The Estimation of Trustworthy of Grid Services Based on Neural Network

Zhengli Zhai, Wei Zhang
Computer Engineering Institute, Qingdao Technological University
Qingdao 266520, P. R. China
{zhaizhl, zwq2000}@163.com

Abstract—Though research on the Grid Services has progressed at a steady pace, its promise has yet to be realized. One major difficulty is that, by its very nature, the Grid Service is a large, uncensored system to which anyone may contribute. This raises the question of how much credence to give each source. The concept and definition of trustworthy of Grid Service is given. Estimating trustworthy of Grid Services with the method of Neural Network from the aspect of trustworthy history sequence is proposed. The principle of the method, applicable Neural Network structure, Neural Network constructing, input standardization, training sample constructing, and the procedure of estimating trustworthy of Grid Services with trained Neural Network are presented. Experiments confirm that the methods with Neural Network are feasible and effective to estimate trustworthy of Grid Service, and do not put unreasonable expectations on users. We hope that these methods will help to move the Grid Service closer to fulfilling its promise.

Index Terms—Grid Services, Trustworthy, Estimation, Trustworthy History Sequence, Neural Network

I. INTRODUCTION

OGSA integrates Grid technology with Web Service and considers all (including resource) are services. A Grid Services is a software system designed to support interoperable machine-to-machine interaction over a network [1]. Grid Services are increasingly being used in daily life for electronic commerce, Web-based access to information and inter-personal interactions via electronic mail rather than voice or face-to-face, but there is still major concern about the trustworthiness of these services. There are no accepted techniques or tools for specification and reasoning about the trust. There is a need for a high-level, abstract way of specifying and managing trust, which can be easily integrated into applications and used on any platform. Typical applications requiring a formal trust specification include content selection for Web documents [2], medical systems [3], telecommuting [4], mobile code and mobile computing [5, 6], as well as electronic commerce [7-13].

Trust decisions are currently hard-coded into an application, which adds to the complexity of the application and the inability to adapt to changes in trust and lack of flexibility when setting up new relationships. A separation of the application’s purpose and its trust management framework will offer a more scalable and flexible solution for the distributed environment.

Trust is a vital component in every business transaction. Customers must trust that sellers will provide the services they advertise, and will not disclose private customer information (name, address, credit card details, purchases etc.). Trust in the supplier’s competence and honesty will influence the customer’s decision as to which supplier to use. Sellers must trust that the buyer is able to pay for goods or services, is authorized to make purchases on behalf of an organization or is not underage for accessing service or purchasing certain goods. Thus, for Internet commerce to achieve the same levels of acceptance as traditional commerce, trust management has to be an intrinsic part of e-commerce.

The migration from centralized information systems to internet-based applications will mean that transactions have to span a range of domains and organizations [14], not all of which may be trusted to the same extent. Inconsistencies in current trust relationships highlight the need for a flexible, general-purpose trust management system that can navigate these (possibly) complex trust domains. A domain may need to support a range of different trust relationships and hence be capable of supporting different types of security policy [15].

Trust is usually specified in terms of a relationship between a trustor, the subject that trusts a target entity, which is known as the trustee i.e. the entity that is trusted. Trust forms the basis for allowing a trustee to use or manipulate resources owned by a trustor or may influence a trustor’s decision to use a service provided by a trustee. Thus, trust can form an important factor in decision-making [16-18]. The level of trust has an approximate inverse relationship to the degree of risk with respect to a service or an e-commerce transaction [19, 20], but there has been very little work on using risk management frameworks for trust management or on the analysis of the exact relationship between risk and trust. In many current business relationships, trust is based on a combination of judgment or opinion based on face-to-face meetings or recommendations of colleagues, friends and business partners. However, there is a need for a more formalized approach to trustworthy establishment, estimation and analysis to support Grid Services, which generally do not involve human interaction.
Trust and reputation systems represent a significant trend in decision support for Grid Service provision. The basic idea is to let parties rate each other, for example after the completion of a transaction, and use the aggregated ratings about a given party to derive a trust or reputation score, which can assist other parties in deciding whether or not to transact with that party in the future. A natural side effect is that it also provides an incentive for good behavior, and therefore tends to have a positive effect on market quality. Reputation systems can be called collaborative sanctioning systems to reflect their collaborative nature, and are related to collaborative filtering systems. Reputation systems are already being used in successful commercial online applications. There is also a rapidly growing literature around trust and reputation systems, but unfortunately this activity is not very coherent [21].

With the widespread proliferation of Grid Services, Grid Services requester must correctly estimate Grid Services and select the appropriate one to use. We define the result from estimation of Grid Service as Grid Service trustworthy. Some works have been developed to solve this problem [22, 23]. However, the method used is both inefficient and unwise. In this paper, we propose an intelligent, feasible and effective method based on Neural Network to estimate trustworthy of Grid Service. So far as we know, it is an initiation.

Trustworthy can be obtained from experience of transaction with the Grid Service requester or from recommendation of others. The trustworthy obtained from experience of requester is surveyed for the following reasons:

- Trustworthy is context specific and multi-faced [21]. Accordingly, requester would be more interested in his or her own experience.
- In some cases, requester must monitor the trustworthy of Grid Services continually [24]. So the experience of requester own can describe the trustworthy of Grid Service exactly.
- Trustworthy directly obtained from experience of requester is the foundation of Grid Services trustworthy recommendation.

The experience of requester exchanging with Grid Service makes a Grid Service trustworthy history sequence. From the sequence, trustworthy that completely reflects the trustworthy status of Grid Service can be obtained by means of model identification. As Artificial Neural Network has the ability of model identifying [25], we can apply it to estimate trustworthy of Grid Service from trustworthy history sequence.

II. TRUSTWORTHY OF GRID SERVICE

There is considerable variation in the meaning of trust or trustworthy as used in the literature.

Trust is a complex subject relating to belief in honesty, truthfulness, competence, reliability etc. of the trusted person or service. There is no consensus in the literature on what trust is and on what constitutes trust management [19], though many research scientists recognize its importance [26]. The significance of incorporating trust in distributed systems is that trust is an enabling technology. Its inclusion will enable Internet commerce and seamless, secure agent-based applications. Despite the need to standardize trust and its related concepts, many researchers simply use and assume a definition of trust in a very specific way relating to topics such as authentication, or ability to pay for purchases. However, a few authors have tried to view trust in a generic way.

Kini and Choobineh [27] in their considerations on the theoretical framework of trust, examine it from the perspectives of personality theorists, sociologists, economists and social psychologists. They state that trust, as defined in the Webster dictionary, is:

- An assumed reliance on some person or thing. A confident dependence on the character, ability, strength or truth of someone or something.
- A charge or duty imposed in faith or confidence or as a condition of a relationship.
- To place confidence (in an entity).

They highlight the implications of these definitions and combine their results with the social psychological perspective of trust to create their definition of trust in a system – “a belief that is influenced by the individual’s opinion about certain critical system features”. Their discussion, though general in concept, concentrated on human trust in Electronic Commerce, but did not address trust between the entities involved in an E-Commerce transaction.

The European Commission Joint Research Centre defines trust as “the property of a business relationship, such that reliance can be placed on the business partners and the business transactions developed with them” [28]. This view of trust is from a business management perspective and offers an interesting analysis of what must be done to enable trust in E-Commerce. They state that the issues of the identification and reliability of business partners, the confidentiality of sensitive information, the integrity of valuable information, the prevention of unauthorized copying and use of information, guaranteed quality of digital goods, availability of critical information, the management of risks to critical information, and the dependability of computer services and systems (specifically the availability, reliability and integrity of infrastructure, the prevention of unauthorized use of infrastructure, guaranteed level of services and the management of risks to critical infrastructure) are key to the emergence of E-Commerce as a feasible commercial activity.

The Oxford Reference Dictionary states that trust is “the firm belief in the reliability or truth or strength of an entity”. A trustworthy entity will typically have a high reliability and so will not fail during the course of an interaction, will perform a service or action within a reasonable period of time, will tell the truth and be honest with respect to interactions and will not disclose confidential information. Competence is a better term
than strength for the environment related to services and computing system, i.e. an entity should be capable of performing the functions expected of it or the service it is meant to provide correctly and within reasonable timescales. Thus, trust is really a composition of many different attributes – reliability, dependability, honesty, truthfulness, security, competence, and timeliness, which may have to be considered depending on the environment in which trust is being specified.

Trust is a vast topic that involves trustworthy establishment, trustworthy management and security concerns. The lack of consensus with regards to trust has led authors to use the terms trust, authorization and authentication interchangeably. The outcome of a trust decision is based on many things such as the trustor’s propensity to trust, its beliefs and past experiences relating to the trustee.

Trustworthy management was proposed to solve the authorization problem in distributed environment where identifying strange requester is impossible, but traditional security models assume that system can identify requester effectively[29,30]. In Grid Services, requester faces the problem how to select strange Grid Service.

The trustor trusts the trustee to provide a service that does not involve access to the trustor’s resources. Note this may not be true of many services such as Grid Services that download applets and cookies, and so do require access to resources owned by the trustor.

Application service providers (ASPs) [31-33] are prime examples of entities that would require service provision trust to be established. Currently, in these domains, trustworthy is often an unstated implication of establishing a relationship, which is difficult to enforce or monitor. Mobile code and mobile agent based applications obviously must trust the execution environment provided by the remote system (provision of service trustworthy) but the execution environment should not be damaged by the mobile code (access to resources trustworthy).

There are some examples of service provision trustworthy:

- I trust a film recommendation service to only recommend films that are not pornographic.
- I trust website xyz to provide information that is non-offensive.
- I distrust sexy-Susan website.

The above examples are a form of confidence trust in that the trustor has confidence in (or specifically distrusts) the standard of service provided by the service provider. This type of trustworthy maps into a form of access control, which is subject-based, in which the subject is only permitted to access trusted services. This type of access control can be implemented by some Web browser as a means of screening sites visited by children [2, 34].

Some forms of service trustworthy relate to competence of the trustee:

- I only trust fourth year students who have an aggregate A grade to do this project.
- I will only purchase PCs from IBM Company.

A trustor’s trust in the competence of the trustee’s ability to provide a service differs from confidence trust in that, confidence applies to entities the trustor will use and competence applies to entities that perform some action on behalf of the trustor.

Another form of service trustworthy relates to reliability or integrity of the trustee. In E-Commerce and E-Banking, the customer trusts the vendor or bank to support mechanisms that will ensure that passwords are not divulged and to prevent transactions from being monitored. The vendor or bank is also trusted to maintain the privacy of any information such as name, address and credit card details, which it holds about the customer. Examples of this form of service trustworthy are:

- I will store these critical files on QQ’s network hard disk (as it has a RAID file system and it is archived every 2 hours). Note that in this case the trustee does have access to the trustor’s resources.
- I trust the News Center to email me an electronic newspaper every morning before 8 am.
- I trust my internet bank not to divulge my name and address to companies for electronic marketing.

Certification of Trustees is a type of trustworthy is based on certification of the trustworthiness of the trustee by a third party, so trustworthy would be based on a criteria relating to the set of certificates presented by the trustee to the trustor. Certificates are commonly used to authenticate identity or membership of a group in Internet applications [35, 36]. This may imply competence if the identity is a well-known organization. However, professional certification is a common technique used to indicate competence in the medical world, commerce and engineering, so it could be applied to Grid Services.

There are some examples of trustee certification:

- I trust Dr. Tom’s medical advice site as he is registered with the BMA.
- I will only use downloaded software updates, which have Microsoft certificates.
- I trust the identity of anyone authenticated by the Kerberos server in my domain.

Note that the certification authority is in fact providing a trust certification service, so this is a special form of service provision trustworthy but involves a third party in establishing the trustworthy.

Summarized as the above, in order to get the function of service, requester Agent often has to send sensitive data to Grid Service. From the viewpoint of requester, trustworthy of Grid Service should include security, privacy and QoS [37]. These concepts have some overlap [38], so we use the main aspects to define trustworthy of Grid Service, which is shown in the following:

- Availability: Whether the Grid Service is ready for immediate use.
- Integrity: How the Grid Service maintains the
The correctness of the interaction in respect to the source.

- Confidentiality: Only authorized people or systems can access protected data.
- Privacy: Data of requester should not be revealed to other people or systems without the permission of the requester.
- Performance: Measured in terms of throughput and latency.

**Definition 1 Trustworthy of Grid Service** is the general estimation result of availability, integrity, confidentiality, privacy, and performance of Grid Service. It can be described with the product of these aspects as Eq.(1).

\[ t = a \times i \times c \times v \times p \]  

(1)

Meansings of these symbols are listed in the Table I.

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Meaning</th>
<th>Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>t</td>
<td>Trustworthy</td>
<td>[0,1]</td>
</tr>
<tr>
<td>a</td>
<td>Availability</td>
<td>0 or 1</td>
</tr>
<tr>
<td>i</td>
<td>Integrity</td>
<td>0 or 1</td>
</tr>
<tr>
<td>c</td>
<td>Confidentiality</td>
<td>0 or 1</td>
</tr>
<tr>
<td>v</td>
<td>Privacy</td>
<td>0 or 1</td>
</tr>
<tr>
<td>p</td>
<td>Performance</td>
<td>[0,1]</td>
</tr>
</tbody>
</table>

Definition 1 is used to calculate trustworthy of one transaction between requester and Grid Service. In the experiments presented in Section IV, Eq.(1) will be used to calculate trustworthy of Grid Service.

### III. ESTIMATION OF TRUSTWORTHY WITH NEURAL NETWORK

#### A. Principle of trustworthy estimating with Neural Network

Let there is a trustworthy history sequence \( A \), \( A = (a_1, a_2, ..., a_s) \), \( a_i \) is the trustworthy of the \( i \)th exchanging between requester and Grid Service. It can be calculated by Eq.(1). Let there is a complex system \( S \) that can produce a trustworthy \( T \) from \( A \). Let’s denote it as \( T = S(A) \). In order to estimate trustworthy \( T \) from \( A \) with Neural Network, \( A \) must be designed. Let’s denote it as \( T' = N(A) \). In order to make sure that the output of Neural Network satisfies the requirement, formula \( \frac{1}{2} (T' - T) \) \( < \varepsilon \) should be hold. Where, \( \varepsilon \) denotes a small positive number as needed.

The principle of trustworthy estimation network is shown in Fig.1.

![Fig.1 Principle of trustworthy estimating with neural network](image-url)

The constructing procedure of Neural Network \( N \) is shown in the following:

**Step 1** Get a set of input and output of \( S \) as training samples;

**Step 2** Design a Neural Network \( N \) and train it with the training samples;

**Step 3** If the precision of \( N \) meets the requirement, constructing is end, otherwise do step 2 again.

**Definition 2 Trustworthy history sequence** \( A \) is a history record of trustworthy of Grid Service which the requester has traded with. It can be denoted with an ordered \( n \) tuple, \( A = (a_1, a_2, ..., a_s) \), \( a_i \) is the trustworthy of the \( i \)th transaction between requester and Grid Service.

**Definition 3 Active trustworthy history sequence** \( B \) is the recent trustworthy history sequence. It can be denoted with an ordered \( m \) tuple \( B = (b_1, b_2, ..., b_s) \). Let \( A = (a_1, a_2, ..., a_s) \), then \( B = (a_{\text{last}}, a_{\text{last-1}}, ..., a_1) \). Let’s note it as \( B = \angle (A, m) \).

**Definition 4 Constrictive trustworthy history sequence** \( C \) is the subsection average of active trustworthy history sequence. Let \( B = (b_1, b_2, ..., b_s) \), then constrictive trustworthy history sequence of \( B \) is \( C = (c_1, c_2, ..., c_s) \). Let’s note it as \( C = \langle (B, k) \rangle \). \( k \) is the number of input of Neural Network.

Let \( s = \frac{m}{k} \),

When \( i \times s \leq m \), \( c_i = \frac{1}{s} \sum_{j=m}^{i} b_{i-(m-i+1)} \);

When \( i \times s > m \), \( c_i = \frac{1}{r} \sum_{j=m}^{i} b_{j-m} \), \( r \) is arithmetic compliant of \( m \) and \( k \).

In order to estimate trustworthy with Neural Network, requester must record the active trustworthy history sequence \( B \) at least.

The Artificial Neural Network that can estimate trustworthy from Grid Services trustworthy history sequence should be a multi-input and one-output Neural Network with model identifying ability. BP Neural Network can be applied for this purpose [25]. The structure of BP Neural Network is shown as Fig.2.

© 2010 ACADEMY PUBLISHER
Every node (except input node) in Neural Network has multiple inputs and one output, but this one output can affect many other nodes. It can be described as Fig.4. The relationship of node’s input and output can be denoted with formula \( y = f(\sum_{i=1}^{n} \omega_i x_i - \theta) \). Where, \( y \) is output;
\( f \) is effect function; \( \theta \) is threshold; \( \omega_i \) is the connection weight of the \( i \)th input; \( x_i \) is the \( i \)th input; \( n \) is the count of input node. The Neural Network calculates from the input layer to the out layer. The output of out layer is the output of the Neural Network. \( f \) can be selected within threshold function, line function and Sigmoid style function, e.g. hardlim, purelin, tansig, etc [25]. The number of layers, number of nodes, \( \omega \) and \( \theta \) can be selected through experiment.

The number of input \( k \) presents the length of trustworthy history sequence which Neural Network can deal with. In order to balance between precision and efficiency, \( k \) can not be too big. Because \( k \) is limited and \( n \), length of trustworthy history sequence \( A \), is not limited, \( A \) should be standardized.

### B. Constructing Training Sample and Neural Network Training

There are two sources to get training sample. One is the real trustworthy history of Grid Service, and another is the one which is specially designed. The procedure of getting training sample from real Grid Service is shown as follows:

**Step 1** Get trustworthy history sequence \( A \) of Grid Service;

**Step 2** Make active trustworthy history sequences \( B \) from \( A, B = \angle(A, m) \);

**Step 3** Make constractive trustworthy history sequence \( C \) from \( B, C = \angle(B, k) \);

**Step 4** \( C \) and \( T \) can make a training sample \( (C, T) \), where, \( T \) is the given trustworthy of Grid Service \( x \).

The samples obtained from real Grid Service make the result of Neural Network close to the actual trustworthy. The samples specially designed can lead output of the Neural Network to puniness or encourage some action model.

The procedure of designing special sample is to construct trustworthy history sequence according to \( k \), the number of input of Neural Network, and to give a trustworthy.

### C. Trustworthy Estimation

If there is a trained Neural Network, the trustworthy estimation is very simple. The procedure is shown in the following:

**Step 1** Get the trustworthy history sequence \( A \);

**Step 2** Make active trustworthy history sequence \( B \) from \( A, B = \angle(A, m) \);

**Step 3** Make constractive trustworthy history sequence \( C \) from \( B, C = \angle(B, k) \);

**Step 4** Using \( C \) as input of Neural Network, the output of Neural Network is trustworthy.

From the procedure we can see that the complexity of time to estimate trustworthy with trained Neural Network is \( O(k) \).

### IV. Experiments

In order to estimate the effect of the method proposed in this paper, we developed three data storage Grid Services and a client Agent on Microsoft .Net platform. The first one acts on a random trustworthy by dropping service request randomly. The second one drops service request periodically with little random. The third one periodically drops service request completely.

Client Agent requests these data storage Grid Services to store data for it separately, and check the data status randomly [24]. Check results are calculated by Eq.(1). The first 300 check results are used to train the Neural Network. Then the trained Neural Network was used to estimate the trustworthy of Grid Service in the next interactions. The estimating results are presented in Fig.5.
Grid Services acting on a little random trustworthy and Neural Network can ideally estimate the trustworthy of trustworthy. In Fig. 5(b) and Fig. 5(c), we can see that estimate trustworthy of Grid Services acting on a random trustworthy in Jane’s ability to determine who is trustworthy to verify identity [29]. In Abdul-Rahman’s system, John’s trustworthy in Jane, and John’s trustworthy in Jane’s ability to determine who is trustworthy, are separate, though discrete and only qualitatively valued [39]. Such a separation would be interesting to consider in our framework as well.

The analog of belief combination for the World Wide Web is estimating the quality and relevance of Web pages. Information retrieval methods based solely on the content of the page (such as TFIDF [40]) are useful, but are outperformed by methods that also involve the connectivity between pages [41-43].

Gil and Ratnaker [44] present an algorithm that involves a more complex, though qualitative, form of trustworthy based on user annotations of information sources, which are then combined. One shortcoming of such an approach is that it derives values of “trustworthiness” that are not personalized for the individual using them, requiring all users – regardless of personal values – to agree on the credibility of sources. Secondly, by averaging the statements of many users, the approach is open to a malicious attacker who may submit many high (or low) ratings for a source in order to hide its true credibility. By employing a network of trustworthy, our approach surmounts both of these difficulties (assuming users reduce their trustworthy in a user that provides poor information).

Kamvar et al’s EigenTrust algorithm [45] computes global trustworthy as a function of local trustworthy values in a peer-to-peer network, EigenTrust computes a global trustworthy value (similar to PageRank) and emphasizes security against malicious peers who aim to disturb this calculation.

Pennock et al. looked at how Web-based artificial markets may combine the beliefs of their users [46]. Social network algorithms have been applied to network of trustworthy in order to identify users with high network influence [47, 48]. Applying the same methods to the Grid Service’s network of trustworthy may prove fruitful in identifying useful contributors, highly respected entities, etc. Also in a similar skeleton is the ReferralWeb project, which mines multiple sources to discover networks of trustworthy among users [49]. Also interesting is collaborative filtering [50], in which a user’s belief is computed from the beliefs of users she is similar to. This can be seen as forming the network of trustworthy implicitly, based solely on similarity of interests.

VI. CONCLUSION

If it is to succeed, the Grid Services must address the issues of information quality, relevance, inconsistency and redundancy. This is done on today’s Web using algorithms like PageRank, which take advantage of the link structure of the Web. This paper proposes the concept of trustworthy of Grid Service. The formal definition with availability, integrity, confidentiality, privacy, and performance are given. We apply Neural Network to Grid Services trustworthy estimating for the first time. The principle of the approach is described. The Neural Network constructing, input standardization, training sample constructing, and the procedure of estimating trustworthy of Grid Services with trained Neural Network are described. Experiments show that Neural Network can ideally estimate the trustworthy of Grid Services act on a little random trustworthy and exactly estimate trustworthy of Grid Services act on a periodically trustworthy.

The trustworthy schemes cover a wide range of application and are based on many different type’s mechanisms, and there is no single solution that will be suitable in all contexts and applications. When designing or implementing new systems, it is necessary to consider the constraints and the type of information that can be used as input parameters.

ACKNOWLEDGMENT

This research was partially supported by National Natural Science Foundation of China (No. 60673160, 60673053, 90718011).

REFERENCES


Zhengli Zhai was born in County Fei, Shandong Provence, P. R. China, in 1972. Zhengli received the B.Sc. degree in applied mathematics from Shandong University, M.Sc. degree in the software and theory of computer from Shandong University of Science and Technology and Ph.D. degree in computer application technology from the University of Science and Technology Beijing in 1994, 2003 and 2007, respectively.

After worked in College of Information, Linyi Normal University from 1994 to 2003, he is currently an Associate Professor at Qingdao Technological University and Deputy Director of the Software Engineering Teaching and Research Group there. His current research interests include Grid Computing, Petri net theory and its application, Algorithm Design and Analysis, Multi Agent System, etc.

Dr. Zhai has authored over 30 fully refereed publications in above research fields. He was Session Chair of the 2008 IEEE International Conference on Automation and Logistics (IEEE ICAL 2008) and reviewer of IEEE Transactions on Systems, Man and Cybernetics, Part A: Systems and Humans.

Wei Zhang was born in County Dingzhou, Hebei Provence, P. R. China, in 1971. Wei Zhang received the B.Sc. degree in electrical equipment from Hebei University of Technology, M.Sc. degree in computer application technology from Hebei University in 1994, 2002 respectively.

After worked in College of Information, Agriculture University of Hebei from 1994 to 2002, she is currently an Associate Professor at Qingdao Technological University and Deputy Director of the Common Computer Teaching and Research Group there. Her current research interests include Computer Network Security, Grid Computing, etc.

Prof. Zhang has authored over 20 fully refereed publications in above research fields.