The Journal of Systems and Software 000 (2015) 1–11

Contents lists available at ScienceDirect

The Journal of Systems and Software

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

A fuzzy-based credibility model to assess Web services trust under uncertainty

Zohra Saoud [a,*], Noura Faci [a], Zakaria Maamar [b], Djamal Benslimane [a]

[a] Boulevard Niels Bohr, 69622 Villeurbannex Cedex, France
[b] Zayed University, Po Box 19282, Dubai

ARTICLE INFO

Article history:
Received 15 October 2014
Revised 24 July 2015
Accepted 30 September 2015
Available online xxx

Keywords:
Web service
Trust
Credibility

ABSTRACT

This paper discusses the assessment of Web services trust. This assessment is undermined by the uncertainty that raises due to end-users' ratings that can be questioned and variations in Web services performance at run-time. To tackle the first uncertainty a fuzzy-based credibility model is suggested so that the gap between end-users (known as *strict*) and the current majority is reduced. To deal with the second uncertainty two trust approaches (i.e., deterministic and probabilistic) are proposed so that trust levels for future interactions with WSs are made available to users. The deterministic approach takes account end-users' credibility values and the probabilistic one is built upon probabilistic databases and a fuzzy-based credibility model. A series of experiments are carried out to validate the suggested credibility model and these trust approaches. The results show that the probabilistic approach improves significantly trust quality and is more robust compared to the deterministic one. Future work consists of incorporating several credibility models into a single probabilistic trust model.

1. Introduction

It is largely accepted that current Web services (WSs) selection approaches rely on either non-functional properties (*aka* Quality of Service (QoS)) that providers announce publicly or on collecting qualitative/quantitative values that end-users share with respect to past experiences of using these Web services. Qualitative/quantitative values permit to establish feedback/ratings that indicate the satisfaction of end-users with the overall performance of WSs. However a complete reliance on both providers and end-users raises trustworthiness concerns among future potential end-users due to biases such as beefing-up a WS's QoS and/or undermining a WS performance both done purposely. To address these biases two types of trust models are reported in the literature. The first model uses end-users' feedback/ratings to compute a trust value (e.g., Xiong and Liu, 2004). And, the second model observes the behaviors of WSs over a period of time to compute a trust value (e.g., Wang and Singh, 2007). We are particularly interested in the first trust model. Indeed end-users with either limited or non-existent experience of using WSs cannot provide adequate trust values. When establishing trust these end-users "wrestle" with two kinds of *uncertainties*:

Uncertainty (U_1) over feedback/rating. U_1 arises from the lack of consistent ratings that end-users provide over time. Credibility should help tackle U_1 when aggregating end-users' feedback/ratings into a common trust value (e.g., Xiong and Liu, 2004; Selcuk et al., 2004).

Uncertainty (U_2) over the capacity of a WS in fulfilling the QoS that its provider announces and thus, satisfying end-users' requests. U_2 arises from the inconsistency that affects the assessed QoS values due to a WS's dynamic nature and/or malicious behavior. Trust should help tackle U_2 (e.g., Kim and Kim, 2005).

Feedback/ratings concurrently mitigate and introduce uncertainty. Uncertainty arises due factors like end-user's subjectivity and provider's reliability. We should assess trust despite these factors.

Bordens and Horowitz (2001) decomposed credibility into two components: (i) **expertise** that stems from end-user's knowledge, background, notoriety, etc.; and (ii) **trustworthiness** that "... *refers to the audience's assessment of the communicator's character as well as his or her motives for delivering the message*". Credibility-based trust approaches given by Malik and Bouguettaya (2009) and Noor et al. (2013) assume that end-users have good expertise and/or are untrustworthy. When end-users disagree on a certain feedback/rating on a WS a consensus needs to be reached using the majority opinion. End-users' ratings close to the majority opinion are more credible than those with distant ratings. However these approaches do not

* Corresponding author. Tel.: +33 783060937.
E-mail address: saoud.zohra@gmail.com (Z. Saoud).

http://dx.doi.org/10.1016/j.jss.2015.09.040

consider end-users who are both expert and trustworthy. We refer to such end-users as *strict* (*severe*) *experts*. They usually do not have any interest (e.g., making extra income) in aligning themselves with the majority. For the sake of achieving consensus fuzzy clustering technique would reduce the gap between *strict experts*' feedback/ratings and the current majority opinion.

There are a number of credibility-based trust approaches that assess trust as a scalar value (e.g., Wang and Singh, 2007; Ries et al., 2011; Jøsang, 2001). However these approaches struggle with establishing trust based on direct end-users' experiences and/or peers' feedback/ratings. A scalar value fails to represent first, the uncertainty over possible trust values and second, the lack of consistency across different feedback/ratings. The obtained trust value is subject to ambiguous interpretations by end-users.

Feedback/rating inconsistencies lead to disagreement amongst end-users' opinions. Troffaes (2006) shows that probabilities can address this disagreement . As stated earlier end-user's credibility helps tackle uncertainty over feedback/ ratings (U_1). Therefore we associate credibility with probabilities. Let assume three end-users, u_1, u_2, and u_3 who have experienced WS_j and let the following statement $\mathcal{S}$: u_i has **correctly** observed that WS_j satisfies his requests. The uncertainty here reflects the probability that $\mathcal{S}$ happens. This probability can be estimated by computing u_i's credibility (Cr_i). Let e_1, e_2, and e_3 denote respectively, the events that u_1, u_2, and u_3 state each that WS_j satisfies their requests. Combining e_1, e_2, and e_3 when computing trust raises issues like what is the probability that u_1, u_2, and u_3 **jointly** state that WS_j satisfies their requests, and what is the probability that u_1 and u_2 **only** state that WS_j satisfies their requests? Probabilistic databases permit to represent these kinds of events by associating an occurrence (or existence) probability with each statement (Dalvi and Suciu, 2007). These databases can also support develop complex queries that combine selection criteria (e.g., only end-users who provide at least n ratings).

Our contributions include: (i) modeling *end-user's credibility* based on a fuzzy clustering technique so that *strict end-users*' ratings are taken into account; (ii) developing strategies for establishing the majority opinion; (iii) assessing trust under uncertainty using probabilistic databases; (iv) building a distributed trust assessment framework based on a proposed credibility model; and (v) developing a system that measures the quality of trust.

The remaining of this paper is organized as follows. Section 2 identifies some work related to WS trust assessment. Section 3.2 motivates the use of fuzzy clustering that underlies our credibility model and describes how end-user's credibility is established. Section 4 depicts two approaches for trust assessment; the first consolidates end-users' ratings taking into account end-user's credibility while the second relies on probability theory coupled with possible worlds semantics. Section 5 gives details on the proposed trust assessment framework and discusses experiments. Finally, concluding remarks and future work are reported in Section 6.

2. Related work

Uncertainty like U_1 and U_2 reported in Section 1 impacts the way WS trust is established. In the following we discuss two research streams for tackling U_1 and U_2, respectively: deterministic (credibility-based) and probabilistic.

2.1. Deterministic trust

Deterministic trust approaches rely on end-users' experiences (i.e. feedback/ratings) build upon former interactions. They assess end-user's credibility as a degree of uncertainty that a WS will successfully satisfy a request.

Xiong and Liu (2004) developed Peertrust, a credibility-based trust framework in the context of P2P networks. In Peertrust a peer's feedback means the satisfaction of this peer about the participation of others in joint operations. A peer may send others false feedback/ratings because of some malicious motives, for example. The feedback from peers with higher credibility have more weight than those with lower credibility. The authors use two metrics to compute the credibility value of a peer (p_i): QoS provided by p_i and feedback similarity between p_i and p_j.

Whitby et al. (2004) looked into biased feedback. These feedback often have a different statistical pattern compared to unbiased ones. The authors proposed a beta distribution-based filtering technique as a statical pattern for feedback representation. This technique applies the majority rule to exclude biased feedback by tagging feedback as biased when they are distant from a majority's referrals. This technique is only effective when the majority of ratings are unbiased.

Weng et al. (2005) examined unfair ratings in the online *Bayesian* rating systems. These systems collect sellers' behaviors over past transactions so that future transactions' life cycles is predicted. The authors use entropy (i.e., measure *uncertainty* in information (Cover and Thomas, 1991)) to evaluate the quality of ratings. Entropy excludes a particular buyer's rating from the majority opinion if this rating significantly either improves or degrades the quality of the already-aggregated majority opinion (i.e., above or below a certain threshold).

Malik and Bouguettaya (2009) discussed trust for WSs selection and composition. They propose several decentralized trust assessment techniques to ensure a better accuracy of the feedback collected over time. Malik and Bouguettaya consider that feedback of highly credible end-users are most trusted than those with low credibility. To this end, they examine the feedback based on the distance from the majority opinion using $\mathcal{K}$-means clustering and group similar feedback into clusters in order to define this majority. The highly (i.e., most dense) populated cluster is the majority cluster whose centroid represents the majority feedback. Along with the majority principle, the authors' trust model takes into account other social metrics such as end-users' feedback history, personalized reputation evaluation using end-users' personal preferences, and temporal sensitivity. These metrics help adjust the credibility value when the number of end-users with biased ratings is above the number of those with unbiased ratings and the majority rule does not hold as well.

Noor et al. (2013) proposed a credibility model that distinguishes credible from misleading feedback in a cloud context. This model uses factors such as majority consensus and feedback density. To measure how close a cloud end-user's feedback is to the majority's feedback, Noor et al. use the slandered (i.e., root-mean-square) deviation. Feedback density overcomes the problem of misleading feedback from end-users. These latter give multiple feedback to a certain cloud service in a short period of time.

2.2. Probabilistic trust

In existing probabilistic trust management approaches (e.g., Teacy et al., 2006; Zhou and Hwang, 2007; Yu and Singh, 2002) peers rely on direct use experiences with services or feedback/ratings that other peers share. False feedback/ratings are handled through a suitable filtering mechanism. In the following we describe three relevant probabilistic approaches.

TRAVOS is a trust model used in open agent systems (Teacy et al., 2006). An agent trusts a peer based on previous direct interactions. Interactions' outcomes use a binary rating to express successful/unsuccessful interaction. The obtained binary ratings are then used to form the probability-density function that models the probability of a successful interaction with an agent. If there are not enough direct experiences the model uses other agents' experiences to compute the trust value. The model determines the credibility of agents