Abstract

Cooperative communication is a technique that helps to improve the communication performance in wireless networks. It allows the nodes to rely on their neighbors when transmitting packets providing some diversity gain. Wireless sensor networks (WSNs) can benefit from cooperative communication to, which was proven by other researcher in the field. In this paper we consider security issues in WSNs with cooperative communications. We study such issues at each of the main protocol layers: physical layer, data link layer, network layer, services (topology) layer, and application layer. For each layer, we clarify the main task, enumerate the main attacks and threats, specify the primary security approaches and techniques, if any, and discuss possible new attacks and problems that may arise with the use of cooperative communications. Further, we showed for some attacks (e.g. jamming, packet dropping, and wormhole) that using cooperative communication improves the network resiliency and reliability. This paper builds the foundations and clarifies the specifications for a needed security protocol in WSNs with cooperative communications that can enhance its performance and resiliency against cyber-attacks.