Peer-To-Peer Self Organizing Confidence Model Systems

[1]V. V. Sharma, [2]R. B. Wagh
[1,2]Dept. of Computer Engineering, R. C. Patel Institute of Technology, Shirpur, India

Abstract
In peer-to-peer interconnection applications are largely used in distinct systems. Peer-to-Peer is relay on gather of peers in sequence to obtain the process. However due to the open nature of Peer-to-Peer applications, there are many number of security issue associated. In Peer-to-Peer applications, it is simple to perform the any malicious activity and this becomes the large security threat. Designing the long term confidence relationship between the distinct peers may deliver more secure environment by reduced the uncertainty and risk in upcoming Peer-to-Peer intercommunications. But the major issue is to establish the confidence in unknown peer under the malicious environment. Additionally, confidence is nothing but social things which is extremely complex to compute with the numerical values. Such metrics are required to present the confidence in computational models. This becomes the problem statement for Peer-to-Peer systems. To resolve such issues in Peer-to-Peer applications, number of solution introduced in literature but failed to optimize the security against different malicious peers in network.

Keywords
Peer-to-peer applications, confidence management, reputation, security, System malicious peers Search, Dispense Ei-gen credit Algorithm.

I. Introduction

P2P (Peer-To-Peer) applications bargain on cooperation of the peers to accomplish process. Ease of dispatch the malicious action in a threat for security of P2P applications. Generating lengthy-term trust relationships between the peers can supply the much secure environment by decreasing danger and uncertainty in future of the P2P communications. Institute trust in an unknown establishment is the complex in such malicious environment. However, trust is the social portion and hard to compute with the mathematical values. Metrics are required to present the belief in computational model. Identify the peers as either trust moral or un-trust-worthy is not enough in most cases. Metrics should have the precision so peers can categorize in conformity to trust worthiness. Communications and feedback of peers supply information to compute the trust between peers. Communications with the peer supplied the unavoidable information about peer but feedback might comprise deceptive information. This makes the assessment of trust-worthiness the provocation. In present of authority, the middle server is preferred the route to store and handle trust information, e.g., eBay. The middle server reliable store trust information and represent the trust metrics. Since there is no middle server in most P2P applications, peers utilize to store and manage trust information about every other. Management of trust information is based to structure of P2P network. In dispense hash table depend on approaches every peer become a trust holder by storing feedback about another peer. Global trust information stored, trust container can be entry. In un-structured network, every peer store trust information about the peers in its neighbourhood peers communicated in past. A peer transmits the trust queries to learn the trust information of another peer trust query is either flooded to network or transfer to neighbourhood of query initiator. Basically, measured the trust information is not global and does not affect the belief of all peer. Aim to reduce the malicious activity in a P2P application by establishing the trust between peers in their proximity. A priori information or trusted peer is used to leverage the trust establishment. Peer does not try to gathers trust information from all peers. Every peer develops its own local view of trust about peer communicated in past. In this route, good peers form the dynamic trust sets in their proximity and can isolate the malicious peers. Since peers basically trend to communicate with small groups of peers [7], forming trust relation in proximity of peer helps to alleviate attacks in a Peer-2-Peer application.

In Peer-2-Peer Self-Organizing Confidence Model Systems, peers are assumed to best ranger to every other at initiating. A peer become an acquaintance of other peer after supply the service, e.g., uploading a file. If a peer has no acquaintance, it selects to trust strangers. Using the service of a peer is the communication, which is evaluated, depends on the weight and recentness of the communication, and satisfaction of requester. An acquaintances feedback about a peer, recommendation, is evaluated based on the direction trust-worthiness contain the recommender own experience about peer, information gathered from direction acquaintances and direction level of trust in the direction. The level of trust is less; the direction has a low value in evaluation and effect the less trust-worthiness of the exhortations.

The peer is a decent service to supplier but a bad direction, Peer-2-Peer Self-Organizing Confidence Model Systems, Assumed supplying services and giving the directions as distinct process and denoted as two contexts of confidence service and directions contexts. Information about the past communications and directions are stored in particular histories to assess competence and combination of acquaintances in these contexts.

We construct the Peer-to-Peer file sharing simulation tool and implement experiment to understand the impact of Peer-2-Peer Self-Organizing Confidence Model Systems in malicious activity. Signatures concerned to the peer capabilities, peer behavior and resource distributions are approximated to various empirical outcomes. To make much reliable observation on evolution of confidence relationship we analyzed the sixteen kinds of malicious peer state, which has performs the both service and directions-depend activity attacks. Peer-2-Peer Self-Organizing Confidence Model Systems, integrate service-based attacks in every case. Directions-depend activity was contained except when malicious peers are in big numbers, e.g., 50 percent of all peers. Experiments on Peer-2-Peer Self-Organizing Confidence Model Systems show that good peers can defend against malicious peer without having the global confidence of information Peer-2-Peer Self-Organizing Confidence Model Systems trust of peer assess trust-worthiness of another peers depend on the local information.

Outline of the paper is as follows: Section II discusses the related research. Section III explains the proposed model of Peer-2-Peer Self-Organizing Confidence Model Systems, Section IV presents the summarizes the results and possible future work directions.

II. Literature Survey

We are presenting the survey on Peer-2-Peer Self-Organizing Confidence Model Systems.

In [1] author N. Tran, B. Min, J. Li, and L. Subramanian, Obtaining user opinion (using votes) is essential to ranking user-generated online content. However, any content voting system is susceptible to the Sybil attack where adversaries can out-vote real users by creating many Sybil identities. In this paper, we present SumUp, a Sybilresilient vote aggregation system that leverages the trust network among users to defend against Sybil attacks. SumUp uses the technique of adaptive vote flow aggregation to limit the number of bogus votes cast by adversaries to no more than the number of attack edges in the trust network (with high probability). Using user feedback on votes, SumUp further restricts the voting power of adversaries who continuously misbehave to below the number of their attack edges. Using detailed evaluation of several existing social networks (YouTube, Flickr), we show SumUp's ability to handle Sybil attacks.

In [2] the author R. Zhou, K. Hwang, and M. Cai In peer-to-peer (P2P) networks, reputation aggregation and ranking are the most time-consuming and space-demanding operations. This paper proposes a new gossip protocol for fast score aggregation. We developed a Bloom filter architecture for efficient score ranking. These techniques do not require any secure hashing or fast lookup mechanism, thus are applicable to both unstructured and structured P2P networks. We report the design principles and performance results of a simulated GossipTrust reputation system. Randomized gossiping with effective use of power nodes enables light-weight aggregation and fast dissemination of global scores in $O(\log_2 n)$ time steps, where n is the P2P network size. The Gossip-based protocol is designed to tolerate dynamic peer joining and departure, as well as to avoid possible peer collusions. The scheme has a considerably low gossiping message overhead, i.e. $O(n \log_2 n)$ messages for n nodes. Bloom filters demand at most 512 KB memory per node for a 10,000-node network. We evaluate the performance of GossipTrust with distributed P2P file-sharing and parameter-sweeping applications. The simulation results demonstrate that GossipTrust has small aggregation time, low memory demand, and high ranking accuracy. These results suggest promising advantages of using the GossipTrust system for trusted P2P applications.

In [3] K. Hoffman, D. Zage, and C. Nita-Rotaru eputation systems provide mechanisms through which multiple parties can quantify the trust between one another. These systems seek to generate an accurate assessment in the face of unprecedented community size, while providing anonymity and resilience to malicious attacks. We focus on attacks and defense mechanisms in reputation systems. We present an analysis framework that allows for general decomposition of existing reputation systems. We classify attacks against reputation systems by identifying which system components and design choices are the target of attacks. We survey defense mechanisms employed by existing reputation systems. Finally, we analyze several landmark systems, characterizing their individual strengths and weaknesse

In [4] the author Y. Zhong Trust characterizes the probability that a user will not harm the operations of an information system. User or site trustworthiness is needed in transaction processing, distributed database processing (consistency, integrity), peer-to-peer systems, web based e-commerce systems, and building routes in ad hoc networks. We argue that credentials are not sufficient to certify that a user is trustworthy.

This research is developing formal model for trust, authorization, fraud, and privacy. It incorporates the comprehensive aspects of trust in social life and computer science applications. Considering associated contexts, it automates the evaluation of trust under uncertain evidence and dynamic interactions. Trust is being integrated with authorization and authentication mechanisms for use in an open computing environment so that applications can use these models.
This research presents an authorization framework based on uncertain evidence and dynamic trust. A prototype called TERA (Trust-Enhanced Role Assignment) has been built for experimental studies. The TERA prototype evaluates the trust of a user from her behaviors. It decides whether a user is authorized for an operation based on the policies, the evidence, and the degree of trust. The reliability of the evidence is based on the trust of the evidence provider. A user's trust value is dynamically updated when additional data on behaviors is available. The trust information is managed by a reputation server.

In [5] Z. Despotovic and K. Aberer, The vast majority of the interactions in typical online communities nowadays is between complete strangers. In such settings reputation reporting and trust management models play a crucial role for proper functioning of those communities. A lot of work has been done on the issues of collecting and spreading reputations and subsequent computation of trust. The application of such data for decision making, however, is far less explored. In this paper we present a solution for scheduling exchanges among participants of an online community which takes into account their trustworthiness. In this way we can enable exchanges that would otherwise not be taking place. Thus this work also demonstrates that trust can in fact increase economic activity.

In [6] S. Boyd, A. Ghosh, B. Prabhakar, and D. Shah, Motivated by applications to sensor, peer-to-peer, and ad hoc networks, we study distributed algorithms, also known as gossip algorithms, for exchanging information and for computing in an arbitrarily connected network of nodes. The topology of such networks changes continuously as new nodes join and old nodes leave the network. Algorithms for such networks need to be robust against changes in topology. Additionally, nodes in sensor networks operate under limited computational, communication, and energy resources. These constraints have motivated the design of "gossip" algorithms: schemes which distribute the computational burden and in which a node communicates with a randomly chosen neighbour.

[7] Y. Wang and J. Vassileva , Trust and reputation are two related, but different concepts. In this paper, we first distinguish the two concepts and compare the trust and reputation mechanisms in centralized systems with those in decentralized systems. Then we propose a Bayesian network based trust model in peer-to-peer networks. Since trust is multifaceted, even in the same context, peers still need to develop differentiated trust in different aspects of other peers' behaviors. The peer's needs are different in different situations. Depending on the situation, a peer may need to consider its trust in a specific aspect of another peer's capability or in multiple aspects. Bayesian networks provide a flexible method to present differentiated trust and combine different aspects of trust. A Bayesian network-based trust model is presented for a file sharing peer-to-peer application.

In [8] R. Guha, R. Kumar, P. Raghavan, and A. Tomkins, A (directed) network of people connected by ratings or trust scores, and a model for propagating those trust scores, is a fundamental building block in many of today's most successful e-commerce and recommendation systems. We develop a framework of trust propagation schemes, each of which may be appropriate in certain circumstances, and evaluate the schemes on a large trust network consisting of 800K trust scores expressed among 130K people. We show that a small number of expressed trusts/distrust per individual allows us to predict trust between any two people in the system with high accuracy. Our work appears to be the first to incorporate distrust in a computational trust propagation setting.

[9] Prior literature focuses on trust, while largely ignoring distrust, partly because of the assumption that an Information Technology (IT) design that builds trust in the IT will also prevent distrust-building. However, this assumption may not be true if trust-building processes and distrust-building processes in the context of IT usage are different. This paper proposes a two-process view of trust and distrust building, i.e., that trust-building and distrust-building processes are distinct and separate. In the context of recommendation agent (RA) usage in electronic commerce, a trust (distrust) process is defined as a customer's favorable (unfavorable) interpretation of his or her interactions with an RA, resulting in a positive (negative) expectation that the RA can be relied upon for his or her shopping decisions. This study empirically tests a process theory rather than a variance theory.

[10] J. Douceur, Most current P2P file sharing systems treat their users as anonymous, unrelated entities, and completely disregard any social relationships between them. However, social phenomena such as friendship and the existence of communities of users with similar tastes may be well exploited in such systems, to increase their usability and performance. In this paper we present a novel social-based P2P file-sharing paradigm that exploits social phenomena by maintaining social networks and using these in content discovery, content recommendation, and downloading. Based on this paradigm's first class concepts such as taste groups, friends, and friends-offriends, we have designed and implemented the TRIBLER P2P filesharing system as a set of extensions to Bittorrent. We present and discuss the design of TRIBLER, and we show evidence that TRIBLER enables fast, trusted content discovery and recommendation at a low additional overhead, and a significant improvement in download performance.

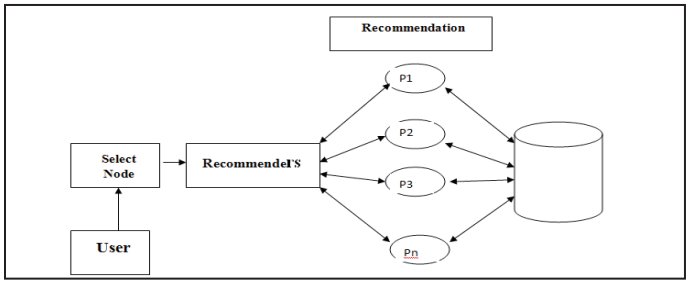
III. Proposed Work and Architechture

A. Proposed Work

There are distinct kinds of malicious activities either performed by either insider node or outsider nodes. In this project we are presenting the Peer-2-Peer Self-Organizing Confidence Model Systems for P2P systems. In existing SORT method is proposed currently for reducing the impact of malicious activities in P2P applications. In Peer-2-Peer Self-Organizing Confidence Model Systems, we are designing the algorithm to handle the confidence over the all entire P2P applications which was missing in existing SORT. We first represent the distributed techniques which allow peer node to cause about trustworthiness of another peer depending on previous directions and communications. The own confidence of network is formed by peers in their own proximity using local information. While evaluating the recommendation, trustworthiness and trust of directions are assumed. Then proposing the naive approach for obtaining the global confidence of all over the P2P applications in order enhance the security of previous techniques against the malicious peer activities. The experimental analysis of proposed approach will be done depend on the simulation analysis and performance is measured against the SORT techniques.

B. Proposed System Architecture

Following architecture diagram shows the system design can contain proposed work.



IV. Algorithms

A. Algorithms

Algorithm 1. Dispense Ei-gen credit

Algorithm

1. **Input:** n, n1, n2+....., n+1 up to 100.
2. N- Represent the number of available nodes.
3. Each peer i do
4. {
5. All peers n ∈ Ai for t (0) j = pn ;
6. Repeat
7. Compute ti (k+1) i = (1 − a)(c1it (k) 1 + c2it (k) 2 + . . . + cnit (k) n) + api;
8. Send cin t (k+1) i to all peers j ∈ Bi;
9. Compute δ = |t (k+1) i − t (k) i |;
10. Wait for all peers n ∈ Ai to return cnit (k+1) j ;
11. Until δ < ∈.;
12. }

Algorithm 2 System malicious peers Search

1. **Input:** R=[R1, R2, … , RN]
2. Ri is the ith nodes of R
3. **Output:** SMPS ∆suspicious malicious peers set
4. obtain reconstructed reputation values matrix
5. R= [R1, R2, R3,…, Rn] of R through SMP
6. for each node i
7. calculate QRi
8. end for
9. obtain QR vector QRV=[QR1, QR2, … , QRN]
10. for each QRi in QRV
11. if QRi < γ
12. i is considered as a malicious peer, add i to SMPS
13. end if
14. end for.

B. Hardware and Software

1. Hardware Configuration

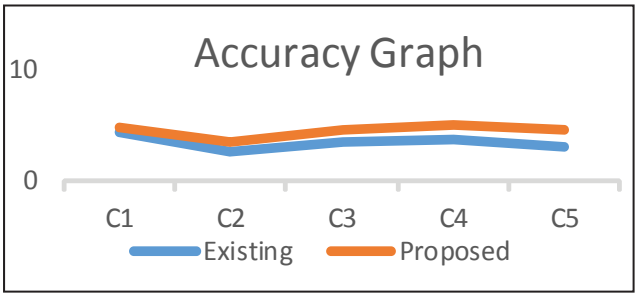
- Processor: - Intel Core I3 2.10 GH.
- RAM :- 4GB (Minimum)
- DISK :- 350GB

2. Software Configuration

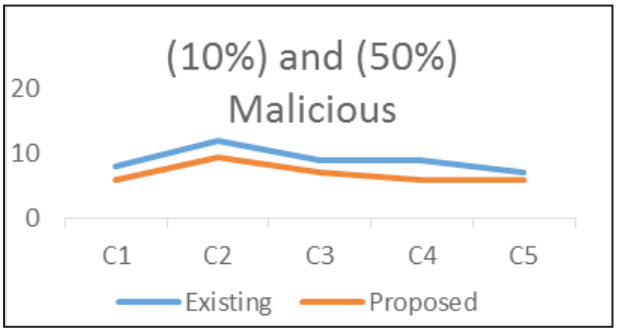
- Operating System : - Windows 7 / 8/ 10
  Programming Language: - JAVA,

V. Expected Results/Performance Evaluation

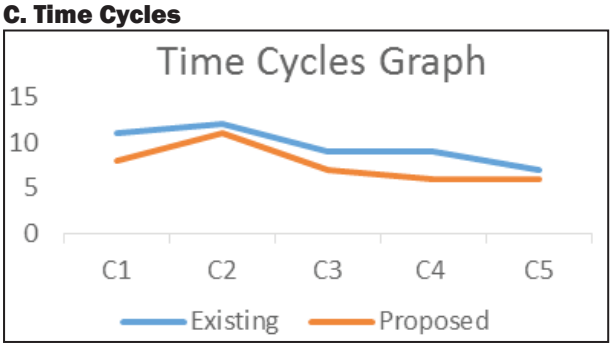
A. Accuracy Graph



B. (10%) & (50%) Malicious



C. Time Cycles



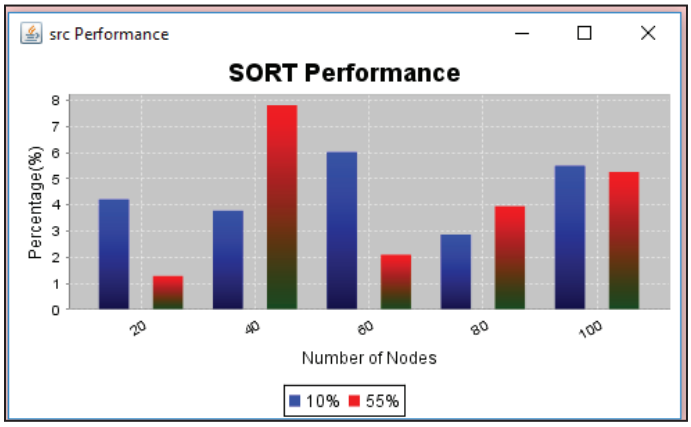
D. SORT Table:

Malicious Node	Value
11	0.96
8	0.95
18	0.84
7	0.64
10	0.42
9	0.51
2	0.41
14	0.75
19	0.26
19	0.03
1	0.02
8	0.62
15	0.24
8	0.54
11	0.19
2	0.09

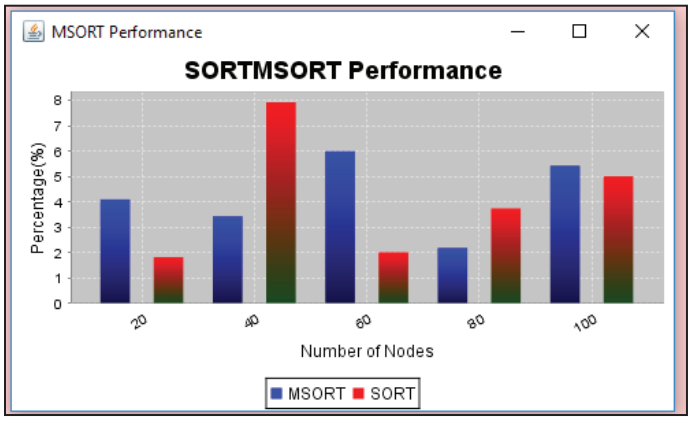
E. MSORT Table:

Node	Arrival Time	Request Time
7	0.1380000000000001	0.1380000000000001
14	0.1540000000000001	0.1540000000000001
3	0.16400000000000012	0.16400000000000012
6	0.22000000000000017	0.22000000000000017
0	0.23700000000000018	0.23700000000000018
7	0.3080000000000002	0.3080000000000002
1	0.3840000000000003	0.3840000000000003
1	0.3980000000000003	0.3980000000000003
2	0.4090000000000003	0.4090000000000003
4	0.44000000000000034	0.44000000000000034
9	0.47400000000000037	0.47400000000000037
13	0.4840000000000004	0.4840000000000004
9	0.5130000000000003	0.5130000000000003
1	0.5510000000000004	0.5510000000000004

F. SORT Performance:



G. SORT And MSORT Performance:



VI. Conclusion

A confidence model for the Peer-to-Peer networks is represented, in which a peer can implement the confidence network in proximity. Peer can isolate malicious peer around itself it construct the confidence relationship with decent peers. Two context of confidence, service and directions contexts, are denoted to compute the abilities of peers in supplied services and giving the directions. Communication and direction are assumed with satisfaction, weight, and fading effect signature. Are commendation contains there commanders own experience, information from its acquaintances, and level of confidence in the recommendation. These parameters supplied us a better assessment of trust-worthiness. Particular, collaborative and pseudonym varying attackers are analyzed in experiments. Damage of collaboration and pseudo spoofing is based to attack

behavior. Although recommendations are vital in hypocritical and oscillatory attacker, pseudospoofer and collaborators, they are minimum useful in novel and discriminatory attackers Peer-2-Peer Self-Organizing Confidence Model Systems integrate both service and direction-based attacks in most experiment. However, in extremely malicious environments such as a 50 percent malicious network, collaborators can continue to the disseminates big amount of misleading directions. Other problem about Peer-2-Peer Self-Organizing Confidence Model Systems is handling the confidence of all over network. If a peer vary point of attachment to network, it might lose the section of its confidence network. These problems might be analysis as the future work to advance confidence model. Using confidence information does not solve all security issues in Peer-2-Peer applications but can improve the security and effectiveness of applications. If communications are model perfectly, Peer-2-Peer Self-Organizing Confidence Model Systems to several Peer-2-Peer applications, i.e., CPU sharing, storage networks and P2P gaming.

References

[1] N. Tran, B. Min, J. Li, L. Subramanian,"Sybil-Resilient Online Content Voting," Proc. Sixth USENIX Symp. Networked Systems Design and Implementation (NSDI), 2009.

[2] R. Zhou, K. Hwang, 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.

[3] K. Hoffman, D. Zage, 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.

[4] Y. Zhong,"Formalization of Dynamic Trust and Uncertain Evidence for User Authorization", PhD thesis, Dept. of Computer Science, Purdue Univ. 2004.

[5] Z. Despotovic and K. Aberer, "Trust-Aware Delivery of Composite Goods," Proc. First Int'l Conf. Agents and Peer-to-Peer Computing, 2002.

[6] R. Guha, R. Kumar, P. Raghavan, A. Tomkins, "Propagation of Trust and Distrust," Proc. 13th Int'l Conf. World Wide Web (WWW), 2004.

[7] S. Boyd, A. Ghosh, B. Prabhakar, D. Shah,"Randomized Gossip Algorithms," IEEE/ACM Trans. Networking, Vol. 52, No. 6, pp. 2508-2530, June 2006.

[8] R. Sherwood, S. Lee, B. Bhattacharjee,"Cooperative Peer Groups in Nice," Computer Networks, Vol. 50, No. 4, pp. 523-544, 2006.

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

[10] A. Habib, D. Xu, M. Atallah, B. Bhargava, and J. Chuang, "A TreeBased Forward Digest Protocol to Verify Data Integrity in Distributed Media Streaming," IEEE Trans. Knowledge and Data Eng., Vol. 17, No. 7, pp. 1010-1014, July 2005.

[11] Y. Wang, J. Vassileva,"Bayesian Network Trust Model in Peer-to-Peer Networks," Proc. Second Workshop Agents and Peer-toPeer Computing at the Autonomous Agents and Multi Agent Systems Conf. (AAMAS), 2003.

[12] R. Guha, R. Kumar, P. Raghavan, A. Tomkins, "Propagation of Trust and Distrust," Proc. 13th Int'l Conf. World Wide Web (WWW), 2004.

[13] J. Douceur,"The Sybil Attack," Proc. First Int'l Workshop Peer-toPeer Systems (IPTPS), 2002.

[14] S. Staab, B. Bhargava, L. Lilien, A. Rosenthal, M. Winslett, M. Sloman, T. Dillon, E. Chang, F.K. Hussain, W. Nejdl, D. Olmedilla, V. Kashyap,"The Pudding of Trust," IEEE Intelligent Systems, Vol. 19, No. 5, pp. 74-88, 2004.

[15] A.A. Selcuk, E. Uzun, 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.