Abstract

The fast growth in wireless communication and digital electronics has led to the development of low-cost and low-power sensor nodes that are small in size and may communicate over short distances. Sensor nodes are deployed in hostile environment in large number, which makes their physical protection against tampering difficult or more prone to be compromised by an adversary force. By doing that, an adversary can modify the behavior of the compromised nodes and launch routing misbehavior attacks. One most common type of such attacks is gray hole attack. Adhoc On Demand Distance Vector (AODV) in its pure form does not have any mechanism to deal with such type of attack. In this paper, we simulate gray hole attack on AODV routing protocol and evaluate AODV's performance by considering different metrics and scenarios. NS2 simulator has been used to conduct simulation of gray hole attack. Our simulation results show the influence of gray hole attack on the performance of AODV which suffers from decreased delivery ratio and increased packet loss. Furthermore, some countermeasures against gray hole attack are also provided.
References


Index Terms

Computer Science Wireless

Keywords