Ad Hoc Networks 33 (2015) 154–167

Contents lists available at ScienceDirect

Ad Hoc Networks

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

Hierarchical trust management of community of interest groups in mobile ad hoc networks

Ing-Ray Chen *, Jia Guo

Department of Computer Science, Virginia Tech, United States

ARTICLE INFO

Article history:
Received 26 March 2014
Received in revised form 2 January 2015
Accepted 5 May 2015
Available online 14 May 2015

Keywords:
Hierarchical trust management
Community of interest groups
Intrusion detection

ABSTRACT

In mission-critical applications deployed in mobile ad hoc networks, very frequently a commander will need to assemble and dynamically manage Community of Interest (COI) mobile groups to achieve the mission assigned despite failure, disconnection or compromise of COI members. In this paper, we present a *dynamic hierarchical trust management* protocol that can learn from past experiences and adapt to changing environment conditions (e.g., increasing misbehaving node population, evolving hostility and node density, etc.) to enhance agility and maximize application performance. With trust-based misbehaving node detection as an application, we demonstrate how our proposed COI trust management protocol is resilient to node failure, disconnection and capture events, and can help maximize application performance in terms of minimizing false negatives and positives in the presence of mobile nodes exhibiting vastly distinct QoS and social behaviors.

1. Introduction

In military operation or emergency response situations, very frequently a commander will need to assemble and dynamically manage *Community of Interest* (COI) mobile groups to achieve a critical mission assigned despite failure, disconnection or compromise of COI members. COI-HM [8,12] was proposed to achieve scalability and reconfigurability following the command chain of commander → leader → COI members. Under COI-HM, a COI is divided into multiple subtask groups to accomplish a mission. Each subtask group would be governed by a subtask group leader (SGL) dynamically appointed by the COI commander responsible for relaying commands from the commander to the COI group members in the subtask group, and filtering messages sent by COI members in the same subtask group to COI members located in other subtask groups. COI members in one subtask group may be reassigned to another subtask group for tactical reasons, thus triggering registration/deregistration actions to the subtask group leaders to maintain the hierarchical structure.

This hierarchical management structure is generic and can be applied to various mission scenarios. Subtask groups may be physically co-located or separated. A node may be assigned to one or more subtasks, depending on node properties (e.g., manned or unmanned) and subtask group characteristics (functionality, difficulty, urgency, importance, risk, size, and composition). Thus, a node's mobility model reflects its assignment, de-assignment or reassignment to subtask groups, as well as its mobility pattern moving around the subtask groups it is assigned to. In military applications, very frequently a COI consists of heterogeneous nodes with vastly different levels of functionality, capacity and resources. A SGL is presumably a higher-capacity node and would be assigned, de-assigned, or reassigned dynamically by the COI-commander to lead a subtask group.

* Corresponding author.
E-mail addresses: irchen@vt.edu (I.-R. Chen), jiaguo@vt.edu (J. Guo).

http://dx.doi.org/10.1016/j.adhoc.2015.05.004
1570-8705/© 2015 Elsevier B.V. All rights reserved.

Despite providing scalability and reconfigurability, COI-HM does not provide tolerance against node compromises and collusion as there is no mechanism to defend against inside attackers or malicious nodes. Existing intrusion detection system (IDS) techniques based on anomaly or pattern-based detection are either centralized (especially for wired networks) which creates a single point of failure, or too complex for distributed execution in heterogeneous mobile networks at runtime.

In this paper, we propose COI *dynamic hierarchical trust management* (COI-HiTrust) for intrusion tolerance and survivability. COI-HiTrust runs on top of COI-HM, so it can achieve scalability and reconfigurability since nodes will only interact with peers in the same subtask group and do not assess trust about every node in the network. In addition as we will demonstrate later, it also achieves trust resiliency and accuracy against inside attackers or malicious nodes.

In the literature there is a large body of trust management protocols for MANETs [1,9,10,11,16,17,20,23,27,36–40]. However, there is very little research on hierarchically structured trust management protocol design for MANETs. Verma et al. [16] and Davis [17] considered hierarchical trust management for MANETs. However, their schemes heavily rely on the certificates issued off-line or by trusted third parties which typically are not available in MANET environments. Bao et al. [14,24] and Li et al. [19] considered hierarchical trust management in wireless sensor networks without considering node mobility. Zhang et al. [25] proposed a hierarchical trust architecture for wireless sensor networks and considered the dynamic aspect of trust by introducing a trust varying function. However, their work is theoretical in nature without addressing what trust attributes should be used (a trust composition issue), how trust is aggregated accurately (a trust aggregation issue), or what weights should be put on trust attributes to form trust (a trust formation issue). On the contrary, our work addresses all three aspects of trust management. Moreover, we propose the concept of dynamic hierarchical trust management by which trust protocol parameter settings can be dynamically adjusted in response to changing environments to minimize trust bias and maximize application performance.

We envision the following original contributions from this work:

1. Unlike most existing reputation and trust management schemes for mobile ad hoc networks in the literature [10], we consider not only traditional "*QoS trust*" derived from communication networks, but also "*social trust*" derived from social networks [2,3] to obtain a composite trust metric as a basis for evaluating trust of mobile nodes in COI applications. Moreover, we are the first to propose the new design notion of *mission-dependent trust formation* with the goal to enhance mission agility and maximize mission survivability despite the presence of malicious, erroneous, partly trusted, uncertain and incomplete information.
2. We design and validate COI-HiTrust as a *dynamic hierarchical trust management* protocol that can learn from past experiences and adapt to changing environment conditions (e.g., increasing or decreasing hostility, increasing misbehaving node population, etc.) to maximize application performance and enhance operation agility. This is achieved by addressing critical issues of hierarchical trust management for COI applications, namely, trust composition, aggregation, propagation, and formation. The learning process and adaptive designs of COI-HiTrust are reflected in trust aggregation, trust propagation and trust formulation. For trust composition, aggregation and propagation, we first explore novel social and QoS trust components and then devise trust aggregation and propagation protocols (for trust data collection, quality-of-information dissemination and analysis) for peer-to-peer subjective trust evaluation of *individual* social and QoS trust components, and prove the accuracy by means of theoretical analysis with simulation validation. The weights to direct trust and indirect trust are dynamically adjusted based on environment conditions to minimize trust bias. For trust formation, we explore a new design concept of *mission-dependent trust formation* allowing trust being formed out of social and QoS trust components to maximize application performance. We use a *misbehaving node detection* application as an example to illustrate the design concept. Dynamic trust management (to be discussed in more detail in Section 7) is achieved by first determining the best trust formation model given a set of model parameters specifying the environment conditions (e.g., percentage of malicious nodes), and then at runtime COI-HiTrust learns and adapts to changing environment conditions by using the best trust formation model identified from static analysis.
3. To achieve the goals of identifying the best trust composition and trust formation for mission-oriented COI mobile group applications, we develop a novel model-based analysis methodology for analyzing and validating COI-HiTrust. The novelty lies in the new design notion of *objective trust* derived from global knowledge or *ground truth* derived from the mathematical model describing a COI against which *subjective trust* obtained as a result of executing COI-HiTrust may be compared and validated.

This paper substantially extends from [41] by adding simulation validation using ns-3 (Section 5) as well as new materials, including a theoretical analysis of the protocol's convergence, accuracy and resiliency properties (Section 4), a sensitivity analysis of the effect of trust formation on application performance (Section 6), and a discussion on applicability (Section 7). The rest of the paper is organized as follows. Section 2 describes the system model and COI Architecture. Section 3 describes COI-HiTrust and explains the hierarchical trust protocol design for managing COI groups in MANETs. Section 4 conducts a theoretical analysis of the convergence, accuracy and resiliency properties of COI-HiTrust. Section 5 develops a novel model-based approach to describe dynamic behaviors of nodes in MANETs in the presence of misbehaving nodes with the objective to yield objective trust against which subjective trust from executing COI-HiTrust may be compared for trust bias minimization.