Chapter 7
Conclusions and Future Work

This chapter concludes the thesis through summarizing the research work, revising the contributions, and finally examining the possible areas of this research work.

7.1 Summary

In MANETs, the data services and routing mechanisms are very susceptible to many kinds of security threats due to its complex characteristics. Although many efforts have been made in the literature for securing the MANETs but most of the work has concentrated to protect the MANETs for a particular type of attacks. Hence, the motivation of this thesis egresses from actualizing the need to secure the MANETs from different kinds of attacks so that this research investigates the use of soft computing techniques, specially neuro-fuzzy classifiers for developing a new generalized IDS for MANETs that can protect MANETs from different types of attacks. We have seen very few applications of soft computing techniques in the field of intrusion detection on MANETs whereas in conventional networks, soft computing techniques have already posed the significant promise for developing the IDS. Our proposed solution also concentrates on the specific characteristics of MANETs such as lack of central points, dynamic topology and limited resource.

In this thesis, we develop and introduce our proposed solution in three incremental phases. In the first phase, we describe the use of Mamdani fuzzy inference system, and Sugeno fuzzy inference system in the field of intrusion detection and show that how these inference systems can help in detecting the attacks in MANETs. In the second phase, we propose a solution that provides a framework for using hybrid of soft computing techniques (neuro-fuzzy) to build a binary classifier that can act better than the single soft computing technique and presents the detail how to use the neuro-fuzzy classifier to derive an IDS for MANETs.

In the third phase, we extend this neuro-fuzzy classifier based protection method to a generalized solution i.e. Generalized Intrusion Detection System Using Soft Computing
(GIDSSC) that can secure the MANETs from different types of known and unknown (new) attacks using the combination of misuse based and anomaly based intrusion detection techniques and the proposed GIDSSC system is also able to find out the type of the detected attack. Moreover, this research also concentrates on the intrusion detection architectures and developed two architectures for local, and cooperative detection by using GIDSSC system. Furthermore, we carried out the performance analysis of the GIDSSC system through extensive simulations for detecting the various attacks (such as PDA, SDMF, and RDA attacks) with varying traffic rates and mobility speeds in respect of the local, and cooperative detection schemes, and then compared the performance of both the developed local, and cooperative intrusion detection schemes by using GIDSSC system.

7.2 Overview of Thesis Contributions

The main contributions of this thesis are presented as follows:

1. **Soft computing techniques for intrusion detection in MANETs**

   This research work examines the use of soft computing techniques for developing new generalized IDS for MANETs that can detect the various kinds of known and unknown (new) attacks. In this respect, firstly we present that how a fuzzy inference system can help in detecting the attacks in MANETs so that we apply Mamdani, and Sugeno fuzzy inference systems for detecting PDA, and SDMF attacks. MANETs work as an open medium for attackers due to its complex properties so that this research concentrates to classify the normal and suspicious activities in the MANETs. For this purpose, the binary neuro-fuzzy classifier based IDS has been introduced to categorise the normal and abnormal activities. The performance of the binary neuro-fuzzy classifier is examined on simulated networks under the varying traffic rates and mobility speeds. The results show a good performance for detecting PDA, and SDMF attacks. Furthermore, we extend this binary neuro-fuzzy classifier based protection method to a generalized solution i.e. Generalized Intrusion Detection System Using Soft Computing (GIDSSC) that can secure the MANETs from different types of attacks.

2. **Development of a new generalized IDS for MANETs**

   Realizing the requirement to secure the MANETs from different types of attacks, we developed a generalized IDS using soft computing techniques i.e. GIDSSC by extending our binary neuro-fuzzy classifier protection method. The proposed GIDSSC system monitors
most of the network performance statistics and characteristics of the network layer. The GIDSSC system used the combination of misuse based and anomaly based intrusion detection techniques to protect the MANETs from different kinds of attacks. The proposed generalized mechanism, first detect the attack in the network and then also determines the type of the detected attack. To assess the performance and applicability of the GIDSSC system, we simulated the network with different attacks under the varying traffic rates and mobility speeds and presented that GIDDSC system can protect the MANETs from different kinds of attacks, including unknown or new attacks (that are not a part of training phase of GIDSSC).

3. A combination of misuse based and anomaly based intrusion detection techniques

This research work presents a generalized IDS using soft computing for detecting the routing attacks against AODV routing protocol in MANETs. The aim of GIDSSC system is to detect the known and unknown (new) attacks in MANETs and also determines the type of the detected attack through GIDSSC so that, this research work employed both the detection techniques i.e. misuse based and anomaly based. In this aspect, every classifier in the first layer of the proposed GIDSSC system works as a misuse based classifiers to select a good training and checking datasets for learning phase and after learning, each classifier works as an anomaly detector.

4. Development of two intrusion detection architectures for local and cooperative detection

This research has developed two intrusion detection architectures for local, and distributed and cooperative detection by using GIDSSC system. The comparison amongst both the local, and cooperative detection schemes has been also done in this thesis. We also suggested an alternative solution for reducing the consumption of resources during the distributed and cooperative intrusion detection scheme.

To conclude, in this thesis we have presented the potential use of soft computing techniques to find out the complex properties of MANETs and proposed a new generalized IDS for this new environment. This newly proposed IDS is extremely suitable and effective to secure the MANETs from different types of routing attacks and it also determines the type of the detected attack. The proposed solution also concentrates on some specific characteristics of MANETs such as lack of central points, dynamic topology and limited resource. The areas of future work will be discussed in the section 7.3.
7.3 Suggestions for Further Work

The possible areas of this research work are described below:

1. Applying soft computing techniques to other areas

   In this research work, we present how to apply soft computing techniques to intrusion detection in the field of MANETs for detecting the known and unknown attacks. The proposed work in this research can be easily adapted to other complex areas such as wireless sensor networks because security is also a big concern in the wireless sensor networks.

2. Optimizing our approach

   Our proposed GIDSSC system in this research employed a five inputs and single output based Mamdani fuzzy inference system to increase the system performance for making the decision in respect to the attack detection. The use of genetic algorithm could be used to optimize the performance of our fuzzy decision making system for attaining the best results. Moreover, the features could also be reduced by the methods of feature selection for the classifiers.

3. Exploration of the new attacks

   In this research, we considered PDA, SDMF, and RDA attacks for analyzing the performance of our proposed GIDSSC system. Consequently, the proposed GIDSSC system could be evolved with the different categories of the similar attacks which have the interchangeable consequences on the network such as DoS attacks so that it could be more effective and cover more attacks. This research could detect distributed attacks such as network scan by using our proposed cooperative intrusion detection scheme, because distributed attacks cannot be detected locally to a node in the network.

   To conclude, we believe that soft computing techniques are the best choice for the development of IDSs for the challenging environments such as MANETs.