Trust Management Framework for Efficient Service Provisioning in Dynamic Distributed Computing Environments

Malamati Louta*, *Member, IEEE,* and Angelos Michalas

***Abstract*— In dynamic distributed computing environments, system entities may be classified into two main categories that are, in principle, in conflict. These are the Service Resource Requestors (SRRs) wishing to use services and/or exploit resources offered by the other system entities and the Service Resource Providers (SRPs) that offer the services/resources requested. Seeking for the maximisation of their welfare, while achieving their own goals and aims, entities may misbehave (intentionally or unintentionally), thus, leading to a significant deterioration of system's performance. In this study, a reputation mechanism is proposed which helps estimating SRPs trustworthiness and predicting their future behaviour, taking into account their past performance in consistently satisfying SRRs' expectations. The reputation mechanism is distributed, considers both first-hand information (acquired from the SRR's direct past experiences with the SRPs) and second-hand information (disseminated from other SRRs' past experiences with the SRPs), while it exhibits a robust behaviour against inaccurate reputation ratings.**

***Index Terms*— Collaborative Reputation Mechanism, Intelligent Multi Agent Systems, Service Resource Requestors/Providers, Distributed Computing Environments.**

I. Introduction

In the highly dynamic distributed computing environments (including pervasive, peer-to-peer, grid computing, mobile ad-hoc & sensor networks and electronic communities), from a market-based perspective, the roles of the system entities may be classified into two main categories that, in principle, are in conflict. These two categories are: the entities that wish to use services and/or exploit resources offered by other system entities (*Service/Resource Requestors* - SRRs) and the entities that offer the services / resources requested (*Service/Resource Providers* - SRPs). In general, SRPs' main role is to develop, promote and provide the desired services and resources trustworthily, at a high quality level in a time and cost effective manner.

Efficient system operation requires for a cooperation of high degree among the various entities, which may at the same time act as a requestor and as a provider for different services/resources. However, seeking for the maximization of their welfare, while achieving their own goals and aims, entities may misbehave (intentionally or unintentionally), acting selfishly, thus, leading to a significant deterioration of system's performance. Therefore, trust mechanisms should be exploited in order to build the necessary trust relationships among the system entities [1], enabling them to automatically adapt their strategies to different levels of cooperation and trust.

Traditional models aiming to avoid strategic misbehaviour (e.g., authentication and authorization schemes [2], [3], Trusted Third Parties (TTPs) [4]) may be inadequate or even impossible to apply due to the complexity, the heterogeneity and the high variability of the environment. Reputation Mechanisms are employed to provide a "softer" security layer, sustaining rational cooperation and serving as an incentive for good behaviour as good players are rewarded by the society, whereas bad players are penalized [5]. In general, reputation mechanisms establish trust by exploiting learning from experience concepts in order to obtain a reliability value of system participants in the form of rating based on other entities' view/opinion. Reputation related information may be disseminated to a large number of system participants in order to adjust their strategies and behaviour, multiplying thus the expected future gains of honest parties which bear the loss incurred by cooperating and acting for the maximization of the social welfare. Current reputation system implementations in e-marketplaces consider feedback given by Buyers in the form of ratings in order to capture information on Seller's past behavior, while the reputation value is computed as the sum (or the mean) of those ratings either incorporating all ratings or considering only a period of time (e.g., six months) [6], [7].

In the context of this study, our focus is laid on the evaluation of the reliability of SRPs. To this respect, a collaborative reputation mechanism is proposed, which takes into account the SRPs' past performance in consistently satisfying SRRs' expectations. To be more specific, the reputation mechanism rates the SRPs with respect to whether

*Corresponding Author. Malamati Louta is with the Department of Business Administration, Technological Educational Institute of Western Macedonia and with the Department of Information and Communication Technologies Engineering, University of Western Macedonia, Kozani, 50100, GREECE (phone: +302461038772; fax: +302461039682; e-mail: louta@telecom.ntua.gr).

Angelos Michalas is with the Department of Informatics and Computer Technology, Technological Educational Institute of Western Macedonia, Kastoria, 52100, GREECE (amichalas@kastoria.teikoz.gr)

they honoured or not the agreements established with the SRRs, thus, introducing the concept of trust among the involved parties. Most reputation based systems in related research literature aim to enable entities to make decisions on which parties to negotiate/cooperate with or exclude, after they have been informed about the reputation ratings of the parties of interest. The authors in this study do not directly exclude / isolate the SRPs that are deemed misbehaving, but instead, base the SRRs' decision concerning the most appropriate SRP on their respective reputation rating (*reliability related factor*), under the assumption that all candidate SRPs serve the SRRs service/resource requests with the same terms and conditions. The reputation mechanism considers both first-hand information (acquired from the evaluator SRR's past experiences with the target SRP) and second-hand information (disseminated from other SRRs), is decentralized and exhibits robust behaviour against inaccurate reputation ratings intentionally and/or unintentionally provided.

This study is based upon the notion of interacting intelligent agents which participate in activities on behalf of their owners, while exhibiting properties such as autonomy, reactiveness, and proactiveness, in order to achieve particular objectives and accomplish their goals [8]. Thus, two agent categories are introduced: the *Service/Resource Requestor Agents* (SRRAs) and the *Service/Resource Providers Agents* (SRPAs) acting on behalf of the SRRs and SRPs respectively. SRRAs and SRPAs are both considered to be rational and self-interested, while aiming to maximise their owners' profit.

The rest of the paper is structured as follows. In Section 2, the fundamental concepts of the proposed collaborative reputation mechanism are presented, aiming to offer an efficient way of building the necessary level of trust in the intelligent distributed computing environments. In Section 3, the reputation ratings system is mathematically formulated. In Section 4, the related research literature is revisited. Finally, in Section 5, initial findings are reported, conclusions are drawn and directions for future plans are given.

II. Reputation Mechanism Fundamentals

The proposed reputation mechanism is collaborative in the sense that it considers both first-hand information (acquired from the SRRA's past experiences with the SRPAs) and second-hand information (disseminated from other SRRAs). To be more specific, each SRRA keeps a record of the reputation ratings of the SRPAs it has negotiated with and has been served by in the past. This rating based on the direct experiences of the evaluator SRRA with the target SRPA forms the first factor contributing to the overall SRPA reputation. Concerning the SRPAs' reputation ratings based on feedback given by other SRRA on their experiences in the system (the second factor contributing to the overall SRPA reputation rating based on witness information), a centralized approach may be adopted (e.g., a system component could maintain and update a collective record of the SRPAs' reputation ratings formed after taking into account each SRRA view on the SRPAs' performance [1]). This approach on one hand has significant computational, communicational, time and storage advantages, but on the other hand it may suffer from the classical disadvantages of all centralized methodologies (e.g., introduction of performance bottlenecks and single point of failure in the system).

In the context of this study, we adopt a decentralized approach with respect to witness SRRA's information concerning SRPAs reputation ratings. Specifically, a basic assumption is that each SRRA is willing to share its experiences and provide whenever asked for the reputation ratings of the SRPAs formed on the basis of its past direct interactions. Thus, the problem is reduced in finding proper witnesses, i.e., obtaining a reference of the SRRAs that have previously been served by the SRPAs under evaluation. In the current version of this paper, we assume that a Service/Resource Provider Reputation Broker component (SRPRB) maintains a list of the SRPAs providing a specific service / resource as well as a list of SRRAs that have previously interacted and been served by a specific SRPA. At this point it should be noted that the reliability of SRPAs is treated as a behavioural aspect, independently of the services / resources provided. Thus, the witnesses list may be composed by SRRAs which have had direct interactions with the specific SRPA in the past, without considering the service / resource consumed. Additionally, SRPAs have a solid interest in informing SRPRB with respect to services / resources they currently offer, while the SRRAs are authorized to access and obtain witness references only in case they send feedback concerning the preferred partner for their past interactions in the system. This policy based approach provides a solution to the inherent incentive based problem of reputation mechanisms in order for the SRPRB to keep accurate and up to date information.

True feedback cannot be automatically assumed. Second-hand information can be spurious (e.g., parties may choose to misreport their experience due to jealousy or in order to discredit trustworthy Providers). In general, a mechanism for eliciting true feedback in the absence of TTPs is necessitated. According to the simplest possible approach that may be adopted in order to account for possible inaccuracies to the information provided by the witnesses SRRAs (both intentional and unintentional), the evaluator SRRA can mostly rely on its own experiences rather on the target SRPA's reputation ratings provided by witnesses SRRAs. To this respect, SRPA's reputation ratings provided by the witness SRRAs may be attributed with a relatively low significance factor.

In this paper, we consider that each SRRA is associated with a trust level dynamically updated, which reflects whether the SRRA provides feedback with respect to its experiences with the SRPAs truthfully and in an accurate manner. In essence, this trust level is a measure of the credibility of the witness information. To be more specific, in order to handle intentional inaccurate information, an honesty probability is

attributed to each SRRA, i.e., a measure of the likelihood that a SRRA gives feedback compliant to the real picture concerning service provisioning. Second-hand information obtained from trustworthy SRRAs (associated with a high honesty probability), are given a higher significance factor, whereas reports (positive or negative) coming from untrustworthy sources have a small impact on the formation of the SRPAs' reputation ratings. Concerning the provision of inaccurate information unintentionally, the authors take into account the number of transactions a witness SRRA has performed with the target SRPA and the sum of the respective transaction values. Specifically, it is quite safe to assume that SRRAs that have been involved with the target SRPA only for a few times will not have formed an accurate picture regarding its behaviour. Additionally, if the reputation rating is formed on the basis of low-valued transactions, there is a possibility that it does not reflect the real picture (e.g., an SRPA may strategically exhibit good behaviour in case its potential profits in a context of a transaction are low and cheat when the expected earnings are high).

The evaluator SRRA uses the reputation mechanism to decide on the most appropriate SRPA, especially in cases where the SRRA doubts the accuracy of the information provided by the SRPAs. A learning period is required in order for the SRRAs to obtain fundamental information for the reliability related behavioral aspects of the SRPAs. During the learning period and/or in case reputation specific information is not available to the SRRA (both through its own experiences and through the witnesses) the SRPs may be selected randomly or on round-robin basis (e.g., the service/resource requests are served by iterating the candidate SRPs list).

Considering that the SRRAs have initially acquired the fundamental reliability related information for the SRPAs (that is after the learning period), only the reputation rating of the "best" SRPA (i.e., the one selected on the basis of the SRPAs' reliability related values) will be updated, after the user finally accesses the service. Thus, the system can only verify the behaviour of the "most" appropriate SRPA and has no means to identify potential changes to other SRPAs' behaviour with respect to their compliance to the established contract terms and conditions. Furthermore, initial SRPAs' reliability rating values are taken equal to 0.1. A quite low reputation rating value has been assumed (that is all SRPAs initially are considered to be dishonest entities) in order to avoid the bad consequences of changing identities so as to wipe out possible misbehaviour in the past). Therefore, assuming that the "good" SRPAs do not alter their policies, the misbehaving SRPAs have to improve on their potential performance so as to overcome the barrier raised by their low reputation rating.

In order not to exclude new SRPAs or SRPAs that initially did not honour the terms and conditions of the contracts established, thus being attributed with a small reliability related value after the learning period, and give them a chance to re-enter to the system and improve their reputation rating, the simplest possible approach that could be adopted is to base the SRRAs' decision concerning the most appropriate SRPA after a specific time period, or after the completion of a specific number of transactions on a random scheme until possible outdated information the system possesses is updated. Otherwise, a Boltzmann exploration strategy could be adopted [9].

It should be noted that the reputation mechanism comes at the cost of keeping reputation related information at each SRRA and updating it after service provision / resource consumption has taken place. Finally, the estimation of the reliability rating value of the SRPAs requires in some cases (e.g., when consumption of network or computational resources are entailed in the service provision process) a mechanism for evaluating whether the service quality was compliant with the picture promised during the negotiation phase.

III. Formulation of the Reputation Rating System

Let us assume the presence of M candidate SRPAs interacting with N SRRAs concerning the provisioning of services / resources $s = \{s_1, s_2, ...\}$ requested in a distributed intelligent computing environment. Let the set of agents that represent *Service Resource Providers* be denoted by $P = \{P_1, P_2, ...P_M\}$ and the set of agents that represent *Service Resource Requestors* be denoted by $R = \{R_1, R_2, ...R_N\}$. We hereafter consider the request of a SRRA R_i (evaluator) regarding the provision of service s, which without loss of generality is provided by all candidate SRPAs $P = \{P_1, P_2, ...P_M\}$ with the same terms and conditions. The evaluator SRRA R_i will base its decision on the most appropriate SRP for the provision of service s on the SRPAs' reputation ratings, considering its own direct experiences as well as the opinion of a number of witnesses. Thus, in order to estimate the reputation rating of a target SRPA P_j at time instance t_c, the evaluator SRRA R_i needs to retrieve from the SRPRB the list R_w of n witnesses ($R_w \subseteq R = \{R_1, R_2, ...R_N\}$). Thereafter, the R_i contacts the n witnesses in order to get feedback reports on the behaviour of the P_j.

A. Estimating target SRPA's reputation rating based on SRRAs' direct experiences

Concerning the formation of the reputation ratings $RR^{R_x}(P_j)$, each SRRA R_x may rate SRPA P_j with respect to its reputation on the basis of R_x direct experiences with P_j after a transaction d has taken place at time instance t_d in accordance with the following equation:

$$RR_{post}^{R_x,t_d}(P_j) = RR_{pre}^{R_x}(P_j) + k_r \cdot l(RR_{pre}^{R_x}(P_j)) \cdot \{rr(P_j) - E[rr(P_j)]\} \quad (1)$$

where RR_{post} and RR_{pre} are the SRPA P_j reliability based rating after and before the updating procedure. It has been

assumed that RR_{post} and RR_{pre} lie within the [0,1] range, where a value close to *0* indicates a misbehaving Seller. $rr(P_j)$ is a (reward) function reflecting whether the service quality is compliant with the picture established during the negotiation phase and $E[rr(P_j)]$ is the mean (expected) value of the $rr(P_j)$ variable. In general the larger the $rr(P_j)$ value, the better the SRPA P_j behaves with respect to the agreed terms and conditions of the established contract, and therefore the more positive the influence on the rating of the P_j. Factor k_r ($k_r \in (0,1]$) determines the relative significance of the new outcome with respect to the old one. In essence, this value determines the memory of the system. Small k_r values mean that the memory of the system is large. However, good behaviour will gradually improve the SPRA's P_j reputation ratings. $l(RR_{pre}^{R_x}(P_j))$ is a function of the P_j reputation rating $RR_{pre}^{R_x}(P_j)$ and is introduced in order to keep the P_j rating within the range $[0,1]$. In the current version of this study, $l(RR_{pre}^{R_x}(P_j)) = \frac{1}{1-e} \cdot [1 - \exp(1 - RR_{pre}^{R_x}(P_j))]$, for which it stands $l(RR_{pre}^{R_x}(P_j)) \underset{RR_{pre}^{R_x}(P_j) \to 0}{\to} 1$ and $l(RR_{pre}^{R_x}(P_j)) \underset{RR_{pre}^{R_x}(P_j) \to 1}{\to} 0$.

It should be noted that Seller's misbehaviour (or at least deterioration of its previous behaviour) leads to a decreased post rating value, since the $\{rr(P_j) - E[rr(P_j)]\}$ quantity is negative. The $rr(P_j)$ function may be implemented in several ways. In the context of this study, it was assumed without loss of generality that the $rr(P_j)$ values vary from 0.1 to 1.

B. Estimating target SRPA's overall reputation rating

The target SRPA's P_j reputation rating $RR(P_j)$ may be estimated by the evaluator SRRA R_i in accordance with the following formula:

$$RR^{R_i,t_c}(P_j) = w_{R_i} \cdot RR^{R_i}(P_j) + \sum_{k=1}^{n} w_{R_k} \cdot RR^{R_k}(P_j) \quad (2)$$

where $RR^{R_x}(P_j)$ denotes the reputation rating of the target SRPA P_j as formed by SRRA R_x on the basis of its direct experiences with P_j in the past. As may observed from (2), the reputation rating of the target P_j is a weighted combination of two factors. The first factor contributing to the reputation rating value is based on the direct experiences of the evaluator agent R_i, whereas the second factor depends on information regarding P_j past behaviour gathered from the n witnesses.

Weight w_{R_x} provide the relative significance of the reputation rating of the target SRPA P_j as formed by the SRRA R_x (i.e., $RR^{R_x}(P_j)$) to the overall reputation rating estimation by the evaluator R_i. In general, w_{R_x} is a measure of the credibility of witness R_x and may be a function of the trust level attributed to each SRRA R_x by the evaluator R_i, the number of interactions R_x has performed with P_j and the sum of the respective transaction values (e.g., the more transactions with high transactional value have been performed, the higher the possibility is for the R_x to possess an accurate picture of P_j behaviour). Additionally, it has been assumed that weights w_{R_x} are normalized to add up to 1 (i.e., $w_{R_i} + \sum_{k=1}^{n} w_{R_k} = 1$). Thus, weight w_{R_x} may be given by the following equation:

$$w_{R_x} = \frac{TL^{R_i}(R_x) \cdot N_T(R_x, P_j) \cdot \sum_{m=1}^{N_T} TV(R_x, P_j)}{\sum_{x \in i \cup \{1,\ldots n\}} TL^{R_i}(R_x) \cdot N_T(R_x, P_j) \cdot \sum_{m=1}^{N_T} TV(R_x, P_j)} \quad (3)$$

where $TL^{R_i}(R_x)$ is the trust level attributed to SRRA R_x by the evaluator R_i, $N_T(R_x, P_j)$ is the number of interactions R_x has performed with P_j and $\sum_{m=1}^{N_T} TV(R_x, P_j)$ is the sum of the respective transaction values. It has been assumed that $TL^{R_i}(R_x) \in [0,1]$ with level *1* denoting a fully trusted witness R_x in the eyes of the evaluator R_i. One may easily conclude that for the evaluator R_i it stands $TL^{R_i}(R_i) = 1$.

C. Updating trustworthiness of witnesses

Trustworthiness of witnesses $TL^{R_i}(R_x)$ initially assumes a high value. That is all witnesses are considered to report their experiences to the R_i honestly. However, as already noted, the trust level is dynamically updated in order to account for potential dissemination of misinformation by the witnesses in the system. Specifically, a witness R_x is considered to misreport his/her past experiences, if the target P_j overall reputation rating $RR^{R_i,t_c}(P_j)$ as estimated by (2) is beyond a given distance of the rating $RR^{R_x}(P_j)$ obtained from the witness R_x (formed in accordance with (1)), in which case the following expression holds:

$$\left| RR^{R_i,t_c}(P_j) - RR^{R_x}(P_j) \right| > e \quad (4)$$

where e is the predetermined distance level.

As it may be observed, this approach may be quite efficient in case the population of the witnesses reporting honestly their

experiences is quite large with respect to the dishonest witnesses. Thus, to account for such cases, the evaluator takes also into account the distance of the reputation rating of the target P_j as formed considering its own direct experiences $RR^{R_i,t_d}(P_j)$. In case it stands $\left|RR^{R_i,t_d}(P_j) - RR^{R_x}(P_j)\right| > e$ (assuming that the evaluator R_i has obtained the information required based on its direct experiences and has formed an accurate picture of the target P_j reliability) the evaluator may conclude that the witness misreports its experiences. Otherwise, in case the evaluator R_i does not have a real picture of the target P_j behaviour, it adjusts the trustworthiness of the witnesses considered for the formation of P_j reputation, only in case P_j is selected for the provisioning of the service / resource and after service provisioning has taken place and the reputation rating has been accordingly updated by (1).

Witnesses' trustworthiness may be updated on the basis of the following expression, in a similar manner to (1):

$$TL^{R_i}_{post}(R_x) = TL^{R_i}_{pre}(R_x) + k_b \cdot l(TL^{R_i}_{pre}(R_x)) \cdot a \quad (5)$$

where $TL^{R_i}_{post}(R_x)$ and $TL^{R_i}_{pre}(R_x)$ are the witness R_x trustworthiness after and before the updating procedure. It has been assumed that $TL^{R_i}_{post}(R_x)$ and $TL^{R_i}_{pre}(R_x)$ lie within the [0,1] range, where a value close to *0* indicates a dishonest witness. For the reward / penalty parameter a the following expression holds:

$$a = \begin{cases} a < 0, \left|RR^{R_i,t_{c/d}}(P_j) - RR^{R_x}(P_j)\right| > e \\ a > 0, \left|RR^{R_i,t_{c/d}}(P_j) - RR^{R_x}(P_j)\right| < e \end{cases} \quad (6)$$

$l(TL^{R_i}_{pre}(R_x))$ is a function of the Buyer's trustworthiness $TL^{R_i}_{pre}(R_x)$ and is introduced in order to keep the witness trustworthiness level within the range $[0,1]$. In the current version of this study, in accordance with equation (1), $l(TL^{R_i}_{pre}(R_x)) = \frac{1}{1-e} \cdot [1 - \exp(1 - TL^{R_i}_{pre}(R_x))]$, for which it stands $\underset{TL^{R_i}_{pre}(R_x)\to 0}{l(TL^{R_i}_{pre}(R_x))} \to 1$ and $\underset{TL^{R_i}_{pre}(R_x)\to 1}{l(TL^{R_i}_{pre}(R_x))} \to 0$. Factor k_b ($k_b \in (0,1]$) determines the relative significance of the new outcome with respect to the old one, constituting, thus, the memory of the system.

D. Introducing the time effect in the target SRPA's overall reputation rating estimation

In order to introduce the time effect in our mechanism and model the fact that more recent events should weigh more in the evaluation of the target SRPA's P_j reputation rating $RR(P_j)$ by the evaluator SRRA R_i at time instance t_c, (2) may be rewritten as following:

$$RR^{R_i}(P_j) = w_{R_i} \cdot RR^{R_i,t_c}(P_j) + \sum_{k=1}^{n} w_{R_k} \cdot RR^{R_k,t_c}(P_j) \quad (7)$$

where the rating $RR^{R_x,t_c}(P_j)$ is a function of $RR^{R_x,t_d}_{post}(P_j)$. A wide range of functions may be defined. We restrict our attention to two families of functions: exponential and polynomial. Other functions could be defined as well. Expressions (8) and (9) provide a formal model of the exponential and polynomial related family of functions concerning the $RR^{R_x,t_c}(P_j)$ reputation rating.

$$RR^{R_x,t_c}(P_j) = [1 - \{\frac{1}{1-e} \cdot [1 - \exp(\frac{t_c - t_d}{t_c})^{1/\vartheta}]\}] \cdot RR^{R_x,t_d}_{post}(P_j) \quad (8)$$

$$RR^{R_x,t_c}(P_j) = [1 - (\frac{t_c - t_d}{t_c})^{1/\vartheta}] \cdot RR^{R_x,t_d}_{post}(P_j) \quad (9)$$

for which it stands $\underset{t_c \to t_d}{RR^{R_x,t_c}(P_j)} \to RR^{R_x,t_d}_{post}(P_j)$ and $\underset{t_c >> t_d}{RR^{R_x,t_c}(P_j)} \to 0$. Specifically, the bigger the quantity $t_c - t_d$ is, the lower is the reputation value for the SRPA P_j acquired. As it may be observed from (8) and (9), these families of functions represent an infinite number of different members, one for each value of ϑ. Parameter ϑ has been included in order to highlight the different patterns with respect to the adopted rate of decrease. For example, adopting a Boulware policy [10] could lead to minor modification (decrease) of the reputation rating, until $\frac{t_c - t_d}{t_c} \to 1$ (i.e., $\frac{t_d}{t_c} \to 0$), whenupon, the minimum reputation value is assumed. Otherwise, exploiting the Conceder policy [11] could lead to the minimum reputation value in quite a short time period (the quantity $t_c - t_d$ is quite small).

IV. Related Research

The issue of trust has been gaining an increasing amount of attention in a number of research communities. In [12], the current research on trust management in distributed systems is surveyed and some open research areas are explored.

In [13] a typology is proposed summarizing existing works on reputation across diverse disciplines (i.e., economical studies, scientometrics, computer science, evolutionary biology, sociology). Specifically, reputation is assumed to be context dependent, it can be viewed as global or personalized, can be used to describe an individual or group of individuals. Individual reputation can be derived either from direct encounters or/and observations made about other agent's encounters with others (direct reputation) or from inferences based on information gathered indirectly (indirect reputation) comprising prior beliefs an agent has about strangers,

reputation estimates of the group an agent belongs to and information gathered according to a mechanism similar to the "word of mouth" propagation of information for human. Based on this typology, the authors have studied the relative strengths of different notions of reputation in a set of evolutionary games.

In [14] the authors, after discussing on desired properties for reputation mechanisms for online communities, describe Sporas and Histos reputation mechanisms for loosely and highly connected online communities, respectively, that were implemented in Kasbah electronic marketplace. Sporas reputation mechanism provides a global reputation value for each member of the online community, associated with them as part of their identity. Histos builds a more personalized system, illustrating pairwise ratings as a directed graph with nodes representing users and weighted edges representing the most recent reputation rating given by one user to another.

In [15], the authors base the decision concerning the trustworthiness of a party on a combination of local information acquired from direct interactions with the specific party (if available) and of information acquired from witnesses (trusted third parties that have interacted with the specific party in the past). In order to obtain testimonies from witnesses, a trust net is built by seeking and following referrals from its neighbours, which may be adaptively chosen. Their approach relies upon the assumption that the vast majority of agents provide honest ratings, in order to override the effect of spurious ratings generated by malicious agents. In [16], some models of deception are introduced and it is studied how to efficiently detect deceptive agents following these models based on a variant of the weighted majority algorithm applied to belief functions. Specifically, each agent maintains a weight for each of the other agents whose testimonies it requests. This weight estimates how credible the given witness is. The weights from witnesses are tuned so that the relative weight assigned to the successful advisors is increased whereas it is decreased for the unsuccessful witnesses.

V. Conclusions

From a market based perspective, entities composing dynamic distributed computing environments may be classified into two main categories that are, in principle, in conflict. These are the Service Resource Requestors (SRRs) wishing to use services and/or exploit resources offered by the other system entities and the Service Resource Providers (SRPs) that offer the services/resources requested. In general, under the assumption that a number of SRPs may handle and serve the SRRs requests with the same terms and conditions, the SRRs may decide on the most appropriate SRP for the service / resource requested on the basis of their reputation rating (*reliability related factor*). In this study, a reputation mechanism is proposed which helps estimating SRPs trustworthiness and predicting their future behaviour, taking into account their past performance in consistently satisfying SRRs' expectations. Specifically, SRPs are rated with respect to whether they honoured or not the agreements they have established with the SRRs. The reputation mechanism is distributed, considers both first-hand information (acquired from the SRR's direct past experiences with the SRPs) and second-hand information (disseminated from other SRRs' past experiences with the SRPs), while it exhibits a robust behaviour against inaccurate reputation ratings.

The reputation framework designed has been adopted by self-interested autonomous agents and has performed well. Initial results indicate that the proposed SRP selection scheme (based only on their reputation ratings) exhibits a better performance with respect to random SRP selection, which is on average 30%, in case honest feedback provision is assumed for the vast majority of the witnesses. Future plans involve our frameworks' extensive empirical evaluation incorporating witnesses misbehaviour and against existent reputation models and trust frameworks.

References

[1] M. Louta, I. Roussaki, and L. Pechlivanos, "Reputation Based Intelligent Agent Negotiation Frameworks in the E-Marketplace," in *2006 Proc. International Conference on E-Business*, Setubal, Portugal, pp. 5-12.

[2] J. Callas, L. Donnerhacke, H. Finney, D. Shaw, R. Thayer. (2007). *OpenPGP Message Format* (RFC 4880, IETF). Available: http://www.ietf.org/rfc/rfc4880.txt.

[3] D. Cooper, S. Santesson, S. Farell, S. Boeyen, R. Housley, W. Polo. (2007). *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile* (Internet Draft, IETF). Available: http://www.ietf.org/internet-drafts/draft-ietf-pkix-rfc3280bis-09.txt.

[4] Y. Atif, "Building Trust in E-Commerce," *IEEE Internet Computing Magazine*, vol. 6, no. 1, pp. 18-24, 2002.

[5] G. Zacharia and P. Maes, "Trust management through reputation mechanism," *Applied Artificial Intelligence Journal*, vol. 14, no. 9, pp. 881-908, 2000.

[6] eBay, http://www.ebay.com.

[7] OnSale, http://www.onsale.com/exchange.htm.

[8] M. He, N. Jennings, and H. Leung, "On agent-mediated electronic commerce," *IEEE Transactions on Knowledge and Data Engineering*, vol. 15, no. 4, pp. 985-1003, 2003.

[9] L. Kaelbling, M. Littman, and A. Moore, "Reinforcement Learning: A Survey," *Journal of Artificial Intelligence Research*, vol. 4, pp. 237-285, 1999.

[10] H. Raiffa, *The Art and Science of Negotiation*. Cambridge, USA: Harvard University Press, 1982.

[11] D. Pruitt, *Negotiation Behavior*. Academic Press Inc., 1981

[12] H. Li and M. Singhal, "Trust Management in Distributed Systems," *IEEE Computer*, vol. 40, no.2, pp. 45-53, 2007.

[13] L. Mui, A. Halberstadt, and M. Mohtashemi, "Evaluating Reputation in Multi-Agent Systems," in *Trust, Reputation, and Security: Theories and Practice*, LNAI vol. 2631, R. Falcone et al;, Eds. Berlin Heidelberg: Springer-Verlag, 2003, pp. 123-137.

[14] G. Zacharia, A. Moukas, and P. Maes, "Collaborative Reputation Mechanisms in Electronic Marketplaces," in *Proc. 32nd Hawaii International Conference on System Sciences*, Los Alamitos, CA, USA, 1999, pp 1-7.

[15] B. Yu and M. Singh, "A social mechanism of reputation management in electronic communities," in *Cooperative Information Agents IV - The Future of Information Agents in Cyberspace*, LNCS vol. 1860, M. Klusch and L. Kerschberg Eds. Berlin Heidelberg: Springer-Verlag, 2000, pp. 154-165.

[16] B. Yu and M. Singh, "Detecting Deception in Reputation Management," in *Proc. 2nd International Joint Conference on Autonomous Agents and Multi-Agent Systems*, Melbourne, Australia, 2003, pp. 73-80.