This thesis presents an intrusion detection mechanism for mobile ad hoc networks. The aim of the protection solutions for wireless networks is to offer security services like confidentiality, authentication, accessibility, integrity, and secrecy to mobile users. Different type of attacks has been for MANET at different levels, like internal, external, at routing layers, at the application layer. For intrusion detection and protection three tiers are discussed application, routing and trust. The data transfer takes place between different nodes. First a trusted connection is established between different nodes. The trust value is calculated on successful and unsuccessful interactions then trustworthy, untrustworthy nodes are identified. Second the routing policy is conformed for all nodes. Finally at the application layer data is routed on the type of application. The node not following trust or routing policy is considered a malicious node. In this research simulation different types of attacks has been done and also pseudo code for different attacks like route invasion, eavesdrop, sinkhole is provided. Then the performance of these attacks against the proposed algorithm has been calculated and result is displayed.

In the proposed algorithm after initialization each node in the network is expected to declare their policies for different tiers that is trust tier, routing tier, application tier. When each node is have their own policies they can communicate in the network in a secured manner. When a new node joins the network its lowest tier is checked whether the given node is trusted node. If the given node is trusted node then only it can join the network otherwise it cannot join the network. Then the requested node is checked for Routing algorithm here if the requested node is asked for the routing protocol. In the network all the nodes follow same routing policy. The requested node should also have the same policy otherwise it cannot join the network. When the requested node has same tier and routing policy as that of the network it can join the network. Now the requested node is asked for the application tier.
The implementation was done using OPNET Modeler. OPNET provides three domains network domain, node domain process domain. The trust tier was implemented using process domain and node domain, the routing tier was implemented using network domain. The application tier was implemented with node domain. Different scenarios for of 25, 50, 100 nodes were created and the performance of the algorithm was checked on different parameters.

Following statistics were collected for results delay, throughput, total traffic sent (Bits/sec, Packets/sec), total traffic received (Bits/sec, Packet/sec), total packets dropped. All the statistics were collected by changing type of routing algorithm AODV, DSR, OLSR algorithm. It was observed better performance with a DSR algorithm. The performance of the algorithm was checked with different types of attacks; for which MTTM got better throughput compared to other algorithms presented by other authors. The results have been included.