2009 International Conference on Advanced Information Networking and Applications Workshops

Social Network-based Trust for Agent-based Services

Jamal Bentahar[1], Babak Khosravifar[1], and Maziar Gomrokchi[1]
[1]Concordia Institute for Inf. Sys. Eng., Concordia University, Canada
$bentahar@ciise.concordia.ca, b\_khosr@encs.concordia.ca,$
$m\_gomrok@encs.concordia.ca$

***Abstract*— In service-oriented environments, reputation-based service selection is gaining increasing prominence. We propose in this paper a social network-based approach to model and analyze trust when a given service, called customer service or customer, should select another service, called provider service or provider, in a composition scenario. Trust is modeled as a game between customer and provider services and represented in the network through two types of nodes and labelled edges linking customer nodes to each other and customer nodes to provider nodes. To analyze the different situations using a game-theoretic and mechanism design representation, each service is associated to a rational agent where decisions are based on the gaining utilities. This allows us to capture, assess and analyze the possible strategies in such a game. An overall trust assessment is provided and some interesting properties are discussed. Some simulation results are also presented.**

I. Introduction

The emerging service-oriented architecture holds out the promise of making applications smoothly interoperate and their components loosely coupled. Many research projects have been launched to address different issues of this architecture, particularly service discoverability, composability, autonomy, context awareness and security [8], [10], [15], [16]. In the particular context of service selection for composite purposes, trust is a fundamental selection criterion [9], [13], [14]. Trust is essential in service settings to provide a social control in service interaction and composition [14]. It is defined as "*the trustfulness of a trustor: the extent to which the trustor is willing to take the risk of trust being abused by the trustee*" [1]. Trust is also the measure of willingness that the trustee will fulfill what he agrees to do and computed by considering direct interaction experiences with the trustor and collecting suggested ratings from others (i.e. witnesses) [7].

Modeling, computing and analyzing trust in this context is a challenging issue. The reason is that services have dynamic behaviors and continuously new services appear and some old services become obsolete. We propose in this paper a new trust model for service selection based upon social network analysis to capture the emergence of trust via service networks where nodes are services and edges are the possible existing links between them. Social network analysis is a rich model in conceptualization and analysis. It provides a powerful set of metaphors, concepts and techniques for designing, modeling and analyzing complex distributed situations [1].

In our framework, services in a social network are considered as members of a community. Thus, if services are informed regularly about the behavior of other services via the network, trust will grow among these services. The idea is to allow a given service, called *customer service or customer*, to assess the trust of another service, called *provider service or provider*. To assess provider's trust in such a setting, we propose two techniques exploiting the existing links: 1) direct assessment technique where an edge exist between the customer and provider, which means the customer have had transactions with the provider; 2) indirect assessment technique where other customer services, which are supposed to be linked to the provider, are solicited to share the experiences they have had with that provider. These two techniques are combined according to the importance of direct and indirect transactions in the network.

Beyond using social network metaphor, we model trust among services as a game using game theory and mechanism design techniques [2]. Game theory aims to model situations in which multiple players engage in interactions and affect each other's outcomes. Mechanism design provides techniques to design game rules in order to achieve a specific outcome such as truthfulness. Using a game-theoretic approach to mechanism design allows us to analyze the properties of our trust game aiming at encouraging participant services to reveal the truth about their past experiences with a given provider. The idea is to model services as rational agents seeking to maximize the utility they can gain by participating in the game.

This paper aims at advancing the state-of-the-art in trust for service selection. It proposes two main contributions: 1) modeling and analyzing trust for service selection using social networks; and 2) providing the rules of a trust game satisfying interesting properties such as *incentive compatibility*, which means the best strategy is truth-telling. In Section II, we present our framework based on social network structure and provide computational techniques to evaluate services' trust. In Section III, we analyze our framework using social network analysis and model trust using game theoretical mechanism design. Different strategies and their properties are discussed in this section. Section IV provides a brief related work and discusses some simulation results comparing our framework to some existing proposals. Section V concludes the paper.

II. A Social Network Representation for Trust Evaluation

In this section, we formalize the trust game between customer services and provider services as a social network.

978-0-7695-3639-2/09 $25.00 © 2009 IEEE
DOI 10.1109/WAINA.2009.56

Each customer service c_i is linked to a set of customers it knows and a set of provider services it has interacted with in the past. The issue is how a customer c_i can evaluate providers to select the best one. A direct evaluation of a provider p_j is possible if the customer had enough transactions with that provider. Three elements are used to characterize the relationship between the customer and provider: 1) how much the customer trusts the provider: $Tr_{c_i}^{p_j}$; 2) the number of past transactions: $NT_{c_i}^{p_j}$; and 3) the time recency of the last transactions: $TiR_{c_i}^{p_j}$. If the direct evaluation is not possible because the past history between c_i and p_j is not enough to obtain an accuracy evaluation, the customer uses the social network to get information about the provider from other customers that potentially know the provider and accept to share their experiences. The information gathered from another customer c_k is dealt with considering: 1) how much c_i trusts c_k: $Tr_{c_i}^{c_k}$; 2) the number of past interactions: $NI_{c_i}^{c_k}$; and 3) the time recency of the last interactions: $TiR_{c_i}^{c_k}$. Formally, we define a social network for service selection as follows:

***Definition** 1: A social network for service selection is a tuple $\langle C, P, \longrightarrow_{cc}, \longrightarrow_{cp}\rangle$ where C is a set of customer services, P a set of provider services, $\longrightarrow_{cc} \subseteq C \times \mathbb{R}^3 \times C$ is a ternary relation (for labelled edges linking customers) and $\longrightarrow_{cp} \subseteq C \times \mathbb{R}^3 \times P$ is a ternary relation (for labelled edges linking customers to providers).*

We use the usual notation for the labelled edges: if $c_i, c_k \in C$ and $v \in \mathbb{R}^3$, then $(c_i, v, c_k) \in \longrightarrow_{cc}$ is written as $c_i \xrightarrow{v}_{cc} c_k$. In the same line, we write $c_i \xrightarrow{v}_{cp} p_j$ instead of $(c_i, v, p_j) \in \longrightarrow_{cp}$. Our social network for service selection has two types of nodes: type 1 for customer services and type 2 for provider services and two types of edges: type 1 for edges between customers and type 2 for edges linking customers to providers. The edges of type 1 represent friendship relations in the network, while edges of type 2 capture business relationships. The existence of an edge of type 1 $c_i \xrightarrow{v}_{cc} c_k$ means that c_i knows (is friend of) c_k such that: $v = (Tr_{c_i}^{c_k}, NI_{c_i}^{c_k}, TiR_{c_i}^{c_k})$. The existence of an edge of type 2 $c_i \xrightarrow{v}_{cp} p_j$ means that c_i had transactions with p_j such that: $v = (Tr_{c_i}^{p_j}, NT_{c_i}^{p_j}, TiR_{c_i}^{p_j})$. We note that there is no edges in this social network between providers. This does not mean that there is no social link between providers, but only the existing links (which could be collaborations or competitions) are not used in our framework.

The direct evaluation of a provider p_j by a customer c_i is based on the ratings c_i gave to p_j for each past interaction (r_l) combined with the importance of that interaction (w_l) and its time recency. Let n be the number of total transactions between c_i and p_j ($n = NT_{c_i}^{p_j}$), equation 1 gives the formula to compute this evaluation.

$$DTr_{c_i}^{p_j} = \frac{\sum_{l=1}^{n}(w_l.TiR_{c_i}^{p_j}.r_l)}{\sum_{l=1}^{n}(w_l.TiR_{c_i}^{p_j})} \quad (1)$$

To perform the indirect evaluation, the customer c_i solicits information about the provider p_j from other customers c_k such that there is an edge $c_i \xrightarrow{v}_{cc} c_k$ in the social network. The set of these customers c_k is denoted $\mathcal{T}_{c_i}$. The equation computing the indirect trust estimation is given by equation 2.

$$ITr_{c_i}^{p_j} = \frac{\sum_{c_k \in \mathcal{T}_{c_i}} wTr_{c_i}^{c_k}.Tr_{c_k}^{p_j}.TiR_{c_k}^{p_j}.NT_{p_j}^{c_k}}{\sum_{c_k \in \mathcal{T}_{c_i}} wTr_{c_i}^{c_k}.TiR_{c_k}^{p_j}.NT_{p_j}^{c_k}} \quad (2)$$

where $wTr_{c_i}^{c_k} = Tr_{c_i}^{c_k}.NI_{c_i}^{c_k}.TiR_{c_k}^{c_i}$

To compute $Tr_{c_i}^{p_j}$, the direct and indirect evaluations are combined according to their proportional importance. The idea is that the customer relies, to some extent, on its own history (direct trust evaluation) and on consulting with its network (indirect trust evaluation). This merging method considers the proportional relevance of each trust assessment, rather than treating them separately. To this end, c_i assigns a contribution percentage value for the trust assessment method (ω for direct trust evaluation and $1-\omega$ for indirect trust evaluation).

The value ω is obtained from equation 3. Basically, the contribution percentage of each approach in the evaluation of p_j is defined regarding to: (1) how informative the history is in terms of the number of direct transactions between c_i and p_j and their time recency; and (2) how informative and reliable the consulting customers are from c_i's point of view. Therefore, consultation with other agents is less considered if the history represents a comparatively higher entropy value, which reflects lower uncertainty.

$$\omega = \frac{\ln(Tr_{c_i}^{p_j}.NT_{c_i}^{p_j}.TiR_{c_i}^{p_j})}{\sum_{c_k \in \mathcal{T}_{c_i}} \ln(Tr_{c_i}^{c_k}.NI_{c_i}^{c_k}.TiR_{c_i}^{c_k})} \quad (3)$$

Respecting the contribution percentage of the trust assessments, c_i computes the trust value for p_j using equation 4.

$$Tr_{c_i}^{p_j} = \begin{cases} \omega.DTr_{c_i}^{p_j} + (1-\omega).ITr_{c_i}^{p_j} & \text{if } \omega \leq 1 \\ \omega.DTr_{c_i}^{p_j} & \text{if } \omega > 1 \end{cases} \quad (4)$$

Generally, the merging method is used to obtain the most accurate trust assessment. However, after a number of transactions, customers should analyze the quality of the received services regarding to what is expected (represented here by $Tr_{c_i}^{p_j}$) and what is actually performed (so-called observed trust value $\widehat{Tr}_{c_i}^{p_j}$). To this end, an adjustment trust evaluation should be periodically performed. The idea is to learn from past experiences, so that witnesses providing bad trust values, which are far from the observed one, will be removed from the list of potential witnesses in the future. This can be represented by the following equation:

$$\min_{c_k \in \mathcal{T}_{c_i}} |Tr_{c_k}^{p_j} - \widehat{Tr}_{c_i}^{p_j}| \quad (5)$$

III. Social Network and Game theory Analysis

To analyze our social network for service selection, many parameters described in the literature about social networks could be considered. A detailed list of such parameters are presented in [1]. For space limit, we consider only four parametrs and provide equations to compute them in our context of trust for service selection:

1) *Outdegree*: is a parameter for the extent to which a customer in the network conveys information regarding some providers to the trustor. The idea is to reflect the fact that a customer who is connected to more reliable providers and customers has a higher outdegree than a customer linked to less reliable ones. Equation 6 computes this parameter.

$$D_{out}(c_i) = \sum_{c_k \in \mathcal{T}_{c_i}} wTr_{c_i}^{c_k} + \sum_{p_j \in \mathcal{T}'_{c_i}} wTr_{c_i}^{p_j} \quad (6)$$

where $\mathcal{T}'_{c_i} = \{p_j \in P \mid \exists\ c_i \xrightarrow{v}_{cp} p_j$ in the social network$\}$

2) *Indegree*: is a parameter for the extent to which a customer in the network receives information regarding some providers from other customers. Equation 7 computes this parameter.

$$D_{in}(c_i) = \sum_{c_k \in \mathcal{S}_{c_i}} wTr_{c_k}^{c_i} \quad (7)$$

where $\mathcal{S}_{c_i} = \{c_k \in C \mid \exists\ c_k \xrightarrow{v}_{cc} c_i$ in the social network$\}$

3) *Outdegree Quality*: is a parameter for the extent to which a customer can reach others in two steps. The idea is to indicate the extent to which a customer is linked to providers and to other customers who have high degrees. Equation 8 computes this parameter.

$$\begin{array}{l} Q_{out}(c_i) = \sum_{\substack{c_k \in \mathcal{T}_{c_i} \\ p_j \in \mathcal{T}'_{c_i}}} (wTr_{c_i}^{c_k} + wTr_{c_i}^{p_j} - D_{out}(c_i)). \\ \qquad (D_{out}(c_k) - \sum_{c_{k'} \in \mathcal{T}_{c_i}} D_{out}(c_{k'})) \end{array} \quad (8)$$

4) *Indegree Quality*: is a parameter for the extent to which a customer can be reached by others in two steps. Like outdegree parameter, the idea is to indicate the extent to which a customer is linked to other customers who have high degrees. Equation 9 computes this parameter.

$$\begin{array}{l} Q_{in}(c_i) = \sum_{c_k \in \mathcal{T}_{c_i}} (wTr_{c_k}^{c_i} - D_{in}(c_i)). \\ \qquad (D_{in}(c_k) - \sum_{c_{k'} \in \mathcal{T}_{c_i}} D_{in}(c_{k'})) \end{array} \quad (9)$$

The emergence and maintenance of trust among customer and provider services depend not only on the social network parameters, but also on the payoffs associated with transactions and with revealing information to some customers about some providers. As argued in [5], providing rewards and incentives will encourage participants to provide feedback in a trust management system, which is compatible with game theory widely used in economics. We use this theory to model and analyze this issue in order to capture the different possible choices and predict the participants' behavior. To this end, we propose to model customer and provider services using rational agents. Here agents are rational in the sense that they are utility maximizers. The main challenge is how to design a mechanism (i.e. the rules of the trust game) so that the best strategy (set of agent actions) for customer agents will be revealing exactly what they believe about provider agents (truth-telling). In game theoretical terminology, this property is called *incentive compatibility*. To define more clearly this notion, we need to introduce the notion of equilibrium.

In game theory, an equilibrium is a solution concept of a game (e.g. our trust game) in terms of determining possible agents' strategies leading to a stable situation so that agents are unlikely to change their behaviors. In an equilibrium situation, agents will not gain better utility if they change their strategies under certain assumptions. Thus, the objective in a game is to find such equilibrium. Many equilibria have been proposed in the literature. In this paper, we only consider the traditional and broadly used Nash equilibrium, in which no player can obtain better utility by changing only its strategy while the other players keep their strategies unchanged. Thus, a set of strategies is a Nash equilibrium if no player can do better by unilaterally changing its strategy. Formally, We define this equilibrium as follows:

***Definition** 2: Let S_k be the strategy set for player c_k $(1 \leq k \leq m)$, $S = S_1 X S_2 ... X S_m$ is the set of strategy profiles and $u = (u_1(x), ..., u_m(x))$ is the payoff or utility function. Let x_{-k} be a strategy profile of all players except for player c_k. When each player $k \in \{1, ..., m\}$ chooses strategy x_k resulting in strategy profile $x = (x_1, ..., x_m)$, then player c_k obtains payoff $u_k(x)$. A strategy profile $x* \in S$ is a Nash equilibrium if no unilateral deviation in strategy by any single player is profitable for that player, that is:*

$$\forall k, x_k \in S_k, x_k \neq x_k^* : u_k(x_k^*, x_{-k}^*) \geq u_k(x_k, x_{-k}^*).$$

The utility depends on the strategy profile chosen, i.e. on the strategy chosen by player c_k as well as the strategies chosen by all the other players. In this context, incentive compatible means that the Nash equilibrium strategy, which is the best strategy under Nash equilibrium, is truth-telling.

Let $T \in \mathcal{TR}$ be a vector of $m = |\mathcal{T}_{c_i}|$ elements including the trust values of the provider agent p_j conveyed by the customer agents $c_k \in \mathcal{T}_{c_i}$ $(1 \leq k \leq m)$. This vector has the form $T = (Tr_{c_1}^{p_j}, \ldots, Tr_{c_m}^{p_j})$. $\mathcal{TR}$ is then the set of all possible mappings of $\mathcal{T}_{c_i}$ to $\mathbb{R}^m$. $Tr_{c_i}^{p_j}(T)$ is the trust value as computed in equation 4 using a vector T. The desired outcome of the mechanism we aim to design for our trust game is the vector T^* so that the distance between the computed trust value for p_j and the observed one be minimal, which means that resolving the following equation:

$$T^* = \arg\min_{T \in \mathcal{TR}} |Tr_{c_i}^{p_j}(T) - \widehat{Tr}_{c_i}^{p_j}| \quad (10)$$

Our objective is to find a utility function for customer services satisfying the incentive compatibility under Nash equilibrium. Using such a utility function, customer agents will find no better option than to reveal the true trust value they have about the provider service.

In our trust game, each agent has a set of strategies. For space limit reasons, we only focus on the customer service agents. Each customer service agent, when asked by another agent about the trust value of a provider, has three possible strategies: 1) reveal the information; 2) refuse to reveal; and 3) reply by informing the trustor that the asked information is not available. The second strategy implies that the agent confirms that it has the information, but refuses to share it. In the third strategy, the agent could not be reliable. We limit

our selves to systems where it is possible to check that agents had or not transactions with each other. In such systems, the third strategy is eliminated. If the agent decides to play the first strategy, two choices are possible: telling the truth or lying. The trustor should provide incentives to the asked agents (witnesses) encouraging them to reveal the truth. However, these agents should also be penalized if they lie.

On one hand, to be encouraged to participate in the trust game about a given agent provider, customers should not wait until the revealed information is verified by the trustor against the real behavior of the trustee. On the other hand, the trustor cannot reward or punish the participants without doing some verifications. For that reason, we propose a 3-step incentive mechanism, where customer agents can obtain rewards or receive penalties depending on their strategies in 3 steps. The strategy x_k of each agent c_k is defined in terms of the provider's trust value this agent reveals. Thus, the utility function of a customer agent c_k is defined as follows (equation 11):

$$u_k(x) = f_k(x) + g_k(x) + c.h_k(x) \tag{11}$$

where $f_k(x) > 0, f_k(x) < |g_k(x)|$ and $f_k(x) + |g_k(x)| < |h_k(x)|$. $f_k(x)$ is the first positive reward the trustor gives to the customer agent c_k rewarding its acceptance to cooperate (step 1). Different customer agents can receive different rewards $f_k(x)$ depending on their importance in the social network and on the relationship with the trustor. $g_k(x)$ is the second value (step 2) the agent c_k will receive depending on the similarity of the information this agent has revealed with the information received from other witnesses. Less the distance between the provider's trust value revealed by c_k and the mean of the trust values revealed by all witnesses for the same provider, high is the reward. $g_k(x)$ can be negative if this distance is high, which captures a sort of punishment. Equation 12 gives the mean of the provider's trust values as revealed by the witnesses, and equation 13 computes the second step incentive.

$$\mu = \frac{\sum_{c_k \in \mathcal{T}_{c_i}} Tr_{c_k}^{p_j}}{\mid \mathcal{T}_{c_i} \mid} \tag{12}$$

$$g_k(x) = a_k.v_k.\frac{1}{|\mu - Tr_{c_k}^{p_j}|^2}$$
where:
$$v_k = \begin{cases} 1 & \text{if } \mid \mu - Tr_{c_k}^{p_j} \mid \leq \epsilon \\ -1 & \text{if } \mid \mu - Tr_{c_k}^{p_j} \mid > \epsilon \end{cases} \tag{13}$$

The factor a_k depends again on the importance of c_k in the social network and the relation it has with the trustor. This second incentive captures the majority effect: it is more likely that the majority has the good information. The reward or punishment $g_k(x)$ can be received just when the witnesses send their information to the trustor.

The third step incentive $h_k(x)$ is calculated in terms of the distance between the revealed information and the actual (observed) trustee's behavior. Consequently, this incentive is included in the utility function ($c = 1$) only if the trustor decides to have a transaction with the provider, which means that the computed trust value $Tr_{c_i}^{p_j}$ using equation 4 is greater than a given threshold λ; otherwise, c will be set to 0. The resulting reward (if the distance is small) or punishment (if the distance is high) is received after a period of time. Equation 14 computes this incentive as follows:

$$h_k(x) = b_k.v'_k.\frac{1}{|Tr_{c_k}^{p_j} - \widehat{Tr}_{c_i}^{p_j}|^2}$$
where:
$$v'_k = \begin{cases} 1 & \text{if } \mid Tr_{c_k}^{p_j} - \widehat{Tr}_{c_i}^{p_j} \mid \leq \epsilon' \\ -1 & \text{if } \mid Tr_{c_k}^{p_j} - \widehat{Tr}_{c_i}^{p_j} \mid > \epsilon' \end{cases} \tag{14}$$

The fact that $f_k(x) < |g_k(x)|$ and $f_k(x) + |g_k(x)| < |h_k(x)|$ means that each incentive is more important to the summation of the previous ones. This condition is important to guarantee the incentive compatibility. To prove that we need first to prove the following lemmas:

***Lemma** 1:* Revealing the true trust value about the provider p_j (truth-telling) is a Nash equilibrium strategy in the trust game.

Proof: Each agent has the objective of maximizing its utility function u_k. If all agents play the strategy of revealing the true trust value, $g_k(x)$ will get maximized. By changing this strategy, each customer agent c_k will lose because its revealed value will be far from the mean. Consequently, c_k will obtain $g_k(x) < 0$. Furthermore, if by revealing the truth, c is equal to 1 (because the computed trust is greater than λ), changing the strategy by lying will result in another loss, because the revealed value will be far from the actual provider's behavior. Therefore, c_k will obtain $h_k(x) < 0$. Telling the truth is then a Nash equilibrium strategy. ■

We consider a revealed trust value as false if there is a considerable difference between it and the believed one.

***Lemma** 2:* If the provider p_j is untrustworthy, revealing a false trust value about it is not a Nash equilibrium strategy in the trust game.

Proof: By playing the strategy of revealing false information while the provider is untrustworthy, c will be equal to 1 (because the computed trust value $Tr_{c_i}^{p_j}$ will reveal that the provider is trustworthy). In this case, we have $v'_k = -1$. Therefore, every customer agent c_k will obtain a negative $h_k(x)$. Because $|f_k(x) + g_k(x)| < |h_k(x)|$, the obtained utility $u_k(x)$ will be negative although $g_k(x)$ is getting maximized. Thus, every agent will gain more by changing the strategy because its $h_k(x)$ will be maximized. ■

***Lemma** 3:* If the provider p_j is trustworthy, revealing a false trust value about it is a Nash equilibrium strategy in the trust game.

Proof: If the provider is trustworthy, playing the strategy of revealing false information will result in $c = 0$. Therefore, the third incentive $h_k(x)$ will not be considered. Customer agents c_k will get a positive utility since $g_k(x)$ is getting maximized. Changing this strategy unilaterally will not result

TABLE I
SIMULATION SUMMARIZATION OVER THE OBTAINED MEASUREMENTS.

SP type	Density in community	Utility range	Utility SD
Good	15.0%	$]+5,+10]$	1.0
Ordinary	30.0%	$]-5,+5]$	2.0
Bad	15.0%	$]-10,-5]$	2.0
Fickle	40.0%	$]-10,+10]$	–

in a better utility, since the resulting $g_k(x)$ will be negative while $h_k(x)$ always equal to 0. Consequently, the result follows. ■

***Proposition** 1:* The designed mechanism for trust game using u_k utility function satisfies the incentive compatibility under Nash equilibrium.

Proof: From Lemmas 1, 2, and 3, a customer agent c_k has an incentive to lie only if $c = 0$ and $g_k(x) > 0$. In this case, the gained utility is: $|f_k(x)+g_k(x)|$. However, by telling the truth, the gained utility is $|f_k(x)+g_k(x)+h_k(x)|$. Because telling the truth is the best strategy under Nash Equilibrium, we are done. ■

IV. EXPERIMENTAL RESULTS AND RELATED WORK

The Testbed and Experimental Results. To evaluate our model, we implemented a proof of concept prototype using Java and $Jadex^{©TM}$ (for agent implementation). The implemented testbed environment is populated with two service types associated with two agent types: (1) *provider service agents*; and (2) *customer service agents*. The simulation consists of a number of consequent RUNs in which agents are activated and build their private knowledge, keep interacting with one another, and update their knowledge about the environment. Table I represents four types of the provider services we consider in our simulation: good, ordinary, bad and fickle. The first three provide services regarding to the assigned mean value of quality with a small range of deviation. Fickle providers are more flexible as their range of service quality covers the whole possible outcomes. Upon interaction with provider services, customer service agents obtain some utilities.

Looking for a good provider service to gain high utility, the customer service agent evaluates the providers and if needed pays others to obtain relative information. After interaction, the customer agent rates the provider and provides the third part of the reward to the satisfactory witnesses. In the simulation environment, agents are equipped with different trust models in the sense that their provider selection policies are different. In our experiment, we compare the effectiveness of the proposed model agents with agents that are equipped with other trust models in the literature in different perspectives so that their overall performance comparison could be obtained.

Performance Comparison. In order to discuss the proposed model's performance, we compare it with BRS [6], Travos [11] and Fire [4] trust models. These models are similar to the proposed model in the sense that they do consider other agents' suggestions while evaluating the trust of some specific agent and discard inaccurate suggestions aiming to perform best selection. However, they differ from ours in the trust assessment mechanism and do not encourage other agents by providing incentives in order to obtain most accurate information. The comparison between these models is illustrated in Figure 1-a representing the cumulative utility gained of the four models. The experimental results show that the proposed model agents outperform others in selecting best providers and thus gaining more utility. This can be explained by the fact that the consulting agents are encouraged to truthfully reveal their believes, which would cause more accurate trust assessments. The proposed model agents are learning who are the best providers and upon evaluation, with respect to incentives they receive, they pass the accurate information about the trustworthy providers. This enables them to adapt with the environment faster than regular rating mechanism and its distribution. We will discuss the effectiveness of the proposed model in more details in the following subsection.

Proposed Model Performance. In the proposed model, we try to establish a trust mechanism where a customer, firstly can maintain an effective trust assessment process and secondly, accurately updates its belief set, which reflects the other participants likely accuracy. In order to confirm the mentioned characteristics, we compare the proposed model with other trust models in two perspectives. In the first comparison view, we use the services that only perform a direct trust assessment process. We refer to this group of services as *Direct Trust Group* (DTG). In the second view, we use the services that, in addition to the direct trust assessment mechanism, provide incentives for the consulting services (witnesses) in order to increase their information accuracy. We refer to this group of services as *Incentive Trust Group* (ITG).

First we compare the models in terms of good provider selection percentage. In such a biased environment, the number of good providers are comparatively low. Therefore, the service agents need to perform an accurate trust assessment to recognize the best providers. As it is clear from the Figures 1-b and 1-c, DTG services function better than other models (Fire, Travos and BRS). The reason is that in this model, agent services are assessing the credibility of the providers using other services suggestions depending on their credibility and to what extent they know the provider. Afterwards, these services rate the provider, which would be distributed to other services upon their request. Not excluding the fact that DTG services are considering partial ratings for witnesses, we state that they weakly function when the environment contains services that do not truthfully reveal their believes. ITG services in addition to the direct trust assessment, provide incentives for the witnesses, which encourages them to effectively provide the information aiming to gain more utility. Figures 1-b and 1-c show that ITG services outperform other models in best provider selection. This is expressed by the fact that ITG services recognize the best providers ensuring that the best selected provide would provide the highest utility.

Fire is a trust-certified reputation model, which addresses the problem of lack of direct history. However, this model do not recognize the inaccurate information provided by

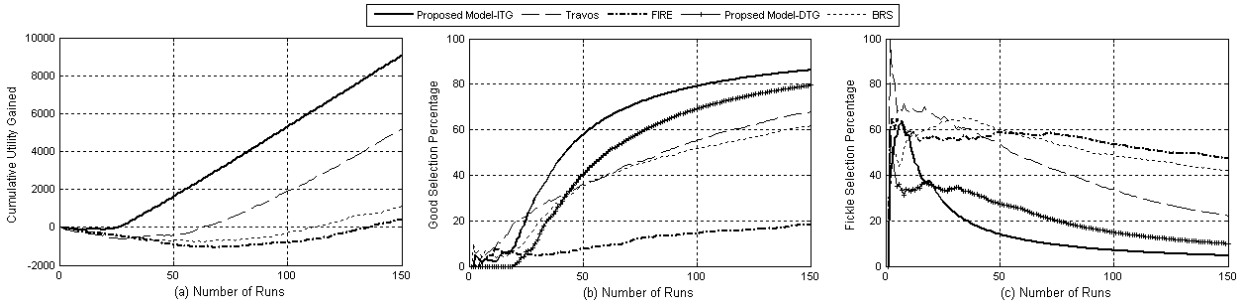

Fig. 1. Overall comparison of the proposed model with Fire, Travos and BRS in terms of (a) cumulative utility gained; (b) good selection percentage; and (c) fickle selection percentage.

witnesses. This causes misleading trust assessment, and leads to poor performance in an environment in which agents are less likely to truthfully reveal their believes. Therefore, good providers are not effectively clarified (figure 1-b) and thus higher number of fickle providers are selected (figure 1-c).

In BRS model, the trustor in the assessment process uses beta distribution method and discards the ratings that deviate the most from the majority of the ratings. Concerning this, BRS is comparatively a static trust method, which causes a low-efficient performance in very dynamic environment. In general, if a BRS service agent decides to evaluate another service agent that it is not acquainted with, it considers the majority of ratings, which are supposed to be truthfully revealed about the trustee service. In such a case that the trustee has just changed its strategy, the trustor would loose in trust assessment and does not verify the accuracy of the gained information. Thus, as illustrated in figures 1-b and 1-c, BRS services have less percentage of good providers selection and relatively higher percentage of fickle providers selection.

Travos [11] trust model is similar to BRS in using beta distribution to estimate the trust based on the previous interactions. Travos model also does not have partial rating. Hence, the trustor merges his own experience with suggestions from other services. However, unlike BRS model, Travos filters the surrounding witnesses that are fluctuating in their reports about a specific trustee service. To some extent, this feature would cause a partial suggestion consideration and thus, Travos service agents would adapt faster comparing to BRS service agents. Rates concerning the good and fickle selection percentage shown in figures 1-b and 1-c reflect higher efficiency of Travos compared to BRS. However, Travos model considers that witnesses do not change their behavior towards the elapsing time. These missing assumptions affect the accuracy of trust estimation in a very biased environment.

V. Conclusion

The contribution of this paper is the proposition of a new social network-based trust model for service selection. The effective assessment procedure is performed while the strategy of truth-telling is encouraged. This is proved using game theory and mechanism design techniques. The proposed model would enhance the accuracy of the trust assessment process as the communicated information are more accurate. This mechanism is compared with other related models and the carried simulations showed its high efficiency. Our plan for future work is to advance the assessment techniques by considering other equilibrium concepts. We also plan to investigate in more details the optimization part and to formalize it to be adaptable to diverse situations.

References

[1] V. Buskens. Social Networks and Trust. Kluwer Academic Publishers. 2002.

[2] R. Dash, N.R. Jennings and D. Parkes. Computational-mechanism design: a call to arms. IEEE Intelligent Systems, 18(6) pp. 40-47, 2003.

[3] T. Dong-Huynh, N.R. Jennings and N.R. Shadbolt. Certified reputation: how an agent can trust a stranger. Proc. of The 5^{th} Int. Joint Conf. on Autonomous Agents and Multiagent Systems, pp. 1217-1224, Japan2006.

[4] T. Dong-Huynh, N.R. Jennings and N.R. Shadbolt. Fire: An integrated trust and reputation model for open multi-agent systems. Journal of Autonomous Agents and Multi-Agent Systems 13(2) pp. 119-154, 2006.

[5] A. Fernandes, E. Kotsovinos, S. Ostring, B. Dragovic. Pinocchio: Incentives for Honest Participation in Distributed Trust Management. iTrust, pp. 63-77, 2004.

[6] A. Jesang and R. Ismail. The beta reputation system. 15^{th} Bled Electronic Commerce Conf. e-Reality: Constructing the e-Economy, June2002.

[7] B. Khosravifar, J. Bentahar, M.Gomrokchi, and R. Alami. An approach to comprehensive trust management in multi-agent systems with credibility. 2^{nd} Int. Conf. on Research Challenges in Info. Science, pp. 53-64, 2008.

[8] Z. Maamar, G.K. Mostefaoui, D. Benslimane. A policy-based approach to secure context in a web services environment. ICEIS (4), pp. 100-105, 2006.

[9] E.M. Maximilien, and M.P. Singh. Reputation and endorsement for web services. ACM SIGEcom Exchanges, 3(1):24-31, 2002.

[10] E. Shakshuki, L. Zhonghai, and G. Jing. An agent-based approach to security service. International Journal of Network and Computer Applications. Elsevier, 28(3): 183-208, 2005.

[11] W. T. Teacy, J. Patel, N.R. Jennings, and M. Luck. Travos: Trust and reputation in the context of inaccurate information sources. Autonomous Agentsand Multi-Agent Systems, 12(2):183-198, 2006.

[12] Y. Wang and M.P. Singh. Formal trust model for multiagent ststems. Proceedings of the 20th International Joint Conference on Artificial Intelligence (IJCAI), pp. 1551-1556, 2007.

[13] L. Xiong and L. Liu. PeerTrust: supporting reputation-based trust for peer-to-peer electronic communities. Journal of IEEE Transactions on Knowledge and Data Engineering, 16(7):843-857, 2004.

[14] P. Yolum and M.P. Singh. Engineering self-organizing referral networks for trustworthy service selection. IEEE Transaction on Systems, Man, and Cybernetics, 35(3):396-407, 2005.

[15] M. Younas, I. Awan, R. Holton and D. Duce. A P2P network protocol for efficient choreography of web services. Int. Conf. on Advanced Information Networking and Applications (AINA), pp. 839-846, 2007.

[16] M. Younas, Y. Li, C. Lo and Y. Li. An efficient transaction commit protocol for composite web services. Int. Con. on Advanced Information Networking and Applications (AINA), pp. 591-596, 2006

[17] G. Zacharia, and P. Maes. Trust management through reputation mechanisms. Applied Artifitial Intelligence, 14(9):881-908, 2000.