A Robust Reputation-Based Computational Model for Trust Establishment in Pervasive Systems

Stylianos Kraounakis, Ioannis N. Demetropoulos, Angelos Michalas, *Member, IEEE*, Mohammad S. Obaidat, *Fellow, IEEE*, Panagiotis G. Sarigiannidis, *Member, IEEE*, and Malamati D. Louta, *Senior Member, IEEE*

***Abstract*—Distributed systems built in open competitive and highly dynamic pervasive environments are composed of autonomous entities that act and interact in an intelligent and flexible manner so as to achieve their own goals and aims. 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 maximization of their welfare, entities may misbehave, thus leading to a significant deterioration of system's performance. The scope of this paper is to present a computational model for trust establishment based on a reputation mechanism, which incorporates direct SRRs' experiences and information disseminated from witness SRRs on the basis of their past experiences with SRPs. The designed mechanism discriminates between unfair feedback ratings intentionally and unintentionally provided, takes into consideration potential changes to providers' behavior, and weighs more recent events in the evaluation of the overall reputation ratings. The proposed model has been extensively evaluated through simulation experiments. It exhibits good performance, as the reputation computation error introduced due to false feedback provision decreases significantly.**

***Index Terms*—Collaborative reputation mechanism, intelligent multiagent systems, pervasive systems, trust management systems.**

I. Introduction

DISTRIBUTED systems are built in open, uncertain, competitive, and highly dynamic environments. These systems are composed of autonomous entities that act and interact in an intelligent and flexible manner so as to achieve their own goals and aims. From a market-based perspective, the roles of the system entities may be classified into two main categories that, in principle, are in conflict [1]. These two categories are as follows: 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, while a single entity may, at the same time, act as a Requestor and as a Provider for different services/resources. Seeking for the maximization of their welfare, entities may act selfishly, leading this way to a significant deterioration of the system's performance. Furthermore, entities may discard their original identities in order to "whitewash" previous bad behavior or even "bad-mouth" potential competitors, while they may appear and disappear at any time. The success of these systems depends highly on trust mechanisms building the necessary trust relationships among the parties [2], [3], enabling them to automatically adapt their strategies to different levels of cooperation and trust.

Trust is often described as the belief of an entity in the competence and benevolence of another entity to act honestly, reliably, and dependably [4]. Two main types of trust may be distinguished [5]: functional trust expressing the belief that the trustee has a specific property or attribute and recommendation trust, which expresses the belief that the trustee can recommend other entities with the specific property over a certain number of recommendation hops. Trust, in general, is a multifaceted concept: subjective, nonsymmetric, dynamic, and context specific. On the other hand, misbehavior may be defined as deviation from regular functionality, which may be unintentional due to faults or intentional in order for selfish parties to take advantage of certain situations. Misbehavior can significantly degrade the system's performance, which still requires high degree of cooperation among its various entities. Traditional models aiming to avoid strategic misbehavior are based on the authentication of identities and authorization schemes by exchanging digital cryptographically signed certificates/credentials [6] or involve trusted third parties (TTPs) or intermediaries [7] that monitor every transaction. However, these models may be inadequate or even impossible to apply due to the complexity, heterogeneity, and high variability of the pervasive environment. Reputation mechanisms are employed to provide a "softer" security layer, considered to be sufficient for many multiagent applications [8].

Reputation mechanisms establish trust by exploiting learning from experience concepts [9] in order to obtain a reliability value of system participants in the form of rating based on observations, past experiences, and other entities' view/opinion.

Manuscript received December 13, 2012; revised April 22, 2014 and June 21, 2014; accepted July 1, 2014.

S. Kraounakis is with the Hellenic Telecommunications Organization S. A., 151 24 Maroussi, Greece, and also with the Department of Informatics and Telecommunications Engineering, School of Engineering, University of Western Macedonia, Kozani 50100, Greece (e-mail: skraounakis@yahoo.gr).

I. N. Demetropoulos, P. G. Sarigiannidis, and M. D. Louta are with the University of Western Macedonia, School of Engineering, Department of Informatics and Telecommunications Engineering, Greece (e-mail: idimitr@uowm.gr; psarigiannidis@uowm.gr; louta@uowm.gr).

A. Michalas is with the Department of Informatics and Computer Technology, Technological Educational Institute of Western Macedonia, Kastoria 52100, Greece (e-mail: amichalas@kastoria.teikoz.gr).

M. S. Obaidat is with the Department of Computer Science, Monmouth University, West Long Branch, NJ 07764, USA (e-mail: obaidat@monmouth.edu).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/JSYST.2014.2345912

The usefulness of a reputation system highly depends on its underlying trust model, i.e., the representation of trust values and the methods to reason with and to calculate trust values [5]. 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 the 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) [10]. In [11], on the basis of a decentralized scheme grounded in gossip-based algorithms, it is shown that the higher an agent's reputation is above a threshold set by its peers, the more transactions it would be able to complete within a certain time unit.

In general, various systems for trust establishment have been proposed, a number of which exploit both experiences directly acquired (referred to as first-hand information) as well as feedback collected from other systems' entities (referred to as witnesses), reflecting their opinion/view on the entities under evaluation (referred to as second-hand information). In this line of work, a number of related research studies rely on the assumption that the vast majority of opinions are honest (e.g., [1]–[3] and [12]). However, as in [13], we believe that such studies provide a rough guideline of how many credible raters exist in a rating-based reputation community. True feedback cannot be automatically assumed. Second-hand information can be misleading, provided by system entities intentionally or unintentionally. In general, a mechanism for eliciting true and accurate feedback in the absence of TTPs or intermediaries is necessitated when reputation is built following referrals from other parties.

In this paper, we design a fully decentralized collaborative reputation-based computational model for trust establishment in pervasive systems, enhanced with mechanisms for handling inaccurate ratings both intentionally and unintentionally provided by witness SRRs, so as to efficiently rate the SRPs with minimal impact. The reputation mechanism rates the SRPs with respect to whether they honored or not the agreements established with the SRRs in the system, based on SRRs' direct experiences and the collected opinions of a number of other SRRs (witnesses) on their past experiences with SRPs, exploiting learning from experience principles. Our work shares several common aspects with [1]–[3], yet it is different in a number of ways. Specifically, in [1]–[3], a centralized (i.e., [2]) or semicentralized (i.e., [1] and [3]) architecture is adopted, assuming a central component for the estimation of the reputation ratings [2] or utilizing a centralized component for the witness reference acquisition [1], [3]. In contrary, this work presents a fully decentralized architecture, seeking witnesses in an evaluator's friendly entities' network, dynamically formed drawing ideas from sociology axioms (e.g., the friend of my friend is my friend) and considering the entities' owners in the real world. Additionally, in [1]–[3], emphasis is laid on the reputation rating formation following referrals from other parties, assuming honest feedback provisioning from the vast majority of the witnesses. Even though some preliminary measures are described so as to account for the potential dissemination of misinformation in the system, the authors merely discuss, without, however, evaluating witnesses' misbehavior. In this paper, our focus is laid on the evaluation of the witnesses' credibility, reflecting whether feedback is returned truthfully and in an accurate manner in order to minimize the impact of false feedback provisioning to the estimated rating of the considered entity. Extensive evaluation results indicate the efficiency of our proposed schemes, incorporating various degrees of providers' and witnesses' misbehavior. Our proposed mechanisms prove to be effective even in case the misbehaving witnesses collude in order to add credits to specific providers and discredit others.

The rest of this paper is structured as follows. In Section II, the related research literature is reviewed, laying emphasis on entities' misbehavior, witnesses' credibility, and feedback acquisition that are the main contributions of this study. Section III highlights the general aspects of our proposed model. Section IV describes the novelties and the contributions of the current work. Section V presents the software architecture that supports the computational trust model proposed. In Section VI, the reputation rating system with emphasis on assessing the witness' credibility is mathematically formulated. Section VII provides a set of indicative results of the efficiency and robustness of the proposed model, incorporating various degrees of providers' and witnesses' misbehavior. Finally, in Section VIII, conclusions are drawn, and directions for future plans are given.

II. Related Work

The issue of trust has been gaining an increasing amount of attention in a number of research communities (e.g., pervasive systems [14], [15], e-commerce domain [16], [17], social networks and recommendation systems [18], [19], peer-to-peer networks [20], [21], Web [22], cloud computing [23], ad hoc and wireless sensor networks [24]–[27], and software systems [28]). A wide variety of trust and reputation models with advanced features have been developed in recent years, which however lack coherence, as there is no consolidated set of well-recognized principles for building trust and reputation systems.

In [29], the current research on trust management in distributed systems is surveyed, and some open research areas are explored, one of which is the mitigation of the impact of false accusations/malicious behavior. Specifically, the authors consider that one of the fundamental challenges in distributed reputation management is to understand vulnerabilities and develop mechanisms that can minimize the potential damages to a system by malicious nodes. Many trust/reputation models evaluate the trust/reputation values of the parties of interest but fail to properly evaluate trust when malicious agents start to behave in an unpredictable way or become ineffective when agents exhibit an oscillating behavior [30].

The work in [31] presents TrustGuard, a framework for building distributed dependable reputation management systems with countermeasures against three vulnerabilities: 1) strategic behavior oscillation of malicious nodes that continuously change their behavior in order to gain unfair advantage in the system; 2) fake transactions (i.e., malicious nodes may misuse the system by providing feedback with fake transactions); and 3) dishonest feedback, including feedback filed by malicious nodes through collusion. Dishonest feedback is differentiated from honest one by assigning a credibility value to a feedback source. Feedback credibility is assigned with each node's trust

value, even though the authors recognize that a node may maintain a good reputation by providing high quality services but send malicious feedback to its competitors. Subsequently, they use a personalized similarity measure to rate the feedback credibility through a node's personal experience, considering the differences in the feedback provided over a set of common nodes with whom it has interacted. However, their approach does not consider the time periods that the transactions have taken place (e.g., a node may have changed its behavior) and differences in the transaction scope (different number of transactions and transaction values).

In [32], the authors examine the problem of potential unfair ratings (both high and low), a security threat of reputation and trust mechanisms that arise in case a buyer agent elicits opinions about seller agents from other agents in the marketplace. Specifically, a personalized approach for effectively handling unfair ratings of sellers provided by advisors is described. Their approach considers both private (taking into account preference similarity between buyer and advisor agents) and public knowledge about advisors, allowing buyers to weigh these two aspects, so as to compute a value for the trustworthiness of the advisors. Their approach is used as part of a centralized reputation system, while the ratings assume binary values. The main weakness of this approach is that it presupposes that the number of fair/unfair ratings is correctly identified, which is the case only when the majority of advisors are behaving honestly, since a rating is considered fair if it is consistent with the majority of ratings. In contrary, our proposed model is decentralized, while for deciding on the accuracy of a rating provided by a witness, we consider its consistency with the overall reputation of the target entity as estimated by the evaluator entity, taking into account the opinion of the contacted witnesses and its consistency with the evaluator's view, exhibiting robust behavior even in case the majority of the witnesses are misbehaving.

In [33], the authors introduce 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. Regarding the credibility factor of the feedback, the authors considered only a function of the acquired trust value of the respective source as its credibility value, i.e., 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, a problem which is acknowledged by the authors, even though it is considered as an exceptional case. Our work has several common aspects to [33] in terms of the factors taken into account for trust estimation. However, their emphasis is laid on the roles of the different trust parameters in computing the trustworthiness of peers, while the precision of credibility of feedback is considered as a stand-alone hard research issue. Recently, in [34], instead of considering feedback credibility, the authors defined a reputation evaluation method based on two attributes: reputation value and reputation prediction variance, which serve as a quality measure of the reputation value computed based on the aggregation of feedbacks. They focus on the design of the trust model, and they do not examine issues concerning the feedback collection.

In [35], the authors suggest a trust reputation and recommendation system for mobile applications called TrueBeRepec. A trust behavior model is built using principal component analysis and confirmatory factor analysis, identifying three types of trust behaviors, namely, the using, reflection, and correlation behavior. The system uses a client–server model to provide application reputation based on the users' trust behaviors. The server receives individual trust information and votes from the mobile devices and subsequently generates application reputations and recommendations. The Trust Manager service located at the user mobile device, receives recommendations from the server, estimates user's individual trust, and periodically sends back to the server local trust information. In [36], the authors present PerChatRep, a reputation system for social chatting relying on a centralized trusted server. In particular, the trusted server accumulates local experiences of mobile chat nodes and estimates general reputation ratings. The general reputation assessments are issued to the nodes to evaluate their local reputation. Additionally, the trust server provides users' identification in case pseudonyms for each node are adopted and changed frequently. The same authors in [37] developed PerContRep, a reputation management system evaluating the node recommendation of content services in a framework of frequent modification of node pseudonyms. The architecture of the system is similar to the PerChatRep; however, reputation and trust evaluation is supported either in a centralized or even in a distributed mode in case the trust server is unavailable. The main weakness of the proposed approach is that the system achieves better performance and improves content reputation evaluation when the trust server is used due to the fact that more information about node behavior is assembled at the trust server, making the system, in this way, not fully decentralized.

Concerning the problem of storing and obtaining feedback from a set of proper witnesses so as to minimize the cost of storing and communicating reputation-related information as well as the impact of unfair ratings, different strategies have been presented in related research. In [38], 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 [31], when a node k is interested in the trust value of node m, it can obtain all positive feedbacks about node m directly from node m and obtain all negative feedbacks about node m from a set of R nodes that hold complaints against the node under evaluation. The work in [39] presents a 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. A number of research works favor the ignorance strategy, following advice only of trusted recommenders and ignoring distrusted and unknown ones. Finally, in [40], trustworthy providers are looked for by querying a number of neighboring to the requestor entities, adaptively selected based on their usefulness from the requestor's acquaintances. An entity's usefulness is estimated on the basis of its expertise (the quality of the services that it provides) and its sociability (the quality of the referrals

that it provides). In case the neighbors cannot provide a reply themselves, the query is, in turn, passed to their neighbors. Thus, a trust net is built. As expected, among other guidelines provided, the authors show that the neighbor selection policy, the neighbor set size, and referral graph type and depth affect the efficiency and effectiveness of the referral system. Our work implements a variant of their referral system, incorporating sociology axioms, while constraining the witness set size to n. Specifically, the evaluator seeks for trustworthy feedback through a network of neighboring friendly entities, which is dynamically formed on the basis of entities' credibility, while sociology axioms are exploited (e.g., the friend of my friend is my friend), considering the entity owners in the real world. The number of witnesses is confined to the n most appropriate ones (the n ones with the highest trustworthiness), in order to take into account possible communication and/or computational limitations and time constraints imposed to the entities concerning service provisioning.

III. General Concepts

In general, various systems for trust establishment have been proposed, a number of which utilize the opinion/view that other system participants have on the entities under evaluation. The common pitfall of these systems is that trust computation corresponds to service quality assessment with respect to consumers' needs and desires, not taking into account the malicious behavior of the otherwise competent service provider. In this paper, following the general concepts of [1]–[3], trust refers to the providers' reliability, i.e., whether the providers finally provide to the requestors the service/resource as specified in the established contract. Providers' reliability is quantified by a reputation mechanism that forms providers' reputation as a measure of the subjective probability that providers will honor the agreements established with the requestors, adhering to the specified contract terms and conditions in an environment characterized by incomplete knowledge and uncertainty. Providers' reliability is treated as a purely behavioral aspect, independent of the services/resources provided and the degree up to which each service/resource satisfies the needs, requirements, and constraints of the requestors. In essence, trust computation is relieved from service offer quality assessment, referred to as performance-related factor, which reflects the competence and capability of a provider in satisfying requestors' special needs, requirements, and constraints in a personalized fashion. A positive side effect of this is that the formation of SRP reputation ratings is enabled in a time-efficient manner.

Additionally, most of the related studies 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. This work, in line with [1]–[3], is based on a different approach according to which the SRPs that are deemed misbehaving should not be directly excluded/isolated, but instead the SRRs' decision on the most appropriate SRP should be based on both performance- and reliability-related factors, enabling requestors to select different providers with respect to the quality of the providers' offers and their own attitude to the perceived risk. To this respect, a composite utility function may be utilized, expressing the overall requestor's satisfaction stemming from a specific offer returned by a provider, taking into account both the provider's competence in satisfying the requestor's special needs and the provider's reliability, reflecting potential misbehavior, e.g., service level agreement (SLA) breach. Thus, the quality of service offer as perceived by the requestors, quantified by the overall utility function, is affected by the provider's reliability, and in this sense, performance- and reliability-related factors are interrelated. In the simplest case, this composite utility function may be formulated as a weighted combination of the performance- and reliability-related factors, where the weights provide the relative significance of the two factors in the overall utility estimation and may be dynamically selected accounting for users exhibiting different behaviors with respect to the risk involved (e.g., risk lovers, risk neutral, and risk-averse users). More sophisticated composite utility functions may be defined. This study focuses on assessing the reliability-related factor; the determination and the experimentation with the performance-related factor and the composite utility function are considered as a stand-alone issue to be addressed in the future.

Furthermore, in contrary to some related works (e.g., [41]), in order not to exclude untrustworthy SRPs forever from the system and give them a chance to reenter the system and improve on their reputation rating in case they abide by the established SLA terms and conditions, we propose to form SRRs' decision on the basis of SRPs' performance factor after prespecified time intervals. Moreover, in our model, the time effect has been taken into account, and more recent events weigh more in the evaluation of the overall reputation rating of the target entity, yielding thus more accurate reputation ratings, which is not considered in some research studies (e.g., [42]).

Concerning the "cold start" issue, a low reputation value for new providers is assumed in order to avoid the establishment of new identities that whitewash previous bad reputation ratings. However, we should note that newcomers are not excluded from the system, as the most appropriate service/resource provider is selected on the basis of a composite utility function that takes into account both the quality of the service offer (i.e., the degree up to which each service/resource as offered satisfies the needs, requirements, and constraints of the requestors) and the providers' reputation ratings. Thus, highly competent providers may be selected for service provisioning even from the very beginning by risk lovers or risk neutral requestors on the basis of the quality of their offer and built on their reputation by exhibiting proper behavior in the system. Additionally, since, in our system, the decision on the most appropriate service provider is based only on the performance-related factor after prespecified time intervals, newcomers may be selected for service provisioning on the basis of the quality of their offer, overcoming thus the barrier raised by their low reputation rating.

As a final note, the proposed model for trust establishment has been designed having in mind e-commerce environments, with the aim to assist Buyers in finding and associating each time with the most appropriate Seller for service provisioning. However, the computational model is quite generic, enabling thus its application in different contexts [e.g., peer-to-peer (p2p) networks and mobile ad-hoc networks (MANET)], adapting

each time the model's parameters in accordance with the distinct features and constraints of the specific setting considered.

IV. Novelties and Contribution

Our mechanism elicits true feedback considering and discriminating between intentional and unintentional inaccurate information provisioning, enabling thus the SRPs' rating formation effectively and efficiently with minimal impact, even in case of misbehaving witnesses' collusion. Intentional inaccurate information provisioning refers to the case where an SRR acting as a witness provides, in purpose, false evaluation report, different from its true valuation on the target SRP's reliability (e.g., due to jealousy in order to discredit trustworthy providers or, in contrast, to add credits to untrustworthy providers). Unintentional inaccurate information provisioning refers to the case where a witness SRR, even though reports his/her true valuation on the target SRP, has not formed an accurate picture on the behavior of the SRP under evaluation and thus gives a rating not close to the real one. This may be attributed to either a limited number of transactions conducted between the two parties and/or potential changes to SRPs' strategy concerning service provisioning. To this respect, each witness SRR is associated with a weight reflecting the credibility of the witness in the eyes of the evaluator. Specifically, witness credibility expresses whether requested information is provided truthfully and accurately, accounting for both intentional and unintentional feedback provisioning. Witness credibility provides the relative significance of reputation rating provided by the witness to the overall reputation rating formation.

In this paper, witness credibility takes into account the following: (a) the trust level attributed to each SRR by the evaluator (i.e., measure of the likelihood that the witness SRR gives feedback compliant to his/her real SRP valuation), which is dynamically updated in order to follow the system's dynamics and accurately reflect whether feedback is reported honestly; (b) the number of transactions that a witness SRR has performed with the target SRP (considering that the reputation rating formation is an outcome of a learning process that takes into account feedback from the environment, it is quite safe to assume that SRRs that have been involved with the target SRP only for a few times will not have formed an accurate picture regarding his/her behavior, as the learning process will not have been completed); and (c) the sum of the respective transactional values (consider the case of an SRP that may strategically exhibit good behavior in case its potential profits in a context of a transaction is low and cheat when the expected earnings are high). In essence, the (b) and (c) factors account for the case of misleading feedback unintentionally provided, weighing accordingly the significance attributed to the feedback returned in the overall reputation rating formation. In order to account for SRPs that oscillate, strategically modifying their behavior, honoring their agreements in case the profits in the context of a transaction are low and cheating when the expected earnings are high, we attribute higher credibility to those witnesses that have performed more transactions with higher transactional value, as they possess an accurate picture of the SRP's behavior with higher possibility.

Feedback accuracy is determined on the basis of its consistency with the overall reputation rating of the target SRP as estimated by the evaluator entity, taking into account the opinion of the contacted witnesses and its consistency with the evaluator's view, exhibiting robust behavior even in case the majority of witnesses are misbehaving. Additionally, our model supports witnesses that are believed to have unintentionally provided inaccurate information in order not to be severely punished, by accordingly outweighing their trust level adaptation through the introduction of a time-related factor that takes into account the time that the last transaction has taken place in order to account for potential modifications of SRPs' behavior.

Concerning the witness set determination, a number of related works do not clearly describe how the evaluator entities find in the system feedback sources (witnesses) used for the overall evaluation of the target entities or assume a semicentralized architecture in order to acquire references of proper witnesses (e.g., [3]). Our study provides a fully decentralized solution considering a variant of the [40] referral system, forwarding the evaluator's request for feedback provision to appropriate entities through a network of neighboring friends, drawing ideas from sociology axioms.

In a nutshell, our study, on the basis of a fully decentralized architecture, discriminates between and addresses both intentional and unintentional inaccurate reputation ratings given by witnesses, providing a robust manipulation-resistant reputation model for trust establishment in pervasive systems.

V. Software Architecture

This study is based upon the notion of interacting intelligent agents, which participate in activities on behalf of their owners in order to achieve particular objectives and accomplish their goals [43]. An SRR 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. SRP 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 maximize their owners' profit.

Fig. 1 shows a sketch of the designed architecture supporting the decentralized reputation mechanism. It can be seen that each SRR comprises a Reputation Formation Engine, a Witness Set Determination & Feedback Provision Engine, and a Witness Trustworthiness Update Engine. In the context of evaluating the reliability of a target SRPA, the evaluator SRRA first calls the Witness Set Determination & Feedback Provision Engine in order to contact a list of witnesses and obtain feedback information regarding the behavior of the target SRPA. As aforementioned, each witness SRRA is associated with a weight, which is a measure of the credibility of the witness in the eyes of the evaluator and reflects whether the witness

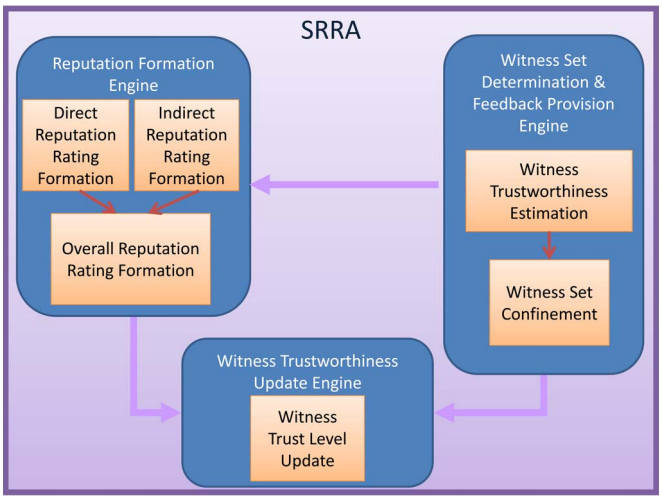

Fig. 1. System architecture supporting the proposed trust management framework.

SRRA provides feedback with respect to its experiences with the SRPAs truthfully and in an accurate manner. The Witness Set Determination & Feedback Provision Engine implements a variant of the [40] referral system. Specifically, the evaluator agent contacts its neighbors (a subset of its acquaintances) constituted by its friends (e.g., friends and collaborators of the agent's owner in the real world), whose opinion in general is expected to coincide with its own. Since friends in the real world provide (whenever asked for) advice, this is also assumed in our system, i.e., the entities of a certain owner share their experiences in the system whenever asked for by a friendly entity in the trust chain formed. Based on ideas drawn from status and balance theory of sociology (e.g., "the friend of my friend is my friend") [44], in case a neighbor is not able to provide a rating on the behavior of the target SRPA (e.g., it has not acquired an accurate picture concerning the target SRPA's behavior), it sends to the evaluator the references of its own neighboring SRRAs (its own friends) to be contacted by the evaluator along with their trustworthiness level, as their opinion most probably would be close to its view. Thus, witnesses are sought in specific circles of trust from the evaluator entity. The trust network can be enhanced considering also lists of friends of the evaluator retrieved from various social networking applications where the evaluator entity participates (e.g., members of the user's roll), denoting users that the evaluator trusts and/or shares the same interests/opinion with. At this point, it should be noted that, in conjunction to the reputation rating of the target SRPA, a witness provides also the number of transactions conducted with the target SRPA, the respective transactional values, and the time instance that the last transaction occurred.

Taking into account possible computational and/or communication limitations and constraints, in conjunction with a huge number of potential witnesses, we confine the set of witnesses to the n most appropriate ones on the basis of their trustworthiness. Specifically, we consider that the witness set for the feedback provision process is constrained to the n first acquired witnesses whose trustworthiness is beyond a predefined threshold. It should be stressed that, in case a reference of an SRRA potential witness is returned to the evaluator and no direct

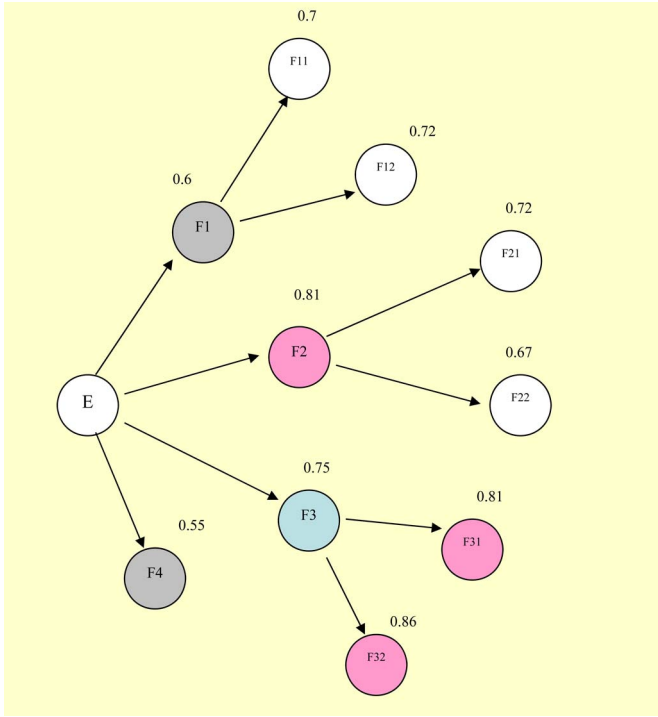

Fig. 2. Witness set determination example.

prior knowledge with respect to its trustworthiness exists, the evaluator takes the potential witness trustworthiness equal to the minimum value of the trustworthiness levels of the SRRAs contacted across the path from the evaluator to the witness.

Fig. 2 presents an illustrative example of the witness set determination and feedback provision process with $n = 3$ and the trustworthiness threshold value equal to 0.7. The evaluator entity E contacts its neighboring friends $F1$, $F2$, $F3$, and $F4$ and estimates their trustworthiness level concerning the target SRPA (0.6, 0.81, 0.75, and 0.55, respectively). $F1$ and $F4$ (gray colored) are not considered as witnesses since their trustworthiness is below the predefined threshold, and $F3$ (blue colored) does not have direct experience concerning the behavior of the target SRPA and returns to the E the references of its friends $F31$ and $F32$ along with their trustworthiness levels (0.81 and 0.86, respectively). $F31$ and $F32$ (pink colored) are considered as witnesses for the evaluator as the estimated trustworthiness (i.e., the minimum of the respective path -0.75 in both cases) is above the predefined threshold.

In the sequel, the Reputation Formation Engine is activated, so as to estimate the overall reputation of the SRPA under evaluation. The Reputation Formation Engine is constituted of three components. The first is the Direct Reputation Formation component, which exploits learning from experience concepts in order to estimate the SRPA's reliability on the basis of the evaluator SRRA's past experiences. This component is activated after the service provisioning/resource consumption process has been completed by introducing a reward/penalty function reflecting whether the service/resource quality is compliant with the picture established during the negotiation process. The better/worse the SRPA behaves with respect to the agreed terms and conditions, the more positive/negative the influence of the reward/penalty function on the SRPA's rating. A system

parameter determines the relative significance of the new outcome with respect to the old one, constituting, in essence, the memory of the system, while untrustworthy SRPAs are enabled to improve gradually their reputation rating in case they abide by established contract terms and conditions. The second is the Indirect Reputation Formation component, which estimates the SRPA's reputation rating based on the opinion of the selected witnesses, given their credibility values as calculated by the Witness Determination & Feedback Provision Engine. The third is the Overall Reputation Formation component, which returns the overall reputation rating value of the target SRPA, considering the results of the Direct Reputation Formation component and Indirect Reputation Formation component. At this point, it should be noted that SRRAs keep a record of the reputation ratings, the number of transactions, the transactional values, and the time instance that the last transaction occurred with respect to the SRPAs having been involved in a transaction with, while they are willing to share their experiences whenever asked for.

As a next step, after service provision/resource consumption has taken place, the Witness Trustworthiness Update Engine is invoked, so as to update the trustworthiness level of each witness. As a first step, the Witness Trustworthiness Update Engine decides on feedback accuracy on the basis of its consistency with the overall reputation of the target SRPA as estimated by the evaluator entity, taking into account the opinion of the contacted witnesses and its consistency with the evaluator's view. In the sequel, learning from experience principles are exploited in a similar manner to the direct reputation rating formation, so as to reward/penalize a witness depending on whether feedback is provided truthfully and in an accurate manner. A time-related factor is introduced in order to account for potential modifications to the SRPA's strategies concerning service provisioning.

At this point, we should note the following.

First, in case direct experiences are not available (i.e., the evaluator has not been involved in a transaction with the target SRPA), the accuracy of feedback is decided on the basis of its consistency with the overall reputation of the target entity. In such a case, untrustworthy witnesses cannot be identified prior to service provisioning only when the overall reputation rating for the target SRP is significantly affected, i.e., when the majority of witnesses collude, raising the reputation of specific service providers or discrediting others. However, considering that the Witness Trustworthiness Update Engine responsible for updating the trustworthiness level of each witness is invoked after service provision/resource consumption has taken place, the evaluator entity has assessed whether the service provided is compliant to that promised during the negotiation phase and thus, based on its own experience, may identify misleading feedback. Furthermore, in all other cases where the overall reputation rating of the target SRPA is not significantly affected, misleading feedback could be identified, even without the existence of direct experiences.

Second, since witness trustworthiness is dynamically updated, the witness set is adaptively formed each time.

Finally, the reliability rating value of the SRPAs requires in some cases (e.g., when consumption of network or computational resources is entailed in the service provisioning process) a mechanism for evaluating whether the service quality was compliant with the picture promised during the negotiation phase.

VI. Formulation of the Witnesses' Trustworthiness and Its Impact to the Reputation Rating Formation

Let us assume the presence of M candidate SRPAs interacting with N SRRAs concerning the provisioning of services/resources $s = \{s_1, s_2, \ldots\}$ requested in an intelligent pervasive environment. Let the set of agents that represent *SRPs* be denoted by $P = \{P_1, P_2, \ldots P_M\}$ and the set of agents that represent *SRRs* be denoted by $R = \{R_1, R_2, \ldots R_N\}$. We hereafter consider the request of an SRRA R_i regarding the provision of service s_l, which, without loss of generality, is provided by all candidate SRPAs $P = \{P_1, P_2, \ldots P_M\}$.

A. Witness Set Determination and Feedback Provisioning Engine

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 activates the Witness Set Determination and Feedback Provisioning Engine so as to contact its neighbors in order to get feedback reports on the behavior of the P_j. As already explained, proper witnesses are obtained through a network of friends, exploiting the transitivity property of trust and borrowing ideas from sociology axioms.

The Witness Set Determination and Feedback Provisioning Engine confines the set of witnesses to the n most appropriate SRRAs R_x $(x = 1, \ldots n)$ on the basis of their trustworthiness level estimated by the evaluator R_i, denoted by $TL^{R_i}(R_x)$. In the sequel, for each selected witness R_x, it provides to the Reputation Formation Engine (and specifically to the indirect reputation rating component) the direct reputation rating of the target SRPA P_j as formed by the witness R_x after a transaction d_x has been completed at time instance t_{d_x} on the basis of its direct experiences with P_j in the past, $RR^{R_x,t_{d_x}}(P_j)$, the number of transactions R_x has performed with P_j, $N_T^{R_x}(P_j)$, the sum of the respective transaction values, $\sum_{m=1}^{N_T^{R_x}(P_j)} TV_m^{R_x}(P_j)$, and the time instance that the last transaction occurred t_{d_x}.

B. Reputation Formation Engine

Direct Reputation Rating Formation: Concerning the formation of the direct reputation ratings $RR^{R_k}(P_j)$ $(k = i \cup x \in \{1, \ldots n\})$, a reinforcement learning from experience mechanism is exploited, rewarding or punishing the SRPA's behavior on the basis of the SRRA's R_k direct experiences with SRPA P_j. Specifically, each SRRA R_k may rate SRPA P_j with respect to its reputation after a transaction d_k has taken place at time instance t_{d_k} in accordance with the following equation:

$$RR^{R_k,t_{d_k}}(P_j) = RR_{pre}^{R_k}(P_j) + m_r \cdot l\left(RR_{pre}^{R_k}(P_j)\right) \cdot \left\{rr^{R_k}(P_j) - E\left[rr^{R_k}(P_j)\right]\right\} \quad (1)$$

where $RR^{R_k,t_{d_x}}(P_j)$ and $RR^{R_k}_{pre}(P_j)$ are the SRPA P_j reputation rating after and before the updating procedure. It has been assumed that $RR^{R_k,t_{d_k}}(P_j)$ and $RR^{R_k}_{pre}(P_j)$ lie within the [0,1] range, where a value close to 0 indicates a misbehaving SRP. $rr^{R_k}(P_j)$ is a (reward) function reflecting whether the service quality is compliant with the picture established during the negotiation phase, and $E[rr^{R_k}(P_j)]$ is the mean (expected) value of the $rr^{R_k}(P_j)$ variable. In general, the larger the $rr^{R_k}(P_j)$ 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 m_r $(m_r \in (0,1])$ 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 m_r values mean that the memory of the system is large. However, good behavior will gradually improve the SPRA's P_j reputation ratings. $l(RR^{R_k}_{pre}(P_j))$ is a function of the P_j reputation rating $RR^{R_k}_{pre}(P_j)$ and is introduced in order to keep the P_j rating within the range [0,1]. In the current version of this study, $l(RR^{R_k}_{pre}(P_j)) = (1/(1-e)) \cdot [1 - \exp(1 - RR^{R_k}_{pre}(P_j))]$, for which it stands that $l(RR^{R_k}_{pre}(P_j)) \underset{RR^{R_k}_{pre}(P_j)\to 0}{\to} 1$ and $l(RR^{R_k}_{pre}(P_j)) \underset{RR^{R_k}_{pre}(P_j)\to 1}{\to} 0$.

It should be noted that the SRP's misbehavior (or at least the deterioration of its previous behavior) leads to a decreased post rating value since the $\{rr^{R_k}(P_j) - E[rr^{R_k}(P_j)]\}$ quantity is negative. The $rr^{R_k}(P_j)$ function may be implemented in several ways. In the context of this study, it was assumed without loss of generality that the $rr^{R_k}(P_j)$ values vary from 0.1 to 1. Additionally, initial SRPAs' reputation rating values are taken equal to 0.1. As already explained, a quite low reputation rating value has been assumed in order to avoid the bad consequences of whitewashing (changing identities so as to wipe out possible misbehavior in the past).

Indirect Reputation Rating Formation: Each witness SRRA is associated with a weight, hereafter denoted by $w^{R_i}_{P_j}(R_x)$, which reflects whether the witness SRRA provides feedback with respect to its experiences with the SRPAs truthfully and in an accurate manner. In essence, weight $w^{R_i}_{P_j}(R_x)$ $(x \in \{1,2,\dots n\})$ provides the relative significance of the reputation rating of the target SRPA P_j as given by the witness SRRA R_x to the overall reputation rating estimation by the evaluator R_i. In general, $w^{R_i}_{P_j}(R_x)$ is a measure of the credibility of witness R_x and may be a function of the trustworthiness 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. Additionally, it has been assumed that weights $w^{R_i}_{P_j}(R_x)$ are normalized to add up to 1.

Weight $w^{R_i}_{P_j}(R_x)$ may be given by the following equation:

$$w^{R_i}_{P_j}(R_x) = \frac{TL^{R_i}(R_x) \cdot N^{R_x}_T(P_j) \cdot \sum_{m=1}^{N^{R_x}_T(P_j)} TV^{R_x}_m(P_j)}{\sum_{x \in i \cup \{1,\dots n\}} \left[TL^{R_i}(R_x) \cdot N^{R_x}_T(P_j) \cdot \sum_{m=1}^{N^{R_x}_T(P_j)} TV^{R_x}_m(P_j) \right]}. \quad (2)$$

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.

The indirect reputation rating $IRR^{R_i,t_c}(P_j)$ of the target SRPA P_j is formed by the evaluator SRRA R_i at time instance t_c that a service/resource request has originated from the evaluator R_i in accordance with the following formula:

$$IRR^{R_i,t_c}(P_j) = \sum_{x=1}^{n} \left[w^{R_i}_{P_j}(R_x) \cdot TrF\,(t_c, t_{d_x}) \cdot RR^{R_i,t_{d_x}}(P_j) \right]. \quad (3)$$

$TrF(t_c, t_{d_x})$ is a time-related factor outweighing the significance of old information. Specifically, it is introduced in order to weigh up (down) recent (old) information. Thus, the impact of inaccurate ratings due to potential modifications of the SRPA's behavior in the time period from the last time that an SRRA has interacted with the target SRPA to the current time that the SRPA is under evaluation is addressed. A wide range of functions may be defined for the estimation of the $TrF(t_c, t_{d_x})$ factor (e.g., polynomial and exponential), for which it should stand that $TrF(t_c, t_{d_x}) \underset{t_c \to t_{d_x}}{\to} 1$ and $TrF(t_c, t_{d_x}) \underset{t_c \gg t_{d_x}}{\to} 0$. Specifically, the larger the quantity $(t_c - t_{dx})$, the lower the reputation value for the SRPA P_j acquired. In this paper, the $TrF(t_c, t_{d_x})$ factor is taken equal to

$$TrF\,(t_c, t_{d_x}) = 1 - \frac{t_c - t_{d_x}}{t_c}. \quad (4)$$

Overall Reputation Rating Formation: The target SRPA's P_j overall reputation rating $ORR^{R_i}(P_j)$ may be estimated by the evaluator SRRA R_i at time instance t_c in accordance with the following formula:

$$ORR^{R_i,t_c}(P_j) = w^{R_i}_{P_j}(R_i) \cdot TrF\,(t_c, t_{d_i}) \cdot RR^{R_i,t_{d_i}}(P_j) + \sum_{k=1}^{n} \left[w^{R_i}_{P_j}(R_k) \cdot TrF\,(t_c, t_{d_k}) \cdot RR^{R_k,t_{d_k}}(P_j) \right]. \quad (5)$$

As may be observed from (5), 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 constitutes the indirect reputation ratings and depends on information regarding P_j past behavior gathered from n witnesses. Additionally, for the estimation of parameter $w^{R_i}_{P_j}(R_i)$, the trustworthiness level of the evaluator R_i is taken equal to 1 (i.e., $TL^{R_i}(R_i) = 1$).

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 behavioral aspects (e.g., they have been involved with P_j for at least a predefined number of transactions with a transactional value above a prespecified threshold, in which case we assume that a learning period has been completed).

Witness Trustworthiness Update Engine: Trustworthiness $TL^{R_i}(R_x)$ of neighboring witnesses R_x to the evaluator entity R_i initially assumes a high value, i.e., all neighboring witnesses are considered to report their experiences to the R_i honestly. In case the evaluator R_i does not have any prior direct knowledge

with respect to a non-neighboring witness R_x, its trustworthiness level is taken equal to the minimum of the trustworthiness levels of the SRRAs along the path. However, as already noted, the trustworthiness level is dynamically updated in order to account for potential dissemination of misinformation by the witnesses in the system. Specifically, assuming that SRPA P_j does not modify its behavior with regard to the service/resource provisioning in between the $[t_{d_x}, t_c]$ time period, R_x is considered to misreport his/her past experiences if the target P_j overall reputation rating $ORR^{R_i,t_c}(P_j)$ as estimated by (5) is beyond a given distance from the rating $RR^{R_x,t_{d_x}}(P_j)$, in which case the following expression holds:

$$\left|ORR^{R_i,t_c}(P_j) - RR^{R_x,t_{d_x}}(P_j)\right| > e \tag{6}$$

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 their experiences honestly is quite large with respect to the dishonest witnesses. To account for the case where a significant percentage of the witnesses provide misleading information, the evaluator takes also into account the distance of the reputation rating of the target P_j as formed considering its own direct experiences $RR^{R_i,t_{d_i}}(P_j)$. Thus, in case it stands that

$$\begin{aligned}&\left|RR^{R_i,t_{d_i}}(P_j) - RR^{R_x,t_{d_x}}(P_j)\right| > e \;\&\\ &\left|ORR^{R_i,t_c}(P_j) - RR^{R_x,t_{d_x}}(P_j)\right| < e\end{aligned} \tag{7}$$

the evaluator may conclude that the witness misreports its experiences, under the assumption that the evaluator R_i has formed an accurate picture of the target P_j reliability based on its direct experiences.

Thus, assuming that the evaluator R_i has interacted and has been serviced by the target P_j for a number of transactions with transactional value beyond a predefined threshold (i.e., after the completion of a learning period) and P_j does not change its strategy between the $(t_{d_i} - t_{d_x})$ time period, the following distinct cases may be identified.

1) $|ORR^{R_i,t_c}(P_j) - RR^{R_x,t_{d_x}}(P_j)| > e$, and $|RR^{R_i,t_{d_i}}(P_j) - RR^{R_x,t_{d_x}}(P_j)| > e$. In this case, the evaluator is quite confident that the witness R_x misreports its experiences as its view regarding the reliability of the target P_j coincides with the opinion of the majority of the contacted witnesses.
2) $|ORR^{R_i,t_c}(P_j) - RR^{R_x,t_{d_x}}(P_j)| < e$ and $|RR^{R_i,t_{d_i}}(P_j) - RR^{R_x,t_{d_x}}(P_j)| < e$. In this case, the evaluator is quite confident that the witness R_x provides feedback honestly with respect to its experiences.
3) $|ORR^{R_i,t_c}(P_j) - RR^{R_x,t_{d_x}}(P_j)| < e$, and $|RR^{R_i,t_{d_i}}(P_j) - RR^{R_x,t_{d_x}}(P_j)| > e$. In this case, the evaluator believes that the witness R_x misreports its experiences and the majority of the witnesses have provided misleading information.
4) $|ORR^{R_i,t_c}(P_j) - RR^{R_x,t_{d_x}}(P_j)| > e$, and $|RR^{R_i,t_{d_i}}(P_j) - RR^{R_x,t_{d_x}}(P_j)| > e$. In this case, the evaluator concludes that the witness R_x reports honestly its experiences with respect to P_j behavior, contradicting with the opinion of the majority of the witnesses.

Up to this point, we have assumed that the SRPA P_j does not modify its behavior with regard to the service/resource provisioning in between the $[\min\{t_{d_x}, t_{d_i}\}, t_c]$ time period. In order to take into account inaccurate information unintentionally provided due to P_j behavioral changes and not severely punish or reward unintentionally misleading witnesses, we have incorporated a time-related factor in order to weigh down the penalty/reward in case of old feedback. Finally, in case the evaluator R_i has not formed a picture of the target P_j behavior (i.e., the learning period has not completed or direct experiences are not available), the accuracy of feedback is decided, and the trustworthiness of the witnesses considered for the formation of P_j reputation is adjusted after service provisioning has taken place and the reputation rating of the selected P_j has been accordingly updated.

Witnesses' trustworthiness may be updated on the basis of the following expression, exploiting learning from experience concepts:

$$\begin{aligned}TL^{R_i}_{post}(R_x) = TL^{R_i}_{pre}(R_x) + k_b \cdot l\left(TL^{R_i}_{pre}(R_x)\right)\\ \cdot RF \cdot TrF\left(\min\left\{t_{d_x}, t_{d_i}\right\}, t_c\right)\end{aligned} \tag{8}$$

where $TL^{R_i}_{post}(R_x)$ and $TL^{R_i}_{pre}(R_x)$ are the witness R_x trustworthiness as evaluated by the SRRA R_i 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 factor RF, the following expression holds:

$$RF = \left\{\begin{array}{ll} -1 \le RF < 0, & \text{for 1 and 3 cases} \\ 0 < RF \le 1, & \text{for 2 and 4 cases}\end{array}\right\}. \tag{9}$$

$l(TL^{R_i}_{pre}(R_x))$ is a function of the witness trustworthiness $TL^{R_i}_{pre}(R_x)$, is introduced in order to keep the witness trustworthiness level within the range [0,1], and is defined in a similar manner to $l(RR^{R_k}_{pre}(P_j))$. 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. Factor $TrF(\min\{t_{d_x}, t_{d_i}\}, t_c)$ is introduced in (8) in order to account for potential modifications to the SRPs' strategy within the time period $[\min\{t_{d_x}, t_{d_i}\}, t_c]$. The more the time elapsed between time instance t_{d_x}/t_{d_i} when the last transaction among witness R_x/evaluator R_i and SRPA P_j under evaluation has taken place and the time instance t_c that the request for service/resource provisioning has been issued, the more probable the deviation from the witness opinion concerning the reliability value to be attributed to SRP P_j due to potential changes in the SRP's P_j strategy. In such a case, the witness R_x does not misreport its experiences. Thus, the adaptation of the trustworthiness level associated to the witness R_x by the evaluator R_i should be accordingly outweighed. One could argue that this could constitute a disincentive for providing honest feedback. However, it should be stressed that the impact of such misleading information is minor as the significance attributed to old feedback for the estimation of the overall reputation rating of the target SRPA P_j is also accordingly outweighed.

Table I presents, for all parameters used in our model, the notation adopted as well as the respective value scopes.

TABLE I
NOTATIONS

M	The total number of candidate Service/ Resource Provider Agents (SRPAs)
N	The total number of Service/ Resource Requestor Agents (SRRAs)
S	The set of services/resources $s = \{s_1, s_2, ...\}$
s_l	The service/resource requested
P	The set of SRPAs $P = \{P_1, P_2, ...P_M\}$
P_j	The Service/ Resource Provider Agent P_j
R	The set of SRRAs $R = \{R_1, R_2, ...R_N\}$
R_i	The evaluator SRRA R_i
R_x	The witness SRRA R_x
n	The total number of the most appropriate witnesses SRRAs for the evaluator SRRA R_i concerning the evaluation of SRPA P_j
$TL^{R_i}(R_x)$	The trustworthiness level (within the [0,1] range) of R_x witness as estimated by the evaluator R_i
$RR^{R_x,t_{d_x}}(P_j)$	The direct reputation rating (within the [0,1] range) of the target SRPA P_j as formed by the SRRA R_x after a transaction d_x has been completed at time instance t_{d_x}
d_x	The transaction d_x
t_{d_x}	The time instance that transaction d_x has been completed
$N_T^{R_x}(P_j)$	The number of transactions witness SRRA R_x has performed with SRPA P_j.
$TV_m^{R_x}(P_j)$	The transaction value of transaction m performed by witness SRRA R_x with SRPA P_j
$\sum_{m=1}^{N_T} TV_m^{R_x}(P_j)$	The sum of the respective transaction values performed by witness SRRA R_x with SRPA P_j
$RR_{pre}^{R_k}(P_j)$	The direct reputation rating (within the [0,1] range) of the target SRPA P_j as formed by the R_k SRRA ($k = i \cup x \in \{1,...,n\}$ before the updating procedure
$rr^{R_k}(P_j)$	The reward function (within the [0,1] range), reflecting whether the service quality is compliant with the picture established during the negotiation phase
$E[rr^{R_k}(P_j)]$	The mean (expected) value of the $rr^{R_k}(P_j)$ variable
m_r	The factor within the [0,1] range, determining the relative significance of the new reputation rating with respect to the old one
$l(RR_{pre}^{R_k}(P_j))$	The function of the SRPA's P_j reputation rating $RR_{pre}^{R_k}(P_j)$ introduced in order to keep the P_j reputation rating of formula (1) within the range [0,1]
$w_{P_j}^{R_i}(R_x)$	The credibility weight (within the [0,1] range) of witness SRRA R_x estimated by the evaluator SRRA R_i reflecting whether R_x provides feedback with respect to its experiences with the SRPAs truthfully and in an accurate manner
$IRR^{R_i,t_c}(P_j)$	The indirect reputation rating (within the [0,1] range) of the target SRPA P_j formed by the evaluator SRRA R_i at time instance t_c
t_c	The time instance that a service/resource request has originated from the evaluator SRRA
$TrF(t_c, t_{d_x})$	The time-related factor (within the [0,1] range) considering the time period from the last time t_{d_x} that an SRRA has interacted with the target SRPA up to the current time t_c that the SRPA is under evaluation
$ORR^{R_i}(P_j)$	The overall reputation rating (within the [0,1] range) of the target SRPA P_j estimated by the evaluator SRRA R_i at time instance t_c
e	The predetermined distance level (within the [0,1] range) concerning returned reputation ratings
k_b	The factor (within the [0,1] range) determining the relative significance of the new trustworthiness level with respect to the old one
$l(TL_{pre}^{R_i}(R_x))$	The function of the R_x witness trustworthiness $TL_{pre}^{R_i}(R_x)$ introduced in order to keep the R_x trustworthiness rating of formula (8) within the range [0,1]

VII. PERFORMANCE EVALUATION RESULTS

In this paper, our aim is to extensively evaluate our framework and provide indicative evidence of the efficiency of our proposed scheme, incorporating various degrees of witnesses' misbehavior. We hereafter assume the existence of an area that falls into the domain of $\mathrm{M} = 10$ candidate SRPAs $P = \{P_1, P_2, \ldots P_M\}$ (i.e., a specific request may be handled by any of the candidate SRPAs belonging to the set P). Furthermore, it is assumed that $\mathrm{N} = 1000$ different SRRAs access the area. Each SRRA may be potentially a witness for the reputation formation of an SRP in the context of a specific request of another SRRA. Thus, the witness set is constituted by, at most, 999 witness SRRAs.

In order to evaluate SRPs' reliability, each SRP has been associated with a reliability probability, i.e., a measure of the likelihood that the SRP delivers the service in accordance with the agreement established. This probability has uniformly been set to the following values: 0.1 for SRPA P_1, 0.2 for SRPA P_2, 0.3 for SRPA P_3, 0.4 for SRPA P_4, 0.5 for SRPA P_5, 0.6 for SRPA P_6, 0.7 for SRPA P_7, 0.8 for SRPA P_8, 0.9 for SRPA

P_9, and 1 for SRPA P_{10}. A mixture of extreme and moderate values has been chosen in order to test the schemes under diverse conditions. In essence, with probability 0.1, SRPA P_1 complies with its promises, while P_9 maintains its promises with probability 0.9.

Fig. 3 depicts, for all SRPAs, the direct and overall reputation ratings, as estimated by 100 evaluator SRRAs (mean values are displayed), under the assumption that all witness SRRAs behave honestly, reporting their true valuation on the target SRPA's behavior (i.e., they provide to the evaluator the direct reputation rating of the target SRPA as formed on the basis of their past experiences in the system). The number of transactions conducted between all SRRAs with each SRPA in the system is a random variable uniformly distributed in the range [150,200]. From the obtained results, it may be observed that our model succeeds in estimating a reputation rating (overall and direct) very close to the assumed SRPAs' reliability probability, which is depicted in the x-axis (mean deviation is approximately 8%).

As a next step, we would like to test our framework's resilience to witnesses' misbehavior. To this end, we incorporated witness cheating behavior in our framework by gradually increasing the portion of misbehaving witnesses (i.e., the witnesses returning false feedback to the evaluator agent) as well as the distance of the false feedback reported to the evaluator from the actual valuation of the target SRPA's rating (i.e., the estimated rating formed by each witness SRRA on the basis of its direct experiences with the SRPAs). We consider the worst case scenario, i.e., the misbehaving witnesses collude, adding credits or discrediting providers, all modifying their estimated rating toward the same direction (either incrementally or decrementally) in accordance with the specified distance in order to form the feedback that would be returned to the evaluator SRRA. Specifically, we have considered that 10% up to 90% incremented by a step of 10% of the set of witnesses are providing inaccurate reputation-related information to the evaluator agent, varying in each case the distance of the inaccurate rating from their estimated rating to 10%, 30%, 50%, 70%, and 90% (both incrementally and decrementally toward the same direction each time). Several runs per experiment (50 runs) have been performed, while the mean values are illustrated in the figures. The standard deviation ranges between ± 0.05 around mean values, which show that the results acquired are close enough to the mean values displayed in the figures.

In the light of the aforementioned aspects, we examine the impact of witnesses' misbehavior to the overall reputation rating formation compared to the case of honest feedback provisioning. As a first step, we assume that witnesses' trustworthiness assumes its initial value (equal to 1) and is not dynamically updated, i.e., all witnesses are, in the eyes of the evaluator agent, behaving honestly, even if this is not the case. As a next step, this assumption is withdrawn, and the witnesses' trustworthiness is dynamically adjusted in accordance with the proposed model. For each of the aforementioned cases, Fig. 4(a) presents, for all SRPAs, the mean deviation of the estimated SRPAs' overall rating with respect to the corresponding rating estimated when all witnesses behave honestly. The mean deviation of the SRPAs' reputation rating given in the first group of bars

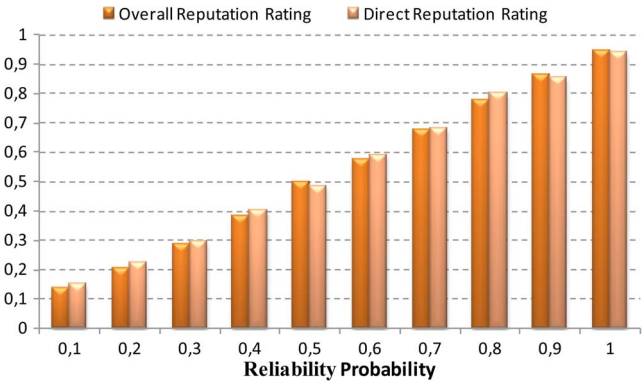

Fig. 3. Direct and overall reputation ratings for all SRPAs.

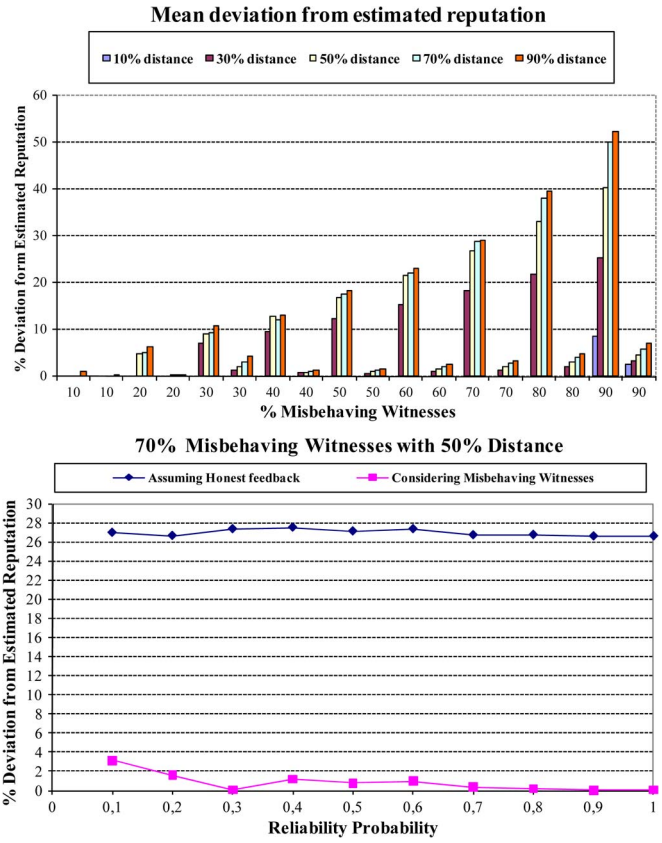

Fig. 4. (a and b) Mean deviation from estimated reputation for all SRPAs.

per misbehaving witnesses' percentage corresponds to the first case (the witnesses' trustworthiness level is not modified). The mean deviation of the SRPAs' reputation rating given in the second group of bars per misbehaving witnesses' percentage corresponds to the second case (identification of misbehaving witnesses and dynamic update of the respective witnesses' credibility). As it may be observed from Fig. 4(a), the mean deviation of the SRPAs' reputation rating estimation decreases significantly when dynamic adaptation of witness trustworthiness is performed in accordance with the proposed model. For example, the mean deviation from 12.5% (in the case of 50% misbehaving witnesses with feedback modification of 30% without dynamic adaptation of witness trustworthiness) drops to approximately 0.7% when adjusting their trustworthiness.

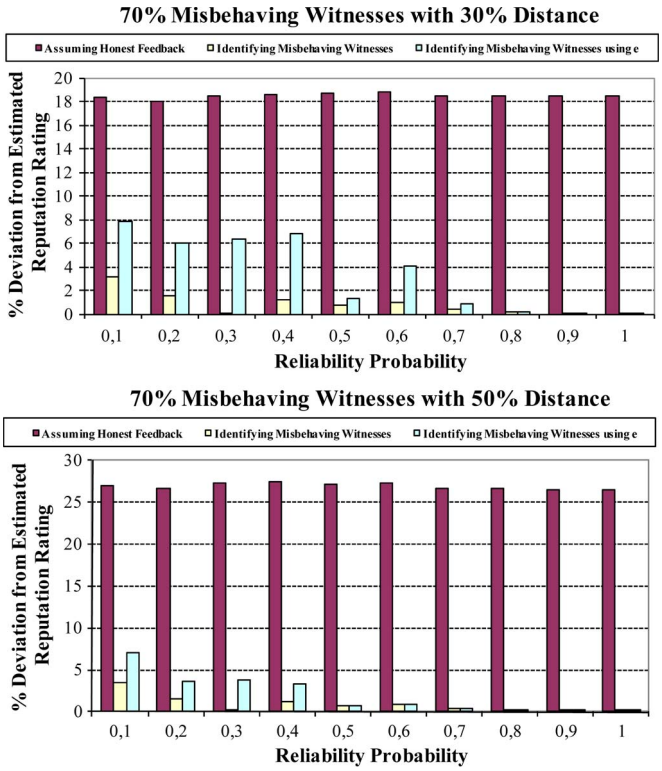

Fig. 5. (a and b) Deviation (%) of each SRPA's reputation rating estimation.

The same stands for the case of 50% misbehaving witnesses with feedback modification of 50% where the mean deviation drops from 17% to 1% as well as for the case of 90% misbehaving witnesses with feedback modification of 50% where the mean deviation drops from 40.3% to 4.7%. At this point, it should be noted that the distance from the estimated rating is either incrementally or decrementally taken for all misbehaving witnesses considered. This is, however, the worst case (as already discussed); otherwise, we would expect to see even more decreased mean deviation from the estimated rating.

Fig. 4(b) depicts the deviation of the SRPAs' overall reputation rating from the corresponding rating when all witnesses behave honestly, indicatively, for the case where 70% of the witnesses considered provide inaccurate reputation information and the distance of the disclosed information from the actual rating is 50%. From the obtained results of Fig. 4(b), it can be observed that the deviation drops below 3% when dynamic adaptation of witness trustworthiness is performed. Thus, due to the dynamic adaptation of the trustworthiness level of the misbehaving witnesses, our framework succeeds in introducing minimal impact to the overall estimated SRPA reputation rating (below 8%), even when a large portion of witnesses provide false feedback to the evaluator SRRA.

Considering that the distance level e constitutes an important parameter of our model as it defines the portion of misbehaving witnesses that are identified as such, in the following experiments, we aim to test its impact on SRPAs' overall reputation rating formation. In Fig. 5(a) and (b), the deviation of each SRPAs' overall reputation rating from the rating of SRPAs when all witnesses are honest is presented, taking into account three cases. In the first case, all witnesses are behaving

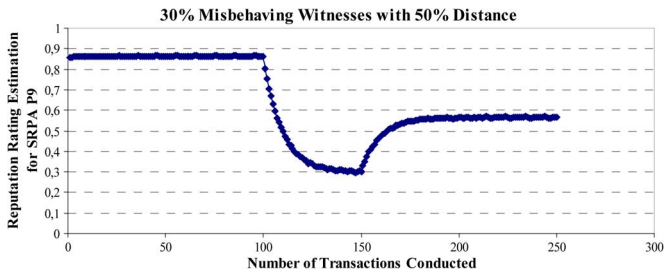

Fig. 6. Responsiveness of our proposed scheme to SRPA reliability-related behavioral modifications.

honestly in the eyes of the evaluator agent (no update of witnesses' trustworthiness takes place). In the second case, all misbehaving witnesses are identified (i.e., e assumes a very low value and is taken equal to 0.05), and the respective weighting factor taken into account in the SRPA's rating estimation is dynamically updated. In the third case, only the witnesses with feedback modification greater than the distance level $e = 0.25$ are identified as misbehaving, and their weighting factor is updated similarly to the previous case. We have considered 70% of misbehaving witnesses with 30% and 50% feedback modifications to their actual estimated rating. From the obtained results, it may be observed that, with distance level $e = 0.25$, acceptable deviations from actual reputation values are produced. To be more specific, as may be seen from Fig. 5(a) and (b), for all SRPAs, mean deviations on the order of 3.34% and 2.02% are introduced, respectively. Moreover, in Fig. 5(b), the deviation is decreased with respect to Fig. 5(a), as the distance value is larger; thus, more misbehaving witnesses could be identified in accordance with the proposed approach. It should be noted that it is quite logical to assume that most of the misbehaving witnesses in a real system are not expected to intentionally provide only slight feedback modifications (e.g., 10% or 20% feedback modification). Thus, under this assumption, the percentage of not identified misbehaving witnesses that provide false feedback will not produce significant errors to the reputation rating formation, as considered in the current version of this study.

Finally, we would like to examine the responsiveness of our scheme with regard to SRPA reliability-related behavioral modifications. We consider SRPA P_9 attributed with reliability probability 0.9. After 100 transactions have taken place, SRPA P_9 decides to take advantage of the reputation rating earned on the basis of its good behavior in the past and modifies its strategy so as to abide by the contract terms and conditions for the 30% of the transactions (i.e., reliability probability equal to 0.3). Finally, after the completion of 150 transactions, SRPA P_9 updates its behavior so as to adequately serve 60% of the service/resource requests. The experiment has been performed 50 times, while Fig. 6 illustrates the mean reputation values of SRPA P_9 with respect to the number of transactions conducted in the presence of 30% misbehaving witnesses with a feedback modification of 50%. As it may be observed, the reputation ratings acquired in accordance with our proposed framework follow in a quite efficient manner the SRPAs' strategy modifications.

VIII. Conclusion

In general, the scope of this paper is to propose a computational model for trust establishment based on a reputation mechanism, which incorporates direct service requestors' experiences and information disseminated from witness requestors in the system on the basis of their past experiences with service providers. Entities are rated with respect to whether they honored or not the agreements that they have established in the system, differentiating thus trust computation from service quality assessment. Our contribution lies in the fact that the designed mechanism discriminates between and addresses false ratings that are provided intentionally and unintentionally by witnesses in the system, minimizing their impact to the overall providers' reputation rating estimation. Witness credibility is efficiently formed, taking into account and dynamically updating the witness trust level, the number of transactions performed, and the respective transactional values. Our model caters for potential changes to providers' behavior, does not severely punish witnesses that are believed to unintentionally provide misleading feedback, does not exclude a misbehaving entity forever from the system, and weighs more in the evaluation of the overall reputation ratings recent events, enabling rating formation in an accurate manner. Additionally, the model proposed is fully distributed; witnesses are found in a completely decentralized manner, borrowing ideas from sociology, while the confinement of the witness set relieves the system from extra computational and communication overhead. Finally, treating reputation as a behavioral aspect independent of the services provided enables rating determination in a time-efficient manner.

Concerning future work, we consider adopting a similar to [22] approach for defining the initial reputation value assumed for SRPs and the initial trust level attributed to witnesses by the evaluator SRR. Additionally, consideration of an adaptive value following the percentage of misbehaving providers may provide a better alternative in terms of accuracy and fairness. Finally, similarly to [39], for the determination of the witness set, we consider moving the burden of obtaining trust information from the evaluator SRR to the SRPs being evaluated.

References

[1] M. Louta, "Towards a collaborative reputation based service provider selection in ubiquitous computing environments," in *Proc. UIC*, vol. 5061, *Lecture Notes in Computer Science*, F. E. Sandnes, Y. Zhang, C. Rong, L. T. Yang, and J. Ma, Eds., 2008, pp. 520–534.

[2] M. Louta, I. Roussaki, and L. Pechlivanos, "Reputation based intelligent agent negotiation frameworks in the E-marketplace," in *Proc. Int. Conf. E-Bus.*, Setubal, Portugal, 2006, pp. 5–12.

[3] M. Louta, A. Michalas, I. Anagnostopoulos, and D. Vergados, "Trust management framework for intelligent agent negotiations in ubiquitous computing environments," *Telecommun. Syst.*, vol. 41, no. 2, pp. 141–157, Jun. 2009.

[4] In Gambetta, Diego (ed.), Trust: Making and Breaking Cooperative Relations, electronic edition, Department of Sociology, University of Oxford, (13), 2000, 213–237 D. Gambetta, Can we Trust Trust? [Online]. Available: http://www.sociology.ox.ac.uk/papers/gambetta213-237.pdf

[5] A. Gutscher, "Reasoning with uncertain and conflicting opinions in open reputation systems," *Electron. Notes Theoretical Comput. Sci.*, vol. 244, pp. 67–79, Aug. 2009.

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

[7] Y. Atif, "Building trust in E-commerce," *IEEE Internet Comput. Mag.*, vol. 6, no. 1, pp. 18–24, Jan./Feb. 2002.

[8] G. Zacharia and P. Maes, "Trust management through reputation mechanism," *Appl. Artif. Intell. J.*, vol. 14, no. 9, pp. 881–908, 2000.

[9] R. S. Sutton and A. G. Barto, *Reinforcement Learning: An Introduction (Adaptive Computation and Machine Learning*. Cambridge, MA, USA: MIT Press, 1998.

[10] [Online]. Available: www.ebay.com

[11] Y. Bachrachm, A. Parnes, A. Procaccia, and J. Rosenschein, "Gossip-based aggregation of trust in decentralized reputation systems," *Auton. Agents Multi-Agent Syst.*, vol. 19, pp. 153–172, 2009.

[12] P. Resnick and R. Zeckhauser, "Trust among strangers in internet transactions: Empirical analysis of eBay's reputation system," *Econ. Internet E-Commerce*, vol. 11, pp. 127–157, 2002.

[13] Z. Malik and A. Bouguettaya, "Reputation bootstrapping for trust establishment among web services," *IEEE Internet Comput.*, vol. 13, no. 1, pp. 40–47, Jan./Feb. 2009.

[14] D. Trcek, "Trust management in the pervasive computing era," *IEEE Security Privacy*, vol. 9, no. 4, pp. 52–55, Jul./Aug. 2011.

[15] A. Boukerche and R. Yonglin, "A secure mobile healthcare system using trust-based multicast scheme," *IEEE J. Sel. Areas Commun.*, vol. 27, no. 4, pp. 387–399, May 2009.

[16] Y. Wang and K.-J. Lin, "Reputation-oriented trustworthy computing in E-commerce environments," *IEEE Internet Comput.*, vol. 12, no. 4, pp. 55–59, Jul./Aug. 2008.

[17] C. J. Hazard and M. P. Singh, "Interpersonal discount factors as a measure of trustworthiness in electronic commerce," *IEEE Trans. Knowl. Data Eng.*, vol. 23, no. 5, pp. 699–712, 2011.

[18] I. Varlamis, M. Eirinaki, and M. Louta, "A study on social network metrics and their applications in trust networks," in *Proc. Adv. Social Netw. Anal. Mining*, 2010, pp. 168–175.

[19] I. Varlamis, M. Eirinaki, and M. Louta, "Application of social network metrics to a trust-aware collaborative model for generating personalized user recommendations," in *Proc. Influence Technol. Social Netw. Anal. Mining*, vol. 6, *Lecture Notes in Social Networks*, T. Özyer, J. Rokne, G. Wagner, and A. H. P. Reuser, Eds., 2012, Springer-Verlag Wien.

[20] C. Jia, L. Xei, X. Gan, W. Liu, and Z. Han, "A trust and reputation model considering overall peer consulting distribution," *IEEE Trans. Syst., Man, Cybern. A, Syst., Humans*, vol. 42, no. 1, pp. 164–167, Jan. 2012.

[21] L. Xiaoyong, Z. Feng, and Y. Xudong, "Scalable Feedback Aggregating (SFA) overlay for large-scale P2P trust management," *IEEE Trans. Parallel Distrib. Syst.*, vol. 23, no. 10, pp. 1944–1957, Oct. 2012.

[22] Z. Malik and A. Bouguettaya, "RATEWeb: Reputation assessment for trust establishment among web services," *VLDB J.*, vol. 18, no. 4, pp. 885–911, 2009.

[23] K. Hwang and D. Li, "Trusted cloud computing with secure resources and data coloring," *IEEE Internet Comput.*, vol. 14, no. 5, pp. 14–22, Sep./Oct. 2010.

[24] J.-H. Cho, A. Swami, and I.-R. Chen, "A survey on trust management for mobile ad hoc networks," *IEEE Commun. Surveys Tuts.*, vol. 13, no. 4, pp. 562–583, 2011.

[25] S. K. Dhurandher, M. S. Obaidat, K. Verma, P. Gupta, and P. Dhurandher, "FACES: Friend-based ad hoc routing using challenges to establish security in MANETs systems," *IEEE Syst.*, vol. 5, no. 2, pp. 176–188, Jun. 2011.

[26] K. Lin, J. J. P. C. Rodrigues, G. Hongwei, X. Naixue, and L. Xuedong, "Energy efficiency QoS assurance routing in wireless multimedia sensor networks," *IEEE Syst.*, vol. 5, no. 4, pp. 495–505, Dec. 2011.

[27] Z. Guoxing, S. Weisong, and J. Deng, "Design and implementation of TARF: A trust-aware routing framework for WSNs," *IEEE Trans. Dependable Secure Comput.*, vol. 9, no. 2, pp. 184–197, Mar./Apr. 2012.

[28] Z. Yan and C. Prehofer, "Autonomic management for a component-based software system," *IEEE Trans. Dependable Secure Comput.*, vol. 8, no. 6, pp. 810–823, Mar./Apr. 2011.

[29] H. Li and M. Singhal, "Trust management in distributed systems," *IEEE Comput.*, vol. 40, no. 2, pp. 45–53, Feb. 2007.

[30] A. Das, "SecuredTrust: A dynamic trust computation model for secured communication in multiagent systems," *IEEE Trans. Dependable Secure Comput.*, vol. 9, no. 2, pp. 261–274, Mar./Apr. 2012.

[31] M. Srivatsa and L. Liu, "Securing decentralized reputation management using TrustGuard," *J. Parallel Distrib. Comput.*, vol. 66, no. 9, pp. 1217–1232, Sep. 2006.

[32] J. Zhang and R. Cohen, "Evaluating the trustworthiness of advice about seller agents in e-marketplaces: A personalized approach," *Electron. Commerce Res. Appl.*, vol. 7, no. 3, pp. 330–340, Nov. 2008.

[33] L. Xiong and L. Liu, "PeerTrust: Supporting reputation-based trust for peer-to-peer electronic communities," *IEEE Trans. Knowl. Data Eng.*, vol. 16, no. 7, pp. 843–857, Jul. 2004.

[34] W. Xiaofeng, L. Ling, and S. Jinshu, "RLM: A general model for trust representation and aggregation," *IEEE Trans. Services Computing*, vol. 5, no. 1, pp. 131–143, Jan.–Mar. 2012.

[35] Z. Yan, P. Zhang, and R. H. Deng, "TruBeRepec: A trust-behavior-based reputation and recommender system for mobile applications," *J. Pers. Ubiquitous Comput.*, vol. 16, no. 5, pp. 485–506, Jun. 2012.
[36] Z. Yan, Y. Chen, and Y. Shen, "A practical reputation system for pervasive social chatting," *J. Comput. Syst. Sci.*, vol. 79, no. 5, pp. 556–572, Aug. 2013.
[37] Z. Yan, Y. Chen, and Y. Shen, "PerContRep: A practical reputation system for pervasive content services," *J. Superomputing*, vol. 2014, pp. 1–24, 2014.
[38] K. Averer and Z. Despotovic, "Managing trust in a peer-2-peer information system," in *Proc. 10th Int. Conf. Inf. Knowl. Manag.*, Atlanta, GA, USA, 2001, pp. 310–317.
[39] T. Huynh, N. Jennings, and N. Shadbolt, "Certified reputation: How an agent can trust a stranger," in *Proc. 5th Int. Joint Conf. Auton. Agents Multi-Agent Syst.*, Hakodate, Japan, 2006, pp. 1217–1224.
[40] P. Yolum and M. P. Singh, "Engineering self-organizing referral networks for trustworthy service selection," *IEEE Trans. Syst., Man, Cybern. A, Syst., Humans*, vol. 35, no. 3, pp. 396–407, May 2005.
[41] A. Boukerche and Y. Ren, "A trust-based security system for ubiquitous and pervasive computing environments," *Comput. Commun. J.*, vol. 31, no. 18, pp. 4343–4351, Dec. 2008.
[42] P. Xu, J. Gao, and H. Guo, "Rating reputation: A necessary consideration in reputation mechanism," in *Proc. 4th Int. Conf. Mach. Learn. Cybern.*, 2005, pp. 182–187.
[43] M. He, N. Jennings, and H. Leung, "On agent-mediated electronic commerce," *IEEE Trans. Knowl. Data Eng.*, vol. 15, no. 4, pp. 985–1003, 2003.
[44] D. Cartwright and F. Harary, "Structural balance: A generalization of Heider's theory," *Psychological Rev.*, vol. 63, no. 5, pp. 277–292, Sep. 1956.

Stylianos Kraounakis is an Electrical Engineer graduate from the National Technical University of Athens, Athens, Greece. He holds an M.Phil. degree from the City University, London, U.K., and is currently working toward the Ph.D. degree in telecommunication networks at the Department of Informatics and Telecommunications Engineering, School of Engineering, University of Western Macedonia, Kozani, Greece.

He works as a Telecommunications Engineer for the Hellenic Telecommunication Organization (O.T.E. A.E.), Athens.

Ioannis N. Demetropoulos received the Ph.D. degree from Cambridge University, Cambridge, U.K., for research in the subject of molecular simulation (1975).

He held academic posts at the University of Ioannina, Ioannina, Greece, and subsequently became a Professor at the Department of Informatics and Telecommunications Engineering, University of Western Macedonia, Kozani, Greece. His work focuses on molecular informatics and the development of optimization algorithms for nonlinear multidimensional functions. His current interests include artificial intelligence, natural language evolution, and connectomics.

Angelos Michalas (M'10) is an Associate Professor at the Department of Computer Engineering, Technological Educational Institute of Western Macedonia, Kastoria, Greece. His research interests focus on telecommunication networks, advanced distributed network services, and quality of service/experience. He is the author of several peer-reviewed publications in these areas.

Mohammad S. Obaidat (F'05) received the Ph.D. and M.S. degrees in computer engineering with a minor in computer science from The Ohio State University, Columbus, OH, USA.

He is a Full Professor of Computer Science at Monmouth University, West Long Branch, NJ, USA. He has received extensive research funding, has published about 30 books and about 600 refereed technical articles in scholarly international journals and proceedings of international conferences, and is currently working on three more books. His research interests are wireless communications and networks, information and computer systems, algorithms and networks, applied neural networks and pattern recognition, and speech processing. For more information, see http://bluehawk.monmouth.edu/mobaidat/.

Panagiotis G. Sarigiannidis (S'05–M'07) received the B.Sc. and Ph.D. degrees in computer science from the Aristotle University of Thessaloniki, Thessaloniki, Greece, in 2001 and 2007, respectively.

He is currently a Lecturer at the Department of Informatics and Telecommunications Engineering, School of Engineering, University of Western Macedonia, Kozani, Greece. He has published over 60 peer-reviewed papers in international journals, conferences, and book chapters. His research interests include optical and wireless networks.

Malamati D. Louta (SM'13) received the M.Eng. and Ph.D. degrees in electrical and computer engineering and the M.B.A. degree from the National Technical University of Athens, Athens, Greece, in 1997, 2000, and 2004, respectively.

She is currently an Associate Professor at the Department of Informatics and Telecommunications Engineering, School of Engineering, University of Western Macedonia, Kozani, Greece. She is the author of more than 80 peer-reviewed publications. Her research interests include telecommunication networks and advanced telecommunication services engineering. For more information, see http://users.uowm.gr/louta.