Development of the Hierarchal Trust Management System for Mobile Cluster-based Wireless Sensor Network

Submitted by grigby1 on Tue, 09/05/2017 - 1:49pm

Abstract

In this paper a model of secure wireless sensor network (WSN) was developed. This model is able to defend against most of known network attacks and don't significantly reduce the energy power of sensor nodes (SN). We propose clustering as a way of network organization, which allows reducing energy consumption. Network protection is based on the trust level calculation and the establishment of trusted relationships between trusted nodes. The primary purpose of the hierarchical trust management system (HTMS) is to protect the WSN from malicious actions of an attacker. The developed system should combine the properties of energy efficiency and reliability. To achieve this goal the following tasks are performed: detection of illegal actions of an intruder; blocking of malicious nodes; avoiding of malicious attacks; determining the authenticity of nodes; the establishment of trusted connections between authentic nodes; detection of defective nodes and the blocking of their work. The HTMS operation based on the use of Bayes' theorem and calculation of direct and centralized trust values.