Towards Trust Establishment in Ubiquitous Computing Environments

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

[1]Technological Educational Institute of Western Macedonia, Department of Business Administration
[1]University of Western Macedonia, Department of Information and Communication Technologies Engineering
GR-50100, Kozani, 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. In this study, a reputation mechanism is proposed which helps estimating SRPs trustworthiness and predicting their future behaviour, taking into account their past performance in consistently satisfying SRRs' expectations. The 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.

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. 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, 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 rest if this study is organized as follows. In the next section, the fundamental considerations of the proposed mechanism are given, while section 3 discusses on initial findings of the efficiency of our scheme.

2. Reputation Mechanism Fundamentals

Assuming the presence of 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.

The proposed reputation mechanism is collaborative in the sense that it considers both first-hand information (acquired from the SRRA's past experiences with the SRPAs) and second-hand information (disseminated from other SRRAs). To be more specific, each SRRA keeps a record of the reputation ratings of the SRPAs it has negotiated with and 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 SRRA's 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 SRRA that have previously been served by the SRPAs under evaluation. In the current version of this paper, we assume that a Service/Resource Provider Reputation Broker component

(SRPRB) maintains a list of the SRPAs providing a specific service / resource as well as a list of SRRAs that have previously interacted by a specific SRPA. 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. 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 trust level dynamically updated, which reflects whether the SRRA provides feedback with respect to its experiences with the SRPAs truthfully and in an accurate manner. In essence, this trust level is a measure of the credibility of the witness information. To be more specific, in order to handle intentional inaccurate information, an honesty probability is attributed to each SRRA, i.e., a measure of the likelihood that a SRRA gives feedback compliant to the real picture concerning service provisioning. Second-hand information obtained from trustworthy SRRAs (associated with a high honesty probability), are given a higher significance factor, whereas reports (positive or negative) coming from untrustworthy sources have a small impact on the formation of the SRPAs' reputation ratings. Concerning the provision of inaccurate information unintentionally, the authors take into account the number of transactions a witness SRRA has performed with the target SRPA and the sum of the respective transaction values. Specifically, it is quite safe to assume that SRRAs that have been involved with the target SRPA only for a few times will not have formed an accurate picture regarding its behaviour. Additionally, if the reputation rating is formed on the basis of low-valued transactions, there is a possibility that it does not reflect the real picture (e.g., an SRPA may strategically exhibit good behaviour in case its potential profits in a context of a transaction are low and cheat when the expected earnings are high).

The evaluator SRRA uses the reputation mechanism to decide on the most appropriate SRPA, especially in cases where the SRRA doubts the accuracy of the information provided by the 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.

3. Discussion

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.

4. 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.