Abstract

A Wireless Sensor Network (WSN) is a network made up of a set of sensor nodes and gateway nodes where sensor nodes monitor physical parameters such as temperature, moisture etc. and send it to gateway nodes. Security in WSN plays an important aspect since it provides sustainability to the network. Security threats can be introduced in WSN through various means, where the ongoing data transmissions can be tampered with or the nodes can be altered to behave in an unpredictable manner. The proposed research work uses biological inspirations and takes aspects from machine learning and social psychology for improving security in WSNs. The proposed work is a two-step model, where the detection of fraudulent nodes is the first step and reducing the effect of these nodes using bio-inspirations is the second step. For detection of fraudulent nodes, two approaches based on machine learning and social psychology has been proposed. The machine learning model is based on techniques like k-means and Support Vector Machine. Sociopsychological model is another model which is less complex to deal with fraudulent node detection. It enhances the performance by taking concepts from social psychology. After the detection of the fraudulent nodes, an immune model is instantiated. Biological immune systems have intelligent capabilities of detecting foreign bodies which attack our body. Moreover they have inherent insightful capabilities to remember the same foreign body when it hits the body again. In this work, a similar healing procedure is instigated in WSN to quickly recover from the attack. The proposed work has been implemented in LabVIEW platform and extensive simulations were carried out to study its performance for the metrics such as detection and recovery time, reliability, robustness, scalability, complexity etc. Further, it is experimentally evaluated on hardware test bed of size 16 nodes to obtain results that demonstrate the accuracy and robustness of the proposed model.

...