Collaboration and the Knowledge Economy: Issues, Applications, Case Studies
Paul Cunningham and Miriam Cunningham (Eds)
IOS Press, 2008 Amsterdam
ISBN 978–1–58603–924-0

Efficient Trust Aware Resource Allocation in Distributed Computing Environments

Malamati LOUTA[1], Angelos MICHALAS[2], Ioannis ANAGNOSTOPOULOS[3]
[1]*Harokopio University of Athens, Department of Informatics and Telematics, 70 El. Venizelou Str., Athens, 17671, Greece*
Tel: +302109549100, Fax: + 302109577050, Email: louta@telecom.ntua.gr
[2]*Technological Educational Institute of Western Macedonia, Department of Informatics and Computer Technology, P.O.Box 30, Kastoria, 52100, Greece*
Tel: +302467087260, Fax: +302467087063, Email: amichalas@kastoria.teikoz.gr
[3]*University of Aegean, Department of Information and Communication Systems Engineering, Karlovassi, Samos Island, 83200, Greece*
Tel: +302273082220, Fax: +302273082008, Email: janag@aegean.gr

Abstract: Dynamic distributed computing environments are composed by various entities, which, seeking for the maximization of their welfare while achieving their own goals and aims, may act selfishly, thus, leading to a significant deterioration of system's performance. In general, system entities may be classified into two main categories: the Resource Requestors (RRs) wishing to use and/or exploit resources offered by the other system entities and the Resource Providers (RPs) that offer the resources requested. In this study, a reputation mechanism is proposed which helps estimating RPs trustworthiness, taking into account their past performance in consistently satisfying RRs' expectations. The trust management framework is distributed, considers both first-hand information (acquired from the RR's direct past experiences with the RPs) and second-hand information (disseminated from other RRs), while it exhibits a robust behaviour against inaccurate reputation ratings. The designed mechanisms have been empirically evaluated, exhibiting improved performance with respect to random RP selection.

1. Introduction

The roles of system entities in dynamic distributed computing environments may be classified into two main categories that, in principle, are in conflict. These two categories are: the entities that wish to use and/or exploit resources offered by other system entities (Resource Requestors - RRs) and the entities that offer the resources requested (Resource Providers - RPs). The aim of this paper is to propose enhancements to the sophistication of the functionality that can be offered by distributed computing environments. Resource Requestors should be provided with mechanisms that enable them to find the most appropriate Resource Providers, i.e., those offering the resources required at an acceptable quality level 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 in order to establish the 'best' possible service level agreement terms (SLAs) and conditions with respect to resource access and provision [1], in conjunction with trust mechanisms [2] 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. In case RPs do not abide by the agreed SLA terms and conditions, penalties are

imposed, so as to reimburse RRs that incur the loss. In parallel, *Reputation Mechanisms* may be employed to provide a "softer" security layer, considered to be sufficient for many multi-agent applications [6], emerging in complex, heterogeneous and highly variable environments. Reputation mechanisms establish trust by exploiting learning from experience concepts [7] 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) [8]. 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.

In the context of this study, our focus is laid on the evaluation of the reliability of RPs. To this respect, a collaborative reputation mechanism is proposed, which takes into account the RPs' past performance in consistently satisfying RRs' expectations. To be more specific, the reputation mechanism rates the RPs with respect to whether they honoured or not the agreements established with the RRs, thus introducing the concept of trust among the involved parties.

The rest of the paper is structured as follows. Section 2 presents the software architecture that supports the proposed trust management framework, while the software elements required are identified. Section 3 discusses on the fundamental concepts and methodology followed for the proposed collaborative reputation mechanism, aiming to offer an efficient way of building the necessary level of trust in the distributed computing environments. Section 4 provides a set of indicative results of the efficiency of the proposed trust management framework. Section 5, provides a brief overview of the related research literature and subsequently highlights the contribution of this study. Finally, in Section 6, conclusions are drawn and directions for future plans are given.

2. Software Architecture & Technology Adopted

In accordance with the service oriented architectures concept [9],[10],[11] and exploiting advanced software paradigms (e.g., distributed object computing [12] and intelligent mobile agents [13],[14]), the service logic is realised by a set of autonomous co-operating components, which interact through middleware functionality that runs over Distributed Processing Environments (e.g., CORBA, Parlay). Intelligent Mobile Agent Technology (MAT) has been considered as a paradigm that can help service designers to handle the potential increased functionality involved in service creation and deployment. According to a simple definition, intelligent mobile agents are software components incorporating intelligent functionality that can at a certain point in time migrate to perform a specific task.

This study is based upon the notion of interacting intelligent agents which participate in activities on behalf of their owners, while exhibiting properties such as autonomy, reactiveness, proactiveness, social ability and adaptivity in order to achieve particular objectives and accomplish their goals [15]. Thus, Resource Requestor Agent (RRA) is introduced and assigned with the role of capturing the RR preferences, requirements and constraints regarding the requested resource, delivering them in a suitable form to the appropriate RP entity, acquiring and evaluating the corresponding RPs' offers, and ultimately, selecting the most appropriate RP on the basis of the quality of its offer and its reputation rating. Resource Provider Agents (RPAs) are the entities acting on behalf of the RPs. Their role would be to collect the RR preferences, requirements and constraints and to make a corresponding offer, taking also into account certain environmental criteria. RRAs

and RPAs are both considered to be rational and self-interested, while aiming to maximize their owners' profit.

3. Fundamental Considerations & Methodology Followed

In the following subsections, the authors discuss on the basic concepts and assumptions, taken into account in the overall trust aware resource allocation framework designed.

3.1 RPs' Overall Reputation Rating Estimation

The proposed reputation mechanism for the reliability related factor estimation is collaborative in the sense that it considers both first-hand information (acquired from the RRA's past experiences with the RPAs) and second-hand information (disseminated from other RRAs). To be more specific, each RRA keeps a record of the reputation ratings of the RPAs it has negotiated with and been served by in the past. This rating based on the direct experiences of the evaluator RRA with the target RPA forms the first factor contributing to the overall RPA reputation and is formed on the basis of learning from experience techniques (e.g., reinforcement learning [7]). In the context of this study, a basic assumption is that the reputation ratings lie within the [0,1] range, where a value close to *0* indicates a misbehaving RP. Concerning the RPAs' reputation ratings based on feedback given by other RRA on their experiences in the system (the second factor contributing to the overall RPA 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 RPAs' reputation ratings formed after taking into account each RRA view on the RPAs' performance [2]). This approach on one hand has significant computational, communicational, time and storage advantages, but on the other hand it may suffer from the classical disadvantages of all centralized methodologies (e.g., introduction of performance bottlenecks and single point of failure in the system).

In the context of this study, we adopt a decentralized approach with respect to witness based information concerning RPAs' reputation ratings. Specifically, a basic assumption is that each RRA is willing to share their experiences and provide whenever asked for the reputation ratings of the RPAs 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 RRAs that have previously been served by the RPAs under evaluation. In the current version of this paper, we assume that a Resource Provider Reputation Broker component (RPRB) maintains a list of the RPAs providing a specific service / resource as well as a list of RRAs that have previously interacted with a specific RPA.

At this point some clarifications with respect to the proposed model should be made. First, the reliability of RPAs is treated as a behavioural aspect, independent of the resources provided. Thus, the witnesses list may be composed by RRAs which have had direct interactions with the specific RPA in the past, without considering the resource consumed. Second, RPAs have a solid interest in informing RPRB with respect to resources they currently offer, while the RRAs 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 RPRB to keep accurate and up to date information.

3.2 Obtaining Accurate Feedback from Witnesses

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 RRAs (both intentional and unintentional), the evaluator RRA can mostly rely on its own experiences rather on the target RPA's reputation ratings provided after contacting the RRAs. To this respect, RPA's reputation ratings provided by the witness RRAs may be attributed with a relatively low significance factor.

In the context of this study, we consider that each RRA is associated with a weighting factor dynamically updated, which reflects whether the RRA provides feedback with respect to its experiences with the RPAs truthfully and in an accurate manner. In essence, this weighting factor is a measure of the credibility of the witness information. To be more specific, in order to handle intentional inaccurate information, an honesty probability is attributed to each RRA, i.e., a measure of the likelihood that a RRA gives feedback compliant to the real picture concerning service provisioning. Second-hand information obtained from trustworthy RRAs (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 RPAs' reputation ratings. Concerning the provision of inaccurate information unintentionally, the authors take into account the number of transactions a witness RRA has performed with the target RPA and the sum of the respective transaction values. Specifically, it is quite safe to assume that RRAs that have been involved with the target RPA 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 RPA 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). Furthermore, time effect has been considered and incorporated in our mechanism in order to model the fact that more recent events should weigh more in the target RP's overall reputation evaluation.

3.3 Decision on the Most Appropriate RP Concerning the Resource Provisioning

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

The evaluator RRA uses the reputation mechanism to decide on the most appropriate RPA, especially in cases where the RRA doubts the accuracy of the information provided by the RPA. A learning period is required in order for the RRAs to obtain fundamental information for the RPAs. During the learning period and in case reputation specific information is not available to the RRA (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 RPA selection. Thus, the RP'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 RRA and updating it after resource consumption has taken place. Finally, it should be mentioned that the reliability rating value of the RPAs 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.

3.4 Updating Outdated RPAs' Reputation Related Information

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

In order to take into account new RPAs that enter the system and/or not to exclude RPAs that initially did not honour the terms and conditions of the contracts established, thus being attributed with a small reliability related value after the learning period, and give them a chance to re-enter to the system and improve their reputation rating in case they abide by the SLA terms and conditions, the simplest possible approach that could be adopted is to base the RRAs' decision concerning the most appropriate RPA (after a specific time period, or after the completion of a specific number of transactions) on the RPAs' performance and omit the RPAs' reputation rating values until possible outdated information the system possesses is updated. In the context of this study, the authors consider the reduction of the RPs' reliability related values to the pre-specified minimum (i.e., 0.1) in case a predetermined number of transactions have been completed in the system, whenupon the RPRB component sends a warning message to all RRAs registered in its database. At this point it should be noted that the predetermined number of transactions is considered to assume a quite big value in order not to constitute a disincentive for honest behavior.

4. Results

This section provides some indicative results on the behaviour of the Resource Provider trust aware selection mechanisms that are proposed in this paper. We hereafter assume the existence of an area that falls into the domain of $P = \{P_1, P_2, ...P_M\}$ candidate Resource Providers (that is a specific request may be handled by any of the candidate RPs belonging to the set P). Regarding the different Resource Requestors that access the area, it is assumed that N classes exist. RR classes are interested for the same resource, differentiated however with respect to the quality/quantity level required. Without loss of generality, all RPs are assumed to offer the required quantity/quality levels. Hereafter, it is assumed that $N = 10$ and $M = 10$.

The proposed framework was empirically evaluated by simulating the interactions among RRAs and RPAs. At this point, a basic assumption is that the RPAs propose exactly the same offer to the evaluator RRAs (exactly the same terms and conditions for the potential SLA). In the light of the assumption made, the Resource Provider selection is reduced to choosing the one with the highest reputation value. This way, the acquisition of an initial set of indicative results that show the behaviour of our proposed trust aware framework is enabled.

In order to evaluate the RPs' reliability, each RP has been associated with an honesty probability, i.e., a measure of the likelihood that the RP delivers the service compliant with the agreement established. This probability has been set to the following values: 0.9 for RPAs P_1 and P_5, 0.8 for P_4, 0.7 for P_7 and P_8, 0.6 for P_3 and P_6, 0.4 for P_2 and P_9, and 0.3 for P_{10}. In essence, with probability *0.9* RPA P_5 complies with its promises concerning resource provisioning during simulation runtime, whereas P_{10} maintains its promises with probability *0.3*. A mixture of extreme and moderate values has been chosen in order to test the schemes under diverse conditions.

Figure 1 depicts the formation of the reputation ratings of RP P_6 for five different RRAs, based on their direct experiences. As it may be observed, 20 transactions are required in order to obtain an accurate picture concerning the RP's reputation rating. The reputation rating variations around 0.6 (the honesty probability assigned to RP P_6) illustrated in Figure 1 may be attributed to the fact that the rating estimations are affected by RP's past behaviour concerning resource provisioning, which in our experiments is determined by a random variable.

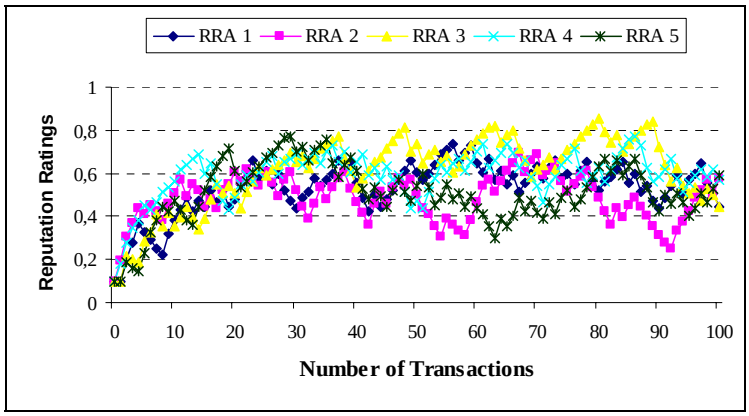

Figure 1: RP's P_6 Reputation Rating Formation for Five Different RRAs on the Basis of Their Direct Experiences in the System.

Figure 2 illustrates the reputation ratings of each RP, as estimated after 1000 transactions have been conducted (with each RP) in the system. In the context of the experiments conducted, all RR classes are considered to be witnesses and their vast majority is assumed to behave in an honest manner. As may be observed from Figure 2, the most appropriate RP is P_5 (ranked first), followed by RP P_1 (ranked second), followed by RP P_4 (ranked third), followed by P_7, P_8, P_3, P_6, P_2, while the RP P_9 occupies the 9th ranking position and P_{10} the 10th ranking position.

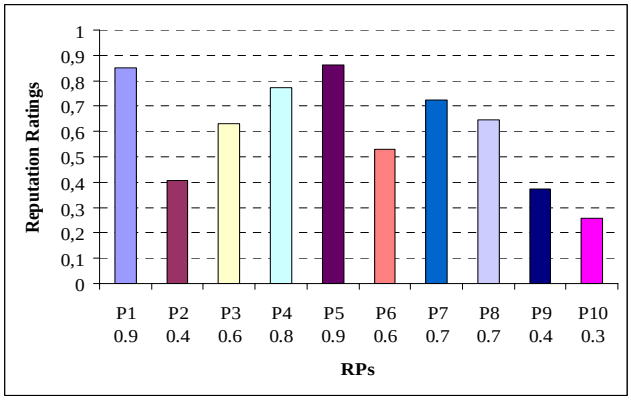

Figure 2: Reputation Ratings for All RPs Serving Resource Requests Originating from the RR Classes Considered in the System

Finally, comparing the effectiveness of our RP selection mechanism on the basis of the reliability ratings of the RPs with respect to the random RP selection scheme (i.e., the RP for resource provisioning is selected randomly), we may note that in general our designed framework exhibits increased RR satisfaction, which on average is 30%, due to the fact that in our mechanism RPs honouring in the past the agreements established with the RRs are selected for resource provisioning in the future.

5. Related Research Overview

The focus and contribution of this study is laid on the design of a trust management framework, assessing RPs' reliability in an accurate and time – efficient manner by means of a decentralized, collaborative reputation mechanism, forming RPs reputation ratings, which reflect whether RPs provide to the RRs the resource that corresponds to the established contract terms or not. The proposed reputation management mechanism considers both direct RRs experiences with RPs and witnesses information disseminated from other RRs on the basis of their past experiences with the RPs under evaluation, while being resilient to inaccurate information intentionally and/or unintentionally provided.

The work of this paper is related to pertinent previous work in the literature, since trust establishment and management is a topic that attracts attention of the researchers [16], [17]. Most reputation based systems in related research literature aim to enable entities to make decisions on which parties to negotiate/cooperate with or exclude, after they have been informed about the reputation ratings of the parties of interest. The authors in this study do not directly exclude / isolate the RPs that are deemed misbehaving, but instead base the RRs' decision on the most appropriate RP on a weighted combination of the evaluation of the quality of the RPs' offer (potential SLA's terms and conditions) and of their reputation rating (reliability related factor).

Various systems for trust establishment have been presented (e.g., [18], [19]), a number of which utilize the opinion / view other system participants have on the entities under evaluation. However, a number of them do not clearly describe how the evaluator entities find in the system feedback sources used for the overall evaluation of the target entities. Additionally, our mechanism in order to elicit true feedback considers intentional as well as unintentional inaccurate information provisioning, taking into account, in addition to witness trustworthiness, the number of transactions a witness RR has performed with the target RP and the sum of the respective transactional values. Finally, in our framework, 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, while untrustworthy RPs are given a chance to re-enter the system and improve their reputation rating in case they abide by the established SLA terms and conditions.

6. Conclusions

The scope of our paper is to enhance the functionality that may be offered by distributed computing environments. Under the assumption that a number of Resource Providers (RPs) may handle and serve the Resource Requestors (RRs) requests with the same SLA terms and conditions, the RRs may decide on the most appropriate RP for the resource requested on the basis of their reputation rating. The reputation mechanism adopted is distributed, considers both first-hand and second-hand information, 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 RPAs and RRAs and has performed well. Our obtained results indicate that the proposed RP selection scheme exhibits increased RR satisfaction with respect to random RP 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. Furthermore, the authors consider moving the burden of obtaining trust information from the evaluator RRA to the RPAs being evaluated.

References

[1] 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.

[2] 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.

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

[9] The Parlay Group http://www.parlay.org/

[10] OSGi (1999) Open Service Gateway Initiative, http://www.osgi.org

[11] B. Benatallah, Q. Sheng, and M. Dumas "The Self-Serve Environment for Web Services Composistion", IEEE Internet Computing, vol. 7, no.1, pp.40-48, 2003.

[12] S. Vinoski "CORBA: Integrating diverse applications within distributed heterogeneous environments", IEEE Communications Magazine, vol. 35, no. 2, pp. 46-55, 1997.

[13] P. Morreale "Agents on the move", IEEE Spectrum, vol. 35, no. 4, pp. 34-41, 1998.

[14] N. Jennings, K. Sycara, and M. Wooldridge "A Roadmap of Agent Research and Development", Autonomous Agents and Multi-Agent Systems, vol. 1, no. 1, pp. 7-38, 1998.

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

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

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

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

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