Credible Reputation Systems for P2P e-Communities

Eleni Koutrouli[1]

National and Kapodistrian University of Athens
Department of Informatics and Telecommunications
ekou@fi.uoa.gr

Abstract. Reputation mechanisms for distributed e-Communities are vital tools for facilitating trust decisions regarding transactions between entities. Motivated by the current challenges in the area of P2P reputation systems regarding their desgign, credibilty enhancement and objective evaluation, in this thesis we worked towards (1) creating a framework for the development and evaluation of secure reputation systems, and (2) designing and evaluating a credible reputation system for P2P communities with incentives for honest recommendations. We have thus created a conceptual model and a credibility framework for the design of credible reputation systems. We also proposed an evaluation framework for reputation systems for their objective evaluation and comparison. We then developed a credible reputation system (CREPARS) which consists of (a) credibility-enhanced reputation estimation algorithms and processes and (b) a novel recommendation exchange mechanism which is based on recommendation trustworthiness of entities and uses a PKI-based payment scheme. For the evaluation of the proposed reputation system we used credibility analysis and simulation in various attack scenarios and in comparison with other well-known reputation systems. The results have shown that the proposed reputation mechanisms exhibit resilience to various attacks and offer incentives for honest recommendations, leading to increased efficiency.

Keywords: reputation systems, trust, credibility, threat analysis, evaluation of reputation systems, simulation of reputation systems, trust management

1 Dissertation Summary

Contemporary e-Communities have emerged in various application and technological contexts. One of their basic characteristic is the need of their users to be supported in their decision about other users and objects which they have to trust for their transactions. Efficient Reputation Systems (RSs), which integrate the concepts of trust and reputation and support trust decisions in applications for distributed e-Communities, have become vital components for these applications. The systematic

[1] Dissertation advisor: Aphrodite Tsalgatidou, Associate Professor

study of RSs, with a focus on P2P RSs, has revealed a number of issues which impede their efficiency and consequently the efficiency of the application they support. These challenges, specifically the lack of (a) reference reputation models that could facilitate their design, (b) a comprehensive threat analysis and (c) methods and frameworks for the objective evaluation of P2P reputation systems and their comparison, have motivated us towards defining the goals of this thesis, which are the following:

1. Creation of a generic framework for the development and evaluation of secure reputation systems
2. Development of a secure and credible reputation system for P2P e-Communities with incentives for honest recommendations based on the defined generic framework
3. Evaluation of the efficiency and resilience of the proposed reputation system against various attacks and various forms of malicious behavior, in comparison with other RSs, based also on the developed generic framework.

For the satisfaction of the first goal we created a *conceptual model* for the design of reputation systems, a *credibility framework* for the integration of credibility factors in a reputation system, and an *evaluation framework* for the evaluation of reputation systems through suitable methods or through a common evaluation and comparison framework. For the satisfation of the second and third goals we used the proposed conceptual framework for the design, implementation and evaluation of a credible RS for decentralized e-Communities with incentives for honest recommendations. These results are described in Section 2, whereas the main contributions of the thesis are summarized in Section 3.

2 Main Results

2.1 Conceptual Model for P2P Reputation Systems

In order to to facilitate the design of decentralized RSs we present a reference reputation system for P2P RSs, which comprises the concepts, roles, relationships, functionality and design characteristics of such RSs. A detailed description can be found in [12].

Reputation systems use information related with the transactional behavior of entities for the estimation of their reputation and consequently for making trust decisions. They are based either on a centralized structure (e.g. eBay [1]) or on decentralized structures (e.g. [2]-[4]), found mainly in P2P systems, where reputation management is distributed to the participating entities.

In a decentralized RS the participating entities play interchangeably the roles of the *trustor*, the *trustee* and the *recommender*. The trustor is an entity which wants to make a trust decision regarding whether to participate in a transaction with another entity, the trustee. A transaction can involve accessing a resource, an e-Commerce trade, etc. The recommender is the entity that provides the trustor with information regarding the trustworthiness of the trustee (recommendation). In file sharing P2P applications, recommendations may also be given for objects, e.g. files. To make a trust decision the trustor tries to predict the future behavior of the trustee by forming a view of the trustee based on experience about its earlier actions. This subjective view is formed by

estimating an indicator of the quality of the trustee regarding its services and comprises the trustee's *reputation* or *trustworthiness* from the trustor's point of view. To form a reputation view, the trustor needs to gather experience information, either by referring to its own earlier experience with the trustee, or by acquiring it from other entities in the form of recommendations. Recommendations can be based on the recommender's personal experience alone, or on a combination of personal experience and earlier recommendations from others. The various roles of the participating entities in a decentralised RS are illustrated in the UML diagram of Figure 1.

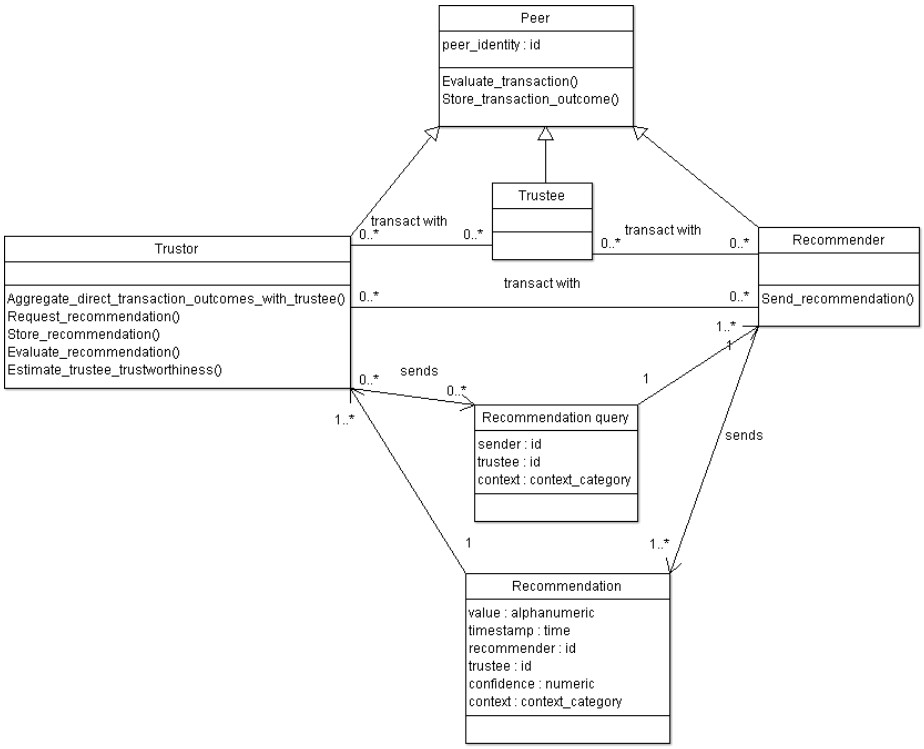

Fig. 1. Conceptual Representation of a Decentralized Reputation System

We outline below the basic characteristics) of a RS (presented also in [5]) for which various design choices can be made in order to cover the related requirements.

1. **Recommendation Content and its Representation**. A recommendation can be an arithmetic value, a combination of a value and associated semantic information, such as confidence or context, etc. Various formats can be used, such as binary, scalar or continuous values in a specific interval.
2. **Recommendation Formation**. It can be done based on the evaluation of a single transaction or on aggregated ratings regarding transactions with the the trustee.
3. **Selection of Recommenders**. This can be done based on recommenders' credibility, on social relationships, on recommendation similarity of the recommender and the trustor regarding commonly evaluated peers, etc.

4. **Reputation Estimation**. As described in [6], reputation estimation approach can be either deterministic, probabilistic or based on fuzzy logic.
5. **Storage and Dissemination of Reputation Information**. Reputation values may be estimated either reactively or proactively. They are stored by the trustor or the trustee or by other special peers. Their communication to the interested parties is done either upon request, or using a disseminating technique.
6. **The Way a Trust Decision is Made**. Trust decisions are threshold-based or rank-based; they are based on the estimated reputation values, therefore, the latter should be translated in a manner that facilitates trust decisions.

2.2 Taxonomy for RSs for Social Network (SN)-based applications

In SN-based applications the concept of reputation is expanded to new meanings, such as "user influence", and RSs use various indirect mechanisms, i.e. mechanisms which are based on social network-related information, rather than ratings. We have thus proposed a taxonomy for such RSs based on their identified dimensions. This taxonomy can be used for the classification of RSs for various types of SN-based applications and for facilitating the design of a RS for a particular SN-based application [7].

2.3 Credibility Framework and Threat analysis of Decentralized RSs

The accuracy of reputation estimation, and thus the credibility of a RS, are affected by a number of factors which we present, grouped in three categories, in Table 1:

Table 1. Credibility Factors of a Reputation System

Factors related to **Recommendation Creation/Content**	Factors related to **Recommendation Selection**	Factors related to **Reputation Reasoning**
Type of recommendation information (value, statement, etc.)	Recommender's credibility	Aggregation method (estimation formula, recency considerations, reputation value translation)
Creation method (transaction rating or opinion)	Uncertainty awareness	History of transactions and recommendation information
Type of experience (negative and/or positive) evaluated in a recommendation	Recommender selection method, considerations about possible bias or pressure	Storage and dissemination methods for reputation values
Recommender's identity	Storage and dissemination methods for recommendations, considerations about possible bias or pressure	Evaluation of estimated reputation
Recommender's confidence on recommendation	Mediator's credibility	Secure storage and retrieval of global reputation values
Binding recommendations with transactions	Who collects recommendations, possible bias	

Entities participating in reputation systems can distort the credibility of the latter in various ways, either as individuals or in cooperation with others, depending on the specific application and social setting of the reputation system. We have classified reputation attacks or misbehavior in the following three main categories:

- **Unfair recommendations**: Entities can spread unfair ratings for other entities in order to lower or increase the reputation of the target entities unfairly. Unfair ratings can be due to lying, misjudging the outcome of a transaction, or making a mistake in the recommending procedure.
- **Inconsistent behavior**: Peers may strategically have an inconsistent behavior that can lead to an incorrect estimation of their reputation allowing them to misbehave and still keep a high reputation. For example, they can misbehave part of the time or towards a subset of peers or change their behavior suddenly or periodically.
- **Identity management related attacks**: A deciding factor for attacks in this category is the identity scheme used in a RS. For example, when the identity scheme permits the use of multiple identities by the same peer, a malicious peer may behave dishonestly and then escape its low reputation by entering the system with a new identity. Furthermore, when an entity A can communicate or store a recommendation produced by an entity B for an entity C without linking its identity and B's identity with the recommendation, then A can easily manipulate the recommendation value. Also, if the system permits it, peers may refuse having sent a recommmendation.

A detailed taxonomy of the attacks against RSs is depicted in Figure 2, and thoroughly described in [10], together with a detailed presentation of the related defense mechanisms. The identified defense mechanisms have been then mapped with the attacks which they confront and with the specific categories of credibility factors to which they belong [10]. This mapping can be used as a guide for the implementation of suitable defense mechanisms in the process of designing a RS.

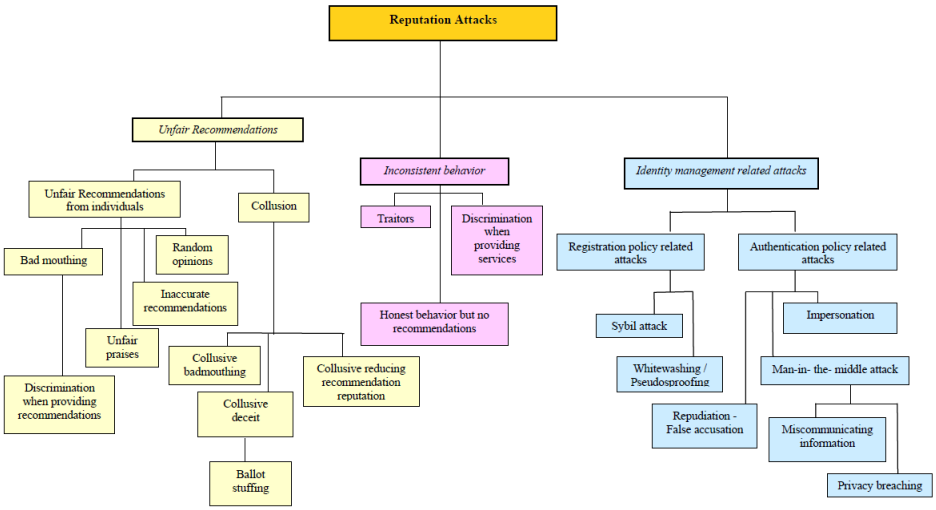

Fig. 2. Taxonomy of Attacks against Reputation Systems

2.4 Evaluation Framework for Reputation Systems

The plethora and heterogeneity of works regarding RSs for various e-Communities creates the need for objective evaluation and comparison between different RSs under the same conditions. Most of the evaluation approaches used in the proposed reputation systems are either proprietary or common experiments under restricted cases. However, the emerged need for generic evaluation approaches led to a number of research works which focus on the development and use of generic frameworks for evaluation and comparison of reputation systems, to which we refer as Common Evaluation Frameworks (CEFs). These works are either theoretic, i.e. they study how a reputation system deals with a number of criteria or attacks, or offer simulation and implementation platforms / tools for the evaluation, comparison and fine-tuning of reputation systems through experimentation. We have classified the various available approaches for RS evaluation according to the taxonomy presented in Figure 3 [11].

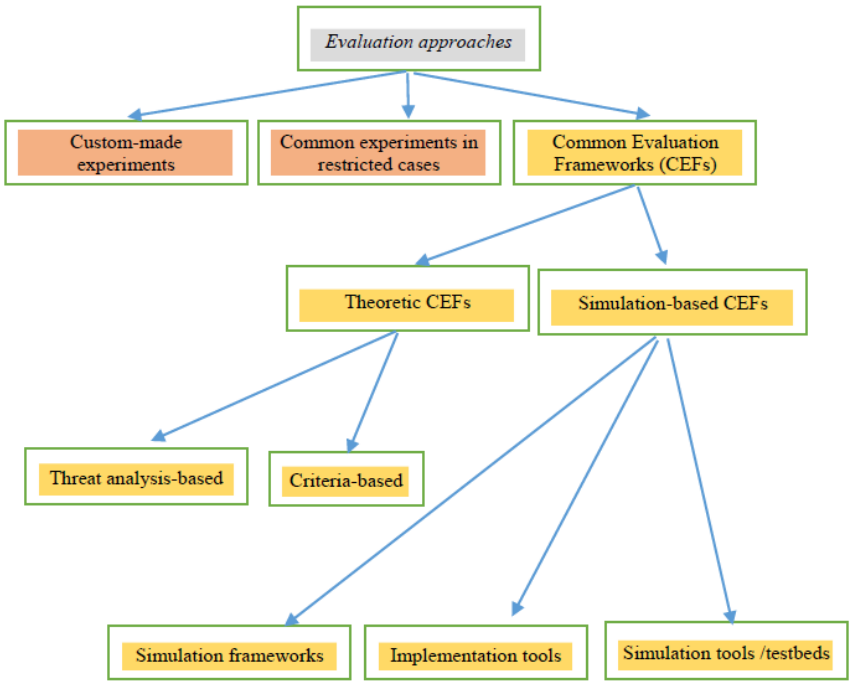

Fig. 3. Taxonomy of Evaluation Approaches

We have focused on works offering CEFs and we have formulated a set of characteristics / properties that are desirable for a generally accepted CEF in order to produce reliable comparisons, as follows: (1) *Standardization*, (2) *Independence of the reputation system characteristics*, (3) *Flexibility*, (4) *Ease of implementation of new reputation systems and new tests*, (5) *Availability of existing implementations of reputation system tests*. In [11] we present the level of conformance of a number of

simulation-based CEF found in the literature to the desirable characteristics, according to the information provided by the authors. We have also defined a number of factors that affect the desirable characteristics. The proposed evaluation framework facilitates (a) finding suitable evaluation methods/CEFs and (b) defining generally accepted CEFs.

2.5 Credibility-enhanced & Payments-based Reputation System for Decentralized Systems (CREPARS)

The proposed reputation system aims at providing credible reputation estimation with incentives for honest recommendations (ratings) and excibiting thus resilience to various attacks. It comprises (a) a reputation model which involves the algorithms for the estimation of the various reputation components and the final reputation value which is based on these components, and (b) a recommendation exchange mechanism which is based on virtual payments and a Public Key Infrastructure (PKI).

Reputation Model. The proposed RS estimates an *overall reputation* value for the trustee which comprises:

a) the *direct reputation* of the trustee from the point of view of the trustor, which is the time weighted average of the transaction evaluation values regarding the direct transactions between the trustor and the trustee.
b) the *indirect repuation* value of the trustee, which is based on third parties' recommendations.

Together with direct reputation, a *confidence factor* is estimated, which takes into considertion the number of direct transactons, the deviaton of the direct transaction evaluation values and the timestamp of the last transaction. A recommendation is the direct reputation estimated by the recommender for the trustee and is provided together with the related confidence. When a transaction takes place, the trustor evaluates the transaction and updates the *recommendation trustworthiness* of the recommending entities, based on the divergence between the transaction evaluation and the provided recommendations. Indirect reputation is estimated as a weighted average of the recommendations, where each recommendation is weighted with the related confidence value and with the recommendation trustworthiness of the recommender. The proposed reputation estimation process, comprising the involved activities and the estimation formulas, are thoroughly presented in [12].

*Evaluation***.** For the evaluation of the proposed reputation model we used the reputation systems simulator TRMSim-WSN [13]. We implemented our model in the simulator and evaluated it using four scenarios (static network, dynamic network, oscillating behavior and collusive bad-mouthing). For each scenario specific network properties and attacks with different percentages of malicious users were simulated. Our model was compared with four other reputation systems (EigenTrust [8], PeerTrust [3], PowerTrust [14] and BTRM-WSN [15]) which are reference reputation systems in the literature. The evaluation metrics that were estimated are the following: (a) *Accuracy* of

the model, i.e. the percentage of the successful selections of honest providers in the all provider selections, and (b) *Average path length*, i.e. the number of the intermediate nodes between the client and the selected service provider, as a performance indicator.

The simulation results show that the proposed system behaves efficiently in all the examined scenarios. It has a scalable performance in static networks, where the number of nodes increases and the number of malicious nodes is 70%, while in dynamic networks, where the topology of the network or the behavior of the nodes changes, the simulation of the proposed system has good results even if the percentage of malicious nodes is quite large. The good performance of the proposed reputation metric is attributed to the integrated credibility factors, namely the *recommendation reputation* of the recommenders, the *time decay function* that is used for weighting recommendations, the estimated *confidence factor* which is attributed to a recommendation and to direct reputation values and which takes into consideration the *number of transactions* and the *deviation of transaction evaluation values*, and to *weighting direct reputation more highly* than indirect reputation in the final reputation estimation. Our various experiments verify the resilience of the proposed reputation model against bad-mouthing, osclillatory behavior and traitor's attack.

CRedibility Enhanced Payments Scheme (CREPS). The proposed reputation system CREPARS involves also a payments scheme for the recommendation exchange, which gives incentives for honest recommendations. The goal of this mechanism is to provide resilience against sybil attack, repudiation, badmouthing and recommendation free-riding. Peers which participate in CREPS have *virtual accounts* and use them to make payments for acquiring recommendations. A peer A (recommendation buyer) which wants a recommendation from a peer B (recommendation seller) pays a value v for it to B. The value depends on both the recommendation reputation values that A and B have estimated for each other (RecRepA(B) and RecRepB(A)) according to the following formula:

$$v = \frac{RecRep_A(B)}{RecRep_B(A)}$$

Each entity has an *Initial Account Balance* for its participation in CREPS. After a recommendation exchange, the account balances of the participating entities are upadated (credited / debited). In order for an entity to participate in CREPS, her recommendation reputation should be higher than a minimum value which is defined according to a threshold value (t_{seller}, t_{buyer} for the recommendation seller and buyer respectively). For the management of virtual accouts we suggest the use of Special Peers (SPs) which are organized in a Distributed Hash Table, so that each SP is responisble for a number of entities. Payment analysis [14] shows that CREPS offers incentives for providing honest recommendations, since (a) the possibility of aquiring honest recommendations is linked with high recommendation reputation, and (b) the access of dishonest reccommenders to the recommendation exchange mechanism is prohibited after a number of recommendation exchanges, depending on the defined threshold values and Initial Account Balance.

CREPS involves also a recommendation exchange protocol based on a Public Key Infrastructure (PKI), which is depicted in Figure 4. According to this protocol signed messages are exchanged between (a) the recommendation buyer and seller, and (b) the participating entities and their SPs, for crediting and debiting the related accounts.

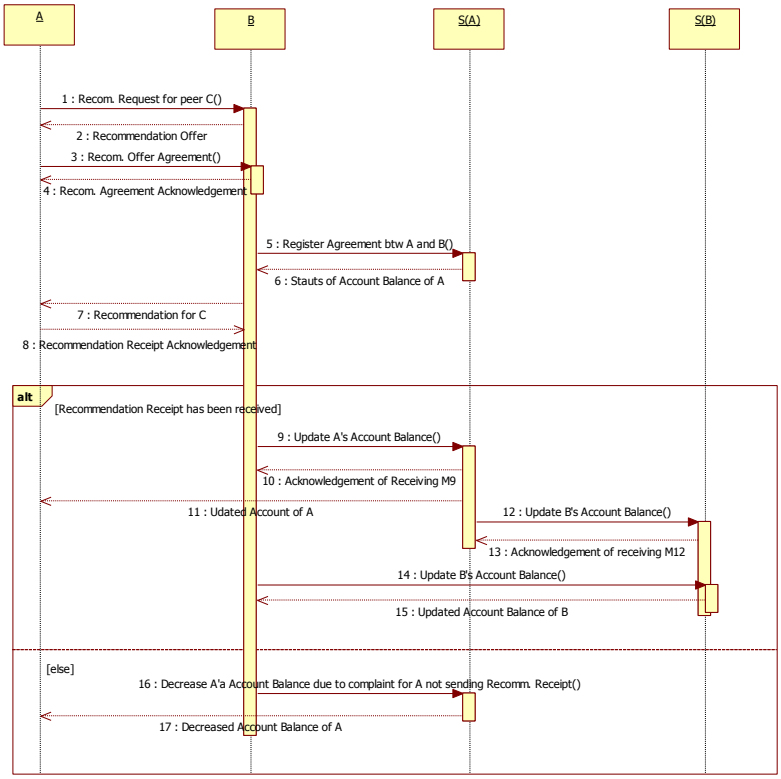

Fig. 4. Exchange of Signed messages during the Recommendation Process

For the evaluation of CREPS we have qualitatively compared it with a number of reputation systems which are based on a PKI. The analysis is based on the level that each reputation system fulfills the following requirements: (i) Privacy / confidentiality, (ii) Non-repudiation, (iii) Traceability, (iv) Ballot-staffing prevention, (v) Sybil Attack prevention, (vi) Whitewashing attack prevention, and (vii) Message integry . Our analysis shows that the various PKI-based reputation mechanisms deal with the aforementioned requirements in various levels depending on the goals and priorities set in each model. The simple PKI-based mechanims of CREPS offer message integrity via encryption, and traceability, non-repudiation and resilience to bad-mouthing via digital signatures. Entities' privacy is covered partially, as the exchanged recommendations and the updated account balances are made aware only to involved entities and to Special Peers which are responsible for them.

3 Contributions

The challenges revealed in the area of reputation systems, regarding their design, threat analysis, credibility enhancement and evaluation, have motivated this thesis, the results of which are composed of the following components:

1. A *generic framework for the development and evaluation of credible reputation systems* for distributed e-Communities, which consists of (a) a conceptual model for reputation systems design, (b) a framework for the integration of various credibility factors in reputation systems, (c) a framework that enables choosing / setting up suitable evaluation methods for specific RSs and also choosing or creating Common Evaluation Frameworks for reputation systems.
2. A *reputation system with integrated credibility factors*, which make it resilient against various attacks. Such factors include recommendation reputation, time decaying, confidence regarding provided recommendaitons and direct reputation values, and adjusting the weights of direct and indirect reputation.
3. A *novel recommendation exchange mechanism based on virtual payments*, which gives incentives for honest recommendations. This mechanism is suitable for reputation systems the efficiency of which depends on honest recommendation provision, as well as on recommendation integrity and confidentiality.

Specifically, the main contributions of the thesis are:

- Two reference models for reputation systems for distributed communities: a conceptual representation of the structure and functionality of a RS which contains the involved entities, attributes, relationships and operations (depicted in Figure 1) and a representation of the workflow of activities of the reputation estimation process in a distributed reputation system which involves a recommendation acquiring activity. The provided formalization of RSs shortens the gap in the research regarding standardization and formalization of reputation systems, which have the following characteristics: (1) reputation estimation is done locally by the trustor, based on direct experience and third-party recommendations, and (2) each peer keeps track of the recommendation reputation of other peers from which it has received recommendations. It also helps researchers in approaching reputation systems in a unified way and thus facilitates their design process.
- Four taxonomies: one for P2P reputation systems [5], one for reputation systems attacks and defence mechanisms [10], one for reputation systems for social network-based applications [7], and one for RS evaluation approaches [11]. The first two taxonomies have been used in a number of research works, appearing in the state-of-the-art of the corresponding fields, or offering a basis for new approaches of RSs and defense mechanisms, e.g. [6-21]. The third taxonomy contributes to the formalization of the more abstract reputation mechanisms which are proposed for the vast and continuously growing area of Social Network-based communities. İt also facilitates the design process of reputation systems for specific types of Social Network-based RSs, as shown in [7]. We note that such RSs are expected to have extensive application in various fields, such as in marketing and social network analysis. The fourth taxonomy enlightens RS designers as to eligible evaluation methods for their RSs.

- A framework for the credibility evaluation of RSs, consisting of a set of credibility criteria which together with the aforementioned taxonomy of attacks and defense mechanisms can be used for assessing the credibility of reputation systems and their resilience to attacks, as presented in [10].
- A thorough survey in the field of reputation systems evaluation, which provides a roadmap for objective evaluation and comparison of reputation systems through a Common Evaluation Framework [11].
- A set of credible reputation metrics for e-Communities and a novel credible recommendation exchange mechanism. The reputation metrics incorporate various credibility factors and provide resilience to attacks against reputation systems. The evaluation results show the efficiency of our reputation metrics in various scenarios and also indicate their usability in real applications. The proposed reputation metrics have been used in a number of research works, such as [22, 23]. The proposed recommendation exchange mechanism uses a credit-based scheme for payments for recommendation exchanges, which offers incentives for honest recommendations, and has been presented in [16]. It has been used as a reference incentive-based mechanism representing state-of-the-art in incentive-based reputation systems, e.g. in [24-26].

We state that our work enhances the area of RSs in various aspects, especially the aspects of design, credibility, evaluation and incentives; this belief has been supported by the adaptation of parts of our work by other research works, as aforementioned. Our future work plans include expanding our work in the fields of credit-based, social network-based and e-Commerce supporting RSs, and further work on benchmarking of reputation systems, i.e. on defining and implementing a CEF which will be grounded on or extend current CEF approaches and will incorporate the desirable characteristics identified in this thesis. Subsequently, we plan to use such a CEF for thoroughly experimenting with the evaluation of the reputation metrics we have developed [16] and other reputation systems in various application environments, contributing thus to the design of optimal RSs for specific e-Community contexts.

References

1. eBay, http://www.ebay.com. Accessed on 1/8/2016
2. Song, S., Hwang, K., Zhou, R.: Trusted P2P Transactions with Fuzzy Reputation Aggregation. IEEE Internet Computing, Special Issue on Security for P2P and Ad Hoc Networks,. 9, 6, 24-34 (2005)
3. Xiong, L., Liu, L.: PeerTrust: Supporting reputation-based trust for peer-to-peer electronic communities. IEEE Transactions on Knowledge and Data Engineering, 16, 7, 843–857 (2004)
4. Dillon, T. S., Chang, E., Hussain, F.K.: Managing the Dynamic Nature of Trust. IEEE Journal Of Intelligent Systems, 19, 5, 79-82 (2004)
5. Koutrouli, E., Tsalgatidou, A.: Reputation-based Trust Systems for P2P Applications: Design Issues and Comparison Framework. In: 3rd Intl. Conf. on Trust, Privacy and Security in Digital Business, pp. 152-161, Springer-Verlag, Berlin, Heidelberg (2006)
6. Hussain, O. K., Chang, E., Hussain, F. K., Dillon, T. S.: A methodology to quantify failure for risk-based decision support system in digital business ecosystems. Data Knowl. Eng. 63, 3, 597-621 (2007) DOI=http://dx.doi.org/10.1016/j.datak.2007.03.014
7. Koutrouli, E., Kanellopoulos, G., Tsalgatidou, A.: Reputation Mechanisms in on-line Social

Networks – The case of an Influence Estimation System in Twitter. Accepted for publication in South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conf. (SEEDA-CECNSM 2016), ACM (2016)
8. Kamvar, S., Schlosser, M., Garcia-Molina, H.: The EigenTrust Algorithm for Reputation Management in P2P Networks. In: World Wide Web Conf. 2003, pp. 640-651. ACM (2003)
9. Stoica, I., Morris, R., Liben-Nowell, D., Karger, D. R., Kaashoek, M. F., Dabek, F., Balakrishnan, H.: Chord: a Scalable Peer-to-Peer Lookup Protocol for Internet Applications, IEEE/ACM Transactions on Networking, 11, 1, 17-32 (2003)
10. Koutrouli E., Tsalgatidou, A.: Taxonomy of Attacks and Defense Mechanisms in P2P Reputation Systems—Lessons for Reputation System Designers. Computer Science Review, 6, 2-3, 47-70 (2012)
11. Koutrouli E., Tsalgatidou, A.: Reputation Systems Evaluation Survey. ACM Computing Surveys, 48, 3, 1-28 (2015)
12. Koutrouli, E., Tsalgatidou, A.: Credibility Enhanced Reputation Mechanism for Distributed e-Communities. In: 19th Euromicro Intl. Conf. on Parallel, Distributed and Network-Based Computing (PDP 2011), pp. 627-634. IEEE Computer Society, Washington, DC, USA (2011)
13. Mármol, F. G., Pérez, G. M.: TRMSim-WSN, Trust and Reputation Models Simulator for Wireless Sensor Networks. In: IEEE Intl. Conf. on Communications (IEEE ICC 2009), pp. 915-919. IEEE Press, Piscataway, NJ, USA (2009)
14. Zhou, R., Hwang, K.: Powertrust: A Robust and Scalable Reputation System for Trusted Peer-to-Peer Computing. IEEE Transactions on Parallel and Distributed Systems, 18, 4, 460-473 (2007)
15. Mármol, F. G. and Pérez, G. M.: Providing Trust in Wireless Sensor Networks Using a Bio-Inspired Technique. Telecommunication Systems, 46, 2, 163-180 (2011)
16. Koutrouli, E., Tsalgatidou, A.: Credible Recommendation Exchange Mechanism for P2P Reputation Systems. In: Trust, Reputation, Evidence and other Collaboration Know-how (TRECK) Track, ACM Symposium on Applied Computing 2013, pp. 1943-1948. ACM (2013)
17. Li, X., Gui, X.: Research on Dynamic Trust Model for Large Scale Distributed Environment. Journal of Software, 18, 4, 460-473 (2007)
18. Clarke, S., Christianson, B., Xiao, H.: Extending Trust in Peer-to-Peer Networks. In: 13th East European conference on Advances in Databases and Information Systems (ADBIS'09), pp. 145-152, Springer-Verlag, Berlin, (2009)
19. Hendrikx, F., Bubendorfer, K., Chard, R.: Reputation Systems: A Survey and Taxonomy. Journal of Parallel and Distributed Computing, 75, 184-197 (2015)
20. Vavilis, S., Petkovic, M., Zannone, N.: A reference model for reputation systems. Decision Support Systems, 61, 147-154 (2014)
21. Sänger, J., Richthammer, C, Rösch A., Pernul, G.: Reusable Defense Components for Online Reputation Systems. In: 9th IFIP WG 11.11 Intl. Conf. (IFIPTM 2015), Hamburg, Germany, pp. 195-202, Springer, Berlin (2015)
22. Vallée, T., Bonnet, G.: Using KL Divergence for Credibility Assessment, In: 2015 Intl. Conf. on Autonomous Agents and Multiagent Systems (AAMAS '15), pp. 1797-1798, Intl. Foundation for Autonomous Agents and Multiagent Systems, Richland, SC (2015)
23. Dadhich, P., Dutta, K., Govil, M. C: Detection of Slanders through Euclidean Distance Similarity Assessment for Securing e-Commerce Agents in P2P Decentralised Electronic Communities. Intl. Journal of Security and Networks, 11, 1/2, 48-65 (2016)
24. Lafuente, C. B., Seigneur, J. M.: Extending Trust Management with Cooperation Incentives: A Fully Decentralized Framework for User-Centric Network Environments. Journal of Trust Management, 2, 7, Springer (2015)
25. Seddiki, M., Benchaïba, M.: Gpop: A Global File Popularity Measurement for Unstructured P2P Networks. Int. J. Distrib. Syst. Technol. 6, 3, 51-64 (2015)
26. Haddi F. L., Benchaïba, M.: A survey of Incentive Mechanisms in Static and Mobile P2P Systems. Journal of Network and Computer Applications, 58, C, 108-118 (2015)