Abstract

MANETs are vulnerable to different kinds of attacks due to inherent properties such as wireless medium, dynamic topology, distributed operation and constrained capability. One of the well-known attacks is the Black Hole attack which is most common in the on-demand routing protocols such as AODV. In this paper, we simulate the Black-hole attack in AODV using NS2 Simulator for both SANETS and MANETS by varying node density in the context of responsive and non-responsive traffic. From the simulation results, the impact of Black-hole attack on the performance of AODV QOS metrics i. e. , throughput, packet delivery ratio is less, for end-to-end delay, routing load is high in MANET and SANET under responsive (TCP) and non-responsive traffic (UDP).

References

- Constantine Manikopoulos and Li Ling, "Architecture of the Mobile Adhoc Network Security (MANS) System", CONEX Laboratory, NJWINS Center
Investigating the Impact of Black Hole Attack on AODV Routing Protocol in MANETS under Responsive and Non-Responsive Traffic

- Cryptography and Network Security – William Stallings

Index Terms

Computer Science  Networks

Keywords

MANETs  SANETs  AODV  black hole attack  NS2  throughput
end-to-end-delay
packet delivery ratio
normalized routing load.