Abstract

The work presented in this thesis attempts to improve the performance of wireless mobile ad hoc networks by protecting the network layer. Few simulations are presented as a study on the network and the malicious node behaviour. An Intrusion Detection scheme is implemented and the performance of the network is analysed on the basis of Network Throughput, Average Packets Dropped and the Average Latency.

*Mobile Ad-Hoc Network (MANET)* is an infrastructure-less, dynamic, self-organizing and self-configuring multi-hop wireless network. The mobile devices participating in the network should have wireless communication capabilities with limited range of the transmitters. They can directly communicate with other devices that are within their radio range. A few of the devices voluntarily forward some of the messages they receive and acts as routers, they form a multi-hop network with a wider reach. As there is no fixed or defined infrastructure, the network is dynamic and keeps on changing continuously. The routers are elected on demand amongst the communicating mobile nodes. The dynamic networking issues are handled in an ad-hoc manner. These mobile networks are useful when we consider collaborative applications among mobile participants. The best example would be to deploy such nodes in a search-and-rescue mission, military applications and in emergency situations where all participant nodes wish to share information about their immediate surroundings with their peers.

Here, the routers are considered to be trusted entities, the ad-hoc network routing is performed by the devices themselves. Thus, there is a high risk that some of the nodes of an ad-hoc network would not respect the networking protocols. This
can be due to maliciousness, or simply selfishness of the node. This nature of the Adhoc network necessitates the requirement of a reliable broadcast protocol for ad-hoc networks.

Securing Wireless Network has emerged as one of the most researched areas in the field of wireless mobile ad hoc networking. In the absence of fixed infrastructure and dedicated routers, providing security to the network becomes a challenging task in ad hoc networks. Traditional routing protocols do not provide the required security at the required level.

Routing protocols, Ad Hoc on Demand Distance Vector (AODV) routing protocol and Dynamic Source Routing (DSR) protocol, typically assume a trusted and cooperative environment. Hence they become easy prey, a malicious attacker can readily become a router and disrupt network operations by its malicious activity like the Black Hole attack and Gray Hole attack.

The security solution should encompass the protection of both ad hoc routing and packet delivery as they form the backbone of network-layer operations. Malicious nodes may disrupt routing algorithms by transmitting a false hop count; by dropping data packets and by routing the packets through unintended routes and so on. In this project an IDSAODV is proposed to prevent the security threats of the Black Hole and Gray Hole attacks by notifying the other nodes in the network of the incident. The simulation results in NS2 (version 2.35) demonstrate that the protocol not only prevents Black Hole attack and Gray Hole attack but consequently improves the overall performance of AODV in presence of these attacks.