The basic aim of incorporating this chapter into present thesis is to highlight the outcome of the present research work. These outcomes are represented in section 8.1. Further during this research journey, author feels that there are certain areas which remain untouched which can be pursued as the future scope of the work as discussed in section 8.2.

8.1 CONCLUSION

The techniques of outlier detection in Data Mining act as a motivational factor to identify outlier nodes from the mobile ad hoc networks. The outlier node in such type of networks means nodes which perform different to other nodes in the network. These nodes may be some malicious nodes which deliberately do harm to the network or may be some selfish nodes which deny performing any activity because of scarcity of resources available. In this research work, these terms are explored in literature and identified a number of approaches to deal with such types of threats. It is found that in MANETs, every communication is dependent on cooperation amongst the nodes in the network. In the present research work, trust between the nodes is calculated as a medium to find out the reliability of the nodes. So various trust management approaches are covered in the literature review in chapter 2. By taking into consideration, the issues of energy restriction and scalability, the concepts of clustering in MANETs are also explored in literature survey.

Through the review of the literature, the problem of evaluating trust and detecting outlier nodes in MANETs application is identified in Chapter 3, and various objectives to be accomplished throughout the research have been identified. In addition, it also details the research methodology employed with proposed layout and tools offered to accomplish the set goals. The data set required for the implementation is also described.

In chapter 4, a trust model is described which evaluates trust on three different dimensions. The model is fully decentralized and it is based on three parameters such as knowledge gained through direct observations, experience obtained through past observations with the help of classifier and recommendations obtained through
indirect observations. An appropriate weights are assigned to each parameters by putting more weight on the direct knowledge parameter so that false recommendations if possible do not destroy the trust evaluation process.

To identify the list of outlier nodes from the network, an outlier detection algorithm is proposed in Chapter 5. The working of the proposed outlier detection algorithm is defined by means of a layered structure model. The layered structure model is divided into three layers. Each layer defines the respective part of the algorithm. Trust generation deals with generating trust values of neighboring nodes based on the proposed trust model. Trust tables are exchanged between peer nodes and based on the received tables, every node updates its own table and finally a global table of trust is generated which contains trust values of all the nodes in the network out of which a list of outlier nodes is generated which is the output of the algorithm. The accuracy is measured by randomly introducing different number of malicious nodes in network and then performance is calculated.

As in MANETs, nodes are limited in energy so to use resources effectively the concept of clustering is introduced in chapter 6. The proposed clustering algorithm provides a secure and efficient cluster because it considers important parameters of the network which are connectivity, energy and security, all of which play an important role in selecting the efficient cluster head. The performance of SECHAM is evaluated by comparing with LID (Lowest Identifier) algorithm and results shows that SECHAM outperformed LID in terms of energy efficiency as it distributes the load among different cluster heads by suitably updating cluster head which overcomes the limitation of LID.

Finally the outlier detection algorithm (OUTM) is combined with clustering algorithm proposed in chapter 7 to identify outliers from the clustered network. By performing this, the work load of trust generation and maintenance is shifted from all the nodes to cluster heads only and it improves the network performance under varying environment conditions. The time complexity is also reduced as compared to the outlier detection algorithm OUTM hence it outperforms the existing algorithms for outlier detection.

A general conclusion which is obtained from the results of the present research work is that in MANETs, the trust value of nodes, generated through three dimensions
based trust model, reflect the behavior of the nodes accurately. Based on trust values, co-operation can be achieved among nodes in the network. The nodes which are found to be untrustworthy are selected as outliers by using OUTM. By introducing clusters in the network, there is enhancement in performance of outlier detection process. OUTCM is capable of observing outlier nodes from the cluster based MANETs even if node density or occurrence of malicious nodes in the network increases.

8.2 FUTURE SCOPE

During present research work; the author feels that there are few areas where upcoming researchers can conduct their research work to contribute to society, academics and research environment. Such areas are given as below:

- The comparative study of various Data Mining Algorithms for identification of outlier nodes can be performed which helps in selection of an appropriate technique.
- In resource constrained environment of MANETs, there are various points of failures. To enhance the decision making on trustworthiness of nodes, more social and quality of services can be included in trust evaluation process.
- A comprehensive research to explore the trade-offs between precision of trustworthiness and performance of the network is desired in future.
- The proposed algorithm for outlier detection OUTCM can further be applied in some specific applications for filtering out dishonest nodes from the network.
- Different modes of implementation such as simple, average and high level can be suggested to deal with ever-changing environment of mobile ad-hoc networks. These levels show different complexity requirements according to the resources available at the nodes.