CHAPTER 7

CONCLUSIONS AND FUTURE WORK

7.1 Summary and Conclusions

The prime objective of the thesis was to develop secured routing protocol using trust estimation model. For achieving this we have gone throw a detailed literature survey. In the process first we have carried out a detailed ns2 based comparative simulation study of the performance characteristics of DSDV and DSR. The simulation results show that at higher mobility DSR outperforms DSDV in terms of packet delivery performance. At lower mobility, however, DSDV performs better than DSR. For average end-to-end delay we see that DSDV has less delay in comparison to DSR. The network being relatively stable, at the time of packet delivery, all the routes are already available in DSDV due to its proactive nature. This results in greater packet delivery fraction. Hence, in DSDV, nodes need to exchange only incremental dumps rather than full dumps. This results in lesser overhead of DSDV. Thus we can conclude that if routing delay is of little concern, then DSR shows better performance at higher mobility in terms of packet delivery fraction and normalized routing load in hybrid networking scenario. Under less stressful scenario, however, DSDV outperforms DSR in terms of all three metrics.

Secondly a Trust model is developed for secured routing in MANET. MANET is often attacked by malicious nodes. For a better MANET, an efficient security model is needed to counter attacks on security. In this thesis, a new trust establishment scheme is used to detect and prevent routing attacks. The trust function is used in DSR protocol. A reasonable outcome is observed. Then again the model has been improved by modifying the trust function. The simulation result shows the improvement in the efficacy and efficiency of the proposed model. The improved trust model is able to improve performance of DSR protocol upto a notable degree in case of route modification, packet dropping and flooding of nodes.

Also the trust model is modified for prevention of blackhole attack. In the model, the DSR header file is modified to measure trust in the network. The proposed TIDSR

improves the network performance at approximately 11% without compromising to security although it has increased the intermediate hop count little more.

By using the trust functiont a security solution of grayhole attack is developed. The performance of the proposed technique is evaluated with respect to routing overhead, PDR, dropping nodes and throughput. The performance matrix shows a reasonable outcome. Also to mitigate the dishonest recommendation problem a recommendation based trust model has been developed to mitigate the dishonest recommender problems. The research work carried out in this investigation contributes the design and development of trust model for securing the MANET. The trust model is able to prevent various attacks such as flooding, route modification and packet dropping up to a reasonable extent. Also the trust model designed is able to prevent blackhole attack as well as grayhole attack. The model designed in this study can further be applied in preventing other security threads and also applicable to other routing protocols by petty modification. These enhance the general applicability of the work performed in the thesis.

7.2 Future Scope of Work

When a significant progress in the security of MANET is made using trust function in this study, the performance of the MANET protocols can be further improved using a more secured trust model. Also the trust model can be applied in all routing protocols in hybrid environment. The performance of the hybrid protocol can be further improved by adjusting the algorithmic framework of the technique. Also the trust model can be further extended in pervasive computing environment by modifying only in the algorithmic approach of the routing technique.