ABSTRACT

Wireless ad-hoc networks are clusters of self managed autonomous nodes without any infrastructure. By this, an ad-hoc network gets a dynamic nature which permits a node to join or leave the network any time. Since in ad-hoc network, nodes communicate with each other without an infrastructure, it is suitable for places where a fixed infrastructure cannot be created. In ad-hoc network nodes use some routing protocols like AODV, DSDV, OLSR, ZRP and provide connectivity by forwarding packets over themselves. Thus a node not only acts as a host but also acts as a router to discover a path and forwards the packets to the correct destination in the network.

Wireless networks are more sensitive to security threats than wired networks because of their nature and properties. It makes wireless network more vulnerable to attacks both from inside and outside. This thesis mainly addresses the attacks on MANETs and their challenges and detection along with counter measures.

In particular, we have analyzed various attacks on MANETs like Black hole attack, Worm hole attack, Grey hole attack, Sybil attack in great detail. In particular we have analyzed the challenges in detection of these attacks and shortcomings of their countermeasures. We have analyzed the vulnerabilities of routing protocol and classified the attacks according to their consequences. This knowledge enables us to propose a light weight and non cryptographic detection method for MANETs.

Finally to mitigate the effect of the wormhole attack, we propose WPT concept with AODV to avoid overheads due to overhearing and for the Black hole attack in MANET, we propose a timer based buffer mechanism for black hole attack detection. We also propose a novel attack in this thesis AODV that is Collision BWhole attack and analyze the impact on network performance.