CHAPTER 6

CONCLUSION AND FUTURE ENHANCEMENTS

6.1 SUMMARY OF WORK DONE

Many challenges are being faced by researchers in designing an energy efficient and secure routing protocol for MANET using BCO (Bee Colony Optimization).

The work carried out in this thesis is the designing of the two protocols

- BM-AODV
- BEEM-DSR

to improve the energy efficiency and secured routing by mitigation of blackhole attack during transmission.

The proposed Bee Mating Ad-hoc Demand Distance Vector Routing Protocol (BM-AODV) is an improved version of AODV routing protocol. This improvement is achieved by using the honey bee mating optimization principle. The BM-AODV chooses routes by considering the nodes energy level and shortest distance uniformly. BM-AODV runs with the iterations of Queen selection, drone selection, and brood production. This causes the load to be distributed uniformly among routes and leads to increased life time of the network.
Initially the energy list is created in each node to store the energy level of the corresponding node. Here, the energy of the node is compared to the bees life time. The energy is calculated by using the energy formulae. The neighbour node to the source node acts as an intermediate node (drone) and next node to intermediate node (drone) acts as a next neighbour node (brood). The neighbour node having higher energy transmits data to the destination. Hence, this action maximizes the lifetime of network and provides an effective multipath data transmission in an efficient manner. The performance of the protocol is compared with the existing protocols using simulation. Based on the results the BM-AODV protocol proved better performance with higher packet delivery ratio, reduced delay, energy utilization and blackhole detection when compared to the existing AODV, BCO, PEEBR routing protocol.

The proposed Bee Mimetic Dynamic Source Routing Protocol (BeeM-DSR) is an enhancement of DSR routing protocol for mobile ad hoc networks to ensure secure routing in MANET. This improvement is achieved by using the bee food search principle. The MANET network is considered as a colony of artificial bees. This colony consists of three groups of bees: Scouts (source node, Si) they are sent when a scouting process is initialized in order to discover new paths towards a given destination.

Each node maintains one cache for storing the routing information such as energy of the nodes, hop count, Des_Seq_No, timer and all the employee bees selects the recent shortest route, if the scout bee wants to send any packet that broadcasts a RREQ (route request). The request reaches the foragers via employee bee and the foragers send the RREP (route reply) based on shortest path which is recent. Then, through the RREP path the scouts transmit the packets to foragers. The experiments for the evaluation of the
scheme against packet delivery ratio and end to end delay are carried out using the network simulator. The results proved improved performance when compared to existing schemes in terms of packet delivery ratio and reduced delay.

The proposed Bee Mimetic process uses the Artificial Bee Colony algorithm to detect the Black Hole Attack. The Scout bees are used to search the black hole node. The Employee bee informs the network for the Black Hole node, thus by identifying the blackhole node, that node can be omitted from the network.

Bee Mimetic –Mitigation Of Blackhole Attack Algorithm (BeeM-MBA) algorithm is used to identify and to remove black hole attack in dynamic network. The principle of this algorithm is each cache of a trusted node is set with destination sequence number. After route discovery it is necessary to check whether the route is secure or not. To do so, the DSN is compared with the threshold value by scout bee. If the DSN value is greater than the threshold value then it is identified as a malicious node. After detecting the malicious node the dictator node sends the groupID to trusted node having DSN. The node having the groupID only can transmit the RREP to the scout bee($S_b$). Hence, the malicious node is detected and removed from the network and the data packets are transmitted securely by using BeeM-MBA algorithm.

The performance of the protocol is compared with the existing protocols using simulation. Based on the results the BeeM-MBA algorithm proved better performance with blackhole detection when compared to the existing protocols.
6.2 FUTURE ENHANCEMENT

The proposed method has improved the energy utilization for 50 nodes and it can be extended to more number of nodes to reduce the energy conservation. The blackhole attack detection was 20% - 40% which can be improved further to achieve better performance by using other protocols with the use of some machine learning techniques.