Fuzzy Approach for the Evaluation of Trust and Reputation of Services

Simone A. Ludwig, Venkat Pulimi, Andriy Hnativ
Department of Computer Science, University of Saskatchewan, Saskatoon, Canada
{ludwig,pulimi,hnativ}@cs.usask.ca

Abstract

A service-oriented environment has special characteristics that distinguishes it from other computing environments: (i) the environment is dynamic; (ii) the number of service providers is unbounded; (iii) services are owned by various stakeholders with different aims and objectives; (iv) there is no central authority that can control all the service providers and consumers; (v) service providers and consumers are self-interested. Given these special characteristics, the evaluation of trust and reputation is very important in such an open, dynamic and distributed environment. Therefore, a fuzzy-based trust and reputation approach using three trust sources was developed. Simulating the real world in which deception happens, an evaluation is performed showing the usefulness and robustness of the fuzzy approach by a comparison with a weighted approach.

1. Introduction

A service-oriented environment has special characteristics that distinguishes it from other computing environments: (i) The environment is dynamic - indicating that service providers are non-persistent and may become unavailable unpredictably. This means the environment will change over time as the system operates. The same principle is applied for service consumers. (ii) The number of service providers is unbounded. (iii) Services are owned by various stakeholders with different aims and objectives. There may be unreliable, insecure or even malicious service providers. (iv) There is no central authority that can control all the service providers and consumers. (v) Service providers and consumers are self-interested. In a service rich environment, it is necessary to provide support for automated service discovery. This is necessary to enable direct interaction between software sub-systems (acting as clients and servers) [1].

Due to the changing nature of service-oriented environments, the ability to locate services of interest in such an open, dynamic, and distributed environment has become an essential requirement. Traditional approaches to service discovery have generally relied on the existence of pre-defined registry services, which contain descriptions that follow some shared data model. Often the description of a service is also very limited in such registry services, with little or no support for problem-specific annotations that describe properties of a service.

One approach to select the "right" service is to use a Quality of Service (QoS) metric. This QoS metric can consist of attributes such as: execution time, price, reputation, reliability and availability [2].

Another approach is to select a service based on the notion of trust. Trust is a dynamic and complex concept in service transactions. The difficulty in measuring trust and predicting trustworthiness in service-oriented environments is a challenging problem. In order to tackle this problem, issues to consider include how to measure the willingness and capability of users and how to assign a concrete level of trust to a service or user [3,4].

There are three main approaches of trust in literature. The first approach of trust concerns the design of security protocols and mechanisms of interactions. This approach plays a role as a security instrument to provide a waterproof protection for the interaction between the system entities. The second approach concerns providing the system users with the ability to reason about the reliability, honesty and reputation of the other users. This approach acts as a social control instrument. It assumes that there are unwanted intruders in the system and it tries to identify them and prevent them from harming the other users. The third approach concerns the design of agreement driven transactions which bind the transaction parties with a legal agreement. The agreement describes the rules and obligations of each party, and defines a framework for monitoring agreement compliance at

978-1-4244-3597-5/09/$25.00 ©2009 IEEE

runtime. Therefore, this approach acts as a legal protection instrument.

In this paper, the focus lies on the second (provision of reasoning) and the third requirement (agreement of rules and obligations). A fuzzy-based trust model is designed to address these two requirements.

The remainder of this paper is as follows. Section 2 gives an account of related work in the area of trust and reputation. Section 3 describes our approach followed by an evaluation in Section 4. The conclusions of this research work are given in Section 5.

2. Related Work

Manifestations of trust are easy to recognize because we experience and rely on it every day, but at the same time trust is quite challenging to define because it manifests itself in many different forms and refers to a range of different problems and approaches. In the computer and information sciences literature, there has been much work and progress on defining trust since the first crystallization of this concept. Recent work on trust is motivated by applications in security, electronic commerce and social networks, which all may use trust in different ways.

A lot of research activity has been going on over the years in many application areas. We will only list a few approaches which have been proposed, starting with the work of Josang [5], who states that assessing trust becomes a problem in electronic transactions due to the impersonal aspects of computer networks. He proposes a scheme for propagating trust through computer networks based on public key certificates and trust relationships, and demonstrates how the resulting measures of trust can be used for making decisions about electronic transactions.

Page et al. [6] state that the importance of a Web page is an inherently subjective matter, which depends on the readers interests, knowledge and attitudes. But there is still much that can be said objectively about the relative importance of Web pages. In their paper they describe PageRank, a method for rating Web pages objectively and mechanically, effectively measuring the human interest and attention devoted to them. A comparison of PageRank with an idealized random Web surfer is done and presented.

Another approach, stating that situational details can have an impact on the trust that a trustor assigns to some trustee is discussed and formalized using functions for determining context-aware trust. A system implementing such functions takes into account the trustee's profile realized by quality attributes. Furthermore, the system is aware of some context attributes characterizing additional aspects of the trustee, of the trustor, and of the environment within they reside [7].

Fuzzy logic has been introduced in the area of Web services for the discovery or matching of services by Straccia [8] for Description Logics (DL), called SHOIN(D). They have introduced a fuzzy version of SHOIN(D) by defining fuzzy sets and fuzzy modifiers for DL.

Kuester et al. [9] are proposing a framework for automated service discovery, composition, binding and invocation on the web using fuzzy sets to capture user's preferences. This paper presents a service-description language and its associated matchmaking algorithms. Together they precisely capture requester preferences through fuzzy sets, express and use instance information for matchmaking, and deal efficiently with multiple effects.

Huang et al. [10] have developed a moderated fuzzy web service discovery approach by modeling subjective and fuzzy opinions and to assist service consumers and providers in reaching a consensus. It is an iterative approach by allowing further fuzzy opinions and preferences to be added to improve the precision of web service discovery.

In the area of service selection, which is also explored in this paper, Wang et al. proposed a fuzzy model for the selection of Quality of Service (QoS) aware web services. The model exploits fuzzy logic to locate and select the right service based on a customer's preference or satisfaction degree. The aim is to compute both functional and non-functional weightings of QoS criteria and to assist customers to make the right choice in selecting web services [11].

We propose a fuzzy-based trust approach based on three requirements as outlined in Section 3. Different trust sources have been taken to evaluate the overall trust of a service. The robustness of our approach will be evaluated by comparing the fuzzy-based trust approach with a weighted trust approach.

3. Fuzzy Approach

In order to develop a trust and reputation model, it should consist of the following properties [12]:

- It should take various different sources of trust information into account.
- Each service consumer should be able to evaluate their own trust.
- It should be robust against possible lying from service providers.

Fuzzy logic provides a simple way to arrive at a definite conclusion based upon vague, ambiguous, imprecise, noisy, or missing input information. Furthermore, fuzzy logic emulates how a person makes decisions and performs reasoning; however, fuzzy logic does it much faster. Therefore, a fuzzy-based trust and reputation model was devised. Our fuzzy trust model relies on three different trust sources as shown in Figure 1.

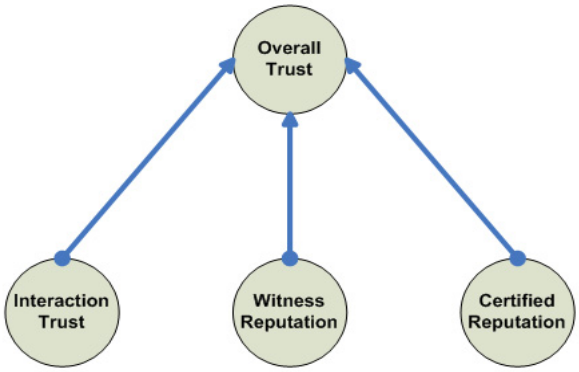

Figure 1. Components of overall trust evaluation

These three trust sources are: interaction trust, witness reputation and certified reputation. Interaction trust results from the past experience from direct interactions with a particular service. Witness reputation identifies witness accounts about a service's behavior. Certified reputation provides a reference by other users about a service's behavior.

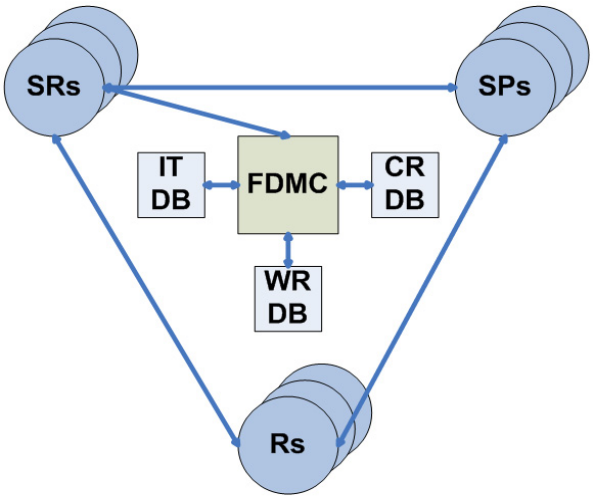

Figure 2. Trust architecture

It is important to combine a variety of alternative sources of trust information, especially in particular situations. For example, if a user has not interacted with a particular service before, it has no information to calculate its interaction trust. Therefore, witness and certified reputation are useful.

In general, a service-oriented architecture is comprised of the following components (as shown in Figure 2): Service requesters (SRs) which are the service consumers, service providers (SPs) which supply the services, and the registries (Rs) where all the information about the services and service providers is stored.

In addition, the interaction trust database (IT DB), the witness reputation database (WR DB) and the certified reputation database (CR DB) are used for our trust evaluation. The databases get populated with trust and reputation values after a service requester and a service provider interacted with each other. The service requester stores a trust value into the IT DB and also the WR DB, whereas the service requesters add and store trust values into the CR DB. These trust values stored in the three databases are then being used to calculate a value specifying how trustworthy one particular service is over other ones. This helps the service requester to choose the service with the highest expected trust value. When a service requester is looking for a trustworthy service, the fuzzy decision maker component (FDMC) is queried. It is the heart of this architecture as the trust evaluation takes place there and based on the evaluation a recommendation about a service is made to the service requester. It contains the fuzzy input sets, fuzzy output sets, fuzzy rules, and the fuzzy inference component. Based on the three different input trust values obtained from the three sources, the overall trust is evaluated.

4. Implementation

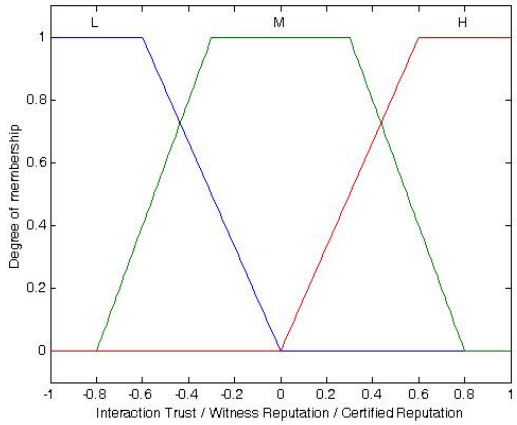

Figure 3. Input fuzzy sets for interaction trust, witness reputation and certified reputation

The fuzzy trust evaluation method uses three fuzzy sets for the input parameters and five fuzzy sets for the

output as shown in Figure 3 and 4 respectively. We have chosen triangle and trapezoid fuzzy sets as they provide an adequate representation of the given trust knowledge. These shapes also significantly simplify the process of computation.

The three inputs which are interaction trust, witness reputation and certified reputation consist of three fuzzy sets each which are low (L), medium (M) and high (H) with their corresponding membership values. The fuzzy sets for the inputs and the output were adaptively chosen and revised via an engineering process, in order to achieve a comparable evaluation between the weighted approach and the fuzzy approach.

The output fuzzy sets contain the five fuzzy sets very low (VL), low (L), medium (M), high (H) and very high (VH). The degrees of membership for these five fuzzy sets are shown in Figure 4.

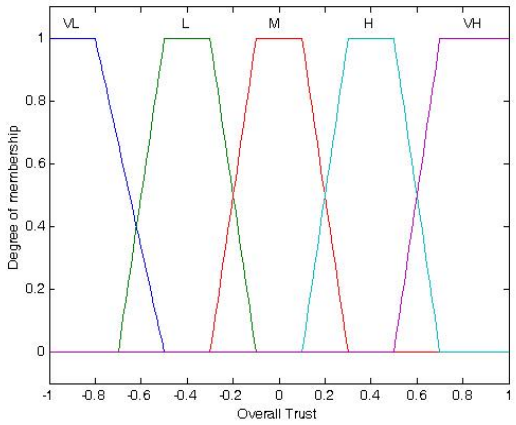

Figure 4. Output fuzzy sets

Twenty-seven rules are implemented as shown in Table 1. The first rule listed in the second row reads as follows: IF IT=L AND WR=L AND CR=L THEN OT=VL; i.e., if the interaction trust is low and the witness reputation is low and the certified reputation is low then the overall trust is very low.

We have used AND rules as our trust values are tightly coupled with one another, meaning that interaction trust, witness reputation and certified reputation are dependent on each other. OR rules and a combination of OR and AND rules are used for loosely coupled variables only.

The Mamdani inference method was used, and for the aggregation of the fuzzy values the centroid technique was exploited for the defuzzification. We have used the Mamdani inference, not the Sugeno inference technique, because it allows capturing the expert knowledge in a more intuitive, human-like manner. The drawback of the Mamdani method is that it is computationally more intensive; however, in our case, with a relatively small set of rules and only three input and one output variables, the Mamdani method is suitable and efficient.

IF IT	AND WR	AND CR	THEN OT
L	L	L	VL
M	L	L	L
L	M	L	L
L	L	M	L
M	M	L	L
L	M	M	L
M	L	M	L
H	L	L	L
L	H	L	L
L	L	H	L
L	M	H	M
L	H	M	M
M	L	H	M
M	H	L	M
H	L	M	M
H	M	L	M
M	M	M	M
H	H	L	H
L	H	H	H
H	L	H	H
H	M	M	H
M	M	H	H
M	H	M	H
M	H	H	H
H	H	M	H
H	M	H	H
H	H	H	VH

Table 1. Rules for fuzzy trust evaluation

5. Evaluation

In order to evaluate the robustness of the chosen fuzzy approach, a comparison with the weighted approach is conducted for cases in which service providers are deceiving users with wrong trust values. The deception can happen in both directions; service providers can either artificially increase or decrease their trust value.

The weighted trust calculation takes the average of all three trust sources i to obtain an overall trust value as such:

$$OverallWeightedTrust = \sum_{i=1}^{3} w_i \cdot trustValue_i$$

Assume the weight of each trust source w_i is equal, summing up to 1. The aim is to estimate the error rate

between the deceived trust values compared to the evaluation with the normal trust values.

For the evaluation, combinations of trust values in the range of -1 to +1 in steps of 0.1 are considered for all three trust sources and the overall weighted and the fuzzy trust values are calculated. For the sake of simplicity, we assume that only the witness reputation is biased. It undergoes negative and positive deception. The negative deception starts for all combined values by adding -0.1, -0.2, -0.3, -0.4 and -0.5 to the normal trust values, and similarly in steps of 0.1, 0.2, 0.3, 0.4 and 0.5 for positive deception. Finally, the overall weighted and fuzzy trust values were calculated and compared. In particular, for the normal trust values, the following test set was chosen:

```
testSetTrustNormal = [-1;-0.9;-0.8;
-0.7;-0.6;-0.5;-0.4;-0.3;-0.2;-0.1;0;
0.1;0.2;0.3;0.4;0.5;0.6;0.7;0.8;0.9;1
];
```

For the base evaluation, all three trust sources consisted of values from the `testSetTrustNormal` testset. This set was taken and the weighted average and the fuzzy values were calculated.

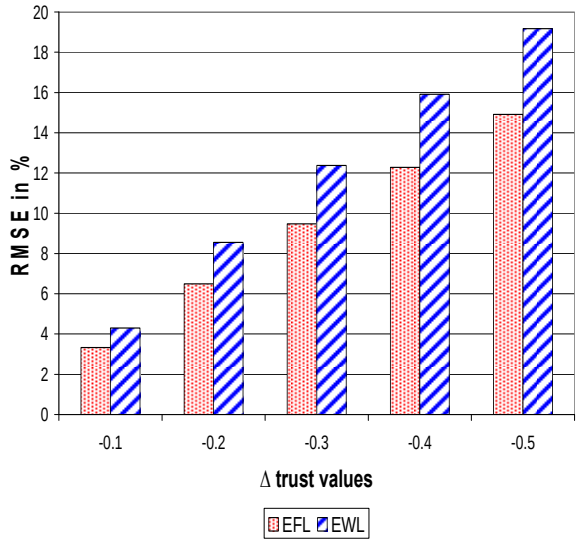

Figure 5. Comparison of RMSE for weighted estimation and fuzzy estimation for negatively biased trust values

Afterwards, the factor of deception was evaluated. The following test set shows a negative deception of trust values by a factor of -0.1.

```
testSetTrustLow = [-1;-1;-0.9;-0.8;
-0.7;-0.6;-0.5;-0.4;-0.3;-0.2;-0.1;0;
0.1;0.2;0.3;0.4;0.5;0.6;0.7;0.8;0.9];
```

Similarly, five different test sets ranging from -0.1 to -0.5 in intervals of 0.1 were created and evaluated. In order to evaluate the normal values with the deception values, the root mean square error (RMSE) was used. RMSE is a frequently-used measure of the differences between values predicted by a model or an estimator and the values actually observed, and is a good measure of accuracy.

Figure 5 shows the RMSE for five delta trust values. The dotted bars show the error rate of the fuzzy evaluation (EFL) and the striped bars show the error rates of the weighted evaluation (EWL). The fuzzy evaluation estimates the error rate between the normal evaluation trust values and the deceived trust values. Similarly, the weighted evaluation estimates the error rate between the normal evaluation trust values and the deceived trust values. The figure shows clearly that the error rates for the fuzzy evaluation are smaller than for the weighted evaluation. A factor of 0.771 is calculated.

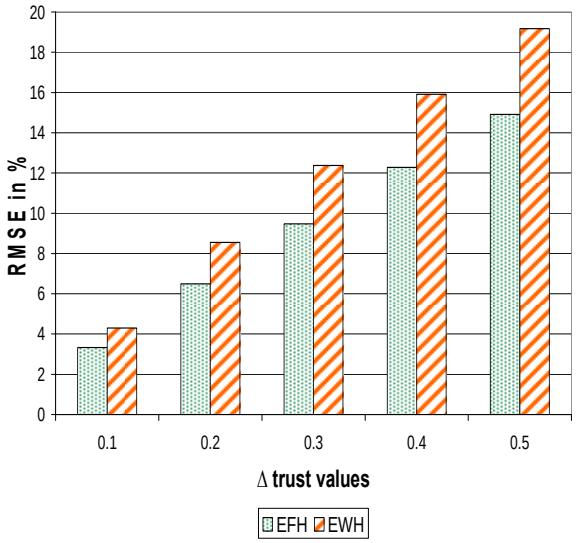

Figure 6. Comparison of RMSE for weighted estimation and fuzzy estimation for positively biased trust values

A similar evaluation was done for the positive deception of the trust values. This time the trust values were deceived in the positive direction, starting with a deception with an increase of +0.1 up to +0.5 in steps of 0.1. An example test set with positive deception of +0.1 is shown below:

```
testSetTrustHigh = [-0.9;-0.8;-0.7;
-0.6;-0.5;-0.4;-0.3;-0.2;-0.1;0;0.1;
0.2;0.3;0.4;0.5;0.6;0.7;0.8;0.9;1;1];
```

In Figure 6, the RMSE bars show the same trend compared to Figure 5. The weighted evaluation estimates the error rate (shown as the striped bars and denoted as EWH) between the normal weighted trust values and the deceived trust values, whereas for the

fuzzy evaluation the error rate of the fuzzy values (shown as the dotted bars and denoted as EFH) for the normal trust values compared to the deceived trust values are estimated. The figure shows that the error rates for the fuzzy evaluation are smaller than for the weighted evaluation by a factor of 0.771. As expected, the positively biased and the negatively biased trust graphs show the same error rates; therefore, we can conclude that the evaluation in both directions is symmetrical.

6. Conclusion

The evaluation of trust and reputation is a very important issue in an open, dynamic and distributed service-oriented environment. Due to the characteristics of service-oriented environments and the fuzzy nature of trust, a fuzzy-based trust and reputation approach was developed. The trust model takes interaction trust, witness reputation and certified reputation as the three input parameters and calculates an overall trust value as the output. From the comparison of the proposed approach with the weighted approach it is clear that in cases of deception, i.e. positively or negatively biased values, the fuzzy trust method outperforms the weighted method by a factor of 0.771. The fuzzy trust method allows the "deceived" trust value to be balanced out when deception occurs. This concludes that the fuzzy method is a robust and sensible approach to choose in environments where deception can occur.

Further work includes the development of a prediction method for deception, so that once deception is detected, the computed trust value can be adjusted automatically to the true valuation. This would decrease the error rate estimates drastically, especially in cases of larger deceptions. Furthermore, as the fuzzy sets were constructed by hand, an automatic construction method would be very useful. It can be envisioned that a genetic algorithm could be a good approach to construct the fuzzy input sets according to the domain the method is used in.

7. References

[1] S. A. Ludwig, O. F. Rana, "Performance Evaluation of Semantic Registries: OWLJessKB and instanceStore", Journal of Service Oriented Computing and Applications, vol. 2, no. 1, pp. 41-46, 2008.

[2] S. A. Ludwig and S. M. S. Reyhani, "Selection Algorithm for Grid Services based on a Quality of Service Metric", Proceedings of 20th International Symposium on High Performance Computing Systems and Applications (HPCS), Saskatoon, Canada, May 2007.

[3] E. Chang, P. Thomson, T. Dillon and F. Hussain, "The Fuzzy and Dynamic Nature of Trust", Lecture Notes on Trust, Privacy and Security in Digital Business, vol. 3592/2005, pp. 161-174, Springer, 2005.

[4] E. Chang, F. Hussain, and T. S. Dillon, "Fuzzy nature and dynamic trust modeling in service oriented environments", in Damiani, E. and Maruyama, H. (ed), Second Workshop on Secure Web Services (SWS), Nov 11 2005, pp. 75-83. Fairfax, USA.

[5] A. Josang, "Trust-based decision making for electronic transactions", Proceedings of the Fourth Nordic Workshop on Secure Computer Systems (NORDSEC), 1999.

[6] L. Page, S. Brin, R. Motwani, T. Winograd, "The PageRank Citation Ranking: Bringing Order to the Web", Technical Report, Stanford Digital Library Technologies Project, 1998.

[7] S. Toivonen, G. Lenzini, I. Uusitalo, "Context-aware Trust Evaluation Functions for Dynamic Reconfigurable Systems", Proceedings of the Models of Trust for the Web workshop (MTW), vol. 190, May 2006.

[8] U. Straccia, "A Fuzzy Description Logic for the Semantic Web", In Capturing Intelligence: Fuzzy Logic and the Semantic Web, Elie Sanchez, ed., Elsevier, 2006.

[9] U. Kuester, B. Koenig-Ries, M. Klein, M. Stern, "A Matchmaking-Centered Framework for Automated Service Discovery, Composition, Binding and Invocation on the Web", International Journal of Electronic Commerce (IJEC), Special Issue on Semantic Matchmaking and Retrieval, vol. 12 no. 2, 2007.

[10] C.-L. Huang, C.-C. Lo, K.-M. Chao, M. Younas, "Reaching consensus: A moderated fuzzy web services discovery method", Information and Software Technology, Volume 48, Issue 6, WAMIS 2005 Workshop, June 2006.

[11] P. Wang, K.-M. Chao, C.-C. Lo, C.-L. Huang, Y. Li, "A Fuzzy Model for Selection of QoS-Aware Web Services", IEEE International Conference on e-Business Engineering (ICEBE), 2006.

[12] T. D. Huynh, N. R. Jennings, N. Shadbolt, "Developing an integrated trust and reputation model for open multi-agent systems", In Proceedings of the 7th International Workshop on Trust in Agent Societies, pp. 62-77, New York, USA, 2004.