Weeding Wormhole Attack in MANET Multicast Routing Using Two Novel Techniques - LP3 and NAWA2

Abstract

Mobile Adhoc Network (MANET) with its unique and special characteristics is prone to a host of security threats from within and outside the network. The MANET architecture is well suited
for conducting multicast communications as this greatly reduces the number of multicast packets traversing the network. The replication of multicast packets by the intermediate downstream multicast router is demand based and is determined by the number of fresh receivers in the group. This greatly paves way for network resource optimization and a good trail of performance parameters like MPDR, Throughput, Jitter and End-to-End Delay. It is literally bogging down to construe a localized MANET as a single flat larger group. So the concept of orchestrating hierarchical group architecture within MANET dawned which led to the definition of lulus framework. The hierarchical secure multicast distribution tree created within MANET backed by lulus framework is prone to a array of attacks. One such prominent insider attack is wormhole attack where the two colluding adversaries conspire to short-circuit the flow of packets to a foreign network through an out-of-band high bandwidth link. The implication of this attack in unicast routing of MANET is less pronounced due to the limited number of participating entities. But this attack has a large telling effect on multicast routing as it involves multiple receivers and numerous intermediate multicast routers. The possibility of compromising the internal group node as a wormhole colluding agent is more common in multicast than in unicast. This threat marks an unprecedented intensity by divulging more faction of data thereby rendering the remedial process a huge flop. The real intent of the attacker is not to disrupt the multicast communication but in abetting the mass divulgence of multicast data to unauthorized group members. Two novel solutions viz., Limiting Packet Propagation Parameter (LP3) and Neighbor Aware Wormhole Adversary Axing (NAWA2) has been proposed to counter this menace.

Reference

- Mohapatra, P., Gui, C., and Li, J., “Group Communications in Mobile Ad Hoc Networks”, University of California, Davis.
Routing Protocol resilient to Byzantine Failures”, Dept. of Computer Science, Johns Hopkins University, Baltimore MD 21218 USA.

Index Terms

Computer Science Wireless

Key words

Rushing attack Iolus framework
Multicast communication

RIMR

ROMR