Abstract

Recent advances in wireless networks have prompted much research attention in the area of wireless sensor network (WSN). Sensor network consists of hundreds to thousands of low power multifunctioning sensor nodes operating in hostile environment with limited computational and sensing capabilities. These sensor devices are susceptible to various attacks such as selective forwarding or sinkhole attacks when operated in a wireless medium. Reactive routing protocols such as ad-hoc on demand distance vector routing (AODV) of sensor networks have been developed without considering security aspects against these attacks. In this paper, a secure routing protocol named secured ad hoc on demand distance vector routing (S-AODV) is proposed for mobile sensor networks by incorporating trust based mechanism in the existing AODV. Zigbee hardware prototype is also implemented and tested by increasing the sizes of data and distances in indoor and outdoor environment. Simulation results prove that S-AODV outperforms the AODV by reducing the overhead and improving the delivery ratio of the networks.
Reference


Index Terms

Computer Science  Wireless Networks
Key words

Wireless sensor networks
Secured ad-hoc on demand distance vector routing
Sink hole
Route trust
Node trust