CHAPTER 7

CONCLUSIONS AND FUTURE WORK

7.1 CONCLUSIONS

The secure key model facilitates secure successful communication between the nodes in the network without any loss of data. The security of the communication is better in the secure key model with the operation of reputation system, ranking in node clustering and group key agreement protocol. The reputation system expertly determines the reputation value based on the threshold value. The reputation value rejects the unauthenticated node to involve in the communication. The rank is designed with reputation value in the ranking model. The ranking model clusters the nodes efficiently and selects the cluster head for an improved outcome in packet transmission. The cluster head is elected from the group formation based on the best threshold value of nodes. In order to enhance the lifespan of the network, the secret key is created and circulated by all cluster heads.

Authenticated group key agreement protocol chooses the secret key in authenticating group. As a result, not only the malicious nodes are avoided, the node attack and communication failure are also avoided. The authenticated group key agreement protocol also guides to pass the packet data in an efficient manner. The performance evaluation showed that the secure key model supports secure communication in ad hoc network in terms of malicious node detection efficiency, node reputation, performance rate in node clustering and computational cost. The results also showed 30% higher
percentage in detecting malicious node, improving the security in MANET. Finally, SKM performs well in providing secure communication over the nodes in the network.

The hybrid approach for node co-operation based clustering in MANET is based on the node cooperativeness range reducing the chance of message loss. After estimating the cooperativeness range of each node, the reorganization of nodes take place in its own. In order to improve the lifespan of the network, node cooperativeness range is computed. Based on the range, the clustering and communication process is done. Then, the clustering of node is carried out efficiently and the CH is elected for enhancing the good transmission over the network. As a result, not only the malevolent nodes are discarded, the communication failures are also highly reduced. Finally, the hybrid approach for node cooperation based clustering enhances the security level through forecasting weightage of node cooperativeness and increases network lifespan by self-organizing the nodes. The experimental results showed that the hybrid approach for node cooperation based clustering perform well in a secure communication over the nodes in the MANET network in terms of node cooperativeness of about 20-25% compared to an existing FESCIM model and ERP-SCDS.

Efficient node cooperation and security mechanism defeats the existence of selfish nodes in MANET with node cooperation by generating authentication among nodes through node cooperation. The ENCS mechanism supports high security by eliminating the misbehavior nodes from replacing the security associations with unidentified nodes. Security associations are only replaced with nodes in trusted community, enhancing the security inside group of trusted nodes. Security associations presented the realization of features in every node inside the group. The security features are selected based on the validation of common usage of nodes in the
specified network. Experimental results showed that the ECNS mechanism outperforms well in terms of packet transmission efficiency, average information leakage, average cost and security level in the range of 15-25% high compared to the existing value iteration algorithm and ODMRP-HT.

Routing aware packet reserving framework in MANET considers the end to end routing condition with maximal throughput. RAPR is complimentary system where the packet reserve utilizes local routing information. The local routing holds the information of the node clustering, node co-operation and security level. RAPR follows the approach of shortest path travel earlier approach. The mobile nodes select the packet which travels in shortest distance earlier from the queue to reduce the delay count. Path setup in RAPR estimates the security level of the system, and symbolizes the end-to-end routing by controlling the clogging. RAPR reaches the packet to the destination with high probability ratio and minimal delay count. Simulation results attain the maximal network security level, end to end throughput rate and resource utilization efficiency. On the other hand simulation results also reduce the communication overhead, cost and delay time in RAPR framework. Finally, RAPR designed to perform effective resource utilization with 15.3% improved end to end throughput maintenance.

7.2 FUTURE WORK

The security of the communication is enhanced in the secure key model with the utilization of reputation system, ranking in node clustering and group key agreement protocol. As the ranking process involves calculation of nodes activity and computation of forwarding time, it results in high computational cost. Future work may be planned to reduce the computational time. In group key agreement the fact that a group member will compute a bad key remains unnoticed, mostly if the group is huge. As authenticated group key management prevents any exchange of messages only with two users.
However, there are limitations of reputation based mechanism. First, as there is a probability of collision, a packet obviously drops even in the nonexistence of a selfish node. This makes it hard to determine whether the packet drop is due to normal reasons or selfish behavior of node. Second, the selfish nodes isolated from the network using reputation based scheme cannot be used in data forwarding.

Hybrid approach in node cooperation based clustering will be unable to co-operate nodes, if data is forwarded using a different path without complaint. Another limitation of node cooperation is when a node has enough recognition to send its own data; it decides not to cooperate anymore and starts dropping packets. Further, efficient technique will be required to control the dropping of packets, if node cooperation fails. Again in efficient node cooperation and security mechanism the time taken to evaluate quantitative trust value is high. Future work may plan in reducing the time consumption of evaluating trust values.