ABSTRACT

Mobile Ad hoc Networks are gaining great popularity and getting deployed all over the world due to its dynamic nature and ease of implement without any base station. One of the most popular MAC protocols in wireless local area networks is the Carrier Sense Multiple Access (CSMA) for scheduling the network access. Wireless Medium Access Protocols (MAC) such as IEEE 802.11 use distributed contention resolution mechanisms for sharing the wireless channel. The wireless networks are easily vulnerable to attack and impose additional constraints on the design of communication protocols due to lack of central management. Certain participants would try to exploit the autonomous nature to obtain more gain such as higher throughput and bandwidth than the well behaved nodes. This gain is always achieved at the expense of well behaved participants that hold on to the communication rules.

Malicious node does not follow the IEEE 802.11 MAC protocol rules. Instead, they disobey by selecting either a smaller backoff value or by choosing Short Distributed Inter Frame Space (S-DIFS) where it does not double the backoff value after collision. Chances of accessing the channel increases by the misbehaving nodes which modifies the protocol parameters such as by decreasing its DIFS or by transmitting frame after SIFS. This type of attack can be defined as Time-Out (TO) attack. This work proposes three novel methods to detect TO attack in order to improve the security and
network performance. The NS-2 simulator is used to study the performance of the above mentioned methods.

The first method, Timeout Misbehavior Detection Algorithm (TMDA) is used to detect and penalize the misbehaving nodes. Initially the expected TO\textsubscript{CTS} value (TO\textsubscript{CTS}) is calculated. During the frame transmission, the algorithm computes the TO\textsubscript{CTS} actual value and at each iteration, this value is compared with TO\textsubscript{CTS} value. If both the values are equal then there is no misbehavior and the algorithm will stop. If the values are not equal, then the misbehavior is detected and the algorithm monitors the communication of the particular node for a particular duration which is set based on a threshold value. The threshold value is determined by the number of times a node’s misbehavior can be pardoned. If the number of misbehavior equals the threshold value, then the node is deviated from the network. The modified Request-To-Send (RTS) frame is designed to identify the Media Access Control (MAC) layer misbehavior using IEEE 802.11 Distributed Coordination Function (DCF) mode. The goal of the modified RTS (T-RTS) packet is to simplify the misbehavior detection. T-RTS packet contains TimeOut Bit (TOB), which is set to 1 if misbehavior exists.

To identify the sender or receiver misbehavior, compare the TO\textsubscript{CTS} with the TO\textsubscript{CTS} actual. If TO\textsubscript{CTS} is greater than TO\textsubscript{CTS} actual then it is said to be sender misbehavior. If the value is less then it is said to be receiver misbehavior. After detecting the misbehaving node, the correction procedure
has been carried out. The performance of the proposed protocols is analyzed in terms of the throughput, packet delivery ratio, delay, misdetection and correct detection ratio. The simulation is performed using Network Simulator – 2 (NS-2). On comparing, the performance of the TMDA with IEEE 802.11 MAC, it is observed that TMDA achieves better throughput, packet delivery ratio and correct detection ratio.

The second method uses Particle Swarm Optimization (PSO) algorithm which improves the security in order to detect and penalize the misbehaving nodes. At the initial stage of PSO, initial population of particles with random positions and velocities is created. In consequent iterations, each particle adjusts its position and velocity by its own experience or from other particles information. The performance of each particle is measured according to a pre-defined fitness function. Here the inertia weight $\omega$, is employed to balance the local and global exploration abilities. The PSO algorithm searches for the best value of SIFS and $T_{O_{CTS}}$ of each node $i$. Based on the deployment decision at time $t$, the locations of the misbehaving nodes at time $t + 1$ are determined.

The performance of the PSO algorithm is evaluated by comparing with and without the PSO algorithm. Based on the results, the performance of the PSO is evaluated and it is observed that, the throughput and packet delivery is increased significantly after implementing the PSO algorithm.
The third method, a RTS-CTS Collision Avoidance (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 collisions, selfish nodes try to choose a small backoff value to get more access than the well behaved nodes. Hence, the selfish misbehaving nodes are prevented indirectly. Here the RTS-CTS collisions are avoided by introducing Collision Avoidance Packet (CAP). CAP contains Active Neighbour Bit (ANB) bit, which gives information about whether any communication is going on within the transmission range. Based on this information, the nodes can decide themselves to send the data packet or to stop the communication.

The performance of the RCCA algorithm is compared with IEEE 802.11 MAC protocol. It is also observed that, the RCCA performs better in terms of throughput, packet delivery ratio and correct detection ratio. The delay is also reduced considerably for the above proposed protocol.