Intrinsic resource constraints and vulnerability to a variety of malicious attacks hinders the widespread deployment of wireless sensor networks (WSNs). One of the malicious attacks is the so-called sinkhole attack where one or more compromised nodes, pretending to be closer to the base station, disseminates a false advertisement. The event reporting nodes start forwarding their reports to these compromised nodes. These compromised nodes can take control of the network traffic, eavesdrop on real communication, and forge reports that are then forwarded to the base-station. In the localized encryption and authentication protocol (LEAP) key management protocol, compromised nodes can expose the keys to the adversary. Therefore, it is crucial to detect and evict compromised nodes instead of using a key sharing approach. In this paper, a fuzzy logic system-based method to detect the compromised nodes and to prevent sinkhole attacks is proposed. Proposed method use neighbor information (i.e., number of common neighbors and their parent node information) to detect compromised nodes. Experimental results demonstrate the validity of the proposed approach in that it provides maintained safeguards and reduces communication cost.
References


Index Terms

Computer Science Security
Keywords

Wireless sensor network, Sinkhole attack, Fuzzy logic, Genetic algorithm.