CHAPTER 1

INTRODUCTION

1.1 Mobile Ad hoc Networks

A mobile ad hoc network (MANET) is a collection of mobile nodes or routers which are connected by wireless link forming an arbitrary topology. MANETs are different from conventional networks in the sense that they are dynamic in nature having no fixed infrastructure. Ad hoc Networks provide communication in the absence of a fixed infrastructure without a central administrating authority, which makes them an attractive technology for various applications such as rescue operations, disaster recovery, tactical operations, environmental monitoring, mobile conferences, etc.

Ad hoc network was first set up in 1970s as a part of a defence research project and was called a Packet Radio Network (PRNET). It then evolved into Survivable Adaptive Radio Networks (SURAN) programme in the early 1980s which provided a packet-switched network to the mobile field in an infrastructure-less environment. This program was quite beneficial in improving the radio performance and made these networks cheaper, smaller and resilient to electronic attacks. Since 1990s, the concept of commercial ad hoc networks emerged with the arrival of notebook computers, PDAs, mobile phones and other viable communication equipments.

There are certain inherent features of MANETs. Nodes in the network move independently in an unrestricted geographical topology. Each node can freely join or leave the network as there is no specific entry or exit point. Nodes have limited battery power, memory and CPU capacity. There is no central administrating authority for managing the task of routing in the network. Nodes act as both hosts as well as routers and rely on their neighbours to route their traffic to the destination. Features such as rapid deployment, flexibility and adaptability make MANETs a very promising technology.
1.2 Salient Features of MANETs

MANETs comprise of mobile nodes or routers that are equipped with wireless transmission and reception circuitry which operate using omni-directional antennas. Formation of links between nodes depends upon the relative position of nodes, transmission power and signal interference etc. Salient features of MANETs are as follows:

1. Dynamic Topology

Nodes, in MANETs, can roam freely in an arbitrary fashion resulting in frequent and unpredictable changes in the network topology. Furthermore, nodes can enter or exit the network randomly which leads to arbitrary loss of connectivity in the network.

2. Autonomous Configuration

MANET nodes operate in an infrastructure-less environment in the absence of any central administrative authority. Nodes are self-configuring in nature and act as host nodes as well as routers to perform the task of routing in the network. MANETs provide increased robustness than centralized networks where a failure of a single node may paralyse the functioning of the whole network.

3. Heterogeneous

Plethora of devices is available to work in mobile computing environment. These mobile devices range from PDAs to mobile phones and pagers which are small hand-held devices and are low on power to large devices having much more computing power like laptops, pocket computers, etc. MANETs provide a flexible and interoperatable platform that allows these diverse nodes to work in a unified environment.

4. Node Interdependence

Nodes, in MANETs, have limited transmission range and can communicate directly with other nodes lying within their transmission range. However, to communicate with distant nodes lying outside their transmission range, nodes rely on other nodes (acting
as routers) in the network for performing vital network functions such as routing of data packets on behalf of source node. Therefore, node co-operation is indispensable in infrastructure-less, decentralized networks like MANETs.

5. Paucity of Resources

Mobile nodes in MANETs are battery-powered and are dependent on some exhaustible energy resource available with the nodes. This makes energy optimization an integral part of protocol design for MANETs. Moreover, the wireless nature of link creates a bandwidth constrained environment. Furthermore, due to signal interference, noise, fading, multiple access the realized throughput is low with respect to maximum capacity of channels.

6. Prone to threats

Due to inherent features of MANETs such as node interdependence, infrastructure-less environment, lack of central administrating authority and paucity of resources, they are more pregnable than their wired counterparts. This leads to increased threats such as denial of service, spoofing, eavesdropping, masquerading etc. Moreover, autonomously configured nodes may tend to misbehave in absence of centralized authority in order to conserve their resources. These nodes may refrain themselves from participating in the network functions while exploiting other nodes by using their services. Such kind of misbehaviour or security threats can paralyse or may completely disrupt the network operations.

These above stated features of MANETs form the premise for protocol design for the task of routing in such versatile networks.

1.3 Applications of MANETs

MANETs provide communication in the absence of a fixed infrastructure without any central administrating authority, making them suitable for various applications. Various applications
of MANET are as follows:

1. Instant Infrastructure-less Networking

Creation of infrastructure for networks require a great detail of planning, installation and expenditure whereas, MANETs do not require any kind of underlying infrastructure such as base stations for communication amongst the nodes. This makes MANETs suitable for establishing instantaneous networks in applications like unscheduled meetings, inter-personal communication etc.

2. Strategic Networking

Intrinsic features of MANETs make them optimal for use in military applications, environmental monitoring and other tactical operations etc. There has been a significant increase in use of technology in modern warfare such as drones, surveillance equipments, combat bots etc. MANETs provide an efficient solution for strategic communication in the battlefield where development of infrastructured networks is not practicable.

3. Disaster and Rescue Operations

Natural disasters such as floods, hurricanes, tsunamis, earthquakes etc. may cause immense damage in the affected areas and result in loss of property, infrastructure and lives. In such catastrophic situations, rescue and search teams can rely on autonomously configuring networks like MANETs to carry out the relief operations. MANETs provide an adequate and efficient replacement for destroyed network infrastructure in case of natural disasters as well as emergency situations.

4. Commercial Applications

MANETs may prove to be a promising technology in applications where using existing infrastructure or creating a new one could be too expensive. MANETs are useful for commercial sectors such as e-commerce, mobile offices etc. They can be used for short range communication between mobile devices such as in conference halls, smart classes, virtual classrooms etc. Organizations may use MANET to create temporal networks in remote areas, construction sites, hostile terrains such as deserts, mountains
etc. MANETs can be deployed to provide services such as weather forecasting, road accident reporting etc.

5. Personal Applications

MANETs can be used to establish personal area networks for inter-personal communication using small hand-held devices such as tablets, PDAs, smart phones, notebooks etc. It eliminates the requirement of any wires for connection amongst the devices involved. It can be used for entertainment purposes such as gaming, P2P chat, home theatre systems etc. In addition, MANETs can also be used for extending internet coverage to the devices.

1.4 Routing Protocols for MANETs

A routing protocol can be defined as a standard or a set of rules which allow the nodes to determine a way to route packets between any two nodes in the network. Routing Protocols in Mobile Ad hoc networks can be abstracted into three categories: Proactive Routing Protocols (Table Driven), Reactive Routing Protocols (On-Demand) and Hybrid Routing Protocols. Classification of routing protocols in MANETs is illustrated in Figure 1.1.

In Proactive Routing Protocols nodes maintain tables storing routes/paths to every other node in the network. In order to do so, nodes disseminate topology information at regular intervals within the network. Routes are updated periodically based upon topology information received from other nodes. Table Driven Routing Protocols ensure availability of routes to any destination in the network whenever required. However, it increases the routing overhead in the network due to periodic sharing of topology information among the nodes. Destination Sequenced Distance Vector (DSDV), Optimized Link State Routing (OLSR) and Wireless Routing Protocol (WRP) are some of the prominent examples of Proactive Routing Protocols for MANETs.

Unlike Proactive Routing Protocols, nodes in Reactive Routing Protocols do not maintain any table of routes to other nodes in the network. Rather, the routes are determined by source
nodes whenever required. The nature of reactive protocols makes them suitable for bandwidth constrained environments as they do not require any periodic sharing of topology information, which reduces the routing overhead in the network. Moreover in networks where topology changes rapidly reactive protocols are more suitable than proactive protocols as fast changing topology may lead to inconsistency between the topology information stored at the nodes and real network scenario. However, a major limitation of reactive protocols is that the delay in route setup is higher as the routes are not readily available. Dynamic Source Routing (DSR), Ad-hoc On-demand distance Vector protocol (AODV), Admission Control enabled On-demand Routing (ACOR) and Associativity Based Routing (ABR) are few examples of reactive protocols.

Hybrid Routing Protocols or Hierarchical routing protocols are confluence of both proactive and reactive protocols. These protocols divide the network into a number of groups called clusters. Each cluster of nodes has an elected cluster head which is responsible for inter cluster communication. Nodes can communicate with other nodes lying outside their clusters through the cluster head of their corresponding clusters, whereas nodes within a cluster can communicate directly with each other. A major drawback of such routing protocols is the com-
plexity involved in cluster head election process as nodes may refrain themselves from being selected as a cluster head. Zone routing Protocol (ZRP), Temporary Ordered Routing Algorithm (TORA), Hazy Sighted Link State (HSLS) and OrderOne Routing Protocol (OORP) are some of the examples of hybrid protocols.

1.5 Dynamic Source Routing Protocol

Dynamic Source Routing (DSR) Protocol is an efficient on-demand routing protocol for mobile ad hoc networks. DSR enables network nodes to communicate without any fixed infrastructure in the absence of any central administrating authority. DSR automatically determines and maintains the routing information in accordance to the rapidly changing topology in MANETs.

DSR is a source routing protocol in which the route to destination is determined by the source node itself and is transmitted along with the data packet. The routing information contained in the packet header can be cached by intermediate nodes for future use. DSR provides low routing overhead and ensures successful delivery of packets by rapidly reacting to mobility of nodes in the network.

DSR protocol employs two processes, namely: Route Discovery and Route Maintenance for the task of routing. Route Discovery process is invoked by the source node when it wishes to communicate with a node in the network to which the route is not already known. Route Maintenance process is invoked by the source node when it detects that a link in an existing route to the destination is broken. Source node can either use another route stored in the route cache or can attempt to find a new route to the destination.

Due to on-demand invocation of Route Discovery and Route Maintenance process in DSR, there is no regular exchange of routing information among nodes which immensely decreases the overhead in the network. Moreover, intermediate nodes and nodes overhearing data packets can cache multiple routes to various destinations in the network which can be used when primary route fails and further decreases the amount of control information in the network.
1.5.1 Route Discovery Process

When a source node attempts to transmit a packet to the destination, it encapsulates the complete sequence of nodes in the packet header through which it has to travel to reach the destination. Firstly, the source node searches its route cache to determine any existing routes to the destination. If the route does not exist, the source node invokes the route discovery process in order to find a new route to the destination.

Figure 1.2 shows how a source node U discovers a route to node V by invoking Route Discovery process. Node U generates and broadcasts a ROUTE REQUEST (RREQ) packet containing the address of the source node (Initiator), destination node (Target) and an empty route record. A unique id is associated with each ROUTE REQUEST packet by the source node. Route record consists of the addresses of nodes through which the corresponding RREQ packet has travelled. RREQ packet is received by all one-hop neighbours of node U that lie within its transmission range. Upon receiving a RREQ, a node checks whether it is the destination (Target) node specified in the RREQ packet. If so, it generates a ROUTE REPLY (RREP) containing the collected route record stored in the RREQ packet. The RREP can be transmitted to the source node by the destination in three ways. Firstly, the destination node can use the route stored in its route cache to determine the route from node V to node U. Secondly, if no route is found in the route cache, it can invoke the route discovery process to determine a new route to node U. Thirdly, it can simply reverse the route contained in the route record of the received RREQ packet. Upon receiving a RREP packet, the source node U transmits the data packet through the route received in the RREP packet.

Each source node maintains a buffer known as send buffer which stores a copy of packets for which the route to the destination is yet to be determined. Each packet has a time-out period associated with it. After the expiry of this time-out, the packet is removed from the buffer. Until the packet resides in the buffer, the source node iterates the route discovery process in order to find a route to the destination. However, a node may sometimes be unreachable due to mobility of nodes in the network. This may lead to unnecessary routing information in the network. DSR uses exponential back-off to limit the rate at which route discovery process can
be invoked for the same destination. If the node tries to transmit additional data packets to the same destination node more frequently than exponential back-off limit, the subsequent packets are buffered until a RREP is received providing a route to that destination, but the node is not allowed to start a new Route Discovery process until the minimum allowable timer between new Route Discovery processes for that destination expires.

1.5.2 Route Maintenance Process

Each intermediate node is responsible for relaying the packet to the next hop in the source route and providing confirmation that the packet has been received by the next node. If no confirmation is received, the packet is retransmitted until the receipt of confirmation or maximum number of allowable attempts is exhausted.

Figure 1.3 illustrates how node $U$ transmits a packet destined for node $V$ through intermediate nodes $A$, $B$ and $D$. Each hop is responsible for confirming the receipt of packet the next hop. For example, node $A$ holds the responsibility that the packet is delivered to node $B$ and
so on. If maximum number of allowable retransmissions is exhausted and no confirmation is received, the corresponding intermediate node generates a ROUTE ERROR (RERR) message for the source node. Figure 1.3 also depicts how node $B$ transmits a RERR message to node $U$ on detecting a failure of link between node $B$ and node $D$. On receiving a RERR message, node $U$ either uses another route available in route cache or re-invokes route discovery process to determine route for destination $V$.

### 1.5.3 Other Features of Route Discovery process

Some additional features of Route Discovery process in DSR protocol are discussed below:

#### 1.5.3.1 Route Caching

An intermediate hop that relays a received packet or a node that overhears a packet on wireless channel may store the route record, given in the packet header, in its cache for future
use. Routing information may be cached from packets by a node to which they are destined, broadcasted or overheard in promiscuous mode.

### 1.5.3.2 Route Reply using Cached Information

An intermediate node, on receiving a RREQ packet, may use the routing information stored in its route cache to generate RREP message. If a valid route is found in route cache, the corresponding node concatenates this information to the route record received in the RREQ packet and transmits the RREP message to the source node. DSR prohibits nodes from generating RREP messages based upon cached routes if duplicate nodes are found in the route record after concatenation of the routing information. In such a case, no RREP message is generated and the RREQ packet is discarded by the intermediate node.

### 1.5.3.3 Avoiding RREP storms

RREP storms is the phenomenon in which all the one-hop neighbours of the initiating node, on receiving RREQ packet, generate and propagate RREP messages with their corresponding cached routes to the source node. This may lead to bandwidth wastage, collision and congestion in the network. To prevent such RREP storms, DSR adopts a mechanism in which a node postpones the transmission of RREP message for $d$ units of time given by:

$$d = H \ast (h - 1 + r)$$  \hspace{1cm} (1.1)

where $H$ is the fixed delay, $h$ is the number of hops in the cached route and $r$ is a number lying between 0 and 1. During this period, the node promiscuously listens to the wireless channel in order to find out if the source node has begun its transmission using a shorter route. If so, a node refrains itself from sending RREP message as the source node already has a better route.

Hop limit is an integer that is associated with each RREQ message. It signifies the number of hops that can propagate the corresponding route request message. Whenever an intermediate node propagates the RREQ packet, it decrements the value of its hop limit by one. When this
value reaches zero, the RREQ packet is discarded and not propagated any further. DSR uses this procedure to generate two kinds of RREQ messages non propagating (hop limit equals to zero) and propagating RREQ messages (no hop limit). Non propagating RREQ messages are a way to find whether the destined node is one-hop neighbour of the node initiating RREQ packet, or if any of its one-hop neighbour has a cached route to the desired destination. If none of the one-hop neighbours of the source node sends back RREP message then, second type of RREQ message i.e., propagating RREQ message is generated to determine the route to the destination.

1.5.4 Other Features of Route Maintenance process

Some additional features of Route Maintenance process in DSR protocol are discussed below:

1.5.4.1 Packet Salvaging

An intermediate node detecting a link failure generates a RERR message to the source node indicating the broken link and it may try to salvage the packet during the transmission of which the link failure is detected. In order to do so, the node searches for an alternate route in its cache to the next hop. If such a route is found, it is used to relay the packet. The salvaged packet is marked to avoid it from entering into a loop where nodes may send the packet to each other again and again in order to salvage the packets.

1.5.4.2 Automatic Route Shortening

DSR provides the mechanism of gratuitous RREP message that are generated by the intermediate node which detects that a shorter path than the one used by the source node can be established through it. On listening a packet in promiscuous mode, if a node detects that it is not the next hop in sequence but appears later in the route record, it implies that the hops appearing before the corresponding node are not required in the route. This information about
the better route is transmitted to the source node by the corresponding node in the form of gratuitous RREP message.

1.5.4.3 Piggybacking of RERR messages

DSR uses the mechanism of piggy backing RERR messages on RREQ messages in order to ensure better propagation of RERR messages in the network. All the nodes receiving this information update the routing information (stored in their cache) by removing the stale routes based on the piggybacked RERR message.

1.5.4.4 Caching negative information

On receiving information about link failure in the network, the source node saves this ‘negative information’ in its cache. This information is used by the source node to ensure that it does not utilize the RREP containing the route through the broken link. A time-out period is associated with every negative information stored in the cache, after the expiry of which the node will reconsider the broken link. This is done to avoid rejection of link by the source node even when the link failure is rectified.

1.5.5 Advantages of DSR

This section entails the various advantages of DSR protocol.

DSR protocol reduces the routing overhead in the network by eliminating the need for regular exchange of control information among nodes. It does not require any neighbour sensing mechanism or regular topology control messages for maintenance of routing information, thereby, decreasing control traffic in the network, conserving bandwidth as well as the battery life of nodes.

It does not require large routing tables to be maintained at each node in order to store routes for the transmission of data packets as the source route is provided by the source node itself
in the packet header. Nodes maintain routes only for the nodes with which they wish to communicate, thereby, decreasing the complexity of route maintenance process.

Nodes, in DSR, cache the routes given in packet header when they are acting as intermediate nodes during a communication or while overhearing a transmission on wireless channel. These cached routes are used by nodes for replying to RREQs or for their own data transmission which, in turn, decreases the number of times route discovery process is initiated by the nodes, consequently, reducing the overhead in the network.

DSR is capable of finding appropriate routes in an environment where asymmetric links may exist between nodes due to signal interference, varying strength of antennas or voluntary use of asymmetric links etc. Other Classical protocols like link state and distance vector may fail to find correct routes in such environment, whereas DSR protocol efficiently finds relevant routes by taking into account asymmetric nature of links in the network.

1.5.6 Limitations of DSR

This section entails various limitations of DSR protocol. One of the major limitations of DSR is scalability. It works efficiently in networks having small number of nodes but has scalability issues for networks having more than 200 nodes.

It consumes more processing power of nodes as compared to other protocols. Nodes are required to process the received control data to obtain routing information, even if they are not the target (destination) node.

Another limitation of DSR is the delay in route setup. As the initiator node which generates RREQ message has to wait until it receives RREP message before starting the data transmission. RREP storm is another limitation of DSR protocol where the initiator node receives large number of RREP messages, resulting in contention.

DSR lacks any mechanism to remove stale routing information from route cache of nodes. RREP messages generated using outdated information may pollute the routing information stored at other nodes.
Route maintenance process, in DSR, does not provide any mechanism to repair the broken links at local level. The information about the broken link is merely conveyed to the source node without taking any further actions for local repair of the link.

Due to source routing in DSR, the packet header size grows immensely with increasing the number of hops in the route. Flooding of RREQ messages by nodes may increase the number of collisions in the network. Flooded RREQ message reaches almost all the nodes in the network. The first node that has the route to the destination generates a RREP message to the source node. An idle node lying beyond the node that has generated RREP message processes the RREQ message even when the source node has already received RREP message from some other node. This results in loss of processing resources of the nodes in the network.

1.6 Routing Misbehaviour

Due to intrinsic factors of MANETs such as lack of central administrating authority, no fixed infrastructure, dynamic topology etc., co-operation among nodes forms the basis for communication in the network. Nodes having limited transmission range share resources and co-operate to provide connectivity in the network. But owing to limitation of resources like battery power, memory, CPU time etc., nodes find it economically logical to exhibit non-cooperating behaviour. Such nodes try to conserve their resources by refraining themselves from providing network services to other nodes. However, they continue exploiting the resources of other nodes in the network. These nodes are termed as misbehaving nodes and can be classified as follows:

1. Malicious Node: It misleads nodes by responding positively to the route request but may not actually participate well in forwarding of packets. It may exhibit the following types of misbehaviour:

- Packet Drop: A node actively participates in the route formation but later drops packets of other nodes in the guise of forwarding them hence, misleading other nodes into unsuccessfully sending their traffic through it. Such nodes act as sinks;
Figure 1.4: A Malicious Node

posing a serious threat to resource availability in the network.

- Partial data forwarding: A node may stop forwarding packets after transferring a few of them and try to cheat the monitoring system. Such nodes reduce the availability of resources to other nodes in the network.

- Tampering of data packets: A node participates in route discovery process, but once the route is established and packets are being transmitted, it may tamper with the data while forwarding it. This kind of misbehaviour is a threat to integrity of data shared in the network.

Figure 1.4 illustrates the behaviour of a malicious node. As shown in Figure 1.4, node $A$ is a malicious node which forwards the route request from node $U$ but when once the route is formed and node $U$ starts transferring the packets, it intentionally drops these packets instead of forwarding them to node $B$.

2. Selfish Node: It is the one that conceals itself by being non-responsive in order to conserve resources and exhibits the following type of misbehaviour:
Non-participation: A node may not respond to route request for preserving its resources but may exploit others by sending its own traffic through the network. It enjoys network services but refuses to forward the packets of other nodes. Its participation is limited to just sending and receiving its own packets. Such nodes deny services to other nodes causing serious threat to availability of network services.

Figure 1.5 depicts the behaviour of a selfish node. In Figure 1.5, node $A$ is a selfish node that does not participate in forwarding the route request generated by node $U$. Therefore, another route i.e. from node $U \rightarrow F \rightarrow G \rightarrow V$ is formed. However, node $A$ tries to transfer its own packets through other nodes.

3. Erroneous Node: It is a well-behaving node which does not aim to interrupt network operations but may not be able to participate in networks functions due to some kind of error in the system. After recovering from failure, it resumes its functioning as a well-behaving node and hence, must not be misunderstood and treated as selfish or malicious node. Erroneous nodes exhibit the following type of misbehaviour:
Unintentional Packet dropping or Non-participation: A node willing to participate in network operations may fail to do so due to failure. It has no intention of dropping packets of other nodes but is unable to relay them due to some failure in the system, such as transient link failure, hardware or software failure etc. As the node is unable to forward the packet within a specified time limit, the packet is declared as being dropped.

Figure 1.6 shows the behaviour of an erroneous node. In Figure 1.6, Node A is an erroneous node that is not able to forward the packets of node U to node B due to failure in its system. Node C is also an erroneous node which is unable to forward route request of node U to node E due to some kind of error in its system.

1.7 Terminology Used

This section presents a list of significant terms that have been frequently used in this work.
• Misbehaving Node: A node that wishes to conserve its own resources by avoiding participation in network functions while exploiting others by using their services.

• HELLO message: It is a periodically generated neighbour sensing message which is used to discover all the one-hop neighbours of the originating node.

• Route-Request Packet: A packet generated by the source node to find route to a desired node in the network. This packet is received by all the one-hop neighbours of the source node. These nodes either forward the packet or generate route reply message to the source depending upon whether they have the route to the desired destination or not.

• Reputation: It is the opinion of one node about another.

• Local reputation-based scheme: A scheme in which a node makes an assessment about the behaviour of another node by directly communicating with it.

• Global reputation-based scheme: A scheme in which a node gathers information about the behaviour of a node from other nodes in the network.

• MPR Nodes: Specific nodes that are selected for the purpose of broadcasting information such as topology control messages etc.

• MPR Selector Node: A node that selects MPRs from its one-hop neighbour set to relay its information in the network.

• Flooding MPRs: Nodes that are used to spread topology control information in the network.

• Routing MPRs: Nodes that are used for relaying data packets for the selector node.

• Packet Delivery Ratio: It is the ratio of number of data packets received by the destination to the number of data packets sent by the source node.

• Throughput: It is defined as the number of data packets correctly delivered to the destination in an observed duration of time.

• Average End-to-End Delay: It is the time taken for a packet to be transmitted across a network from source to destination.
• Routing Overhead: It is taken as the ratio of number of control packets generated to the number of data packets sent.

• Network Lifetime: It is defined as the time when the first dead node is detected in the network.

1.8 Organization of the Thesis

Following the introduction to the thesis in Chapter 1, the rest of the thesis is organized as follows:

The Chapter 2 presents the literature survey. It includes the review of various schemes that deal with the problem of routing in MANETs. It has helped in the development of new reputation based scheme for handling misbehaviour in mobile ad hoc networks.

The Chapter 3 includes the formulation of research problem. It discusses the various research gaps in the existing literature. Based on these identified gaps, research objectives have been defined. This chapter also includes the methodology used for achieving the objectives. It also entails the contributions made by this research work.

The Chapter 4 describes the proposed scheme used for detecting and mitigating the effect of Selfish, Malicious and Erroneous nodes in mobile ad hoc networks. It presents a reputation and collaboration technique through route-request to efficiently handle the problem of routing misbehaviour. It includes the implementation of the scheme in Network Simulator NS-2. It also provides a comparative analysis of this scheme with other existing reputation based schemes.

The Chapter 5 presents an adaptive model for handling dynamic behaviour of nodes in mobile ad hoc networks. It provides an Adaptive Requiting and Punitive Mechanism (ARPM) to requite the well behaving nodes and punish the misbehaving ones. Implementation of this scheme is performed using NS-2. This chapter also includes the comparison of this scheme with traditional DSR protocol.
The Chapter 6 discusses an energy efficient and secure technique for Multipoint Relay (ES-MPR) selection in mobile ad hoc networks. This scheme works with OLSR protocol. This chapter analyses the effect of misbehaving nodes on network performance. It provides a novel technique which considers both energy and security metrics during MPR selection process. It also includes the performance evaluation and comparative analysis of ES-MPR with other existing schemes.

The Chapter 7 gives concluding remarks on the research by highlighting the significant contributions of the work done. Future directions of the implemented research work have also been presented in this chapter.

1.9 Chapter Summary

This chapter gives an introduction to mobile ad hoc network along with its salient features and applications. It presents a brief description of various routing protocols in MANETs. Details about basic working of Dynamic Source Routing (DSR) Protocol are provided along with its advantages and limitations. This chapter also explains the problem of routing misbehaviour in MANETs.

The next chapter presents the review of various schemes that deal with the problem of routing misbehaviour and energy efficiency in MANETs.

Research Publication out of this Chapter