Abstract

A Mobile Ad-hoc Network (MANET) is a type of infrastructure-less as well as wireless network. MANET depends mainly on mobile nodes for its functionality. MANETs are highly dynamic networks characterized by the absence of physical infrastructure. Nodes of these networks functions as a routers which discovers and maintains the routes to other nodes in the network. In such networks, nodes are able to move and synchronize with their neighbours. Due to mobility, connections in the network can change dynamically and nodes can be added and removed at any time. Since nodes are mobile and distributive in nature and also communicating devices or nodes are resource-restricted and equipped with micro or bio sensors to acknowledge the signals where only traditional security systems based on cryptography and encryption are not sufficient for promising level security assurance. In this thesis we explore trust and security challenges to improve security assurance for MANET. We put our efforts to present a secure trusted model to influence the security assurance and significant adaptation of trustworthy communication. We propose a trust computation metric based on node's impulsive behaviour to become malicious in dynamic scenario and proposed algorithms for trust evaluation of every node. We incorporate the concept of trust into the MANET, and build a trust estimation model to quantify the trust level of every node in the network. Our model incorporates a new evaluation function for calculating Blind Trust value, Referential Trust value and a relationship function to combine both Blind and Referential Trust value. The new protocol TSRM captures the evidence of trust worthiness for other nodes from the security model and in return assists them to make better security decision. Also in this study a new Dynamic Source Routing Protocol for MANET based on trust model is developed to mitigate grayhole attack. Trust is calculated based on trust function. Nodes are selected based on the values of trust function and threshold value. The modified DSR protocol can effectively detect the grayhole nodes and isolate them from taking part on routing. We also propose a trust based mechanism for mitigating blackhole attack. Here also we improve the DSR header to calculate trust in the network. Almost improvement is being noticed in the modified DSR as compared with original DSR. Finally, a recommendation based trust model is designed for resisting dishonest recommendation problems. The effect of bad mouthing and ballot stuffing attacks are minimized through the proposed technique.