



A reference model for reputation systems



Sokratis Vavilis^{a,*}, Milan Petković^{a,b}, Nicola Zannone^a

^a Eindhoven University of Technology, Den Dolech 2, Eindhoven 5612AZ, Netherlands

^b Philips Research Eindhoven, High Tech Campus 34, Eindhoven 5656AE, Netherlands

ARTICLE INFO

Article history:

Received 9 November 2012

Received in revised form 6 February 2014

Accepted 12 February 2014

Available online 22 February 2014

Keywords:

Reputation systems

Reference model

Trust requirements

ABSTRACT

Recent advances in ICT have led to a vast and expeditious development of e-services and technology. Trust is a fundamental aspect for the acceptance and adoption of these new services. Reputation is commonly employed as the measure of the trustworthiness of users in on-line communities. However, to facilitate their acceptance, reputation systems should be able to deal with the trust challenges and needs of those services.

The aim of this survey is to propose a framework for the analysis of reputation systems. We elicit the requirements for reputation metrics along with the features necessary to achieve such requirements. The identified requirements and features form a reference framework which allows an objective evaluation and comparison of reputation systems. We demonstrate its applicability by analyzing and classifying a number of existing reputation systems. Our framework can serve as a reference model for the analysis of reputation systems. It is also helpful for the design of new reputation systems as it provides an analysis of the implications of design choices.

© 2014 Elsevier B.V. All rights reserved.

1. Introduction

Advances of ICT have led to overall digitization of processes in data lifecycle management and consequently resulted in improved efficiency and cost savings. Each of us is constantly exposed to emerging digital technologies, either at home or at work, with an increasing number of business transactions daily carried out over the internet. However, to fully exploit the potentials of e-services (e.g., e-commerce, e-business, e-health) and facilitate their adoption, it is important to establish and manage trust among the parties involved in the transactions [1].

Reputation systems play an important role in the process of trust establishment and management. When a user needs to make a trust decision whether to engage or not in an interaction with an e-service, he takes very much into account the reputation of the service. The user's past experience as well as the experience of the other users with the service influences his decision whether to repeat this interaction in the future. Therefore, a reputation system, which helps in managing reputations in the digital world (for example by collecting, distributing and aggregating feedback about entity's behavior), becomes a fundamental component of the trust and security architecture of any ICT system or service.

However, the application and adoption of reputation systems in e-services rely on their ability to address the trust challenges that such services have to deal with. Therefore, the design of reputation

systems requires identifying the trust needs of e-services and of the application domain in which such services are deployed. In addition, when selecting a reputation system to be applied to an e-service, it is important to verify whether the selected reputation system meets the trust requirements for such a service.

In this paper we address these issues by presenting a framework for the analysis of reputation systems. In particular, we:

- elicit the requirements for reputation systems from a literature study;
- identify the features necessary to fulfill these requirements;
- present a reference framework for the analysis and evaluation of reputation metrics;
- demonstrate the applicability of the framework by comparing and classifying several well-known reputation systems.

The analysis presented in this work aims to serve both researchers that develop reputation systems and practitioners that intend to employ reputation systems for their services. On the one hand, it provides researchers an analysis of the implication of design decision. On the other hand, it provides practitioners a reference framework that can assist them in the selection of a reputation system that meets their needs.

Several surveys on reputation systems can be found in the literature [2–13]. Similar to most of these surveys, our work identifies the main features to be supported by reputation systems and evaluate existing systems against the defined features. In contrast to them, this work mainly focuses on the trust information used to assess the reputation and aggregation method, offering a more fine-grained analysis of reputation metrics. Moreover, existing surveys present features as abstract concepts. In contrast, we identify features from the requirements for

* Corresponding author.

E-mail addresses: s.vavilis@tue.nl (S. Vavilis), milan.petkovic@philips.com (M. Petković), n.zannone@tue.nl (N. Zannone).

reputation systems; features employed in this work are, thus, closer to the real needs of reputation systems.

The remainder of the paper is organized as follows. Next section introduces the basic concepts of reputation systems. Section 3 discusses the requirements for reputation systems along with the features needed for their fulfillment. Section 4 analyzes existing reputation systems with respect to the identified features and requirements. Section 5 provides guidelines on the application of the framework. Finally, Section 6 discusses related work, and Section 7 concludes the paper.

2. Overview of reputation systems

Reputation has been proposed as a measurement of a user's trustworthiness based on his past behavior [14] and it is used to predict his future behavior [15].

Typically, users rate other users on the basis of their interactions. In particular, a *rating* is the judgment that a user (*origin*) gives to another user (*target*) about a certain interaction that occurred between them (*scope*). Reputation systems assess the reputation of a user by aggregating the ratings that other users have given to that user.

Reputation systems can be analyzed from three dimensions [9], namely *formulation*, *calculation* and *dissemination*. The formulation dimension describes the mathematical model and input for the assessment of reputation values. It includes two main aspects: the reputation *measure* and the mathematical model (*metric*) used to aggregate ratings. Reputation can be measured using discrete or continuous values. Metrics can be based on simple summation or average of ratings [16], fuzzy logic [17,18], flow-based models [19–22], probabilistic models such as Bayesian systems [23–25], beta probability density [26,27] and subjective logic [28,29].

The calculation dimension addresses the practical design and implementation of the algorithm for assessing reputation, whereas the dissemination dimension focuses on the mechanisms for the distribution and storage of ratings and reputation values among entities within the system. The main feature of the calculation and dissemination dimensions is the *structure* of the reputation system, which can be either *centralized* or *decentralized*. Centralized systems like auction or expert sites are characterized by the presence of a central authority which is responsible for the collection and storage of user's ratings, and for the calculation of reputation values and their dissemination. On the other hand, decentralized systems like Peer-to-Peer (P2P) networks and Multi-agent Systems (MAS) have neither a central authority nor a fixed network topology that can be used to control the entities within the system; rather each entity is responsible for controlling its data and resources. In these systems, the storage of ratings and calculation of reputation are distributed among the entities within the system.

3. Requirements and features for reputation systems

This section presents the main requirements for reputation systems along with the features needed to achieve such requirements. The elicited requirements and features form a reference model for the analysis and comparison of reputation systems.

3.1. Requirements

For the correct and secure functioning of reputation systems several desirable requirements should be satisfied. In this work, we are mainly interested in requirements which ensure that assessed reputation values reflect the actual trustworthiness of users. Based on a literature study, we have identified three groups of requirements (Table 1). Requirements in the first group focus on the formulation dimension. The other two groups contain requirements about the fair treatment of newcomers and the integrity of reputation values (w.r.t. the calculation and dissemination dimensions).

The first group of requirements (R1 to R8) focuses on the information and aggregation method used for the assessment of reputation values. R1 and R2 require ratings and reputation values to accurately discriminate user behavior. R3 and R4 focus on the “quality” of information used to assess reputation values. A user can (un)intentionally provide incorrect ratings about an interaction he had. For instance, a malicious user may give negative ratings to a user with the purpose of decreasing its reputation [9,22]. Moreover, he can subvert the reputation system by first creating a large number of pseudonymous entities, and then using them to influence the reputation of a target user [30]. In particular, if users are able to rate themselves, they can provide a series of self-promoting ratings, leading to an unfair increasing of their own reputation [9]. To prevent such attacks, reputation systems should be able to discriminate “incorrect” ratings (R3). R4 refines R3 by explicitly forbidding self-rating.

Requirements R5 to R8 deal with the type and amount of information used to assess reputation values. Interactions between entities can differ significantly in their nature, making it difficult to draw conclusions about the reputation of entities. For instance, aggregating the ratings referring to different types of interactions would result in reputation values that may not accurately reflect the trustworthiness of entities. Therefore, reputation values should be assessed using comparable trust information (R5). However, the reliability of reputation values depends on the amount of information used to calculate them [31]. Due to the restrictions imposed by R5, reputation may only rely on a small amount of information. R6 relaxes R5 by allowing the use of a larger amount of information in the assessment of reputation, while ensuring that the obtained reputation values remain meaningful. Interactions between entities may also differ in their “cost” (e.g., economic transactions) [32]. For example, in an online auction site, a user can build his reputation through transactions involving a small amount of money, and then take advantage of his gained reputation to cheat other users in a transaction involving a substantial amount of money. R7 requires reputation systems to differentiate ratings with respect to the cost of transactions. Finally, R8 focuses on temporal aspects. Reputation is built upon the knowledge of past interactions. The behavior of a user can change over time. For instance, a malicious entity might be fair in his interactions for a period in order to build positive reputation and be able to successfully deploy his attack. Therefore, user behavior evolution should be captured in the assessment of reputation to reflect the actual trustworthiness of users.

The second group of requirements (R9 and R10) addresses the fair treatment of new users. When new users join the system, their behavior is unknown. Typically, reputation systems assign a default reputation value to new users. Such a value, however, should not penalize them for their status. If newcomers are treated as users with a bad reputation, they may never be selected by other users and thus they cannot build their reputation [20]. At the same time, reputation systems should prevent users to gain advantage of their new status. Indeed, to avoid the consequences of their actions, users with bad reputation may change their identity by re-joining as a new user (the so called white-washing attack [33]). Requirements R9 and R10 define the boundaries in the selection of the reputation value for new users.

The last group of requirements (R11 to R13) addresses calculation and dissemination issues regarding the integrity of reputation values and ratings. R11 and R12 impose reputation systems to protect ratings and reputation values from unauthorized manipulation during transmission and storage. This, however, may not be sufficient to guarantee their integrity. If users are involved in the calculation of their own reputation, they may influence the obtained value. R13 aims to prevent such a malicious behavior.

3.2. Features

The requirements in Table 1 constitute the basic and desirable characteristics that a reputation system should satisfy. Their fulfillment

Download English Version:

<https://daneshyari.com/en/article/553462>

Download Persian Version:

<https://daneshyari.com/article/553462>

[Daneshyari.com](https://daneshyari.com)