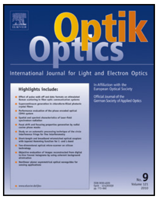
Optik 125 (2014) 2692–2701

Contents lists available at ScienceDirect

Optik

journal homepage: www.elsevier.de/ijleo



A robust decentralized reputation management system for service selection

Quanwang Wu*, Qingsheng Zhu, Xing Jian

Chongqing Key Laboratory of Software Theory & Technology, Chongqing University, Chongqing, China

ARTICLE INFO

Article history:
Received 5 June 2013
Accepted 5 November 2013

Keywords:
Reputation
Service selection
QoS
Robustness
Decentrality

ABSTRACT

Reputation mechanism is a novel approach to automate QoS-aware service selection in service oriented computing. The reputation system collects ratings on QoS that consumers feedback and aggregates them to derive a reputation value, which can in turn assist other consumers in service selection in future. However, current approaches fail to combat the malicious ratings and hence the calculated reputation values can be biased severely or even manipulated. Moreover, the centralized management of rating data restricts its application to large open environment. In this paper, we present a robust decentralized reputation system which can resist various unfair ratings and manipulation behaviours. It can evolve and become more mature against malicious ratings with the system running continuously. At last, we experimentally verify the robustness of the proposed approach through a simulation study.

1. Introduction

Service oriented computing (SOC) [1] is a novel paradigm for distributed computing which aims at changing the way software applications are designed, delivered, and consumed. In SOC, computing resources are modeled as services, which can be used directly or composed into other services. Nowadays, more and more services have been published online, and how to select a required service with the best quality of service (QoS) from numerous candidates becomes a critical research issue. It is not reliable and maybe misleading to make decisions only based on the advertised QoS, as in a dynamic environment, it is hard for a service provider to guarantee his advertised QoS. Moreover, some providers might deliberately advertise high QoS values which they cannot achieve to attract more customers. Some authors [2,3] present approaches to actively monitor each web service's dynamic performance. However, it is too costly for large open systems to adopt.

Reputation mechanism has emerged as an important risk management solution to solve trust problems in online communities. The basic idea of the reputation mechanism is to let consumers evaluate services and feed back the rating to the reputation system after the completion of an interaction, and the reputation system use the aggregated ratings to derive a reputation score, which can in turn assist other consumers in deciding whether or not to interact with the specific service in future [4].

The reputation mechanism is also studied in SOC and a number of reputation systems [5–15] have been presented to automate QoS-aware service selection. Based on the reputation mechanism, the reliability of service composition can also be enhanced [16–18]. However, these approaches mostly have not taken the presence of malicious ratings into account or only preliminary safeguard measures are proposed [10,12], which can be broken through by sophisticated deception behavior. In the real world application, where malicious users can always gain knowledge about the reputation system and adjust the attack strategies based on their observation, even a small loophole can be extremely exploited and delivers a crushing blow to the reputation system. Hence, designing a reputation system which is robust enough to detect and mitigate the effects of malicious ratings is a fundamental issue.

Meanwhile, almost all current reputation systems for SOC are centralized [19], i.e. there is a centralized reputation manager responsible for collecting and storing ratings from consumers. This restricts the scalability of the application environment and leads to the risk of a single-point failure. Furthermore, the reputation manager is supposed to be totally trustworthy.

This paper presents a deception-resilient decentralized reputation system which can resist various unfair ratings and manipulation behaviors. In our approach, service consumers are wrapped by autonomous agents and these consumer agents form a decentralized structured P2P network. Rating data, which are used to compute reputation values of services, are stored and accessed across the P2P network instead of in a central database.

* Corresponding author.
E-mail addresses: wqw@cqu.edu.cn (Q. Wu), qszhu@cqu.edu.cn (Q. Zhu), jx@cqu.edu.cn (X. Jian).

http://dx.doi.org/10.1016/j.ijleo.2013.11.052
0030-4026/© 2014 Elsevier GmbH. All rights reserved.

By capturing most aspects of real-world social reputation and incorporating them into the reputation evaluation model, the proposed reputation system can identify and address different types of malicious ratings. In addition, with transactions conducted continuously, the reputation system can evolve and become more mature against malicious ratings.

The remainder of this paper is organized as follows. Section 2 discusses the related works in this field. Section 3 describes our resilient reputation evaluation model, while Section 4 presents a decentralized implementation. Empirical studies are shown in Section 5. Finally, Section 6 concludes the paper and gives future work.

2. Related works

In this section, we first discuss traditional strategies against malicious feedbacks, and then we give an overview of current reputation systems in SOC.

2.1. Strategies against malicious ratings

As we have mentioned above, although a number of reputation systems have been presented in SOC, only a few of them take malicious ratings into account. In the domains such as e-commerce, multi-agent systems, peer-to-peer systems (P2P), trust and reputation mechanisms have been studied for a long time. These studies can provide valuable guidelines and theories for the studies in SOC. Thus, the strategies used to defend against malicious feedbacks we are going to discuss here are not limited to the SOC domain. We classify these strategies mainly into two categories: endogenous and exogenous.

Endogenous safeguard approaches exclude or give low weights to presumed unfair ratings based on analyzing and comparing the ratings themselves. For example, Whitby et al. [20] propose a statistical filtering technique to detect and exclude ratings that are likely to be unfair when judged by the majority-based statistical analysis. Cluster filtering in [21] and entropy-based detection in [22] also belong to this category. The heuristics proposed in [10] make the ratings which agree with the majority of ratings and previous assessed reputation values a higher weight during aggregating ratings.

The approaches in this category can only work well when the assumption that majority of the raters are honest holds. That is to say, if a large number of raters are dishonest, the calculated reputation values can be largely biased or even be manipulated. This assumption is challenged in practice from the following two aspects. First, the popularity of the web resources follows the power–law distribution [23] and the number of consumers for most of the services is very small. Thus, it is pretty easy for the reputation of these services to be biased or manipulated. Second, rating aggregation is always performed in the latest time window to catch the dynamic characteristics of the services [24]. In this case, the majority opinion can be dominated by malicious raters in the latest time window, even when the honest clients heavily outnumber the malicious ones.

Exogenous safeguard approaches utilize external factors (such as the rater's credibility) to determine the weight given to ratings. The assumption is that raters with low credibility are more likely to give unfair ratings and vice versa. In P2P systems, where a peer acts as both a service consumer and a service provider, the reputation of a peer can be straightforward utilized as its credibility by coupling feedback trust and service trust together. Eigen trust [25] and Peer trust [26] are examples of this kind. In SOC, where service consumers and providers are usually independent entities, it is not practicable to couple feedback trust and service trust together. In [27], the consistency is checked between ratings and the actually perceived QoS values and the credibility is modeled as the expectation value of the beta function $\beta(a, b)$, where a and b denote the times of consistency and inconsistency, respectively. The rationale of credibility assessment in [12] is similar to [27].

The vulnerability of exogenous safeguard approach is that it assumes that raters behave consistently, which may not be the case in real world. For instance, a tricky malicious rater may lie only in certain situations, but behave honestly in other situations to hide his maliciousness. Another disadvantage is that there is a period of cold start for new users whereas endogenous safeguard approaches can be used at any time.

In addition, there are two SOC-specific methods to combat malicious ratings. In [7], a few trustworthy third parties are deployed to monitor services and produce credible QoS reports. Based on these credible reports, a trust-distrust propagation approach is employed to detect malicious ratings. To keep a high precision of service selection, the percentage of services monitored by trusted agents should be more than 6.0%. The approach suffers from extra network overheads and a low scalability. In [9], reporting incentives are created through a payment mechanism where every client gets paid for submitting feedbacks. It is proven that truthful reporting maximizes the expected revenue (due to feedback payments) of a client, motivating equilibrium where every client reports honestly. However, it is not feasible to integrate a payment mechanism for feedback into current SOC model as no entity in the model is willing to afford the payments.

2.2. An overview of reputation systems in SOC

Since the problem of trust is exacerbated in SOC due to its inherent open, highly dynamic and large-scale nature, a number of reputation approaches have been proposed for automating service selection. Although these approaches share the same idea of reputation mechanism, they are different in their focuses. For instance, Maximilien and Singh [5] concentrate on building a QoS ontology, which is used for QoS advertising and rating. Liu et al. [6] proposed an algorithm about how to combine different QoS metrics to get a fair overall rating for a service. Xu et al. [8] propose a model of reputation-enhanced services discovery which combines an augmented service registry to publish QoS data and a reputation manager to assign reputation scores to the services based on customer feedback of their performance. Hang and Singh [14] adopt Bayesian networks for the reputation model, which takes binary ratings as input and computes reputation values by statistically updating beta probability density functions. The approach is effective even if only incomplete observation on services is available.

Current reputation systems in SOC are mostly centralized. They depend on a central reputation manager to collect and store feedbacks from consumers. As far as we know, the only exception is the reputation system proposed by Vu et al. [7]. In [7], a number of reputation managers are deployed to collect and store feedbacks from consumers and these reputation managers are organized in a special P2P structure called *p*-grid. Each manager is responsible for managing rating data of a part of services.

Based on the safeguard strategy and architecture feature, current reputation systems for SOC in the literature are mainly summarized in Table 1.

Our approach incorporates most aspects of real-world social reputation into the reputation evaluation model and both the endogenous and exogenous strategies are adopted. It can combat various malicious ratings. Our decentralized architecture is different from the one in [7], as the P2P network is constituted by consumer agents, instead of independent reputation managers in [7]. Rating data are stored and accessed across the P2P network instead of a central database.