Enhanced Reputation Mechanism for Mobile Ad Hoc Networks

Jinshan Liu and Valérie Issarny

INRIA - Rocquencourt,
Domaine de Voluceau, Rocquencourt, BP 105, 78153 Le Chesnay Cedex, France
Jinshan.Liu,Valerie.Issarny@inria.fr
http://www-rocq.inria.fr/arles/

Abstract. Interactions between entities unknown to each other are inevitable in the ambient intelligence vision of service access anytime, anywhere. Trust management through a reputation mechanism to facilitate such interactions is recognized as a vital part of mobile ad hoc networks, which features lack of infrastructure, autonomy, mobility and resource scarcity of composing light-weight terminals. However, the design of a reputation mechanism is faced by challenges of how to enforce reputation information sharing and honest recommendation elicitation. In this paper, we present a reputation model, which incorporates two essential dimensions, time and context, along with mechanisms supporting reputation formation, evolution and propagation. By introducing the notion of recommendation reputation, our reputation mechanism shows effectiveness in distinguishing truth-telling and lying agents, obtaining true reputation of an agent, and ensuring reliability against attacks of defame and collusion.

1 Introduction

The pervasiveness of lightweight terminals (e.g., handhelds, PDAs and cell phones) with integrated communication capabilities facilitates the ambient intelligence vision of service access anytime, anywhere. This necessitates interactions between terminals belonging to different authorities, which are marginally known or completely unknown to each other. Trust management to enable such interactions has thus been recognized as a vital part of mobile ad hoc networks (MANET), which features lack of infrastructure, openness, node mobility, and resource scarcity (e.g., network, energy and storage space) of composing light-weight terminals.

In closed networks, trust establishment is managed by an authentication mechanism that assigns roles to agents. By agent, we mean a software entity working for and representing a node in MANET; each agent also has some reachable neighbor agents named peers. In an open environment such as MANET, fixed role assignment has to be replaced by dynamic decisions. An important factor affecting the decision making is an agent’s reputation.
Reputation assessment requires knowledge, information and evidence about the evaluated agent, which can be derived from an agent’s own experiences. However, openness implies significant opportunities of meeting with strangers an agent has never encountered before. Furthermore, more accurate estimation of an agent’s reputation becomes possible with sharing of reputation information among peers. Reputation mechanism has been widely used and implemented in electronic market places [12] and online communities [3]. For example, visitors at “amazon.com” or eBay usually read previous customers’ reviews and feedbacks before deciding whether to make transactions.

However, the design of a reputation mechanism is faced by a number of challenges, including: (i) the “free-rider” problem, i.e., agents do not share reputation information with peers; and (ii) the honest elicitation problem, i.e., agents may report false reputation information. There are multiple reasons for agents to be reluctant to report evaluations or to do so honestly [1]. Agents may withhold positive evaluations if a seller’s capacity is limited, e.g., wise parents are reluctant to reveal the names of their favorite baby-sitters. Agents may be reluctant to give positive recommendations because it lifts the reputation of the evaluated agent, which is a potential competitor. Agents may wish to be considered “nice”, or be afraid of retaliation for negative feedbacks. And last but not least, the reputation information agents provide only benefits other peers.

Therefore, it is necessary to build a reputation mechanism to enforce both active reputation information sharing and truthful recommendation elicitation, which are necessary for a reputation system to operate effectively [4]. Our target reputation mechanism aims to defend against the following three kinds of attacks:

- Inactivity: This refers to agents’ free-ride activities by not sharing reputation information with peers.
- Defame: This refers to agents’ activities of propagating a victim’s reputation that is lowered on purpose.
- Collusion: This refers to agents’ activities of propagating good reputation to promote each other.

Hence, the desired properties of a reputation system for MANET are:

1. Valid: The system is effective in the sense that agents are able to distinguish honest from dishonest agents through the reputation system.
2. Distributed: The system should not assume access to any trustworthy entity (e.g., Certificate Authority), or centralized storage of reputation values.
3. Robust: The system is robust to the attacks listed above.
4. Timely: The system should be dynamic and be able to reflect the trustworthiness of an entity in an up-to-date manner.
5. Resource-saving: The reputation system should take into account the limited computation power and storage space of each terminal in MANET.

Existing reputation systems either do not address the aforementioned incentive problems (e.g., [5,6]), or depend on some (centralized) trustworthy entity (e.g., [17]). Our approach, which is targeted at mobile ad hoc networks, does