CHAPTER 1

INTRODUCTION

A decade of exponential growth in wireless networks has profoundly impacted our lifestyle, from cellular telephones to wireless Internet access. A wireless network without any fixed infrastructure is referred to as a mobile ad hoc network (MANET), as the wireless nodes are capable of moving freely. It is a mobile, wireless, multi-hop network that operates without the benefit of any existing infrastructure, except for the nodes themselves (Charles Perkins 2001). Such networks are assumed to be self-forming and self-healing. These unique characteristics allow them to be used in special applications such as the army, emergency/ rescue operations, habitat monitoring etc. Routing in such networks is challenging because typical routing protocols do not operate efficiently in the presence of frequent movements, intermittent connectivity, and network splits/joints. Moreover, the use of wireless links makes these networks very vulnerable to security attacks, ranging from passive eavesdropping to active interfering.

1.1 SECURITY ISSUES AND CHALLENGES IN MANETS

MANETs are highly vulnerable to security attacks compared to wired networks, due to their unique characteristics (Sivaram Murthy and Manoj 2001). Certain features that make the implementation of security a highly challenging task in such networks are:
Shared broadcast radio channel – the data transmitted by a node is received by all the nodes within its direct transmission range. This allows the malicious node to easily obtain the data being transmitted in the network.

Insecure operational environment – In applications such as battlefields, the nodes may move in and out of hostile and insecure enemy territory, where they would be highly vulnerable to security attacks.

Lack of central authority – Since ad hoc networks do not have central points to monitor the traffic on the network, it is difficult to implement security mechanisms at such points.

Limited resource availability – Resources such as bandwidth, battery power and computational power are scarce in MANETs. Hence, it is difficult to implement complex cryptography-based security mechanisms.

1.2 SECURITY ATTACKS ON MANETS

Ad hoc networks that make extensive use of wireless links are vulnerable to several types of attacks due to the inherent nature of the network (Farooq Anjum 2007). Attacks against the network may come from malicious nodes that are not part of the network and are trying to join the network without authorization. Such nodes are typically called outsiders. Networks are protected from malicious outsiders through the use of cryptographic techniques. Such techniques allow nodes to securely verify the identity of other nodes, and can therefore, try to prevent any harm being caused by the malicious outsiders. Attacks also come from nodes that are authorized to be part of the network and are typically called insiders. Insider nodes may launch attacks because they have been compromised by an unauthorized user (e.g. hacker) through some form of remote penetration, or have been physically captured by a malicious user. The attacks may be classified as
passive or active, based on their behaviour (William Stallings 2003). Attackers do not disrupt the normal operation in a passive attack, and listen to the network in order to get information. Attackers carry out malicious actions such as modification of data stream, and denial of service in active attacks. The attackers aim at all the layers of the MANET protocol stack. Figure 1.1 provides the classification of active attacks on various layers.

![Security Attacks Diagram](image)

**Figure 1.1 Classification of attacks on MANET**

It is clear from the figure that the attacks occur in all layers of the network. However, the attacks aimed at the network layer draw major attention, as the functions of this layer are crucial for the proper operation of the MANETs. Some of the major network layer attacks are presented in this section.

1.2.1 **Network layer attacks**

a. **Wormhole attack**

The attacker receives the packets at one location in the network and tunnels them to another location in the network, from where they are resent to the network. This tunnel between two colluding attackers is referred to as a wormhole. It could be established through a single long-range wireless link or even through a wired link between the colluding attackers.
b. **Information disclosure**

A compromised node may leak confidential information to unauthorised nodes in the network. Such information may be regarding the network topology, geographic location of the nodes or optimal routes to the authorised nodes in the network.

c. **Routing attacks**

There are several types of attacks mounted on the routing protocol, which are aimed at disrupting the operation of the network. Examples of such attacks are: route table overflow, routing table poisoning, packet replication and rushing attack.

This research work focuses on one of the major network layer attacks, the blackhole attack, which is capable of paralysing the network operation. It is performed by compromised insiders, and hence is difficult to detect.

1.3 **BLACKHOLE ATTACK**

In this attack, a malicious node uses the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept. The attacker will then receive the traffic destined for the other nodes, and can then choose to drop the packets to perform a denial-of-service attack, or alternatively use its place on the route as the first step in a man-in-the-middle attack by redirecting the packets to nodes pretending to be the destination. In classic reactive routing protocols, the malicious node targets the route discovery process to launch the blackhole attack. Vulnerable fields, such as the hop count and sequence number in the route reply (RREP) packets are exploited by the adverse node. As soon as the blackhole node receives a
route request (RREQ), it generates a RREP with the least hop count and highest sequence number, without checking its routing table. This RREP is sent to the source in a fast manner, using high transmission power. Moreover, it does not forward the RREQ to the neighbouring nodes, even if it does not have a path to destination. In this way, it makes the source node to select it in the path from the source to the destination. When it has made itself available as part of a communication path, the blackhole node does not forward the data packets to the intended destination, but drops them. Figure 1.2 illustrates the blackhole attack. The nodes labelled A to E in the illustration are genuine nodes, and the one labelled M is the adverse node that launches the blackhole attack. The links shown between the wireless nodes A to E and M are logical links. When the source node D tends to communicate with the sink node C, it starts the route discovery process by flooding the RREQ packets. The blackhole node M replies to D with the shortest and fresh route through fake RREP. This makes D to send the packets to M, where they are dropped.

![Figure 1.2 Blackhole attack](image-url)

As illustrated, the blackhole node attracts the traffic, by placing itself in a strategic position on the wireless network and disrupts the normal
functioning. The traditional authentication mechanisms are not sufficient in detecting this attack, and a second line of defence in the form of an intrusion detection scheme is required. This research work has attempted to design schemes to detect such alarming attacks in MANETs.

1.4 INTRUSION DETECTION SYSTEM (IDS) AND ITS TYPES

Intrusion is any set of actions that try to compromise any of the security mechanisms in the network. Intrusion detection is the process of monitoring the events occurring in a system or network, and IDS is the software that automates the intrusion detection process (Behrouz Forouzan 2012). The types of IDS are differentiated primarily by the types of events that they monitor, and the ways by which the features are achieved. They are:

**Misuse Detection:** In misuse detection or signature detection, decisions are made on the basis of the knowledge of a model of the intrusive process, and what traces it might leave on the observed system. Such a system tries to detect intrusion, irrespective of any knowledge regarding the background traffic (Amitabh Mishra et al 2004). There are several approaches in signature detection, which differ in the representation and matching algorithms employed to detect the intrusion patterns.

**Anomaly detection:** This technique establishes a "normal activity profile" for a system and the states varying from the established profile by statistically significant amounts are identified as intrusion attempts. It flags the observed activities, that abnormally deviate from the recognized normal usage as anomalies. It must first be trained using normal data, before it can be released in an operative detection mode. The main advantage of this model is that it can detect unknown attacks. On the other hand, the disadvantage is that it has a high false positive alarm rate, when the normal user profiles, operating system, or network behaviour vary widely from their normal behaviour.
**Specification-based detection:** Specification-based detection defines a set of constraints that describe the correct operation of a protocol, and monitors the execution of the protocol with respect to the defined constraints. This technique may provide the capability to detect previously unknown attacks, while exhibiting a low false positive rate.


1.5 **SOFT COMPUTING TECHNIQUES**

Soft computing is a multidisciplinary system defined by Lotfi Zadeh, as the fusion of the fields of Fuzzy logic, neuro computing, genetic computing and probabilistic computing. Soft computing is used to model and enable solutions for real world problems, which are difficult to solve using mathematical techniques.

1.5.1 **Artificial Neural Network (ANN)**

The term **neural network** was traditionally used to refer to a network or circuit of biological neurons. The modern usage of the term often refers to artificial neural networks, which are composed of artificial neurons or nodes. The nodes can be seen as computational units. They receive inputs, and process them to obtain an output (Carlos Gershenson 2011). This processing might be very simple (such as summing the inputs), or quite complex (a node might contain another network). The connections determine the information flow between the nodes. They can be unidirectional, when the
information flows only in one direction, and bidirectional, when the information flows in either sense. The interactions of the nodes through the connections lead to a global behaviour of the network, which cannot be observed in the elements of the network.

An artificial neuron is a computational model inspired by natural neurons. These basically consist of inputs, which are multiplied by weights (strength of the respective signals), and then computed by a mathematical function, which determines the activation of the neuron. Another function computes the output of the artificial neuron. ANNs combine artificial neurons in order to process information. The structure of an artificial neuron is shown in Figure 1.3.

![Figure 1.3 Structure of an artificial neuron](image)

An artificial neural network is an information processing system that is inspired by the way biological nervous systems, such as the brain, process information. The ANN is developed with a systematic step-by-step procedure, which optimizes a criterion commonly known as the learning rule. The input/output training data is fundamental for these networks, as it conveys the information, which is necessary to discover the optimal operating point. In addition, the non-linear nature makes neural network processing elements a very flexible system.

The ANN is composed of a large number of highly interconnected processing elements working with each other to solve specific problems. Each
processing element is basically a summing element followed by an active function. The output of each neuron (after applying the weight parameter associated with the connection) is fed as the input to all the neurons in the next layer (Muna Muhammad et al 2010). Multilayer perceptrons (MLPs) are layered feed forward networks, typically trained with static back propagation. The multilayer feed-forward neural network has several neurons structured in layers, such as the input layer, hidden layers and output layers. A multilayered feedforward neural network with backpropagation has been used in this study.

1.5.2 **Fuzzy Logic and Fuzzy Inference System (FIS)**

The concept of fuzzy logic was conceived by Lotfi Zadeh (1974), and presented as a way of processing data by allowing partial set membership rather than crisp set membership or non-membership. Fuzzy logic does not require precise inputs, is inherently robust, and can process any reasonable number of inputs. Simple, plain-language IF X AND Y THEN Z rules are used to describe the desired system response in terms of linguistic variables rather than mathematical formulas. There is a unique membership function associated with each input parameter. The membership functions associate a weighting factor with the values of each input and the effective rules. These weighting factors determine the degree of influence or degree of membership (DOM) each active rule has. The logical product of each rule is inferred to arrive at a combined magnitude for each output membership function. This can be done by max-min, max-dot, averaging, Root-Sum-Square (RSS), or other methods. The magnitudes are mapped into their respective output membership functions after it has been inferred. The "fuzzy centroid" of the composite area of the member functions is computed, and the final result taken as the crisp output. Tuning the system amounts to "tweaking" the rules
and membership function definition parameters, to achieve an acceptable system response.

Fuzzy logic is a rigorous mathematical field, and provides an effective vehicle for modeling the uncertainty in human reasoning. It is a set of concepts and approaches designed to handle vagueness and imprecision. The FIS (Jang et al 2010), is a popular computing framework based on the concepts of the fuzzy set theory, if-then rules and fuzzy reasoning. It has found successful applications in a wide variety of fields, such as automatic control, data classification, decision analysis and pattern recognition. A Sugeno type fuzzy inference system, using various membership functions is designed in this research work to detect blackhole attacks.

1.5.3 Genetic Algorithm (GA)

Genetic algorithms were invented to simulate evolutionary processes observed in nature, so that the survival or optimisation in a changing environment could be achieved. The GA manipulates the ‘chromosomes’, which encode a set of parameters of the target system to be optimised. The GA uses three operators: selection (or reproduction), mutation, and crossover – to achieve the goal of evolution. The single piece of information a GA receives from the environment is a scalar indicator that evaluates the performance of each chromosome. The GA then uses that evaluation to bias the selection of chromosomes, so that those with better scores tend to reproduce more often than those with worse scores. The various processes of the genetic algorithm are appropriately applied in the detection scheme presented in this thesis.
1.6 CROSS LAYER DESIGN

As wireless communications and networking fast occupy center stage in research and development activity in the area of communication networks, the suitability of one of the foundations of networking, the layered protocol architecture, is coming under close scrutiny from the research community (Vineet Srivastava and Mehul Motani 2005). It is repeatedly argued that although layered architectures have served well for wired networks, they are not suitable for wireless networks. To illustrate this point, a cross-layer design proposal is usually presented. Generally, cross-layer design refers to the protocol design done by actively exploiting the dependence between the protocol layers to obtain performance gains. This is unlike layering, where the protocols in the different layers are designed independently. This kind of design is easier in wireless networks as the wireless medium allows richer modalities of communication than wired networks. For example, nodes can make use of the inherent broadcast nature of the wireless medium and cooperate with each other. The cross-layer design represents a suitable technology to overcome some of the current limitations of the TCP/IP stack, especially in the case of wireless networks. Its core idea is to maintain the functionalities associated with the original layers but to allow coordination, interaction and joint optimization of protocols crossing different layers. Adopting a cross layer approach in the design of a detection scheme allows flexibility, improved performance and ease of implementation. The results presented in this dissertation substantiate the inference.

1.7 MOTIVATIONS AND OBJECTIVES OF THE RESEARCH WORK

The issues and challenges in implementing the security mechanisms for a MANET were discussed in the previous sections. The new paradigm cross layer design improves the performance of any system. Many
cryptography and authentication algorithms were developed to protect communication in MANETs. These mechanisms are capable of securing the network against outside attackers. The compromised wireless nodes residing within the network and possessing valid authentication and/or cryptographic keys may elude such mechanisms. Hence, an additional line of defence is required to guard the MANET from insider attacks. The IDS serves the purpose by identifying the attacker nodes and reporting to all the nodes in the network. Employing a cross layer design improves the effectiveness of detection. The motivation for this research work was derived from the aforementioned factors.

The foremost objective of this research is to design a detection scheme that will detect the blackhole attacks in MANETs. In designing such a scheme, the aim is to use a hybrid approach that combines the anomaly and specification based methodologies so as to make use of their benefits. This research work aims at experimenting with the design, using the fundamental soft computing approaches such as fuzzy logic, genetic algorithm and artificial neural network. This work also focuses on adopting a cross layer technique to improve the detection efficiency of the proposed schemes. This research work aims at testing the proposed schemes in a simulated environment and measuring their performance, in terms of the true positive rate, false positive rate, false negative rate and the time taken for detection.

1.8 ORGANIZATION OF THESIS

This thesis is organized as eight chapters. The chapter organization is as follows:

Chapter 1 presents the introduction to the research work. The design and analysis of credit based hybrid schemes to detect blackhole attacks using soft computing approaches are presented in this dissertation. Chapter 1 offers
the background to the research work by providing the basics of the various techniques and terms used. It briefly describes the MANET, its security challenges, the various means to protect it and the fundamentals of intrusion detection techniques.

The related works in this area are discussed in Chapter 2. Many existing schemes attempt to address the routing attacks in MANETs, in specific to the blackhole attacks. The existing intrusion detection schemes and their drawbacks are outlined in this chapter.

Chapter 3 throws light on the detection schemes using ANN and fuzzy. These schemes use the data from the simulated environment, and extract only a set of protocol-specific features. The design of ANN based detection scheme involves the generation of a multi-layer feed-forward, backpropagation ANN, which adjusts the weights to reduce the mean square error. The design parameters and the associated outputs are provided in this chapter. In the fuzzy based design, the credit allocation scheme is applied on the derived data set. A clustering process is carried out on this data set followed by the generation of a Sugeno FIS. The detection scheme uses the defuzzified output of the FIS to identify the adverse nodes that perform the blackhole attack. The detailed algorithm and the various processes involved in the proposed scheme using FIS, are discussed in this chapter. The experimental results are illustrated and discussed.

Chapter 4 shows the improvement in the detection efficiency, using a neuro-fuzzy structure. The scheme involves an adaptive neuro-fuzzy inference system (ANFIS) that combines the benefits of the neural network and fuzzy logic. This chapter explains the various features of the ANFIS based detection scheme, the associated steps and the experimental results.
Chapter 5 provides the proposed cross layer detection scheme. A loosely coupled cross layer algorithm is illustrated in this chapter, that further increases the efficiency of detection schemes using FIS/ANFIS. The physical layer parameter is also included to increase the detection efficiency of these two schemes, and to reduce the false alarms. This chapter provides an overview of the cross layer approaches. The proposed schemes, their experimental results and the improvements in the performances of the mentioned systems are also presented in this chapter.

The details of the genetic detection scheme are presented in Chapter 6. The genetic algorithm is an evolutionary computing technique based on natural selection. A proper fitness function and the choice of population decide the efficiency of the scheme. This chapter provides the algorithm for the scheme and its performance improvement, in terms of an increased detection rate along with the experimental results.

Chapter 7 offers the network simulation details. The MANET simulation scenario, using the ns2 simulator is presented in this chapter. A large database of mobile network with various traffic scenarios is required to design a hybrid detection scheme and to execute that using soft computing techniques. This chapter presents the details of the simulation of MANET with blackholes, and the assumptions made during the simulations.

Chapter 8 provides the performance analysis of the proposed schemes and their comparison with the existing schemes. The holistic framework of the detection schemes and the comparison of their performances in terms of the detection accuracy, false alarm rate and the detection time is presented.
Chapter 9 presents the summary of the research work by outlining the conclusion of this thesis. The possible future works such as the practical applicability, and implementation possibilities are also listed in this chapter.

Appendix 1 provides the sample data sets used by the various schemes of this research work to detect blackhole attack. The data sets corresponding to the different network sizes, blackhole densities and various traffic scenarios for single and cross layer approaches are given in this appendix.