Abstract

Wireless Mesh Networks (WMNs) is an emerging technology. Amongst number of challenging issues, security is a very serious issue in WMNs. If the network is not secured, network will be confined to a limited and controlled environment. In WMNs, the static mesh routers (MRs) cooperate with each other to forward packets. The routing protocols assume that all the routers in the network are reliable. Due to open architecture of the WMNs, it suffers from various types of denial of service attacks like collision attacks, packet dropping and misdirection, blackhole attack and multiple blackhole attack. In black hole attack, the routers advertise itself to have a valid route to a destination router, though the route is unauthentic. Some routers can also co-operate with each other to implement multiple blackhole attacks. Many Intrusion Detection
Mitigation of Multiple Blackhole Attack in WMN

Systems (IDSs) such as use of honeypot and routing protocols like modified Ad hoc On-Demand Distance Vector Routing (AODV) have been introduced. In this paper, an algorithm for intrusion detection against multiple blackhole attacks has been proposed. The proposed scheme uses the Data Routing Information Table (DRI) to accurately diagnose multiple black hole attack.

References


Index Terms

Computer Science

Wireless
Keywords
Blackhole  Data Routing Information  Intrusion Detection  Multiple Blackhole  Wireless Mesh Networks.