Abstract

Wireless Sensor Networks (WSNs) are composed of many sensor nodes and a base station for collecting event information from a wide local area. However, an attacker can easily intrude into a network through external nodes by exploiting characteristics of wireless communication and the limited hardware resources of sensor nodes. Specifically, an attacker can intrude into a sensor network and launch a sinkhole attack in order to capture and redirect event reports of WSNs. Intrusion-tolerant routing for wireless sensor networks (INSENS) has been proposed to prevent sinkhole attacks via intrusion of an external node. INSENS blocks the intrusion of an external node using three symmetric keys to prevent the sinkhole attack. However, even in the presence of INSENS, a sinkhole attack can again be launched by the compromised node because the network does not account for compromised nodes. In this paper, proposed method with three steps involving the interactive authentication method prevent sinkhole attacks by a compromised node. The proposed method detects fake route request messages and drops the compromised node. Proposed method improves the number of the delivered event reports to the base station (BS) by around 65.72% when compared to INSENS. Thus, it improves the...
reliability of the network and reduces the average energy consumption by around 22.32% because it prevents internal sinkhole attacks.

References

13. Index Terms

Computer Science          Networks
Keywords

Wireless sensor networks, Sinkhole attack, Intrusion tolerance, Secure routing, Interactive authentication.