

# Reputation-based Trust Systems for P2P Applications: Design Issues and Comparison Framework

Eleni Koutrouli<sup>1</sup>, Aphrodite Tsalgaidou

Department of Informatics & Telecommunications, National & Kapodistrian University of  
Athens, Greece  
[\[ekou.atsalga\]@di.uoa.gr](mailto:ekou.atsalga@di.uoa.gr)

**Abstract.** In Peer-to-Peer (P2P) computing area trust issues have gained focus as a result of the decentralized nature of P2P systems where autonomous peers interact with each other without relying on any central authority. There is, thus, the need of a trust system to ensure a level of robustness against malicious nodes. Various reputation-based trust models have been proposed for P2P systems which use similar concepts but focus on different aspects and address different set of design issues. As a result, there is a clear need to investigate the design aspects of reputation-based trust systems that could be deployed in P2P applications. In this paper we present the basic elements and design issues of such systems and compare representative approaches, aiming at supporting the design of reputation systems suitable for particular P2P applications.

## 1 Introduction

Peer-to-Peer (P2P) systems are decentralized applications where heterogeneous peers, which are autonomous and have intermittent presence in the network and a high level of anonymity interoperate for purposes such as file sharing, distributed computing and eCommerce transactions without the need of a centralized server. The decentralized nature of P2P systems poses the need for enhanced trust between peers that will enable the reliable communication and exchange of services between them.

Peers in P2P systems need to make trust decisions for choosing peers they will transact with or resources they have asked for among the offered ones. There is, thus, the need of at least a minimal trust system to ensure a satisfying level of robustness against various kinds of attacks that have been monitored in P2P systems [8]. Such a trust system should be decentralized so that each peer can make autonomous trust decisions based on other peers' reputation. By "peer reputation" we refer to a measure that indicates the trustworthiness of a peer in a particular context. This measure is estimated based on both direct experiences and other peers' transaction information.

Reputation-based trust models for P2P systems have recently gained a lot of attention by the research community in the areas of trust and P2P systems. Several

---

<sup>1</sup> Eleni Koutrouli is also with the Bank of Greece, Panepistimiou 21, Athens, Greece, email: ekoutrouli@bankofgreece.gr

trust models are found in the literature that use similar concepts (like reputation, trustworthiness, recommendation, etc.) but focus on different aspects (like social or probabilistic modeling of behavior, trust data management, etc.). In most cases, these models, although having been simulated and tested, have not been deployed in real P2P applications and, thus, they usually do not fully address all the design aspects that should be taken into account for the design of an effective reputation system that could be deployed in a real P2P application. They also differentiate regarding their approach to the various design issues (such as the kind of input information, the methods of reputation estimation, the reputation representation, etc.).

As a result, no general model for P2P reputation systems exists and the choice of a reputation model for a particular P2P application is challenging. Furthermore, the designer of a decentralized reputation-based trust system needs to take the necessary design issues into consideration and make critical decisions about them.

In this paper we present the concepts which are central to any *reputation-based trust model* for P2P applications and a conceptual representation of such a model. We also present the components and design considerations of a *reputation-based trust system* that could be deployed in a P2P application to provide reputation-based trust functionality. Furthermore, we provide a comparison framework for P2P reputation systems and compare existing approaches. Our objectives are to

- identify the elements of reputation-based trust models for P2P systems and present the major considerations for reputation-based trust systems design
- enable the right choice of either a reputation system or specific elements of a reputation system for particular P2P applications through our comparison.

The rest of the paper is organized as follows: in section 2 we discuss the concept of trust and its applicability in P2P systems and present a conceptual representation of a P2P reputation-based trust model. In section 3 we discuss the components and design considerations of a reputation system, as well as our classification framework, based on these considerations. In section 4, we present representative P2P reputation systems for various application areas and use our framework to compare them according to the presented issues. Discussion and conclusions follow in section 5.

## 2 Trust, Reputation and P2P Systems

Trust in computer science is a concept that has been borrowed from the human society, where people constantly apply it in their interactions. In the World Wide Web, where interactions in widely-distributed, open, decentralized systems that span multiple administrative domains are enabled, the need for establishing trust between interacting entities is posed. As a result, recent research focuses on trust management as a framework for decentralized security decisions in such systems.

Trust is a complex, multifaceted, and context-dependent notion, which is representatively defined in Sloman [15] as “the quantified belief by a trustor with respect to the competence, honesty, security, and dependability of a trustee within a specific context”. In P2P systems, peers which do not know each other need to exchange services and resources without central control. There is, thus, the need for a decentralized trust system that will support peers to identify reliable peers [1][13][14],

reliable resources [14], or malicious peers [11]. Various trust systems for P2P applications have been proposed that can be classified in the following categories:

- **Policy-based trust systems**, where peers use credential verification to enable access control to restricted resources [12]
- **Reputation-based trust systems**, which use information considering previous interactions with an entity to establish a reputation measure that will support a trust decision [1][5][11][14][16][18][19]. In our paper we examine this category of trust systems, due to their wide applicability in P2P systems.

## 2.1 Conceptual Representation of P2P Reputation-based Trust Systems

The basic elements of a reputation-based trust model are the following:

1. **Trustee**: the entity that is given a reputation value for a service it provides, e.g. the output of a transaction, or an attribute it possesses, e.g. the genuity of a file.
2. **Trustor**: the peer that needs to evaluate the trustee's reputation in order to make a trust decision about it, such as to decide whether to perform a transaction with it.
3. **Third Party or Witness**: a peer that provides a recommendation for the trustee based on its own experiences with the latter.
4. **Context**: The reputation of a peer depends on the specific context in which it applies, like a specific service the trustee provides, attributes of such a service, etc.
5. **Recommendation**: refers to the feedback provided by peers about another peer's trustworthiness. In the following we will alternatively use the terms *recommendation*, *trust information*, or *feedback* to refer to this kind of information.
6. **Trustworthiness or reputation**: an indicator of the quality of the trustee's services or attributes, based on recommendations, as well as the specific context and time.

Figure 1 provides a graphical representation of the elements of a reputation-based trust model, based on the conceptual models presented in [4].

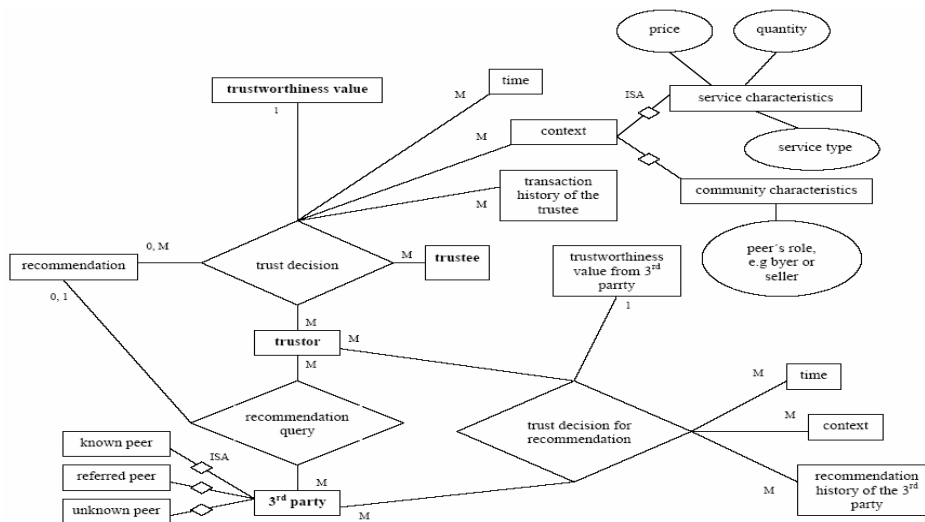


Fig. 1. Conceptual model of a reputation-based trust system

### 3 Design of P2P Reputation Systems & Comparison Framework

In general, a reputation-based trust system assists peers in choosing a reliable peer to transact with. To provide this function, a P2P reputation system:

- collects information on the transactional behavior of each peer. Transacting entities produce ratings about each other's performance, which are often locally aggregated to form an entity's opinion about others. Individual ratings or opinions constitute recommendations, which are distributed in the P2P network. Each peer can store such information and can provide it on request or by propagating it in the network.
- aggregates the trust information that concerns the transactional behavior of the trustee and produces a trustworthiness (or reputation) value for it. As it is often impossible or too costly to obtain ratings or opinions resulting from all interactions with a given peer, a reputation score is based on a subset of ratings.
- ranks peers according to their trustworthiness or compares a peer's trustworthiness with a threshold in order to allow the trustor to choose a peer to transact with and the system to take action against malicious peers while rewarding contributors.

The functionality of reputation system can, thus, be broken down into the components illustrated in Figure 2. When designing each component, various design issues should be taken into consideration, which we present in the following. These design issues constitute our *comparison framework*, which has been used for evaluating a number of P2P reputation systems that are presented in Section 4. The result of this comparison is illustrated in Table 1.

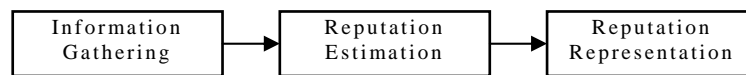


Fig. 2. Components of a P2P reputation-based trust system

#### 3.1 Design Considerations for Information Gathering

1. **Trust information storage, dissemination and search mechanisms:** An important issue in a decentralized trust system is data management, which refers to which trust information is used, where it is stored and how it is propagated and acquired. Some P2P reputation systems [1] use the underlying P2P structure to store and retrieve trust information. In others [14][19] each peer keeps information regarding both its own transactions and a set of neighbors, which it can ask for recommendations. Broadcasting, flooding and probabilistic flooding methods can be used to send queries for recommendations or disseminate own experiences.
2. **Local control over trust information stored locally on a peer.** Whether peers have or do not have local control over the trust information that is stored locally on them, has impact on the reliability of the reputation system, as a malicious peer with local control could change the information stored locally on it.
3. **Credibility of the recommender:** As peers may provide inaccurate recommendations, the recommender's credibility should be taken into account.

Some systems suggest maintaining separate ratings on a peer's likelihood to defect on a transaction and its likelihood to recommend malicious peers. Some others use the trustworthiness value of a peer with respect of the services it provides as a filter for the recommendations it makes, assuming that a peer, which provides trusted services will also provide honest recommendations.

4. **Type of behavior taken into account:** Reputation evaluation can be based only on positive behavior (e.g. contribution rate in a file sharing system), or only on negative behavior (e.g. cheating in a transaction), or both on positive and negative behavior of the trustee. In the last case negative behavior should normally be taken into account with a higher weight, as it has a greater impact on the trustworthiness of a peer than its positive behavior.
5. **Context dependency:** Reputation estimation and trust decisions depend on the particular context of a transaction. This context can constitute of transaction related factors, such as quantity and price of a transaction in the case of e-commerce applications or can refer to the type of the transaction, such as service provision or recommendation provision. Some trust systems (e.g. [13][18]) take context into account explicitly or implicitly while some others (e.g. [14]) ignore context, assuming that it is the same for all transactions.

### 3.2 Design Considerations for Reputation Estimation

1. **Initialization of trust information:** Assigning an initial value to a peer, when no information about its transactions exists, is challenging, as it is important to distinguish between a new peer and a peer with poor long term performance and also prevent peers with poor trustworthiness to enter into the system with a new identity in order to gain higher trustworthiness. The choice of an initial trust value depends on the strategy followed: it can represent complete distrust, complete trust, neutral trust, or default values depended on the role of the peer in a community.
2. **Scope of trust information (global vs. localized information):** some reputation systems ([1][18]) assume that every peer has the same access to existing trust information and, thus, when different peers evaluate the trustworthiness of another peer their evaluation will be the same. In these systems, trust has a global scope and can be said to be objective. In other systems ([13][19]), trust evaluation is a localized process, based on direct information and on information coming from a set of trustor's neighbors. In localized trust systems trustworthiness is subjective.
3. **Trustworthiness estimation method:** Feedback regarding past interactions with the trustee is aggregated to produce the trustee's trustworthiness value. Various aggregation methods have been proposed such as simple statistic functions (e.g. average), probabilistic methods, fuzzy logic, etc.
4. **Transitivity extent:** Trust transitivity is implicitly taken into account in reputation-based trust systems, as they assume that if A trusts B and B trusts C and B recommends C to A then A can estimate a trustworthiness metric for C based on B's recommendation and A's trust in B. Transitivity is assumed either through a recommendation chain (multiple levels of trust indirection) or only through one level of trust indirection.

5. **Recency dependency:** While estimating reputation more recent transaction behavior should have a greater impact on a peer's score than older transactions, e.g. weights or aging factors can be used to give more importance to recent experience.

### 3.3 Design Considerations for Trustworthiness Representation

1. **Range of trustworthiness values:** Trustworthiness values can be discrete or continuous and can have a varying range reflecting different trust semantics. Examples of such domains are the interval  $[0,1]$  (e.g. when a value represents a probability) and the set  $\{0,1\}$  where 0 represents distrust and 1. Another example is the use of a specific interval which is divided in smaller intervals to represent different levels of trust [7].
2. **Rank or threshold based:** Trust decisions in reputation systems are usually taken either after comparing a peer's trustworthiness with a threshold (threshold-based systems) or after comparing the trustworthiness of different peers (rank-based systems). When a threshold is used, its selection depends on the semantics of trustworthiness values and the requirements of the specific implementation.
3. **Distrust representation:** Representation of distrust can isolate malicious peers. In some trust systems distrust is explicitly represented, either as a specific range of reputation values or by keeping different ratings of trust and distrust.

## 4 Comparison of P2P Reputation Systems

We have used the comparison framework described in Section 3 to examine and compare a number of reputation systems, with respect to the way they address the identified issues and, thus, identify existing approaches, deficiencies and possible design choices. Most existing P2P reputation systems have been developed for general-purpose P2P applications, such as file sharing. However, reputation systems have been proposed for other classes of P2P systems too, such as cooperative and P2P e-commerce applications. We have selected systems which we believe that are representative works on reputation in the aforementioned P2P application areas, although further approaches exist (e.g.[10]), which are not presented here due to space limits. Finally, we present our observations in Table 1, which illustrates both our framework and the choices of the various reputation-based trust systems regarding the identified design considerations.

In the following, we briefly describe the selected reputation-based trust systems:

- **Regret [13]:** Regret is a reputation system, designed for multiagent marketplaces, which is based on the social relations between peers. It concerns three different dimensions of reputation: *individual dimension* considers only the direct interactions between peers, *social dimension* considers information about the trustee coming from other peers and from the social relations between peers, and *ontological (or context dependent) dimension* refers to combining reputations on different aspects. Various kinds of reputation along with their reliability measures are estimated and then combined to form the final reputation of a peer.

- **A Social Mechanism for Reputation [19]:** in this system peers can have two kinds of reputations: for providing services and for providing recommendations. Peer A assigns a rating to B based on its direct experience with B as well as recommendations, and A's ratings to recommenders. A peer receiving a query decides whether it has the expertise to answer or not and forwards the query to a set of neighbouring peers. A response can contain an answer, or a recommendation, or both, or neither and can be used to evaluate the expertise of the responding peer and of its recommenders.
- **Managing the Dynamic Nature of Trust [7]:** in this system when a peer wants to make a trust decision about another peer within the current time slot, it uses its local rating if it has interacted with the trustee in the same time slot. Otherwise, it asks for reputation information and estimates the trustee's trustworthiness as an average of the received reputation values, weighted with the witnesses' trustworthiness. The trustworthiness of a peer for a future time slot can also be estimated probabilistically. After an interaction the trustor modifies both the trustworthiness values of the trustee and those of the witnesses.
- **PeerTrust [18]:** PeerTrust is designed for P2P eCommerce communities. It takes into account the feedback in terms of the amount of satisfaction a peer obtains through transactions, the number of the trustee's transactions, the credibility of the feedback, the transaction context factor, addressing transaction characteristics, and the community context factor, referring to community characteristics (such as the availability of pre-trusted peers). Each peer stores a small portion of the trust data using the P-Grid structure [2]. A peer collects the necessary trust data and evaluates the trustworthiness of another peer on the fly when needed.
- **FuzzyTrust [16]:** a fuzzy logic reputation system for P2P eCommerce applications. Peers perform fuzzy inference on local parameters to generate local scores for the peers with whom they have transacted. These local scores are collected from qualified peers, which meet an aggregation threshold and aggregated into global reputation values. The FuzzyTrust system uses a DHT-based P2P overlay network for the global reputation aggregation.
- **Managing Trust [1]:** this system is based on binary trust. If a peer cheats in a transaction, it becomes untrustworthy and a complaint is formed against it and stored and replicated in a P-Grid data structure [2]. When a peer wants to calculate the trustworthiness of another peer, it searches for complaints that this peer has both received and filed. Trustworthiness of a peer is then evaluated based on the global knowledge on these complaints.
- **Maximum Likelihood Estimation based trust system (MLE) [5]:** The proposed system uses a structured P2P overlay for the storage and retrieval of trust information, which consists of reports on a peer's performance. These reports are either 0 if the peer acted dishonestly or 1 if the peer acted honestly. The reputation of a peer is its probability to perform honestly in its transactions with others. This is estimated based on a probabilistic method, taking into account the probability of a peer to lie when it reports on another's peer's performance.
- **A Reputation-based Trust Management System for P2P systems [14]:** in this system, which is designed for P2P file sharing, every peer can estimate trust and distrust ratings for other peers, based on binary trust vectors. A peer receiving responses for a resource query organizes them into groups according to their file

hash value. A trust score for each file version is calculated as the average of the trust ratings of the offering peers. If there is not enough local information about a peer, trust queries are issued about it. Credibility ratings of the responses are used as weights for the trust rating estimation of the recommended peer. The file version with the highest trustworthiness is downloaded from one of the peers who offer it.

- **NICE [11]:** NICE is designed for Internet cooperative applications. After a transaction, each transacting peer signs its opinion regarding the quality of the transaction. If this signed opinion (cookie) is positive it is stored in the other transacting peer, otherwise, it is stored in the peer signing it. When a peer A wants to access B's resources, it has to prove its trustworthiness to B and, thus, sends B cookies signed by B. If A does not have such cookies, it may collect chains of cookies from B to A and present them to A.

Table 1 contains a comparison of the aforementioned reputation systems against the design considerations issues identified in section 3. When no information is given in the description of a system regarding one of these issues, the respective cell of the table has been filled with "N/A", whereas in some cells additional explanative information is provided. This table can also be viewed as a multifaceted classification of reputation systems as well as a supporting tool for the designing procedure.

## 5 Discussion

Reputation plays a vital role in the process of establishing trust between communicating peers in a P2P system. Motivated by the lack of a complete design framework for reputation systems for P2P applications, we have presented the elements of reputation-based trust systems and the basic issues that need to be taken into account in the design of reputation systems that can be used in P2P applications. We have also examined some representative approaches for three P2P application areas and have compared them against the way they deal with these issues.

The designer of a reputation-based trust system for P2P systems should consider the presented design issues and make careful decisions about them in order to develop an effective solution for reputation functionality in such systems. Our presented comparison aims at supporting the right choices regarding these issues when designing a reputation system for a particular P2P application.

However, there are further issues regarding the design of a reputation-based trust system for P2P applications that need to be addressed, such as handling of anonymity, supporting fault tolerance and scalability and various types of misbehavior and attacks that can affect a reputation system's reliability. We are aiming at examining these issues in future work in order to provide a more comprehensive framework for the design of effective reputation systems for P2P applications.

## Acknowledgements

This work has been partially funded by the European Commission under contract 04559 SODIUM and by ELKE under contract 70/4/5829.

**Table 1. Comparison of reputation-based trust systems for P2P systems**

Design Issues		P2P Ecommerce applications				File Sharing			Cooperation		
		Regret	Social mechanism for reputation	Managing the dynamic nature of trust	PeerTrust	FuzzyTrust	Managing Trust	Maximum Likelihood Estimation	Reputation-based trust management	NICE	
Information Gathering	Storage of trust information	each peer stores information about the social relationships in its environment and also about its transactions	each peer stores an interest vector, an expertise vector and information about its neighbours' expertise and reputation	each peer stores trustworthiness ratings for the peers with whom it has interacted and witness trustworthiness ratings	each peer stores a small portion of the trust data (transaction history and feedbacks) using the P-Grid Structure	each peer maintains transaction records and remote peers' evaluated trust scores, DHT-based overlay	P-Grid Structure	structured P2P network based	each peer stores a trust vector for each peer it has dealt with at the past	each peer stores positive reputation information concerning itself or negative reputation information concerning other peers	
	Feedback dissemination and search mechanisms	fuzzy logic based mechanisms for witnesses identifying	<ul style="list-style-type: none"> <li>recommendations are answers to queries for services</li> <li>negative ratings are propagated without explicit query</li> </ul>	N/A	P-Grid based	DHT-based overlay network	P-Grid based	structured P2P network based	first generation P2P systems based, e.g. Gnutella	probabilistic flooding-based search	
	Local control	yes	yes	yes	no	yes	no	no	yes	yes	
	Recommender's credibility	yes, based on <ul style="list-style-type: none"> <li>social relationships of witness and trustee and</li> <li>witness's trustworthiness regarding its services</li> </ul>	yes (a witness's recommendation is taken into account if the witness's trust rating is above a threshold)	yes (a witness trustworthiness is estimated based on its recommendation and the result of an interaction)	yes (as a function of the witness's trustworthiness or using a personalized similarity measure)	yes (trust score of a peer is taken into account as a weight for global reputation estimation)	indirectly (it is very likely that a peer providing a lot of complaints about others lies)	yes (possibility of a peer to lie when providing a recommendation)	yes (different trust and credibility scores)	no	can be incorporated
	Positive/negative behavior	positive and negative	positive and negative	positive and negative	positive and negative	positive and negative	negative	positive and negative	positive and negative	positive and negative	
	Context dependence	yes	no	yes	yes (transaction context and community context)	yes (local transaction parameters)	no (could be integrated)	N/A	no	no	
Method of Feedback Aggregation	Initialization of trust information:	default value based on peer's role	initial trust rating = 0	initial trust rating = 0	default value = 1	N/A	at the beginning every peer is trusted	N/A	N/A	depends on the chosen algorithm	
	Method of feedback aggregation	statistic	Statistic	statistic & probabilistic (Markof matrix)	statistic	statistic, fuzzy logic for the estimation of weights	probabilistic	probabilistic	statistic	statistic	
	Transitivity level of trust indirection	one level of indirection	recommendation chain	one level of indirection	one level of indirection	one level of indirection	one level of indirection	one level of indirection	one level of indirection	recommendation chain	
	Recency dependence	yes, a time function is used as a weight	yes (each time trust rating is updated based on the previous rating)	yes (weights give more importance to recent experiences)	yes (can be incorporated in the context)	yes (transaction date is taken into account. Recent transactions lead to higher weights)	no	N/A	yes	no	can be incorporated
	Scope of trust: global vs localized	localized	localized	localized	global	localized	global	global	localized	localized	
Output	Threshold/Rank	threshold	threshold	threshold (=5)	threshold	N/A	rank	threshold	rank	threshold	
	Range of trust values	[-1,1]	[-1,+1]	[0,6]	[0,1]	N/A	no specific range, the higher price means less trust	[0,1]	trust ratings and credibility ratings: [0,1]	depends on the chosen scheme	
	Distrust Representation	N/A	yes, if a peer's trust rating is below a threshold it will not be trusted	yes (a specific range)	No	N/A	yes	N/A	yes (distrust ratings)	no	can be incorporated

## References

- [1] Aberer, K., Despotovic, Z., Managing trust in a peer-2-peer information system, 10th Intl Conference on Information and Knowledge Management (CIKM), Atlanta, 2001
- [2] Aberer, K., P-Grid: A self-organizing access structure for P2P information systems, 6th Intl Conference on Cooperative Information Systems (CoopIS), 2001
- [3] Chang, E., Dillon, T., Hussain, F. K., Trust and Reputation Relationships in Service-Oriented Environments, 3rd Intl Conference on Information Technology and Applications
- [4] Chang, E., Hussain, F. K., Trust and Reputation Relationships in Service-Oriented Environments, Keynote, ICITA 2005
- [5] Despotovic, Z., Aberer, K., Maximum Likelihood Estimation of Peers' Performance in P2P Networks, 2nd Workshop on the Economics of Peer-to-Peer Systems, 2004
- [6] Despotovic, Z., Aberer, K., Possibilities for Managing Trust in P2P Networks, Technical Reports in Computer and Communication Sciences (EPFL Technical Report IC/2004/84), November 2004
- [7] Dillon, T.S., Chang, E., Hussain, F.K., Managing the dynamic nature of trust, IEEE Transaction of Intelligent Systems, vol. 19, no. 5, pp. 79-82, Sept/Oct 2004
- [8] Jøsang, A., Ismail, R., Boyd, C., A Survey of Trust and Reputation Systems for Online Service Provision (to appear), Decision Support Systems, 2005
- [9] Jurca, R., Faltings, B., An Incentive Compatible Reputation Mechanism, IEEE Conference on E-Commerce, Newport Beach, CA, USA, 2003
- [10] Kamvar, S., Schlosser, M., Garcia-Molina, H., The EigenTrust Algorithm For Reputation Management in P2P Networks, 12th Intl World Wide Web Conference, 2003
- [11] Lee, S., Sherwood, R., Bhattacharjee, B., Cooperative Peer Groups in NICE, 22<sup>nd</sup> Conference of the IEEE Computer and Communications Societies (INFOCOM), 2003
- [12] Li, N., Mitchell, J., RT: A Role-based Trust-management Framework, 3<sup>rd</sup> DARPA Information Survivability Conference and Exposition (DISCEX), Washington, 2003
- [13] Sabater, J., Sierra, C., Reputation and social network analysis in multi-agent systems, 1st Intl Joint Conference on Autonomous Agents and MultiAgent Systems, Bologna, 2002
- [14] Selcuk, E. Uzun, and M. R. Pariente, A Reputation-Based Trust Management System for P2P Networks, 4th Intl Workshop on Global and Peer-to-Peer Computing (GP2PC), 2004
- [15] Sloman, M., Trust-management in Internet and pervasive systems, IEEE Intelligent Systems, vol. 19, no. 5, pp. 77-79, Sept/Oct 2004
- [16] Song, S., Hwang, K., Zhou, R., Kwok, Y. K., Trusted P2P Transactions with Fuzzy Reputation Aggregation, IEEE Internet Computing Magazine, Special Issue on Security for P2P and Ad Hoc Networks, Nov/Dec 2005
- [17] Suryanarayana, G., Taylor, R., A Survey of Trust Management and Resource Discovery Technologies in Peer-to-Peer Applications, ISR Technical Report # UCI-ISR-04-6, 2004
- [18] Xiong, L., Liu, L., A Reputation-Based Trust Model for Peer-to-Peer eCommerce Communities, IEEE International Conference on E-Commerce (CEC), 2003
- [19] Yu, B., Singh, M. P., A social mechanism of reputation management in electronic communities, 4<sup>th</sup> Intl Workshop on Cooperative Information Agents, 2000