Hindawi Publishing Corporation
Mathematical Problems in Engineering
Volume 2014, Article ID 189213, 11 pages
http://dx.doi.org/10.1155/2014/189213

Research Article

Prevention and Trust Evaluation Scheme Based on Interpersonal Relationships for Large-Scale Peer-To-Peer Networks

Lixiang Li,[1,2,3,4] Jürgen Kurths,[5] Yixian Yang,[2] and Guole Liu[2]

[1] *Institute of Network Coding, The Chinese University of Hong Kong, Shatin, NT, Hong Kong*
[2] *Information Security Center, State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, P.O. Box 145, Beijing 100876, China*
[3] *Shenzhen Research Institute, The Chinese University of Hong Kong, Shenzhen 518057, China*
[4] *Shenzhen Key Laboratory of Network Coding Key Technology and Application, Shenzhen 518057, China*
[5] *Potsdam Institute for Climate Impact Research, 14473 Potsdam, Germany*

Correspondence should be addressed to Lixiang Li; li_lixiang2006@163.com

Received 21 July 2014; Accepted 24 August 2014; Published 29 September 2014

Academic Editor: Haipeng Peng

In recent years, the complex network as the frontier of complex system has received more and more attention. Peer-to-peer (P2P) networks with openness, anonymity, and dynamic nature are vulnerable and are easily attacked by peers with malicious behaviors. Building trusted relationships among peers in a large-scale distributed P2P system is a fundamental and challenging research topic. Based on interpersonal relationships among peers of large-scale P2P networks, we present prevention and trust evaluation scheme, called IRTrust. The framework incorporates a strategy of identity authentication and a global trust of peers to improve the ability of resisting the malicious behaviors. It uses the quality of service (QoS), quality of recommendation (QoR), and comprehensive risk factor to evaluate the trustworthiness of a peer, which is applicable for large-scale unstructured P2P networks. The proposed IRTrust can defend against several kinds of malicious attacks, such as simple malicious attacks, collusive attacks, strategic attacks, and sybil attacks. Our simulation results show that the proposed scheme provides greater accuracy and stronger resistance compared with existing global trust schemes. The proposed scheme has potential application in secure P2P network coding.

1. Introduction

In P2P networks, due to their characteristics of openness, anonymity, and dynamic nature of P2P networks without verifications, peers can freely join in and leave the systems, which leads to a P2P system being vulnerable and easily attacked by malicious peers [1–16]. In P2P systems about 50% of the network peers perform malicious behaviors, which are providing false services, spreading malicious codes or viruses, and so forth [1, 4, 5, 10, 11]. In order to encourage and stimulate peers to participate in the system, it is very important to ensure the authenticity of shared resources and to resist malicious peers. One approach is building trust and reputation management to promote a good collaborative relationship among peers in the P2P systems. In these trust and reputation systems, the two matters of prime importance are ensuring the highly accurate trustworthiness of calculating trust and being robust to malicious peers. Currently, most trust and reputation systems focus on evaluating the credibility of resource providers [1–16], but in the absence of any central authority, repository, and global information there is no silver bullet for securing P2P networks [5, 10, 11].

In this paper, we present a prevention and trust evaluation scheme based on interpersonal relationships for large-scale P2P networks. The major contributions of this paper are as follows.

First, although some existing schemes consider the weights of peers, they believe that the weights of those peers with high credibility are greater than those of the peers with low credibility in the trust computing. From the point of view of interpersonal relationships, this view may not be completely reasonable. We put forward that the weights of

the peers who are familiar with the request peer are greater than those of the peers who are not. We also believe that the early experiences have a small impact on the trust evaluation, whereas the recent experiences contribute more.

Second, when it comes to the trust of peers, the existing schemes take it for granted that the QoS is equal to credibility. As a consequence, a request peer evaluates only the QoS of the provider. Considering the recommendation of other peers, the request peer merely considers the credibility of these peers, and how to calculate the credibility is very complex. In response to this problem, we distinguish QoS and QoR among peers. For one specific transaction, we propose that the request peer evaluates the QoS of the service provider and the QoR of the recommenders as well, which can easily improve the ability of resisting malicious behaviors.

Third, in order to prevent and describe the unpredictable and uncertain behaviors from malicious peers, we take all risk factors into consideration such as peer's trust value, context, transactions, and the accumulated speed of trust included. The risk value is used to prevent and measure various malicious behaviors, such as fluctuating behavior and misusage of trust. In our design, the weights of the risk factor are adjustable so that they can be effectively applied to different environments with different requirements.

2. Related Works

The main problem of reputation systems is how to deal with trust networks [13]. A trust network is a virtual network on top of a P2P system as shown in Figure 1, in which the bottom layer is the physical entities composed of the terminal machines, the middle layer is the logic layer of P2P systems, and the top layer is the trust layer composed of the trust ratings after peers' transactions.

The EigenTrust scheme [1] computes a global trust value for a peer by performing a distributed algorithm approaching the eigenvector of the trust matrix over the peers. The scheme relies on a reliable selection of some pretrust peers, who are supposed to be trusted by all peers and have higher trust. This assumption may not always be matched in a distributed computing environment. Because the pretrust peers may not exist lastly, and once they behave any malicious actions and score badly after some transactions, the system may not work reliably.

In a PeerTrust scheme [2], Xiong and Liu proposed three basic trust parameters and two adaptive factors to compute the trustworthiness of peers. They incorporated the concepts of a trust value and similarity with itself to compute credibility and satisfaction. The trustworthiness of a peer is considered to be a mean value of the evaluation of peers' behaviors, while the evaluation is given by the nearby peers. However, the limitation of this approach is that the computation convergence rate in large-scale P2P systems is not provided. The five factors used in their trust scheme may be retrieved with a heavy overhead.

In a R2Trust scheme [10], peers' trust values are evaluated from direct interactions and peers referrals. The scheme

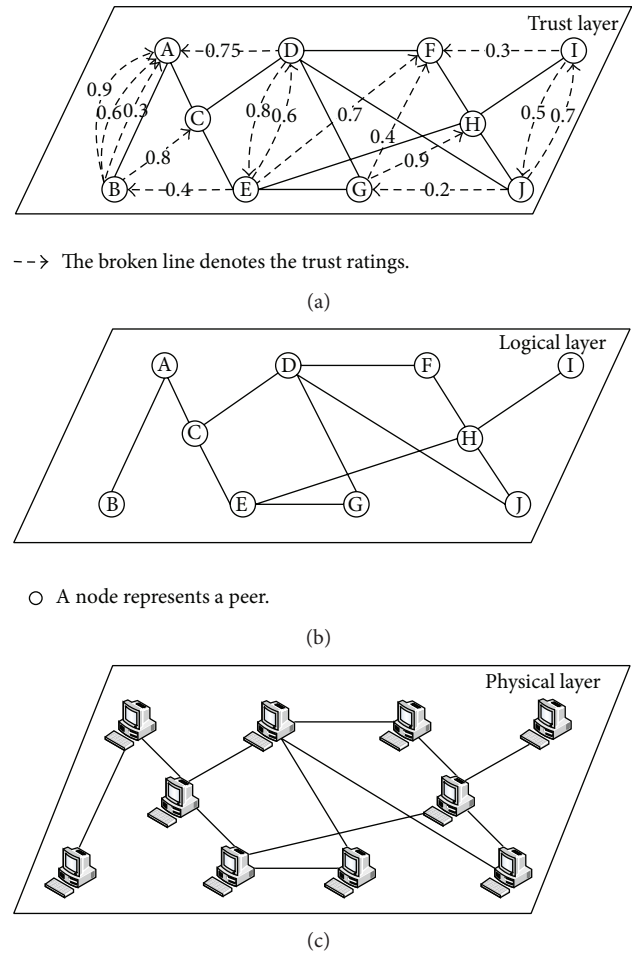


Figure 1: Trust overlay networks for a P2P system (color online).

distinguishes the credibility of peers. As a result, the aggregated trust value will filter out the noises and provide more accurate trust values. It can defend against several malicious attacks, such as simple malicious attacks, collusive attacks, and strategic attacks. But it has not taken measures to restrain fake and sybil attacks [17–19]. Li et al. [11] proposed multiple factors to be incorporated to reflect the complexity of trust. The weighted moving average and ordered weighted averaging combination algorithms can dynamically assign the properties (weights) of the multiple factors and calculate a more accurate trust value. But they did not give detailed analysis about resisting against peers' malicious behaviors of the scheme.

The above P2P trust and reputation systems are based on the assumption that the better the peer's QoS is, the higher the reputation of the peer is. These schemes only use a one-sided trust factor to quantify and predict trustworthiness among peers, which leads to lower resistance to malicious behaviors. In this paper, considering the interpersonal relationships among peers, the reputation of the peer is divided into service trust and recommendation trust. In addition, we put forward the comprehensive risk factors to prevent the malicious behaviors and propose a robust and efficient P2P reputation

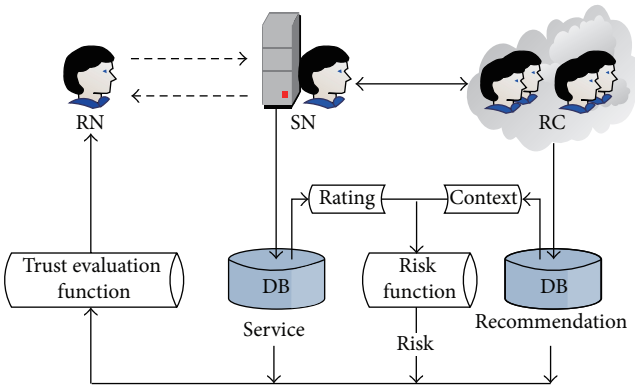


Figure 2: System structure of the prevention and trust evaluation scheme (color online).

system. We construct a mathematic scheme to discuss the capacity of resisting against malicious behaviors. Finally, we conduct simulations to illustrate them.

3. The Prevention and Trust Evaluation Scheme

In this section, we will present the basic framework of the prevention and trust evaluation scheme in detail.

3.1. Basic Framework. The behaviors of the network peers are determined by the operators and the peers should reflect the characteristics of operators. Based on the various roles in P2P systems, peers can be divided into three types: service node (SN), request node (RN), and recommendation node (RC). SN represents the peers who provide services for others in the networks, RN is the peers who request services, and RC denotes the peers who had transactions with SN in the past and recommend feedback to others. The detailed framework is shown in Figure 2.

Before a request node deals with a service node, the request node needs to consider three factors: the history records, the recommendation information, and the comprehensive risk factor. The decision information formed by the three factors through a trust evaluation function is sent to the request node. Then the request node determines whether the transaction is with the service node or not.

A peer enters the system with a unique identity, and it needs to be authenticated to communicate with other peers. When a new peer joins the P2P system, it cannot gain all the authority. It can only provide services to other peers, and when the number of the services is greater than the initial threshold (ϕ), the new peer can enter into the normal trust accumulation. With an the increase of the trust, the peer will have more authority. The accumulation of the trust is very slow, and once the peer has malicious behaviors, the accumulated trust is quickly reduced. Once a peer turns into a malicious one, it will lose all privileges.

Table 1: The transaction ratings of quality of service and quality of recommendation.

QoS	QoR	Description	Value
Good	*Good*	The peer is good.	(0.5, 1]
Common	*Common*	The peer is correct.	(0, 0.5]
Dishonest	*Dishonest*	The peer is dishonest.	[−0.5, 0)
Malicious	*Malicious*	The peer is malicious.	[−1, −0.5)

3.2. Trust Evaluation. Peers' trust evaluation consists of three parts: QoS trust value, QoR trust value, and risk factor value. All these three parts are calculated based on the history records of transaction ratings. We first classify the transaction ratings based on the quality of the provided by the SN and the RC, as shown in Table 1. We define the quality set QS = {*Good*, *Common*, *Dishonest*, *Malicious*}. The rating *Good* represents the good and honest peers, *Common* represents the peers who cause some damage, *Dishonest* represents the peers who provide false services or false recommendation, and *Malicious* represents the peers who spread the viruses or malicious codes. Note that the classification is flexible, and more classes or subclasses can be introduced if it is necessary [11, 13].

How to calculate these three parts' trust values will be discussed in Sections 4.1–4.3 in detail. The overall trust value of a peer is the maximum value of the three parts, and let $\mathrm{TV}_{i,j}$ denote the overall trust evaluation of the service provider j from the view point of the request peer i. Let $\mathrm{TS}_{i,j}$ denote the QoS trust value of peer j, $\mathrm{TR}_{i,j}$ is the QoR trust value of these peers having transactions with peer j in the past, and $R_{i,j}$ is the risk factor value of the service provider j. Therefore, the overall trust value for the service provider j at request peer i is defined as

$$\mathrm{TV}_{i,j} = \max\left(\alpha \mathrm{TS}_{i,j}, \beta \mathrm{TR}_{i,j}, \gamma R_{i,j}\right), \quad (0 \le \alpha, \beta, \gamma \le 1), \quad (1)$$

where α, β, γ are the weights of the related trust value and $\alpha + \beta + \gamma = 1$.

4. Trust Calculation and Analysis of the Resistance to Malicious Behaviors

In this section, we will present the trust calculation of our IRTrust scheme and analyze how to resist peers' malicious behaviors.

4.1. Service Trust Value. Let us assume that the request peer i finds the resource located in the peer j. The peer i has k transactions with peer j in the current time cycle m. The ratings that peer j got from peer i is the rating sequence $\{r_1, r_2, \ldots, r_k\}$. Peer j' accumulated a service trust value of the

kth transaction in the current time cycle m which is defined as

$$V_{i,j}(k) = \begin{cases} V_{i,j}(k-1) + e^{-a_1 * |r_k - 0.5|}, & r_k \in (0.5, 1], \\ V_{i,j}(k-1) + e^{-a_2 * |r_k + 0.5|}, & r_k \in (0, 0.5], \\ V_{i,j}(k-1) - e^{-a_3 * |r_k - 0.5|}, & r_k \in [-0.5, 0), \\ V_{i,j}(k-1) - e^{-a_4 * |r_k + 0.5|}, & r_k \in [-1, -0.5), \end{cases} \quad (2)$$

where a_1, a_2, a_3, a_4 are the adjustment factor of the accumulated reputation. The function e^{-x} decreases with the increasing of x, the accumulated reputation of *Good* rating should be better than that of *Common* rating, and the lost reputation of *Dishonest* rating should be less than that of *Malicious* rating. Thus, the adjustment factor should meet the following conditions $a_1 < a_2$, $a_3 > a_4$, which merge the accumulation function and the penalty function. The accumulated service trust value of the current time cycle m is defined as

$$\mathrm{AS}_{i,j}(m) = \frac{\sum_{i0=1}^{k} V_{i,j}(k)}{k}. \quad (3)$$

If there are n time cycles $\{t_1, t_2, \ldots, t_n\}$ from the beginning T_{start} to the end T_{end} and peer i has the number of transactions with peer j in each time cycle, the direct service trust value $\mathrm{TS}_{i,j}$ is computed directly from peer i's historical ratings for peer j. We define $\mathrm{TS}_{i,j}$ as follows:

$$\mathrm{TS}_{i,j} = \begin{cases} \dfrac{\sum_{i1=1}^{n} \mathrm{AS}_{i,j}(i1)}{n}, & \mathrm{AS}_{i,j}(i1) > 0, \\ 0, & \mathrm{AS}_{i,j}(i1) = 0. \end{cases} \quad (4)$$

4.2. Recommendation Trust Value. In a fully distributed P2P system involving numerous nodes, it is often not possible for a request peer to directly connect the service peer and to assess the trust value of the service provider. Instead, the request peer needs to resort to other peers in the P2P system and rely on the collective opinions to assess the trust. Although some trust schemes based on recommendation have already been proposed [2, 4, 5, 8, 9], they also lead to new challenges, such as how to determine the accuracy of collected opinions and how to efficiently aggregate referrals from diverse recommenders with different trustworthiness.

The recommenders' reputations are different from each other. The referrals from peers with high reputation are more trustworthy than those from peers with low reputation [2]. However, the referrals are treated equally and their credibility are not considered. In order to neutralize different reputation reports, Tian and Yang [10] proposed the credibility to weigh the feedback of the referrals. The recommenders from peers with high credibility are more trustworthy than those from low credibility peers. In this paper, we consider the peers in the P2P system as reflecting the characteristics of the interpersonal relationships. Due to that the peers with high reputation or credibility may not be willing to give recommendations to new peers. For example, a respected famous person may probably not write a recommendation for a stranger whom he (she) never knows. Therefore, the weight of the peers with high reputation or credibility may not be the greatest for the request peer. We deem that the acquainted peers of the request peer should have higher recommending weights.

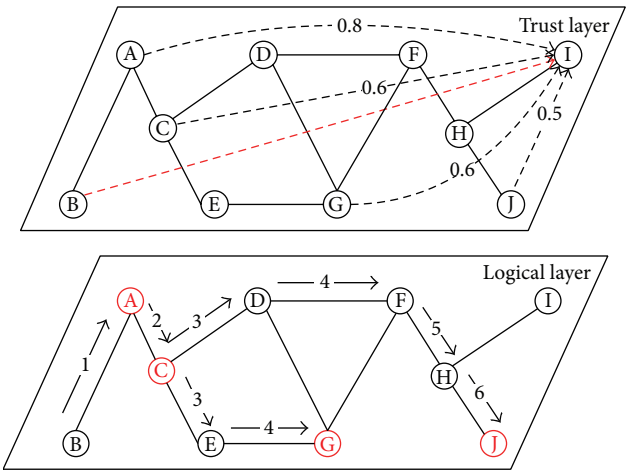


Figure 3: Computing the jumps of referrals (color online).

In IRTrust scheme, we use the jumps among peers of the logical layer to describe the relationships. When the jumps value is 1, the neighbors are the most acquainted ones to the request peer. The more the jumps are, the more remoter the relationships between the request peer and the recommenders are. For example, as shown in Figure 3, the service provider is peer I, the request peer is B, and the referral peers $\{A, C, G, J\}$ have transactions with the service provider in the trust layer. In the logical layer, the jumps with peer B are $\{1, 2, 4, 6\}$. Maybe the reputation or credibility of the peer J is the highest, but the recommending weight of peer A is the highest.

Suppose that the peer i has had k transactions with peer j in the current time cycle m. The referral peer P got the recommended rating sequence $\{c_1, c_2, \ldots, c_k\}$ from peer i. In the current time cycle m, we define the P accumulated recommendation trust value of the kth transaction as

$$C_{i,j}(k) = \begin{cases} C_{i,j}(k-1) + e^{-b_1 * |r_k - 0.5|}, & r_k \in (0.5, 1], \\ C_{i,j}(k-1) + e^{-b_2 * |r_k + 0.5|}, & r_k \in (0, 0.5], \\ C_{i,j}(k-1) - e^{-b_3 * |r_k - 0.5|}, & r_k \in [-0.5, 0), \\ C_{i,j}(k-1) - e^{-b_4 * |r_k + 0.5|}, & r_k \in [-1, -0.5), \end{cases} \quad (5)$$

where $C_{i,j}$ is the recommended rating sequence from i to j, and b_1, b_2, b_3, b_4 are the adjustment factors of the accumulated recommendation trust and they should meet $b_1 < b_2$, $b_3 > b_4$. The accumulated recommendation trust value of peer P in the current time cycle m is defined as

$$\mathrm{AR}_{i,j}(P, m) = \frac{\sum_{i0=1}^{k} C_{i,j}(k)}{k}. \quad (6)$$

If there are n time cycle $\{t_1, t_2, \ldots, t_n\}$ from the beginning T_{start} to the end T_{end} and the peer i has the number of transactions with the peer j in each time cycle, the recommendation

trust value $\mathrm{AR}_{i,j}(P)$ is computed from the peer i's historical ratings for the peer P. We define $\mathrm{AR}_{i,j}(P)$ as follows:

$$\mathrm{AR}_{i,j}(P) = \frac{\sum_{i2=1}^{n} \mathrm{AR}_{i,j}(P, i2)}{n}. \tag{7}$$

Assume that peers $\{P_1, P_2, \ldots, P_n\}$ are referrals to request peer i and that the relationship distances with peer i are $\{h_1, h_2, \ldots, h_n\}$. The inverse of h is the weight of referrals. If the h value is too large, it means that the request node needs to traverse the whole network, which will very strongly increase the computational effort. Here, we use the flooding algorithm with TTL to search the referrals. (The maximum of TTL value is 7 [20–22].) If $h > 7$ or the referral peer has left the network, we conform its h value to 10. Thus, the indirect recommendation trust value $\mathrm{TR}_{i,j}$ is defined as

$$\mathrm{TR}_{i,j} = \frac{\sum_{i3=1}^{n} (1/h_{i3})\, \mathrm{AR}_{i,j}(P_{i3})}{n}. \tag{8}$$

4.3. Risk Factor Value. The risk factor is used to describe the probability of the service provider's being a malicious peer. The reputation of service trust is an accumulative value for the past behaviors and reflects the overall evaluation got from the responding peers. However, it is not sensitive enough to perceive suddenly malicious behaviors of peers, because the value is posterior, and it will be decreased after the peer is spoiled. Thus, the risk factor is used to portray the unpredictable and uncertain behaviors of those potential malicious peers.

Li et al. [11] proposed the risk window to calculate the risk. The smaller of risk window size, the more accurate the risk assessment. But this will decrease the availability of the resources, because less risk for cooperation is requested and less peers are qualified to be cooperative. In R2Trust, the risk value is computed by applying the concept of information entropy which has been proven to be applicable in dealing with uncertain problems [10]. In this paper, the risk factor includes three parts: the rating risk factor (rr), the context risk factor (rt), and the cumulative speed factor (rs).

The rating risk factor rr can be used to restrain the simple and collusive malicious attacks. The rating risk factor is defined as

$$\mathrm{rr} = \frac{N_0}{N}, \tag{9}$$

where N is the number of ratings and N_0 is the number of ratings which are less than zero.

The contexts are complete transaction records including size, category, and time stamp. Here, we uniform the turnover of transactions. The context risk factor is used to restrain the strategic attack of peers. We define it as

$$\mathrm{rt} = \frac{\mathrm{turnover}_c}{\sum_{\mathrm{past}} \mathrm{turnover}}, \tag{10}$$

where $\mathrm{turnover}_c$ is the current transaction turnover.

The cumulative speed factor is the increased speed of trust of a service provider. It is also used to restrain the strategic attack which is defined as

$$\mathrm{rs}(m, m-1) = \frac{\mathrm{AS}(m) - \mathrm{AS}(m-1)}{T}, \tag{11}$$

where m is the current time cycle, $m-1$ is the pretime cycle, and T is the length of time cycle. If there are n time cycles $\{t_1, t_2, \ldots, t_n\}$ from the beginning T_{start} to the end T_{end},

$$\mathrm{rs} = \frac{\sum_{i4=1}^{n} \mathrm{rs}_{i4}}{n}. \tag{12}$$

The risk factor value is the overall value of the three parts and is defined as

$$R_{i,j} = \max(\mathrm{rr}, \mathrm{rt}, \mathrm{rs}). \tag{13}$$

The larger the risk factor value, the higher the probability that the service provider is the malicious peer.

4.4. Simple Attack Analysis. When this kind of malicious peers attacks, the vicious behaviors are isolated. They always provide the inauthentic services, maliciously slander the QoS of good peers, exaggerate the QoS of malicious peers, or fake the peers with high reputation [1–16]. For this kind of malicious peers attack, some literatures have already proposed corresponding measures. In PeerTrust, the feedback of a peer and the credibility factor for the feedback are used to resist the exaggerating and slandering [2]. In R2Trust, a reputation evaluation factor is proposed to resist the malicious behaviors [10]. In [23], digital signature is used to restrain the fake behaviors. In this paper, we described our measures which can restrain these malicious behaviors.

If a peer provides inauthentic services, such as false files, malicious code, and Trojan virus, the penalty function as is given in (2) will reduce its service reputation quickly, and this will seriously weaken the role of the peer in the network. When its service reputation is low enough, the peer will lose its effectiveness, that is, downloading and recommending. If a peer maliciously slanders the QoS of good peers or exaggerates the service quality of malicious peers, its corresponding reputation will be reduced when one of the others is communicated with the peer which is maliciously slandered or exaggerated. Then the peer will lose the corresponding effectiveness. To avoid a peer faking other peers with high reputation, we adopt the authentication technology based on identification in the process of peers' communication.

4.5. Collusion Attack Analysis. Collusion attack is broadly defined as any malicious coordinated behavior of a group of users aimed at gaining undeserved benefits or at damaging well behaved users. Thus, this kind of attack behavior is a kind of joint attack of a group of peers. In the group, each peer is well behaved and never provides inauthentic services or defames the reputation of other members. But this type of malicious peers can form a malicious cycle by assigning a high trust value to other malicious peers in the network.

Collusive peers provide inauthentic services to outsiders when selected as download sources and provide denigrated ratings for those noncollusive peers [2, 7, 24–30].

The collusive peers can hide their malicious intentions in an unstructured P2P system by assigning high trust value to each other. To solve this problem, Xiong and Liu assumed that there is no similarity in the evaluation to peers mutually, when a collusive peer does a good rating to the target peer [2]. The tolerance to the collusive attack has been improved to put weight on the evaluation value by using this similarity. Sato proposed the trust estimation method to give a defense against the collusive attack: the maximum likelihood estimation method [7]. Some literatures use encryption algorithms, game theory, and economics to resist a collusion attack [27–30].

In this paper, being different with previous literatures, the reputation of peers is divided into service reputation and recommendation reputation. When peers communicate or trade with each other, the request peer needs to evaluate the QoS of the service peer, and at the same time, it is required to evaluate the QoR of the peers who have connections with the service peer. This measure can effectively resist collusion attack. Once one of the collusion peers maliciously attacks the request peer, not only the service reputation of the peer but also all its neighbors' recommendation reputation will be punished by the penalty function as is given in (5). Namely, if a peer maliciously attacks, the whole group will be punished.

4.6. Strategy Attack Analysis. This kind of malicious attack behavior has a clear purpose. In the beginning, the malicious peers are well behaved and accumulated the reputation by honest services. Once these peers build good reputation, then they will start to abuse their credibility to mislead other peers [1]. They always adopt low cost to increase their reputation when they do a strategy attack. Taking the overdraft of credit card as an example, one person wants to overdraw the credit card maliciously. First, he/she needs to increase his/her credit in order to get more amounts. The strategy is to pay the small overdraft back promptly. The credit is accumulated by the frequent consumption-repayment process. When the credit reaches to a certain degree, the person will own more overdraft amounts. Eventually the person can overdraw all the amounts and does not pay the debts again.

Strategy attack is also called onCoff attack in some literatures. To address such potential dynamic behaviors of peers, Xiong and Liu proposed a simple adaptive time window-based algorithm to better react to the above behaviors [2]. Tian and Yang introduced a risk factor value and information entropy to the trust computation in order to portray the unpredictable and uncertain behaviors of these malicious peers [10]. In this paper, we retain the parameter of the context risk factor, and at the same time, we define the reputation accumulative speed as is given in (10) and (12).

4.7. Sybil Attack Analysis. A sybil attack is the one in which a malicious attacker subverts the reputation system of P2P network by creating a large number of pseudonymous entities and uses them to gain a disproportionately large influence. The reputation system's vulnerability to a sybil attack depends on (i) how cheaply identities can be generated, (ii) the degree to which the reputation system accepts inputs from entities that do not have a chain of trust linking them to a trusted entity, and (iii) whether the reputation system treats all entities identically.

A sybil attack is a powerful threat faced by any decentralized distributed P2P system that has no central, trusted authority to vouch for a one-to-one correspondence between users and identities [1]. Generally, the users only have a rating describing how well the user behaves in a reputation system. For example, eBay ratings are based on users' previous transactions with other users. Buyers and sellers in eBay rate each other after every transaction, and the overall reputation is the sum of these ratings over the last six months. Sybil attacks can create a large number of sybil nodes that collude to artificially increase a user's rating.

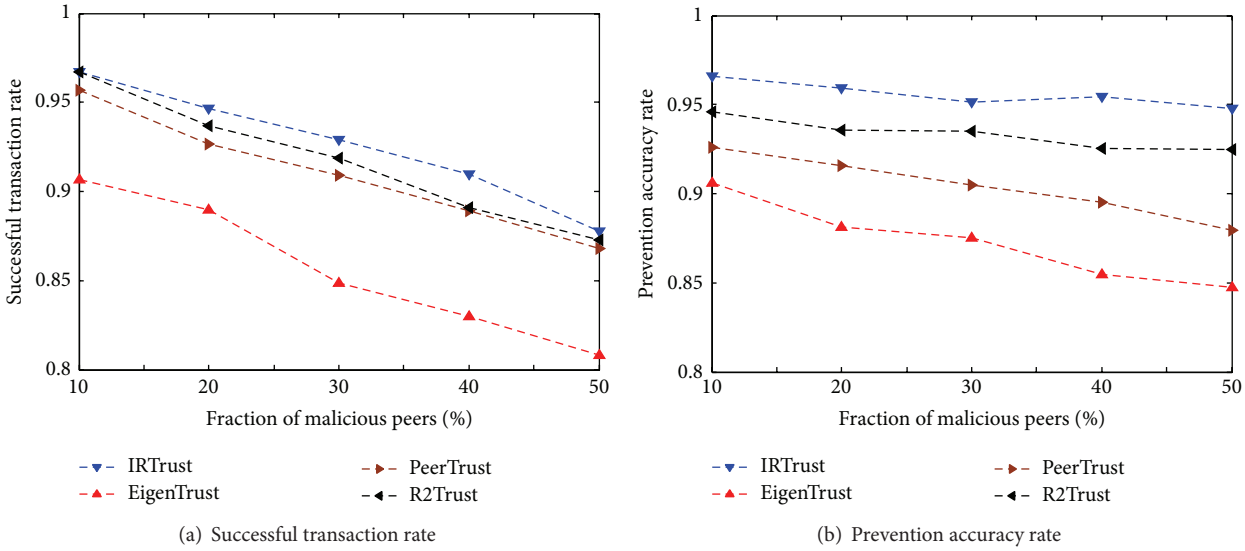
The existing literatures have done some researches on this type attack. Cheng and Friedman [17] surveyed and found that many existing reputation mechanisms were not resistant to this type of attack behavior. They used a static graph formulation of reputation and formalized the notion of sybilproofness. Yu et al. [18] proposed a detection mechanism (called SybilGuard) that relies on social networks of P2P users to limit the corruptive influences of sybil attacks. Quercia and Hailes [19] proposed an effective way of identifying sybil attackers for in-range portable devices (MobID) to reduce the number of interactions with sybil attackers and consequently enable collaborative applications.

In this paper, identity-based authentication techniques are used to prevent sybil attacks and dismiss masquerading hostile entities. When a peer joins the reputation system, it can only be one identity, and it is not allowed to create multiple identities. We use the SHA-1 hash function to realize the uniqueness and the anonymity. In addition, we set the transaction threshold ϕ (such as 50) to limit the permission of the new intrant peers. Namely, the new peers only provide service and have no permission to other operations. Once the number of service is more than the threshold, the peers may enter into the normal trust assessment. These measures can effectively resist sybil attacks.

5. Experiments and Comparisons

In this section, we will present results of our experiments which will show the effectiveness of our trust scheme. Firstly, we repeat the EigenTrust [1], the PeerTrust [2], and the R2Trust [10] simulator experiments using the Query Cycle Simulator and Matlab 2008. In our evaluation, we assess the performance of our scheme and compare it with the EigenTrust [1], the PeerTrust [2], and the R2Trust [10] schemes. We study their performance under a variety of malicious threat behaviors (discussed in Sections 4.2–4.7). We perform 100 query cycles in our simulations and the simulation results are the average expectations.

5.1. Simulation Environment. Considering the characteristics of P2P networks, such as the node degree distribution with



(a) Successful transaction rate

(b) Prevention accuracy rate

FIGURE 4: Performances of IRTrust, EigenTrust, PeerTrust, and R2Trust in simple attack (color online).

a power-law distribution, we construct the P2P network based on a BA scale-free network to approach to real-world networks. There are two types of peers: honest and malicious ones. The honest peers always give the correct service and feedback, but the malicious peers always give the opposite opinion to others when they own the corresponding power. In our experiments, we use the flooding algorithm to compute the interpersonal distance between peers; the detailed algorithm is given in the literature [20].

In the simulation we assume that there are 5000 peers in the network. Among them, there are 500–2500 malicious peers and the query message is flooded with TTL = 7. In the experiment, the peer's changing is in the uptime stage and is uniformly distributed over $[0, 1]$. The change of issuing queries in the uptime is uniformly distributed over $[0, 0.5]$. In addition, different types of peers also vary in their behaviors when responding to queries and providing files. For good peers, the probability of providing authentic files is 100%. Simple malicious peers will respond to all queries when they have received and provide inauthentic files with a probability of 100%. Collusive peers provide with a probability of 100% malicious files to other peers. Other parameters in the experiments are given in Table 2.

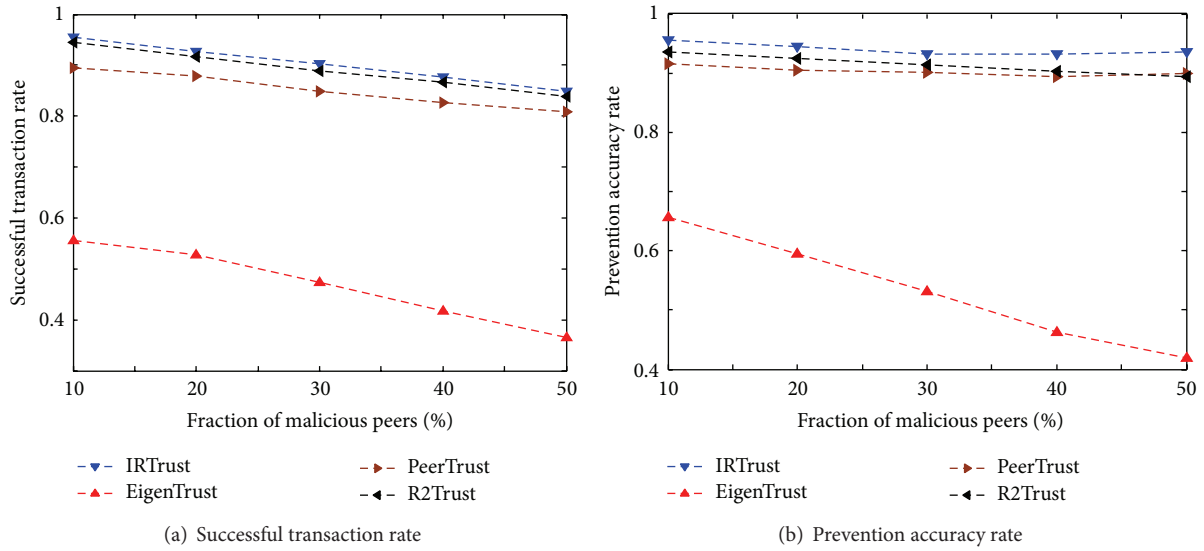
We compare the successful transaction rate and the prevention accuracy rate of our scheme with the EigenTrust, the PeerTrust, and the R2Trust under the conditions of simple, collusive, strategic, and sybil attacks. The metrics, successful transaction rate, is the ratio of the number of the successful transactions over the total number of transactions. It is typically used to evaluate the efficiency of a trust scheme [2, 10]. The prevention accuracy rate is the ratio of the number of successful transactions with forecasting the peer's status correctly over the total number of transactions.

5.2. Simple Attack. Figure 4 depicts our simulations under the condition of simple malicious peers. In Figure 4(a), when the ratio of malicious peers is low in the system, all the four schemes perform high successful transaction rates. With the fraction of malicious peers increasing, the successful transaction ratio of all the schemes decreases, but it decreases most intensely in the EigenTrust scheme. However as a whole, the four schemes keep high efficiency, because they punish the malicious peers. The successful transaction ratio of EigenTrust scheme drops more quickly than the other schemes because the EigenTrust scheme does not differentiate the reliability of all the referrals. In comparison with the PeerTrust scheme and the R2Trust scheme, the proposed IRTrust scheme retains a very high successful transaction rate, and it even retains about 90% when the fraction of malicious peers is 50%.

Figure 4(b) depicts the prevention accuracy rate of these four schemes. Compared to all the four schemes, the rate of the EigenTrust scheme is the least and decreases with the increasing of the fraction of malicious peers. Although the experimental results show some fluctuations, the rate of the IRTrust scheme is the best and can reach 96%. But as a whole, the four schemes keep high efficiency, because they have punishment measures to malicious peers. In addition, the

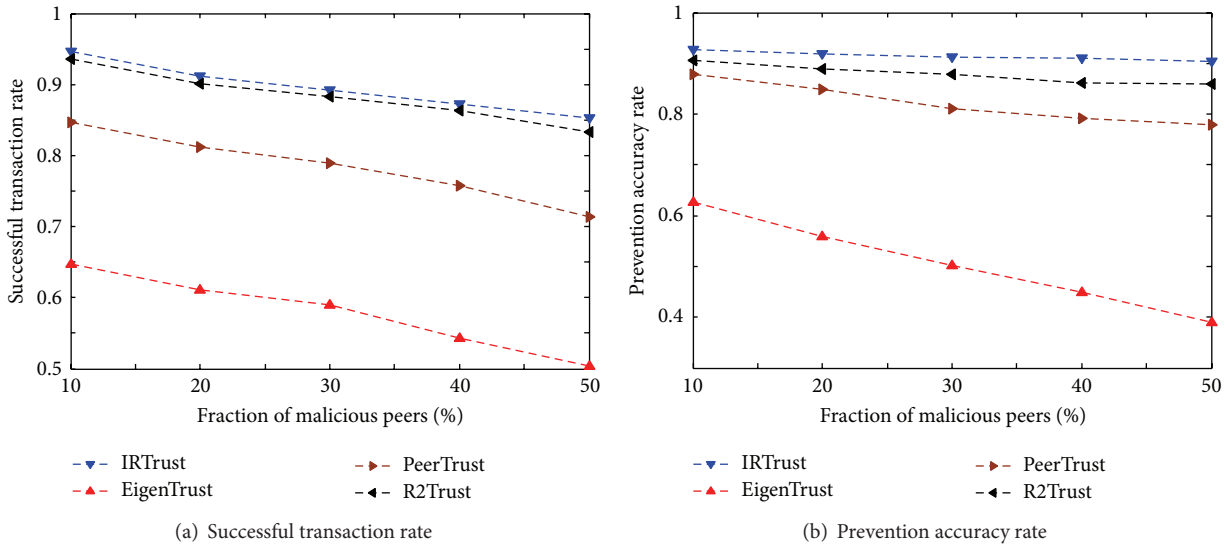
TABLE 2: The parameters and their values in the simulations.

Parameters	Description	Value
(α, β, γ)	Weight of direct trust value, indirect recommendation value, and peer's risk value	(0.3, 0.2, 0.5)
(a_1, a_2, a_3, a_4)	Adjustment factors	(3, 6, 4, 8)
(b_1, b_2, b_3, b_4)	Adjustment factors	(3, 6, 4, 8)
η	The ratio of malicious peers	(0.1–0.5)
ϕ	Threshold of the number of services	50
N	The size of P2P networks	5000



(a) Successful transaction rate (b) Prevention accuracy rate

FIGURE 5: Performances of IRTrust, EigenTrust, PeerTrust, and R2Trust in collusion attack (color online).



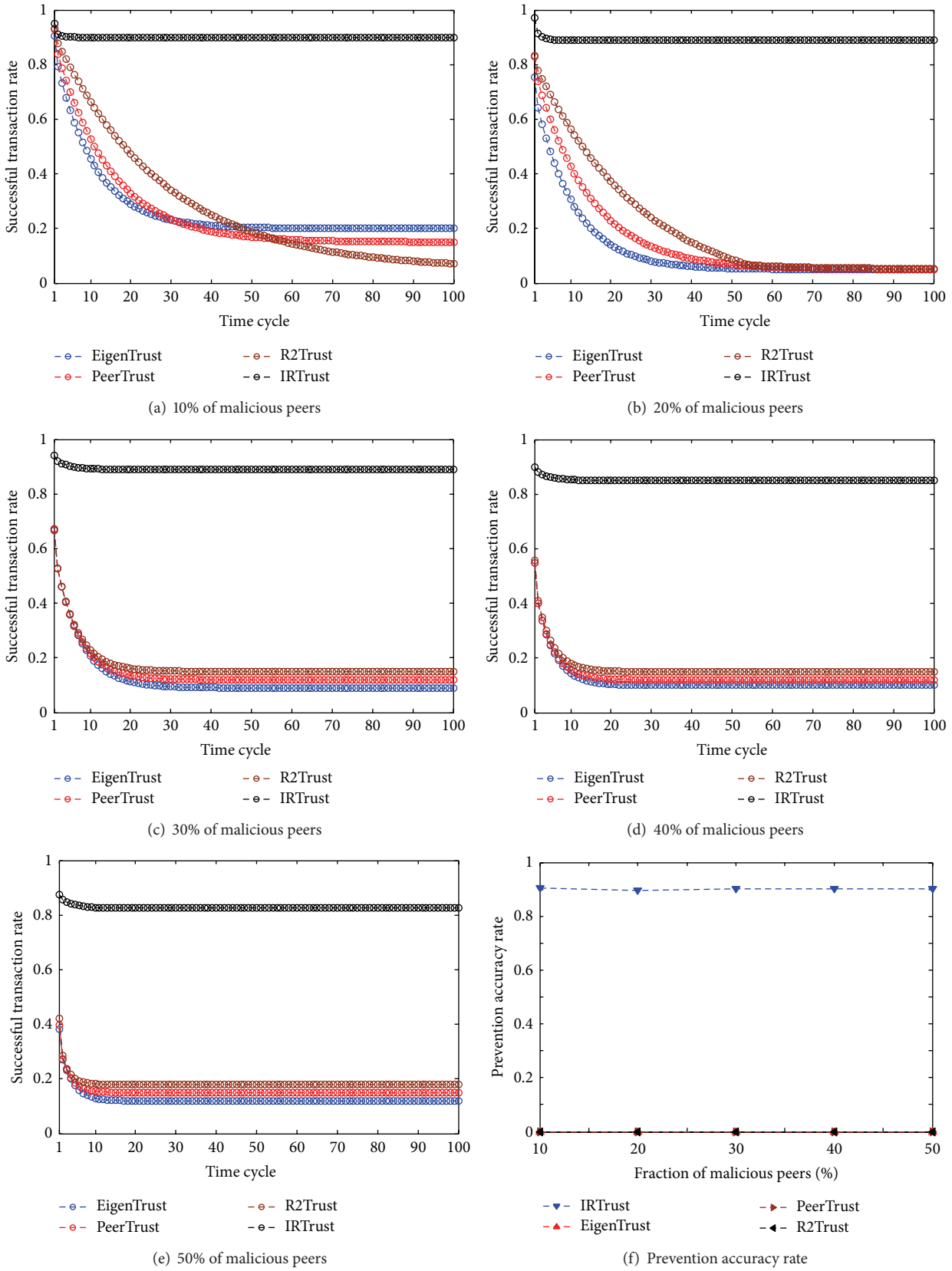
(a) Successful transaction rate (b) Prevention accuracy rate

FIGURE 6: Performances of IRTrust, EigenTrust, PeerTrust, and R2Trust in strategy attack (color online).

R2Trust scheme and the IRTrust scheme have risk assessment measures.

5.3. Collusion Attack. Figure 5 shows the simulations under the condition of collusive malicious peers. Each peer in the colluding group provides inauthentic services to the peers outward, boosts the trust value of their accomplices regardless of their behaviors, and downplays the trust value of good providers. In Figure 5(a), we can see that the successful transaction rate of the EigenTrust scheme descends obviously when the number of malicious peers increases. Because it does not give clear differentiations about the reliability of all the referrals, namely, more malicious peers will lead to more computations. Although the PeerTrust scheme owns high efficiency, it has no risk factor of peer, and it is inferior to the two other schemes. Compared to the R2Trust scheme, the IRTrust scheme is designed to tackle collusive attacks with differentiating the service and recommendation, and therefore it is proved more robust against collusive attacks.

In Figure 5(b), we can see that the prevention accuracy rate of the EigenTrust scheme descends evidently when the number of malicious peers increases. Since the scheme can not differentiate the reliability of the referrals, the more malicious peers, the more transactions with the malicious peers. In the PeerTrust scheme, it has community factor to resist the collusive attack, and the R2Trust scheme uses the relative reputation difference to identify the collusive attack. Therefore, they can maintain a higher prevention accuracy rate to this type of malicious attack. Compared to the rest schemes, the IRTrust scheme is designed to tackle collusive



(a) 10% of malicious peers

(b) 20% of malicious peers

(c) 30% of malicious peers

(d) 40% of malicious peers

(e) 50% of malicious peers

(f) Prevention accuracy rate

FIGURE 7: Performances of IRTrust, EigenTrust, PeerTrust, and R2Trust in sybil attack (color online).

attacks with differentiating the service and recommendation, and the efficiency is stable and the highest.

5.4. Strategy Attack. Figure 6 depicts the simulations under the condition of strategic malicious peers. Figure 6(a) depicts the transaction rate of these four schemes. Although the EigenTrust scheme uses the global trust value to resist this type of attack, the demand of close cooperation of peers and time synchronization is higher. The more peers and more malicious ratio, the lower successful transaction ratio. The PeerTrust can effectively restrain the strategic attack, but the trust accuracy of PSM algorithm is affected by the width of the sliding window. Its performance is inferior to the R2Trust scheme and IRTrust scheme. Compared to PeerTrust scheme and R2Trust scheme, the proposed IRTrust scheme retains higher successful transaction rates. Even the fraction of malicious peers is 50% and the successful transaction rate maintains about 86%.

Figure 6(b) depicts the prevention accuracy rate of them. To this type of malicious attack, a good idea is to keep all the transaction records and the contexts. The EigenTrust scheme needs to keep closer cooperation of peers and higher time synchronization, which defends against this kind of attack. Thus, its prevention accuracy ratio is the least which decreases quickly with the malicious peers increasing. The PeerTrust scheme can effectively restrain the strategic attack by adopting the PSM algorithm, but the performance of PSM algorithm seriously relies on the width of the sliding window. As a result, this scheme is inferior to the R2Trust scheme and IRTrust scheme. Compared to PeerTrust scheme and R2Trust scheme, the proposed IRTrust scheme keeps higher and more stable prevention accuracy rates. Even the fraction of malicious peers is 50% and the prevention accuracy rate is about 90%.

5.5. Sybil Attack. Figure 7 shows the simulations under the condition of sybil malicious peers. In Figures 7(a)–7(e), these simulations are the successful transaction ratios in the different size of malicious peers. When the ratio of malicious nodes is small, at the initial stage, the transaction success rate is relatively high, but as the increase of time period, the malicious node will attack scope which will be larger and larger and the transaction success rate will rapidly decline. Because these three models (EigenTrust, PeerTrust, and R2Trust) can not distinguish sybil attacks, the more the malicious nodes, the lower the transaction success rate. The successful transaction ratio of the IRTrust scheme decreases with the increasing of the fraction of malicious peers, and it is about 85% when the fraction of malicious peers is 50%.

Figure 7(f) depicts the prevention accuracy ratio of these four schemes. A peer joins the system with multiple identities, and it provides inauthentic services or malicious attack to the others using one of the identities. When its reputation is reduced by the system, the peer can exit the system and rejoin the system with a new identity again. Although the EigenTrust, PeerTrust, and R2Trust schemes adopt the global trust value to restrain the malicious attack of peers, they can not address the problem of sybil attack. In IRTrust scheme, we use identity-based authentication techniques, set the service threshold, and restrict the reputation accumulative ratio to put off and restrain the sybil attack. Therefore, our trust scheme can effectively prevent the peers' malicious behaviors, and the prevention accuracy ratio is stable and can keep about 90% in the simulations.

6. Conclusion

To encourage resource sharing among peers and resist malicious behaviors, trust management is essential for peers to assess the trustworthiness of others and to interact selectively with more reputable ones. In this paper, we fully consider the interpersonal relationships among peers and present an IRTrust scheme. To improve the resistance of malicious peers, the proposed scheme adopts the identity authentication, distinguishes the service and recommendation, and uses the comprehensive risk factor to prevent malicious attack and evaluate the trustworthiness of a peer. The IRTrust scheme is highly resistant to the malicious behavior attacks of peers, such as simple attacks, collusive attacks, strategic attacks, and sybil attacks. The simulation results prove that our trust scheme performs well even when the fraction of malicious peers in the system reaches 50%.

The study of secure network coding scheme suitable for P2P networks is a hot topic, and the scheme and analysis method of different attacks in this paper have potential application in designing secure P2P network coding.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgments

This paper is supported by the AoE Grant E-02/08 from the University Grants Committee of the Hong Kong Special Administration Region, China, the Hong Kong Scholars Program (Grant no. HJ2012005), the China Postdoctoral Science Foundation Funded Project (Grant no. 2012T50209), the Shenzhen Key Laboratory of Network Coding Key Technology and Application (Grant no. ZSDY20120619151314964), the Peacock Scheme (Grant no. KQCX20130628164008004), the Fundamental Research Fund (Grant no. JCYJ2013401171935815), Shenzhen, China, and the National Natural Science Foundation of China (Grant nos. 61170269, 61121061).

References

[1] S. D. Kamvar, M. T. Schlosser, and H. Garcia-Molina, "The eigentrust algorithm for reputation management in p2p networks," in *Proceedings of the 12th International Conference on World Wide Web (WWW '03)*, pp. 640–651, May 2003.

[2] L. Xiong and L. Liu, "PeerTrust: Supporting reputation-based trust for peer-to-peer electronic communities," *IEEE Transactions on Knowledge and Data Engineering*, vol. 16, no. 7, pp. 843–857, 2004.

[3] Z. Liang and W. Shi, "PET: a personalized trust model with reputation and risk evaluation for P2P resource sharing," in *Proceedings of the 38th Annual Hawaii International Conference on System Sciences*, January 2005.

[4] A. Jøsang, R. Ismail, and C. Boyd, "A survey of trust and reputation systems for online service provision," *Decision Support Systems*, vol. 43, no. 2, pp. 618–644, 2007.

[5] R. Zhou and K. Hwang, "PowerTrust: a robust and scalable reputation system for trusted peer-to-peer computing," *IEEE Transactions on Parallel and Distributed Systems*, vol. 18, no. 4, pp. 460–473, 2007.

[6] K. Watanabe, Y. Nakajima, T. Enokido, and M. Takizawa, "Ranking factors in peer-to-peer overlay networks," *ACM Transactions on Autonomous and Adaptive Systems*, vol. 2, no. 3, article no. 11, 2007.

[7] F. Sato, "Estimation of trustworthiness for P2P systems in a collusive attack," *International Journal of Web and Grid Services*, vol. 4, no. 1, pp. 24–34, 2008.

[8] K. Chen, K. Hwang, and G. Chen, "Heuristic discovery of role-based trust chains in peer-to-peer networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 20, no. 1, pp. 83–96, 2009.

[9] M. Jamali and M. Ester, "TrustWalker: a random walk model for combining trust-based and item-based recommendation," in *Proceedings of the 15th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD '09)*, pp. 397–405, July 2009.

[10] C. Tian and B. Yang, "R 2Trust, a reputation and risk based trust management framework for large-scale, fully decentralized overlay networks," *Future Generation Computer Systems*, vol. 27, no. 8, pp. 1135–1141, 2011.

[11] X. Li, F. Zhou, and X. Yang, "A multi-dimensional trust evaluation model for large-scale P2P computing," *Journal of Parallel and Distributed Computing*, vol. 71, no. 6, pp. 837–847, 2011.

[12] G. Ciccarelli and R. Lo Cigno, "Collusion in peer-to-peer systems," *Computer Networks*, vol. 55, no. 15, pp. 3517–3532, 2011.

[13] Z. Despotovic and K. Aberer, "P2P reputation management: probabilistic estimation vs. Social networks," *Computer Networks*, vol. 50, no. 4, pp. 485–500, 2006.

[14] P. Dewan and P. Dasgupta, "P2P reputation management using distributed identities and decentralized recommendation chains," *IEEE Transactions on Knowledge and Data Engineering*, vol. 22, no. 7, pp. 1000–1013, 2010.

[15] A. Satsiou and L. Tassiulas, "Reputation-based resource allocation in P2P systems of rational users," *IEEE Transactions on Parallel and Distributed Systems*, vol. 21, no. 4, pp. 466–479, 2010.

[16] Y. Wang and A. Nakao, "Poisonedwater: an improved approach for accurate reputation ranking in P2P networks," *Future Generation Computer Systems*, vol. 26, no. 8, pp. 1317–1326, 2010.

[17] A. Cheng and E. Friedman, "Sybilproof reputation mechanisms," in *Proceedings of the ACM SIGCOMM 3rd Workshop on the Economics of Peer-to-Peer Systems (P2PECON '05)*, pp. 128–132, August 2005.

[18] H. Yu, M. Kaminsky, P. B. Gibbons, and A. Flaxman, "Sybilguard: defending against sybil attacks via social networks," in *Proceedings of the 6th ACM SIGCOMM Conference on Internet Measurement*, 2006.

[19] D. Quercia and S. Hailes, "Sybil attacks against mobile users: friends and foes to the rescue," in *Proceedings of the INFOCOM*, 2010.

[20] A. Iamnitchi, M. Ripeanu, and I. Foster, "Small-world file-sharing communities," in *Proceedings of the 23rd Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM '04)*, vol. 2, pp. 952–963, March 2004.

[21] E. Meshkova, J. Riihijärvi, M. Petrova, and P. Mähönen, "A survey on resource discovery mechanisms, peer-to-peer and service discovery frameworks," *Computer Networks*, vol. 52, no. 11, pp. 2097–2128, 2008.

[22] M. Yang and Z. Fei, "A novel approach to improving search efficiency in unstructured peer-to-peer networks," *Journal of Parallel and Distributed Computing*, vol. 69, no. 11, pp. 877–884, 2009.

[23] J. Liu, R. Sun, and K. Kwak, "Fair exchange signature schemes," *Science China Information Sciences*, vol. 53, no. 5, pp. 945–953, 2010.

[24] T. Gamer, "Collaborative anomaly-based detection of large-scale internet attacks," *Computer Networks*, vol. 56, no. 1, pp. 169–185, 2012.

[25] S. Marti and H. Garcia-Molina, "Taxonomy of trust: categorizing P2P reputation systems," *Computer Networks*, vol. 50, no. 4, pp. 472–484, 2006.

[26] L. Mekouar, Y. Iraqi, and R. Boutaba, "Peer-to-peer's most wanted: malicious peers," *Computer Networks*, vol. 50, no. 4, pp. 545–562, 2006.

[27] E. J. Anderson and T. D. H. Cau, "Implicit collusion and individual market power in electricity markets," *European Journal of Operational Research*, vol. 211, no. 2, pp. 403–414, 2011.

[28] Y. Chen, W. S. Lin, and K. J. R. Liu, "Risk-distortion analysis for video collusion attacks: a mouse-and-cat game," *IEEE Transactions on Image Processing*, vol. 19, no. 7, pp. 1798–1807, 2010.

[29] J. H. Park and D. H. Lee, "Fully collusion-resistant traitor tracing scheme with shorter ciphertexts," *Designs, Codes and Cryptography*, vol. 60, no. 3, pp. 255–276, 2011.

[30] Y. Zhu, L. Huang, W. Yang, and X. Yuan, "Efficient collusion-resisting secure sum protocol," *Chinese Journal of Electronics*, vol. 20, no. 3, pp. 407–413, 2011.