Trust Based Service Selection in Service Oriented Environment

Jun Li, College of Computer Science, Zhejiang University, China
Xiaolin Zheng, College of Computer Science, Zhejiang University, China
Deren Chen, College of Computer Science, Zhejiang University, China
William Wei Song, Dalarna University, Sweden

ABSTRACT

In a service-oriented environment, it is inevitable and indeed quite common to deal with web services, whose reliability is unknown to the users. The reputation system is a popular technique currently used for providing a global quality score of a service provider to requesters. However, such global information is far from sufficient for service requesters to choose the most qualified services. In order to tackle this problem, the authors present a trust based architecture containing a computational trust model for quantifying and comparing the trustworthiness of services. In this trust model, they firstly construct a network based on the direct trust relations between participants and rating similarity in service oriented environments, then propose an algorithm for propagating trust in the social network based environment which can produce personalized trust information for a specific service requester, and finally implement the trust model and simulate various malicious behaviors in not only dense but also sparse networks which can verify the attack-resistant and robustness of the proposed approach. The experiment results also demonstrate the feasibility and benefit of the approach.

Keywords: Service Selection, Service-Oriented Environment, Social Network, Trust, Web Services

INTRODUCTION

In recent years, the Web has started a steady evolution to become a distributed, dynamic, service-oriented environment (SOE) where applications can be automatically invoked by other clients over the Web. As an autonomous, platform-independent, and computational element, web services laid a foundation for constructing a distributed and collaborative web. A web service is a self-describing software system that can be advertised, located, and used across the Web based on a set of standards, such as WSDL, UDDI, and SOAP (Papazoglou, 2003). All these standards are based on Extensible Markup Language (XML), which allows Web services to interact with each other over the Web.

Although the development of web services seems very promising, there are some challenging problems. A plethora of Web services competing in offering similar functionalities bring a great challenge in selecting a suitable web service. The goal for service selection is to
find a best set of services, available at runtime, reliable, taking service requesters preferences into consideration and so on. Thus, service requesters need to know not only the functional attributes, but also the non-functional attributes of web services, i.e., Quality of Service (QoS) properties. Web services are executed on the hardware of their respective providers, in different containers, separated by firewalls and other trust barriers (Sung, 2009). Therefore, the major challenge lies in providing a framework for evaluating the trustworthiness of service providers without any prior interactions. In an open environment, where anyone can publish services, a service requester may select a poor quality, time-consuming, expensive, or even harmful service. Therefore, mechanisms are needed to help service requesters to distinguish the quality of Web services. There is a growing consensus that the Web service ‘revolution’ would not eventuate until trust related issues are resolved (Briman, 2006).

Currently, researches on trust management in SOEs are gaining an increasing momentum. Most of the studies focus on establishing trust between entities based on third-party platform or intermediary mechanism (Singh, 2004, 2005; Maximilien, 2002). Research results also show that reliable reputation systems have helped to increase user’s trust in the Web (Dellarocas, 2003). Online businesses including eBay and Amazon have made a great profit by using reputation systems, where the clients provide feedbacks to the quality of service (QoS) after each transaction, and the mathematical methods are used to generate the reputation scores for service providers. Although such a reputation model provides a certain security measure for transactions, it also contains typical malicious behaviors, such as providing dishonest opinions and collusion (Sungkeun, 2005). The reputation-based model in Maximilien (2005) requires human participation in the Web services and the agents that recommend trust information are assumed to be the trusted parties without considering their possible malicious behaviors. In addition, these approaches seldom consider the social relations among entities and preferences of the service requesters. However, in the real world we almost ask our trusted friends for their recommendations on products and services. Therefore, we make the following assumptions for the SOE based on the observations of the real world:

1. A participant in a SOE can act one or more roles: (1) As a service requester, (2) As a service provider, and (3) Or as both a requester and a provider. The service requester can select the most trustworthy service provider through some specific techniques.

2. Service requesters are more likely to accept recommendations from the participants who have similar preferences to them or from their friends in the social network than from those with whom they do not have any relationships.

3. The trust relations between two participants can be generated in two ways: (1) They share similar preferences, and (2) They had direct interactions in the past. A trust relation between participants is transitive and composable.


According to the points discussed, we present in the upcoming section, a trust-based service selection framework in a community based and centralized service oriented environment. With this framework, we propose a computational trust model, based on the social network, for quantifying and comparing the trustworthiness of web services. An experimental system is developed to simulate the trust model in SOEs with the entities which can act as both requesters and providers of services. Then, a local trust metric is proposed to test the simulated system and the trust model by propagating trust over the network which contains both good and malicious participants. Finally, we conduct a set of experiments to analyze and discuss the study results.
Efficient Transport Bindings for Web Service Messages
[www.igi-global.com/chapter/efficient-transport-bindings-web-service/31211?camid=4v1a](www.igi-global.com/chapter/efficient-transport-bindings-web-service/31211?camid=4v1a)

Discovering Knowledge Hidden in Big Data From Machine-Learning Techniques
[www.igi-global.com/chapter/discovering-knowledge-hidden-in-big-data-from-machine-learning-techniques/217856?camid=4v1a](www.igi-global.com/chapter/discovering-knowledge-hidden-in-big-data-from-machine-learning-techniques/217856?camid=4v1a)