An Efficient Attack-Resistant Trust Model for P2P Networks

Chunqi Tian, Shihong Zou, Wendong Wang, Shiduan Cheng

State Key Laboratory of Networking and Switching
Beijing University of Posts and Telecommunications
Beijing, P.R.China, 100876

Summary
Building trust relationship between participants in a large-scale distributed Peer-to-Peer(P2P) file-sharing system is a challenging research topic because of peer anonymity, peer independence, high dynamics of peer behaviors, and the absence of an effective security mechanism. However, it is difficult to built trust simply by the traditional mechanism. Recommendation based trust models which are similar with and come from social relationship can resolve the problem, but face the challenges of subjectively, experiential weighting recommendation information when aggregating them. This paper presents ARTrust—an Attack Resistant Trust management model, a novel recommendation based trust model for P2P networks. The trust model consists of two parts: reputation evaluation and penalty evaluation. Reputation represents the accumulative assessment of the long-term behavior and the penalty part which is further divided into conflicting value and misusage value is employed to deal with the dynamic or spoiling behavior of peers, which makes ARTrust differ from other trust models based on the reputation only. For the problem of security, some measures are also proposed to defense against several malicious attacks. Subsequent experimental results show that, compared to the existing trust models, our model is more robust on trust security problems and more advanced in successful transaction rate.

Key words:
Peer-to-Peer ; trust ; credibility ; local trust value .

Introduction

Peer-to-peer file-sharing networks have many benefits over standard client-server approaches to data distribution, including increased robustness, scalability, and diversity of available data. However, the open and anonymous nature of these networks leads to a complete lack of responsibility for the content a peer puts on the network, opening the door to abuses of these networks by malicious peers. Consequently, a major challenge for large-scale P2P systems is how to establish trust between different peers without the benefit of trusted third parties or authorities.

Trust management systems have been widely used in p2p systems as effective mechanisms for deciding whether to trust another party based on its past history when two unknown peers transact with one another. Online systems like eBay and Amazon have been designed to foster trust among strangers in electronic commerce. However, most existing online reputation systems are centralized and may not be compatible with the design philosophy of P2P systems. Some researchers have presented several recommendation-based approaches in P2P systems, where peers keep track of and share the rating information about each other [1][2][8][10][11]. Nevertheless, they are not designed to handle malicious and deliberate attack on the trust models. In order to make accountable referrals to the users, trust management systems need to be able to detect possible attacks or threats that malicious users pose to the system. To reduce the amount of negative experience, it is necessary for the trust management system to warn users of possible bad attempts and discourage them from performing such behavior.

Bearing these issues in mind, we present an attack resistant trust management framework for decentralized P2P systems, with emphasis on efficiently aggregating referrals which include conflicts and inconsistency, as well controlling such possible attacks and threats as denigration, collusion, and strategic attacks. This paper focuses on the design of reputation mechanisms on unstructured P2P systems, and does not consider structured P2P systems with Distributed Hash Tables (DHTs), e.g. CAN [5] and Chord [4]. One reason is that DHTs are mainly designed for distributed storage systems, while the high turnover rate caused by frequent join and leave of peers in dynamic P2P systems causes significant overhead for DHTs.

This paper goes beyond existing approaches in the following three ways.

First, the ratings in most existing approaches are binary [1][2][3][7][8]. In the binary ratings, a peer rates the services from another peer as one of two values, commonly interpreted as either one (e.g., positive or satisfactory) or zero(e.g., negative, unsatisfactory). Binary ratings may not adequately represent a peer's experience of the quality of service (QoS) with other peers, e.g., the quality of files the peer sends. Our approach considers quality of service as probabilistic ratings in the interval [0,1] and focuses on how to aggregate these ratings.

Second, Ratings Aggregation. Although some of the existing approaches consider the credibility of recommenders in the recommendation based mechanisms, they don't consider how to effectively evaluate and precisely update the credibility of a recommender in presence of dishonest or unreliable referrals. We propose a method for credibility computation and update for the first time, as is proved that can efficiently distinguish reliable

Manuscript received November 5, 2006.
Manuscript revised November 25, 2006.

peers from deceptive or unreliable peers. One of the focuses of this paper is on quantitating the credibility of a referral and minimizing the effect of ratings from these denigrating or collusive peers.

Third, in order to portray the unpredictable and fluctuating behavior of malicious peers, we introduce penalty value to the computation for the trust value of a peer. The penalty value incorporates the penalty measure for various malicious behaviors such conflicting, and misusage of trust.

This paper is organized as follows. In section 2, we review some existing works. Section 3 introduces several malicious attack models, Section 4 presents our approach for peer trust evaluation. Some experiment results are illustrated in section 5. In section 6, we conclude our work.

2. Related Works

P2PRep proposed by Cornelli et al. [1][2] is a P2P protocol where servants can keep track of information about the reputation of other peers and share them with others. Their focus is to provide a protocol complementing existing P2P protocols, as demonstrated on top of Gnutella. However, there are no formalized trust metric in the paper validating their approach. The approach adopts a binary rating system and it is based on the Gnutella query broadcasting method using TTL limit.

Another work is EigenRep proposed by Kamvar et al. [3]. Their algorithm again focuses on a Gnutella like P2P file sharing network. They based their approach on the notion of transitive trust and addressed the collusion problem by assuming there are peers in the network that can be pre-trusted. While the algorithm showed promising results against a variety of threat models, we argue that the pre-trusted peers may not be available in all cases and a more general approach is needed. Another shortcoming of their approach is that the implementation of the algorithm is very complex and requires strong coordination and synchronization of peers.

Wang and Vassileva [6] propose a Bayesian network based trust model that uses reputation built on recommendations. They differentiate between two types of trust: trust in the host's capability to provide the service and trust in the host's reliability in providing recommendations.

Xiong and Liu [7] present a reputation-based trust supporting framework. They introduce three basic parameters and two adaptive parameters. They incorporate the concepts of a trust value and the similarity with oneself to compute credibility and satisfaction.

Liang and Shi [8] propose PET, a personalized trust model with reputation and risk evaluation for P2P resource sharing. In PET, risk factor is considered to complement the reputation evaluation. Risk evaluation represents the opinion of short-term behavior while reputation is the accumulative assessment of long-term behavior. The main contribution in PET is to introduce risk to the computation of trust value of a peer.

This paper focuses on the design of robust and efficient reputation mechanisms in P2P systems and studies possible attacks of reputation mechanisms in P2P systems. We construct a mathematic model of referral using credibility, and then adopt it to aggregate the referrals .Finally, we discuss such problems on security as denigration, collusion and oscillating behaviors of malicious peers and also address the solutions to these problems.

3. ARTrust Trust Model for P2P Networks

Due to the existence of all kinds of malicious peers, it is obvious that trust relationship between peers must be set up to make P2P system work efficiently. More and more researches indicate that P2P service availability is affected by unreliable QoS brought by the peers' voluntary operations as well as a large amount of cheating behaviors. Therefore, these factors must be taken into account when building trust management model.

To make ARTrust more reliable we add two characteristics to it. First, bad behavior makes the trustworthiness value drop faster and good behavior increases the value slower. We consider this to be important, since malicious peers may take advantage of any trust model that lacks this characteristic and perform malicious actions frequently while retaining their trust level. Another characteristic of our trust model is maintaining a personal storage of trust information rather than using a system-level trust information repository. An advantage of this approach is that it enables peers to retrieve trust information selectively from other peers chosen based on their credibility. On the other hand, a central repository based approach suffers from being a single point of failure and provide less meaningful information resulting from summarizing the reports of all the peers, including the ones that are not credible.

3.1 Overview

Before depicting our model, we list three principles for the design:

1. Peer will always trust itself.
2. If a peer continually behaves badly, it will be a bad peer prone.
3. The recommendations from others will not dominate the calculation of the trustworthiness value, but it will gain more weight when no direct interactions happen before.

Our trust metrics is composed of two parts – reputation value and penalty value. The reputation value is

measured by aggregating the referrals from all recommenders and penalty value is divided into two parts: conflicting value (C value) and misusage value (M value) in accordance with abnormity of peer behavior (see Section 4.3). The overall trust value of a peer is evaluated by subtracting the penalty value from the trust value. Let T_{ij} denote the overall trust value of provider j in the viewpoint of peer i, RE_{ij} and P_{ij} the reputation value and penalty value of peer j respectively, a, β the corresponding weight for RE_{ij} and P_{ij}. Therefore the trust value for peer j is:

$$T_{ij} = \alpha RE_{ij} - \beta P_{ij} (0 \le a, \beta \le 1) \quad (1)$$

The values for a, β should be chosen based on how optimistic a peer is. The more optimistic a peer becomes towards providers' behavior, it will choose the values for a, β such that α / β is large so that the overall trust value is less affected by penalty value. On the other hand, the more pessimistic a peer becomes towards other providers' behavior, it will choose the values for a, β such that α / β is small so that the overall trust value is sensitive to the value of the penalty.

P2P networks are overlaying networks that consist of a large number of nodes. For conveniences, we use file-sharing systems as example in the whole paper.

According to the quality of files provided by cooperating peers, we classify services into four categories, as shown in Table I. We formalize the quality set as Q = {G, C, I, M}.This coarse-grain classification is flexible enough to apply to any resource sharing. More subclasses can be introduced if necessary.

Table 1: Margin specifications

File Quality	Description
G(Good)	The file is as good as expected.
C(Common)	The file is correct, but with some degradation
I(Inauthentic)	The file is inauthentic
M(Malicious)	The file is malicious (e.g. virus or Trojan Horse)

Considering such downloading, we define a Map function f, as shown in Equation (2). From it, we can see that if the quality of file downloaded from responding peer is Good or Common, the ratings of requesting peer for responding peer increase but to a degree, whereas if the quality of file is Inauthentic, especially Malicious, the ratings decrease to a large degree.

$$f(x) = \begin{cases} v_1, x = G, 0 < v_1 < 1 \\ v_2, x = C, 0 < v_2 < v_1 \\ v_3, x = I, v_3 < 0, |v_3| > v_1 \\ v_4, x = M, -1 \le v_4 < 0, |v_3| < |v_4| \end{cases} \quad (2)$$

3.2 Reputation Evaluation

Let P_m denote peer *m*.

Definition1: $R^t_{mj} = R^t(P_m, P_j)$ is a local rating of peer *m* for peer *j* during the period of *t* by virtue of statements shown in table1. It is of great necessary to introduce time factor to differentiate the transactions

Local rating. In the following, we call the peer to request file and rate other peers *rater*, the peer to response and be evaluated *ratee*, and the peer that sends the trustworthiness value of the known peers to others the recommender. In ARTrust after a direct interaction between *rater* and *rate*, *rater* will rate the *ratee* according to the quality of file provided by *ratee* and then locally store the results.

If P_m has a N_{mj} number of interactions with P_j, the rating of P_m for P_j is

$$R^t_{mj} = R^t(P_m, P_j) = \begin{cases} \dfrac{\sum_{x=G,C,I,M}^{N_{mj}} f(x)}{N_{mj}}, N_{mj} \ne 0 \\ 0, N_{mj} = 0 \end{cases} \quad (3)$$

It is indispensable to differentiate the effect of transaction period on computing the trust value of a peer in current trust models since individual behavior changes over time. To solve the problem, a time based evaluation method that fresher interactions are more important than old ones is adopted widely, that is, assigning more weights to recent interactions and less weight to previous interactions. We present a decay function to achieve the same purpose, furthermore, decay function is more operable, more easy controllable, more flexible than weight application. Because weight distribution is absolutely experiential and subjective, however, decay function is operated and restricted by inner parameter.

Definition2: Decay function f is in fact a timing discount function, is described as

$$f(k) = f_k = \rho^{n-k}, 0 < \rho < 1, 0 \le k \le n,$$

where f_k is a function value, also is decay factor for the k^{th} time window. As can be seen from the definition, the weight for the first interaction is $f_1 = \rho^{n-1}$, that is, decay degree is maximal; the current interaction's weight is $f_n = 1$, that is, decay degree is 0.

If P_m has a number of interactions with P_j during period $[t_{start}, t_{end}] = [t_1, t_2 \cdots t_n]$, where $1 \le k \le n$, it can evaluate P_j's local trust value as follows:

$$R_{mj} = \sum_{k=1}^{n} f_k R_{mj}^{t_k} \Big/ \sum_{k=1}^{n} f_k \quad (4)$$

where f_k is the decay factor of period t_k, and $0 < f_k < f_{k+1} \le 1$, $1 \le k < n$. Equation (3) weights more to recent interactions.

Reputation value. In a reputation system, a peer makes decisions based on its experience and other peers'

recommendation. The peer *i* (*rater*) rate another peer *j* (*ratee*) after they directly transact with each other. Local trust value is evaluated by virtue of quality of file that *ratee* have provided. But to evaluate the trustworthiness of a given party comprehensively, *rater* can not rely on only direct experience. So the recommendation-based trust models are presented. In referral process, *rater* issues a query for *ratee*'s reputation, other peers who have interacted with the same peer (*ratee*) — termed recommenders—may response to query and give there feedbacks that are interaction experience with *ratee* to *rater. Rater* then can incorporate the knowledge of other peers according to its acquaintanceship degree to them so as to whole know *ratee.*

One challenging problem in reputation mechanism is how to aggregate referrals from diverse recommenders with different trustworthiness in an efficient manner. In [8], the referrals are treated equally and reliabilities of theirs are not taken into account. [11] proposes a trust system that collects the referrals of the first few peers joining networks. In [12] authors employ an adaptive scheme for evaluating referral's reliability. The fact is that the reputation of recommenders is different and the referral from the peer with high reputation value is more reliable than that with low reputation. Therefore, we should differentiate these referrals. In the following, we employ "*credibility*" to represent the measurement of recommendation trust and further propose an updated method.

In ARTrust, we employ the credibility of a recommender to weigh its referral and aggregate overall referrals to obtain the reputation value of a responding peer. The reputation value of peer j is:

$$RE_{ij} = \frac{\sum_{m \in \mathrm{Re}G} R_{mj} CR_{im}}{\sum_{m \in \mathrm{Re}G} CR_{im}} \tag{5}$$

where RE_{ij} is the reputation value of peer *j* from the viewpoint of peer *i*, *ReG* represents the collective of the recommenders for peer *j*, R_{mj} is the local trust value of recommender m for peer *j*, CR_{im} is the credibility of peer *i* for recommender *m*. As can be seen from formula (5), peer *i* give a higher weight to a referral from a peer whose credibility value is large (from its viewpoint). When the reputation value of peer *j* is attained, peer *i* may update the credibility of recommender *m* so as to measure its coming referrals.

Credibility. In ARTrust, the credibility of a peer is used to weigh the feedback it reports. If a peer gives wrong feedback about other peers its credibility value is decreased and its subsequent reports have a reduced impact on the reputation of another peer. Similarly, if a peer's feedback is consistently good, i.e., in agreement with other reporting peers, its credibility always goes up. Credibility values are based on first-hand experience only and, unlike ratings, they are not shared with other peers. Credibility values are normalized so that they lie between 0 and 1.

In the following, we define an equation for credibility update, which is based on historic credibility

Definition 3: Given the credibility CR_{im}^{k} for peer *m* after the k[th] recommendation, the new credibility can be calculated by peer *i* as follows:

$$CR_{im}^{k+1} = \begin{cases} CR_{im}^{k} + \delta(1 - CR_{im}^{k})(1-\varepsilon), 0 \le \varepsilon \le 1, k > 0 \\ CR_{im}^{k} - \gamma CR_{im}^{k}(1 - \frac{1}{\varepsilon}), \varepsilon > 1, k > 0 \\ 0.5, k = 0 \end{cases} \tag{6}$$

where δ, γ are two impact factors and $0 < \delta < \gamma < 1$, CR_{im}^{k} is the credibility of peer *m* after k reports to peer *i*, and $\varepsilon = \left| RE_{ij} - R_{mj} \right| / s_{ij}$ is a deviation, RE_{ij} is the reputation value of peer *j* computed by peer *i*, R_{mj} is the local trust value of recommender m for peer *j*, and s_{ij} is the standard deviation of all the reported opinions about peer j.

In equation (6), the new credibility CR_{im}^{k+1} results from the current credibility CR_{im}^{k} and the deviation. The change may be an increment or a decrement, which results from δ, γ and ε. That means if $\varepsilon < 1$, it is an increment. Otherwise it is a decrement, which has the following properties.

Property1: If $\left| RE_{ij} - R_{mj} \right| = s_{ij}$, then $\varepsilon = 1$; this property means that $\left| RE_{ij} - R_{mj} \right| = s_{ij}$, there is no change with CR_{im}^{k+1} and CR_{im}^{k}.

Property2: If $\left| RE_{ij} - R_{mj} \right| \neq s_{ij}$, then $\varepsilon < 1$ or $\varepsilon > 1$. This property means that there will be an increment or a decrement for the credibility modification if $\left| RE_{ij} - R_{mj} \right|$ and s_{ij} are different.

Property3: The smaller ε is, the larger CR_{im}^{k+1} is when $\varepsilon < 1$;

Property4: Initial credibility value of a peer is CR_{im}^{0} =0.5. An initial credibility value should be given so that new credibility values can be calculated in the subsequent process. However, in the beginning, peer *i* may not know the credibility of a recommender *m* especially when P_m is a new peer. In this case, P_m can assign a value to each peer's credibility, say, CR_{im}^{0} =0.5. The idea is that suspicion of new peers is socially inefficient since malicious peers are rare in the P2P system [13]. In a P2P system where peers join and leave the system dynamically, it would be more efficient to trust new peers until they are proved untrustworthy. This value may not reflect the true credibility. But with more and more referral the credibility value can be modified which will be closer to the true value.

3.3 Penalty value

The reputation value of a peer is considered as its trustworthiness in the existing trust models [7][9][10].We know that reputation is an accumulative value for the past behavior and reflects the overall evaluation on the responding peer. However, it is not sensitive enough to perceive the suddenly spoiling peer because it needs time to decrease the accumulative score. Penalty value can help to solve this problem, which is further divided into two parties, i.e., conflicting value and misusage value.

Conflicting value—C-value. Conflicting value denotes the deviation degree or similarity between the local trust value of *ratee* in the viewpoint of *rater* and its reputation value. Low C-value may enable *rater* to place high confidence on the reputation party. C-value is computed by calculating the standard deviation of all the feedbacks of peer *i* (*rater*) based on its transactions with provider *j* (*ratee*) where each transaction may have different weight in the computation. The following equation is used for computing C-value:

$$C_{ij}=\sqrt{\frac{\sum_{k=1}^{\max K}\{f_k\times(R_{ij}^k-RE_{ij})^2\}}{\sum_{k=1}^{\max K}f_k}}=\begin{cases}\sqrt{\dfrac{\sum_{k=1}^{\max K}\{f_k\times(R_{ij}^k-RE_{ij})^2\}}{\rho^{n-\max K}(1-\rho^{\max K})/(1-\rho)}}, & \max K<n\\ \sqrt{\dfrac{\sum_{k=1}^{\max K}\{f_k\times(R_{ij}^k-RE_{ij})^2\}}{(1-\rho^{n})/(1-\rho)}}, & \max K=n\end{cases} \quad (7)$$

where $1<\rho<1, \max K\le n$, R_{ij}^k is the local ratings of peer *i* for peer *j* during the k[th] transaction period, f_k is the decay factor of R_{ij}^k, RE_{ij} is the reputation value of *j* computed by peer *i*, and $\max K$ is the maximum length of time for computing C_{ij} and its upper limit is the whole transaction period.

Misusage value—M value. Misusage value denotes the amount of trust value that provider *j* is currently taking advantage of in performing transactions with peer *i*. The goal of incorporating this factor into penalty value is to reflect the cost of behavioral fluctuation to be paid by provider *j*. M-value is computed in the following:

$$M_{ij}=\frac{\sum_{k=1}^{\max K}\{f_k\times\max(0,RE_{ij}-C_{ij}-R_{ij}^k)\}}{\sum_{k=1}^{\max K}f_k}$$

$$=\begin{cases}\dfrac{\sum_{k=1}^{\max K}\{f_k\times\max(0,RE_{ij}-C_{ij}-R_{ij}^k)\}}{\rho^{n-\max K}(1-\rho^{\max K})/(1-\rho)}, & \max K<n\\ \dfrac{\sum_{k=1}^{\max K}\{f_k\times\max(0,RE_{ij}-C_{ij}-R_{ij}^k)\}}{(1-\rho^{n})/(1-\rho)}, & \max K=n\end{cases} \quad (8)$$

where the parameters are the same as ones in formula (7).

Upon computing the C-value and M-value of peer *j*, peer *i* may assign suitable weights to them, for example, a,b respectively, therefore the penalty value of peer j is $aC_{ij}+bM_{ij}$.Thus, the overall trust value of peer *j* in the viewpoint of peer *i* will be $T_{ij}=\alpha RE_{ij}-\beta(aC_{ij}+bM_{ij})$.

3.4 The Approach to Resisting Denigration, Collusion Attack

Denigration will happen when this type of malicious peers are asked for the trustworthy of these peers with which they have transacted and they always provide a untrue, negative ratings for the peers.

Collusive peers form a malicious collective by assigning a high trust value to another malicious peer in the network. Collusive peers provide inauthentic files to peers outside when selected as download source and provide denigrated ratings for these peers.

Compared with some existing models, trust value of a peer is not determined only by its reputation value but influenced by penalty value that makes the trust value sensitive to the malicious behavior and furthermore can detect malicious peer and discriminate potential threats. We have found that a small quantity of denigrations or exaggerations have a slight effect on an established result through a large number of experiments.

We have taken several measures to defense against denigration and collusion in the following.

Firstly, we weigh the referrals according to the recommenders' credibility before combining them and moreover judge whether $\left|RE_{ij}-R_{mj}\right|/S_{ij}>\zeta$ （ζ is a given threshold）come into existence or not. The aim is to estimate the deviation between the local rating of certain recommender for the responding peer *j* and the reputation value of peer *j*. If deviation degree is beyond a threshold, the rating is regarded invalid and discarded. The choice for the value of ζ is important and appropriate value is crucial to detect denigration and exaggeration behavior. Thus the excessive denigration and exaggeration is hard to take effect.

Secondly, we differentiate the referral according to referral's credibility. As shown in formula (5), if a recommender is a discredited one, its recommendation is discounted, that is to say, the lower the referral's reputation is, the more the recommendation is at a discount. Therefore, the low credible peer denigrates its competitor or exaggerates its accomplice very difficultly.

Finally, we prescribe that if there are some evidences which support I or M type of files beyond a given threshold, *rater* may ask *ratee* for transaction records. By checking the records, *rater* will ignore the referral if it finds I or M rating is given to *ratee* very frequently.

We can efficiently restrain malicious peers from

denigrating and colluding by means of these measures and favorable effect is found in the consequent simulations.

3.5 The Solution for Some Problems

Loads equilibrium problem. In some existing schemes, a peer with a high trust value is mostly likely to be chosen as download source. Possibly, this might lead a peer into a vicious circle of accumulating trust by responding to many queries, thus being chosen even more frequently as download source in the future, thus accumulating even more trust but simultaneously overloading easily. In a non-trust based system, this situation does not occur. In ARTrust, we take measures as follows: we assume that the list of responding peers is $\{P_1, P_2, \cdots P_Q\}$ and the corresponding trust values are $\{T_1, T_2 \cdots T_Q\}$. Our method is to allow the requesting peer choose a fit peer as download source among $\min(N, \lfloor Q/2 \rfloor)$ (N is a pre-given parameter) responding peers with high trust value so that a peer with relatively low trust value has a chance to be chosen. The consequent simulation proves that this way may efficiently avoid overload.

New node problem. In ARTrust, a new peer is chosen as download source with a probability of 10%. As a new comer, it has no historic transaction with any peers, therefore, its trust value is 0. To give new peers in the network the chance of building up trust, our model assigns a fixed 10% chance to download from the group of responding peers with trust value 0. Otherwise, new peers would maybe never be chosen as download source, depriving them of the chance to become a trusted member of the network. However, the probability can not be assigned too high in case malicious peers with poor reputation frequently change their identifiers and re-enter the system (i.e. Sybil attack).

4 Experiment result

In this section, we will assess the performance of our scheme as compared to a P2P network where PeerTrust [7] scheme and EigenRep [3] are implemented. We shall demonstrate the scheme's performance under a variety of threat models. The simulations are based on Query Cycle Simulator developed by P2P research group in Stanford University [14][15] .There are 100 query cycles in one experiment and the results are averaged over 3 runs.

4.1 Simulation Environment

In each query cycle, peer *i* in the network may be actively issuing a query, inactive, or even down and not responding to queries passing by. Upon issuing a query, a peer waits for incoming responses, selects a download source among those peers that responded and starts downloading the file until gets the authentic file or tries all the download sources. Then the query cycle finishes and the data is collected.

In simulation we assume that there are 1000 peers in the network among which malicious peers vary between 100 and 500 and the query message is flooded with TTL=5. In the experiment, normal peers are in the uptime with the uniform random distribution over [0%, 100%] and issue queries in the uptime with the uniform random distribution over [0%, 50%], while malicious peers are always up and always issue queries. For good peers, the probability to provide authentic files is 96%, while simple malicious peers will respond to all queries they have received and provide inauthentic files with a probability of 70% for all download requests and collusive peers provide with a probability of 100% to peers outside malicious collective.

The content distribution model is the same as that in [15]. Files are distributed probabilistically to peers based on their popularities and the content categories that peers are interested in. Good peers issue queries in accordance with their interests while malicious peers issue queries randomly just to harm other peers or disturb the system. In simulation environments, there are 10000 numbers of files in all and 100 content categories are hold in the network. Other parameters in the experiments are in the following

Table 2: The parameters in the experiments

Parameter	Value	Description
N	3	Number of simulation
C	100	Cycle of simulation
α	0.8	Weight of reputation value
β	0.2	Weight of penalty value
ρ	0.8	Decay parameter
δ	0.4	Update factor in Equation 6
γ	0.8	Update factor in Equation 6
ζ	2	Threshold of referral deviation
ϕ	2	Punishment factor

In our experiments, we consider different threat models, where a threat model describes the behavior of a malicious peer in the network. Malicious peers' behaviors have been described in Section3 and we do not explain them any more. We classify these malicious peers into four categories, that is, Simple malicious (SM), Denigrating peers (DM), Collusive peers (CM) and Strategic peers (Strategic).

4.2 Successful Transaction Rate (STR)

We compare the successful transaction rate (STR) of our scheme with PeerTrust scheme and EigenRep under these scenarios. The metrics, STR, is the ratio of the number of successful transaction over overall transaction numbers, is used to evaluate the efficiency of trust model.

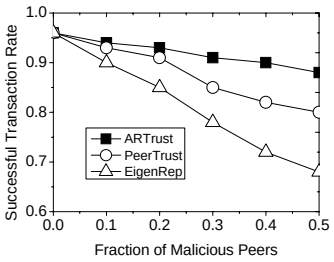

Fig. 1 STRs under SM.

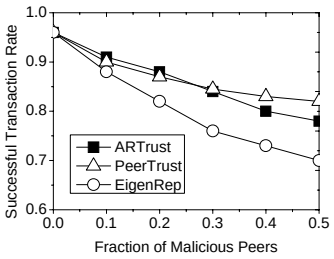

Fig. 2 STRs under DM.

Simple malicious peers and Denigrating peer. The successful transaction rates of three models under SM and DM are shown in Fig.1 and Fig.2 When there is no malicious peers in the system, STR of three schemes are all 96%.With the fraction of malicious peers increasing, STRs of three schemes descend, but our model descends most slightly. Not taking into consideration under SM that malicious peers provide authentic file in certain probability, EigenRep and PeerTrust can not punish these peers and therefore the STRs fall more heavily. In comparison with PeerTrust scheme and EigenRep, the STRs of ARTrust remain high all long and still 87% when the fraction of malicious peers is 50%. Under DM, due to some measures taken in section 3.4 to punish DM peers, our model is robust against malicious behaviors and the STRS is still about 80% when the fraction of malicious peers is 50%.

Collusive peers. The successful transaction rates of three models under Collusive are shown in Figure 3.

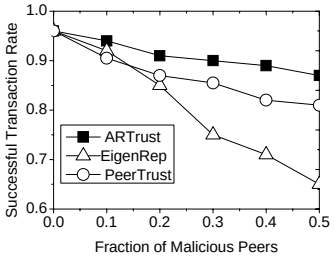

Fig. 3 STRs under Collusive.

Each peer in the colluding group boosted the trust value of their accomplices regardless of their behavior, while downplaying the trust value of good providers. The STR of EigenRep and PeerTrust descends evidently with malicious peers increasing. Compared to both schemes, ARTrust is designed to tackle collusive attacks, therefore to a great extent is proved robust against collusive attacks.

The influence of the collusion with front peers (CF) attack in which these front peers provide authentic files is demonstrated in Figure 4, which shows the STRs when collusive peers' fractions vary from o.1 to 0.5 and the front peers' fraction is 20% of collusive peers. We can see that the CF attack leads to a performance drop since indirect trust information can be inaccurate. However, the performance drop of ARTrust is small because our trust scheme already has defense mechanisms embedded.

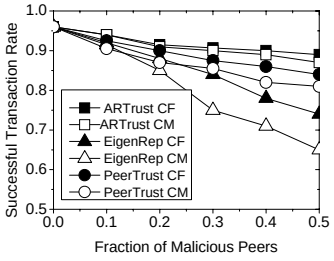

Fig. 4 STRs under CF.

Strategic peers. We also compare the STRs of the system under the strategic peers with EigenRep and PeerTrust scheme. In simulation, suppose the peer whose trust value is less than 0.5 is untrustworthy, and a strategic peer provides true files with a probability of 20% when its trust value is beyond 0.6 and in 60% probability when its trust value is less than 0.6.

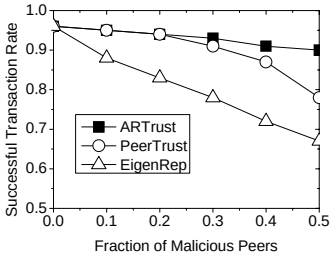

Fig. 5 STRs under strategy.

As can be seen from Fig.5, the successful transaction rate of EigenRep and PeerTrust scheme are lower than that of ARTrust, because both schemes can not efficiently tackle this type of attack and can not recognize malicious peers sensitively. However, the STR of ARTrust is better than the former two trust mechanisms no matter what proportion malicious peers are, the reason is that the

penalty value depict the dynamic behavior of a peer and give an explicit punishment to the peer whose performance drops either deliberately or unconsciously.

4.3 Load equilibrium simulation

In this experiment, we illustrate the load distribution performance of ARTrust. We simulate the percent of the loads for good peers with the trust value over the ones for all the good peers. In this experiment we assume that there only exist simple malicious peers and furthermore the fraction of these peers is 20%. In ARTrust, *rater* selects download sources possessing the same requesting file in terms of the method depicted in Section 3.5 and so the peer with the lower trust value may be selected as download source. As we can see in Figure 6, the loads are distributed to these good peers symmetrically and the transaction results also show that good peers may download authentic files with a high probability.

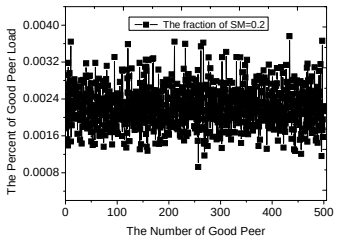

Fig. 6 The percent of good peers load.

5 Result

In this paper we have presented ARTrust, a framework for trust management in P2P networks. Different from the previous schemes, we evaluate the trust value of a peer not only by reputation value of the peer but also the penalty value. Furthermore, we address some methods for resisting such malicious attacks as denigration, collusion and behavior oscillating. The experiments shows that the ARTrust performs very well even when the number of malicious peers in the system is under half. It outperforms the well-known PeerTrust and EigenRep schemes significantly. Therefore, ARTrust can efficiently be applied to a large-scale distributed P2P system.

References

[1] E. Damiani, D. C. di Vimercati, S. Paraboschi, et al.A reputation-based approach for choosing reliable resources in peer-to-peer networks. In Proc. of the 9th conference on Computer and Communications security, pages 207-216. ACM Press, 2002

[2] F. Cornelli, E. Damiani, D. C. di Vimercati, et.al Choosing reputable servents in a P2P network, In Proc. of the 11th WWW Conf. Hawaii: ACM Press, 2002. 441~449.

[3] S. Kamvar, M. Schlosser, The EigenTrust Algorithm for Reputation Management in P2P Networks, In Proceedings of WWW, Budapest, Hungary, 2003

[4] R. Stoica, D. Morris, M. Karger, et al. Chord: A Scalable Peer-to-peer Lookup Protocol for Internet Applications.In Proceedings of the ACM SIGCOMM Conference, 2001.

[5] S. Ratnasamy, P. Francis, M. Handley, R. Karp, and S. Shenker. A scalable content-addressable network. In Proceedings of ACM SIGCOMM San Diego, 2001.

[6] Y. Wang, J. Vassileva. Trust and Reputation Model in Peer-to-Peer Networks, Third International Conference on Peer-to-Peer Computing, IEEE, September 01 - 03, 2003

[7] L.Xiong and L. Liu, PeerTrust: Supporting Reputaion-Based Trust for Peer-to-Peer Electronic Communities, IEEE Transactions on Knowledge and Data Engineering, Vol. 16, No. 7, July 2004.

[8] Z.Q.Liang and W.S.Shi, PET:A Personalized trust model with reputation and risk evaluation for p2p resource sharing. The 38th Hawaii International Conference on System Science,2005.

[9] S.Marti,H.Garcia, Limited reputation sharing in P2P system, In Proceedings of the 9th ACM conference on Electronic commerce,2004

[10] S.S.Song,K.Hwang,R.F.Zhou. Trusted P2PTransactions with Fuzzy Reputation Aggregation, IEEE Internet Computing ,18-28,2005.

[11] J.Avnet ,J.Sala. Towards robust and scalable trust metrics, IEEE International Conference.,2003

[12] W.Sears, Z.Yu, Y.Guan. A adaptive reputation based trust framework for peer-to-peer applications, IEEE International Symposium on Network Computing and Applications ,July,2005

[13] E.Friedman,P.Resnick. The social cost of cheap pseudonyms, Journal of Economics and Management Strategy, 2001.

[14] http://p2p.stanford.edu/www/demos.htm

[15] M. Schlosser, T. Condie, and S. Kamvar. Simulating a File-Sharing P2P Network. In First Workshop on Semantics in P2P and Grid Computing, December,2003.

Chunqi Tian received the B.S. and M.S. degrees in Computer Engineering from Xi'an Jiaotong University and Xidian University in 1998 and 2004, respectively, and worked as a software engineer with companies during 1998-2001. He is currently a Ph.D. candidate in the College of Computer Science at Beijing University of Posts and Telecommunications (BUPT). His research interests are in service management, P2P networks.

Shihong Zou born in 1978, an Assistant Professor. He received his Ph.D. degree in 2004 from Beijing University of Posts and Telecommunications. His research interests include service management, wireless LAN, mobile ad hoc networks, wireless sensor network and quality of service.

Shiduan Cheng is a professor and a Ph.D. supervisor in the Department of Computer Science, BUPT. Her research interests include service management, quality of service, wireless networks, next generation network, network performance and so on.