A Wireless ad-hoc network is a temporary network set up by nodes moving arbitrary in the places that have no network infrastructure. The nodes find a path to the destination node using routing protocols. However, due to security vulnerabilities of the routing protocols, wireless ad-hoc networks are unprotected to attacks of the malicious nodes. One of these attacks is the Black Hole Attack against network integrity absorbing all data packets in the network. Since the data packets do not reach the destination node on account of this attack, data loss will occur. In this paper work, we propose AODVB (Ad hoc On-Demand Distance Vector with Black-hole Avoidance) protocol for avoiding black-hole attack. AODVB forms link disjoint multi-path during path discovery to provide greater path selection in order to avoid malicious nodes in the path using legitimacy table maintained by each node in the network. Non-malicious nodes gradually isolate the black-hole nodes based on the values collected in their legitimacy table and avoid them while making path between source and destination. We simulated AODV protocol with and without Black-hole attack and our solution AODVB protocol. From our simulation results AODV network has normally 3.21 % data loss and if a Black Hole Node is introducing in this network
data loss is increased to 92.59 %. When we used AODVB protocol in the same network, the data loss decreased to 65 %.

References

Index Terms

Computer Science

Networks

Keywords

Black Hole Attack, link disjoint multi-path, legitimacy table.