PREVENTING WORMHOLE ATTACK IN MULTICAST ROUTING PROTOCOLS FOR MANET

MOHANAVEL S, SUNTHARAM A, PRANEV RAM B R & SASHANK S

B.E. Computer Science and Engineering, Sri Venkateswara College of Engineering, Chennai, Tamil Nadu, India

ABSTRACT

Mobile ad hoc networks (MANETs) consist of a collection of wireless mobile nodes which dynamically exchange data among themselves without the reliance on a fixed base station or a wired backbone network. MANET nodes are typically distinguished by their limited power, processing, and memory resources as well as high degree of mobility. Due to the limited transmission range of wireless network nodes, multiple hops are usually needed for a node to exchange information with any other node in the network. Thus secure routing is a crucial issue to the design of a MANET In the field of networking, the specialist area of network security consists of the provisions made in an underlying computer network infrastructure, policies adopted by the network administrator to protect the network and the network-accessible resources from unauthorized access, and consistent and continuous monitoring and measurement of its effectiveness (or lack) combined together. In this paper, we introduce the wormhole attack, a severe attack in ad hoc networks that is particularly challenging to defend against. The wormhole attack is possible even if the attacker has not compromised any hosts and even if all communication provides authenticity and confidentiality. In the wormhole attack, an attacker records packets (or bits) at one location in the network, tunnels them (possibly selectively) to another location, and re-transmits them there into the network. The wormhole attack can form a serious threat in wireless networks, especially against many ad hoc network routing protocols and location-based wireless security systems.

KEYWORDS: Mobile Ad Hoc Networks, Multicasting, Security, Wormhole Attacks, Intrusion Prevention System