Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 65 (2015) 25 – 34

Procedia Computer Science

International Conference on Communication, Management and Information Technology (ICCMIT 2015)

A Novel Multi-Threshold Energy (MTE) Technique for Wireless Sensor Networks

Hosam Rahhala[a] and Rabie A. Ramadan[a]

[a]*Cairo University, Cairo , Egypt*

Abstract

Trust and energy consumption are challenging issues in WSNs. In earlier work, we proposed Trust-Based Cross-Layer Model (TCLM), which uses the direct and indirect observation of the nodes to compute the trust values and ACKs from data link layer and TCP layer are considered to update these values**.** In this paper, we introduce new scheme that consider the limited amount of energy for each sensor, and use multi levels for the remaining energy of the nodes and the degree of the priority which can be given to some of the packets. Also, we apply our proposed technique to TCLM to make it more efficient, called A Trust-Based Cross-Layer Energy-Aware Model. We present simulation results that demonstrate the effectiveness of the proposed scheme in both static WSNs. The new proposed model improves the performance of our earlier work by increasing the malicious detection ratio and decreasing the energy consumption.

Peer-review under responsibility of Universal Society for Applied Research

Keywords: WSNs , milicious node detection, effeceint routing, energy consumption

1. Introduction

Over the last decade a tremendous progress in the field of Wireless Sensor Networks (WSNs) has been achieved making it one of the most promising research areas. In these networks, low-cost wireless sensors equipped with a radio transceiver and set of transducers through which they interact with the surrounding environment, organize themselves in ad hoc multi-hop network, providing the ability to communicate with other network nodes and usually a central collection point, called the sink node. A user can receive and process the data sensed by the network through

Peer-review under responsibility of Universal Society for Applied Research
doi:10.1016/j.procs.2015.09.072

the sink node and additionally inject commands into the sensor network to adjust data collection and network related parameters. Users do not want to reveal their data to unauthorized people as the disclosed information could be used for malicious purposes. This concern is even more relevant to wireless environments where anyone can overhear a message sent over the radio. Therefore, even a very useful and convenient system might not be appealing to the users if it is not secure. Therefore, a smart trust management scheme is needed to identify trustworthiness of sensor nodes in order to distinguish between malicious nodes and good nodes, and to strengthen reliable nodes and weaken suspicious nodes. Trust is currently a hot issue in computer networks which can solve security problems caused by malicious members, so building trust relationships among sensor nodes has been recognized as a novel approach to improve security in WSNs.

For that, in our earlier work[1], we proposed a trust model for Wireless Sensor Networks based on cross-layer idea called A Trust-Based Cross-Layer Model (TCLM) for Wireless Sensor Networks, which uses the direct and indirect observation of the nodes to compute the trust values and ACKs from data link layer and TCP layer are considered to update these values to make the network-layer decision more accurate. On the other hand, battery powered sensor nodes are equipped with very limited energy resource. That makes the reserving of energy in WSNs as one of the most challenging issues for design consideration, which means that the selection of sensor nodes for participating any task should be conducted carefully, in order to prolong the lifetime of WSNs. In addition, if an inappropriate node was chosen, and it has no capability to accomplish the task or cannot complete the task with an acceptable result, the WSN might be ultimately leaded to serious system performance degradation. In addition, by selecting the appropriate sensor node during the cooperation process, the entire system stability of WSNs can be improved. Thus, how to choose one or several suitable nodes as the cooperation partners for any node is one of the most important issues in a WSN. Consequently, in this paper we are going to develop our earlier work by considering the energy consumption in the new proposed model to permit the sensor node to use information on its energy status to adjust its participation in the network. For instance, we suggest adding energy –aware technique allowing every sensor to work in normal , selfish, or sleep mode by using multi thresholds for the residual energy of the nodes and the degree of the priority which can give to some of the packets.

The rest of the paper is organized as follows: related work is summarized in section 2. The description of our proposed Technique is given in section 3. Simulation results are shown in section 4, followed by conclusions in section 5.

2. Related Work

Since sensor nodes have limited resources, in particular battery power, accordingly, the energy consumed by sensor nodes is a factor of paramount importance in WSNs as these networks are designed for many years of unattended operation in harsh environments where infeasible. Improper energy handling will lead to disappearing nodes, network partition andfinally inability to monit or reliably the area of interest[2]. In recent time the issue of energy in wireless Sensor networks has been addressed in several works. The authors in[3] have proposed simplest form of energy-aware algorithm in which nodes enter a sleep state when their stored energy drops below a threshold value and wakeup again when they have been recharged sufficiently by the solar cell. D. Hui-hui et al.[4], have proposed a multi-angle trust mechanism for nodes in Wireless Sensor Networks which adding the sensing data and the node's energy in the factors of trust assessment in addition to communication , and new trust models to calculate the trust values of communication trust, the sensed data and the node's energy.

M. Pushpalatha et al.[5] have proposed a trust- based-energy- aware routing model in MANET. During route discovery, node with more trust and maximum energy capacity is selected as a router based on a parameter called 'Reliability'. Route request from the source is accepted by a node only if its reliability is high. Otherwise, the route request is discarded. In [6],the authors have proposed a secure routing protocol (Ambient Trust Sensor Routing, ATSR) which adopts the geographical routing principle to cope with the network dimensions and relies on a distributed trust model that takes into account the energy of each neighbour. The authors in [7], have proposed a trust mechanism of the human humanity into a WSN and propose a novel power-aware and reliable scheme (PRS) for sensor selection. Based on the PRS, they propose a reliable sensor selection algorithm with power-aware for WSNs. The proposed algorithm not only considers the multi-attribute value of the target node based on its cooperation records among the nodes, but also uses the integrated trust value of the third-party nodes. In[8,] the authors proposed an energy efficient selection of