Journal of Zhejiang University-SCIENCE C (Computers & Electronics)
ISSN 1869-1951 (Print); ISSN 1869-196X (Online)
www.zju.edu.cn/jzus; www.springerlink.com
E-mail: jzus@zju.edu.cn

An incentive model for voting based on information-hiding in P2P networks*

Bo-wei YANG[1,2], Guang-hua SONG[1,3], Yao ZHENG[1,3]

([1]*Center for Engineering and Scientific Computation, Zhejiang University, Hangzhou 310027, China*)

([2]*School of Computer Science and Technology, Zhejiang University, Hangzhou 310027, China*)

([3]*School of Aeronautics and Astronautics, Zhejiang University, Hangzhou 310027, China*)

E-mail: {boweiy, ghsong, yao.zheng}@zju.edu.cn

Received Nov. 27, 2009; Revision accepted Aug. 19, 2010; Crosschecked Sept. 28, 2010

Abstract: We propose an incentive model based on information-hiding to encourage peers to vote for resources in peer-to-peer (P2P) networks. The following are key motives for our model: (1) Some trust and reputation systems have been deployed in modern P2P systems, but a lot of blank rating resources exist in these P2P systems; (2) E-commerce consumer-to-consumer (C2C) websites that adopt simple rating strategies are receiving accusations that false and useless ratings are flooded. We establish an information-hiding based RRR/RIR (resource reputation rating/reputation incentive rating) voting model, which awards or punishes voters according to their behaviors. The RRR generating algorithm and the RIR generating algorithm are presented in detail, and the information-hiding mechanism is given. Experimental results showed that the incentive RRR/RIR model can effectively encourage valid voting and prevent malicious or arbitrary voting in the P2P reputation system.

Key words: Peer-to-peer (P2P), Information-hiding, Incentive, Blank voting, Reputation system
doi:10.1631/jzus.C0910727 **Document code:** A **CLC number:** TP393

1 Introduction

Recently, unfair or malicious behaviors have been propagating over powerful peer-to-peer (P2P) networks. P2P networks have been accused of free-riding (Adar and Huberman, 2000; Feldman *et al*., 2004), copyright infringement, virus corrosion, and so on. The tit-for-tat strategy (Cohen, 2003) and the market mechanism (Freedman *et al*., 2008) were proposed to encourage peers to contribute to the network to eliminate free-riding. Unfair or malicious behaviors and various viruses were restrained mainly by reputation systems.

Reputation systems represent a promising method for fostering trust amongst strangers in P2P networks. Basically, a reputation system aggregates ratings for a resource and derives a reputation score for it, and assists other users in deciding whether or not to transact with that resource in the future.

Most studies about the reputation system make the same assumption that the participators are voluntary and willing to vote for resources. However, as the previous researchers have claimed, many participators are selfish and may even provide other users with false experiences for their own benefits. In reality, few users are willing to vote for the resources, if no incentive strategy is adopted. As a result, many resources are left blank; i.e., no ratings for them exist. For example, users of Gnutella, Napster, and KaZaa could not benefit from the recommendation system as a lot of blank resources existed (Liang *et al*., 2005). An incentive strategy to encourage the participators to vote for the resources is urgently required in current P2P reputation networks.

An ideal incentive strategy should improve the voter turnout rate and increase the trustworthiness of

* Project (No. 2009C14031) supported by the Science and Technology Department of Zhejiang Province, China

the rating for a resource. To implement this strategy, the reputation system must provide a mechanism that not only provides a useful hint for later users, but also hides some details to prevent the speculators from inversely calculating the optimal rating to earn exorbitant profit.

In this paper, we propose an incentive model based on information-hiding to encourage users to vote for the resources they have used. Users in the P2P network are encouraged to attentively report a rating for the resources they have used. Even they are not sure how to rate for resources, a blank rating should be reported; otherwise, they will be penalized.

The main contributions of this paper are:

1. This paper deals with an interesting and challenging problem, i.e., encouraging clients to vote responsibly, in P2P or C2C (consumer-to-consumer) networks. To the best of our knowledge, few studies have focused on this problem.

2. The proposed model guarantees not only the responsibility of the voters but also the quality of the reputation values of resources. Existing reputation systems may benefit from more responsible voters by adopting the incentive model presented in the paper, at an extremely low integrated cost.

3. The incentive strategy is practical and works well even if it is well known to the attackers.

4. Attacking, especially the discriminating behavior, is discussed in detail. Two major problems, blank resources and discriminating resources, existing in the current P2P networks, are handled properly.

2 Related works

Recently, reputation systems have received considerable attention. Mislove *et al*. (2008) proposed Ostra, an attractive credits transfer model. Ostra requires users acquire and maintain a certain number of social links to be able to communicate, and cannot encourage clients to vote for the communications, since the credits are reset after the transactions. Ostra helps resource providers classify clients and stop the malicious unwanted clients, but it cannot avoid the blank resource issues in P2P networks. Kamvar *et al*. (2003) proposed an innovative global reputation aggregation model as EigenTrust. EigenTrust aggregates a part of the historical reputation records for a user from its neighbors in the P2P network and calculates a global reputation for this user. Every later comer in the P2P network can access the pre-generated reputation score before he/she starts transactions. After analyzing the P2P reputation model, Xiong and Liu (2004) refined the trust model in EigenTrust and proposed PeerTrust, which models the reputation for nodes with five factors. Users in EigenTrust or PeerTrust, however, trust only their neighbors, and a freshman or loner is not likely to benefit from the reputation system, for the lack of neighbors. Yang *et al*. (2008) tried to draw the statistical reputation recommendation into a totally decentralized P2P network. But none of the above researches focused on the incentive, so it is difficult for them to work well as expected due to the lack of voting.

As for the incentive models, Antoniadis *et al*. (2004) and Papaioannou and Stamoulis (2005) proposed a simple approach to detecting false and arbitrary feedbacks. They selected two simultaneous feedbacks for the same resource. If the two feedbacks agree, both clients are awarded; otherwise, they are punished. This lightweight approach is very flexible and effective in encouraging voting and detecting false or arbitrary feedbacks; however, it cannot discern the liars. The innocent may be entangled and punished. Yang *et al.* (2007) presented a set of combined trust and incentive matrixes to evaluate the reputation of files and users. The bandwidth quota is an important factor of the reputation. However, the trust and incentive matrix does not concern the detailed incremental incentive algorithm of users, and the system is not able to readily detect malicious and arbitrary voting. Chang *et al.* (2007) and Jin *et al.* (2007) focused on the false or dishonest feedback, both of them trying to separate feedback trust and service trust, to evaluate all past voting, and to identify false or dishonest feedback. However, both of them assume that the consumers will vote for the resources after use.

3 Framework design

3.1 Terms definition

RRR: resource reputation rating, the rating associated with a resource, ranging in [0, 1], to quantify its quality.

RIR: reputation incentive rating, the rating associated with a client to quantify its voting reputation. In general, RIR is positive or zero.

p_R: price of resource, a positive value defined by its provider. A client with its RIR smaller than p_R of a resource will be banned to access the resource. Resources with high p_R are attractive for clients to earn higher rating.

MRVR: most recent voting rating, several fixed slots holding the most recent ratings of a client to reduce the impact of occasional mistakes.

3.2 Framework hypotheses

To simplify the model, we focus on the theoretical P2P model. Our voting model is built on the abstraction of the current P2P network. We assume that this conceptive P2P network has a logically centralized information storage facility and that the public data can be obtained conveniently and securely by any node. Traditional centralized hierarchy and the distributed hash table (DHT) network are possible implementations. The user authentication and authorization is implemented using the RSA algorithm. The issue of IDs and the behaviors of users are watched and handled by the third-party facility such as the E-commerce operations center. These hypotheses are practical, and have been partially adopted by Taobao Inc., China, which has more than 200 million users. Under these constraints, our voting model can be deployed to any centralized or decentralized P2P network.

3.3 Components of the framework

The presented framework is as depicted in Fig. 1. The framework is logically composed of three types of nodes: the consumer, the resource provider, and the bank node. The consumer agent, the provider agent, and the bank agent are deployed on the corresponding nodes, respectively. These agents interact with others in the logical P2P network. The consumer agent may choose to rate for a resource after the user has used it. All of the ratings are maintained in the bank agents.

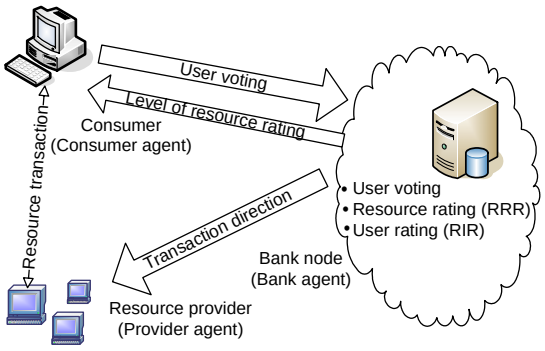

Fig. 1 The framework of the incentive voting model

For an access transaction TR with a resource R, one ending host acts as the resource consumer, denoted as C_{TR}, while the other acts as the resource provider, denoted as P_{TR}. Every resource R in the P2P network is associated with a resource reputation rating, denoted as RRR_R. Every consumer C is associated with a reputation incentive rating, denoted as RIR_C.

Logically, there is only one well-known bank agent in the P2P network. The bank agent is the repository of the reputation system; it manages the reputation information in the P2P network: profiles, public certificates, RIR ratings for users, access counting, voting history, RRR ratings for resources, prices of the resources, and so on. In addition, the bank agent sends the essential rating information to clients, indicates the beginning of a resource transaction, and receives and evaluates the feedback.

3.4 Mechanism of the framework

Here, an example is given to show how each component functions in a resource transaction TR. As shown in Fig. 1, before access to a resource R, C_{TR} asks the bank agent for the level of rating and price (p_R) of R to help make a decision. The level is associated with RRR_R and is a simple mapping to the accurate RRR_R rating. The setting of the mapping algorithm involved in the demo is shown in Table 1. However, the core of information-hiding is not just this simple mapping, as will be depicted in the following sections.

Table 1 Mapping of resource reputation rating (RRR) to the level of rating

RRR	Level of rating	RRR	Level of rating
100%–80%	Excellent	40%–20%	Bad
80%–60%	Good	20%–0	Useless
60%–40%	Neutral		

The accurate RRR will never be leaked, so none of the users in the P2P network know the exact value of RRR. However, the mapping of RRR is proverbial to all logical participators in the network.

C_{TR} may be satisfied with the level of rating and the price of resource R. Thus, it contacts P_{TR} to prepare for the resource accessing, and tells the bank to pay for the resources with its RIR_C. The bank accepts the request from C_{TR}, and reduces RIR_C by p_R. After receiving requests from client C_{TR}, the provider P_{TR} contacts the bank to confirm whether C_{TR} has paid for the resource R. The resource transaction begins if the bank agrees with all of above conditions.

After using a resource, C_{TR} has three choices:

1. To give no response to the bank node.
2. To feed back with a rating for this transaction.
3. To report a blank rating for this transaction.

In the first situation, the bank node does nothing with its RIR_C, so C_{TR} will lose p_R points, since C_{TR} had paid for the resource at the beginning of a transaction. This may result in the resource access denial of the oncoming transaction if RIR_C is smaller than p_R.

To earn their RIR points, users have to provide an accurate rating for this transaction as a feedback. In this situation, the bank receives the accurate rating for resource R from C_{TR}, and generates an RIR rating increment ranging from 0 to $2p_R$ with a statistic model that will be detailed in the next section. The statistic rating strategy guarantees that more accurate rating provided leads to a higher RIR rating increment. Finally, the bank adds the increment to RIR_C.

We may have choice 3 for another situation: A client interrupts the transaction manually after launching it for some purposes, so it cannot give an accurate rating for this resource. The last choice in our system is disposed as a blank rating for this transaction. In this case, the bank adds RIR_C by εp_R ($0<\varepsilon<1$). As the client has consumed p_R for the transaction, he/she will lose $(1-\varepsilon)p_R$ from RIR_C if he/she chooses to report a blank rating for this resource.

Therefore, reporting a blank rating is better than leaving the P2P network without any voting. Users are always encouraged to report a rating attentively for the resources they have used.

4 Detailed design and algorithms

In this section, the algorithms of incremental RRR and RIR generating are provided. The information-hiding mechanism is elaborated.

4.1 Incremental RRR generating algorithm

We assume that the rating given by the client, denoted as R_c, ranges in [0, 1], and I is the mapping level interval in our reputation system. The algorithm maps R_c from [0, 1] to a smaller range $[RRR_R-I/2, RRR_R+I/2]$ and calculates the new RRR rating (denoted as RRR_R') of a resource as follows:

$$\mathrm{RRR}'_{\mathrm{R}}=\begin{cases}0, & f(\mathrm{RRR}_{\mathrm{R}},R_{\mathrm{c}},N_{\mathrm{cr}},I,N)\le 0,\\ f(\mathrm{RRR}_{\mathrm{R}},R_{\mathrm{c}},N_{\mathrm{cr}},I,N), & 0<f(\mathrm{RRR}_{\mathrm{R}},R_{\mathrm{c}},N_{\mathrm{cr}},I,N)<1,\\ 1, & f(\mathrm{RRR}_{\mathrm{R}},R_{\mathrm{c}},N_{\mathrm{cr}},I,N)\ge 1,\end{cases} \tag{1}$$

where

$$\begin{aligned} &f(\mathrm{RRR}_{\mathrm{R}},R_{\mathrm{c}},N_{\mathrm{cr}},I,N)\\ &=\frac{1}{N+1}\left(\mathrm{RRR}_{\mathrm{R}}-\frac{1-2R_{\mathrm{c}}}{2N_{\mathrm{cr}}}\cdot I+N\cdot\mathrm{RRR}_{\mathrm{R}}\right)\\ &=\mathrm{RRR}_{\mathrm{R}}-\frac{1-2R_{\mathrm{c}}}{2N_{\mathrm{cr}}(N+1)}\cdot I, \end{aligned}$$

N is the number of previous votings, and N_{cr} is the number of the votings for a same resource, which is introduced to eliminate the discrimination. The visual representation of Eq. (1) is as shown in Fig. 2.

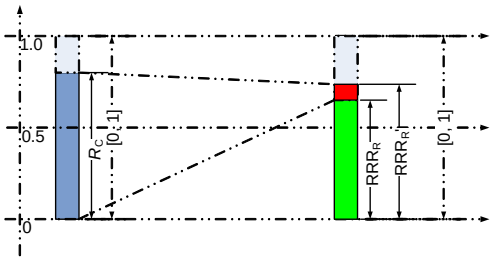

Fig. 2 A visual representation of Eq. (1)

As Eq. (1) states, the rating increment $-\frac{1-2R_{\mathrm{c}}}{2N_{\mathrm{cr}}(N+1)}\cdot I$ indicates that a higher rating (R_c) leads to a more reputable resource.

4.2 Incremental RIR generating algorithm

RIR is a key component in the information mechanism. Using the RIR voting strategy, malicious and arbitrary opportunistic voting can be detected, and careful and precise voting is encouraged.

As above stated, the core of the RIR incentive model is deducting the ratings of clients before transactions, and feeding back a different rating bonus, according to the precision of voting given by clients after transactions. We assume that the ratings of non-malicious voters follow the Gaussian distribution. With the Gaussian assumption, a voter may benefit if his/her rating is similar to most of the previous ones. However, the Gaussian assumption is not a necessity. It is used just for an experimental scenario. Numerous researchers have focused on the modeling of voting distribution (Griffiths, 2005). Their algorithms can also be applied to our RIR incentive model.

The probability density function (pdf) is a function that represents a probability distribution in terms of integrals. We adopt the Gaussian pdf to generate the increment of the user's RIR. The maximum value on the Gaussian pdf distribution curve comes at the mean voting rate. We define the maximum value as V_P, and define $\mathrm{RIR_I}$ as the ratio of the probability density of specified rating to V_P.

Assume that a client gives its rating R_c after using a resource R with the previous voting mean value V_m and variance V_v. The initial incremental RIR seeding of this transaction ($\mathrm{RIR_I}$) is defined as the ratio of the probability at the given rating to that at the maximum rating:

$$\mathrm{RIR_I}=2\cdot\frac{1}{N_{cr}}\frac{\mathrm{pdf}(R_c,\mu,\sigma)}{\mathrm{pdf}(\mu,\mu,\sigma)}=2\cdot\frac{\mathrm{pdf}(R_c,V_m,V_v)}{\mathrm{pdf}(V_m,V_m,V_v)\cdot N_{cr}}$$
$$=\frac{2}{N_{cr}}\cdot\exp\left(\frac{-(R_c-V_m)^2}{2V_v^{\,2}}\right). \quad (2)$$

Fig. 3 presents the simulation results of Eq. (2) under a fixed expected V_m and different V_v. The diagram shows the rating policy for voters. $\mathrm{RIR_I}$ increases with the increase of V_v, and decreases with the increase of (R_c-V_m). The variance of previous voting is out of the control of current voters, so the rating is crucial for the current voter to gain a higher RIR feedback. For example, if the standard deviation of previous voting is 0.3 ($V_v\approx0.1$), a new voter has to make sure that his/her rating for the resource falls in the range [0.38, 0.62] to gain an RIR increment.

Although the rating given by the voter (R_c) varies across resources, the accuracy of ratings ($\mathrm{RIR_I}$) of a same voter should be roughly the same. However, it is impossible for the genuine users to make no mistakes. Occasionally low $\mathrm{RIR_I}$ should not be considered as malicious or arbitrary behaviors. The most recent voting ratings (MRVR) mechanism is introduced to reduce the impact of occasionally low $\mathrm{RIR_I}$.

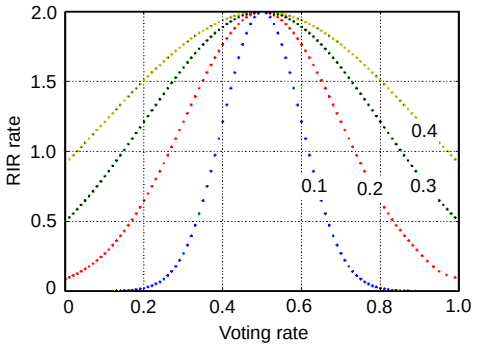

Fig. 3 Mapping of voting to $\mathrm{RIR_I}$ under a fixed voting mean value of 0.5 and different variances

The MRVR facility has several fixed slots to hold the most recent ratings of a client, and is inspired by the exponential average algorithm. A sorted exponential average algorithm is enforced to weaken the effects of occasionally low $\mathrm{RIR_I}$. All of the slots are initialized as 2. The final incremental RIR for the client is formulated as follows:

$$\mathrm{RIR_F}=\frac{1}{2^{n+1}}\sum_{i=1}^{n}2^i\cdot\mathrm{MRVR}_i, \quad (3)$$

where n is the number of MRVR slots for every account. In our demonstration each account has three MRVR slots. The MRVR slots follow the first-in first-out (FIFO) principle, but the ratings held are sorted from high to low to decrease the weight of occasional mistakes during the calculation.

Fig. 4 shows the changing of MRVR slots. It is obvious that the occasionally low $\mathrm{RIR_I}$ of 0.84 does not affect the $\mathrm{RIR_F}$ dramatically.

4.3 Information-hiding mechanism

According to the incremental RRR algorithm stated above, a single voting affects only the growth of RRR. The count of previous voting hidden to users, however, is also crucial to the final RRR of a resource. Thus, it is impossible to infer the vital parameters V_v and V_m in the RIR algorithm from the final RRR level; hence, speculators are prevented.

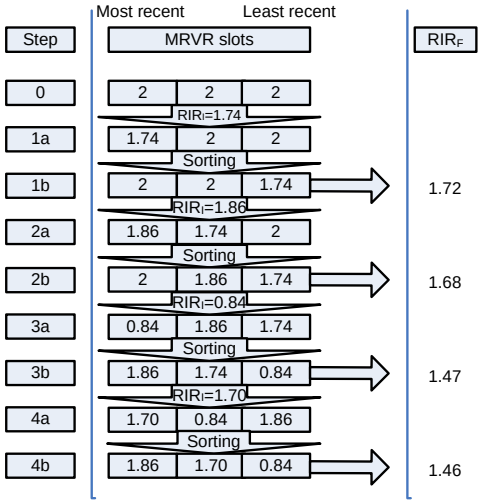

Fig. 4 Illustration of the most recent voting ratings (MRVR) mechanism

The combined RRR/RIR algorithms provide proper reputation information to every client, and hide the vital parameters, to prevent speculators. This combined mechanism encourages responsible voting and raises the valuable voting ratio in the P2P reputation network.

Under the combined RRR/RIR mechanism, a brilliant voter may find out that there is an implicative relationship between the final RRR level provided and the mean value of previous original voting. A 'good' or 'excellent' RRR indicates that the previous voting mean value of a resource is greater than 0.5, and vice versa. Therefore, the voting interval will merely be [0, 0.5] or [0.5, 1]. The only exception is the 'neutral level', which varies from 0.4 to 0.6. Hence, a surplus area with size 0.24 is balanced and is a reasonable policy.

Fig. 5 illustrates the detailed strategy. We assume that the previous ratings follow the Gaussian distribution with μ equal to the expected RRR and σ=0.3. Thus, at any time, V_m in Eq. (2) for resources is an approximately fixed value (approximately equal to their own expected RRR). The surplus areas for every resource are also approximately fixed.

However, the RRR level provided to the last voter changes with the growth of previous ratings. In Fig. 5a, the RRR of the resource reached 0.75 after 156 cycles; in contrast, in Fig. 5b, the RRR of the resource reached 0.75 after 86 cycles. The 157th voter in Fig. 5a and the 87th voter in Fig. 5b obtained the same RRR indications, but the surplus areas for them were definitely different.

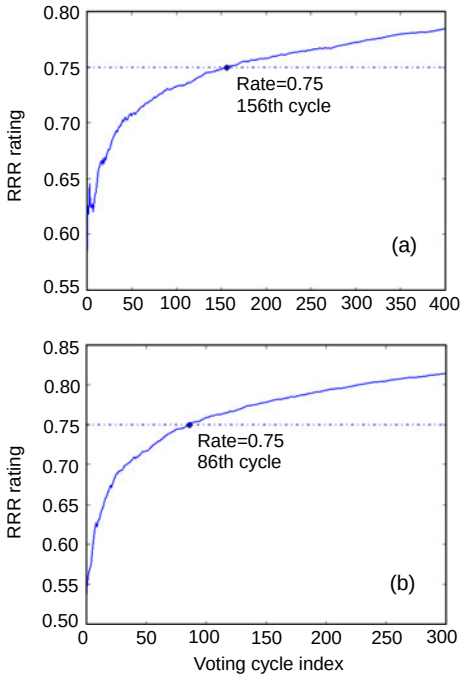

Fig. 5 Comparison of resource reputation rating (RRR) changing with different expected means
(a) 400 voting cycles, expected mean=0.7; (b) 300 voting cycles, expected mean=0.8

4.4 Ban strategy

As stated in Section 3, the bank agent is logically centralized and well known to all of the peers. Thus, it is easy to reject the resource request of a peer. Any activity of banned peers will be prohibited during the ban duration.

In this work, the peers with negative RIR rating are banned. The ban duration is formulated as

$$T_B = \delta \cdot \lceil |\mathrm{RIR}| \rceil, \tag{4}$$

where δ is the ban coefficient. δ is dependent on the specific system.

5 Experimental results

Experiments were carried out to illustrate the performances of the several voting models. For simplification, in the experiments a centralized rating storage facility was adopted in the P2P system.

5.1 Experimental hypotheses

There are some common assumptions for the demonstration:

1. Time is assumed to be slotted. The duration of the time slot is defined as the average interval between two successive resources requests.

2. The vote container has no more than 2000 ratings and the older is truncated to ensure the timeliness of ratings.

3. The system has three MRVR slots to trace the ratings for every peer, and a negative RIR peer is prohibited to conduct any activity for $2\lceil|\mathrm{RIR}|\rceil$ slots.

4. The population of peers is renewed according to a Poisson process with a mean rate of λ=10 peers per slot, while the total size is kept constant, 1500.

5. Every peer requests a resource with a certain probability γ=0.5, and the voting rating follows a Gaussian distribution with the standard deviation σ=0.3 and the mean value μ being the expected mean value of $\mathrm{RRR_R}$.

5.2 Incremental RRR generating algorithm

To demonstrate the effectiveness of the incremental RRR generating algorithm, five different resources were used in our test platform. At each slot, a different peer gave a voting rating for a randomly selected resource.

The five curves in Fig. 6 present the changing of RRR for resources under different mean values. Each vote affected only the increment of RRR, which means that both the rating and the count of previous votes affect the final RRR ratings of the resources. The increments indicated the quality of resources. The quality of a resource that is always receiving a negative increment will never be good.

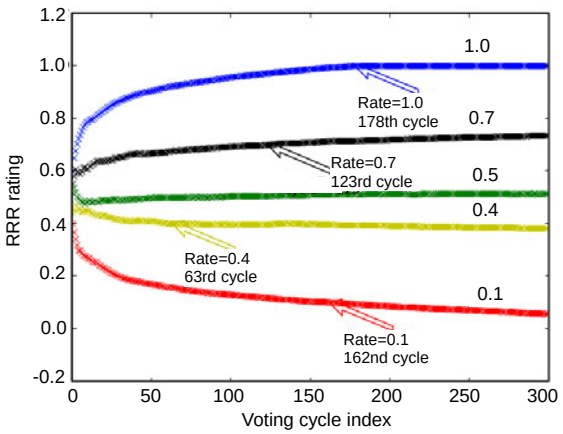

Fig. 6 Idealized resource reputation rating (RRR) under different mean values

5.3 Incremental RIR generating algorithm

The experiments involved arbitrary opportunistic and malicious voters. According to their characteristics, we classify their liar strategies into three possible types, some of which are similar to those in other related works (Dellarocas, 2000; Aberer and Despotovic, 2001; Ngan *et al*., 2003):

1. Destructive—malicious voters always send back a 'useless' feedback.

2. Opportunistic—arbitrary voters always send back an 'excellent' feedback.

3. Malicious—voters always give the collusive 'excellent' feedback cooperatively.

5.4 Generic interferences

Consider the scenario with arbitrary opportunistic peers. The number of arbitrary opportunistic voters was 300 (20% of the total voters).

As shown in Fig. 7, we toggled the ban infrastructure ON or OFF to enable or disable the incentive strategy. The incentive and penalty strategy identified the opportunistic voting and prohibited the arbitrary opportunistic voters. The opportunistic voters always provide 'excellent' feedbacks, so the RRR of an inferior resource was higher than expected without the ban strategy. Compared to Fig. 7a, the RRR ratings of resources were much closer to the expected ones in Fig. 7b.

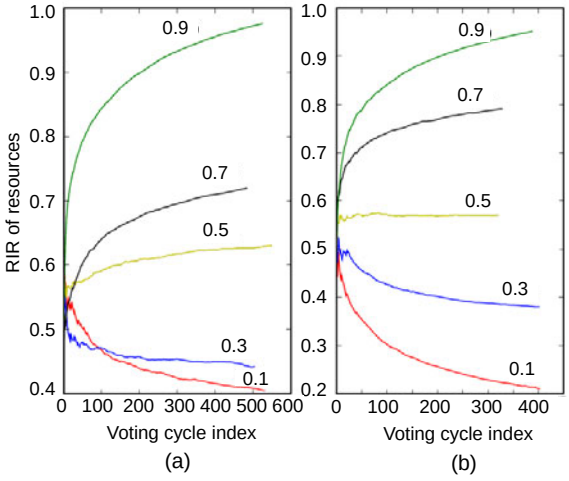

Fig. 7 Influence of the resource reputation rating (RRR) ban strategy on the RRR of resources with different expected RRRs

(a) Ban strategy disabled; (b) BanCycle=20RIR

5.5 Malicious attacks

This scenario involved 300 (20%) arbitrary opportunistic voters and 75 (5%) malicious voters. These malicious nodes all attacked a given resource. The attack models may be divided into two scenarios:

1. The malicious voters attack a well-known resource.

2. The malicious voters attack a blank resource.

Four resources were used in the simulation, and were divided into two groups: one group was attacked only during the second stage, to demonstrate scenario 1; the other was attacked by malicious voters throughout the voting, to demonstrate scenario 2. In either group, we used a reference resource to make a comparison. The expected RRR ratings of the four resources were all 0.9.

Fig. 8 illustrates that the impact of malicious voters on the well-known resources can be ignored, and that it is difficult for a blank resource under attack to gain its fame. In all cases, all of the malicious nodes were banned, and normal voters gained the RIR rating they deserved as time passed. At last, the opportunistic voters took advantage of the high expected RRR ratings of resources, so that they were identified as normal ones.

The misjudgment in the blank resource attacking model affects the fame of not only the victim resources but also the normal voters, as their voting behaviors for these victim resources may also be misjudged. However, attacking blank resources rarely occurs for lack of motivation—never being afraid of the loss of its fame, the blank resources provider may republish the blank resources to reset their rating at a very low cost. Moreover, normal voters generally dodge the attacked 'inferior' victim resources; therefore, the influence of the misjudgment on the normal voters is small.

5.6 Discrimination

In the rating system, every resource provider is eager to obtain a higher RRR rating for some privileges. There are always a small number of cheaters trying to increase their RRR ratings by using illegal approaches rather than improving the quality of services. The discriminating providers provide only their inferior resources to their collusive partners. And, the accomplices certainly provide 'excellent' feedbacks to the bank agent.

As shown in Fig. 9, a discriminating resource with 10 discriminating cheaters (0.67%) gained 17 valid votes, and finally its RRR rating was about 0.83. In contrast, a normal resource in the anchored group received 206 valid votes at the same time, and its RRR exceeded the cheater's.

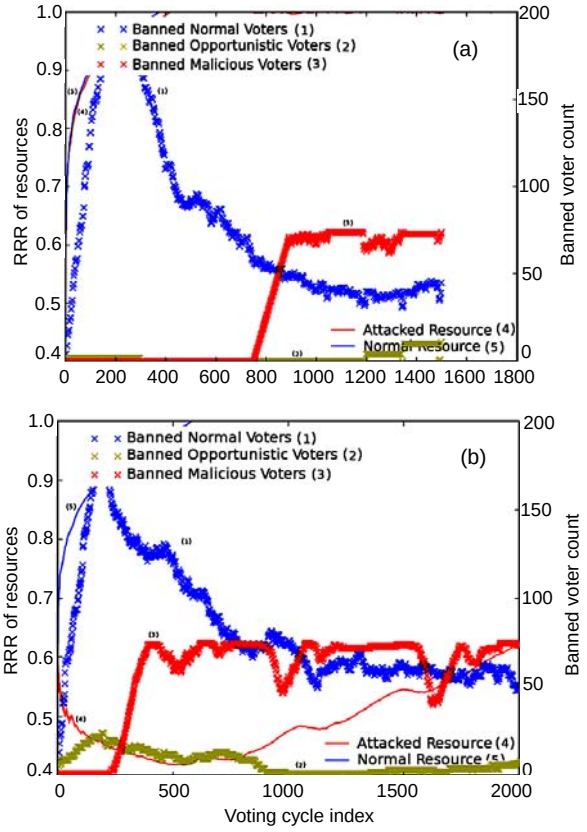

Fig. 8 Resource reputation rating (RRR) of non-blank resources (a) and blank resources (b) (20% opportunistic voters, 5% malicious voters, and BanCycle=20RIR)

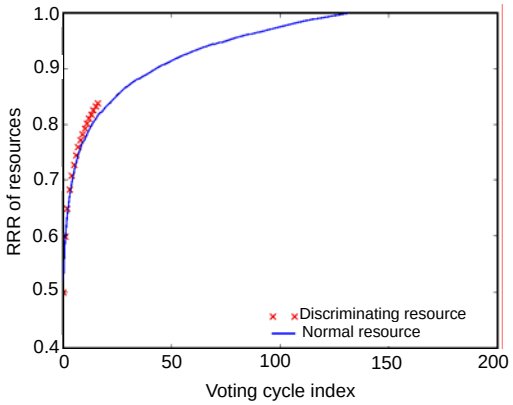

Fig. 9 Discriminating resources with 20% opportunistic voters, 10 discerning voters, and BanCycle=20RIR

6 Conclusions and future work

In this paper, we present an incentive model based on information-hiding to promote feedback in the P2P reputation network. Malicious and discriminating behaviors were discussed under our mechanism. The experimental results showed that the incentive model is very effective in eliminating blank resources and preventing malicious or arbitrary behaviors. In the future, we will exploit the singularity theory to restrict discriminating behaviors.

References

Aberer, K., Despotovic, Z., 2001. Managing Trust in a Peer-2-Peer Information System. Proc. 10th Int. Conf. on Information and Knowledge Management, p.310-317. [doi:10.1145/502585.502638]

Adar, E., Huberman, B.A., 2000. Free Riding on Gnutella. Available from http://www.eecs.harvard.edu/~jonathan/papers/2000 [Accessed on Aug. 3, 2009].

Antoniadis, P., Courcoubetis, C., Mason, R., Papaioannou, T.G., Stamoulis, G.D., Weber, R., 2004. Results of Peer-to-Peer Market Models. Project IST MMAPPS. Available from http://www.mmapps.org [Accessed on Aug. 12, 2009].

Chang, J.S., Wang, H.M., Yin, G., Tang, Y.B., 2007. A New Reputation Mechanism against Dishonest Recommendations in P2P Systems. Proc. 8th Int. Conf. on Web Information Systems Engineering, p.449-460. [doi:10.1007/978-3-540-76993-4]

Cohen, B., 2003. Incentives Build Robustness in BitTorrent. Proc. 1st Workshop on Economics of Peer-to-Peer Systems, p.250-260.

Dellarocas, C., 2000. Immunizing Online Reputation Reporting Systems Against Unfair Ratings and Discriminatory Behavior. Proc. 2nd ACM Conf. on Electronic Commerce, p.150-157. [doi:10.1145/352871.352889]

Feldman, M., Papadimitriou, C., Chuang, J., Stoica, I., 2004. Free-Riding and Whitewashing in Peer-to-Peer Systems. Proc. ACM SIGCOMM Workshop on Practice and Theory of Incentives in Networked Systems, p.228-236. [doi:10.1145/1016527.1016539]

Freedman, M.J., Aperjis, C., Johari, R., 2008. Prices Are Right: Managing Resources and Incentives in Peer-Assisted Content Distribution. Proc. 7th Int. Workshop on Peer-to-Peer Systems, p.1-6.

Griffiths, N., 2005. Task Delegation Using Experience-Based Multi-dimensional Trust. Proc. 4th Int. Joint Conf. on Autonomous Agents and Multiagent Systems, p.489-496. [doi:10.1145/1082473.1082548]

Jin, Y., Gu, Z.M., Gu, J.G., Zhao, H.W., 2007. A New Reputation-Based Trust Management Mechanism Against False Feedbacks in Peer-to-Peer Systems. Proc. 8th Int. Conf. on Web Information Systems Engineering, p.62-73. [doi:10.1007/978-3-540-76993-4]

Kamvar, S.D., Schlosser, M.T., Molina, H.G., 2003. The EigenTrust Algorithm for Reputation Management in P2P Networks. Proc. 12th Int. Conf. on World Wide Web, p.640-651. [doi:10.1145/775152.775242]

Liang, J., Kumar, R., Xi, Y., Ross, K., 2005. Pollution in P2P File Sharing Systems. IEEE INFOCOM, p.1174-1185. [doi:10.1109/INFCOM.2005.1498344]

Mislove, A., Post, A., Druschel, P., Gummadi, K.P., 2008. Ostra: Leveraging Trust to Thwart Unwanted Communication. Proc. 5th USENIX Symp. on Networked Systems Design and Implementation, p.15-30.

Ngan, T.W.J., Wallach, D.S., Druschel, P., 2003. Enforcing Fair Sharing of Peer-to-Peer Resources. Proc. 2nd Int. Workshop on Peer-to-Peer Systems, p.149-159. [doi:10.1007/b11823]

Papaioannou, T.G., Stamoulis, G.D., 2005. An Incentives' Mechanism Promoting Truthful Feedback in Peer-to-Peer Systems. Proc. 5th IEEE Int. Symp. on Cluster Computing and the Grid, **1**:275-283. [doi:10.1109/CCGRID.2005.1558565]

Xiong, L., Liu, L., 2004. PeerTrust: supporting reputation-based trust for peer-to-peer electronic communities. *IEEE Trans. Knowl. Data Eng.*, **16**(7):843-857. [doi:10.1109/TKDE.2004.1318566]

Yang, B.W., Song, G.H., Zheng, Y., 2008. ResourceDog: a Trusted Resource Discovery and Automatic Invocation P2P Framework. Proc. 5th IFIP Int. Conf. on Network and Parallel Computing, p.185-195. [doi:10.1007/978-3-540-88140-7_17]

Yang, M., Feng, Q.Y., Dai, Y.F., Zhang, Z., 2007. A Multi-dimensional Reputation System Combined with Trust and Incentive Mechanisms in P2P File Sharing Systems. Proc. 27th Int. Conf. on Distributed Computing Systems Workshops, p.29. [doi:10.1109/ICDCSW.2007.13]