Impact of Wormhole Attack Against Routing Protocols on MANETs Performance

Nooriya AL Bulushi

Abstract

Mobile Ad hoc Networks (MANETs) have received growing research interests over the past years due to their numerous useful applications such as emergency situations and military applications. Since nodes communicate with each other without an infrastructure, they provide the connectivity by forwarding packets over themselves. To support this connectivity, nodes use a routing protocol such as Ad-hoc On-Demand Distance Vector (AODV) and Optimized Link State Routing (OLSR).

Due to security vulnerabilities in the routing protocols, wireless ad-hoc networks are unprotected from attacks executed by colluding malicious nodes such as wormhole attack. In a wormhole attack, two colluding malicious nodes could capture packets from one end of the network and send them through a tunnel to be relayed in the other end of the network. This confuses legitimate nodes into sending their packets through the wormhole tunnel. The malicious nodes can then drop or manipulate the packets passing through the wormhole tunnel to their advantage.

The goal of this thesis is to compare the severity of the wormhole attack on MANETs performance when AODV and OLSR are used as routing protocols. We consider both static wormhole attack and mobile wormhole attack. The network simulator NS-3 has been used to evaluate the performance of AODV and OLSR under different scenarios. Our simulation results indicate that OLSR is more robust to wormhole attack compared to AODV. Performance metrics such as packet delivery ratio, normalized routing overhead, and throughput exhibit better values using OLSR than with AODV. On the other hand, our analysis shows that there is no significant difference between the static and mobile wormhole attacks in terms of their impact on MANETs performance.