Trust Management Framework for Intelligent Agent Negotiations in Ubiquitous Computing Environments

Malamati Louta[1]✉, Angelos Michalas[2], Ioannis Anagnostoupoulos[3], Dimitrios Vergados[4]

[1]*Harokopio University of Athens, Department of Informatics and Telematics*
GR-17671, Athens, Greece
e-mail: louta@telecom.ntua.gr

[2]*Technological Educational Institute of Western Macedonia, Department of Informatics and Computer Technology*
GR-52100, Kastoria, Greece
e-mail: amichalas@kastoria.teikoz.gr

[3]*University of Aegean, Department of Information and Communication Systems Engineering*
Karlovassi, GR-83200, Samos Island, Greece
e-mail: janag@aegean.gr

[4]*University of Piraeus, Department of Informatics*
Piraeus, GR-18534, Greece
e-mail: vergados@unipi.gr

Abstract

In dynamic ubiquitous 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. Thereafter, under the assumption that a number of SRPs may handle the SRRs requests, the SRRs may decide on the most appropriate SRP for the service / resource requested on the basis of a weighted combination of the evaluation of the quality of their offer (performance related factor) and of their reputation rating (reliability related factor). The proposed trust management framework 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 designed mechanisms have been empirically evaluated simulating interactions among self-interested agents, exhibiting improved performance with respect to random SRP selection.

Key Words: Distributed Computing Environments, Intelligent Multi Agent Systems, Trust Management, Collaborative Reputation Mechanism, Service Resource Requestors/Providers.

1 INTRODUCTION

The establishment of trust constitutes an issue of outmost importance for the success of the highly dynamic ubiquitous computing environments, commonly perceived as offering at the same time both opportunities and threats. Systems are composed by various entities, which, seeking for the maximization of their welfare while achieving their own goals and aims, may misbehave, acting selfishly, thus, leading to a significant deterioration of system's performance. Additionally, system entities may appear and disappear at any time, while anonymity constitutes an easy choice. In general, misbehaviour (i.e., deviation from regular functionality, which may be unintentional due to faults or intentional in order for selfish parties to take advantage of certain situations) can significantly degrade the system's performance, which still requires for high degree cooperation among its various entities. Thus, in order to cope with misbehaviour, trust mechanisms should be exploited so as to build the necessary trust relationships among the parties [1], enabling them to automatically adapt their strategies to different levels of cooperation and trust.

From a market-based perspective, the roles of the system entities in the highly competitive and dynamic ubiquitous computing environments (including pervasive, peer-to-peer, grid computing, Mobile Ad-Hoc Networks, sensor networks and electronic communities), 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 service features trustworthily, at a high quality level in a timely and cost efficient manner. At this point it should be noted that a single entity may at the same time act as a Requestor and as a Provider for different services / resources.

The aim of this paper is, in accordance with efficient service operation objectives, to propose enhancements to the sophistication of the functionality that can be offered by

ubiquitous intelligent computing environments. Service/Resource Requestors should be provided with mechanisms that enable them to find the most appropriate Service/Resource Providers, i.e., those offering the desirable quality of service at a certain time period in a cost efficient manner, while exhibiting a reliable behavior (i.e., abide by established contract terms and conditions). Such mechanisms may entail a wide variety of negotiation mechanisms, including auctions, bilateral (*1* to *1*) and/or multilateral (*M* to *N*) negotiation models and strategies as well as posted offer schemes (i.e., a nonnegotiable, take-it-or-leave-it offer) in order to establish the 'best' possible contract terms and conditions with respect to service/resource access and provision [2], in conjunction with trust mechanisms in order to build the necessary trust relationships among the system entities.

Traditional models aiming to avoid strategic misbehaviour are based on authentication of identities and authorization schemes by exchanging digital, cryptographically signed certificates/credentials in order for the involved parties to establish a trust relationship [3][4] or involve *Trusted Third Parties* (TTPs) or intermediaries [5] that monitor every transaction. However, these models 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, considered to be sufficient for many multi-agent applications [6]. Reputation mechanisms establish trust by exploiting learning from experience concepts [7], [8] in order to obtain a reliability value of system participants in the form of rating based on other entities' view/opinion. Current reputation system implementations in the context of e-commerce systems 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) [9], [10]. In general, a reputation system is considered to sustain rational cooperation and serve as an incentive for good behaviour because good players are rewarded by the society, whereas bad players are penalized. 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.

In the context of this study, under the assumption that a number of SRPs may handle the service/resource requests, the SRRs may decide on the most appropriate SRP for the service/resource provisioning based on an evaluation of the quality of SRPs offer combined with an estimation of SRPs reliability. The quality of the SRPs offers is introduced as there may in general be different levels of SRRs' satisfaction with respect to the various offers, while some proposals may be completely unacceptable, not satisfying the requirements posed by SRRs. The reliability related factor takes into account SRPs behaviour with respect to honouring the agreement contract terms reached via negotiation process in the past and provides an estimation of their expected behaviour in the future, exploiting learning from experience techniques.

Hereafter, 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 they honoured or not the agreements established with the SRRs, thus introducing the concept of trust among the involved parties. The reputation mechanism can be analyzed as depicted in figure 1. In general, its core requires a method for evaluating the target SRP's reputation rating based on SRR's direct experiences, and a method for estimating SRP's overall rating taking into account the view and opinion of a number of other SRRs (*witnesses*) on their past experiences with the SRP. The reputation mechanism is decentralized and exhibits robust behaviour against inaccurate reputation ratings (intentionally and/or unintentionally provided).

The contribution of this paper lies in the design and mathematical formulation of a decentralized and collaborative reputation rating mechanism, enabling the formation of SRPs reputation rating values, reflecting their reliability, in an accurate and time-efficient manner, while being resilient to inaccurate information intentionally and/or unintentionally provided. The work of this paper is related to pertinent previous work in the literature, since trust establishment and management is a topic that attracts attention of the researchers. 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 on the most appropriate SRP on a weighted combination of the evaluation of the quality of the SRPs' offer (*performance related factor*) and of their reputation rating (*reliability related factor*).

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 [11]. Thus, Service/Resource Requestor Agent (*SRRA*) is introduced and assigned with the role of capturing the SRR preferences, requirements and constraints regarding the requested service / resource, delivering them in a suitable form to the appropriate SRP entity, acquiring and evaluating the corresponding SRPs' offers, and ultimately, selecting the most appropriate SRP on the basis of the quality of its offer and its reputation rating. Service/Resource Provider Agents (*SRPAs*) are the entities acting on behalf of the SRPs. Their role would be to collect the SRR preferences, requirements and constraints and to make a corresponding offer, taking also into account certain environmental criteria. 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 related research literature is revisited. Section 3 presents the fundamental concepts and consideration of the proposed collaborative reputation mechanism, aiming to offer an efficient way of building the necessary level of trust in the ubiquitous computing environments. In Section 4 and 5, the reputation ratings system and the SRR's decision on the most appropriate SRP with respect to the service/resource requested are mathematically formulated. Section 6 provides a set of indicative results of the efficiency of the proposed trust management framework. Finally, in Section 7, conclusions are drawn and directions for future plans are given.

2 RELATED RESEARCH

The issue of trust has been gaining an increasing amount of attention in a number of research communities. In [12], a set of aspects is proposed to classify computational trust and reputation models. These classification aspects have been selected taking

into account the characteristics of current computational models. Specifically, the classification dimensions considered are the following: the conceptual model of reference (cognitive or game theoretical trust and reputation models), the information sources taken into account for trust and reputation value calculation (direct experiences & witness information, sociological aspects of agents' behavior, prejudice), the visibility types of trust and reputation (global or subjective values property), the model's context dependence (capability of dealing with several contexts at the same time maintaining different trust/reputation values associated to these contexts for each partner), the capacity of the model to deal with agents showing different degrees of cheating behavior (consideration of non cheating behavior, or incorporation of specific mechanisms to deal with liars), the type of information expected from witnesses (Boolean information or continuous measures), the trust/reputation reliability measure (a single value associated to the trust or reputation value, calculated considering the number of experiences, the reliability of witnesses, how old is the information used to build trust). As a next step a representative selection of trust and reputation models are classified on the basis of the aforementioned criteria. Based on this study, the authors believe that a good mechanism to increase efficiency of actual trust and reputation models and also to overcome the lack of confidence in e-markets is the introduction of sociological aspects as part of these models.

[13] presents a comparative analysis and assessment of on-line reputation mechanisms with respect to legally enforceable contractual arrangements in terms of their ability to promote trust and induce cooperative behavior of involved entities in a wide range of moral hazard settings. For the comparative analysis a binary reputation mechanism was used. The authors concluded that, as a result to the advance of information technology which has enabled the formation of low-cost global reputation networks, online reputation mechanisms may be the preferred institutions to promote cooperation among economic agents, augmenting or substituting for traditional litigation-based contract enforcement mechanisms, or enabling a more efficient outcome in markets where cooperative behavior was unsustainable.

In [14], the current research on trust management in distributed systems is surveyed and some open research areas are explored. Specifically, the authors discuss on

representative trust models in the context of P2P systems, mobile ad-hoc networks and electronic communities including public-key cryptography, the resurrecting duckling model and distributed evidence & recommendation based trust models, while trust / reputation value storage in conjunction with the preservation of its consistency, mitigation of the impact of false accusations / malicious behaviour and combination of trust values of different applications are identified as research issues to be further explored.

In [15], the authors propose a trust management framework, covering reputation based and credential based trust mechanisms in an independent layer in distributed applications. Their TrustEngine System has been designed as an open system, enabling, thus, the incorporation of different, independent trust components. The main goal was to develop trust management infrastructure and tools to be exploited by distributed applications. The TrustEngine architecture was applied in a scenario example based on a set of possible requirements in the federated medical services.

In [16] 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. [17] introduces PeerTrust, an adaptive and dynamic reputation based trust model that helps participants/peers to evaluate the trustworthiness of each other based on the community feedback about participants' past behavior. Five important factors are taken into account for the calculation of trust: the feedback a peer obtains from others, the feedback scope (such as the total number of transactions that a peer has with other peers), the credibility factor of the feedback source, the transaction context factor for discriminating mission critical transactions from less or non critical ones and the community context factor for addressing community related characteristics and vulnerabilities. Regarding the credibility factor of the feedback source, the authors first used a function of the trust value as its credibility value; that is feedback

from trustworthy peers is considered more credible. However, it is possible for a peer to maintain a good reputation by performing high quality services but send malicious feedback to its competitors. In such a case the credibility factor is calculated as a personalized similarity measure between the experiences with other partners in the market.

In [18], reputation is considered to be a multi-faceted concept. Thus, it is built taking into account individual, social and ontological dimensions. Specifically, an agent's reputation is formed considering previous direct interactions with the specific agent (individual reputation formation), the interactions with the other members of the group to which the agent under evaluation belongs, the opinion the group of the requesting agent has about the agent being evaluated, the opinion the group of the requesting agent has about the group the agent being evaluated belongs (social reputation formation) and reputation values on different aspects (ontological reputation formation). In [19], the authors for their trust management model consider only information on dishonest interactions (e.g., complaints filed about one agent) assuming that usually trust exists and malicious behavior is the exception. In order to store and retrieve data on agents' behavioral complaints the authors utilize P-Grid method forming in essence a virtual binary search tree. In [20], reputation is established in relation with the position of each member of a community within the corresponding social network. NodeRanking algorithm (inspired by well-known ranking algorithm for web pages) is proposed for creating a ranking of reputation ratings of community members by means of the social network graph. Reputation systems besides estimating the reliability of a person (or agent representing a system entity) have additionally been utilized for assessing the reliability of a resource offered in a system in order to estimate the level of risk in a specific resource. In [21], reputation sharing is realized through a distributed polling algorithm by which resource requestors can evaluate the reliability of both servents (hosting the resources) and resources before initiating the download.

[22] presents certified reputation model of trust, which allows agents to actively provide third party references about their previous performance as a means of building up trust. In essence, the burden of obtaining and maintaining trust information is moved from the trust evaluator to the agent being evaluated. Their

proposed model is shown to be robust against various types of collusion. Even though the proposed model has lower predictive power than the other types of trust / reputation (where all bad and good ratings can be collected) it has a very low time, communication and processing cost compared to witness reputation frameworks.

3 TRUST FRAMEWORK FUNDAMENTALS

Assuming the presence of M SRPAs negotiating with a SRRA for the terms and conditions of the provision of a service / resource, the SRRA can decide on the most appropriate SRPA based on the evaluation of the SRPA's offer quality combined with an estimation of the SRPA's expected behaviour. In our approach this estimation constitutes the reliability related factor, which is introduced in order to reflect whether the SRP finally provides to the SRR the service / resource that corresponds to the established contract terms or not. The SRPA's reliability is reduced whenever the SRP does not honour the agreement contract terms reached via the negotiation process. The SRPAs' performance evaluation factor is based on the fact that there may in general be different levels of satisfaction with respect to the various SRPAs' offers. In this respect, there may be SRPAs that, in principle, do not satisfy the SRRA with their offer.

In this study, the authors propose a trust management framework for SRPs reliability assessment in an accurate and time-efficient manner exploiting a decentralized and collaborative reputation mechanism, which forms SRPs reputation ratings reflecting whether SRPs abide by the established contract or not. The designed reputation mechanism considers both first-hand information (acquired from the SRRA's past experiences with the SRPAs) and second-hand information (disseminated from other SRRAs), while learning from experience techniques are utilized. To be more specific, each SRRA keeps a record of the reputation ratings of the SRPAs it has negotiated with and 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 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 based information concerning SRPAs' reputation ratings. Specifically, a basic assumption is that each SRRA is willing to share their experiences and provide whenever asked for the reputation ratings of the SRPAs formed on the basis of their 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 SRPs providing a specific service / resource as well as a list of SRRs that have previously interacted with a specific SRP. This solution results to the following advantages. First, the information maintained centrally by the SRPRB is the minimum possible, since the reputation rating values are safely stored in each SRR. Thus, central storage requirements and complexity are minimized. Second, most of the messages are exchanged among the evaluator SRRA and the witnesses SRRAs, resulting in improved system performance characterized by a major reduction of communication between the SRRA and the SRPRB. This dramatically reduces the response time of the SRPRB, which may handle multiple concurrent requests from requestor SRRAs during normal operation of the system. Third, the SRPRB approach allows direct communication among SRRAs for reputation ratings exchange. System robustness is increased since its operation could continue even in cases where the SRPRB is not reachable (either the SRPRB or the network link to the SRPRB is out of service). Fourth, the system exhibits robust behaviour against denial of service attacks and various types of collusion.

At this point some clarifications with respect to the proposed model should be made. First, the reliability of SRPAs is treated as a behavioural aspect, independent 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, enabling this way the formation of SRPs

reliability in a time – efficient manner. Second, 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 after contacting the SRRAs. To this respect, SRPA's reputation ratings provided by the witness SRRAs may be attributed with a relatively low significance factor.

In the context of this study, we consider that each SRRA is associated with a weighting factor 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 weighting factor 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. Potential dissemination of misinformation on behalf of a witness is identified in case the overall SRPs reputation rating as estimated by the evaluator is beyond a given distance from the rating provided by the witness, in which case its honesty probability is accordingly decreased. 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). In order to further improve the correctness of the reputation ratings assessment, time effects have been introduced in our mechanism, modeling the fact that more recent events should weigh more in the evaluation of the target SRPs overall reputation rating by the evaluator. Thus, potential modifications of the SRPs behaviour in recent past are addressed.

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 SRPA. A learning period is required in order for the SRRAs to obtain fundamental information for the SRPAs. During the learning period and in case reputation specific information is not available to the SRRA (both through its own experiences and through the witnesses) or it highly possible to be outdated, the reliability related factor is not considered for the SRPA selection. Thus, the SRP's will be selected only on the basis of the quality of their offers. At this point 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, it should be mentioned that 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 provisioning process) a mechanism for evaluating whether the service quality was compliant with the picture promised during the negotiation phase.

4 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 ubiquitous 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 regarding the provision of service s_i which without loss of generality is provided by all candidate SRPAs $P = \{P_1, P_2, ...P_M\}$. The evaluator SRRA R_i will form the SRPAs' overall 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 witnesses ($R_w \subseteq R = \{R_1, R_2, ...R_N\}$). Thereafter, the R_i contacts the witnesses in order to get feedback reports on the behaviour of the P_j.

4.1 ESTIMATING TARGET SRPA'S REPUTATION RATING BASED ON SRRA'S DIRECT EXPERIENCES

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

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

where $RR^{R_x}_{post}(P_j)$ and $RR^{R_x}_{pre}(P_j)$ are the SRPA P_j reliability based rating after and before the updating procedure. It has been assumed that $RR^{R_x}_{post}(P_j)$ and $RR^{R_x}_{pre}(P_j)$ lie within the [0,1] range, where a value close to *0* indicates a misbehaving SRP. $rr^{R_x}(P_j)$ is a (reward) function reflecting whether the service quality is compliant with the picture established during the negotiation phase and $E[rr^{R_x}(P_j)]$ is the mean (expected) value of the $rr^{R_x}(P_j)$ variable. In general the larger the $rr^{R_x}(P_j)$ 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 $\lim_{RR_{pre}^{R_x}(P_j) \to 0} l(RR_{pre}^{R_x}(P_j)) \to 1$ and $\lim_{RR_{pre}^{R_x}(P_j) \to 1} l(RR_{pre}^{R_x}(P_j)) \to 0$.

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

4.2 EVALUATING TARGET SRPA'S OVERALL REPUTATION RATING

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

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

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 (e.g., consider equation (1)). As may observed from equation (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, while the second factor depends on information regarding P_j past behaviour gathered

from n witnesses. At this point it should be noted that SRRAs may serve as witnesses for the estimation of the overall reputation of the target SRPA P_j in case they have formed an accurate picture regarding the SRPA's reliability related behavioural aspects (e.g., they have been involved with P_j for at least a pre-defined number of transactions with transactional value above a pre-specified threshold, in which case we assume that a learning period has been completed).

Weight $w_{P_j}^{R_i}(R_x)$ ($x \in \{1,2,...n\}$) provides the relative significance of the reputation rating of the target SRPA P_j as formed by the SRRA R_x to the overall reputation rating estimation by the evaluator R_i. In general, $w_{P_j}^{R_i}(R_x)$ 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 transactions 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 $w_{P_j}^{R_i}(R_x)$ are normalized to add up to 1 (i.e., $w_{P_j}^{R_i}(R_x) + \sum_{k=1}^{n} w_{P_j}^{R_i}(R_k) = 1$). Thus, weight $w_{P_j}^{R_i}(R_x)$ may be given by the following equation:

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

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 $\sum_{m=1}^{N_T} TV_m^{R_x}(P_j)$ 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 $TL^{R_i}(R_i) = 1$.

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, witness R_x is considered to misreport his/her past experiences, if the target P_j overall reputation rating $ORR^{R_i}(P_j)$ as estimated by equation (2) is beyond a given distance of the rating $RR^{R_x}(P_j)$, in which case the following expression holds $\left|ORR^{R_i}(P_j) - RR^{R_x}(P_j)\right| > e$, where e is the predetermined distance level. The later expression enhances the system with resilient functionalities against inaccurate reputation ratings provided by malicious agents. For example, assume the existence of an SRRA R_k who wants to manipulate the reputation rating formation of the evaluator agent R_i for SRPA P_l. In the light of this assumption, the SRRA R_k would provide a forged reputation rating $RR^{R_k}(P_l)$. SRRA R_i identifies the false feedback in case $RR^{R_k}(P_l)$ distance from $ORR^{R_i}(P_l)$ exceeds the e predefined value. In such a case, the SRRA's R_k trustworthiness, reflecting in a dynamic manner whether the feedback provided is truthful and accurate, may be decreased in a similar manner to equation (1), while the significance factor of this feedback to the overall reputation rating formation would be accordingly decreased (equation (3)).

4.3 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 overall reputation rating $ORR^{R_i}(P_j)$ by the evaluator SRRA R_i at time instance t_c that a service/resource request has originated from the evaluator R_i, equation (2) may be rewritten as following:

$$ORR^{R_i,t_c}(P_j) = w_{P_j}^{R_i}(R_i) \cdot TrF(t_c, t_{d_i}) \cdot RR^{R_i,t_{d_i}}(P_j) + \sum_{k=1}^{n}[w_{P_j}^{R_i}(R_k) \cdot TrF(t_c, t_{d_k}) \cdot RR^{R_k,t_{d_k}}(P_j)] \quad (4),$$

where the rating $RR^{R_x,t_{d_x}}(P_j)$ is the direct reputation rating of SRPA P_j as formed by SRRA R_x after a transaction d has been completed at time instance t_{d_x}. Factor $TrF(t_c, t_{d_x})$ is a time related factor and is introduced in order to weigh up (down) recent (old) information. A wide range of functions may be defined for the estimation of the $TrF(t_c, t_{d_x})$ factor. We restrict our attention to two families of functions: exponential and polynomial. Other functions could be defined as well. Expressions (5) and (6) provide a formal model of the exponential and polynomial related family of functions concerning the $TrF(t_c, t_{d_x})$ factor.

$$TrF(t_c, t_{d_x}) = 1 - \{\frac{1}{1-e} \cdot [1 - \exp(\frac{t_c - t_{d_x}}{t_c})^{1/\vartheta}]\} \quad (5),$$

$$TrF(t_c, t_{d_x}) = 1 - (\frac{t_c - t_{d_x}}{t_c})^{1/\vartheta} \quad (6),$$

for which it stands $\underset{t_c \to t_{d_x}}{TrF(t_c, t_{d_x})} \to 1$ and $\underset{t_c >> t_d}{TrF(t_c, t_{d_x})} \to 0$. 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 equations (5) and (6), 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 [23] 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 [24] could lead to the minimum reputation value in quite a short time period (the quantity $t_c - t_d$ is quite small).

4.4 UPDATING OUTDATED SRRAS REPUTATION RELATED INFORMATION

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 quality of the offers proposed to the SRRA and 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 (either on the basis of their performance or on the basis of their reliability), the misbehaving SRPAs have to improve on their potential performance so as to overcome the barrier raised by their low reputation rating.

In order to take into account new SRPAs that enter the system and/or not to exclude 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 in case they abide by the contract terms and conditions, 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 the SRPAs' performance and omit the SRPAs' reputation rating values until possible outdated information the system possesses is updated. Otherwise, a Boltzmann exploration strategy could be adopted [25]. In the context of this study, the authors consider the reduction of the SRPs' reliability related values to the pre-specified minimum (i.e., 0.1) in case a predetermined number $N_{\max}$ of transactions have been completed in the system, whenupon the SRPRB component sends a warning message to all SRRAs registered in its database. At this point it should be noted that $N_{\max}$ is considered to assume a quite big value in order not to constitute a disincentive for honest behavior.

5 DECISION ON THE 'BEST' SERVICE/RESOURCE PROVIDER

As already mentioned, under the assumption that a number of SRPs may handle the SRRs requests, the SRRs may decide on the most appropriate SRP for the service / resource requested on the basis of a weighted combination of the evaluation of the quality of their offer (*performance related factor*) and of their reputation rating (*reliability related factor*). Considering a take-it-or-leave-it offer scheme, the evaluator SRRA R_i decides on the most appropriate SRPA P_j (i.e., the SRPA best serving its current service / resource request) and selects the Provider that maximizes the value of the following formula:

$$A_{PR}(P_j) = w_p \cdot U^B(C^{P_j}) + w_r \cdot ORR^{R_i}(P_j) \quad (7),$$

As you may observe, $A_{PR}(P_j)$ is an objective function that models the performance and the reliability of the SRPA P_j. Among the terms of this function there can be the overall anticipated SRRA satisfaction $U^B(C^{P_j})$ with respect to the contract/offer proposed by the SRPA P_j to the evaluator R_i [26], [23] and the reputation rating of the target P_j.

For the calculation of the utility function $U^{R_i/P_j}(C^{P_j})$, quantifying the overall anticipated satisfaction of its owner entity (either SRRA R_i or SRPA P_j) with respect to the contract offered (and ultimately established), we have adopted the methodology proposed in [26]. Specifically, the SRRA's / SRPA's utility function concerning contract C^{P_j} offered by SRPA P_j to the evaluator SRRA R_i is a weighted linear additive function of the utility of each contract issue considered (i.e., $U^{R_i/P_j}(C^{P_j}) = \sum_{l=1}^{n} w_{c_l} \cdot U_{c_l}^{R_i/P_j}$, where c_l with $l = 1,...n$ is the contract issue under negotiation), which in turn may be of any continuous and monotonic functional form (e.g., linear, polynomial, exponential, multiplicative, quasi-linear) of the contract issue value and of the decision issues values (issues that are not under negotiation, but, however, have an impact on the evaluation of the utility function, such as time deadline, delivery date, product expiration date) at the time an offer is given (i.e.,

$U_{c_l}^{R_i/P_j}(v_{c_l}, d_k^t)$, where v_{c_l} is the contract issue's c_l value and d_k^t is the value of the decision issue d_k at time instance t the SRPA's offer is evaluated by the SRRA). For simplicity, utility estimations are normalised for both agents (i.e., belong in the $[0,1]$ interval).

In principle, SRPs and SRRs present conflicting interests and consist opposing forces with respect to the values of the contract issues under negotiation. For instance, any Requestor aims to have access and use high quality services / resources at the lowest possible price, while the most common objective of Providers is the maximisation of their profit, which usually leads them to offer lower quality at high prices. This applies for most contract issues (e.g., the delivery time of the service). Thus, under the same conditions, in case higher values of contract issue c_l result in higher (lower) utility for the SRP, at the same time they result in lower (higher) utility for the SRR. Nevertheless, it must be mentioned that in a few cases the SRPs and SRRs may have a mutual interest for the value of a contract issue [23]. In consequence, the utility functions must verify that given a SRPA P_j and a SRRA R_i negotiating values for contract issue c_l, then: $\left[\frac{\partial(U_{c_l}^{P_j})}{\partial v_{c_l}}\right] \cdot \left[\frac{\partial(U_{c_l}^{R_i})}{\partial v_{c_l}}\right] < 0$.

Weights w_p and w_r provide the relative value of the anticipated user satisfaction and the reputation related part. It is assumed that weights w_p and w_r are normalized to add up to 1 (i.e., $w_p + w_r = 1$). At this point it should be noted that one of the two factors (anticipated SRRA satisfaction or SRPA reputation rating) can be omitted in certain variants of the general problem version considered in this paper.

Hereafter we describe the algorithm, on which the SRRAs and the SRPAs base the accomplishment of their tasks, after the learning period. The steps followed are graphically depicted in Figure 2.

Step 1. The SRRA R_i component is acquainted with the preferences, requirements and constraints of an SRR system entity regarding provisioning of service s_i. The strict requirements and constraints posed are expressed as non-negotiable

parameters that assume a fix value. The preferences are modelled as a set of m issues under negotiation c_l $\{l = 1,...,m\}$, whose acceptable values lie within the range $c_l \in \lfloor m_l, M_l \rfloor$ and the lower limit on the anticipated satisfaction $U_{\min}^{R_i}$ that the SRR wants to experience during the service usage.

Step 2. The SRRA R_i obtains the list of candidate SRPs $P = \{P_1, P_2, ...P_M\}$ and the references of the respective SRPAs from the SRPRB component. Additionally, it retrieves a list of witnesses for each candidate SRPA and their respective references.

Step 3. The SRRA R_i component activates the appropriate negotiator entities (e.g., threads or mobile agents). Each negotiator entity will undertake the interactions with a candidate SRPA $P_j \in P$. The negotiator entities will be under the control of the SRRA R_i.

Step 4. Each SRPA $P_j \in P$ component evaluates the current environmental conditions and based on this estimation provide the respective negotiator entity with an attractive offer for the user preferences, requirements and constraints regarding service s. The offer is assumed to follow a take-it-or-leave-it scheme expressed by a contract C^{P_j} composed of values for each issue c_i under negotiation.

Step 5. Each negotiator entity evaluates the quality of the final offer of each candidate SRPA $P_j \in P$ and the result $U^{R_i}(C^{P_j})$ (if $U^{R_i}(C^{P_j}) \geq U_{\min}^{R_i}$) is sent to the SRRA R_i component.

Step 6. The SRRA R_i component activates the appropriate entities that will undertake the task of retrieving from the relevant witnesses the reputation rating of the candidate SRPAs, whose offer is acceptable by the R_i (i.e., the values of all issues under negotiation lie within the range $c_l \in \lfloor m_l, M_l \rfloor$, and $U^{R_i}(C^{P_j}) \geq U_{\min}^{R_i}$). These reputation ratings are sent back to the SRRA R_i.

Step 7. The SRRA R_i estimates the overall reputation rating of each candidate SRPA $P_j \in P$, comprising both the evaluator's own experiences as well as the view of the witnesses on the basis of the schemes proposed in this section.

Step 8. The SRRA R_i selects a SRPA $P_j \in P$ by comparing the objective function values that each SRPA has scored taking into account its performance and its reliability.

Step 9. The SRRA R_i after the completion of service delivery updates the reputation rating of the selected SRPA P_j.

Step 10. End.

6 RESULTS

This section provides some indicative results on the behaviour of the Service/Resource Provider selection mechanisms that are proposed in this paper. We hereafter assume the existence of an area that falls into the domain of $P = \{P_1, P_2, ...P_M\}$ candidate Service Providers (that is a specific request may be handled by any of the candidate SRPs belonging to the set P). Furthermore, it is assumed that N different Service/Resource Requestors access the area. SRRs are interested for the same service/resource, differentiated however with respect to the quality/quantity level required. Hereafter, SRRs are classified in K different classes on the basis of the requirements and constraints with respect to service / resource provisioning. In order to make the test case more realistic (or general), all SRPs are not assumed to offer all possible quantity/quality levels. SRPs that do not offer the required quality/quantity level for the service/resource as requested by the SRR class R_i constitute the $I(R_i)$ set, which comprises SRPs that are inappropriate for the specific request and should therefore be excluded. Hereafter, it is assumed that $N = 1000$, $K = 10$ (i.e., each SRR class comprises 100 SRRs) and $M = 10$. Table 1 presents the set of SRPs that are inappropriate for service/resource requests originating from each SRR class.

As a first step, the proposed framework was empirically evaluated by simulating the interactions among SRRAs and SRPAs considering the simplest possible case.

Specifically, it was assumed that the SRPAs, which can handle the request satisfying all requirements of the requestor class, offer exactly the same contract to the evaluator SRRAs (the same service/resource characteristics with exactly the same terms and conditions). In the light of the assumption made, the Service/Resource Provider selection is reduced to choosing the one with the highest reputation value (second factor contributing to equation (7)), since the overall satisfaction stemming from the proposed contract (expressed by the first factor of equation (7)) contributes to the objective function value the same amount for all candidate SRPs. This way, the acquisition of an initial set of indicative results that show the behaviour of our proposed trust management framework is enabled.

Figure 3 illustrates the direct reputation ratings of each SRP, as estimated by SRR class R_2 (i.e., mean SRPs reputation ratings considering the 100 SRRs constituting class R_2) after 150 transactions have been conducted with each SRP. In order to test this aspect, each SRP has been associated with a reliability probability, i.e., a measure of the likelihood that the SRP delivers the service compliant with the agreement established. This probability has been set to values illustrated in Table 2. Specifically, with probability *0.9* SRPA P_5 complies with its promises, whereas P_{10} maintains its promises with probability *0.3*. A mixture of extreme and moderate values has been chosen in order to test the schemes under diverse conditions.

Figures 4-6 depict the formation of the reputation ratings of SRPs P_{10}, P_6 and P_5, respectively for five different SRRAs, based on their direct experiences with respect to the number of transactions conducted. Several runs per SRRA and SRP (50 runs) have been performed, while the figures illustrate the mean SRPs reputation rating values. The standard deviation ranges between ±0.05 around the mean values, which shows that the results acquired are close enough to the mean values displayed in the figures. Finally, in the context of the experiments conducted, each SRRA has performed 1000 transactions with each one of the target SRPs. As it may be observed, for SRP P_5 more transactions (less than 30) are required in order to obtain an accurate picture concerning its reputation rating, in comparison with the respective transactions needed for SRP P_{10} and P_6, for which less than 10 and 20 transactions for the same reason are needed, respectively. This was somehow expected, and may be attributed

to the fact that the reputation ratings for SRP P_5 vary between 0.1 to nearly 0.9, while SRPs P_{10} and P_6 vary between 0.1 to 0.3 and 0.6, respectively. At this point it should be noted that the amount of transactions required for reaching the reputation rating is tightly related to $\{rr^{R_x}(P_j) - E[rr^{R_x}(P_j)]\}$, which in our experiment varies from 0.1 to 0.3. Since reputation rating values reach an appropriate level after a small number of transactions have been conducted, we constrain the illustration of the figures to 100 transactions so as to enable the reader to clearly identify the point raised by the authors.

In Table 3 SRPs are ranked with respect to their reliability, which reflects whether the SRP usually meets the quality expectation raised (or promised) by the contract proposed. In the context of the experiments conducted, all SRR classes are considered to be witnesses and their vast majority is assumed to behave in an honest manner (that is $TL^{R_i}(R_x) \to 1$).

As may be observed from Table 3, considering SRR class R_1, the most appropriate SRP is P_5 (ranked first), followed by SRP P_4 (ranked second), followed by SRP P_8 (ranked third), followed by P_7, P_3, P_6, P_9, while the SRP P_2 occupies the 8th ranking position. Empty spaces in Table 3 are attributed to the fact that for a specific SRR class, there may be SRPs that do not offer the required quality/quantity level for the service/resource as requested (i.e., inappropriate SRPs). Slight differences in the SRP ranking position may be additionally observed for different SRR classes. As an example the difference between SRR classes R_2 and R_3 may be noted. Specifically, for SRR class R_2, the 6th ranking position is occupied by SRP P_3, the 7th position by SRP P_6, the 8th position by SRP P_2 and the 9th position by SRP P_9. For SRR class R_3, the 6th position is occupied by SRP P_6, the 7th position by SRP P_3, the 8th position by SRP P_9 and the 9th position by SRP P_2. This change may be attributed to the fact that SRPs P_3/P_6 and P_2/P_9 are associated with the same honesty probability, 0.6 and 0.4, respectively.

Figure 7 illustrates in a graphical manner the SRPs specialization with respect to the interception of the requests from the various SRR classes, based on the results

depicted in Table 3. As may be observed, SRP P_1 handles 40% of the requests originating from all SRRs classes, because of its suitability in adequately serving 4 out of 10 SRR classes (that is, it offers the required quality/quantity level for the service/resource as requested by the SRRs classes in a more reliable manner with respect to the rest SRPs). Additionally, SRP P_5 handles 30% of the requests originating from all SRRs classes. SRPs P_5 and P_1 have been attributed with the same honesty probability, thus, with the same probability (0.9) they abide with the terms and conditions of the contracts established with the SRRs. However, P_1 and P_5 are characterized as inappropriate for five of SRR classes. Finally, each of the SRPs P_4, P_7 and P_8, associated with 0.8, 0.7 and 0.7 honesty probability respectively, serve 10% of the SRR requests. SRP P_4 handles the requests originating from SRR class R_4 due to the fact that the two SRPs with the highest reliability rating (P_1 and P_5) are considered as inappropriate for service/resource provisioning. SRPs P_7 and P_8, even though they are attributed with smaller honesty probability), they serve SRR classes R_6 and R_{10} respectively, since the SRPs P_1, P_5 and P_4 could not handle the service /resource requests.

Following, Figure 8 depicts the improvement introduced on the basis of our proposed SRP selection scheme with respect to the random SRP selection. Comparing the effectiveness of the SRP selection on the basis of the reliability ratings of the SRPs with respect to the random SRP selection scheme, we may note that in general our designed framework exhibits a better performance, which on average is 30%.

Finally, we would like to examine the responsiveness of our scheme with regards to SRPs reliability related behavioural modifications. We consider SRP P_1 attributed with honesty probability 0.9. After 100 transactions have taken place, SRP P_1 decides to take advantage of the reliability rating earned on the basis of its good behaviour in the past and modifies its strategy so as to abide by the contract terms and conditions for the 30% of the transactions. Finally, after the completion of 150 transactions, SRP P_1 updates its behaviour so as to adequately serve 60% of the service / resource requests. The experiment has been performed 50 times, while figure 9 illustrates the mean reputation values of SRP P_1 with respect to the number of transactions

conducted. As may be observed, the reputation ratings acquired in accordance with our proposed framework follow in a quite efficient manner the SRPs' strategy modifications.

7 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, the scope of our paper is to enhance the functionality that may be offered by ubiquitous computing environments. 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 a weighted combination of the evaluation of the quality of their offer (*performance related factor*) and of their reputation rating (*reliability related factor*). In this study, the focus is laid on the trust establishment among the various system entities. More specifically, the contribution of this paper lies in the definition and mathematical formulation of a reputation mechanism 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 takes into account potential dissemination of inaccurate reputation ratings.

The reputation framework designed has been empirically evaluated by simulating interactions among self-interested SRPAs and SRRAs and has performed well. Our obtained 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 various degrees of witnesses' misbehaviour and against existent reputation models and trust frameworks.

8 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] N. Jennings, P. Faratin, A. Lomuscio, S. Parsons, C. Sierra and M. Wooldridge, "Automated Negotiation: Prospects, Methods, and Challenges", International Journal of Group Decision and Negotiation, vol. 10, no. 2, pp. 199-215, 2001.

[3] 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.

[4] 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.

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

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

[7] R.S. Sutton, A.G. Barto, "Reinforcement learning: An introduction (Adaptive computation and machine learning)", MIT Press, March 1998.

[8] V. Cherkassky and F. Mulier, "Learning from Data: Concepts, Theory, and Methods" Adaptive and Learning Systems for Signal Processing, Communications and Control Series, John Wiley & Sons, March 1998.

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

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

[11] 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.

[12] J. Sabater and C. Sierra, “Review on Computation Trust and Reputation Models”, Artificial Intelligence Review, vol. 24, no. 1, pp. 33-60, 2005.

[13] Y. Bakos and C. Dellarocas, “Cooperation without Enforcement? A comparative analysis of litigation and on-line reputation as quality assurance mechanisms”, in Proc. of the 23rd International Conference on Information Systems, Barcelona, Spain, 2002.

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

[15] W. Zhao, W. Varadharajan, and G. Bryan, “A Unified Framework for Trust Management”, in Proc. of the 2nd International Conference on Security and Privacy in Communication Networks (SecureComm and Workshops, 2006), pp. 1-8.

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

[17] L. Xiong and L. Liu, “Reputation and Trust”, Advances in Security and Payment Methods for Mobile Commerce, Idea Group Inc, 2005, pp. 19-35.

[18] J. Sabater and C. Sierra, “REGRET: Reputation in gregarious societies”, in Proc. of the 5th International Conference on Autonomous Agents, Montreal, Quebec, Canada, 2001, pp. 194-195.

[19] K. Averer and Z. Despotovic, “Managing Trust in a Peer-2-Peer Information System”, in Proc. of the 10th International Conference on Information and Knowledge Management. Atlanta, Georgia, USA, 2001, pp. 310-317.

[20] J. Pujol, R. Sanguessa and J. Delgado, “Extracting Reputation in Multi Agent Systems by Means of Social Network Topology”, in Proc. of the 1st International

Joint Conference on Autonomous Agents and Multi-Agent Systems, Bologna, Italy, 2002, pp. 467-474.

[21] E. Damiani, S. Vimercati, S. Paraboschi, P. Samarati and F. Violante, "A Reputation-Based Approach for Choosing Reliable Resources in Peer-to-Peer Networks", in Proc. of the 9th ACM Conference on Computer and Communications Security, Washington, DC, USA, 2002, pp. 207-216.

[22] T. Huynh, N. Jennings, and N. Shadbolt, "Certified Reputation: How an Agent can Trust a Stranger", in Proc. of the 5th International Joint Conference on Autonomous Agents and Multi-Agent Systems, Hakodate, Hokkaido, Japan, 2006, pp. 1217-1224.

[23] H. Raiffa, "The Art and Science of Negotiation", Harvard University Press, Cambridge, USA, 1982.

[24] D. Pruitt, "Negotiation Behavior", Academic Press Inc., 1981.

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

[26] I. Roussaki, M. Louta, L. Pechlivanos, "An Efficient Negotiation Model for the Next Generation Electronic Marketplace", In Proc. of the 12th IEEE Mediterranean Electrotechnical Conference (MELECON 2004), Dubrovnic, Croatia, 2004, pp. 615-618.

List of Figures

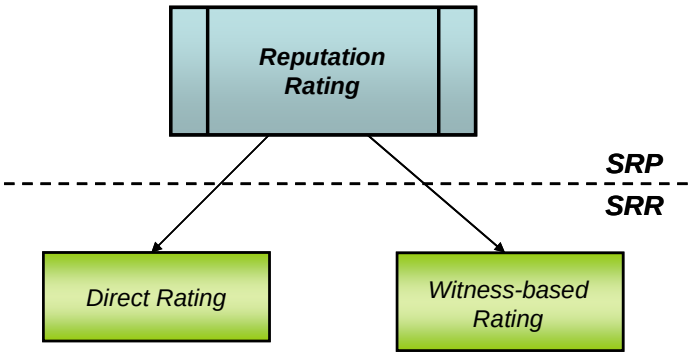

Figure 1. Structure of the reputation mechanism

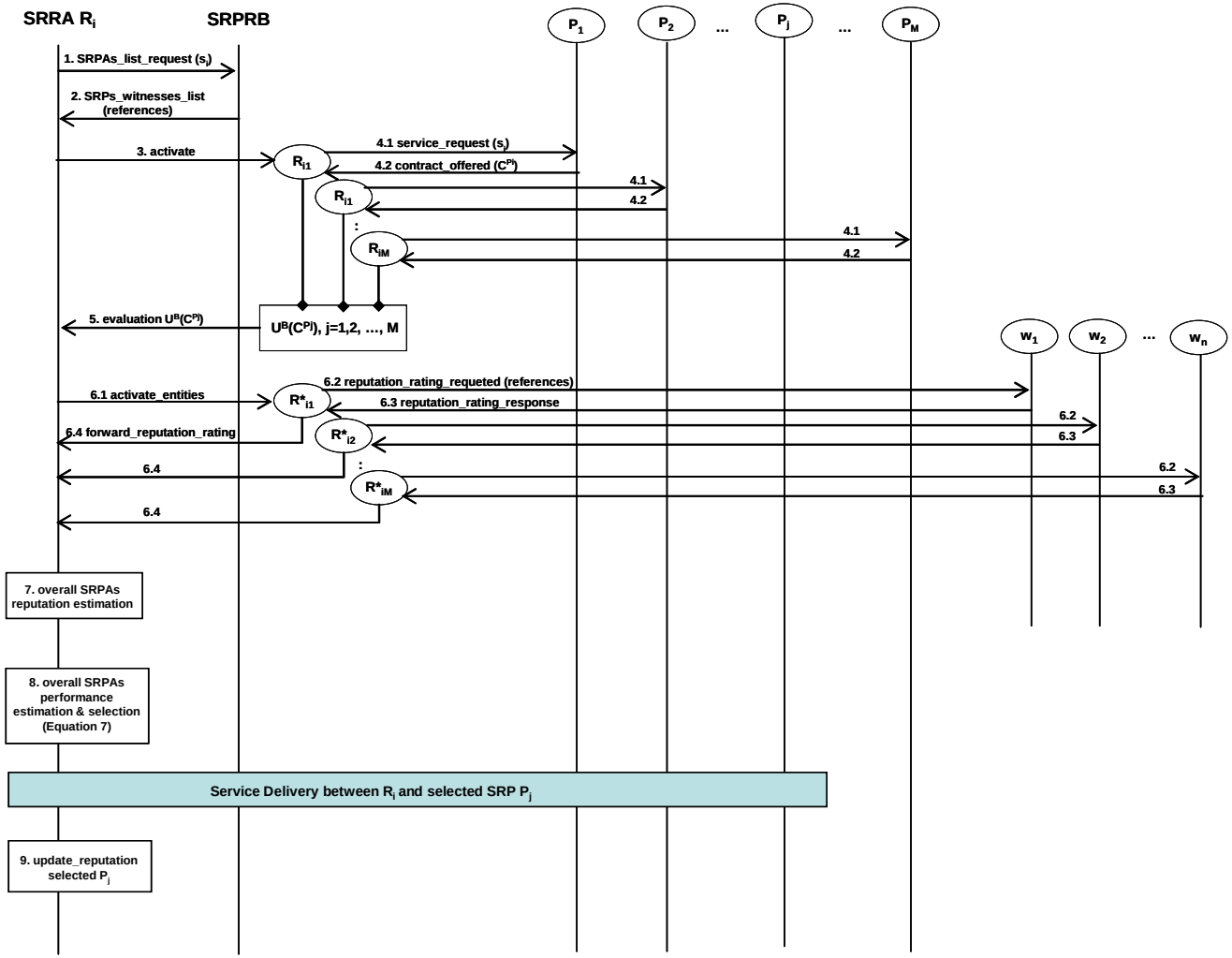

Figure 2. SRP selection considering a service / resource provisioning request

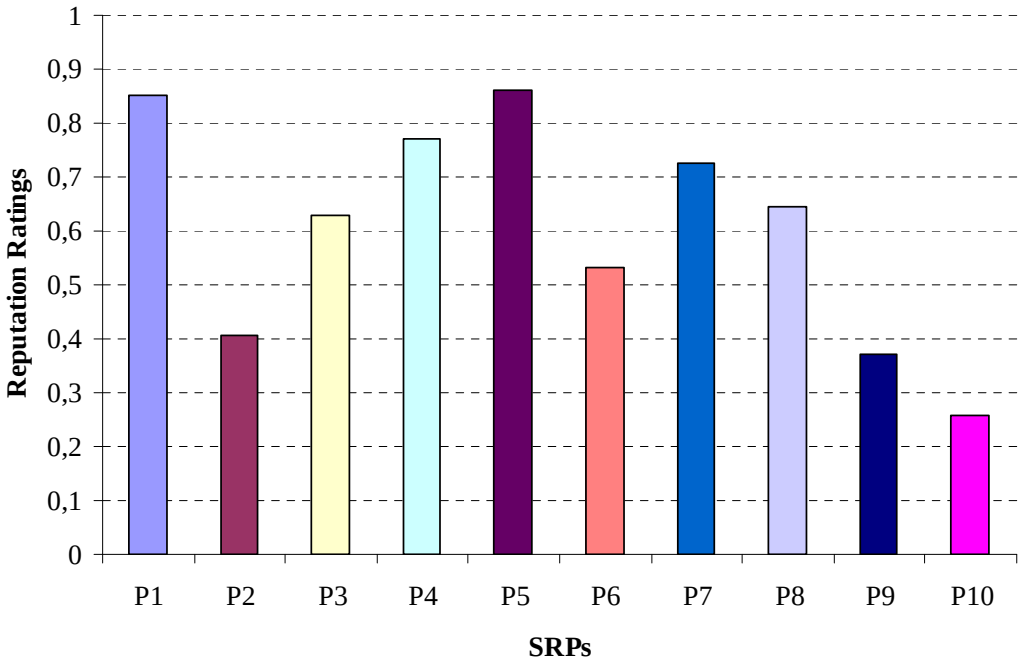

Figure 3. Reputation Ratings for all SRPs that could handle a service/resource request originating from SRR class R_2

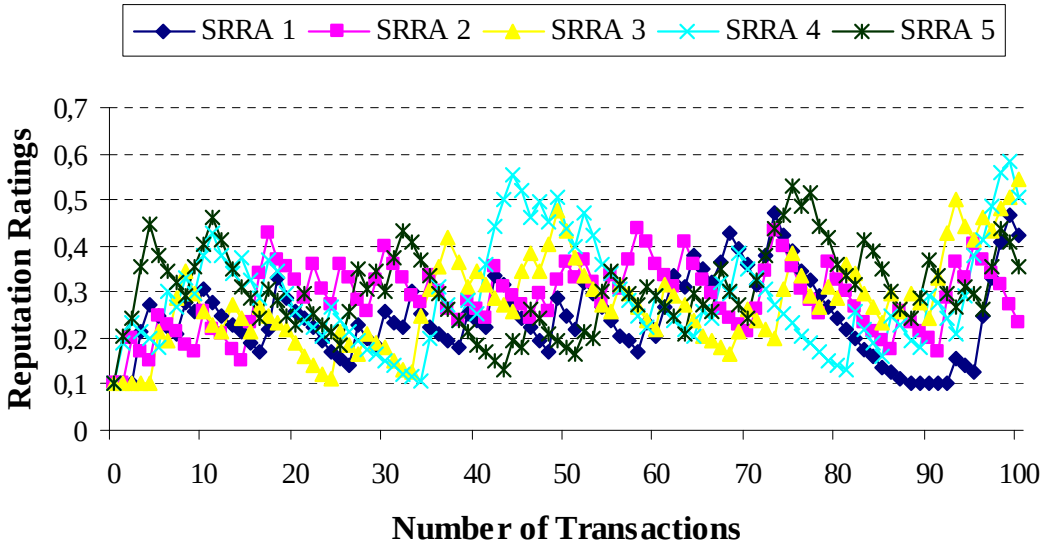

Figure 4. SRP's P_{10} Reputation Rating formation for five different SRRAs on the basis of their direct experiences in the system.

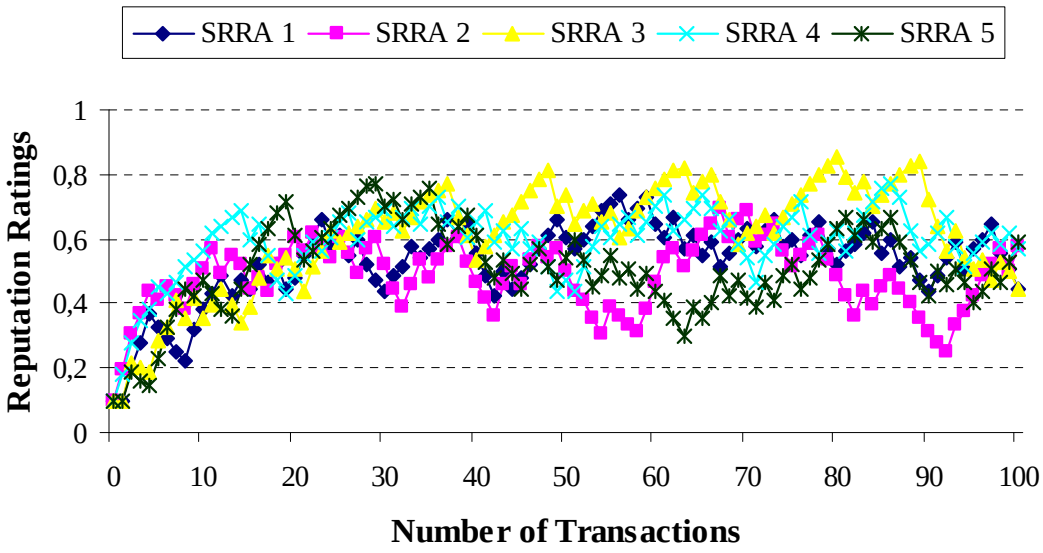

Figure 5. SRP's P_6 Reputation Rating formation for five different SRRAs on the basis of their direct experiences in the system.

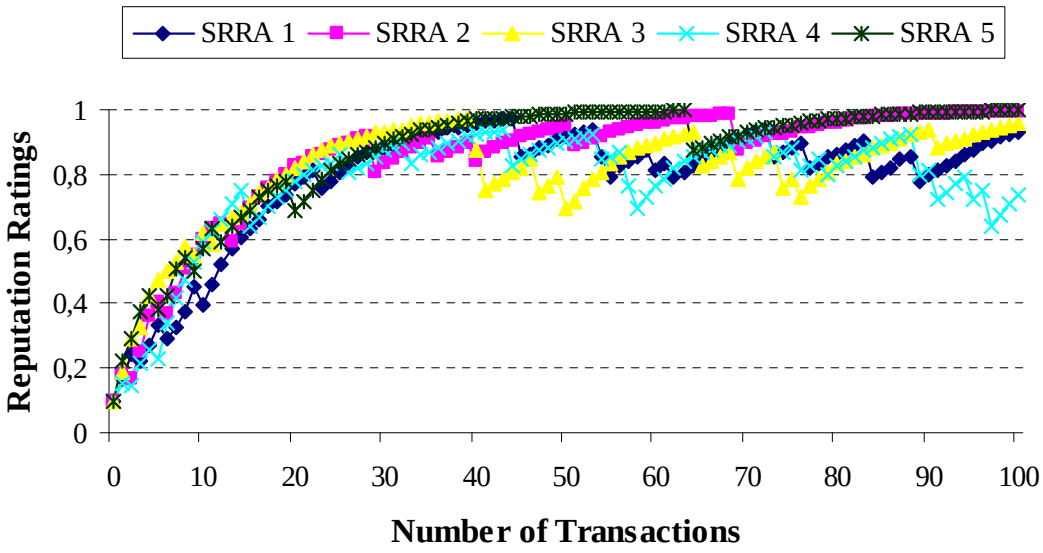

Figure 6. SRP's P_5 Reputation Rating formation for five different SRRAs on the basis of their direct experiences in the system.

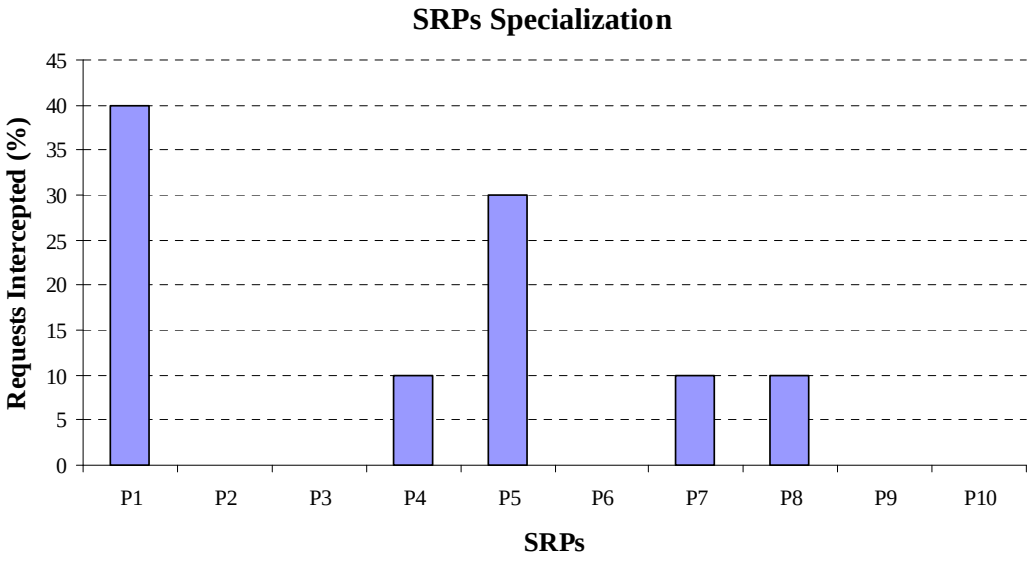

Figure 7. Specialization of the SRPs with respect to the interception of requests for the various SRR classes.

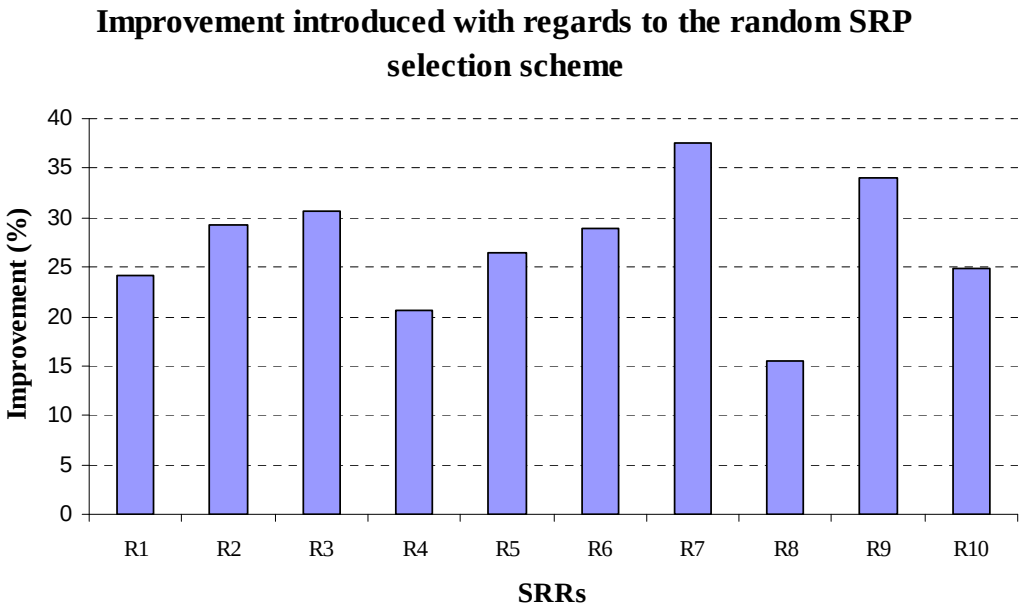

Figure 8. Comparison of our proposed framework and the random SRP selection scheme.

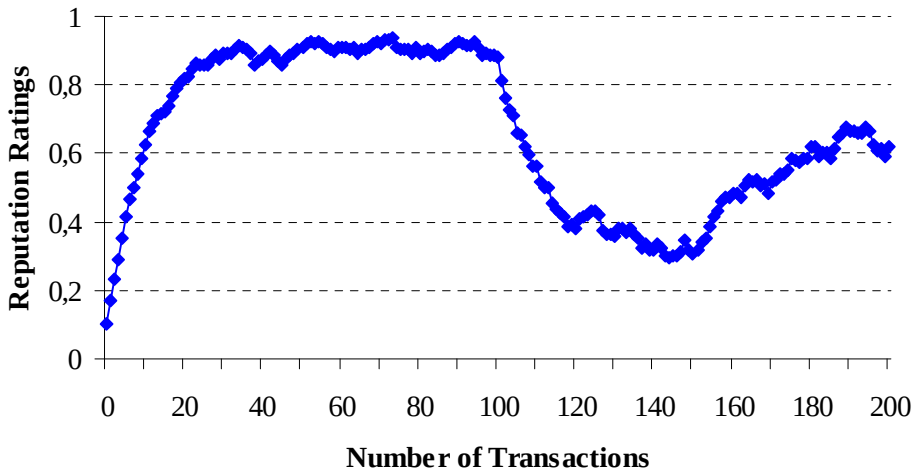

Figure 9. Responsiveness of our proposed scheme to SRP P_1 reliability related behavioural modifications

List of Tables

Table 1. Set of inappropriate SRPs for each SRR class

SRR Class	***Inappropriate SRPs***
R_1	P_1, P_{10}
R_2	-
R_3	-
R_4	P_1, P_5, P_9
R_5	P_5, P_6, P_7, P_8, P_9
R_6	P_1, P_2, P_3, P_4, P_5
R_7	-
R_8	P_3, P_8, P_{10}
R_9	-
R_{10}	$P_1, P_2, P_3, P_4, P_5, P_7$

Table 2. Honesty probability associated to each SRP

SRP	**Honesty Probability**
P_1	0.9
P_2	0.4
P_3	0.6
P_4	0.8
P_5	0.9
P_6	0.6
P_7	0.7
P_8	0.7
P_9	0.4
P_{10}	0.3

Table 3. Service Resource Providers Reliability Ranking

SRR Class	***Service Resource Providers Reliability Ranking***									
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
R_1	P_5	P_4	P_8	P_7	P_3	P_6	P_9	P_2		
R_2	P_5	P_1	P_4	P_7	P_8	P_3	P_6	P_2	P_9	P_{10}
R_3	P_1	P_5	P_4	P_7	P_8	P_6	P_3	P_9	P_2	P_{10}
R_4	P_4	P_8	P_7	P_6	P_3	P_2	P_{10}			
R_5	P_1	P_4	P_3	P_2	P_{10}					
R_6	P_7	P_8	P_6	P_9	P_{10}					
R_7	P_1	P_5	P_4	P_7	P_8	P_6	P_3	P_2	P_9	P_{10}
R_8	P_1	P_5	P_4	P_7	P_6	P_2	P_9			
R_9	P_5	P_1	P_4	P_8	P_7	P_6	P_3	P_9	P_2	
R_{10}	P_8	P_6	P_3	P_2	P_9	P_{10}				