2011

Trust-based service provider selection in service-oriented environments

Minjie Zhang
University of Wollongong, minjie@uow.edu.au

Yi Mu
University of Wollongong, ymu@uow.edu.au

Q. Bai
University of Wollongong, quan@uow.edu.au

Trust-based service provider selection in service-oriented environments

Abstract

Nowadays, agent-based service-oriented systems have been widely applied in many complex domains such as e-markets, grid systems, e-governments and service-oriented software systems, cross Internet and organizations. In this kind of service-oriented multi-agent systems, service providers (agents) and service consumers (agents) are autonomous entities and can enter and leave environments freely. How to select the most suitable service providers according to the requested services from consumers in such an open and dynamic environment is a very challenging issue. The objectives of this paper include (1) studying the challenging issues of trust-based service provider selection, (2) investigating the current approaches of trust models for service provider selection in general service-oriented multi-agent systems, and (3) developing new solutions for service provider selection to overcome several limitations in current approaches.

Disciplines

Physical Sciences and Mathematics

Publication Details

Su, X., Zhang, M., Mu, Y. & Bai, Q. (2011). Trust-based service provider selection in service-oriented environments. International Journal of Computer Science and Network Security, 11 (10), 1-9.

Trust-based Service Provider Selection in Service-oriented Environments

Xing Su†, Minjie Zhang†, Yi Mu†, and Quan Bai††

†School of Computer Science and Software Engineering, University of Wollongong, NSW, Australia
††School of Computing and Mathematical Sciences, Auckland University of Technology, Auckland, New Zealand

Summary
Nowadays, agent-based service-oriented systems have been widely applied in many complex domains such as e-markets, grid systems, e-governments and service-oriented software systems, cross Internet and organizations. In this kind of service-oriented multi-agent systems, service providers (agents) and service consumers (agents) are autonomous entities and can enter and leave environments freely. How to select the most suitable service providers according to the requested services from consumers in such an open and dynamic environment is a very challenging issue. The objectives of this paper include (1) studying the challenging issues of trust-based service provider selection, (2) investigating the current approaches of trust models for service provider selection in general service-oriented multi-agent systems, and (3) developing new solutions for service provider selection to overcome several limitations in current approaches.

Key words:
Multi-agent systems, Service-oriented environments, Trust and reputation, Service provider selection.

1. Introduction

In the past twenty years, Multi-Agent Systems (MASs) have attracted much attention from researchers in computer science, information technology, engineering and so on. Because of the abilities of autonomous learning [1, 2], decision making [3, 4], collaborative problem solving [4, 5], MASs have been widely employed for different applications in open and dynamic environments in recent years. The agent-based service-oriented systems are one of these applications. In a general service-oriented Multi-Agent System (MAS), agents use their services as source to interact with other agents in the system and the agents that offer the service are called service providers while the agents that request the services are called service consumers. In a common interaction among agents, a service consumer first sends a service request to other agents in the system, and then the service providers that can offer the requested service can reply the request. Most of time, there are more than one service providers replying the service request. In this situation, how to choose the best service provider based on the service request is an important issue for most of service-oriented MASs. Normally, we select the best service provider based on the 'trust' of the service provider.

'Trust' is one of important research issues in MASs [6-8]. The definition of trust proposed by Ramchurn *et al.* in paper [9] is that *'Trust is a belief an agent has that the other party will do what it says it will (being honest and reliable) or reciprocate (being reciprocative for the common good of both), given an opportunity to defect to get higher payoffs'*. Therefore, the trust can reflect the ability, future performance, and willing of a service provider for the requested service.

However, special characteristics of the service-oriented MASs create challenges for developing trust-based approaches and strategies for service provider selection. These characteristics can be summarized as follows:

1. **Local views**
   It is hard for an agent in service-oriented MASs has complete information of other agents or a global view about the whole system. The scale of most service-oriented MASs is big and it is also hard or impossible for an agent in such a system to have all of the newest local and global information of the system.

2. **Dynamic environments**
   An agent can freely join and leave the system at any time. The number of agents in the system can very from time to time. This will affect an agent decision making during provider selection

3. **Decentralized nature**
   Normally, there is no a centralized controller to control the decision process of all agents in these system. This feature makes difficult for an agent to dynamically get the newest global information about the whole system situations. Therefore, designing a centralized controller for the system is nearly impossible. Moreover, there is no central database designed for this kind of systems to store the global information. The information is separatively stored in individual agent systems.

Manuscript received October 5, 2011
Manuscript revised October 20, 2011

4. **Complex relationships**
   The relationships among agents in service-oriented MASs are complicated. In a service-oriented MAS, an agent may have multiple roles such as a service consumer, a service provider or a third party, which means that an agent can offer a service, request a service, and evaluate a service. Because of the multiple roles, an agent can have different relationships with other agents. If two agents offer the same service, they may have a completion relationship. If an agent offers a service to another agent, they can have a collaboration relationship.

5. **User-preference service requests**
   The service requirements can be different from case to case. Even if two service consumers request for the same service, they often pay attention to different aspects of the service.

The aim of this paper is to investigate the current trust models for service provider selections, give a new classification of trust models based on their control mechanisms, and propose potential solutions for service descriptions based on rich context, trust information aggregation, and group trust evaluation by the consideration of the characteristics of service-oriented environments, described above

The rest of paper is organized as follows. In Section 2, several trust models are reviewed and analysed in detail. Then, some remaining challenging issues that need to be dealt with is summarized in Section 3. In Section 4, our solutions are introduced to deal with these issues. Finally, the paper is concluded in Section 5.

2. Related Work

Currently, many trust models have been proposed to help a service consumer to evaluate trust values for potential service providers. In this section, we aim to review and analyze several important representative trust models.

2. 1 A New Classification of Current Trust Models

In order to clearly review the representative trust models, we propose a new classification for current trust models based on the view of control mechanisms used in trust models as shown in Fig. 1

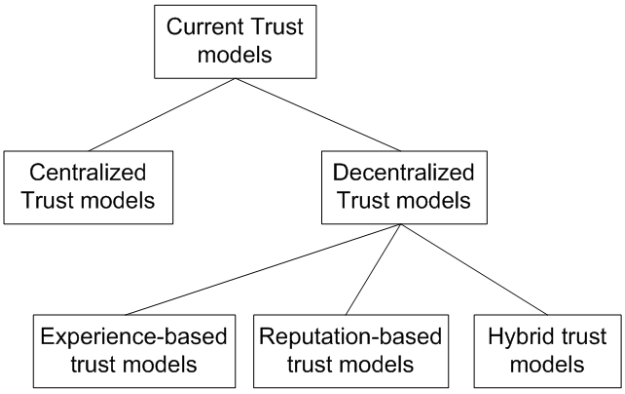


Fig. 1 A new classification of current trust models.

Based on control mechanisms, trust models can be classified into centralized trust models and decentralized trust models. In current literatures, there are more decentralized trust models than centralized models. We further classify the decentralized models into three subcategories, which are experience-based trust models, reputation-based trust models and hybrid trust models.

The advantages of the proposed classification can be outlined as follows.

1. **Balance**
   Although there are less centralized trust models than decentralized models, the centralized trust models still play important roles in real world applications. For example, one of famous centralized trust models is eBay trust model which is widely used in many online transition and auction systems.

2. **Clarity**
   The control mechanism in a trust model is a clear mark for classifying current trust models, since we can easily identify what kind of the system control mechanism a trust model uses.

3. **Relevance to this research topic**
   In this paper, we mainly focus on trust models for service provider selection in service-oriented MASs. Because of the characteristics of the MASs and service-oriented environments, it is hard for a centralized controller to be employed in service-oriented MASs. Based on this classification, we pay much attention on the deep investigation in decentralized trust models and focus on the detail reviews of important models in next section, which are close to this research.

2. 2 Representative Trust Models

In this section, several important trust models are reviewed and analyzed in detail based on the new classification proposed in Subsection 2.1.

Centralized trust models

A centralized trust model generally has a centralized controller to control interactions among agents and to store the trust information of the system. Since service-oriented MASs are decentralized in nature, the centralized control mechanism cannot fit the characteristics of MASs and service-oriented environments in most current applications.

Most of the centralized trust models [10-15] were proposed in the early stage of the trust model development, which ever played or still play an important role in some real world applications or provide basic foundations for the development of new trust models.

The eBay trust model is an example of these models, which has been widely used in online electronic commerce systems including eBay [15], Amazon [16], OnSale [17] and so on. The major features of this type of trust models are simple and easy to use. The eBay trust model only uses historical experience from interaction partners to deduce the trust value of a user. In eBay trust model, after a transition, all of the users (consumers and providers) participating in the transition need to report their feedbacks about partner users in the format of a single value. Then, a centralized unit can dynamically update the trust values for the corresponding users based on the feedbacks. Next time, a new user can make decision about whether a partner can be trusted to do business with based on the updated rating retrieved from the system for this partner. For example, after a transition, the users participating the transition need to rate trust values for each other within the range [-1,1], where -1 indicates a fully negative trust while 1 represents a totally positive trust on a participant, respectively. Then, the feedbacks are sent to the central trust management unit. These feedbacks are summed up with the historical trust values of the corresponding users in a time period (mostly six months). After that, the newest trust values for corresponding users can be obtained and stored by the centralized management unit. Thus, the trust value of a user in eBay trust model can accurately reflect the average performance of a user in a historical period. However, the limitations of eBay trust model can be analyzed as follows.

1. The trust value of a user in eBay trust model is represented by a single value, which can only indicate the trustworthiness of a user. From this value, a user cannot discover any other useful information (i.e. context, situations). Therefore, it is relatively hard for a user to accurately predict the future behaviors of the host of the trust value.

2. The newest trust value of a user is obtained by averagely summing up the trust values of the user in a time period. Therefore, the updated trust value can only reflect the general performance of a user in a time period instead of the newest or recent performance. This mechanism can cause some kinds of malicious behaviors. For example, a user may offer good products for a period of time. However, in recent transitions, the quality of products offered by the user becomes bad. Although the user gets bad ratings for its bad quality products, with the accumulation of its historical good behaviors, another user cannot find great changes in trust value of the user until it offers bad products for a long period of time.

3. The eBay trust model does not consider noisy ratings for users. For example, although a user can get a very good product from its transition partner, the user can deliberately give its transition partner a low rating without any punishment on the user's malicious behaviors.

In summary, the eBay trust model gives us a basic and simple idea on how to evaluate the trust for a user. However, it is hard for eBay trust model to be widely employed in service-oriented MASs.

Another important centralized trust model is the SPORAS trust model proposed by Zacharia and Maes [11]. Being different with the eBay trust model, SPORAS introduced several new mechanisms to overcome the limitations of eBay trust model. For example, SPORAS employed a learning function for updating trust values of agents. Therefore, the trust value of an agent can realistically reflect the recent performance of the agent. SPORAS also introduced the following mechanisms to ensure the accuracy of trust value of agents.

1. New agents in SPORAS can only start with a minimum trust value.

2. The trust value of a user who already had transitions with other agents never falls below the trust value of a new user.

3. After a transaction, the trust values of the involved agents need to be updated according to the feedbacks offered by their partners.

4. Agents with very high trust values can only have very small rating changes after updating.

5. Trust values in former periods need to be discounted according to time, by which the system can ensure that the trust value can reflect the recent performance of the corresponding agent.

From above mechanisms, we can see that the first and second mechanisms can avoid an agent with a bad reputation leaving the system to refresh its bad reputation with a new reputation and identity. The fifth mechanism considers the recency factor of the trust value of an agent. However, although the above mechanisms can overcome some limitations of eBay trust model, the SPORAS has its own problems. For, example, it does not consider the relationships between agents, which may lead to inaccurate ratings. For example, if the agents involved in a transition have collaboration relationships, they may give higher ratings than real values for each other and if the agents involved in a transition have competition relationships, they may give lower ratings than real values for their competitors.

Decentralized trust models

Being different with centralized trust models, a decentralized trust model does not have a centralized controller to control all of agents' behaviors and to manage trust information [8, 18-20]. From this consideration, decentralized trust models are more suitable and encouraged to be applied in service-oriented MASs than centralized trust models. We give brief reviews in experience-based trust models, reputation-based trust models and hybrid trust models, respectively.

(1) Experience-based trust models

In experience-based trust models, an agent evaluates the trust value for a potential partner based on its former direct interactions with the partner or its observation experience of other agents' interaction with the potential partner. The advantages of experience-based trust models are that the trust information is reliable and easy to be obtained, since the experience can directly come from the agent itself. Mostly, the reliable trust information from direct experience needs a number of interactions between two agents. If the scale of most service-oriented MASs is big and the members of these systems are dynamic, it is hard for an agent to have direct interaction or observation experience with most of agents in a system. Moreover, even if an agent wants to use a service offered by a familiar agent, it is possible that the familiar agent might be not in the system at that time. Another important problem in experience-based trust models is that if a system allows the interaction between two agents to be observed by other agents, the system should offer some security mechanisms to protect the privacy of interacting agents.

Sen and Sajja proposed a trust model [21] based on probabilistic calculations of trust values given by a number of agents including both providers and consumers. In their model, surrounding agents of an interaction pair can observe the interaction between the service consumers and providers. Then, the observed service provider's trust information from both the participants and the observing agents is updated using a reinforcement learning rules. When a new consumer needs the reputation of the corresponding service provider, the surrounding agents and the former interaction participants can give the latest reputation of the potential service provider. Their model introduced another example for using direct experience, i.e. the observation experience. The observation mechanism can greatly increase the trust knowledge of an agent on other agents. In Sen and Sajja's model, the interacting agents can also be observed by surrounding agents, which can lead to some security problems in interaction.

Currently, few trust models that only use direct experience as the trust information source. But the direct experience still plays an important role in trust evaluation, since the direct experience is the most reliable trust information source and is also easy to be gained. Many trust models use both the direct experience and the witness information to evaluate the trust values for potential partners.

(2) Reputation-based trust models

In reputation-based trust models, an agent evaluates the trust value for a potential partner based on the witness information of other agents (referees), which may directly or indirectly have interaction with the potential partner before. In some situations, reputation is not very reliable information, since we need to consider the relationships between the potential partner and referees. If the relationship between a referee and the potential partner is collaboration, the referee may give higher reputation value for the potential partner than the real trust value. In contrast to collaboration, if the relationship between the referee and potential partner is competition, the referee may give a relatively lower reputation value for the potential partner. By this consideration, the reputation trust is more complex than the direct experience.

The most famous reputation-based model for trust calculation in recent years is the Certified Reputation (CR) model proposed by Huynh *et al.* [22]. In the CR model, an agent's reputation is derived from the references of the third parties, which had previous interaction experiences

with the agent (provider) before. A provider can collect and present such references to service consumers in order to be trusted by them. Since the CR model allows consumers to evaluate trust values of providers themselves without using a central controller, it can be adapted in a wide range of open and dynamic environments such as service-oriented environments. However, there are two major limitations in the CR model. Firstly, in the CR model, a service is represented by a single item and the evaluation of the service given by a referee is represented by a single value. In the real world, it is hard or even impossible to use a single value to represent complex contexts related to a service [23]. A service provider's performance should be evaluated from different aspects such as speed, cost, quality, reliability etc. In addition, the evaluation result may also depend on the service request and the preferences of consumers. Secondly, the CR model only focuses on the trust evaluation for an individual service based on a single provider, so it cannot handle the problem of group trust evaluation based on multiple providers.

(3) Hybrid trust models

Hybrid trust models use both direct experience and reputation as the trust information source. Currently, most of trust models use both of direct experience and reputation as the information source.

J. Sabater and C. Sierra proposed a famous model, called REGRET, in 2001 [24]. In principle, the REGRET evaluates the trust value of a potential provider from three dimensions which are the individual dimension, the social dimension and the ontological dimension. The individual dimension is the direct experience of the service provider offered by a service consumer who had an interaction with the provider before. The social dimension is the reputation of a group which a service provider belongs to. The ontological dimension represents the reputations of different aspects of the services offered by the provider. Based on above comprehensive considerations, REGRET trust model can have an accurate trust evaluation for a potential provider.

3. Challenging Issues for Trust Model Development

Although many trust models from different considerations and perspectives have been proposed to solve service provider selection problem, there still some issues that need to be solved in current trust models.

3.1 Trust Information Retrieval

If a service consumer wants to find the trust information of a potential service provider, the service consumer often has two choices which are the direct experience with the provider or the reputations of the provider evaluated by third parties. If the service consumer has direct interaction with the potential service provider before, it is very lucky for the service consumer to use the former experience. However, it is not very often for a service consumer to have such experience. Therefore, most of time, the service consumer needs the reputations from third parties. However, searching for reputations of a potential service provider also leads to new problems which are:

1. How to effectively search for the useful trust information in the system, since the information is stored in individual agents.

2. Whether the third parties want to share the trust information with the service consumer, since most of agents are self-interested in most of service-oriented systems.

3. Whether the trust information offered by the third parties can realistically reflect the behaviors of the potential service provider, since the third parties may have different relationships with the potential service provider.

3.2 Trust Information Aggregation

If a service consumer collects a number of trust information for a potential service provider, how to summarize all of the collected trust information to generate the trust value for a potential service provider is also a challenging task, since different third parties may have different views on the same potential service provider.

3.3 Trust Information Description

If an agent has the trust information of another agent, how to quantify this trust information and make the information can be exchanged with other agents and understood by other agents is a challenging issue.

3.4 Full Context Representation

Most of trust models evaluate the trust of a potential service provider for a service request from the reputations offered by the former service consumers to the same service. This evaluation method may neglect the difference between the current and former service requests in terms of the context of the service. For example, in the CR model, a service is represented by a single item and the evaluation of the service given by a referee is represented

by a single value. In the real world, it is hard or impossible to use a single value to express complex contexts related to a service [23]. In contrast, a service provider's performance can be evaluated from different aspects such as speed, cost, quality, reliability etc. In addition, the evaluation results may also depend on constrains of a particular service, as well as the preferences of service consumers.

3.5 Group Trust Evaluation

Most of current trust models are developed to evaluate the trust values of individual service providers. However, in recent years, many complex service requests from service consumers cannot be handled by single services and a group of services from different service providers need to combine together with certain structures and workflows to satisfy these service requests [25, 26]. Therefore, the trust models focusing on the trust evaluations for single service providers cannot deal with the group trust evaluation problem, since the structure and relationships among group members also play important roles on the trust value of the overall service offered by a group. Therefore, how to choose a group of services for a service consumer has become a new challenge for service provider selection.

4. Our Solutions

In this section, we propose our solutions to address challenging issues listed in Section 3.

4.1 Trust Information Retrieval

To deal with the trust information retrieval problem, we borrow the concept of the reference store way proposed by the Certified Reputation (CR) model [22] to solve the problem. In the CR model, the reputation of a service provider which was ranked by the former service provider is encoded and stored by the service provider itself. By using this mechanism, if a service consumer wants to know the reputation of a potential service provider, the consumer does not need to search the system to find the third parties who has ever interact with the service provider before and asks for the reputation for the service provider and the service provider can offer the reputation by itself. Moreover, the service provider would be willing to offer the reputation of itself. By using this mechanism, the trust models can solve the trust information retrieval problem with lots of time and labor saving.

4.2 Full Context Representation

In general, a service can be described by a number of attributes such as price, time, quality, etc. For different requests, the priority on different attributes of the same service can be different. In order to deal with the relationships between attributes and their corresponding priorities, we make a service description in a formal way.

Suppose there are *n* attributes used to describe a requested service and each attribute is in a requested priority as the condition to complete the service. The service can be represented by *n* attributes and their corresponding priorities, respectively.

A *service description* (*SDes*) is the formal description of a service. *SDes* is defined in the following matrix format.

$$SDes = \begin{pmatrix} A_1 & A_2 & A_3 & \dots & A_n \\ W_1 & W_2 & W_3 & \dots & W_n \end{pmatrix}$$

where A_i indicates the i^{th} attribute; W_i is the priority value of A_i and $\sum_{i=1}^{n} W_i = 1$.

4.3 Trust Information Aggregation

To deal with the trust information aggregation problem, the final trust value of a potential service provider can be divided into several attributes and each attribute has a trust value. A service can be represented as follows.

$$\left(T_{att1}, \quad T_{att2}, \quad T_{att3}, \quad ...., \quad T_{attn}\right)$$

where T_{atti} represents the trust value of the i^{th} aspect.

Then, we assign priority values for each attribute according to the importance of the aspect as follow.

$$\left(P_{att1}, \quad P_{att2}, \quad P_{att3}, \quad ...., \quad P_{attn}\right)$$

where P_{atti} represents the priority value of the i^{th} attribute. Moreover, the sum of the priority values of all attributes in a service is 1, which means $\sum_{i=1}^{n} P_{atti} = 1$.

Finally, the trust and the priority values of all of the aspects need to be summarized as follow.

$$T_{Final} = \sum_{i=1}^{n} P_{atti} \times T_{atti}$$

where T_{Final} represents the final trust value of a potential service provider, and T_{atti} and P_{atti} represent the trust value and the priority value of the i^{th} attribute, respectively.

4.4 Group Trust Evaluation

To deal with group trust evaluation problem, we propose a mechanism which can describe the structure and workflow of a service group, develop a formula which can calculate the trust value of a group with dependency relationship among services, and introduce a concept which can evaluate the efficacy of a service group for a requested service.

By using the full context representation way to represent a service, we propose a group service description $GSDes$ as a $m \times n$ matrix, where m is the number of the individual services in a group and n is the number of attributes in service request. $GSDes$ is defined by the following matrix.

$$GSDes = \begin{pmatrix} A_1 & A_2 & A_3 & \dots & A_n \\ P_{11} & P_{12} & P_{13} & \dots & P_{1n} \\ P_{21} & P_{22} & P_{23} & \dots & P_{2n} \\ \dots & \dots & \dots & \dots & \dots \\ P_{m1} & P_{m2} & P_{m3} & \dots & P_{mn} \end{pmatrix}$$

where A_i indicates the i^{th} attribute of the requested service. The i^{th} row (excluding the first row) in the matrix represents the priority distribution on a pervious service completed by the corresponding group member and P_{ij} represents the priority value on the j^{th} attribute of the requested service on that service, where P_{ij}, if the pervious service dose not contain the j^{th} attribute; otherwise P_{ij} is in-between [0, 1], where 0 and 1 represent the highest and lowest priority values, respectively. By using Equation 4, the comprehensive ability of a service group can be described.

To describe the dependency relationship between two services in a service group, we develop the following formula:

$$FT_{ij} = T_{ij} - \frac{\sum_{k=1}^{n} \lambda i_j \cdot (1 - FT_{kj})}{n}$$

where n represents the number of the individual services which the i^{th} service depends on, T_{ij} is the trust value of the i^{th} individual service on j^{th} attributes shown in the reference report and FT_{kj} is the final trust value of the k^{th} dependency service on j^{th} attributes, and λ_{ij} is the dependency degree of the i^{th} individual service depending on the k^{th} dependency service.

To evaluate the efficiency of a service group, we introduce the concept of functionality coverage $FCov$, which can be defined as a vector, $FCov=<ACov_1, ACov_2, ACov_3 \dots ACov_i>$, where $ACov_i$ is a value in-between [0, 1], which represents the functionality coverage value of a service group on i^{th} attribute in the service request. $ACov_i$ can be calculated based on the information in $ACov_i$ as follows.

$$ACov_i = \frac{m - MS_i}{m}$$

where $ACov_i$ represents the functionality coverage value of a service group on i^{th} attribute of the requested service, m represents the number of the individual services in a group and MS_i represent the number of `$m$' (i.e. how many members cannot cover the $i^{th}$ attributes) in the $i^{th}$ column of the matrix $GSDes$. If the functionality coverage on $i^{th}$ attribute is `0', we can say that this service group is not suitable to conduct the requested service.

4. Conclusion

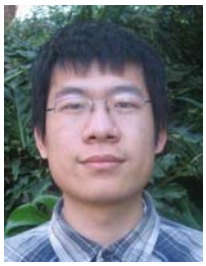
In this paper, we discussed the challenges for service provider selection in service-oriented environment and introduced a new classification of trust models for provider selection. Several important trust models were reviewed and analyzed. The potential solutions to meet current challenges in the development of trust models for service provider selection were proposed.

The main contributions of our solutions includes that (1) a rich context service description to represent a service by dividing a service into different attributes and priority values, (2) a trust information aggregation way by consideration of the different attributes of a service and their priority values, and (3) a group trust evaluation way by considering the structure and workflows of a service group, the dependency relationships between services in a service group, and efficiency of a service group.

In the future, we mainly focus on the improvement of our algorithm and formulas to make the trust evaluation more accurate.

References

[1] Bennett, K.P. and E. Parrado-Hernandez, The interplay of optimization and machine learning research. JOURNAL OF MACHINE LEARNING RESEARCH, 2006. **7**: p. 1265-1281.
[2] Ferber, J., Multi-agent systems: an introduction to distributed artificial intelligence. 1999, Harlow: Addison-Wesley.
[3] Milan, Z., Multiple criteria decision making: Eight concepts of optimality. Human Systems Management, 1998. **17**(2): p. 97.
[4] Jennings, N.R., On agent-based software engineering. ARTIFICIAL INTELLIGENCE, 2000. **117**(2): p. 277-296.
[5] Avouris, N., A. Dimitracopoulou, and V.F. Komis, C., OCAF: an object-oriented model of analysis of collaborative problem solving, in Proceedings of the Conference on Computer Support for Collaborative Learning: Foundations for a CSCL Community. 2002: Boulder, Colorado. p. 92--101.
[6] Conner, W., et al., A trust management framework for service-oriented environments, in Proceedings of the 18th international conference on World wide web. 2009: Madrid, Spain. p. 891--900.
[7] Chang, E., F. Hussain, and T. Dillon, Fuzzy nature of trust and dynamic trust modeling in service oriented environments, in Proceedings of the 2005 workshop on Secure web services. 2005, ACM: Fairfax, Virginia. p. 75--83.
[8] Khosravifar, B., et al., Maintenance-based trust for multi-agent systems, in Proceedings of The 8th International Conference on Autonomous Agents and Multiagent Systems. 2009: Budapest, Hungary. p. 1017--1024.
[9] Ramchurn, S., D. Huynh, and N. Jennings, Trust in multi-agent systems. The Knowledge Engineering Review, 2004. **19**: p. 1-25.
[10] Foner, L., Yenta: A multi-agent, referral-based matchmaking system, in Proceedings of the First International Conference on Autonomous Agents (Agents'97). 1997, ACM Press: Marina Del Rey, CA. p. 301--307.
[11] Zacharia, G., A. Moukas, and P. Maes, Collaborative reputation mechanisms for electronic marketplaces. Decision Support Systems, 2000. **29**: p. 371-388.
[12] Zacharia, G. and P. Maes., Trust Management Through Reputation Mechanisms. Applied Artificial Intelligence, 2000. **14**: p. 881-907.
[13] Ma, M. and C. Meinel, A Proposal for Trust Model: Independent Trust Intermediary Service (ITIS). in Proceedings of the IADIS International Conference WWW/Internet 2002 (ICWI'02). 2002: Lisbon, Portugal. p. 785-790.
[14] Golbeck, J., COMPUTER SCIENCE: Weaving a Web of Trust. Science, 2008. **321**: p. 1640--1641.
[15] eBay. http://www.ebay.com. accessed on 16th August 2011.
[16] Amazon. http://www.amazon.com. accessed on 16th. August 2011.
[17] OnSale. http://www.onsale.com. accessed on 16th August 2011.
[18] Marsh, S., Formalising Trust as a Computational Concept. 1994, University of Stirling.
[19] Huynh, T., N. Jennings, and N. Shadbolt, FIRE: An Integrated Trust and Reputation Model for Open Multi-Agent Systems, in Proceedings of the 16th European Conference on Artificial Intelligence (ECAI'04). 2004: Valencia, Spain. p. 18--22.
[20] Singh, M., Trust as Dependence: A Logical Approach, in Proceedings of the 10th International Conference on Autonomous Agents and Multia-agent Systems (AAMAS'11). 2011: Taipei, Taiwan.
[21] Sen, S. and N. Sajja, Robustness of reputation-based trust: Boolean case, in Proceedings of the first international joint conference on Autonomous agents and multiagent systems (AAMAS'02). 2002: Bologna, Italy. p. 288-293.
[22] Huynh, T., N. Jennings, and N. Shadbolt, Certified Reputation: How an Agent Can Trust a Stranger, in Proceedings of the fifth international joint conference on Autonomous agents and multiagent systems (AAMAS'06). 2006: Hakodate, Japan. p. 1217-1224.
[23] Sensoy, M. and P. Yolum, A Context-Aware Approach For Service Selection Using Ontologies, in Proceedings of the 5th international joint conference on Autonomous agents and multiagent systems (AAMAS'06). 2006: Hakodate, Japan.
[24] Sabater, J. and C. Sierra, REGRET: reputation in gregarious societies, in Proceedings of the fifth international conference on Autonomous agents. 2001: Montreal, Canada. p. 194 - 195.
[25] Vogiatzis, G., I. MacGillivray, and M. Chli, A probabilistic model for trust and reputation, in Proceedings of the 9th International Conference on Autonomous Agents and Multiagent Systems (AAMAS'10). 2010, International Foundation for Autonomous Agents and Multiagent Systems: Toronto Canada. p. 225--232.
[26] Tang, J., S. Seuken, and D. Parkes, Hybrid transitive trust mechanisms, in Proceedings of the 9th international joint conference on Autonomous agents and multiagent systems (AAMAS'10). 2010: Toronto. Canada. p. 233--240.



Xing Su received the B.S. degree in School of Software Engineering from Beijing University of Technology, China, in 2007. He is currently working toward to the M.S. degree under the supervision of A/Prof. Minjie Zhang and A/Prof. Yi Mu. His research interest is artificial intelligence and agent-based multi-agent systems.

Minjie Zhang is an Associate Professor in the School of Computer Science and Software Engineering and the Director of Intelligent System Research Group in the Faculty of Informatics, at University of Wollongong, Australia. She received her BSc. degree from Fudan University, China in 1982 and the PhD degree in Computer Science from the University of New England, Australia in 1996. Her research interests include distributed artificial intelligence, multi-agent systems, agent-based simulation and modeling in complex domains, grid computing, and knowledge discovery and data mining.

Yi Mu received his PhD from the Australian National University in 1994. He currently is an associate professor, Head of School of Computer Science and Software Engineering and the co-director of Centre for Computer and Information Security Research at University of Wollongong, Australia. His current research interests include network security, computer security, and cryptography. He has published over 260 research papers. Yi Mu is the editor-in-chief of International Journal of Applied Cryptography and serves as associate editor for nine other international journals. He is a senior member of the IEEE and a member of the IACR.

Quan Bai currently is a lecturer at the School of Computing and Mathematical Sciences, Auckland University of Technology, New Zealan. He received his PhD (2007) and MSc (2002) from the University of Wollongong, Australia, and graduated with double bachelor's degree (2002) from Tianjin University, China. After he received his PhD, Quan worked as a Postdoctoral Research Follow for the University of Wollongong, Australia (2007-2009), and for the Commonwealth Scientific and Industrial Research Organisation (CSIRO), Australia (2009-2011). Quan's research interests are mainly focussed on Intelligent Systems, Knowledge Discovery and Service-Oriented Computing. He has published more than 40 research papers in related fields.