Computer Networks 72 (2014) 45–61

Contents lists available at ScienceDirect

Computer Networks

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

A novel multiple-level trust management framework for wireless sensor networks

Bo Zhang [a,*], Zhenhua Huang [b], Yang Xiang [b]

[a] College of Information, Mechanical and Electrical Engineering, Shanghai Normal University, Shanghai, PR China
[b] College of Electronics and Information Engineering, Tongji University, 201804 Shanghai, PR China

ARTICLE INFO

Article history:
Received 7 February 2013
Received in revised form 20 May 2014
Accepted 19 June 2014
Available online 24 July 2014

Keywords:
Wireless sensor networks
Multiple-level trust management framework
Belief
Reputation
Recommended trust

ABSTRACT

The distributed deployment nature of wireless sensor networks (WSNs) poses a challenge to the security of node cooperation in them as it is difficult for WSN to ensure that all nodes can recognise a huge number of other individual nodes and select appropriate and trustworthy nodes for cooperation. Node cooperation may therefore be launched in an unreliable environment and might be vulnerable to attacks. Consequently, the security of nodes is of paramount importance for the proper operation of WSNs. The distributed trust management scheme is a feasible solution. With a view to making improvement on the existing trust management mechanisms, we in this paper propose ML-TRUST, a multiple-level trust management framework for trust management in WSN in which three levels of trust are used to establish trustworthy relationships among nodes for their cooperation, namely, (1) a subjective trust, which is defined as belief and is proposed with respect to three aspects: past judgements, witness evidence, and capacity evaluation; (2) an objective trust, which is defined as reputation and is proposed with two factors, number of functioning communities and weighted judgements by rating nodes' reputations, being introduced in reputation rating, and with several rules and fraud factor tests being given to prevent reputation rating from malicious attacks, and (3) the recommended trust method, which is proposed to obtain trustable impressions from strange recommendations with, in connection, several consistency factors being presented to determine the trustworthiness of a recommendation. Besides using a set of lemmas and theorems to back up our ML-TRUST framework, we also list the results of a series of simulation tests to further verify the performance of our mechanism.

1. Introduction

Wireless sensor networks (WSNs) have been garnering increased attention in recent years for both industrial and consumer related activities, such as area, healthcare, and industrial monitoring [1,2,5]. WSNs comprise numerous tiny and cheap nodes that cooperate to achieve complicated application requirements. In contrast to node cooperation in wired network environments (such as the Internet and intranets), node cooperation in WSNs faces certain limitations because the nodes are unreliable devices with various resource constraints, limited access, and security concerns. Because WSNs do not possess centralised management centres to monitor and control risks, their nodes are deployed in an unattended manner and are vulnerable to threats and attacks. Further, weakness and malicious actions from unreliable nodes can endanger cooperation and the ability of a WSN to achieve its goals. Consequently, for proper operation, the security of nodes

[*] Corresponding author.
E-mail address: sh.zhangbo@gmail.com (B. Zhang).

http://dx.doi.org/10.1016/j.comnet.2014.06.015
1389-1286/© 2014 Elsevier B.V. All rights reserved.

in WSNs is of paramount importance. However, the WSN security research field is still in the nascent stage. This paper considers how secure node cooperation can be achieved in order to facilitate efficient large-scale application of WSNs.

In an open and dynamic environment, it is impossible for a node to recognise thousands of other individual nodes and to select appropriate nodes for cooperation. As a consequence, nodes are selected without any objective and creditable standards of measurement, which causes unreliability in WSNs. Trust has recently been suggested as an effective security mechanism to improve reliability and to mitigate attacks within networked environments [2,19,20]. Using this mechanism, node selection decisions can be made in accordance with trust evaluations conducted via subjective and/or objective impressions, i.e., belief and/or reputation. Research has demonstrated that rating node trust and reputation can effectively improve security and promote mutually beneficial node cooperation in WSNs [3,6–10].

Traditionally, trust establishment mechanisms have focused on providing trust relationships among nodes, rating the reputation of nodes, and managing trust among nodes [11]. However, such mechanisms are not efficient because WSNs comprise a large number of sensor nodes with limited communications and unfamiliar relationships. It is therefore impossible for a node to be familiar with all other individual nodes. Consequently, WSNs must utilise strange nodes and ensure cooperation based on the most competent nodes. Moreover, WSNs are deployed in open, unsupervised, and insecure environments that are prone to increased risks of unsuccessful cooperation. In addition, the absence of any centralised authority in WSNs results in difficulties with respect to accurate monitoring of the reputation of individual nodes. Further, nodes can act maliciously and demonstrate detrimental behaviours, such as recommending unqualified nodes for critical functions. Building cooperative relationships therefore depends on the trust relationships between nodes; otherwise, reputation is not a viable solution because evaluating trust relationships between every two nodes or scanning reputation would lead to substantial network flooding costs from request messages [2].

In this paper, we propose a multiple-level trust management framework for WSNs that calculates and manages trust from a more comprehensive perspective. Our objective is to provide a comprehensive trust management scheme that not only promotes efficient, accurate, and robust trust management, but also takes WSN features and limitations into account. We consider that collaborative node functioning in WSNs depends on the following factors: belief in each other (including past judgements, witness evidence, and confidence in capacity), and reputation and creditable recommendation between two strange nodes. Consequently, we propose an ML-TRUST management framework that provides three types of trust evaluations comprising the following factors: subjective trust evaluation between every pair of nodes, an objective trust aggregation rating for nodes, and a recommended trust computation for nodes to obtain reliable recognition of strange nodes. Further, we suggest various means by which trust management can be shielded from malicious attacks.

Compared with other trust management methods, our ML-TRUST framework offers the following: (1) Three kinds of trust management mechanisms for each node: belief, reputation, and recommended trust. Compared with conventional trust management methods, which provide limited trust aspects such as trust relationship, reputation, and recommendation (at most two), our framework enables each node to measure most other nodes' trustworthiness (belief for direct-interacted nodes, reputation for overall trustworthiness, and recommended trust for any strange nodes) in a multi-level manner. Further, because we design distributed and local past data lists for each node in ML-TRUST, no substantial computation for trust is needed. (2) In contrast to trust computation schemes that only utilise the sum/average of past judgements or feedbacks, this paper addresses subjective trust, which is defined as belief with respect to three aspects: past judgements, witness evidence, and capacity evaluation. In our proposed framework, belief can provide functioning effects (past judgements), third-party impression evaluation (witness evidence), and performance forecasting (capacity evaluation) to build a comprehensive trust relationship between two nodes. (3) Reputation is defined as a shareable comprehensive objective trust between nodes within a functioning community. Two factors, number of functioning communities and weighted judgements by rating nodes' reputations, are introduced in reputation rating. Because it is possible for nodes to function in various communities with different identities, the number of functioning communities is also introduced into the reputation rating to adjust the reputation value of nodes in two or more communities. In addition, we address several rules and fraud factor tests, which have not been considered in other research efforts, to prevent reputation rating from malicious attacks. (4) The recommended trust method is proposed for nodes to obtain trustable impressions with respect to strange nodes that are identified from recommendation route composition. In this scenario, we present several consistency factors to evaluate whether a recommendation is trustworthy and to combat potential attacks that occur frequently and are paid less attention in many WSN recommendation management research efforts. (5) Lemmas and theorems are presented to prove the correctness of our proposed mechanism.

The remainder of the paper is organised as follows. Section 2 gives a brief description of the typical related studies concerning trust management with respect to WSNs. Sections 3–5 addresses the computation of subjective trust, which is termed belief in this paper, from three aspects: past judgment, witness evidence and capacity; the computation of reputation rating, the rules of fraud prevention and tests for evaluating fraud attacks, and the recommended trust computation method for nodes based on recommendation route composition and the evaluation for trustworthy degrees of recommendation respectively. Section 6 presents proof of correctness for our trust management framework. Section 7 lists the results of a set of simulations and analysis. Section 8 is the paper's conclusions.