Examination of AODV Routing Protocol with Wormhole Attack

Volume 135
Number 5

Year of Publication: 2016

Authors:
Gulzar Ahmad Wani, Sanjay Jamwal

Abstract

In Adhoc Network, Mobile Adhoc Network (MANET) is vibrant Adhoc network. MANET is collection of mobile network devices that are connected through wireless medium i.e., radio signals. These mobile network devices form a dynamic topology i.e., mobile nodes move freely and quickly, in and out from network. These is no central control for co-coordinating these network device i.e. decentralized network. These devices control each other directly i.e, peer-to-peer connection. The dynamic nature of MANET makes it vulnerable to variety of security threats like wormhole attack, eavesdropping etc. The performance and reliability of the network is affected by making alteration in routing protocols by the attacker. Wormhole attack is a type of tunneling attack where an attacker at one end of tunnel attracts data packets from one hop neighbors and transmits these data packets to another attacker of the tunnel which delivers these data packets to destination node. Transmitting data packets through tunnel may result various security attacks like wormhole attack, black hole attack, eavesdropping attack. This proposed paper examines the consequences of wormhole attack in AODV routing protocol based MANET using OPNET Simulator.
References


Index Terms
Keywords

MANET, Wormhole Attack, AODV Protocol, Route Request (RREQ), Route Reply (RREP), Broadcast.