CHAPTER 7

CONCLUSION AND FUTURE WORK

7.1 THESIS CONTRIBUTIONS

This thesis proposes the design of a novel clustering approach that offers energy-efficiency and security in MANET. The goal of the thesis is improving the energy-efficiency and security for MANET by providing energy-efficient clustering schemes and secure routing schemes. The concept about enhancing security and energy-efficiency of network is discussed in detail in various chapters of this thesis. There are different application areas of MANET in different fields. In every MANET application, it is necessary to ensure security for the sensitive data and make energy-efficiency to prolong network lifetime.

Security issues that occur in the areas such as critical application and healthcare have been explored in this thesis. In healthcare domain, the challenges faced are end-to-end reliable delivery of data, considering the privacy and security of the people. Challenges are faced in many critical situations if there is a player’s reaction and delay between private information. It can send reports about an event in a timely manner to particular groups. There are a number of conventional approaches that are available for achieving security in traditional networks, but they may not be suitable for enhancing security in MANET.
Here, a proposal has been made for providing an energy-efficient clustering scheme and security services for MANET. In this thesis, different security mechanisms have been proposed to reduce the malicious activities that occur during routing. These approaches detect the presence of the malicious nodes in the MANET and prevent the activities of the malicious nodes that make malicious-free routing in a MANET. And also, this thesis offers energy-efficient clustering schemes to prolong network lifetime. The following conclusions were achieved from the present study. Many works have been proposed over the past few years. Some of the works that are related to the problem focused has been surveyed and are presented in this thesis. The surveyed works determine some solutions to the problem focused. Further, some works in the area of security in MANET have been surveyed and presented in Chapter 2 of this thesis.

Dynamic Bayesian Signalling Game model provides secure routing and reliability of the data by reducing the malicious activities in a MANET. Its goal is to analyze the strategy profile for regular and malicious nodes. This scheme reveals the best actions of individual strategy for each node. Perfect Bayesian Equilibrium provides a prominent solution for signalling game to solve incomplete information by making combinations of strategies and beliefs of the players that constitute equilibrium. This approach is suitable for many critical situations if there is a player’s reaction and delay between private information. The proposed scheme significantly outperforms to analyze the effectiveness of malicious nodes’ behaviour. The proposed scheme is highly resilient to packet drop attacks. Results obtained in terms of performance improvement and improvements in security are provided in Chapter 3 of the thesis.
Critical applications of MANET require an energy-efficient task to complete its operation. Clustering scheme is an efficient mechanism to implement applications of the MANET. Energy-efficiency and collaboration of the nodes are the major issues to be focused to develop successful applications. The dynamic genetic algorithms such as Elitism-based Immigrant Genetic algorithm and Memory-Enhanced Genetic Algorithm are used to form energy-efficient stable clusters. The proposed scheme is adopting the topology change to maintain the diversity level of the population and stores the old environments into the memory to deal with the load-balancing problem. It is observed that the proposed scheme forms energy-efficient clusters and selects optimal cluster head by considering the parameters including distance and energy to maintain the stable network structure. The proposed scheme can significantly improve the packet delivery ratio and network lifetime. Results obtained for the energy-efficient clustering scheme are provided in Chapter 4 of the thesis.

Many issues occur due to unstable cluster formation for data delivery and problems regarding selection of malicious-free cluster head during routing. In order to overcome the issues, the proposed scheme uses a secure and fair cluster head selection scheme that focuses on stable cluster formation. The proposed scheme integrates security factors into the clustering approach for achieving secure routing. It makes use of the Hierarchical Cluster technique to form stable clusters in the networks. A secure cluster head selection algorithm takes security component and energy factor to form trusted cluster head. Further, it uses Byzantine agreement-based cooperative technique for attacker identification and classification to make the network more attack-resistant. It is observed that the proposed scheme provides an effective malicious-free routing in the presence of attacker nodes. Results
obtained for secure and fair cluster head selection scheme are provided in Chapter 5 of the thesis.

Secure cluster-based multipath routing scheme is established to increase the reliability and enhance the security in a MANET. The energy-efficient clusters are formed using a hierarchical clustering technique. The cluster weight factor such as highest remaining energy, mobility factor and transmission range are considered to select a cluster head. The proposed scheme creates the multiple paths between source and destination that eliminate unreliable routes. Then, the best path was selected from the multipath by considering the parameters like energy, distance, and link quality. A path with no malicious route is selected by applying dynamic secret encryption. It reduces the attacks during communication. The proposed scheme focuses on stable cluster formation and enhancing security to prolong the network lifetime. The proposed scheme could significantly improve the network lifetime and energy-efficiency through load-balancing. Results obtained for secure cluster-based multipath routing protocol are provided in Chapter 6 of the thesis.

The performances of all the proposed schemes are analyzed, and the results obtained from them are found to be better than those of the existing schemes reported in the literature.

7.2 CONCLUSION

In critical applications, providing security is an important aspect for making communications between mobile nodes. The continuous evolution of MANET and its applications have drastically changed the nature of their security and privacy problems. The cluster-based security becomes more
important for establishing effective routing in MANET because the basics of MANET are forwarding data to the destination. The characteristics of MANET such as open medium, dynamic topology and mobility make it more vulnerable to attackers. It may degrade the network performance. Many schemes have been already proposed for providing security and energy-efficiency, but those schemes are not optimal for MANET. Most of the schemes followed are complex for MANET due to the computations and routing performed while handling those schemes. The proposed schemes are more suitable and optimal for MANET that provides an energy-efficient clustering mechanism and security to increase the network lifetime.

The mechanism proposed for enhancing secure routing offers security and reliability. The basic security features alone cannot provide enhanced performance during routing in a MANET. The proposed schemes achieved security, energy-efficiency and reliability to prolong the network lifetime. The outputs of different schemes are analyzed and a comparative study has been done of various mechanisms used ensuring security and energy-efficiency. Even though, if the numbers of nodes are increased the proposed schemes give better performance. Table 7.1 gives a comparative analysis of the proposed schemes under different performance metrics.

Table 7.1 Comparative analysis of the proposed schemes

<table>
<thead>
<tr>
<th>Performance metrics</th>
<th>SRPDBG</th>
<th>SFCP</th>
<th>SCMRP</th>
<th>EEDLBCS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packet delivery ratio(kb/sec)</td>
<td>90.2</td>
<td>93.43</td>
<td>98.07</td>
<td>97</td>
</tr>
<tr>
<td>Routing overhead (%)</td>
<td>68.57</td>
<td>45.91</td>
<td>40.05</td>
<td>41.45</td>
</tr>
<tr>
<td>Total energy consumption(j)</td>
<td>-</td>
<td>16.34</td>
<td>15.52</td>
<td>17.95</td>
</tr>
<tr>
<td>End-to-End delay(sec)</td>
<td>0.246</td>
<td>0.395</td>
<td>0.6</td>
<td>0.2860</td>
</tr>
</tbody>
</table>
The following observations are made from this analysis.

- The proposed Dynamic Bayesian Signalling Game scheme emphasizes reducing a malicious node’s utility and increases a regular node’s utility when it follows the PBE strategy. The proposed scheme reveals the best actions of individual strategy to minimize the utilities of malicious nodes in MANET. It can conclude that increasing the number of monitoring nodes improves the network performance as a whole.

- The proposed SFCP scheme avoided the impact of compromising nodes by selecting the secure and energy-efficient node as a cluster head. The SFCP can effectively classify the malicious nodes and prevent these nodes from the faulty degree claim in cluster head selection. It is observed that the SFCP scheme is highly resilient to vulnerability in terms of energy consumption and low routing overhead.

- The proposed EEDLBCS considered the distance and energy parameters to form clusters with the help of EIGA and MEGA schemes. The proposed schemes used energy and distance metric for calculating the fitness function and then applied genetic operation for selecting optimal clusters and cluster heads. It is observed that the SFCP scheme outperforms the other schemes in terms of the packet delivery ratio and end-to-end delay. But it does not perform well in the presence of compromise nodes in the network.
The proposed secure cluster-based multipath routing scheme is established to increase the reliability and enhance the security in a MANET. The proposed scheme resists the attacker activities in routing by choosing alternate best path for data transmission with security mechanism. Routing through trustable nodes is reliable that achieved higher packet delivery ratio with increased network lifetime.

Comparison showed that SCMRP scheme outperformed than other proposed schemes in most of the simulation performance measures such as packet delivery ratio, routing overhead, energy consumption except end-to-end delay. It can be concluded that the proposed secure cluster-based multipath routing scheme is highly resilient to vulnerability and reliability as a whole.

7.3 SCOPE FOR FUTURE WORK

Mobile ad hoc networks have attracted considerable attention and interest from the commercial sector as well as the standards community. Many new ad hoc networking applications have been conceived to help enable new commercial and personal communication beyond the domain of tactical networks, including personal area networking, health care systems, law enforcement operations, search and rescue operations, commercial and educational applications, and sensor networks. As the demand increases, the issues that occur while handling critical situations get increased. Hence, it is necessary to protect the private data and the activities performed through unreliable wireless links. Even though the mechanisms proposed in the thesis are able to enhance security and energy-efficiency, it is necessary to extend this security mechanism in the future of the health care systems for providing high security and reliability. The second future direction of this thesis work is to classify the data involved in the healthcare system, based on the priority.