Abstract

Wireless network is a growing technology that facilitates users for sharing of information instantly through wireless electronic devices irrespective of their locations. It can be infrastructure based or infrastructure less (ad hoc networks). An ad hoc network gains more attention because of its convenience, mobility, scalability, cost and easy setup. It is best suitable for applications, where predefined infrastructure is not possible. But ad hoc network is vulnerable to various attacks due to its functionality and deployment scenario. It is a decentralized networks therefore all the routing activities are handled by nodes. Nodes may behave badly in the network and can drop the packets instead of forwarding them. The aim of this research work is to detect these packet dropping nodes in MANET and prevents these packet droppers to be chosen as an active element of the path used for packet forwarding in DSR (Dynamic Source Routing) protocol. For this, we have implemented a trust and cluster based monitoring technique and simulated this environment using network simulator NS2.


Index Terms

Computer Science  Networks
Keywords

MANET; Vulnerable; Packet dropper; Wormhole; Man-in-middle attack; Spoofing.