A TRUST AND REPUTATION MODEL FOR WEB SERVICE SELECTION

Po-Ling Sun, Department of Information Management, National Chung Cheng University, Chia-Yi County, Taiwan, ROC, 886-5-2721500, bolin919@gmail.com
Cheng-Yuan Ku, Department of Information Management and Finance, National Chiao Tung University, Hsin-Chu City, Taiwan, ROC, 886-3-5712121#57413, cooper.c.y.ku@gmail.com

ABSTRACT

With many enterprises moving towards a service-oriented architecture (SOA), the web service is becoming a standard method of sharing data and functionality. Furthermore, web service and service-oriented architecture are being also adopted by enterprises as a competitive advantage to drive business revenues. However, with an increasing number of services providing similar functionalities, it becomes critical for service oriented computing (SOC) to discover the trustworthy services so as to best fit the business needs. Hence a good web service selection mechanism with consideration of trust and reputation is the key component for successful operation of SOC [6].

Up to now, very few research results take all possible security scenarios into consideration, so the designed trust and reputation models may not function well all the time. The accurate and robust trust and reputation management mechanism should be able to effectively handle all possible threats. Hence, based on our earlier review of security threats [7], an adaptive and integrated model of trust and reputation is proposed.

Keywords: web service selection, trust and reputation model, quality of service

INTRODUCTION

The Internet is so easily accessible to anyone, so it can be a really dangerous place. Therefore, how to discover the trustworthy web services is not an easy job as well. Actually, the online situations of variable behavior and conspiracy make this job even much harder. As described by [5], the reputation of service providers may change very quickly partially because of the variable behavior and the malicious cooperation from collusion agents. As well known, most of the trust and reputation mechanisms prove useless for malicious agents to behave in the above way.

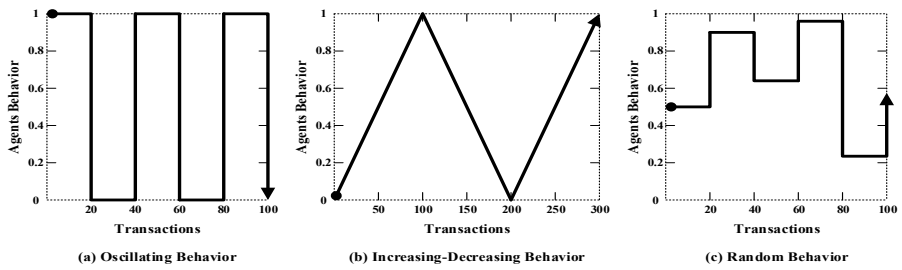

Figure 1 Varying Behavior [5]

Figure 1 shows various types of online behavior [5]. Thus, an effective trust and reputation model is really necessary for proper selection of web services.

THEORETICAL BACKGROUND

The major purpose of web service selection mechanism is to choose trustworthy service among a bunch of services with same or similar functions but with different QoS indexes. Therefore, the accurate assessment of QoS of every service from different web service providers acts as a set of important parameters for reference of purchase for online customers [2,3,4,6]. However, the dishonest service providers may provide inauthentic web services or manipulate the QoS data in order to obtain unjustified benefits [5,8].

It has already been found that the traditional way of rating provided by customers is not enough to indicate the real behavior of service providers in this increasingly complicated Internet. The malicious entities may cooperate to form a huge malicious group to build the fake reputation in community that is very difficult to differentiate [5,8]. As a result, how to assess the dynamic and complex relationship of online trust and reputation for Internet users is still a challenging issue [1].

METHODS

A trust relationship is the confidence association between entities within the social networks. We think this trust could be extended to those entities without direct linkage via the indirect connection of social networks. If the topology of social network for any user is identified, then a trust network of him/her with trust value could be calculated. Reputation is defined as an aggregated value of recommendations about the QoS of a service provider [1,8]. Based on the above-mentioned trust relationship, the adjusted reputation of QoS for some web service could be aggregated and weighted. By the way, we also think, in addition to the trust network, the reputation should be weighted by time. That's because the importance of recommendation information may decay as time goes by.

Then the direct evaluation and indirect information should be combined again to calculate the total and final assessment of QoS for some service we are interested in. Right now, the improvement of our method is still ongoing, other essential parameters may be added in this mechanism to handle any malicious possibility within Internet.

PLANNED VALIDATION

In order to verify the effectiveness of the proposed trust and reputation model, we will plan some experiments or simulations in which we consider two reasonable and realistic assumptions in the dynamic SOA collaboration environment. First, we will assume the normal and random behavior for service providers and consumers, so the performance of service providers/consumers will be modeled and evaluated as a collection of many different agents. It is very possible to adopt the Gaussian

distributions. Secondly, we may further categorize these dishonest entities into three sub-types: a) the badmouthing agents who tend to badly report the services of their competitors, b) the advertising agents who usually exaggerate the performance of their own services and c) uncertain agents who behave as good or bad guys according to the Bernoulli random variables. Based on those data obtained from simulation, we would like to discuss and validate the effectiveness and efficiency of the proposed model.

ACKNOWLEDGEMENT

This research is supported by MOST 103-2410-H-009-053-MY3 of Ministry of Science and Technology, Taiwan, R.O.C.

REFERENCES

[1] E. Chang, T. Dillon, and F. K. Hussain, *Trust and Reputation for Service-Oriented Environments: Technologies for Building Business Intelligence and Consumer Confidence*, John Wiley & Sons, Ltd, 2006.

[2] V. Diamadopoulou, C. Makris, Y. Panagis, and E. Sakkopoulos, Techniques to support web service selection and consumption with QoS characteristics. *Journal of Network and Computer Applications*, 31, 108-130, 2008.

[3] I. Djordjevic, T. Dimitrakos, N. Romano, D. Mac Randal, and P. Ritrovato, Dynamic security perimeters for inter-enterprise service integration. *Future Generation Computer Systems*, 23 (4), 633-657, 2007.

[4] Y. C. Liu and Y. B. Liu, A sort of web service selection strategy based on the fusion of QoS and service reliability. *International Journal of Computer Science Issues*, 10 (1), 414-420, 2013.

[5] F. G. Mármol and G. M. Pérez, Security threats scenarios in trust and reputation models for distributed systems. *Computers & Security*, 28 (7), 545-556, 2009.

[6] T. Rajendran, P. Balasubramanie, and Resmi Cherian, An efficient WS-QoS broker based architecture for web services selection. *International Journal of Computer Applications*, 1 (9), 79-84, 2010.

[7] Po-Ling Sun and Cheng-Yuan Ku, Review of threats on trust and reputation models, *Industrial Management & Data Systems*, 114 (3), 472-483, 2014.

[8] M. Tavakolifard and C. Almeroth, A taxonomy to express open challenges in trust and reputation systems. *Journal of Communications*, 7 (7), 538-551, 2012.