Ad Hoc Networks 19 (2014) 59–74

Contents lists available at ScienceDirect

Ad Hoc Networks

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

Trust management in mobile ad hoc networks for bias minimization and application performance maximization

Ing-Ray Chen [a,*], Jia Guo [a], Fenye Bao [a], Jin-Hee Cho [b]

[a] Department of Computer Science, Virginia Tech, United States
[b] Computational and Information Sciences Directorate, U.S. Army Research Laboratory, United States

ARTICLE INFO

Article history:
Received 19 August 2013
Received in revised form 21 January 2014
Accepted 17 February 2014
Available online 26 February 2014

Keywords:
Trust management
Mobile ad hoc networks
Trust bias minimization
Model-based analysis
Application-level trust optimization
Reliability assessment

ABSTRACT

Trust management for mobile ad hoc networks (MANETs) has emerged as an active research area as evidenced by the proliferation of trust/reputation protocols to support mobile group based applications in recent years. In this paper we address the performance issue of trust management protocol design for MANETs in two important areas: trust bias minimization and application performance maximization. By means of a novel model-based approach to model the ground truth status of mobile nodes in MANETs as the basis for design validation, we identify and validate the best trust protocol settings under which trust bias is minimized and application performance is maximized. We demonstrate the effectiveness of our approach with an integrated social and quality-of-service (QoS) trust protocol (called SQTrust) with which we identify the best trust aggregation setting under which trust bias is minimized despite the presence of malicious nodes performing slandering attacks. Furthermore, using a mission-oriented mobile group utilizing SQTrust, we identity the best trust formation protocol setting under which the application performance in terms of the system reliability of the mission-oriented mobile group is maximized.

© 2014 Elsevier B.V. All rights reserved.

1. Introduction

The concept of "trust" originally derives from social sciences and is defined as the subjective degree of a belief about the behaviors of a particular entity. Blaze et al. [7] first introduced the term "Trust Management" and identified it as a separate component of security services in networks and clarified that "Trust management provides a unified approach for specifying and interpreting security policies, credentials, and relationships." Many researchers in the networking and communication field have defined trust differently such as "a belief on reliability, dependability, or security" [24], "a belief about competence or honesty in a specific context" [3], and "reliability, timeliness, and integrity of message delivery" [25]. Trust management is often used with different purposes in diverse decision making situations such as secure routing [5,31,34,37], key management [9,18], authentication [29], access control [1], and intrusion detection [2,20,23,38,49].

Trust management for mobile ad hoc networks (MANETs) (see [10,48] for a very recent survey of the topic) has emerged as an active research area as evidenced by the proliferation of trust/reputation protocols [2,3,5,6,8–10,14–16,18,19,25–27,29,31,34,35,40,48,50,57–63,72,76,77] to support mobile group based applications in recent years. Untreated in the literature [10,48], in this paper we address the performance issue of trust management protocol design for MANETs in two important areas: trust bias minimization and application performance maximization.

* Corresponding author. Address: Department of Computer Science, Virginia Tech, 7054 Haycock Road, Falls Church, VA 22043, United States. Tel.: +1 (703) 538 8376; fax: +1 (703) 538 8348.
E-mail addresses: irchen@vt.edu (I.-R. Chen), jiaguo@vt.edu (J. Guo), baofenye@vt.edu (F. Bao), jinhee.cho@us.army.mil (J.-H. Cho).

http://dx.doi.org/10.1016/j.adhoc.2014.02.005
1570-8705/© 2014 Elsevier B.V. All rights reserved.

Relative to existing works for MANET trust management cited above, this paper has the following specific contributions:

- First, we develop a new trust management protocol (SQTrust) based on a composite social and QoS trust metric, with the goal to yield peer-to-peer *subjective trust evaluation*. A mobile ad hoc group very frequently comprises human operators carrying communication devices. Thus, in addition to traditional *QoS trust* metrics such as control packet overhead, throughput, packet dropping rate, delay, availability and fault tolerance, one must also consider *social trust* metrics [42] including friendship, honesty, privacy, similarity, betweenness centrality and social ties [12,13] for trust management. We note that prior works such as [12,13,17,20,39,41,44] also considered social trust metrics in communication networks. Our work distinguishes itself from these prior works in that we identify the best *trust aggregation* parameter settings for each individual trust metric (either QoS or social) to minimize trust bias.
- Second, we propose a novel model-based evaluation technique for validating SQTrust based on the concept of *objective trust evaluation* which utilizes knowledge regarding the operational and environment conditions to yield the ground truth against which subjective trust values obtained from executing SQTrust can be compared for validation. Our analysis methodology hinges on the use of Stochastic Petri Net (SPN) modeling techniques [30,36,64–68,73–75] for describing the "actual" dynamic behaviors of nodes in MANETs in the presence of well-behaved, uncooperative and malicious nodes. With this methodology, we identify the optimal trust parameter settings under which SQTrust is most accurate compared with global knowledge and actual node status.
- Finally, we consider a new design concept of *application-level trust optimization* by identifying the best way to form the overall trust out of individual social and QoS trust metrics to maximize application performance. Using a mission-oriented mobile group utilizing SQTrust, we identity the best trust formation protocol setting under which the application performance in terms of the system reliability of the mission-oriented mobile group is maximized.

The rest of the paper is organized as follows. Section 2 describes the system model and assumptions. Section 3 describes SQTrust and explains how it is executed by each node to perform peer-to-peer subjective trust evaluation. Section 4 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 SQTrust may be compared for trust bias minimization, including overhead analysis and an application scenario involving a lead node dynamically selecting a number of nodes it trusts most for mission execution for reliability maximization. Section 5 presents analytical results with physical interpretations given. Section 6 presents simulation results for simulation validation. Section 7 discussed related work so as to differentiate our work from existing work and identity unique features and contributions of our trust protocol design for MANETs. Section 8 discusses applicability. Finally, Section 9 summarizes the paper and outlines future research areas.

2. System model

2.1. Operational profile

We follow the notion of "*operational profiles*" in software reliability engineering [28] as input to specify the anticipated operational and environment conditions. Specifically, a system's *operational profile* provides knowledge regarding (a) environment hostility, i.e., how often nodes are compromised; (b) node mobility, i.e., how often nodes meet and how they interact with each other; (c) node behavior, i.e., how nodes will behave based on node status including good behaviors by good nodes and bad behaviors by bad nodes; (d) environment resources, i.e., the initial energy each node has and how fast energy is consumed by good or bad nodes; and (e) system failure definitions including both operational and security failure conditions. Later in Section 5, we will exemplify the input operational profile for a mobile group application in MANET environments. An operating profile does not represent a controlled setting. For example, hostility and node behavior as part of the operational profile merely specify per-node compromise rate and energy consumption/cooperativeness behavior but do not tell us which nodes are compromised and/or uncooperative over time. In response to operational or environment changes (e.g., change of hostility), the system using the results obtained in the paper can adaptively adjust trust settings to optimize application performance.

2.2. SQTrust design goals

SQTrust is distributed in nature and is run by each mobile node to subjectively yet informatively assess the trust levels of other mobile nodes. Further, SQTrust is resilient against misbehaving nodes. Given the operational profile as input covering a wide range of operational and environment conditions, we aim to satisfy and validate the following two design goals:

- Discover and apply the best trust aggregation protocol setting of SQTrust to make "subjective trust" accurate compared with "objective trust" despite the presence of misbehaving nodes. The desirable output is to achieve high accuracy in peer-to-peer subjective trust evaluation with high resiliency to malicious attacks.
- Discover and apply the best trust formation to maximize application performance. For the mission-oriented mobile group application, the desirable output is to maximize the system reliability given a system failure definition.

2.3. Node behavior

Node behavior is part of the operational profile. While our model-based analysis technique is generally applicable

Download English Version:

https://daneshyari.com/en/article/444398

Download Persian Version:

https://daneshyari.com/article/444398

Daneshyari.com