior percentage is very high and for the medium and large inertia, the misbehavior percentage was found to be zero.

The study on the effect of iterations with percentage misbehavior also found that the misbehavior percentage decreases with increase in iterations. The quality of solutions of PSO preponderates by reducing the iterations. The performance of the PSO algorithm is evaluated and compared with PSO and without PSO algorithm.

In the third method, a RCCA algorithm is developed to prevent the collisions in two hop neighbours. Using this algorithm, number of RTS-CTS collision is reduced considerably compared with the IEEE 802.11 MAC protocol. During the collisions, a selfish node is trying to choose small backoff value to get more access than the well behaved nodes. Hence indirectly the selfish misbehaving nodes are prevented. Here the RTS-CTS collisions are avoided by introducing CAP. Hence, The proposed RCCA algorithm increases the throughput and PDR compared with the IEEE 802.11 MAC protocol. Delay and number of RTS-CTS collisions are decreased significantly.

In the present investigation, the above mentioned methods proved to be a suitable alternative to improve the throughput, packet delivery ratio, correct detection ratio, misdetection ratio and reduces the delay, which indicated that the performance of the network has increased considerably after implementation of the above mentioned methods.
6.2 FUTURE DIRECTIONS

- The PSO algorithm utilized in this work is to find the optimal values which are used to prevent misbehaving node. A new algorithm would be developed to optimize the backoff window.

- Develop an algorithm to support fair bandwidth allocation along with channel utilization.

- Develop a protocol without manipulating the IEEE 802.11 MAC and provide fair channel allocation.