Abstract

Mobile ad hoc network is dynamic in nature and vulnerable for several attacks to be arising in it. Mobile nodes frequently disconnect and join the network; they can arbitrarily moves from one place to another. There are several attacks in MANET. One of the attacks is Black hole attack, it is a kind of active attack, it drops the entire incoming packet between one source and destination. Black Hole nodes or Black Holes actually send a fake RREP packet and advertise itself as the shortest route is found. Sender starts transmitting packets to Black Hole, But packet do not reach the destination node on account of this attack and data packets are also lost. In our work we tried to secure the AODV protocol, so that it can withstand the attack by adding an IDS_node to AODV protocol. We have seen that packet drop ratio is decreased by desirable amount. This will help to improve the performance of Mobile Ad hoc network and decrease the Packet loss ratio, which increased due to the attack. There are lots of detection and defense mechanisms to eliminate the intruder that carry out the Black Hole attack. In this paper, we simulated the attack in various wireless ad-hoc network scenarios and have tried to find a response system in simulations.
References

- Marc Greis, "Tutorial for the Network Simulator (NS2)."
- M. A. Shurman, S. M. Yoo, and S. Park, "Black hole attack in wireless ad hoc networks."
- Reena Karandikar, Rashmit Kaur Khanuja, Surendra Shukla "proposed solution to prevent black hole attack in manet" Volume 2, Issue 2 (February 2012) IJRIM.

Index Terms

Computer Science

Network Security

Keywords

Black Hole attack   IDS_Node   AODV   Sequence Number