IOSR Journal of Engineering (IOSRJEN)
e-ISSN: 2250-3021, p-ISSN: 2278-8719, www.iosrjen.org
Volume 2, Issue 10 (October 2012), PP 01-08

P2P Reputation Management Scheme Using a Cryptographic Protocol

Sivananda.C.K[1], Kalpana.K[2]
[1]*Department of CSE, G.Pullareddy Engineering College,Kurnool, Andhra Pradesh, India*
[2] *Associate Professor Department of CSE, G.Pullareddy Engineering College,Kurnool, Andhra Pradesh, India*

***Abstract*—** *Reputation management in a peer to peer network is difficult as challenges are posed by lack of centralized authority. For this reason P2P (Peer-to-Peer) network is vulnerable which can facilitate non-cooperation, cheating, leaching on the network and propagation of malicious code. The security model used for centralized C/S systems is not suitable for P2P networks as it is centralized in nature. The security challenges in the P2P networks are secure reputation data management, availability of reputation data, Sybil attacks and identity management of peers. This paper presents a new protocol based on cryptography which ensures timely availability of reputation data, at low cost, to other peers and security. The approach is to encapsulate the past behavior of the peer in its digital reputation and then envisaging its actions pertaining to future. Thus a peer's reputation prevents it from doing malicious activities. The protocol is capable of countering Sybil attacks. More over the cryptographic protocol is with features like identity management with the help of cryptographic mechanisms and self certification. The results in the form of simulations reveal that the new cryptographic protocol is secure and efficient in a decentralized peer – to – peer network.*

***Index Terms*—** *Reputations, Identity Management, P2P networks, security, distributed systems.*

I. INTRODUCTION

A P2P network is a network without a dedicated and centralized server. Instead, it is a kind of network with peers without having designated as client or server. All nodes are treated alike. The network lacks a central control. Therefore, the network exposes many security vulnerabilities like spreading malicious code, viruses, worms, and Trojans. It is especially more vulnerable when compared with traditional C/S network. There were plethora of instances that revealed attacks in P2P networks. For instance Gnutella network was infected by worm "VBS.Gnutella" and Trojans are stored in the host system. Due to ad hoc and decentralized nature of P2P networks, it is extremely difficult to provide security to the network. More over they are spread geographically and they are subject to different laws. The conventional mechanisms used to secure C/S systems are in vain in case of P2P networks for the valid reason specified earlier.

The difficulty of securing P2P networks can be greatly mitigating by utilizing services of a CA (Certificate Authority) which is centralized again. The drawback of a centralized authority is that if the authority is compromised, it itself can spoil the whole P2P network. At the same time without its presents, no magic wand is present to ensure security to P2P networks.

In this paper, investigation is made on P2P networks and their reputation systems. A new approach is invented without making use of a centralized authority besides enjoying all the benefits of a P2P network. Peers are estimated whether they are good or malicious based on their reputations. The malicious peers are separated from good peers soon after detecting them. Malicious activities are significantly reduced by eliminating malicious nodes peers from the network. Identity certificates are used to identify all peers in the network. Such certificates are self certified and all peers are like certificate authorities as they have their own CA which issues certificates. Each and every node has its history pertaining to reputation management. When a transaction takes place between two peers, the two-party cryptographic protocol helps in secure exchange of reputation information between peers. The experiments resulted in providing evidence that the proposed infrastructure for reputation management can greatly reduce the percentage of malicious transactions over P2P networks. The significant contributions of this paper are:

- ✓ A simple and light weight reputation model.
- ✓ Cryptographically blind identity mechanisms are used to arrive at a self-certification based identity system.

- ✓ Generation of an authentic global reputation information of a peer with the help of an attach resistant cryptographic protocol

II. RELATED WORK

2.1 Structured and Unstructured P2P Networks

P2P networks are of two types namely structured and unstructured. Proposed system works on both networks. Networks like PASTRY [4], CAN [3] and Chord [2] are structured networks where search process is faster. Unstructured P2P networks are slow in search as there is no super node concept. The reputation scheme of this paper is independent of the type of P2P network.

2.2 Distributed Systems Security

This section describes distributed CAs.

2.2.1 Publius

PUblius [4] is nothing but a set of independent servers in a monolithic system. It allows anonymous users to publish anything as it is censorship resistant. It divides secret among a set of servers with the help of cryptographic secret splitting techniques.

2.2.2 Groove

Groove [5] is builds context sensitive, self-administering and synchronized share spaces in order to share and exchange files. It provides security to spared spaces and authentication of its groups.

2.2.3 SDSI

SDSI [6] can provide means for self – extraction, secure formation of groups, simple access control mechanisms, and local name spaces. It is a simple DSI (Distributed Security Infrastructure). It can also simplify X.509 certificates.

2.2.4 Dynamic Trust Management

In dynamic distributed environments, it encapsulates trust management. Agile Management of Dynamic Collaborations [7] has developed techniques for dynamic trust management, secure group communication protocols, identification of components and their authentication.

2.2.5 RBAC

In 1992 Ferraoilo and Kuhn [8] introduced RBAC (Role Based Access Control). It associates permissions with roles but not users. It is available in four models namely unified, constrained, hierarchical and core.

2.3 Reputation Systems

Reputation systems are used in both P2P and client server networks. The present reputation system can be classified into three categories. The first two categories are related to P2P network [11] while the third one is related to client server network.

2.3.1 Reputation Models

As per Resnick et al. reputation system is "a system that collects, distributes, and aggregates feedback about customer's past behavior." They explain the problem of pseudospoofing in [13] which is a process of making use of multiple pseudonyms in a system by same real life entity. The drawback is that nodes may drop pseudonym and take new one when its reputation goes down.

Hash functions are used by PeerTrust [14] to allocate information pertaining to reputation to a node in the network. Other peers use Network's native search mechanism to get reputation details and take decisions.

2.3.2 Reputation Infrastructure

One of the examples for this is "P2PRep" [20] is a reputation model built on top of Gnutella. It is developed by security group of university Milano. Due to its statelessness, it is highly communication intensive system.

2.3.3 Centralized Reputation Systems

Monster, Amazon and eBay follow this kind of reputation system in which a central server provides pseudonyms to clients. When a client needs to login and start making request, it has to choose a service provider based on its reputation.

III. REPUTATION SYSTEM

3.1Threat Model

In P2P systems, peers connect and leave with insecure communication channels. Peers may have conflicting interests and malicious intentions as well. Malware can also be spread by rogue peers. Peers should be in a position to judge the genuineness of content before involving in transactions. To achieve this goal a perfect mechanism and reputation system is needed. Ballot stuffing and bad mouthing are results of an imperfect reputation system. It all depends on building reputation system to improve reputation mechanism and prevent peers from indulging malicious activities.

3.2 Self Certification

Every peer should have a handle or identity for participating in reputation system. Based on the recommendations received by a peer to participate in transactions, its reputation is calculated. In a decentralized P2P network, as there is not central authority to issue certificates, each node can generate a certificate and thus act as CA (Certificate Authority). Reputations are associated with identities and in turn the combined reputation of all identities comprises the reputation of CA. An attack by name Sybil can cause a peer to misuse self certification by generating so many identities and thus increasing its reputation. This problem can be prevented by restricting a peer to have only one identity or mapping all identities generated by it to its real life identifier.
There is another problem with CA. A malicious peer can generate multiple CAs and then multiple groups of identities. This can be countered by keeping peers divided into groups. Each peer attaches its group certificate and associates it with its CA.

When a group authority receives blinded credentials of a peer, the authority signs the group certificate after verifying the credentials. However, the authority keeps track of information that can be correlated to certificates of peers. The reputation system is developed in such a way that any peer that involves in malicious practice to improve its reputation will be self destructive as its reputation will really go down. Mathematically P is used to denote peer and A is used to denote authority while Pk2 represents the peer's private key and Pk1 represents the public key of the peer P. Ek(T) represents encryption of the phrase (T) key k . The blinding phrase X with key K is represented by EBk(X).

1. $P \rightarrow A$: $B1 = \{ EB_{Ka}(I_{Alice\ r})\}, I_{Alice}$

The peer Alice generates a BLINDING KEY, K_a and another identity for herself ($I_{Alice\ r}$). Alice cannot be identified from her identity ($I_{Alice\ r}$). Subsequently, she blinds her identity ($I_{Alice\ r}$) with the blinding key K_a. B1 represents the blinded identity. Alice sends B1 to the authority with her real identity that proves her membership to a group.

2. $A \rightarrow P$: $B2 = E_{PAuthority\ k2}\ \{ B1 = EB_{Ka}(I_{Alice\ r})\}$

The authority signs the blinded identity, B1 and sends it (B2) back to the peer.

3. $P: E_{PAuthority\ K2}\{I_{Aclice\ r}\} = \{ EB_{Ka}\{B2\}\}$

The peer unblinds the signed identity and extracts the identity authorized by the authority
$E_{PAuthority\ K2}\ \{ I_{Alice\ r}\}$.
In this approach peers are interested in ranks of the prospective providers. This concept was inspired by Google page rank. When genuine recommendations come from peers in the network, this approach can be argued to be unfair as our experiments revealed that minimal change is there with the ranks of providers.

3.3 Reputation Model

A peer joins the P2P network once it gets identity and then it searches using search method for one or more files. It generates a list of peers who have requested files based on the response to the search. RANGE denotes such peers (providers). A cryptographic protocol (explained in the next section) is initiated by the requester with a peer who has highest reputation. The file is downloaded by requester from provider and its quality, authenticity and integrity are verified. Based on the results, recommendations are sent to the provider. It will be between MIN_RECOMMENDATION and MAX_RECOMMENDATION. Then the provider's overall reputation is recalculated. This process is repeated for every transaction.

3.4 Reputation Exchange Protocol

As soon as requester chooses a provider with highest reputation, it initiates reputation exchange protocol with the provider. The following table shows the symbols used in the equations of the phases in the protocol.

SYMBOL	MEANING
R	Requester
P	Provider
Pk2	Private key of the peer P
Pk1	Public key of the peer P
Ek(T)	Encryption of the phrase T with the key K
EBk(T)	Blinding phrase X with key K
H(λ)	One way hash of the value λ
RTS	Transaction
IDR	Identity Certificate of Requester
IDP	Identity Certificate of Provider
TID	Current transaction ID
LTID	Last transaction ID

The reputation exchange protocol has the following steps.

3.5 Analysis of the Protocol

In the network the provider can give only one search request to gather the suggestions obtained from the source. The foremost difficulty in P2P network is to manage the issue of uneven availability of the peer in the network.

1. The provider deliberately sends the incorrect TID in Step 2. Assume that the id which is sent by the provider be TID0 where as the source last transaction Id be LTID. The TID0 must be same as LTID þ 1. If TID0>LTID þ 1, there will be unsolved lost proposal. If TID0 < LTID þ 1, the provider trapped in Step 4 of the protocol, since the last id utilized by the provider was made a public information and is accessible to all peers. If a peer is having the position of provider for the initial time, at that time TID be 0.
2. In Step 8 the provider cannot end the operation. Only after giving the client the requested file the provider can end the operation in Step 8. In Step 9 the provider can end the operation. In these situations the provider won't have the reference for the id TID. If the provider doesn't sign the sightless proposal that the requester sent her, the requester can free the proposal in Step 11 without taking provider's signature. In the next operation TID þ 1, the provider may not be possible to illustrate the proposal for operation, TID to the requester of transaction, TID þ 1. The new requester will look for the network via search method for TID. If it acquires TID, it will as well as obtain the proposal to the provider in the transaction. The requester is responsible as the TID was signed by the provider. The provider have to agree the proposal as it contain the sign of the provider, TID & EPK2 (H(TID)).

If the provider sends back the signed blinded proposal in Step 10, B1 & EPK2(H(B1)), but the requester do not dispatch the key, K_a and skip to Step 10 lacking the middle steps, then the provider can look for the network and obtain the signed proposal of the requester.

1. Collusion by rogues or liar farms. Every standard systems are disposed to complicity due to the environment of a standard systems. Two or more rogues force scheme in order to enlarge all other status. The crash of complicity can be ease by sorting proposal by uniqueness, by allowing agencies, by time, etc., and recognize the outliers. The catalog of colluders can be available, thereby caring other peers from the damage. Peers have an inspiration next to conspiracy because once recognized they may not able to take part in the network.
2. Multiple requesters and concurrency. In the present protocol, a provider may not be possible to apply the similar uniqueness in simultaneous proposals. The first choice for protocol addition is that the providers bring all its requesters to each other. Consequently, the confirmation in Step 4 is made between the collection of requesters and the outcome is familiar so as to include TID variation due to many requesters. After including the expansions, it would quiet be a bi party protocol where first party is the provider and the collection of requesters is the second party.

3.6 Salient Features of the Protocol

The main features of the protocol are as follows:

The genuine global reputation information with respect to a provider is obtainable to all peers at one place. The provider will not start several search requests in the network with the purpose of gathering the suggestion got by the supplier in the previous. It has to concern one search appeal to regain the last operation information of the

provider it also confirm every proposals of the supplier. It decrease the turnaround time of the transaction but also keep significant volume of resource.

The provider is liable to every older transaction. It cannot spitefully interfere with transaction records by addition or deletion of proposal because the proposals are attached in a series and noticed by the earlier supplicant. The provider can't modify proposals because they are digitally signed by the requesters.

The total information of the provider is saved by the provider itself. The protocol will not have an effect by unreliable accessibility of previous recommenders or other peer in the network. The transaction can be finished productively as long as the requester and the provider connected to the network. If any one left the network it returns and completes the transaction.

The supplicant can't unkindly terminate the transaction in the middle. The requester won't take the service from the provider and then logoff without giving a proposal to the provider.

IV. EXPERIMENTS AND RESULTS

4.1 Evaluation of Self-Certification

For knowing the consequence of the size of network N, the size of group d and the quantity of transactions T, a peer-to-peer network was simulated on the Mean Rank Difference M, designed through the common of rank difference, on the whole of the peers in the network. Either the planned identity methods are used or not, the variation in the rank of peer is the rank difference.

The below two queries are endeavor for answering in particular.

1. Will the mean rank difference a fine interpreter of the rank difference of entity nodes? At what variance the rank difference of entity peers is simulated for a specified value of d? For what fraction of nodes the rank difference is identical to the mean rank difference exactly?
2. Will the mean rank difference influenced by cluster dimension d, network dimension N and the amount of transactions T in the network? **In other words, what is the expected mean rank difference for other network configurations which are different (in terms of size, group size d or number of transactions) than the networks simulated by us?**

The cyber network is composed of 1,000 peers of what the peers will execute 20,000 connections for each case imitation by the cluster dimension d=3. Some inimitable IP addresses will be given to the peers. Moreover all peers will be allocated a righteousness cause for the explanation of the truth that a good-quality peer is expected to partake in top amount of transactions rather than a terrible peer. Therefore, the standing of a superior peer is probable to rise quicker than the standing of a terrible peer. 1 was placed for MAX RECOMMENDATION whereas 2 placed for the value of MIN RECOMMENDATION. It was made to make sure that a peer vanished further standing on executing a malevolent dealing in contrast to the standing get by doing a fine dealing. Besides, the outcome will not be differ a large amount if the selection of the values of MAX RECOMMENDATION as well as MIN RECOMMENDATION for outer surface of [-2, 1]. The fraction of malevolent peers was diversified as of 10% to 90%. The chance which a peer will take advantage of was placed to ½ with the intension of explanation of the truth that in the authentic world truthfulness is unsteady along with the differentiation in time and stakes.

To all iterations of the simulation, a haphazardly chosen peer turns out to be the provider as well as one more haphazardly chosen peer unspecified the position of the supplicant. Following the dealing, the supplicant will be provided an advice to the supplier. For every recommendation the supplier received its standing will get increased with the righteousness cause. When completing 20,000 transactions the calculation to the rank of peers takes place with no use of the planned identity management method (d =3). The variation in the ranks will be standard to every peer on the set of connections and the consequences will be arithmetically examined.

This process will continue for 20 times and so the outcome will be an averaged for each one of the below three situations:

1. The cluster dimension will get differ in between 5 and 50 of which step[5] 5 in addition to the extra strictures which are constant. This instance will allow to examine the influence to be around the mean ranks of the peers,
2. The cluster dimension and the system dimension will be maintained in stable wide-ranging the amount of transactions from 2,000 to 20,000 of which step 2,000 and
3. The amount of transactions along with the cluster dimension will be maintained in stable for 20,000 and 10 correspondingly. Also the system dimension will diverse in between 200 and 1,000 peers of step 200.

Lastly, the mean rank difference was designed to all positions of 20 simulations and was arithmetically examined by the usage of regression analysis, Analysis of Variance test (ANOVA) and T-Test [40] for answers of the above two queries to be worked out.

4.2 Self-Certification Results and Analysis

For the first experiment the values are N=1,000, T=20K and d=3 so that the rank difference to be around the peers was 13:246± 0:81 having 95%self-assurance stage. Even if the outcome of the initial experiment be dissimilar to the standard sharing, it is treated as usually sharing data as indicated by the recommendations of the central limit theorem [41] in support of model dimension greater than 30. It is implied that 68% of the nodes existed in the P2P network posses a rank difference in the span of 13:246±13:07. Out of 1,000 nodes, 680 nodes are with a rank difference under 27. The MRD (Mean Rank Difference) can give good picture of differences in rank of nodes because the standard error for this analysis is very low (_0:4).

Incremental regression analysis is done to answer the second question. An ANOVA test is also done to know the variation in network size, group size, the number of transactions and mean rank difference. When there is change in mean rank difference a change in group size is expected. However, in practical it is not so fact that no factor is having an impact on the mean rank difference. This is considered null hypothesis (H0). Equation given below quantifies the variability of factors with respect to mean rank difference.

Mean Rank Difference ¼ _ þ _1 _ d þ _2 _ N þ _3 _ T:

In ANOVA test the significance F value is zero. Therefore the null hypothesis is not proved. A fact that substantiated the inference was that p values for the coefficients, _1, _2 and _3 and they are extremely low. Thus all values have impact on mean rank difference. The values of coefficients such as _1 ¼ 0:52 _ 0:02; _2 ¼ 0:02; _3 ¼ 0:0008, and _ ¼ _19:5 _ 0:98 at the 95 percent confidence level are not in complete conformance to heuristic. The increase in the number of transactions over network has a minimal impact on the mean rank difference. The mean rank difference is influenced by every new transaction. Therefore, when information is calculated without increasing it, the reputation calculated did not increase.

The value of _2 ¼ 0:02 is not in favor of initial hypothesis the network size may not modify the mean rank difference (Fig.2). To observe why the network size varying the mean rank difference, we must do another test. In these test we make a statement that regardless of status, the probability of a node concerned in transaction is same. Goodness factor of all nodes was made to 1 and bad node and good node have a same likelihood of take part in a specified transaction. According to the hypothesis made in the previous tests wherever a good node was with higher goodness features, is different from the present scenario. Thus, accounting comes into consideration for more number of transactions. The outcome of this test proved it has a slight or no difference in mean rank difference with respect to network size, at the time the chance of taking part of all nodes are equal. From Fig 1 the correlation coefficient (r) was 0.09247. Therefore we conditioned that in the first collection of tests, the raise in the network size elevate the number of extremely presumed nodes or with extreme worth of goodness feature. The status variation among the instances, while projected identity method used and if it is not used superior for the top ranked nodes contrast to the least ranked nodes; therefore, the modification in the rank of top rank nodes is bigger. As a consequence, the mean rank variation of the network will be large.

4.3 Evaluation of the Cryptographic Protocol and the Reputation Model

Protocol estimates suggest 5,000 peers take part in 20,000-140,000 transactions. It has been imagined that every file was obtained with 10 probable providers. The client may not have any awareness of rogue nodes. With a probability of ½ the rogue nodes act that is for all two transactions rogues indignant in one. Every replication is performed five times and the total is averaged. Number of replications made to 5 since the fifth iteration of the replication the average values were more or less stable.

4.3.1 Cumulative and Individual Benefits of Using Reputation

We wanted to quantify the holistic and individualistic benefits of using the proposed reputation model for a P2P network. We measured the change in the number of malicious transactions with an increase in the total number of transactions in the network. The number of rogues was set to a constant at 50 percent and the number of transactions was incrementally raised from 20,000 to 140,000. As is visible in Fig. 3, the total number of malicious transactions increased considerably with an increase in the number of transactions when the proposed model was not used but are more or less constant when the proposed model was used. In the presence of an increasing number of rogues (10-90 percent), when the total number of transactions is constant (¼ 140;000), the rate of increase in the number of malicious transactions was much less when reputations were used (Fig. 3).

Subsequently, we analyzed the experience of each peer when the reputations are not used as compared to when they are used. As visible in Fig. 4, when the reputations were not used, the mean of the number of malicious transactions experienced by each good node was 7:966 _ 5:52 with a 95 percent confidence. This mean drastically reduced, when the reputation model is used, to 0:4 _ 1:2 with a 95 percent confidence. From the first three simulations, we concluded that the proposed model reduces the number of malicious transaction from the perspective of the network and from the perspective of each peer.

Last, the performance of the proposed system was compared with Eigen Trust reported by Kamvar et al. [42]. In order to replicate the simulations performed by Kamvar et al., we set the number of peers to 100 with 40 malicious peers and 60 good peers. The number of transactions was set to 1,500. We did not consider the other parameters mentioned by Kamvar et al. because their strategy encapsulates the search function also but the proposed system is used on top of any search function. The results have been illustrated in Fig. 5. The proposed system is more effective in reducing the number of "inauthentic downloads" or "malicious transactions." In a network where 60 percent nodes are malicious, the proposed system reduces the number of malicious transactions from 15 percent (in Eigen Trust) to 2 percent. Fig. 5 also shows that with an increasing number of malicious nodes in the network, the proposed system increasingly becomes more effective.

4.4 Overall Evaluation of the System

AF (Availability Factor) has been added to each node to evaluate the combined benefit of cryptographic protocol and self-certification. For a given peer, the availability factor accounts for the erratic availability of the past recommenders. All peers are randomly allocated AF value between 50 and 90 percent. With the results of 4.3, the numbers of malicious transactions are compared. As results reveal the number of transactions are same with the combination of self-certification and cryptographic protocol.

V. CONCLUSIONS AND FUTURE WORK

This paper presents a cryptographic protocol, a reputation model, an identity management mechanism and self-certification in P2P networks to provide global reputation data that helps peers to quickly detect rogues. In absence of a centralized CA, the identity generation mechanism that is based on self-certification can reduce the threat of malicious peers involving attacks. The process of identity depends on the ranks of peers rather than their absolute reputation value. The difference in the ranks is nothing but the difference in the security.
In this system, the global reputation data is immune to unauthorized modifications by their owner or peers in the network.

Bandwidth per transaction and the number of malicious transactions are reduced by the proposed protocol. The highly probable erratic availability of peers problem is also handled by the protocol. The present system considers the reputation of provider while ignoring the reputation of requester. It can be improved further in order to consider reputations of both requester and provider. More over the reputation values can be updated as per the context of the reputation.

REFERENCES

[1] H. Garett, "Tragedy of Commons," Science, vol. 162, pp. 1243-1248, 1968.
[2] I. Stoica, R. Morris, D. Liben-Nowell, D. Karger, M.F. Kaashoek, F. Dabek, and H. Balakrishnan, "Chord: A Scalable Peer-to-Peer Lookup Service for Internet Applications," Proc. ACM SIGCOMM, pp. 149-160, Aug. 2002.
[3] S. Ratnasamy, P. Francis, M. Handley, R. Karp, and S. Schenker, "A Scalable Content-Addressable Network," SIGCOMM Computer Comm.. Rev., vol. 31, no. 4, pp. 161-172, 2001.
[4] A. Rowstron and P. Druschel, "Pastry: Scalable, Decentralized Object Location, and Routing for Large-Scale Peer-to-Peer Systems," Proc. IFIP/ACM Int'l Conf. Distributed Systems Platforms (Middleware), pp. 329-350, Nov. 2001.
[5] G. Networks, "Groove Networks," http://www.groove.net/ products/workspace/securitypdf.gtml, 2009.
[6] R.L. Rivest and B. Lampson, "SDSI: A Simple Distributed Security Infrastructure," Proc. Crypto '96, pp. 104-109, Aug. 1996.
[7] N. Li and J.C. Mitchell, "RT: A Role-Based Trust-Management Framework," Proc. Third DARPA Information Survivability Conf. and Exposition (DISCEX III), Apr. 2003.
[8] D. Ferraiolo and R. Kuhn, "Role-Based Access Controls," Proc. 15th Nat'l Computer Security Conf., May 1992.
[9] D. Chaum, "Blind Signatures for Untraceable Payments," Proc. Advances in Cryptology (Crypto '82), 1983.
[10] L. Zhou, F. Schneider, and R. Renesse, "COCA: A Secure Distributed Online Certification Authority," ACM Trans. Computer Systems, vol. 20, no. 4, pp. 329-368, Nov. 2002.
[11] M. Chen and J.P. Singh, "Computing and Using Reputations for Internet ratings," Proc. Third ACM Conf. Electronic Commerce, pp. 154-162, 2001.
[12] P. Resnick, R. Zeckhauser, and E. Friedman, "Reputation Systems," Comm. ACM, vol. 43, pp. 45-48, Dec. 2000.
[13] E. Friedman and P. Resnick, "The Social Cost of Cheap Pseudonyms," J. Economics and Management Strategy, vol. 10, no. 2, pp. 173-199, 2001.
[14] L. Xiong and L. Liu, "PeerTrust: Supporting Reputation-Based Trust in Peer-to-Peer Communities," IEEE Trans. Knowledge and Data Eng., vol. 16, no. 7, pp. 843-857, July 2004.
[15] A. Abdul-Rahman and S. Hailes, "Supporting Trust in Virtual Communities," Proc. Hawaii Int'l Conf. System Sciences, Jan. 2000.
[16] K. Aberer and Z. Despotovic, "Managing Trust in a Peer-2-Peer Information System," Proc. 10th Int'l Conf. Information and Knowledge Management (CIKM '01), pp. 310-317, Nov. 2001.

[17] A.I. Schein, A. Popescul, L.H. Ungar, and D.M. Pennock, "Methods and Metrics for Cold-Start Recommendations," Proc. 25th Ann. Int'l ACM SIGIR Conf. Research and Development in Information Retrieval, pp. 253-260, 2002.
[18] C. Dellarocas, "Immunizing Online Reputation Reporting Systems against Unfair Ratings and Discriminatory Behavior," Proc. ACM Conf. Electronic Commerce, pp. 150-157, Oct. 2000.
[19] C. Dellarocas, Building Trust On-Line: The Design of Reliable Reputation Mechanism for Online Trading Communities. MIT Sloan School of Management, 2001.
[20] E. Damiani, S.D.C. di Vimercati, S. Paraboschi, and P. Samarati, "Managing and Sharing Servents' Reputations in p2p Systems," IEEE Trans. Knowledge and Data Eng., vol. 15, no. 4, pp. 840-854, July 2003.
[21] B.C. Ooi, C.Y. Kiau, and K. Tan, "Managing Trust in Peer-to-Peer Systems Using Reputation-Based Techniques," Proc. Fourth Int'l Conf. Web Age Information Management, Aug. 2003.
[22] L. Liu, S. Zhang, K.D. Ryu, and P. Dasgupta, "R-Chain: A Self- Maintained Reputation Management System in p2p Networks," Proc. 17th Int'l Conf. Parallel and Distributed Computing Systems (PDCS), Nov. 2004.
[23] 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, Aug. 2008.
[24] Z. Xu, Y. He, and L. Deng, "A Multilevel Reputation System for Peer-to-Peer Networks," Proc. Sixth Int'l Conf. Grid and Cooperative Computing (GCC '07), pp. 67-74, 2007.
[25] M. Gupta, P. Judge, and M. Ammar, "A Reputation System for Peer-to-Peer Networks," Proc. 13th Int'l Workshop Network and Operating Systems Support for Digital Audio and Video (NOSSDAV), 2003.
[26] M. Piatek, T. Isdal, A. Krishnamurthy, and T. Anderson, "One Hop Reputations for Peer to Peer File Sharing Workloads," Proc. Fifth USENIX Symp. Networked Systems Design and Implementation (NSDI '08), pp. 1-14, 2008.
[27] J. Douceur, "The Sybil Attack," Proc. IPTPS '02 Workshop, 2002.
[28] M. Castro, P. Druschel, A. Ganesh, A. Rowstron, and D.S. Wallach, "Secure Routing for Structured Peer-to-Peer Overlay Networks," Proc. Fifth Symp. Operating Systems Design and Implementation, pp. 299-314, Winter 2002.
[29] J. Camenisch and E.V. Herreweghen, "Design and Implementation of the Idemix Anonymous Credential System," technical report, IBM Research Division, 2002.
[30] L. Alliance, "Identity Systems and Liberty Specification Version 1.1 Interoperability," Project Report, Liberty Alliance Project, technical report, 2003.
[31] M. Hauswirth, A. Datta, and K. Aberer, "Handling Identity in Peer-to-Peer Systems," Proc. Sixth Int'l Workshop Mobility in Databases and Distributed Systems, in Conjunction with 14th Int'l Conf. Database and Expert Systems Applications, Sept. 2003.
[32] P. Zimmermann, The Official PGP User's Guide. MIT Press, 1995.
[33] P. Dewan, "Injecting Trust in Peer-to-Peer Systems," technical report, Arizona State Univ., 2002.
[34] Clausen, "How Much Does it Cost to Buy a Good Google Pagerank?" unpublished, Oct. 2003.
[35] G. Shafer and J. Pearl, Readings in Uncertain Reasoning. Morgan Kaufmann, 1990.
[36] F.K. Robert and A. Wilson, The MIT Encyclopedia of the Cognitive Sciences (MITECS). Bradford Books, 1999.
[37] D.P. Foster and H.P. Young, "On the Impossibility of Predicting the Behavior of Rational Agents," technical report, John Hopkins Univ., 1999.
[38] T. Rabin and M. Ben-Or, "Verifiable Secret Sharing and Multiparty Protocols with Honest Majority," Proc. 21st Ann. ACM Symp. Theory of Computing, pp. 73-85, 1989.
[39] C. Cachin, K. Kursawe, A. Lysyanskaya, and R. Strobl, "Asynchronous Verifiable Secret Sharing and Proactive Cryptosystems," citeseer.nj.nec.com/cachin02asynchronous.html, 2002.
[40] D.C. Montgomery, Design and Analysis of Experiments. J. Wiley and Sons, 2000.
[41] D. Rumsey, Statistics for Dummies. J. Wiley and Sons, 2003.
[42] S.D. Kamvar, M.T. Schlosser, and H. Garcia-Molina, "The Eigentrust Algorithm for Reputation Management in P2P Networks," Proc. 12th Int'l World Wide Web Conf., pp. 640-651, 2003.
[43] E. Damiani, D. di Vimercati, S. Paraboschi, P. Samarati, and F. Violante, "A Reputation-Based Approach for Choosing Reliable Resources in Peer-to-Peer Networks," Proc. Conf. Computer and Comm. Security (CCS '02). pp. 207-216