MANET is a collection of wireless mobile nodes forming a temporary network without the aid of any established infrastructures or centralized administration. MANET remove the dependence on fixed network infrastructure by treating every available mobile node as an intermediate switch, thereby extending the range of mobile nodes well beyond that of their base transceivers. Other advantages of MANET include easy installation, low cost, more flexibility and ability to employ new and efficient routing protocols for wireless communication.

In the first part of this thesis, the characteristics of ad hoc networks and the challenges in securing the ad hoc network is discussed. Further the trust based approaches employed in combating the different types of attacks were discussed. Due to its open and dynamic nature the MANETs are vulnerable to both active and passive attacks. In this thesis different types of attacks and methods to combat those attacks are evaluated by using relevant simulations.

The proposed association based dynamic source routing protocol acts as an extension to existing dynamic source routing protocol to fight against the different types of packet dropping attacks namely selective packet dropping, blackhole attack, cooperative blackhole attack and greyhole attack.

When the nodes starts behaving in a selfish manner, the packet forwarding functions are disabled for all packets that have a source address or
a destination address different from the current selfish node. A packet drop is a kind of denial of service where a malicious node attracts packets and drops them without forwarding them to the destination however, a selfish node that operates following this model participates in the route discovery and route maintenance phases of the DSR protocol.

In order to tackle the packet dropping attack the association based approach by enforcing trust between the nodes is implemented. Each node in the network will monitor its surrounding neighbour and based on certain criteria decides the nature of association between them. This enhances the nodes to select the reliable routes instead of standard shortest route. The simulation results prove that there is a 10% increase in performance of proposed scheme with respect to throughput and packet delivery ratio.

A common mechanism to protect MANETs is through the use of encryption and hashing mechanisms. However, the implementation of these mechanisms generally imposes certain unessential requirements, which are considered as restrictive for unplanned environments. This research work elaborates the dynamic trust based approach through which association between nodes are used to resist selective packet drop attacks. The simulations prove that the proposed scheme achieves 5% to 10% improvement in terms of packet delivery ratio and throughput. The proposed scheme is equipped with technique to identify and isolate the malicious nodes from the active data forwarding and routing.
A black hole attack is a kind of denial of service attack where a malicious node can attract all packets by falsely claiming a fresh route to the destination and absorb them without forwarding them to the destination. The performance metrics of the conventional DSR and the improved DSR fortified with the trust are compared in front of the malicious nodes.

Dynamic trust based scheme analyses the cooperative black hole attack which is one of the new and possible attack in adhoc networks. In this attack a malicious node advertises itself as having the shortest path to the node whose packets it wants to intercept. To reduce the probability it is proposed to wait and check the replies from all the neighboring nodes to find a safe route. If these malicious nodes work together as a group then the damage will be very serious. This type of attack is called cooperative black hole attack. The proposed solution discovers the secure route between source and destination by identifying and isolating cooperative black hole nodes.

The modified dynamic source routing protocol discusses trust evaluation mechanisms in MANETs with a focus on securing systems against greyhole attacks. In specific, the merit of integrating trust in to MANET is displayed through a synthesis of the roles of trust and simulations. To defeat the greyhole attack, the direct trust estimation technique is effectively proposed in this section. As soon as the malicious nodes starts to drop packets, its corresponding direct trust levels maintained by its neighbour start to decrease, subsequently, the greyhole node is bypassed in all route selection. The modified dynamic source routing protocol delivers 10% improved
throughput and 17% increased packet delivery ratio under the greyhole attack scenario.

In this thesis, an improved dynamic source routing protocol fortified with the association based route selection is proposed, in contrast to the current route selection which involves selection of the shortest route to the destination node. For every node in the network, a trust value will be stored which represents the value of the trustiness to each of its neighbor nodes. This trust value will be adjusted based on the experience of which the node has got with neighbor nodes.

When any node wishes to send messages to a distant node, its sends the ROUTE REQUEST to all the neighbouring nodes. The ROUTE REPLY obtained from its neighbour is sorted by trust ratings. The source selects the most trusted path. If it’s one hop neighbour node is a companion, then that path is chosen for message transfer. If its one-hop neighbour node is a known, and if the one hop neighbour of the second best path is a companion then choose companion.

The source selects the shortest and the next shortest path. Whenever a neighbouring node is a companion, the message transfer is done immediately. This eliminates the overhead of invoking the trust estimator between companions. If it is a known or unknown, transfer is done based on the ratings. This protocol will converge to the DSR protocol if all the nodes in the ad hoc network are companions.