CHAPTER 9

CONCLUSION AND FUTURE ENHANCEMENTS

9.1 CONCLUSION

This research study has presented hybrid schemes to detect blackhole attacks in mobile ad hoc networks using soft computing approaches. The hybrid system refers to the combined approach of anomaly and specification based techniques of IDS. Defining normal behaviour by describing rules after training the network is the key feature of anomaly method. Manually crafting the rules specific to the protocol is the key mechanism of specification-based approach. This research work has combined it effectively by training the network to derive the protocol specific parameters meant for defining the normal behaviour.

In addition to the protocol specific behavioural analysis, this work includes an attack-specific approach to improve the performance of the proposed system. Blackhole attack that occurs in the network layer is the problem considered for testing the proposed hybrid design. The features specific to the routing protocol and blackhole were extracted to describe the rule set for normal behaviour. This is carried out after duly training the network for various scenarios. The factors belonging to multiple layers were considered to adopt a cross layer design in the detection scheme. In this thesis, the physical layer features were included in addition to the network layer parameters to design a novel cross layer detection scheme. A credit allocation scheme is introduced to determine the behaviour of nodes.
The credit scheme allotted credits to each node based on its performance in the node. The performance refers to the participation of node in the route discovery and communication process. The credits were allotted for each network parameter used in the rule set, and the final credit for any node was considered to be the sum of individual parameter credits. Lesser the credit for a node, more was the probability of it being detected as a malicious node.

The hybrid credit based design to detect blackhole attack was tested with the fundamental soft computing approaches such as fuzzy logic, neuro-fuzzy, genetic algorithm and artificial neural network.

A feed-forward neural network with back propagation algorithm was developed in such a way that the mean square error in the network was reduced. A learning function modified the weights in the various layers of ANN and resulted in the minimum MSE. The nodes with highest MSE were identified as blackhole nodes. The performance measure of the system was determined by TPR, FNR, FPR and the speed of detection. The detection scheme using ANN produced 100% accurate detection in less time. However, the assumed weight values and the number of hidden layer pose limits on the applicability of this scheme. A simpler technique namely fuzzy inference system was designed to overcome this issue.

In the fuzzy approach, the Sugeno fuzzy inference system was used with the data set resulting from the simulation output. The features specific to routing protocol and the blackhole attack, and the credits form the input data set for the FIS. The proper functioning of the FIS depends on the data conditioning process, clustering. The detection scheme using FIS proposed in this research work was tested with the two fundamental clustering algorithms: subtractive and fuzzy c-means. This scheme produced better detection in less time, with few false alarms.
A neuro-fuzzy approach was developed to improve the TPR and to reduce the false alarms produced by the scheme using FIS. An ANFIS model was generated with a Sugeno-FIS and a neural network with one input, one output and multiple hidden layers. When the neuro-fuzzy structure was trained with a suitable training data, it adapts to the changes in the input data set and adjusts the parameters of the FIS membership functions. A hybrid-learning algorithm was used to reduce the error in every training epoch. The properly trained ANFIS model was tested for various network cases and it proved to perform better than its predecessor FIS, in terms of the detection accuracy. The detection time of scheme with FCM was lesser compared to the subtractive clustering method. However, maximum detection accuracy was not achieved using the ANFIS with single layer parameters.

A cross layer design was developed to increase the efficiency of the system. This included the residual energy value from the physical layer log in the parameter list to form the rule set. The cross layer design is experimented with FIS and ANFIS and it clearly showed improvement in performance of the detection scheme in terms of all the performance measures.

The genetic algorithm was used in the detection scheme to achieve faster detection. The input data set formed the initial population. The encoding process was carried out using the first threshold value and the fitness function determines the survival blackhole node. This method produced better detection with the least false alarm rate.

When comparing the results of all the detection schemes proposed in this dissertation, it is concluded that the cross layer design of ANFIS based scheme with fuzzy c-means clustering algorithm performs better in all aspects. Such a scheme may be realised in the form of high power integrated chip and used in MANET applications where one or more nodes are compromised and launch blackhole attack. On the application part, the ANN
based scheme is suitable in places, where a large database regarding the network traffic and the history of the network is available, and accuracy is the foremost requirement, such as banking/financial applications. The ANFIS based cross layer scheme would be more suitable in applications where it is possible to monitor the physical layer parameters, such as campus communication network.

9.2 FUTURE ENHANCEMENTS

In this research work, certain schemes were presented to detect a virulent network layer attack, the blackhole attack. Further, this work may be enhanced to achieve maximum accuracy and minimum detection time in all the schemes by considering additional parameters. The real-time implementation of the schemes can be attempted in future.

Moreover, the schemes proposed in this dissertation are applicable to on-demand ad hoc routing protocols. These schemes can be suitably modified to detect the blackhole attack in proactive routing protocols. This research work may also be extended to detect other network layer attacks, such as wormhole and grayhole.