CHAPTER 1

INTRODUCTION

1.1 ABOUT MANET

According to Corson et al (1999), a Mobile Ad-hoc Network (MANET) is a collection of wireless mobile nodes which dynamically form a temporary network without using any existing network infrastructure or centralized administration. There are many applications for MANET. These include personal area networking where the mobile nodes may be cell phones, laptops, etc. The MANET is also having a good potential in military operations where the nodes may be soldiers, tanks, or airplanes. In addition, MANET could prove useful in civilian environments as diverse as taxi cab networks, conference rooms, boats and ships, search and rescue operations as well as policing and firefighting. These types of networks have a few trade-offs including limited bandwidth problem, energy consumption problem and most importantly the security problem.

An ad-hoc routing protocol is a convention or standard that controls routing packets between computing devices in MANET. In this thesis, the reliability and security issues of routing in ad-hoc networks are tackled.

1.2 ROUTING IN AD-HOC NETWORKS

Efficient routing of packets is a primary MANET challenge. Conventional networks typically rely on distance-vector or link-state
algorithms, which depend on periodical broadcast advertisements of all routers to keep routing tables up-to-date. In some cases, MANET also uses these algorithms which ensure that the route to every host is always known.

According to Mehran et al (2004), the ad-hoc routing protocols are classified into three types, they are

- Pro-active (Table-driven)
- Reactive (On-demand)
- Hybrid (Pro-Active/Reactive)

The routing protocols have further been classified into three types by Siva et al (2005) as

- Hierarchical
- Geographical
- Power aware

However, these classifications are not mutually exclusive as some protocols fall in more than one class. The existing routing approaches have several problems like

- The periodical broadcast of the information causes increased bandwidth utilization
- Repeated awakening of hosts to send and receive information cause quick battery exhaust
• The propagation of routing information depends on the number of existing hosts and causes overloading, thereby reducing scalability.

• The routes are less reliable because the reliability of nodes are not considered

• The network is insecure because of decentralized architecture

1.2.1 Proactive Routing Protocols

A proactive routing protocol is one in which the processes of route discovery and route maintenance are carried out periodically, by exchanging routing tables at regular intervals. This process helps to maintain the up-to-date view of the network topology. These proactive protocols maintain the global topology information of ad-hoc nodes in the form of tables. Most of the proactive routing protocols are extensions of the wired network routing protocols, and have been designed by extending the distributed Bellman-Ford algorithm (Perkins et al 1994). Proactive routing protocols ensure the availability of routes to all destinations at all times, which considerably reduce the delay in the process of route setup.

1.2.2 Reactive Routing Protocols

Reactive routing protocols execute the path-finding process and exchange the routing information only when a path is required between a source-destination pair. These protocols exchange periodically the control packets between the nodes to share the routing information. In general, reactive protocols are considered efficient because the process of route discovery takes place adequately and the communication is confined to a
limited number of nodes. This makes reactive protocols more suited to large networks with light traffic and low mobility. The limitation of reactive protocols is stale route information, which leads to inconsistencies during the route reconstruction phase. The connection setup delay in reactive protocols is higher than the corresponding delay in proactive protocols as connections are established only on demand. Reactive protocols are dependent on periodic beacons by nodes. These Hello packets inform each mobile node about other nodes in its neighbourhood. These beacons lead to unnecessary bandwidth consumption (Perkins et al 1999).

1.2.3 Hybrid Routing Protocols

Hybrid Routing Protocols use either pure proactive or reactive routing schemes. Hybrid routing protocols reduce the overhead of proactive routing protocols as well as decrease the latency caused by route discovery in reactive routing protocols. Most of the existing hybrid protocols are based on routing zones, which is similar to a cluster with the exception that there is no cluster-head in the zone. Proactive mechanisms are used to route within a zone and reactive mechanisms are followed for routing outside the zones (Haas et al 1997). Some hybrid routing protocols are not zone based and they extract a subset of nodes that are only responsible for state management and route computation (Sivakumar et al 1999).

1.2.4 Hierarchical Routing Protocols

Hierarchical routing protocols group nodes together into a hierarchical structure. A hierarchical protocol allows an administrator to make the best use of the fast powerful nodes as backbone nodes, and the slower, lower powered nodes may be used for access purposes. In this way, the access nodes form the first tier of the hierarchy, and the backbone nodes form the
second tier. Data flow through the access nodes and only enter the backbone when the data try to reach the parts of the network that has no local connections other than the backbone nodes. This allows traffic to flow freely and concentrates long distance data onto the backbone links to flow efficiently to the opposite side thereby minimizing congestion.

### 1.2.5 Geographical Routing Protocols

The geographical routing protocols require

- No routing-tables
- No overhead to find or update routes

But the protocols require information like

- Position

The position of the node is determined via

- internal search-process
- external service

### 1.2.6 Power Aware Routing Protocols

The power aware routing protocols tell in what specific ways the network can save power. There are four possibilities to save the power from the devices and they are

- Minimal Energy Consumption per Packet
- Maximize Network Connectivity
- Minimum Variance in Node Power Levels
- Minimize the Cost
1.3 **PROBLEM DESCRIPTION**

Features of ad-hoc networks such as shared wireless medium, stringent resource constraints, and highly dynamic network topology make the path selected by the routing protocol less reliable (Hao et al 2004). Thus, the existing routing mechanisms select paths which are mostly less reliable. In order to solve the routing problem in the ad-hoc networks, a Reliable Routing Scheme (RRS) is proposed.

The operating environment of mobile ad-hoc networks is highly distributed that does not have a centralized authorization facility. Most of the existing protocols of the ad-hoc networks discover the paths between source-destination pair on the assumption that all nodes are legitimate and cooperating nodes. But in reality, a malicious node may enter the ad-hoc network and compromise the routing protocol functionality (Papadimitratos et al 2002). Hence, it is necessary to devise secure routing protocols to make routing and data forwarding secure. Extensive research by researchers, has led to a number of secure routing protocols and some of them are discussed by Hu et al (2004). Many of these protocols encrypt the routing messages in the processes of route discovery and route maintenance, which result in more communication and computation overhead. A Secure Routing Scheme (SRS) is proposed to solve the secure routing problem in the ad-hoc networks.

1.3.1 **Reliable Routing Scheme**

The RRS is discussed in three phases. The three phases are route discovery phase, reliability computation phase and route maintenance phase. The path selected by this proposed scheme is more reliable than the other existing paths between the source and the destination. This scheme is simple to implement as there is not much special hardware requirements.
1.3.1.1 Route discovery phase

The Route discovery phase is used to find the multiple paths between the source and destination. This phase is initiated when a source is in need to communicate with a destination node, but there is no valid route to the destination. This phase returns the entire path between the source and the destination. The reliability computation phase is called once the routes are discovered.

1.3.1.2 Reliability computation phase

The reliabilities of the various paths are calculated and the packets are routed through the path which is more reliable. The transmission reliability of path $p$ is $R_p = \prod r_i$ where $r_i$ is the reliability of the intermediate nodes in the path between the source and the destination.

1.3.1.3 Route maintenance phase

Route maintenance phase comes into action when a source receives a route error. This phase initiates a new route discovery if the source node still needs the route. Unused routes are dropped from the table when the route is not used for a long time.

1.3.2 Secure Routing Scheme

In SRS, three phases are defined. They are clustering, routing the data packets and intrusion detection. The proposed scheme identifies the clusters and elects the clusterhead which performs intercluster and intracluster routing. The intrusion detection is used to identify the intrusions.
1.3.2.1 Clustering phase

A flat network structure suffers from scalability problem in a large and dynamic MANET (Hong et al 2002). Hence, it is necessary to introduce hierarchy into the mobile ad-hoc networks when they are used for the applications in which the density of the nodes is high and at the same time, the nodes have frequent mobility. Clustering is the process of dividing the nodes of a mobile ad-hoc network into different virtual groups based on certain rules. In a cluster structure, nodes are assigned in various roles such as cluster-head, cluster-gateway and cluster-member. A cluster-head in a cluster serves as the local coordinator and coordinates communication process inside the cluster whereas a cluster-gateway is a non cluster-head node that coordinates communications between nodes, which are in different clusters. Cluster members are responsible for sending and receiving information with the help of cluster-heads and cluster-gateways.

The existing clustering algorithms discussed in Janne et al (2005) require a high refresh rate of cluster dependent information, thus introducing significant control overhead. The number of clusters formed is very large, causing inefficient bandwidth utilization. The main advantage of clustering is to reduce the communication overhead and improve bandwidth utilization. The clustering phase in the proposed scheme consists of two methods called cluster identification and clusterhead election. The Cluster identification is done by either an Artificial Neural Network (ANN) based method or Fuzzy C-Means method depending upon the necessity. The CH election is done by using backpropagation neural network. This process causes less overhead and helps in achieving the real advantage of clustering in the ad-hoc networks.
1.3.2.1.1 Cluster identification

The ANN used for cluster identification, is inspired from the biological neural network. The ANN is composed of many neurons that are connected within themselves. The ANN is based on competitive neural network. This network learns to classify input vector \( x = (x_1, x_2, \ldots, x_k)^T \) according to how they are grouped in the input space as

\[
y_i = \sum_{j=1}^{b} w_{ij} x_j,
\]

where \( w_{ij} \) is the \( (i,j) \)th element of the weight matrix \( w \). The winning neuron is \( y_k = \max_j(y_j) \), where \( k \) is the winning element. A straightforward implementation of the weight adjustment is to make

\[
\Delta w_{kj} = \eta(x_j - w_{kj}),
\]

so that

\[
w_{kj(new)} = w_{kj(old)} + \Delta w_{kj}.
\]

Also, the Fuzzy C-Means method is used for clustering in special cases where, the node set is more overlapping because in fuzzy sets, if one element belongs to a group, it will belong to every group with a specific degree. The degree is between zero and one. The degree is between zero and one. The membership matrix \( U \) is randomly initialized according to

\[
\sum_{i=1}^{c} u_{ij} = 1, \forall j = 1, \ldots, n,
\]

where \( c \) is the number of clusters to be identified. The dissimilarity function is given by the equation

\[
J(U, C_i) = \sum_{i=1}^{c} J_i = \sum_{i=1}^{c} \sum_{j=1}^{n} u_{ij}^{m} d_{ij}^{2},
\]

where \( u_{ij} \) is the value between 0 and 1, \( C_i \) is the centroid of cluster \( i \), \( d_{ij} \) is the euclidian distance between \( i^{th} \) centroid \( C_i \) and \( j^{th} \) data point, \( m \in [1, \infty) \) is the weighting exponent. There are two conditions to reach a minimum of dissimilarity function.
The first condition is

\[ C_i = \frac{\sum_{j=1}^{n} u_{ij}^m x_j}{\sum_{j=1}^{r} u_{ij}^m} . \]

The second condition is

\[ u_{ij} = \frac{1}{\sum_{k=1}^{c} \left( \frac{d_{ij}}{d_{kj}} \right)^{2i(m-1)}} . \]

1.3.2.1.2 ClusterHead (CH) election phase

Decentralization is the main draw back in the security perspective in an ad-hoc network. In order to give a centralized administration to curb the attackers easily, the CH is elected using artificial neural network.

The node with the highest reliability is selected as a CH. The ANN based election method uses the reliability of the nodes for election. An input vector \( G = (G_1, G_2, \ldots, G_u)^T \), is applied to the input layer of the network. The input units distribute the values to the hidden-layer units. The net input to the \( v^{th} \) hidden unit is \( \text{net}^{h}_{uv} = \sum_{z=1}^{A} w_{vz}^h x_{uz} + \theta_{v}^h \), where \( w_{vz}^h \) is the weight on the connection from the \( z^{th} \) input unit, \( \theta_{v}^h \) is the bias term. The ‘\( h \)’ superscript refers to quantities on the hidden layer. Assume that the activation of this node is equal to the net input, and then the output of this node is \( i_{uv} = f_v^h (\text{net}^{h}_{uv}) \). The equations for the output node are
\[ \text{net}_{u_k}^o = \sum_{v=1}^{L} w_{kv}^o \cdot i_{uv}^o + \theta_{k}^o \quad \text{and OUT}_{u_k} = f_k^o (\text{net}_{u_k}^o) , \] where the ‘o’ superscript refers to quantities on the output layer.

### 1.3.2.2 Routing phase

Once the clustering phase completes its task, the routing phase comes into action. In the routing phase, the table driven based protocol is used to forward the data at the intercluster level and on-demand based protocol is used to forward the data at the intracluster level. Thus, the proposed routing approach works on a hybrid basis.

### 1.3.2.3 Intrusion detection phase

Intrusion Detection System (IDS) is a monitoring program, which aims at detecting intruders who are trying to access the resources illegally in a network (Dorothy et al 1987; Rebecca et al 2000; McHugh et al 2001; Fernando et al 2004 and Nong et al 2004).

IDS can be classified into two types, namely, misuse detection and anomaly detection system based on how data analysis is carried out (Yu et al 2005 and Ingo et al 2005). In the misuse detection, patterns are learned from already known attacks. These patterns are searched through the unseen data to find intrusions of the already known types. On the other hand, in anomaly intrusion detection, patterns are learned from normal data. In this approach, the unseen data is checked and searched to find deviations from these learned patterns (Kymie et al 2002). These deviations are called anomalies for possible intrusions. Misuse Detection has the advantage of not only detecting the intrusions but also identifying the type of the particular intrusion and is capable of reducing misclassification rates.
The various research issues to be considered in the design of intrusion detection system are good system architecture (Wenke et al 2000; Srinivas et al 2004 and Marek et al 2006), identification of appropriate audit data sources and a good model of activities in mobile environment.

This research work focuses on the design of ANN based intrusion detection system architecture, to identify two types of attacks. The first one is false route request attack and the second one is the false route reply attack. In order to identify these attacks, the artificial neural network based IDS is activated in every CH.

1.4 IMPLEMENTATION OF THE ROUTING SCHEMES

In this thesis, the proposed routing schemes are implemented in the Global Mobile Information System Simulator (GloMoSim) library (Takai et al 1999). Nodes move according to the random waypoint model (Josh et al 1998). Each node moves towards the destination at a speed distributed uniformly between zero and a maximum speed of 30m/s. The IEEE 802.11 protocol is used as the MAC layer protocol in the experiments.

1.5 RESULTS AND DISCUSSION

The routing of data, based on the proposed reliable routing scheme delivers the packets through the path that is more reliable. This routing scheme gives better throughput reducing the end-to-end delay compared with other existing routing protocols.

The proposed clustering schemes reduce the number of clusters and also the re affiliations count of the nodes when compared with other existing methods.
The proposed ANN based intrusion detection system is trained with various sets of data. The simulation results show that the IDS is able to identify the intrusions in a quick manner with an average classification rate of 90.13%.

The packets are delivered in a secured manner with reduced end-to-end delay and also with higher throughput by the proposed routing scheme. Thus, the secure routing scheme performs better than other existing methods.

1.6 ORGANIZATION OF THE THESIS

This thesis is focused on reliable and secure routing in an ad-hoc network. The thesis is organized into seven chapters.

The current chapter deals with an overview of the thesis where the proposed routing schemes are discussed briefly.

In the second chapter, the literature survey is done. The various research works related to the proposed work are discussed under different classifications. These works are also compared with the proposed work in the corresponding sections.

The third chapter is used to exhibit the system design and architecture of the proposed routing schemes.

The fourth chapter deals with the reliable routing scheme. The route discovery, reliability evaluation and route maintenance phases are described.

The fifth chapter describes the three phases that are used to solve the secure routing problem.
The results of the proposed routing schemes are discussed in the sixth chapter.

In the seventh chapter, the overall conclusion of the routing schemes is given and the future enhancements that can be done on the routing schemes are suggested.