Abstract

Ad hoc networks are vulnerable due to their structure less property. A Mobile Ad-Hoc Network (MANET) is an infrastructure less collection of mobile nodes that can arbitrarily change their geographic locations such that these networks have dynamic topologies and random mobility with constrained resources. They also have capability of network partition. The Wormhole attack
is the most attention seeking attack in ad hoc networks; it consists of two malicious nodes and a tunnel between malicious nodes. In wormhole attack, attacker records the packets at one location and tunnels them in another location in same network or in different network. In this paper, we present a mechanism which is helpful for detection and defend against wormhole attack in ad hoc network is "multipath hop counting analysis" (MHA) in which accepting all route request at destination node with in a fixed time period called time to live (TTL) period and then verification of digital signature of sending node by receiving node because each legitimate node in the network contains the digital signature of every other legitimate nodes of same network. In proposed solution, if sender wants to send the data to destination, firstly it creates a secure path between sender and receiver with the help of multipath hop count analysis with verification of digital signature. If there is presence of any malicious node in between the path then it is identified because malicious node does not have its own legal digital signature.

Reference

Prevention of Wormhole Attack in Ad-Hoc Network


Index Terms

Computer Science Information Technology

Key words

Mobile ad hoc network wormhole attack digital signatures
multipath hop count analysis (MHA)