ABSTRACT

As demand increases for ubiquitous network facilities, infrastructure-less and self-configuring systems like Mobile Ad hoc Networks (MANET) are gaining popularity. In mobile ad-hoc networks, autonomous nodes form a network without any pre-existing infrastructure. The functionality of these networks heavily depends on so called ad-hoc routing protocols for determining valid routes between nodes. The need for cooperation among nodes to relay each other's packets exposes the nodes in wireless Adhoc network to a wide range of security attacks. A particularly devastating attack is the wormhole attack, where a malicious node records control traffic at one location and tunnels them to another compromised node, possibly far away, which in turn replays them locally. Thus malicious nodes fabricate a false scenario on neighbour relations among mobile nodes. Secure routing in Adhoc networks is often equated with strong and feasible node authentication techniques. Unfortunately, the wormhole attack can hardly be defeated by these techniques, as wormhole attackers do not create extra packets in the network. In this report we propose and implemented an approach to detect the wormhole, based on the fact that transmission time between two fake neighbours created by wormhole is much higher than between two real neighbours which are within radio range of each other. Considering this fact, we have use *HELLO* packets in a unique way to effectively detect the wormhole attack in MANETs and have shown the effectiveness of our approach by simulating in NS-2.

Keywords: Wireless Adhoc networks, Wormhole attacks, AODV.