A number of attacks exist at the network layer, i.e. against routing protocols. One of the most severe attacks is the wormhole attack, which consists of at least two colluding attackers, located
at multi-hops distance, that are connected via some unusual means. The attackers replay messages heard at one side to the other side of the network. When this type of attack remains undetected, nodes have the only ability of communicating with at most two-hops neighbor nodes. The detection mechanisms included cryptographic methods and at times the role of specialized nodes which imply either resource-hungry computations or the battery depletion of certain nodes respectively. In this paper, the study of a scalable geocasting routing protocol reveals the required properties, without any costly attack detection mechanism, that render wormhole attacks trivial in a large ad hoc network.

Reference


Index Terms

Computer Science

Network Security

Key words

Wormhole attack ad hoc

network scalability

gaeocasting

security

routing