

An Effective Calculation of Reputation in P2P Networks

RVVSV Prasad¹ Vegi Srinivas² V.Valli Kumari³ KVSVN Raju³

¹Department of Computer Science and Engineering, Bhimavaram Institute of Engineering and Technology,
Pennada-534243, Bhimavaram, India

²Department of Computer Science and Engineering, Dadi Institute of Engineering and Technology,
Anakapalli-531002, Visakhapatnam, India

³Department of Computer Science and Systems Engineering, College of Engineering,
Andhra University, Visakhapatnam-530003, India.

Email: { ramayanam.prasad, srini.vegi, vallikumari, kvsvn.raju }@gmail.com

Abstract — With the advent of sophisticated networking technologies and the related applications, more and more computers are getting hooked to the Internet. This is mainly for utilizing several services ranging from information sharing to electronic transactions. P2P networks which allow decentralized systems, have posed problems related to trust when transactions have to be carried out. Current literature proposes several solutions for trust management and reputation computation. The solutions base their assessment of reputations on the number of successful transactions or on the similarity of the feedbacks. There are some concerns in the feedback ratings if we are not considering the issues like number of transactions, frequency of transactions with the same peer and different peers, age of transaction, how frequently a given peer attends a common vendor, and the number of common vendors between the pairs. This paper puts forward a reputation computation system addressing these concerns. It implicitly allows detection of malicious peers. It also incorporates a corrective mechanism, if the feedbacks are from more number of malicious peers. The implementations and the results that support our claims are also presented.

Index Terms: trust, reputation, peer-to-peer, transaction, recommender systems, credibility, feedback, similarity.

I. INTRODUCTION

The ever-growing demand for peer-to-peer (P2P) networks for applications like file sharing have led to several concerns among which the issue of trust is predominant. Since the trust is multi-faceted, context specific and dynamic [18], peers need to develop differentiated trust in different aspects of other peer's capability. By providing a mechanism for trust and reputation, we can enable (allow) peers to stand for and bring up to date their trust in other peers in decentralized overlay networks. Such systems typically assign each peer a trust value based on the number of transactions it has done with others and the feedbacks received from them. Most of the existing literature suggests that future development of P2P networks depends on the quality of information

provided. Trust on a peer is represented by a measure by which it combines the overall experience or satisfaction on transactions performed with that peer [12]. Peers are more dynamic in particular when the size of the network increases which alleviates the chance of repeated interactions between the peers. Hence, the transacting peers may not have preceding experience and knowledge about its counterpart. Then the peers must rely on a proper reputation mechanism. Majority of the work published considers that reputation systems are the most preferred when trustworthiness is to be computed. This reputation is usually based on the aggregate of the feedback ratings given by several peers. For instance, Amazon and several other e-commerce applications allow users to post their feedback.

Current literature proposes several solutions for trust management and reputation computation based on recommender systems. The solutions rely on their assessment of reputations on number of successful transactions or on similarity of the feedbacks. Only reliance response ratings are of relevant as the feedback given may not depend on number of transactions, the frequency of transactions done and the age of transactions along with the frequency of peer visiting a vendor and the number of common vendors between the peers. Similarity is another important issue. We normally give more credit to a person's recommendation, if one's interests are more similar to ours. In this paper, we presented a reputation computation system considering these issues.

In the current work, first identifies the similarities between the peers and credibility factor. Second, based on the credibility factor that develop a reputation based trust scheme to calculate in what extent the recommending peer is trustworthy. This system mainly depends on feedback similarity, common vendor similarity, interactions similarity and age of transactions.

However, a few of the reputation management works so far have focused on the vulnerabilities of a reputation system itself [3]. Some of these are (i) malicious peer may strategically alter its behavior after it attains high reputation (ii) malicious peers submit dishonest feedback (iii) malicious peers can flood numerous fake feedbacks through fake transactions in transaction based feedback system. Most of the existing reputation systems [4] lack the ability to differentiate dishonest feedback from honest ones and provide no support to incorporate various contexts in evaluating the trustworthiness of peers.

Due to the decentralized nature, trust establishment in P2P systems have to necessarily rely on the collaboration among all of the members [6]. Since there is no centralized peer to serve an authority to supervise peer's behavior and punish peers that behave badly [2]. Some peers might be benevolent in providing services because they are heterogeneous. Peers can also misbehave in different ways [5], such as serving corrupted or low-quality trust data. For the peers to behave honestly, trust needs to be incorporated. Also the trust framework should enable assessing the peers based on the services provided by them.

The paper is organized as follows. Section II gives the related work; Section III covers the details of the proposed reputation system. Section IV presents the results, and Section V concludes the paper.

II. RELATED WORK

Abdul-Rahman and Hailes [1] proposed a model for computing the trust for an agent in a specific context based on the experience and recommendations, which was the basis for many recent papers. Sabater and Sierra [9] review some works regarding reputation as a method for creating trust from the agent related perspective. Reputation is what is generally said or believed about a person's or thing's character or standing. Reputation can be considered as a collective measure of trustworthiness (in the sense of reliability) based on the referrals or ratings from members in a community [8].

Several models discussed in [6] are based on boolean relations or fuzzy logic, techniques to analyse unfair behaviour, models based on Eigen trust algorithms [10], Bayesian systems, discrete models [7] and trust propagation schemes. Xiong and Liu [4, 5] give a reputation based trust supporting framework-*peer trust*. They define a trust metric based on three parameters: (i) feedback a peer receives from other peers, (ii) the total number of transactions a peer performs, (iii) the credibility of the feedback sources

and two adaptive factors (context factor and community context factor). They also identify that previous literature is based on two assumptions as below and that the second one need not be true:

- (i) Untrustworthy peers have a higher probability of submitting false or misleading feedback in order to hide their own malicious behavior.
- (ii) Trustworthy peers are believed to be honest with a high probability on the feedback they provide.

So, they came out with another trust metric based on querying peer's personalized experience.

Existing reputation based trust management frameworks are built on collecting and aggregating the feedback ratings reported by the service consumers. Therefore, the reliability of reputation evaluation mainly depends on the integrity and the accuracy of the reported feedback ratings [7]. As a kind of unfair ratings prejudicial feedbacks will obviously reduce the accuracy of the reputation evaluation in the situation that the feedback data are lacking and insufficient. They cannot deal with strategic dynamic personality of peers. Giorgos Zacharia [13] proposed a reputation mechanism that rely on collaborative ratings and personalized evaluation of the various ratings assigned to the user (peer). This collaborative filtering technique is used to detect patterns among the feedbacks of different users (peers) to make recommendation to peers, based on others who have shown similar taste.

Srivatsa *et. al.*, [3] proposed *Trustguard*, a highly dependable reputation-based trust building framework, which focused on vulnerabilities of a reputation system, like fake transactions, dishonest feedback etc. Bin Yu and Munindar P.Singh [14] develop an evidential model of reputation management based on Dempster-Shafer theory. According to this paper, if no information about the peer is available, it has no reputation at all. It should be noted that there is a difference between having a bad reputation and no reputation at all. R. Aringhieri *et. al.*, [15] addresses two challenges in designing a reputation management system of anonymous P2P networks. First, the design of protocol able to provide secure placement of reputation information. Second, defining a suitable means to represent reputations and synthesizing a set of opinions collected by the protocol in a unique aggregated value.

Work in reputation based trust is essential to identify the correct recommender. One solution to obtain this is to consult a central trusted third party that has had previous experience with the agent and can provide a reputation value. Centralized control of reputation data makes the reputation management systems vulnerable

to a variety of failures. A decentralized P2P trust management system aims at reducing or avoiding single point of failure and increasing scalability of the system performance [5].

Selection of recommender based on short term reputations is highly undesirable and providing reliable reputation ratings is also a big problem for unknown peers or newcomers. Gayatri Swamynathan *et. al.*, [16] addressed this and proposed an idea of proactive reputation, which allow peers to proactively initiate transactions with one or more peers for the express purpose of generating reputation ratings. However, for the processing of proactive requests to be fair and non-biased, anonymity of transaction is required; the receiver must not be able to identify the request initiator. Initializing the transactions lead to bandwidth overhead. Ronald Ashri *et. al.*, [17] addressed the same issue in two different perspectives. First, if the peer interacts with each peer inevitably risks making losses if the counterparts it interacts with are not trustworthy. Secondly, if the peer relies on reputation information, then it cannot be sure that the agents providing the information are doing so truthfully. They developed a methodology for peers to dynamically identify relationships between the transacted peers and then using this information to enhance trust valuations.

Reputation systems produce an entity's (public) reputation score as seen by the whole community. There can be distributed stores where ratings can be submitted, or each participant simply records the opinion about each experience with other parties, and provides this information on request from relying parties. According to Kamvar *et al.* [10], the following issues are important in P2P reputation system: (i) self-policing where no central authority should exist and the peers should enforce the ethical behavior by themselves, (ii) anonymity which means peer reputation should be associated with an opaque identifier, (iii) the system should not assign profit to newcomers, (iv) minimal overhead and (v) robust to malicious collectives of peers.

The reputation system proposed in this paper is based on a file sharing system in P2P network. Each peer plays two roles, the role of file provider offering files to other peers and the role of user using files provided by other peers. In order to distinguish this, when a peer acts as a file provider we call it service provider and otherwise simply as an agent or a consumer. In the trust computation scenario, each provider has reputation which is an aggregate of feedbacks (ratings) given by other consumer peers. Every consumer peer has a rating capability to rate the providers. If a particular agent does not have any experience with the file provider, it would ask other

agents' who had interaction with the file provider with the same criteria. In this way it can take a decision on its own rather than depending on centralized system.

Trust plays a major role in several application areas. It is not a new research topic in computer science, spanning areas such as security and access control in computer networks, reliability in distributed systems, and recommendations in recommender systems. The concept of trust in these different areas differs in how it is evaluated, represented and used. Though this paper is based on Peertrust of Xiong and Liu [4,5], we proposed a different approach by calculating the similarity between the peers which provide feedback in different aspects like number of interactions, assessment of feedback for the same service and the number of common vendors they have. We developed a reputation system adaptable to dynamics and robustness. To build the trust dynamically we compute the satisfaction values considering the 'age of transaction'. For the later, detection of malicious peers can be identified and omitted by comparing their feedback ratings against their interactions.

III. REPUTATION SYSTEM

The use of reputation system can help applications preserve correct operation despite the presence of malicious peers. Trust can be obtained by a peer's belief in another peer's capabilities, honesty and reliability based on its own direct experiences. But it is not possible to compute the trust of a peer if it hasn't any such direct experiences which can be caused in either one or both of the following situations:

- (i) For the peers in large scale P2P networks it is less likely or zero of their own direct experiences with other peers.
- (ii) New peers are entered in to the dynamically growing P2P network whose experience with the existing peers is absolutely void.

Since it is not possible to calculate the trust of a peer without its direct experiences with other peers, we can rely on its reputation from other peers to compute its trustworthiness. The trustworthiness of any peer is viewed as the expectations of cooperative behavior from that peer. The reputation can be measured for the new peers only after having atleast one experience (interaction) with atleast one peer.

Reputation Systems provide a way for building trust without trusted third parties in P2P networks. Most research on reputation-based trust utilizes the information such as community-based feedbacks about

the past experiences and judgment on quality and reliability of the transactions.

There is always a puzzle for the peer to whom it would interact to get the feedback from other peers. To address this, we present a solution for calculating the credibility of a peer by considering the satisfaction, age of transaction and similarity. Exclusion of malicious peers' feedback by a detection mechanism is also incorporated.

A. Satisfaction

Trust is believed to be subjective and that it cannot be calculated directly [2]. In electronic communities it is computed based on successful transactions. The model discussed in this paper suits any electronic commerce scenario, with the exemption that the explanation is based on a file provider-consumer application. The application as introduced in section II has peers assuming two roles of that of a file service provider/vendor and a file consumer. Any peer can act as either the file provider or as a consumer, but not both at the same point of time. The consumer gives ratings to the providers from whom the services were consumed. The ratings may be based on download speed, quality or on number of transactions done. An aggregate of these ratings gives the reputation of a particular file provider. The terminology used in the remaining sections is given below [11].

Target (T) is a peer with which transaction is to be performed.

Requester (Q) is a peer which wants to do transaction with the target.

Recommender (R) is a peer which had transactions with the target and is providing feedback to the requester.

Vendor (V) is a peer with which both requester and recommender have transactions.

Feedback (f) is defined as the ratio of satisfaction and the number of transactions performed. Satisfaction normally depends on the content quality, quality of service etc. Requester requests the recommender for information about the target. The recommender provides feedback based on the transactions it has performed with the target.

Reputation (Re) is defined as the combined feedback that other peers give to a particular peer. Reputation and feedback can be measured.

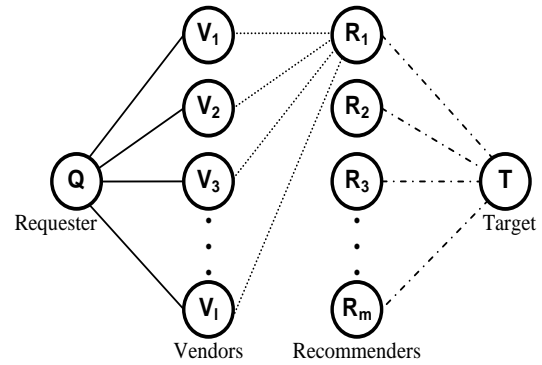


Fig. 1. Reputation in Peer to Peer Network

In the Fig. 1, Q is the requester, T is the target, R₁, R₂, R₃..., R_m are recommenders and V₁, V₂, V₃..., V_i are the vendors with whom R₁ and Q have had interactions with.

Let *j* and *k* be any two peers, then feedback (*f*) about *j* given by *k* is represented by *f_{jk}* and is computed as below.

$$f_{jk} = \frac{\sum_{i=1}^n S_{jki}}{n} \tag{1}$$

where *n* is the total number of transactions performed by *k* with *j*. *S_{jki}* represents the satisfaction of *k* on *j* in *i*th transaction. This measure is assigned by the peer based on the quality of the transaction and its value is always assumed to be between 0 (*not satisfied*) and 1 (*completely satisfied*).

Assume a peer Q wants to do transaction with a peer T as in figure 1. Trust of Q on T is usually based on the number of successful transactions done. If in the first few interactions there is no sufficient information to determine trust, Q computes reputation of T and determines if further transactions can be done or not.

Let R₁ and Q be two peers who have transactions with set of peers V₁, V₂, V₃, ..., V_i. The feedbacks given by R₁ and Q are shown in Table 1.

Table1. Feedbacks given by R₁ and Q

Peers	V ₁	V ₂	...	V _i	T
R ₁	<i>f_{V₁R₁}</i>	<i>f_{V₂R₁}</i>	...	<i>f_{V_iR₁}</i>	<i>f_{TR₁}</i>
Q	<i>f_{V₁Q}</i>	<i>f_{V₂Q}</i>	...	<i>f_{V_iQ}</i>	Nil

A good feedback on T by R₁ means that R₁ has good trust on T. There are two cases in which the recommender R₁ may give wrong feedback about target T to the requester Q. First, if R₁ wants to boost the product related to T then it may exaggerate its feedback (to a value often more than its actual trust value) or may downgrade by giving wrong feedback (to a value often less than its actual trust value). In both the cases R₁ is said to be behaving maliciously. A peer is rated as a good peer if it gives correct feedback. If a peer gives feedback which does not reflect its trust then it is called as a malicious peer. Feedback given by good peer is to be given high weightage and that by a malicious peer should be given low weightage. Trust of a peer about another given peer is known to itself and if not communicated is unknown to other peers. Hence, it is difficult to say whether a peer is good or malicious. To overcome this problem, we calculate the credibility of a peer that is giving feedback about a given target.

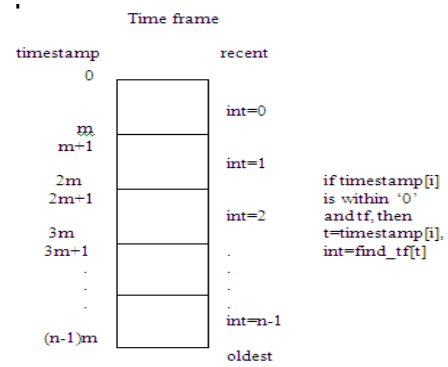
B. Age of transaction

In equation (1), an equal importance is given to the satisfaction values due to the most recent transactions as well as the oldest transactions. While in [3] different weights were attached to the satisfaction values, we suggest another addition to the above equation to show the difference between the most recently performed transaction and not so recently performed transaction. Assume *int* is an interval representing a set of transactions performed during a time period. Let *int=0* represent the most recent period and *int=1* be the next recent period. Assume the *i*th transaction was performed in an interval *int*. Then its corresponding *S_{jk_i}* is adjusted according to the following equation.

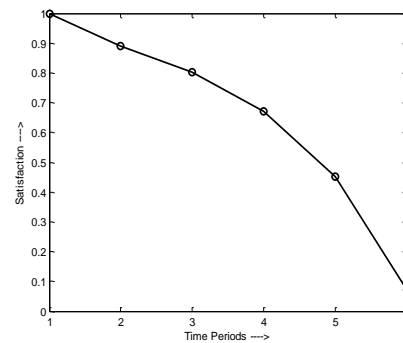
$$f_{jk} = \frac{\sum_{i=1,n} \int_{int=0,|tf|} \left[\frac{(t-2^{int})+1}{t} \right] * S_{jk_i}}{n} \quad (2)$$

where 't' stands for timestamp which represents the exact time taken when the transaction was performed, 'tf' for timeframe where the considerable past time is categorized into intervals 'int' numbered from 0 to |tf| onwards.

Equation (2) allows graceful reduction of feedback ratings as they get old. Figure 2(b) shows how a satisfaction rating fades with time. The significance is that the recent ratings overweigh the past ratings. The advantages are twofold: (i) the recent feedbacks are given more importance and hence, (ii) reputation computation gets more dynamic.



(a)



(b)

Fig.2. Time based satisfaction (a) weight computation for adjusting feedback with time, (b) Fading weight of satisfaction against time.

C. Similarity

Similarity is measured based on i) interactions, ii) feedback, and iii) common vendors.

C.1. Interactions

Similarity between a Requester and a Recommender can be calculated based on the number of transactions done with a common vendor. The more frequently two customers visit a common vendor, the more similar they are. Based on this assumption, we compute a similarity measure considering the number of transactions done with a common vendor.

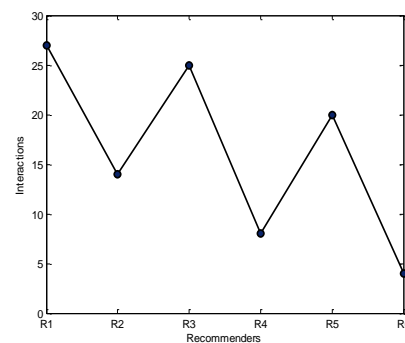


Fig.3. Number of interactions done by the Recommenders with a specific vendor.

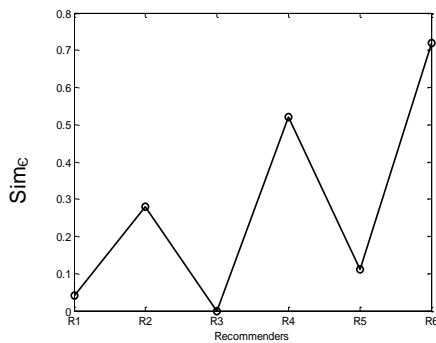


Fig.4. Similarity of the recommenders with a specific vendor for the number of interactions given in figure 3.

Let $I_{(Q,V)}$ and $I_{(R,V)}$ be the number of interactions (transactions) performed with V by Q and R respectively. This means Q and R have had at least one transaction with V. Then Sim_e , the similarity of interactions between Q and R is computed as:

$$Sim_e = \frac{|I_{(Q,V)} - I_{(R,V)}|}{I_{(Q,V)} + I_{(R,V)}} \quad (3)$$

where $0 \leq Sim_e \leq 1$. This equation is used to measure the relatedness between the requester and recommender in terms of interactions.

If the value of Sim_e is '0', then the peers Q and R are exactly similar and if it tends towards '1' then they are considered as dissimilar. For example, if peers A and B are having '70' and '45' interactions with a common vendor respectively, then the value of Sim_e is 0.2174, which is always in between 0 and 1.

If the value of Sim_e is nearer to '0' and less than the given threshold value, we conclude both peers are similar. Depending on the application the threshold value may be assumed. It is obvious that if none of the interactions are made by its counterpart then the two peers are absolutely dissimilar.

However, when the number of interactions is less we consider just the feedback and common vendor similarity.

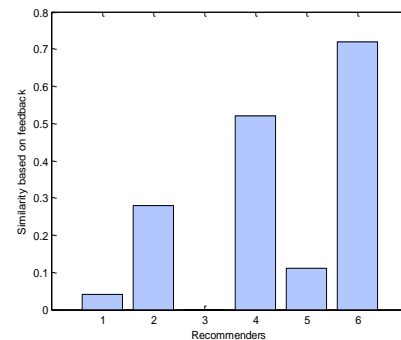
C.2. Feedback

Distance vector can be used to find relationship between two peers and assessment about the same service. If the distance vector yields a small value then their assessment is assumed to be similar. If the distance vector yields a large value then their assessment is thought to be dissimilar.

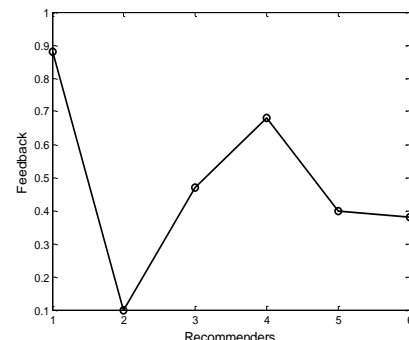
Sim_F has value between 0 and 1 for 'N' common vendors and is computed as:

$$Sim_F = \sqrt{\frac{\sum_{i=1}^N (f_{v_i R_1} - f_{v_i Q})^2}{N}} \quad (4)$$

This equation helps to calculate the similarity between requester and recommender in assessment of a particular service.



(a)



(b)

Fig.5.(a) Similarity versus Recommenders based on feedback (b) Feedback versus Recommenders

If Sim_F is small then assessment of R_1 and Q are similar. Otherwise, If Sim_F is large then assessment of R_1 and Q is dissimilar. Based on the application the threshold values α and β are defined such that $0 < \alpha < \beta < 1$. The values of these thresholds are defined based on the three ranges. If $0 < Sim_F < \alpha$, then Sim_F is small hence the objects on which it is computed are assumed to be similar. If $\alpha < Sim_F < \beta$, then the similarity cannot be defined, hence we go for correlation measure. If $\beta < Sim_F < 1$, then the objects are assumed to be dissimilar.

C.3. Common vendors

The more the number of common vendors for a given pair of peers, the more similar they are. If NV_R , NV_Q are the number of vendors with which R and Q have transacted respectively, the common vendor similarity is given by the following equation.

$$Sim_{cv} = \frac{2 * |NV_R - NV_Q|}{NV_R + NV_Q + 2 * |NV_R - NV_Q|} \quad (5)$$

$|NV_R - NV_Q|$ is the number of common vendors of Recommender and Requester. $NV_R + NV_Q$ is the number of individual vendors of Recommender and Requester and these many not be common to both. This equation gives the resemblance between the requester and recommender on their preferences of making transactions with the common vendors.

D. Detection and correction of malicious peers' feedback

Detection of malicious peers is possible in our approach. If the number of interactions with a vendor is more but the feedback given is low, the peer may be suspected. Hence, all such peers' feedback is excluded when reputation of a target is computed. Assume 'Q' has 25 interactions with the common vendor and has given an overall feedback rating of 0.6. Let the interactions and feedback ratings of the recommenders R1 through R6 about that specific common vendor be as given in Table.2

Table 2. Finding malicious peers

Recommenders	Interactions	Feedback
R1	27	0.04
R2	14	0.28
R3	25	0.06
R4	8	0.52
R5	20	0.11
R6	4	0.72

R6 and R4 are more similar to Q when feedback similarity is considered. R1, R3 and R5 have performed more interactions with the vendor. R1 and R3 give a low feedback even though they have had many interactions with the vendor. Hence, we filter out feedbacks due to recommenders who interacted more and return a low feedback value.

E. Credibility

Credibility gives a measure of the extent to which the feedback given by a peer is dependable. The equation (6) is used to compute the credibility of the recommender by considering the feedback similarity and common vendor similarity.

$$Cr = (1 - Sim_F) * Sim_{CV} \tag{6}$$

The more similar the feedbacks are and the more the number of common vendors, the better is that peers' credibility.

If the same feedback, for example 0.72 is propagated by all the recommenders, it is to be readjusted with the credibility of each individual recommender. The readjusted feedback is shown below in the Table. 3.

Table 3. Transformation of feedback values with respect the credibility of the recommenders.

Recommenders	Credibility (in %)	Readjusted feedback
R1	60	0.432
R2	25	0.180
R3	0	0.000
R4	50	0.36
R5	100	0.720
R6	40	0.288

F. Reputation

Reputation is the amount of trust inspired by a particular person in a specific setting or domain of interest. Reputation can relate to a group or to an individual. A group's reputation can be modeled as the average of all its members' individual reputations, or as the average of how the group is perceived as a whole by external parties.

Let $Rep_{R_1R_2}$ represent reputation of R_1 with respect to R_2 . $Rep_{R_1R_2}$ may not be equal to $Rep_{R_1R_3}$. Let 'N' be the number of peers which have been already interacted with R_1 and peers be $\{V_1, V_2, V_3, \dots, V_N\}$.

$$Rep_{R_1R_2} = \frac{\sum_{i=1}^N (f_{R_1V_i} \times Cr_{R_2V_i})}{\sum_{i=1}^N Cr_{R_2V_i}} \tag{7}$$

$$Rep_{adj_{R_1R_2}} = \frac{\sum_{i=1}^N (f_{R_1V_i} \times Cr_{R_2V_i}^\rho)}{\sum_{i=1}^N Cr_{R_2V_i}^\rho} \tag{8}$$

Cr_{R_1Q} represents the credibility factor of R_1 with respect to Q and its value is between 0 and 1. The inclusion of ρ results in minimizing the participation of low credibility peers in the reputation computation. ρ is a value greater than 0 and depends on the application. If ρ is 1, then the feedback is weighted according to the credibility of the specified peer. In this case, even though a peer with high credibility gives a positive feedback, if several low credibility peers give negative feedback, the reputation will deviate more from the high credibility peer's recommendation.

Hence, in a given scenario, if all are highly credible peers, equation (7) may be used directly for reputation computation. But if there is a considerable number of peers who are malicious or have low credibility, and less number of peers with high credibility, equation (8) may be used and ρ may be assigned with a value greater than or equal to 2. This would minimize the feedback of malicious peers on the reputation computation.

The algorithms we used for above computations are presented below:

Let $V = \{V_1, V_2, V_3, \dots, V_n\}$ are the Vendors and let $R = \{R_1, R_2, R_3, \dots, R_n\}$ are the Recommenders, Q is the Requester, S is the satisfaction value and n is the number of transactions. If there is an edge between V and R and $V_i = Vendors(R_i), V_j = Vendors(R_j)$ then the number of Vendors of R is $NV_R = V_i \cap V_j$ where $R_i, R_j \subseteq R$.

Algorithm1: Age_of_transaction (S,N)

/* This algorithm is used to calculate the difference between the most recent transaction and not so recently performed transaction. Here S is the satisfaction value, N is the number of Common Vendors and f is the feedback */

Input: S, N Output: f

Step 1: Let t be the timestamp

Step 2: Let tv is the transaction value

Step 3: Timeframe(tf) = $\{0, m\}, \{m+1, 2m\}, \dots, \{n-m-1, (n-m-1)+1\}$ where $n, m \in t$

Step 4: Time is categorized into intervals, $int \in tf$

Step 5: If int is in between 0 and tf , then $tv := tv + (t - 2^{int}) + 1/t$, where $t \in tf$

Step 6: Compute feedback(f) := $(tv * S)/N$

Step 7: end.

Algorithm 2: Feedback_Similarity(R,V,Q)

/* This algorithm is used to find the similarity assessment between two peers about the same service. Here Sim_f is the feedback similarity */

Input: R, V, Q Output: Sim_f

Step 1: $f \in [0, 1]$

Step 2: $\exists R_i, \forall V_j$, then $f_{R_i \cap V_j} \in [0, 1]$

Step 3: $\exists Q, \forall V_j$, then $f_{Q \cap V_j} \in [0, 1]$

Step 4: Sim_f is the ratio of square root of the sum of the squares of the deviations of $f_{R_i \cap V_j}$ and $f_{Q \cap V_j}$ to the number of common vendors

Step 5: end.

Algorithm 3: CommonVendor_Similarity (Q,R)

/* This algorithm is used to calculate the common vendor similarity between Recommender and Requester. Here Sim_{CV} is the Common Vendor similarity and NV_R, NV_Q are the number of vendors of Recommender and Requester respectively */

Input: NV_R, NV_Q Output: Sim_{CV}

Step 1: $NV_R \in Z^+$

Step 2: $NV_Q \in Z^+$, where Z^+ is the positive integer values

Step 3: Compute Sim_{CV} is the ratio of twice the absolute difference of NV_R and NV_Q to the sum of NV_R and NV_Q and twice the absolute difference of NV_R and NV_Q

Step 4: end.

Algorithm 4: Reputation_Calculation(R,V,Q)

/* Algorithm to represent Reputation of one recommender with respect to another. Here C_r is Credibility and $Rep_{R_1 R_2}$ is the Reputation of R_1 with respect to R_2 */

Input: R, V, C_r Output: $Rep_{R_1 R_2}$

Step 1: $\exists R_1, \forall V_i$, then $f_{R_1 \cap V_i} \in [0, 1]$

Step 2: $\exists R_2, \forall V_i$, then $Cr_{R_2 \cap V_i} \in [0, 1]$

Step 3: Compute $Rep_{R_1 R_2}$ is the ratio of sum of the products of $f_{R_1 \cap V_i}$ and $Cr_{R_2 \cap V_i}$ to the sum of $Cr_{R_2 \cap V_i}$

Step 4: end

Algorithm 5: Reputation_adjustment (V,R)

/* This algorithm is used to minimize the participation of low credibility peers in the reputation computation. Here f is the feedback and Cr is the Credibility */

Input: R, V, Cr, ρ Output: $Rep_{R_1 R_2}$

Step 1: $\exists R_1, \forall V_i$, then $f_{R_1 \cap V_i} \in [0, 1]$

Step 2: $\exists R_2, \forall V_i$, then $Cr_{R_2 \cap V_i}^\rho \in [0, 1]$, where $\rho > 0$

Step 3: Compute $Rep_{R_1 R_2}$ is the ratio of sum of the products of $f_{R_1 \cap V_i}$ and $Cr_{R_2 \cap V_i}^\rho$ to the sum of $Cr_{R_2 \cap V_i}^\rho$

Step 4: end

Fig.6. Algorithms used for calculating age of transaction, feedback similarity, common vendor similarity, reputation computation and reputation adjustment.

IV. ANALYSIS OF RESULTS

The model was implemented in JADE (Java Agent DEvelopment Framework), a middleware for the development of distributed multi agent applications fully implemented in Java language based on the peer-to-peer communication architecture. Agents never interact through method calls but rather by exchanging asynchronous messages. Thus, each agent has a mailbox where the JADE run-time posts messages sent by other agents. Whenever a message is posted in the mailbox message queue the receiving agent is notified.

The number of peers was initially varied from 10 to 100. Each peer was programmed to behave like a file provider as well as a consumer. The requester Q initially broadcasts its request about feedback on T . The peers (Recommenders) that have already had transactions with T respond. Any peer which has zero interactions will be ignored from the recommenders, if

they respond. The recommenders send the list of vendors they have had transactions with, along with ratings(feedback) about each of those vendors. Q finds a list of common vendors with each recommender and computes similarity between itself and the recommender. The extent of similarity is taken for computing the credibility. The feedbacks of the recommenders are now adjusted according to their credibility and may not be considered if the credibility is zero. Also we are able to identify the suspected recommender whose feedback is proportionally not coinciding with the remaining recommenders and such recommenders are excluded.

While most of the studies carried out in literature base their discussion of reputation on malicious peers' behavior, we base our discussion on the numbers of malicious peers contributing in reputation computation. The equation given in (8) allows minimizing malicious peers contribution by adjusting the value of ρ . In the real electronic communities correcting the malicious peers behavior is practically difficult. Instead of correcting each such malicious peer, if their impact can be minimized, it would be more practical.

In the simulations carried out, feedback ratings for a good peer were collected. It was assumed that malicious peers give bad ratings and good peers always give good ratings. Several simulations have been carried out on peers numbering from 100 to 10000, for varying values of ρ , and varying percentages of malicious peers. The results are shown in the following graphs. Figs. 6 to 8 show the varying reputation, when ρ is varied from 1 to 5. When $\rho = 1$, credibility is taken as it is. When $\rho = 2$ to 5, credibility of a given malicious peer reduces drastically. When $\rho = 5$, least weightage is given to the malicious peers' feedback. Now the question arises as to which peer should be treated as a malicious peer. The simulation experiment has generated feedbacks, such that 90%, 75%, 50%, and 0% peers are malicious. A peer was treated to be malicious if its credibility fell below 0.5.

In Fig. 9 all the peers were assumed to be good peers. The reputation computed for varying values of ρ was the same.

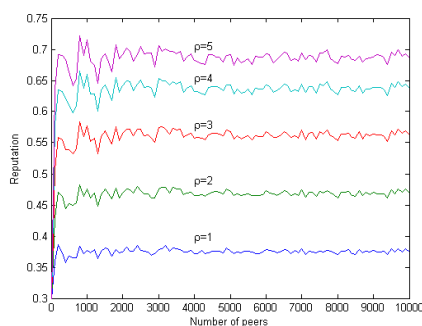


Fig. 6. Reputation with 90% Malicious Peers

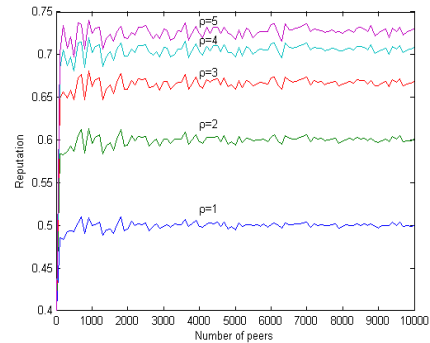


Fig. 7. Reputation with 75% Malicious Peers

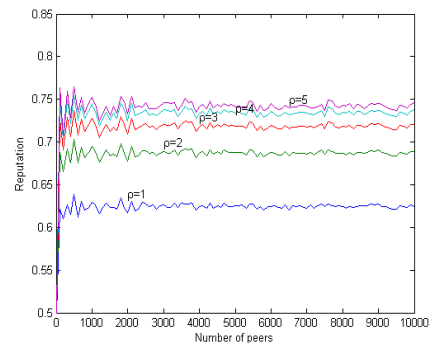


Fig. 8. Reputation with 50% Malicious Peers

In Fig. 10, a comparison of the reputation when computed with varying sizes of malicious peers is plotted.

The following were the observations made from the above plots. When the all the peers are good, irrespective of the value of ρ , the reputation is the same. So, no correction needs to be done. But if it is known for a given application that the most of the peers are malicious, the value for ρ may be high. If it is known that the peers are a mixture of both malicious and good in same proportions, ρ may be fixed to 3. If it is believed that all are good peers, then $\rho = 1$. So, the correction is done based on the electronic communities in general and is not specific to a particular malicious peer.

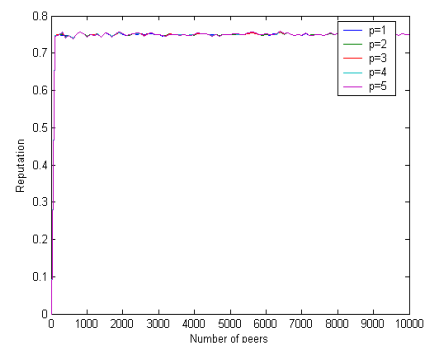


Fig. 9. Reputation with 0% Malicious Peers

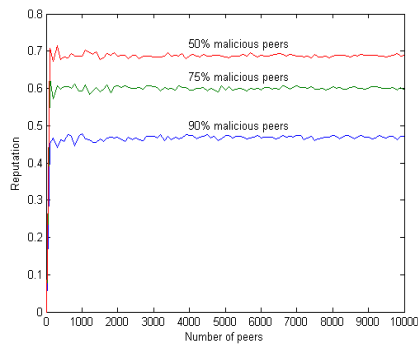
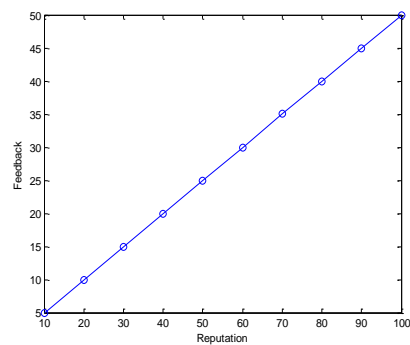
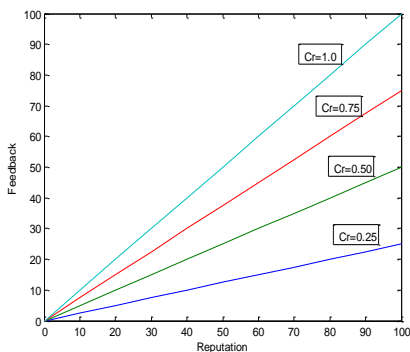


Fig. 10. Comparison of varying Reputation for 90% 75% 50% Malicious Peers when $\rho=1$

The reputation of any peer is merely depending on its feedback. If the feedback is more high (means in the positive sense) the reputation of that peer is also high. Therefore the feedback and reputation are proportionate to each other as shown by the Fig. 11(a). For effective calculation of reputation we calculate the credibility of recommender who is giving the feedback of target peer (T) to requester peer (Q). Fig.11 (b) demonstrates how the reputation will change after calculating the credibility of a recommender (peer). This is because the feedbacks are recomputed by incorporate the credibility of the peer by whom they were given



(a)



(b)

Fig. 11 Relationship between reputation and feedback. (a)before considering the recommenders credibility (b)after considering the credibility of given recommender.

A. Comparison with existing approaches

The model proposed by Abdul-Rahman and Hailes is only suited in a specific context and the trust computation is not dynamic. Our system can be used to compute the reputation for any context. The model 'Peer Trust' gives equal weightage for new and old transactions. To compute the reputation more dynamically, we consider the age of transaction to give more weightage to recent transactions than the old. The 'Trust Guard' proposed an algorithm to filter out dishonest feedbacks made by collusive malicious nodes only. In our system, a detection mechanism is established to identify and to exclude all kinds of malicious peers. Models in [6][10][7] and [3] are computing the reputation based on the recommenders' feedbacks without considering their credibility. We compute the credibility of every recommender and adjust their feedback ratings proportional to their credibility and recomputed the reputation.

V. CONCLUSION AND FUTURE WORK

Past transactions and profiles of recommenders help in determining the reputation of a given peer. Feedback based reputation computation is mostly used in electronic communities. But much of the published work is based on considering an aggregate of weighted feedback. Most of the papers consider correction of malicious peers by giving incentives for positive feedbacks. This paper addresses the issue in a different perspective. We put forward the corrective mechanisms that are close to reality and that people normally use in daily transactions. When a peer is malicious, correcting him takes a high effort and more storage overheads. Even if, a peer is corrected, there is no guarantee that in the next rating, feedback is given honestly. Moreover, a few peers give malicious feedbacks intentionally, and yet a few more may give wrong feedbacks unintentionally. In electronic communities there may be several peers who should be monitored constantly. So, it is felt that that such a mechanism is not feasible practically. In real scenarios, the number of times an agent visits and does interactions with a vendor shows his satisfaction with the vendor. As the transaction gets older the rating gets faded away and satisfaction due to recent transactions are considered for evaluating a given vendor. In this paper, we apply a similar strategy to solve the reputation computation problem. The mechanism suggested in the paper considers the communities in general, and allows reputation correction based on the type of community the particular peer belongs to. The simulation results that support our claims have been presented.

The possible extensions for this work could be in the direction of improving the credibility computation based on context.

Acknowledgements

The authors would like to acknowledge the helpful comments made by the anonymous reviewers which helped in improving the presentation.

REFERENCES

- [1] Abdul-Rahman, A. and Hailes, S., "Using recommendations for managing trust in distributed systems," *Proceedings of the IEEE International Conference on Communication*, 1997.
- [2] Wang, Y. and Vassileva J., "Bayesian network trust model in peer-to-peer networks," *Proceedings of the 2nd International Workshop Peers and Peer-to-Peer Computing*, Melbourne, Australia, 2003.
- [3] Srivatsa, M., Xiong L. and Liu L., "Trustguard: Countering vulnerabilities in reputation management for decentralized overlay networks," *Proceedings of the 14th International Conference of World Wide Web*, pp.422-431, 2005.
- [4] Xiong L. and Liu L., "Peertrust: Supporting reputation based trust of peer-to-peer electronic communities," *IEEE Trans. on Knowledge and Data Engineering*, 16(7):843-857, Jul. 2004.
- [5] Xiong L. and Liu L., "Building trust in decentralized peer-to-peer electronic communities," *Proceedings of the International Conference on Electronic Commerce Research (ICECR-5)*, 2004.
- [6] Zhu B., Jajodia S. and Kankanhalli M.S., "Building trust in peer-to-peer systems: A review," *International Journal on Security and Networks*, Vol. 1, Nos.1/2, pp.103-112, 2006.
- [7] Yanzhon Zou, Liang Gu, Ge Li, Bing Xie, Hong Mei, "Rectifying Prejudicial Feedback Ratings in Reputation based trust management", *IEEE International Conference on Services Computing (SCC 2007)* pp.530-535.
- [8] Audun Jøsang, Roslan Ismail, and Colin Boyd "A Survey of Trust and Reputation Systems for Online Service Provision", *Decision Support Systems*, 43(2) 2007, p.618-644.
- [9] J. Sabater and C. Sierra. "Review on computational trust and reputation models", *Artif. Intell. Rev.*, 24(1):33-60, 2005.
- [10] S.D. Kamvar, M.T. Schlosser, and H. Garcia-Molina. "The eigen trust algorithm for reputation management in p2p networks". In *WWW '03: Proceedings of the 12th international conference on World Wide Web*, pages 640-651, New York, NY, USA, 2003. ACM Press.
- [11] V. Valli Kumari, B. Dinesh Reddy, T. Sri Devi, Ramaprasad R. Kalidindi and KVSVN Raju. "Credibility Based Corrective Mechanism for Reputation Computation in Peer-to-Peer Communities", *IJCSNS International Journal of Computer Science and Network Security*, VOL.8 No.5, pp 95-101, May 2008.
- [12] RVVSV Prasad, Vegi Srinivas, V. Valli kumari and KVSVN Raju, "Credibility based reputation calculation in P2P networks", *Springer-Verlag Berlin Heidelberg 2008, ICDCIT 2008, LNCS 5375*, pp. 188-195, 2008.
- [13] Giorgos Zacharia, "Trust management through reputation mechanisms", *Applied Artificial Intelligence*, Volume 14, issue 9, October 2000, 881-907.
- [14] Bin Yu and Munindar P. Singh, "An Evidential Model of Distributed Reputation Management", *AAMAS'02*, July 15-19, 2002, ACM 1-58113-480-0/02/2007.
- [15] R. Aringhieri, E. Damiani, S. De Capitani Di Vimercati, S. Paraboschi and P. Samarati, "Fuzzy Techniques for Trust and Reputation Management in Anonymous Peer-to-Peer Systems", In proc. of the international conference in fuzzy logic and technology, Zittau, Germany, Sept, 10-12, 2003.
- [16] Gayatri Swaminathan, Ben Y. Zhao and Kevin C. Almeroth, "Exploring the Feasibility of Proactive Reputation", *Recent advances in peer-to-peer systems and security*, ACM, Vol 20, Issue 2 (February 2008), p.155-166, 2008.
- [17] Ronald Ashri, Sarvapali D. Ramchurn, Jordi Sabater, Michael Luck, Nicholas R. Jennings, "Trust Evaluation Through Relationship Analysis", *ACM, AAMAS'05*, July 25-29, Utrecht, Netherlands.
- [18] Yao Wang, ulita Vassileva, "Trust and Reputation Model in Peer-to-Peer Networks", *Proc. of IEEE Conference on P2P Computing*, Linköping, Sweden, September, 2003.

RVVSV Prasad received his Masters degree in computer applications from Madurai Kamaraj University and Master of Philosophy in Computer Science from Alagappa University. He is currently doctoral candidate in the Department of Computer Science & Engineering, Acharya Nagarjuna University, Nagarjuna Nagar, Guntur, India. He is working as Associate Professor in the Department of Computer Science & Engineering, Bhimavaram Institute of Engineering and Technology, Pennada, Bhimavaram, India. His research interests include security, privacy and trust in mobile agents and P2P networks.

Vegi Srinivas received his M.Sc and MTech from Andhra University in Computer Science and Technology. He is currently working as Assistant Professor in Dadi Institute of Engineering and Technology, Anakapalli, Visakhapatnam, India. His main areas of interests are Security, Privacy and trusted computing.

V. Valli Kumari received her B.E. in Electronics and Communication Engineering and M.Tech. and PhD in Computer Science and Engineering all from Andhra University, India and is currently working as Professor in the same department. Her research interests include Security and privacy issues in Data Engineering, Network Security and E-Commerce. She is a member of IEEE and ACM and is a fellow of IETE.

KVSVN Raju received the B.E. in Electrical Engineering from Government College of Engineering, Kakinada, India and M.E. in Control Systems from Andhra University, India and obtained the PhD in Computer Science and Technology from IIT, Kharagpur, India. He is currently working as Professor in the Department of Computer Science and Engineering at A.U. College of Engineering, Visakhapatnam, India. His research interests include Data Engineering, Security Engineering and Software Engineering.