Abstract

Originally *Mobile Ad Hoc Network* (MANET) was conceived as a small isolated ad hoc network that does not have any connection to the outer world. However, over the years MANET has evolved into an important network having applications in various fields that requires communication with other infrastructure networks. This has necessitated MANET's connectivity with the Internet, albeit in a restricted manner. This means, usually MANET will work in isolation but occasionally may connect to an infrastructure network (e.g., Internet) if need arises. This brings us to an important issue of node identification in accordance to the usual IP network. Moreover, IP address facilitates multi-hop routing in mobile ad hoc networks. Upon further investigation we find that the protocols that can be used over such type of ad hoc networks also need to be authenticated so as to protect them from various types of attacks. Most of the existing *Network* and *Transport* layer protocols for MANET either do not consider this aspect or have high overhead or rely on separate security mechanisms. Therefore, we feel that these protocols need to undergo certain modifications so that it can be used efficiently in wireless mobile ad hoc environments and make them complete and self-sufficient. In our first work in this thesis, we present an IP configuration protocol that can allocate IP addresses, in a secured manner, to the authorized nodes of a mobile ad hoc network. The protocol is ID based and is purely distributed in nature with low overhead. In our next work we try to improve upon the address allocation and use AODV as the underlying routing protocol. We use a signature scheme (rather than RSA as used in our first work) for securing the process and thereby reduce network maintenance overhead, addressing latency and also the computational complexity of the security mechanism. In our third work we explore the network and transport layer of MANET and modify the AODV routing protocol and the standard TCP by including RSA based security mechanisms to make it more robust and reliable. We next propose a dynamic routing protocol and make it secure and more efficient by using bilinear pairing elliptic curve cryptography. In our final work we further improve the transmission control protocol by using a prediction

based system to foresee the network conditions which makes it more efficient in dynamic environment of MANETs.

Keywords: MANET, Address Allocation, Routing, Data Transmission, Authentication, Security.