ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

Trust Metrics Evaluation for Peer-to-Peer Systems

[I]S.Nithya, [II]Dr. Kannan Balasubramanian
[I]PG Scholar, Dept. of CSE, Mepco Schlenk Engineering College, Sivakasi, Tamilnadu, India
[II]Professor, Dept. of CSE, Mepco Schlenk Engineering College, Sivakasi, Tamilnadu, India

Abstract
In this paper we propose various trust metrics for the evaluation of trustworthiness among the peers in a Peer-to-Peer (P2P) system. In a P2P system two major problems exists: openness and search for service providers. As any peer can join the network at any point of time, they may be malicious and serves the other peers with the resources they possess and affects them. Moreover currently there is no efficient search mechanism in a P2P system to select a best service provider. By evaluating the trust metrics based on the interaction that happens between the peers, a trust relationship is constructed. This trust is measured in two ways: 1) Based on the service provided by a particular peer; 2) Based on the recommendation collected from a peer about another peer. The results of trust metrics evaluation are analyzed, thereby malicious peers are separated from the network and good peers were able to communicate securely. The peers can also select best service providers among multiple peers based on the trust metric values.

Keywords
Peer-to-Peer systems, trust metrics, security, service, reputation

I. Introduction

P2P system is a self-organizing system of equal, autonomous peers which aims for the shared usage of distributed resources in a networked environment avoiding central services. P2P system depends on the collaboration of peers to complete a task.

In order to establish trustworthiness among the peers in the system, various trust metrics are evaluated. Based on the metric values the peers are categorized as either trustworthy or untrustworthy. The general structure of P2P system is depicted in the Fig 1.

The metrics are evaluated in two contexts: based on the interaction that happens between the peers and based on the feedback that is collected from the peers with whom the interaction happened. In client server architecture the trust information's collected from various peers are stored and managed securely whereas in P2P systems the peers collaborate among themselves and store the trust information [8], [4].

In P2P systems any peer may request for a service from its neighbouring peers in the network, but the service provider may either be malicious or may act as good peer in providing the service. Sometimes the malicious peer may serve as an individual attacker, which exhibits various behaviours like: naive, discriminatory, hypocritical and oscillatory [12].

The naive peers always upload the infected file for its service requestor, whereas a discriminatory peer selects a group of victims and uploads the infected file only for those peers. A hypocritical and oscillatory peer behaves alike, because for a certain period of time they may be malicious and for the rest of the time they behave as good peers.

In this paper we propose a trust model that reduces the maliciousness in the P2P system. By evaluating various trust metric values the peers in the system can be ranked accordingly, based on which the peers for future interaction are chosen. The peer tries to collect only the local trust information from its neighbouring peers, by which the trust model is developed within its proximity or area.

Initially the peers in the system are strangers to each other, but once the service (either uploading or downloading) [13] has been provided they become acquaintance. The interaction and recommendation are measured based on three parameters: satisfaction, importance and fading effect. Satisfaction measures how much the interaction fulfilled the needs of the service requestor. Importance is measured based on the weight age given to the interaction. If any new interaction happens between the peers the old interaction loses its importance, this issue is addressed by the fading effect parameter.

The trust model defines three important metrics: service, recommendation and reputation. Service trust metric is essential when evaluating the trustworthiness of the acquaintance. The Service trust metric value is essential while selecting the best service provider for interaction process.

Recommendation and reputation are needed while measuring the trustworthiness of the stranger. Recommendation trust metric is measured as a result of collecting recommendation from various acquaintance peers

Reputation metric is needed mainly in the initial stage of interaction as the stranger's probability will be high; while the experience with the acquaintance peer increases automatically the reputation loses its importance [1] [5].

The remainder of this paper is organized as follows: Section 2 discusses the related research. Section 3 explains the peer-to-peer file sharing process. Section 4 presents the analysis of the results. Section 5 summarizes the results and future work.

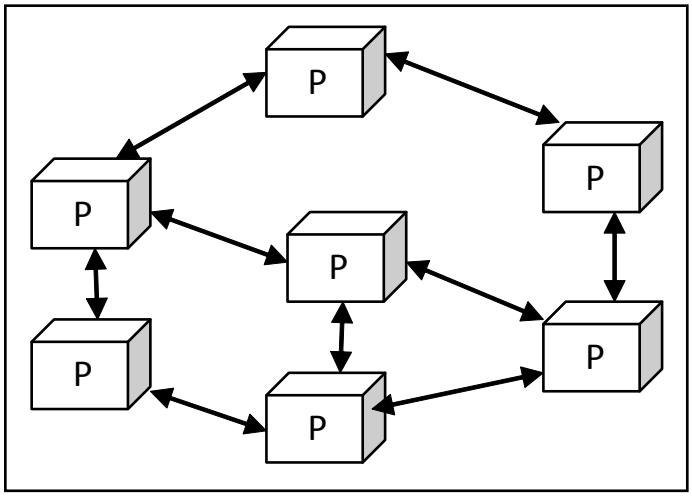

Fig. 1: General structure of a Peer-to-Peer System

The interaction of P_m with its acquaintance (P_q) and stranger (P_n) in collecting recommendation and service is depicted in Fig. 2

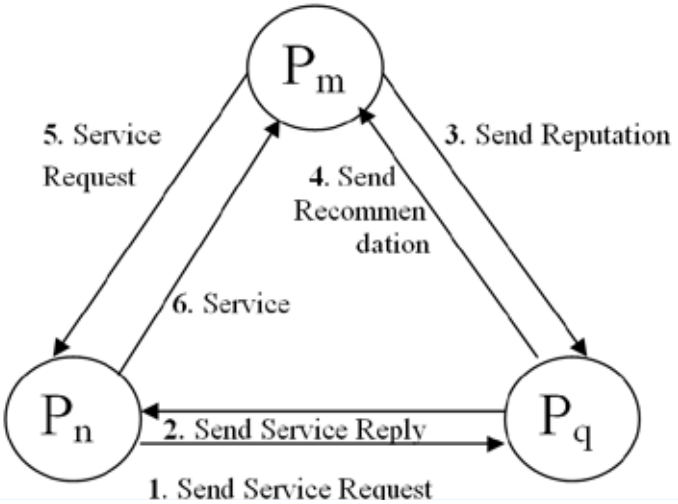

Fig. 2: Interaction between the peers

1. Related Work

Aberer and Despotovic [4] presented a method called P-Grid in order to store the data in P2P system in a decentralized and scalable fashion. Because central server can securly store the trust information and defines trust metrics. Since there is no central server in most P2P systems, peers organize themselves to store the trust information about each other. It provides solution not only for managing the trust information but also provided with an full fledged P2P architechture for information systems. But the disadvantage with this is that the mechanisms which that have been proposed is not incorporated in a practical P2P application and tested.

F.Cornelli et al. [8] proposed an approach to P2P security where servents can keep track , and share with others , information about the reputation of their peers. Reputation sharing is based on the distributed polling algorithm by which resource requestors can assess the reliability of perspective providers before initiating the download. The approach complements the existing P2P protocols and it also keeps the current level of anonymity of requestors and providers, as well as that of the parties sharing their view on the others' reputations. The main advantage of this approach is that it is cose effective.

L.Xiong and L.Liu [6] proposed a reputation-based trust supporting framework, named as PeerTrust which includes a coherent adaptive trust model for quantifying and comparing the trustworthiness of peers based on a transaction- based feedback system, and a decentralized implementation of such a model over a structured P2P network.

PeerTrust model has two main features:

- It includes three basic trust parameters and two adaptive factors in computing trustworthiness of peers:

1. Feedback a peer receives from other peers.
2. The total number of transactions a peer performs.
3. The credibility of the feedback sources.
4. Transaction context factor, and the community context factor.

- It includes a general trust metric inorder to combine the various trust parameters and the adaptive factors mentioned in the above step.

In this Distributed Hash Table (DHT) based approach is used so that each peer becomes the trust holder by storing feedbacks about other peers. Global trust information stored by trust holders can be efficiently accessed through DHT.

A.A. Selcuk et al. [1] presented a vector-based trust metric relying on both interactions and recommendations. A reputation query is sent to neighbors if there are enough neighbors. Otherwise the query is flooded to network. A reputation-based trust management protocol for P2P networks is described where users rate the reliability of parties they deal with, and share this information with their peers. The protocol helps establishing trust among good peers as well as identifying the malicious ones. Each peers stores the trust information about peers in its neighborhood or peers interacted in the past. A peer sends trust queries to learn trust information of other peers. A trust query is either flooded to the network or sent to neighborhood of the query initiator. Generally, calculated trust information is not global and does not reflect opinions of all peers.Five types of malicious attacks has been given which includes naïve, discriminatory, collaborative, oscillatory, hypocritical but the main drawback is that recommendation based attacks have not been handled.

R. Zhou, K. Hwang, and M.Cai [7] proposed a gossip-based reputation system (GossipTrust) for fast aggregation of global reputation scores.It leverages a Bloom filter based scheme for efficient score ranking. GossipTrust does not require any secure hasing for fast lookup mechanism, this is applicable to both unstructured and structured P2P networks. The gossip-based protocol is designed to tolerate dynamic peer joining and departure, as well as to avoid possible peer collusions.In this a query is randomly forwarded to some neighbors instead of all neighbors.Comparing to flooding approach,gossiping reduces reputation query traffic. GossipTrust has small aggregation time, low memory demand, and high ranking accuracy. Thus gossipTrust will be efficient for trusted P2P computing.

R. Zhou and K. Hwang [2] proposed a robust and scalable P2P reputation system, called PowerTrust. The PowerTrust system dynamically selects small number of power nodes that are most reputable using a distributed ranking mechanism. By using a look-ahead random walk strategy and leveraging the power nodes, the PowerTrust significantly improves in global reputation query and aggregation speed. PowerTrust is adaptable to dynamics in peer joining and leaving and robust to disturbance by malicious peers.This power-law guided reputation system design proves to achieve high query success rate in P2P file-sharing applications. The system also reduces the total job makespan and failure rate in large- scale, parameter-sweeping P2P grid applications. The solution on a structured network like this relies on a DHT structure to store trust information. Each peer becomes a trust holder of another peer, which is assumed to provide authentic global trust information. However, a trust holder might be malicious and provide inauthentic information.

M. Virendra et al. [15] proposed a Trust-Domain based architecture for mobile ad-hoc networks (MANETs). The aim of this twofold:

- To use trust as a basis to establish keys between nodes in a MANET.
- To utilize trust as a metric for establishing secure distributed control in infrastructure-less MANETs.

Metrics have been used for nodes to establish and manage trust, and use this mutual trust to make decisions on establishing group and pair-wise keys in the network. The concept of self-organizing trust-based Physical-Logical Domains (PLDs) is used as a mean of grouping nodes for distributed control in the network. Trustworthiness is measured according to lost and misrouted packets. Trust establishment phases are defined for:

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

- For starting up new nodes.
- Maintaining trust of old peers.
- Reestablishing trust in malicious nodes.

A.Josang et al. [3] indicates that trust and reputation systems represent a significant trend in decision support for Internet mediated service provision. After completion of a transaction, and use the aggregated rating about a given party to derive a trust or reputation score, which can assist other parties in deciding whether or not transact with that party in the future. It also provides an incentive for good behaviour, and therefore tends to have a postive effect on market quality. Reputation systems can be called collaborative sanctioning systems to reflect their collaborative nature, and are related to collaborative filtering systems. Thus it implies that reputation systems are vulnerable to incorrect bogus feedback attacks. Thus feedback ratings must be based on objective criteria to be useful.

P. Resnick et al. [5] discusses that reputation is evaluated based on recommendations. It is important when deciding about strangers and new acquaintances. Reputation loses its importance as experience with an acquaintance increases. It describes some difficulties in reputation systems and they
are :

- Ensuring long-lived relationships.
- Forcing feedbacks.
- Checking honesty of recommendations.

K. Hoffma et al. [12] discuss five common attacks in P2P trust models and they are:

- Self-Promoting

Attackers manipulate their own reputation by falsely increasing it.

- Whitewashing

Attackers escape the consequence of abusing the system by using some system vulnerability to repair their reputation. Once they restore their reputation, the attackers can continue the malicious behaviour.

- Slandering

Attackers manipulate the reputation of other nodes by reporting false data to lower the reputation of the victim nodes.

- Orchestrated

Attackers orchestrate their efforts and employ several of the above strategies.

- Denial of Service

Attackers cause denial of service by preventing the calculation and dissemination of reputation values.

It implies that the defence techniques in trust models are dependent to P2P system architechture.

S. Saroiu et al. [13] developed a simple mathematical models to explore and illustrate fundamental performance issues of peer-to-peer file sharing systems. Based on the specification of model parameters the framework has been applied to three different P2P architectures:

- Centralized Indexing.
- Distributed indexing with flooded queries.
- Distributed indexing with hashing directed queries.

Investigations on the effects of system scaling, free loaders, file popularity, and availability on system performance are made. It has been stated that the P2P file sharing systems can tolerate a significant.

2. Peer-to-Peer File Sharing Process

In P2P file sharing; user can use software that connects into a P2P network to search for shared files on the computers of other users connected to the network. Files of interest can then be downloaded directly from other users on the network. Large files are broken down into smaller chunks, which may be obtained from multiple peers and then reassembled by downloader. This is done while the peer is simultaneously uploading the chunks it already has to other peers.

Interaction refers to the usage of a service provided by a particular peer. Here the interaction is considered to be the file sharing process [13]. Collecting feedback from an acquaintance about a peer is called recommendation [15]. A peer may act as a good provider of service but as far as recommendation is considered it may provide poor recommendation and vice versa. So interaction and recommendation are considered to be separate tasks. Separate history is maintained for each and every interaction that happens between the acquaintances, similarly in order to store the recommendations that are acquired from the acquaintances, a history is maintained. To evaluate various trust metrics certain assumptions are made and they are as follows:

- Peers are equal in computational power and responsibility.
- There are no privileged, centralized or trusted peers to manage trust relationships.
- Peers occasionally leave and join the network.
- A peer provides service and uses services of others.

The notations on trust metrics is given in Table 1.

Table 1: The Notations on the Trust Metrics

Notation	Description
fe^{i}_{mn}	fading effect of P_m with P_n in ith interaction
sf^{i}_{mn}	satisfaction of P_m with P_n in ith interaction
wt^{i}_{mn}	weight of P_m with P_n in ith interaction
stm_{mn}	service trust of P_m about P_n
rtm_{mq}	recommendation trust of P_m about P_q
$repm_{mn}$	reputation trsut of P_m about P_n
$hsize_{mn}$	service history size of P_m with P_n

When new interaction happens, old interaction loses their importance. This issue is addressed by the fading effect parameter. It is calculated as follows:

$$fe^{i}_{mn} = \frac{i}{hsize_{mn}} \quad (1)$$

Whenever an interaction is added or removed from service history $serhis_{mn}$, the peer needs to recalculate the fading effect value. If $serhis_{mn}$ reaches the maximum size of the history, an interaction is deleted. Before an interaction happens, the peer that requested for a file declares the amount of bandwidth that it can spend with the service provider. The evaluation of satisfaction includes other parameters like jitter, delay and retransmission of lost packets [14] [19]. The weight of an interaction is calculated based on two variables: file size and popularity. The importance (or) weight of an interaction is not based on the file size. So it is assumed that files over 100MB have same importance.

(i).Evaluation of Service Trust Metric ($sertrust_{mn}$)

Service trust metric is concerned with the evaluation of trustworthiness of the acquaintances on the basis of service they provide. To evaluate this, a peer needs to calculate two parameters: competence belief and integrity belief values. These parameters are evaluated under two criteria's: based on the service and based on the recommendation. In service context competence belief represents how well an acquaintance satisfied the needs of past interactions. [15] [3] [19]. It is calculated as:

$$cb_{mn} = \frac{1}{\beta_{cb}} \sum_{i=1}^{hsize_{mn}} \left(sf_{mn}^{i} * wt_{mn}^{i} * fe_{mn}^{i} \right) \quad (2)$$

Integrity belief represents the level of confidence in predicting the future interaction [19] [3] [15]. It is evaluated as:

$$ib_{mn} = \sqrt{\frac{1}{hsize_{mn}} \sum_{i=1}^{hsize_{mn}} \left(sf_{mn}^{i} * wt_{mn}^{\mu} * fe_{mn}^{i} - cb_{mn} \right)^2} \quad (3)$$

Based on (2) and (3) the service trust metric value is evaluated as:

$$stm_{mn} = cb_{mn} - ib_{mn}/2 \quad (4)$$

The service trust metric value calculated in (4) is purely based on the interaction alone and it does not consider the recommendation and reputation.

(ii).Evaluation of Recommendation Trust Metric (rtm_{mq})

Recommendation trust metric evaluation process involves collecting recommendation about a peer (stranger) from a set of peers (acquaintance) with which the particular peer requesting for service would have had interaction. The recommendations are given based on the interaction process between the peers, so it involves specifying how well a particular peer has satisfied the needs of another peer.

Recommendations are given by the peers based on their own experience with the stranger, and it also collects recommendation from its acquaintances. Competence belief has been measured as an average behaviour in the past interactions. In recommendation context it is evaluated as:

$$rcb_{mq} = \frac{1}{\beta_{rcb}} \sum_{j=1}^{rh_{mq}} \left(rsf_{mq}^{j} * rwt_{mq}^{j} * rfe_{mq}^{j} \right) \quad (5)$$

The integrity Belief value is measured in recommendation context after getting the recommendation reply from the acquaintance peer. It is the level of confidence in predictability of future interactions. Consistency of a peer is as important as competence. Deviation from average behaviour is a measure of the integrity belief. Thus integrity belief in recommendation context is calculated as:

$$rib_{mq} = \sqrt{\frac{1}{rh_{mq}} \sum_{j=1}^{rh_{mq}} \left(rsf_{mq}^{j} * rwt_{mq}^{\mu} * rfe_{mq}^{\mu} - rcb_{mq} \right)^2} \quad (6)$$

Thus by using competence and integrity belief values the recommendation trust metric can be evaluated as:

$$rtm_{mq} = \frac{rh_{mq}}{rh_{\max}} \left(rcb_{mq} - rib_{mq}/2 \right) + \frac{rh_{\max} - rh_{mq}}{rh_{\max}} r_{mq} \quad (7)$$

(iii). Evaluation of Reputation Metric ($repm_{mn}$)

The Reputation metric evaluation involves verifying the trustworthiness of the stranger based on the recommendations collected from the acquaintance. If a peer wants to measure the trustworthiness of the stranger it starts a reputation query. In a single query it could receive maximum number of recommendations, among all those recommendations it selects the recommendation with high trust metric value and then evaluates the reputation metric, based on which it decides whether to interact with a stranger or not. After collecting all the recommendations the peer that requested for recommendation calculates estimation about the reputation of the recommended peer.

As like the estimated competence and integrity belief values are also calculated.

$$ecb_{mn} = \frac{1}{\beta_{ecb}} \sum \left(rtm_{mq} * hsize_{qn} * cb_{qn} \right) \quad (8)$$

$$eib_{mn} = \frac{1}{\beta_{ecb}} \sum \left(rtm_{mq} * hsize_{qn} * ib_{qn} \right) \quad (9)$$

The estimated competence and estimated integrity belief values represents the own experience of the acquaintance of the peer that requested for recommendation with the peer that provided the recommendation.

$$repm_{mn} = \frac{\lfloor \mu_{sh} \rfloor}{sh_{\max}} \left(ecb_{mn} - eib_{mn}/2 \right) + \left(1 - \frac{\lfloor \mu_{sh} \rfloor}{sh_{\max}} \right) er_{mn} \quad (10)$$

The service trust metric value is evaluated once again based on the reputation and recommendation values.

$$stm_{mn} = \frac{hsize_{mn}}{sh_{\max}} (cb_{mn} - ib_{mn}/2) + \left(1 - \frac{hsize_{mn}}{sh_{\max}} \right) repm_{mn} \quad (11)$$

(iv). Finding service provider

Service provider selection is done based on service trust metric, service history size, competence belief, and integrity belief values. When a peer wants to download a file it selects an up loader with highest service trust metric value. Selecting service providers may overload some peers while others are idle. Thus a peer's number of simultaneous download or upload operations are limited to maximum. If a peer reaches its maximum number of uploads, it rejects incoming requests so the requestor can get services from others.

(v). Comparison with Previous Work

We now illustrate the major difference between our work and representative related work [1]. Selcuk et al. [1] presented a vector- based trust metric relying on both interactions and recommendations. A reputation query is sent to neighbours if there are enough neighbours. Otherwise, the query is flooded to network. In comparison, our model requires that the peers need to send reputation queries only to peers interacted in the past, which reduces network traffic compared to flooding based approaches. Furthermore, each peer expands its trust network with time and can obtain more credible recommendations from acquaintances.

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

III. Analysis

(i). Finding service provider without considering recommendation and reputation

The service requestor selects a peer with high service trust metric value for interaction. The service trust metric value is first calculated without collecting recommendation about a peer. Though peer with highest value could be chosen it is not highly trust worthy as it ignores recommendation and reputation. The service trust metric values evaluated for various peers are given in Table 2.

Table 2: Service trust metric values without recommendation and reputation

Service Provider	Service Requestor	File Name	Bandwidth	Service Trust Metric
Peer1	Peer2	ex.txt	1.16513kbps	0.14999
Peer3	Peer2	ex1.txt	1.44067kbps	0.17499
Peer4	Peer2	ex2.txt	1.10434kbps	0.2000
Peer5	Peer2	ex3.txt	1.16513kbps	0.22500
Peer6	Peer2	ex4.txt	1.08547kbps	0.25
Peer7	Peer2	ex5.txt	1.82142kbps	0.224999
Peer8	Peer2	ex1.txt	1.44067kbps	0.20000
Peer9	Peer2	ex.txt	1.16513kbps	0.17499
Peer10	Peer2	ex.txt	1.16513kbps	0.14999
Peer11	Peer2	ex3.txt	1.825kbps	0.125
Peer12	Peer2	ex3.txt	1.825kbps	0.09999
Peer13	Peer2	ex3.txt	1.825kbps	0.07499
Peer14	Peer2	ex5.txt	1.82142kbps	0.04999
Peer15	Peer2	ex5.txt	1.82142kbps	0.02500
Peer16	Peer2	ex.txt	1.16513kbps	0.01000
Peer17	Peer2	ex.txt	1.16513kbps	0.02500
Peer18	Peer2	ex.txt	1.16513kbps	0.05000
Peer19	Peer2	ex4.txt	1.08547kbps	0.07500
Peer20	Peer2	ex2.txt	1.10434kbps	0.09999

(ii). Finding service provider based on recommendation and reputation

In proposed system the selection of service provider is made by focusing on recommendation and reputation. As these metrics measures the trustworthiness of the stranger they are more reliable and ignores maliciousness than the service metric value measured without collecting recommendation. The service trust metric value based on recommendation is depicted in Table 3.

Table. 3: Service trust metric values based on recommendation and reputation

Service Provider	Recommending Peer	Service Requestor	rtm_{mq}	stm_{mn}
Peer3	Peer2	Peer1	2.33808	0.68096
Peer4	Peer3	Peer1	2.24146	0.93219

IV. Conclusion

In this paper, a trust model for P2P networks is presented, in which a peer can develop a trust network in its proximity. A peer can therefore isolate malicious peers around itself as it develops trust relationships with good peers. Two context of trust, service and recommendation contexts are defined to measure capabilities of peers in providing services and giving recommendations. A recommendation contains the recommenders own experience, information from its acquaintances, and level of confidence in recommendation. The interactions are also measured with satisfaction, weight and fading effect. Thus these parameters provide a better assessment of trustworthiness. These trust metric information enhances security and effectiveness of the network and it also selects best service provider for interaction process. Though these trust metric information serves to a great extent in peer-to-peer network they do not solve all the security problems in the network and loses part of its trust network if any peer changes its point of attachment. Trust metric information's have been used in Peer-to-Peer file sharing applications but as a future work it could be adapted for various other P2P applications like CPU sharing, storage networks and P2P gaming.

References

[1] *A.A. Seluck, E. Uzun, and M.R. Pariente, "A Reputation-Based Trust Management System for P2P Networks," Proc. IEEE/ACM Fourth Int'l Symp. Cluster Computing and the Grid (CCGRID), 2004.*

[2] *R. Zhou and K. Hwang, "Powertrust: A Robust and Scalable Reputation System for Trusted Peer-to-Peer Computing." IEEE Trans. Parallel and Distributed Systems, vol. 18, no. 4, pp. 460-473, Apr. 2007.*

[3] *A. Josang, R. Ismail, and C. Boyd, "A Survey of Trust and Reputation Systems for Online Service Provision," Decision Support Systems, vol. 43, no. 2, pp. 618-644, 2007.*

[4] *K. Aberer and Z. Despotovic, "Managing Trust in a Peer-2-Peer Information System," Proc. 10th Int'l Conf. Information and Knowledge Management (CIKM), 2001.*

[5] *P. Resnick, K. Kuwabara, R. Zeckhauser, and E. Friedman, "Reputation Systems," Comm. ACM, vol. 43, no. 12, pp. 45-48, 2000.*

[6] *L. Xiong and L. Liu, "Peertrust: Supporting Reputation-Based Trust for Peer- to-Peer Ecommerce Communities," IEEE Trans. Knowledge and Data Eng., vol. 16, no. 7, pp. 843-857, July 2004.*

[7] *R. Zhou, K. Hwang, and M.Cai, "Gossiptrust for Fast Reputation Aggregation in Peer-to-Peer Networks," IEEE Trans. Knowledge and Data Eng., vol. 20, no. 9, pp. 1282-1295, Sept. 2008.*

[8] *F. Cornelli, E. Damiani, S.D.C. di Vimercati, S. Paraboschi, and P. Saramati, "Choosing Reputable Servents in a P2P Network," Proc. 12th World Wide Web Conf. (WWW), 2003.*

[9] *S. Song, K. Hwang, R.Zhou, and Y. Kwok, "Trusted P2P Transactions with Fuzzy Reputation Aggregation," IEEE Internet Computing, vol. 9, no. 6, pp. 24-34, Nov-Dec. 2005.*

[10] *M. Gupta, P. Judge, and M. Ammar, "A Reputation System for Peer-to-Peer Networks," Proc. 13th Int'l Workshop Network Network and Operating Systems Support for Digital Audio and Video (NOSSDAV), 2003.*

[11] *B. Ooi, C. Liau, and K. Tan, "Managing Trust in Peer-to-Peer Systems Using Reputation-Based Techniques," Proc. Fourth Int'l Conf. Web Age Information Management, 2003.*

[12] *K. Hoffman, D. Zage, and C. Nita-Rotaru, "A Survey of Attack and Defense Techniques for Reputation Systems," ACM Computing Surveys, vol. 42, no. 1, pp. 1:1-1:31, 2009.*

[13] S. Saroiu, P. Gummadi, and S. Gribble, "A Measurement Study of Peer-to-Peer File Sharing Systems," Proc. Multimedia Computing and Networking, 2002.

[14] M. Virendra, M. Jadliwala, M. Chandrasekaran, and S. Upadhyaya, "Quantifying Trust in Mobile Ad-Hoc Networks," Proc. IEEE Int'l Conf. Integration of Knowledge Intensive Multi-Agent Systems (KIMAS), 2005.

[15] S. Xiao and I. Benbasat, "The Formation of Trust and Distrust in Recommendation Agents in Repeated Interactions: A Process-Tracing Analysis," Proc. Fifth ACM Conf. Electronic Commerce (EC), 2003.

[16] G. Swamynathan, B.Y. Zhao, and K.C. Almeroth, "Decoupling Service and Feedback Trust in aPeer-to-Peer Reputation System," Proc. Int'l Conf. Parallel and Distributed Processing and Applications (ISPA), 2005.

[17] S. Marsh, "Formalising Trust as a Computational Concept," PhD thesis, Dept. of Math. and Computer Science, Univ of Stirling, 1994.

[18] L. Mui, M. Mohtashemi, and A.Halberstadt, "A Computational Model of Trust and Reputation for E-Businesses," Proc. 35th Hawaii Int'l Conf. System Sciences (HICSS), 2002.

[19] B. Yu and M. Singh, "A Social Mechanism of Reputation Management in Electronic Communities," Proc. Cooperative Information Agents (CIA), 2000.