Int. J. Electron. Commun. (AEÜ) 70 (2016) 40–49

Contents lists available at ScienceDirect

International Journal of Electronics and Communications (AEÜ)

journal homepage: www.elsevier.com/locate/aeue

A fuzzy fully distributed trust management system in wireless sensor networks

Hossein Jadidoleslamy [a,*], Mohammad Reza Aref [b], Hossein Bahramgiri [a]

[a] Department of Information Technology, Communications and Security, Malek-Ashtar University of Technology (MUT), Tehran, Iran
[b] Department of Electrical Engineering, Sharif University of Technology, Tehran, Iran

ARTICLE INFO

Article history:
Received 26 April 2015
Accepted 27 September 2015

Keywords:
Wireless sensor network (WSN)
Network security
Trust management system (TMS)
Trustworthiness calculation or forecast
Fuzzy distributed trust management system

ABSTRACT

Wireless sensor networks (WSNs) usually consist of many tiny sensor nodes and a Sink. Problems like nodes' misbehavior due to malicious, compromised or selfishness intentions, and WSNs' security vulnerabilities against different attacks due to free and unprotected communications, untrusted and broadcasted transmissions, hostile environments and limited resources, degrade the security and overall performance of WSNs. In another direction, most of the traditional security mechanisms are unsuitable for WSNs. One significant security solution against these problems is Trust Management System (TMS); TMS enhances the security by detecting the nodes' abnormal behaviors; it improves the cooperation between nodes and increases the network performance. But, existing Trust Management Systems (TMSs) have weaknesses such as high overhead and computational complexity, resources' severe consumed and inconsistency with the especial characteristics of WSNs like limited resources, high density, dynamic topology and nodes' mobility. As a result, this paper proposes a fuzzy fully distributed TMS for WSNs, called DTMS. It is different from other existing TMSs in terms of the fuzzy-nature trust calculation criteria, trust calculation procedure and trust forecasting capability. Finally, the performance of DTMS is compared with the performance of PowerTrust and RFSN TMSs; results of simulations and statistical analyses indicate that DTMS is improved in terms of energy consumption, accuracy, scalability and fault tolerance, and execution speed.

1. Introduction

Wireless sensor networks (WSNs) are homogeneous or heterogeneous systems, which usually consist of many tiny sensor nodes and a Sink. Fig. 1 represents different properties of WSNs [1–3].

Sensor nodes must cooperate to achieve higher performance, but nodes' misbehavior due to malicious, compromised or selfishness intentions, and WSNs' security vulnerability against different attacks due to free and unprotected communication channel, untrusted and broadcasted transmissions, hostile environments and limited resources, significantly degrade the security and overall performance of these networks [3–6]. So, security is a vital and complex requirement for WSNs, which should be attended when designing step. Security is usually established through cryptography-based techniques; but they cannot establish a comprehensive security framework for WSNs; due to they cannot prevent from internal attacks and selfishness behaviors; also, they are expensive and inconsistent with the especial characteristics and severe constraints of WSNs. So, most of the traditional security mechanisms are impractical in WSNs and it is necessary to design adaptive security mechanisms for these networks. One significant security solution against the aforementioned problems is trust management system (TMS); Fig. 2 shows different properties of trust management systems (TMSs). Trust is a context-dependent, dynamic and complex concept in WSNs. TMSs calculate the trust values of nodes, detect the malicious, compromised or selfish nodes and then, block or remove them from the network's processes [5–7]. TMSs are powerful tools for improving the cooperation between nodes, increasing the network performance and enhancing the security by detecting the untrustworthy nodes [4,8–10]. But, existing TMSs have weaknesses such as high overhead and computational complexity, resources' severe consumed and inconsistency with especial characteristics of WSNs likes resources' severe constraints, high density, dynamic topology and nodes' mobility.

As a result, this paper proposes a fuzzy fully distributed TMS for WSNs, called DTMS. The main steps of DTMS are presented in Fig. 3.

In DTMS, the trust establishment functionality is uniformly distributed all over the network; so there are no single points of

* Corresponding author. Tel.: +98 9155499109; fax: +98 5433221262.
E-mail addresses: Tanha.hossein@gmail.com (H. Jadidoleslamy), Aref@sharif.edu (M.R. Aref), Bahramgiri@mut.ac.ir (H. Bahramgiri).

http://dx.doi.org/10.1016/j.aeue.2015.09.017
1434-8411/

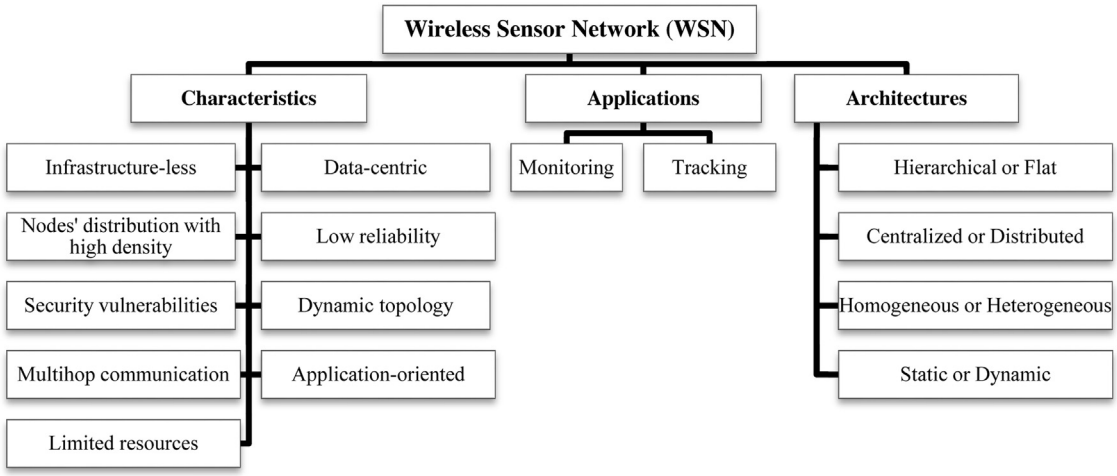

Fig. 1. Different characteristics, applications and architectures of WSNs.

failure in the network. DTMS combines direct trust and indirect trust together; also, it combines past misbehavior with the current status in a comprehensive way to obtain the robust trust values. In DTMS, each node monitors the behaviors of its neighbors; then, it calculates their trustworthiness based on the collected measurements and its observations; finally, it detects the untrustworthy neighbors and removes them from the network's processes. DTMS also can forecast the trust values of nodes; i.e., each node can forecast the trust values of its neighbors based on their previous trust values. It considers fuzzy-nature and multidimensional trust criteria, which is derived from communication and social networks to evaluate the trustworthiness of nodes. DTMS is different from other existing TMSs in terms of the fuzzy-nature trust calculation criteria, trust calculation procedure and trust forecasting capability.

Finally, the performance of DTMS is compared with the performance of PowerTrust and RFSN TMSs; results of simulations (by TRMSim-WSN simulator) and statistical analyses (by Expert Choice and Grey Relationship Analysis tools) indicate that DTMS is improved in terms of energy consumption (vs. remainder energy), accuracy (vs. error rate), scalability and fault tolerance, and execution speed (vs. computational complexity and processing overhead).

The rest of this paper is organized as follows: Section 2 expresses the related work; it briefly reviews some of the popular TMSs in WSNs and MANETs; Section 3 describes the different steps of DTMS, in details; Section 4 evaluates the performance of DTMS and compares it with the performance of PowerTrust and RFSN TMSs; it presents and discusses the reached results of simulations and

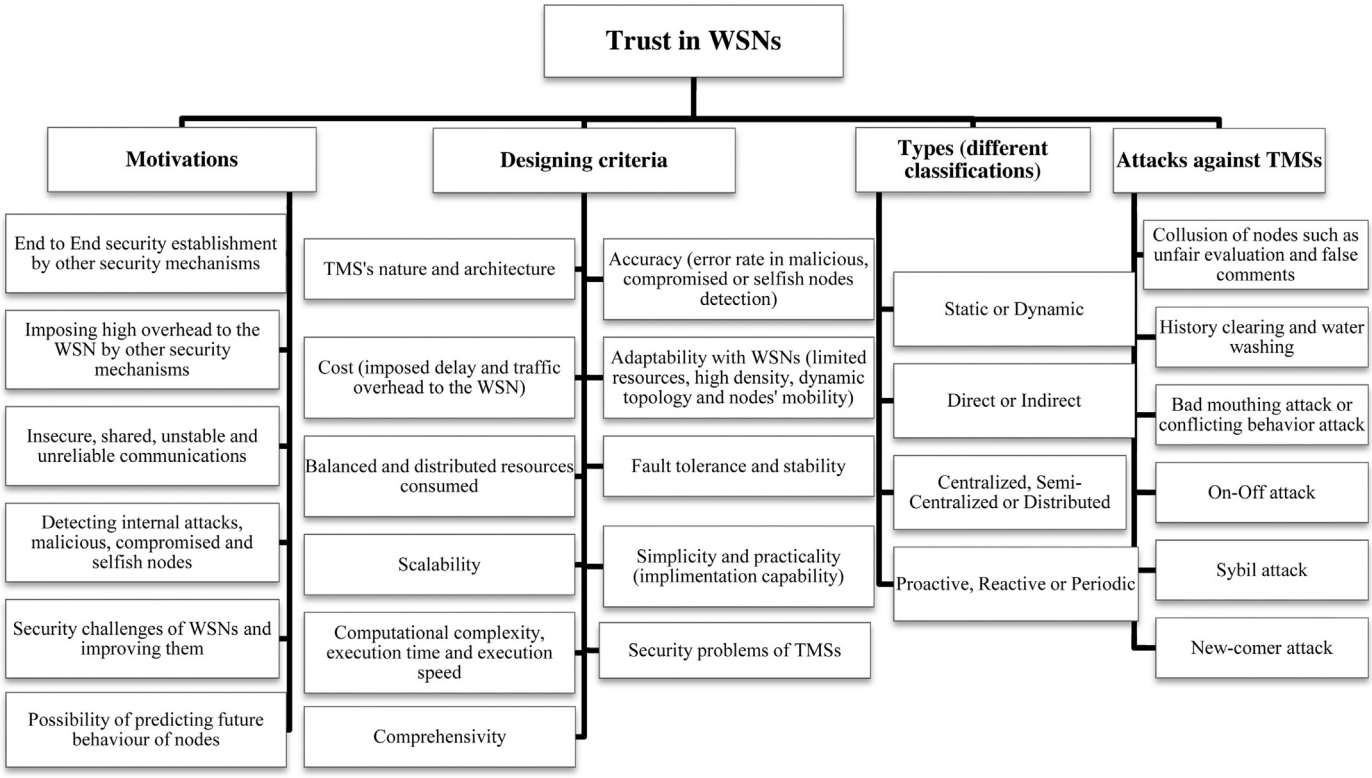

Fig. 2. Trust in WSNs: motivations of using TMSs in WSNs, significant criteria in designing TMSs for WSNs, different classifications of TMSs and existing attacks against TMSs.