Attacks against AODV Routing Protocol in Mobile Ad-HocNetworks

A Mobile Ad hoc NETwork (MANET) is much more vulnerable to attack than a wired network due to the dynamic changes of the network topology, high mobility, limited physical security and lack of centralized administration. Unfortunately, the routing protocols are designed based on the assumption that all nodes trust each other and cooperate without maliciously disrupting the operation of routing. This paper analyzes the impact of security attacks on the performance of the AODV routing protocol. Simulations are setup in the NS-2 network simulator and the performance of the AODV routing protocol is discussed under black hole, flooding and rushing attacks. This analysis is provided in terms of performance metrics, such as a packet delivery ratio, the average end-to-end delay and normalized routing load.