Knowledge-Based Systems 57 (2014) 161–167

Contents lists available at ScienceDirect

Knowledge-Based Systems

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

A Web Service trust evaluation model based on small-world networks

Fengming Liu [a,*], Li Wang [a], Lei Gao [b], Haixia Li [a], Haifeng Zhao [c], Sok Khim Men [d]

[a] School of Management Science and Engineering, Shandong Normal University, Ji'nan 250014, PR China
[b] CSIRO Land and Water, PMB 2, Glen Osmond, Adelaide, South Australia 5064, Australia
[c] The University of California at Davis, One Shields Ave., Davis, CA 95616, United States
[d] Palo Alto University, Arastradero Rd, Palo Alto, CA 94304, United States

ARTICLE INFO

Article history:
Received 15 January 2013
Received in revised form 30 November 2013
Accepted 15 December 2013
Available online 22 December 2013

Keywords:
Web Services
Trust model
Subjective logic
Small-world networks
SOA

ABSTRACT

As a popular innovation, Web Service provides a flexible solution to integrate diverse online applications with existing Internet protocols and open standards. The availability and flexibility of Web Service enable its potential to handle dynamic requests in distributed online collaboration.

However, this potential is limited by Web Service's security concerns due to its uncertainty, openness and fraudulence. A solution to this problem, Trust, an important social concept in all human interactions, has been proven to be a promising way to resolve the security issues raised by these distributed collaborations.

This paper introduces a novel evaluation model of Web Service by leveraging trust as an approach. We first incorporate a trust management module into the standard Service Oriented Architecture (SOA). Then, after transforming a Web Service network to a small-world network based on the trust relationships of service entities, we propose a trust evaluation model with an amendatory subjective logic. The simulation experiments we ran compared our trust evaluation model with two other popular models. The result shows our proposed model outperforms in terms of both detection capability and stability.

1. Introduction

Web Service, an open standard based on existing Internet protocols, provides a flexible solution to web application integration [1,2]. It also interacts with other service entities to compose more complicated Internet-based business applications. The standard architecture of Web Service involves the interactions of three entities [3] (as shown in Fig. 1), including a Web Service provider (SP) that hosts a Web Service and applications, a Web Service broker (SB) that makes Web Service publicly accessible, and a Web Service requestor (SR) that associates Web Service operations with its application environment.

The service provider, such as an enterprise, or ICP (Internet Content Provider), is specified by Web Service Define Language (WSDL) document that contains a formal definition of the service interface. This document specifies the physical location of the services, as well as provide requestors who intend to invoke a service provider knowledge of how to create messages [4]. A service provider builds the service and makes it available on the Internet for consumers. A service requestor (e.g., a client application) invokes an existing Web Service by opening a network connection and sending an XML-SOAP request. Service Broker plays the role as a central place for providers to publish and developers to obtain new services. It serves as a centralized clearinghouse for companies to register their services [5].

The high availability and flexibility of Web Service enable its potential in distributed online collaboration to handle dynamic service requests [6]. In an ideal situation, Web Services are expected to automatically interact with one another, manage objects, derive complicated applications, and adapt to dynamic requirements [7,8]. However, this long-term goal is still far from being achieved. An important reason for this is the lack of guarantee to create a successful collaboration among Web Services [9] due to the challenge of assuring secured communication between services. In order to solve this, the trustworthiness of the services' security in communication is essential. To evaluate trust and establish the trust relationship among services becomes significant.

Trust, a complex concept that relates to a Web Service entity's toward another, is a measurement of the willingness to believe in a service entity based on its perceived honesty and reliability within a specific context at a given time [10,11]. Trust is different from traditional security mechanisms (e.g. access control and cryptographic protocols), where services are protected through controlled access to authorized users with restricted actions. In an open, distributed, and anonymous environment, traditional security mechanisms are unable to protect Web Services, because service entities cannot protect themselves from those who act deceitfully by providing wrong or misleading access information. Trust can overcome this incapability of traditional security mechanisms [12].

* Corresponding author. Tel.: +86 531 86180509; fax: +86 531 86180510.
E-mail address: fmliucn@gmail.com (F. Liu).

0950-7051/$ - see front matter © 2013 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.knosys.2013.12.015

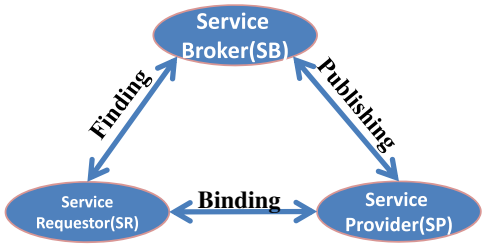

Fig. 1. A demonstration of the Web service architecture.

Trust plays an important role in Web Service. A conceptual trust model of Web Service was proposed by Maximillen et al. [13,14]. It uses the average rating given by end-users to automatically determine the selection of Web Services. This trust measurement approach using average rating cannot capture the degree of variance in the service providers' compliance levels. So, a novel metric named Verity was introduced by Kalepu et al. [15] to quantify the consistency in compliance levels of a service contract. Several Bayesian approaches to compute trust value based on the beta probability density functions were proposed in [16–18]. However, the computation methods for trust mentioned above are in terms of probabilistic models that regard uncertainty of trust as randomness, and neglect the fuzziness of belief. Ardagna et al. [19] presented a model to address service selection problem, but trust happens to be one of those considered quality criteria and this model cannot detect malicious consumers.

Yuan et al. verified that the small-world phenomenon [20] takes place in trust network where nodes are inter-linked by their trust relationships. A small-world network is defined as a network that has (1) large clustering coefficient and (2) short average path length. From our point of view, the network of Web Service can be regarded as trust network, among which service entities (such as SBs, SRs, and SPs) are connected by trust relationships. Based on the small-world of trust networks, this paper proposes a Web Service trust evaluation model which can be used to locate required services, establish new relationships among these services, and group services into a complicated application. We first incorporate a trust management module into the Service Oriented Architecture (SOA) framework where trust information of service entities can be collected and stored. Then we extend Jøsang's subjective logic [21] and build a Web Service trust evaluation model based on small-world networks. The components in the SOA framework are mapped into service entities in a small world network. More importantly, a trust mechanism is incorporated into Web Service interactions in order to generate successful collaborated applications. Finally we evaluate the proposed model against two popular trust evaluation models by simulation experiments. The results show that our proposed model outperforms in terms of both detection capability and stability.

The trust evaluation framework proposed in this paper rest on the following attributes:

(1) It improves the subjective logic on small world by adopting the "forgetting" time for trust value.
(2) A centralized trust framework stores, computes and updates the trust values when a service is invoked by consumer. The trust information is stored by a SP or SR in order to adapt the SOA expansion and the properties of small world.
(3) It takes into account of the trustworthiness of the service requestor which is neglected in certain literatures [21,22].

The rest of the paper is organized as follows. A literature review of related work is presented in Section 2. Section 3 is dedicated to the presentation of our trust evaluation model for Web Service collaboration based on small-world networks. Section 4 shows the simulation experiments and evaluates the results. And finally, our work is concluded in Section 5.

2. Related work

Trust is a personal, subjective and multidimensional phenomenon. Trust mechanism provides security protection for service collaboration against malicious service entities by applying social control mechanisms, which use interactive or collaborative methods for identifying and sanctioning service entities who behave against ethical norms. Thus, trust is one of the hot topics that are currently studied in social network [23,24], large-scale online collaboration [25,26] and Web Service applications [12,27–32]. Various trust computation models have been established to select, rank, or compose Web Services in a trusted way.

Jøsang defines a framework called subjective logic, which is an extension of standard logic that uses continuous uncertainty and belief parameters instead of only discrete truth values [21]. Because of the imperfect knowledge of individuals, opinions about the facts are reflected by the degree of uncertainty, belief, and disbelief. The subjective logic contains some operations specific for belief theory, such as consensus and recommendation. Yuan et al. propose a novel TARS (Trust-Aware Recommender System) model which can effectively overcome the weakness of the conventional TARS model. They verified trust network that has small-world topology by analyzing five trust networks. So, in trust networks, two randomly selected service entities can build a trust relationship within limited link paths, which are also regarded as trust paths.

However, there lack effective solutions to evaluating the trustworthiness. To evaluate the degree of trust, trust information is required to be extracted from the security component of a service based on the needs of an entity, the security policy of the entity, and the security policy of the service [27]. Based on environmental context, a trust computation model is proposed by Ding et al. With different contexts from different service environments, they first presented a fitness function to measure each entity's trust value. Their trust evaluation model is also used to compute trust value of each entity based on service context that helps to make trust decisions of a transaction in a distributed service environment. West et al. [28] classify the discussion into two categories: (1) trust computation, focusing on algorithms to compute trust values and their relative merits; and (2) trust usage, surveying how trust values can be conveyed to end-users to improve application security. They present a trust definition as an 8-dimensional vector that contains trust information needed to calculate trust assessment. Kovač and Trček [12] present an abstract trust model $TM = (G, D, O, \Gamma, P)$ from the qualitative perspective as a formal definition. The trust model takes a socio-cognitive nature of trust into account, and is used as a foundation for the trust engine of SOA-based applications, in the existing security services (WS-Security [33]), and in other WS-$*$ standards (WS-Policy [34]). The RATE-Web model, proposed by Malik and Bouguettaya [29], is a reputation model for the selection and composition of web services by sharing experiences through aggregated feedback ratings on the trustworthiness of service providers.

3. A trust evaluation model of Web Services based on small-world networks

The components in the proposed SOA framework are organized in a small-world way. In order to generate successful collaborated applications, a trust mechanism is incorporated. In this section, a system framework of SOA for trust management is presented first,