Modified AODV Routing Protocol to Improve Security and Performance against Black Hole Attack

A Mobile Ad hoc NETwork (MANET) is a collection of autonomous nodes that have the ability to communicate with each other without having fixed infrastructure or centralized access point such as a base station. This kind of networks is very susceptible to adversary's malicious attacks, due to the dynamic changes of the network topology, trusting the nodes to each other, lack of fixed substructure for the analysis of nodes behaviors and constrained resources. One of these attacks is black hole attack. In this attack, malicious nodes inject fault routing information to the network and lead all data packets toward themselves, then destroy them all. In this paper, we propose a solution, which enhances the security of the Ad-hoc On-demand Distance Vector (AODV) routing protocol to encounter the black hole attacks. Our solution avoids the black hole and the multiple black hole attacks. The simulation results using the Network Simulator NS2 shows that our protocol provides better security and better performance in terms of the packet delivery ratio than the AODV routing protocol in the presence of one or multiple black hole attacks with marginal rise in average end-to-end delay and normalized routing overhead.