Activity Stereotypes, or How to Cope with Disconnection during Trust Bootstrapping

Marc Sánchez-Artigas, *Member, IEEE,* and Blas Herrera

Abstract—Trust-based systems have been proposed as means to fight against malicious agents in peer-to-peer networks, volunteer and grid computing systems, among others. However, there still exist some issues that have been generally overlooked in the literature. One of them is the question of whether punishing disconnecting agents is effective. In this paper, we investigate this question for these initial cases where prior direct and reputational evidence is unavailable, what is referred in the literature as *trust bootstrapping*. First, we demonstrate that there is not a universally optimal penalty for disconnection and that the effectiveness of this punishment is markedly dependent on the uptime and downtime session lengths. Second, to minimize the effects of an improper selection of the disconnection penalty, we propose to incorporate predictions into the trust bootstrapping process. These predictions based on the current activity of the agents shorten the trust bootstrapping time when direct and reputational information is lacking.

Index Terms—Trust bootstrapping, network disconnection, punishment, stereotypes

1 Introduction

Trust-based systems have been proposed for a large variety of applications, ranging from mobile ad-hoc networks, Grids and P2P networks. At present, despite their maturity, some fundamental questions have still left unanswered. One of these important questions relates to the notion of disconnection as a *trust diminishing* event or *punishable* action. In open environments like P2P systems and Grid platforms like BOINC [1], disconnection affects the quality of service (QoS). To wit, in a P2P streaming service, QoS can be achieved as long as a continuous and uninterrupted data flow is maintained. It is basically for this reason that streaming systems like ripple-stream [2] and trust systems like [3], [4], [5] issue negative feedback for agents that are supposed to be providing the service but cannot do so because they are disconnected. The key problem is that in open environments it is not possible to differentiate between negative feedback due to malicious behavior and negative feedback due to disconnection; an agent can disconnect at any time and the trustor cannot tell whether the disconnection was intentional or not.

By the above discussion, one could infer that the most convenient method is to heavily penalize disconnection. However, contrary to intuition, as we show in this work, punishing disconnection might be *counterproductive*. This is especially true in those initial situations where no prior direct and reputational evidence is available. One case is when a new agent enters the system for the first time. In this situation, it is generally not possible for any trustor to form a reliable opinion on that agent. This also occurs when users form an ad-hoc group around a shared goal and disband once the pursued goal is met. In such cases, evidence can only be obtained through direct interaction, when some trustors are willing to take a chance and risk interacting with unknown trustees. It is the risk inherent in bootstrapping trust that can lead to applying little or no penalty on disconnecting agents.

For instance, consider the case that multiple unknown agents offer the same file to download. In this context, a transaction may simply be the transfer of a file piece to a trustor. Since a priori all agents have the same unknown disposition to good action, the first interacting trustee is chosen at random. Now suppose that after completing a certain number of transactions, the interacting trustee is unresponsive. At that point, the trustee may accumulate a certain amount of positive feedback and present a good trust level. Then it is not hard to imagine that the trustor gets confronted with the decision of whether to wait for the trustee to recover or take a chance on another agent.

The magnitude of the penalty determines the outcome of that decision. If the penalty is large, the odds to take a chance on a new agent are higher. In this case the trustor will maximize interaction. But it will be more exposed to abuses. On the contrary, if the penalty is low, the trustee may come online before getting low trustworthiness and continue providing good service. This will minimize the risk of bad interaction but at the expense of more service interruptions.

Our first contribution is to examine this tradeoff, and more generally, to assess to which extent the amount of penalty given to disconnection affects the bootstrapping of trust. To make the analysis tractable, we assume that T time units must elapse after disconnection in order to prefer an unknown agent. A smaller value of T implies a greater penalty, i.e., a higher probability for the trustor to take a chance on a new trustee. Using this parameter, we develop a stochastic model to estimate the expected time to obtain the first confident trust evaluation on an agent, provided that all the agents implementing the service are unknown to the trustor. By "confidence" we refer to the event that the

• *The authors are with the Department of Computer Engineering and Maths, Universitat Rovira i Virgili, Spain.*
Email: {marc.sanchez, blas.herrera}@urv.cat.

Manuscript received 25 Aug. 2013; revised 15 Dec. 2013; accepted 11 Jan. 2014. Date of publication 24 Feb. 2014; date of current version 5 Dec. 2014.
Recommended for acceptance by X. Li.
For information on obtaining reprints of this article, please send e-mail to: reprints@ieee.org, and reference the Digital Object Identifier below.
Digital Object Identifier no. 10.1109/TPDS.2014.2308186