A mobile ad-hoc network is a self-configuring, substructure network of mobile devices associated by wireless links. Loopholes like wireless average, lack of a secure infrastructure, dynamic topology, rapid disposition practices, and the hostile surroundings in which they may be deployed, make MANET susceptible to a wide range of security attacks and Wormhole attack is one of them. During this attack malicious node detentions packets from one location in the network, and channels them to another colluding malicious node at a detached point, which replays them locally. The protocol is an optimization of the traditional link state algorithm personalised to the supplies of a mobile wireless LAN. The key concept used in the procedure is that of multipoint relays. MPRs are selected nodes which advancing broadcast messages during the flooding process. This technique significantly reduces the message overhead as associated to a classical flooding apparatus, where every node retransmits each message when it receives the first copy of the message. In OLSR, link state information is caused only by nodes elected as MPRs. Thus, a second optimization is achieved by reducing the number of control messages flooded in the network. This paper presents a cluster based Wormhole attack
prevention technique. The concept of classified clustering with a novel hierarchical 32-bit node addressing scheme is used for eluding the attacking path during the route discovery phase of the OLSR protocol, which is measured as the underlying routing protocol.

References


Index Terms

Computer Science | Networks
Keywords