Journal of Computer and System Sciences 78 (2012) 1737–1750

Contents lists available at SciVerse ScienceDirect

Journal of Computer and System Sciences

www.elsevier.com/locate/jcss

Behavior-based reputation management in P2P file-sharing networks ☆

Xinxin Fan [a,*], Mingchu Li [a], Jianhua Ma [b], Yizhi Ren [c], Hui Zhao [d], Zhiyuan Su [a]

[a] School of Software, Dalian University of Technology, Dalian 116620, Liaoning, PR China
[b] Faculty of Computer & Information Sciences, Hosei University, 3-7-2, Kajino-cho, Koganei-shi Tokyo 184-8584, Japan
[c] School of Software Engineering, Hangzhou Dianzi University, Hangzhou 310018, Zhejiang, PR China
[d] School of Computer Science & Technology, Shandong University of Technology, Zibo 255000, Shandong, PR China

ARTICLE INFO

Article history:
Received 18 December 2010
Received in revised form 13 May 2011
Accepted 28 October 2011
Available online 1 December 2011

Keywords:
Peer-to-peer file-sharing network
Reputation
Collusion
Trust community

ABSTRACT

Trust research has become a key issue in the last few years as a novel and valid solution to ensure the security and application in peer-to-peer (P2P) file-sharing networks. The accurate measure of trust and reputation is a hard problem, most of the existing trust mechanisms adopt the historical behavior feedback to compute trust and reputation. Thus exploring the appropriate transaction behavior becomes a fundamental challenge. In P2P system, each peer plays two roles: server and client with responsibility for providing resource service and trust recommending respectively. Considering the resource service behavior and trust recommending behavior of each peer, in this paper, we propose a new trust model adopting the technology to calculate eigenvectors of trust rating and recommending matrices. In our model, we define recommended reputation value to evaluate the resource service behavior, and recommending reputation value to evaluate the trust recommendation behavior. Our algorithm would make these two reputation values established an interrelated relation of reinforcing mutually. The normal peers provide authentic file uploading services, as well as give correct trust recommendation, so they can form a trusted and cooperative transaction community via the mutual reinforcement of recommended and recommending reputation values. In this way, the transaction behaviors of those malicious peers are isolated and confined effectively. Extensive experimental results also confirm the efficiency of our trust model against the threats of exaggeration, collusion, disguise, sybil and single-behavior.

1. Introduction

1.1. Background

Peer-to-Peer (P2P) file-sharing network has become a key research issue as a means of sharing and distributing information, in which trust and reputation management plays a crucial role by making the participants establish an interrelated relation of authentic cooperation and mutual benefit. Trust and reputation are two related concepts, but, in fact, they are different. Trust is a personal and subjective phenomenon that is based on various factors or evidence, and that some of those carry more weight than others, an individual's subjective trust can be derived from a combination of received referrals and

☆ Research supported by National Nature Science Foundation of China No.: 90715037, National 973 Plan No.: 2007CB714205, University Doctor Subject Fund of Education Ministry of China No.: 200801410028, Graduate Creative Talents Project of DUT.

* Corresponding author. Fax: +86 411 87571567 / 87571538.
E-mail addresses: xinxinyuanfan@gmail.com (X. Fan), li_mingchu@yahoo.com (M. Li), jianhua@hosei.ac.jp (J. Ma), renyizhi@gmail.com (Y. Ren), eric.hui.zhao@gmail.com (H. Zhao), suzhiyuan2006@gmail.com (Z. Su).

0022-0000/$ – see front matter
doi:10.1016/j.jcss.2011.10.021

personal experience. Reputation can be considered as a collective measure of trustworthiness based on the referrals or ratings from members in a community [1]. The concept of reputation is closely linked to that of trustworthiness, but it is evident that there is a clear and important difference. The most distinguished difference lies in that trust systems produce a score that reflects the trusting entity's subjective view of trusted entity's trustworthiness, whereas reputation is referred to as a single value that represents what the community as a whole thinks about a certain user [2]. In our work, the reputation of a peer aggregates the trust ratings of other transaction peers, which reflects its capability of providing resource services, and the trust of a peer represents the direct trust ratings to the downloading source, which reflects its personal opinion or confidence it has in another. By collecting, distributing and aggregating the feedback about the participants' past behaviors, the reputation-based trust models can help participants to decide whom to trust, encourage trustworthy behavior, and deter participation by those who are unskilled or dishonest [3].

Recently, many researches on reputation mechanism based on various methods, like fuzzy logic theory [4–6], Bayesian network [7,8], subjective logic [9,10], social cognitive [11–14], fined-grained [15,16], and game theory [17–20], have been proposed in this field on which both academia and industry are concentrating their attention.

1.2. Motivation

Studying and analyzing these models mentioned above, we find that each peer's reputation almost depends on other's trust ratings, but ignores the self recommending behavior. In fact, each peer not only uploads files for other requesters to obtain the corresponding trust ratings, but also downloads files from other resource providers and gives personal trust ratings at the same time. Therefore each of them has two transaction roles: recommended object and recommending individual. Considering these two different behaviors, we would like to establish a related relationship between them, and make the system have an accurate measure on reputation and trust. Inspired by the link analysis algorithm [21], we define two reputation values that are called recommended reputation value (RDRV) and recommending reputation value (RGRV) for each peer to reflect the resource service behavior and trust recommending behavior respectively, and make them rely on each other tightly. One's recommended reputation is expressed by aggregating the recommending reputation of other peers which have downloaded files from it; and its recommending reputation is expressed by aggregating the recommended reputation of other peers from which it has downloaded files. RDRV is used to evaluate the behavior of providing resource service for other peers; and RGRV used to evaluate the self recommending behavior. The interaction between RDRV and RGRV can make the entire network form different trust communities corresponding to different types of peers. In this way we are able to identify the normal and malicious peers effectively.

1.3. Previous works

Reputation management can be analyzed from different perspectives. In the eBay system [3], there are a short comment on transaction and three discrete trust rating values: positive (1), negative (-1) and neutral (0). And each peer's reputation is calculated by aggregating the limited trust ratings without considering the short comment. The system is simple and carried out easily, but it does not implement any measure to punish those malicious peers. Kerschbaum et al. propose PathTrust model [22] by exploiting the maximum-weight path to get personalized reputation ratings. The model only focuses on the reputation between initiator and candidates, but ignores other related trust ratings given by other peers to the candidates. These two models only capture local and limited trust rating information to assess the transaction behavior, so the calculated reputation may be one-sided. However, trying to capture the rating information completely, we not only focus on other related trust ratings, but also consider self recommendation.

Kamvar et al. [23] propose the trust model EigenRep based on trust transitivity. At first, the system defines some pre-trusted peers with high reputation, but how to select and distribute these pre-trusted peers is a hard problem in large-scale and decentralized P2P networks. Each peer's reputation relies on the others' trust ratings, if there are few malicious peers, the EigenRep model can properly assess transaction behavior, but if there are a large number of malicious peers, the results would be poor, because each malicious peer will receive plenty of exaggerated ratings from other malicious ones, and in return gives high personal trust ratings to them, which makes a collusion threat. The drawback lies in the trust transitivity between one peer and the other peers without isolating exaggerated ratings effectively. Therefore, how to confine the trust transitivity among malicious ones is the key. Considering the feedback, the total number of transactions, the credibility of the feedback, transaction context and community context factors, Xiong et al. [24] propose PeerTrust model based on P-Grid structure. This model can assess the transaction behavior properly, but it may be attached to the PGrid structure tightly. Malicious peers may obtain relatively high reputation via exaggeration and collusion temporarily. Nevertheless, according to interrelated relation and interaction of our algorithm, a peer, which cannot provide good resource service for other peers, will not be able to give high personal trust rating. Therefore the reputation of malicious peers would become decreasing in the long run.

The primary aim of trust and reputation management research is to form a trusted network and induce participants to cooperate with each other. Driving an arbitrary overlay network into a cooperative, Wang and Nakao [20] propose an evolutionary game theory (EGT)-based overlay topology evolution scheme to characterize the social dilemma for forming links in an overlay network from the viewpoint of peers' local interactions. The goal of literature [25] is to study equilibrium and disequilibrium behavior of artificial agents in such systems, and explore the efficient design of mechanisms to promote

cooperation and coordination of self-interested artificial agents. Allen [26] introduces a new generic model to build up and maintain a dynamic social network of others that they can trust based on similarity of cooperation. This mechanism effectively incentivizes unselfish behavior, where peers with higher levels of cooperation gain higher payoff. These mechanisms all try to make the entire network become cooperative and trusted. In our work, adopting the interaction and reinforcement of RDRV and RGRV, we can make those authentic peers form a trust communities, in which the peers possess high reputation and cooperate with each other.

1.4. Challenging issues and our contribution

The anonymous, autonomous and open natures cannot ensure the P2P file-sharing networks security and application very well. Marmol et al. [27] have shown us nine important security threat scenarios in reputation system, and it is difficult to explore a comprehensive trust mechanism to arrest various threats. Analyzing the existing trust models, we can conclude several challenges as follows: (1) What transaction behaviors are suitable for the measure of trust and reputation? (2) How to identify normal peers and isolate malicious peers effectively, especially the strategic ones? (3) How to resist various threats of manipulation by different types of malicious peers?

To address the challenges, we propose a new trust model Dual-EigenRep adopting the technology to calculate the eigenvectors of trust rating and recommending matrices. Our main contribution includes: (1) Taking the resource service behavior and trust recommending behavior into account, we design two reputation values for each peer. The RDRV reflects the capacity of providing resource service for other peers; and the RGRV reflects the capacity of recommending downloading source peers. (2) We propose the definitions of RDRV and RGRV. Each peer's RDRV aggregates the personal trust ratings and RGRV of other peers which have downloaded files from this peer; and its RGRV aggregates the self trust ratings and RDRV of other peers from which it has downloaded files. The inner interrelated relation and interaction of these two reputation values can drive the entire network into different trust communities, which identify different types of peers. With the increase of transaction amount, the reputation of those normal peers would become higher, and the probability that they are selected as downloading sources also become larger. Thus the transactions with malicious peers are restricted markedly.

1.5. Comparing our new results to related works

In order to verify the availability and rationality of our trust mechanism, we compare the successful downloading percentage with EigenTrust, PathTrust and Random models, and ranking error ratio with HopRec [28] and EigenRep models. We design several types of commonly used threats, as well as another two special types for our model. The experimental results show that our trust model can achieve a better performance against these threats.

The remaining of this paper is organized as follows: in Section 2, we detail the Dual-EigenRep model. In Section 3, we present the simulation parameters, classify peers as different types and analyze the corresponding simulation results. Finally, some conclusions are introduced in Section 4.

2. Dual-EigenRep

In this section, we describe our trust model in detail. Firstly, some simple preliminaries are introduced; secondly, recommended and recommending reputation values are defined respectively, then based on them, we propose the unique global reputation; thirdly, the convergence of our algorithm is proved in theory to verify the stability of entire network; finally, we make an analysis of our trust model.

2.1. Preliminaries

In P2P file-sharing networks, the transaction relation happened among peers can be presented by a directed weighted graph $G(V, E)$, $V = |v|$ denotes the number of system peers, $E = \{i | j \in Trans(i), l_{ij}\}$ represents the personal trust rating, $Trans(i)$ is the set of peers from which peer i has downloaded resource, and l_{ij} is the personal trust rating from peers i to j. After a certain number of transactions, the entire network would form a web of trust, the weight between a pair of arbitrary peers is the personal trust rating as described in Fig. 1.

2.2. Reputation computation

Each time peer i downloads a file from peer j, it may rate their transaction as successful when the downloaded file is satisfactory, or unsuccessful when the downloaded file is unsatisfactory. Based on these feedback information, we define the personal trust rating l_{ij} as successful percentage of individual transactions that peer i has downloaded files from peer j

$$l_{ij} = \begin{cases} \frac{\max(p_{ij},0)}{\sum_m \max(p_{im},0)} & \text{if } \sum_m \max(p_{im},0) \neq 0, \\ 0 & \text{otherwise,} \end{cases} \tag{1}$$

$$p_{ij} = succ(i, j) - unsucc(i, j). \tag{2}$$

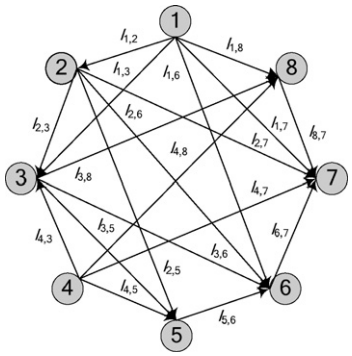


Fig. 1. Web of trust with 8 peers.

Here $succ(i, j)$ is the number of successful transactions peer i deems, $unsucc(i, j)$ is the number of unsuccessful transactions peer i deems, and $\max(p_{ij}, 0)$ represents the larger.

Considering the resource service and trust recommending behaviors, we design RDRV and RGRV for each peer as follows:

Definition 1. Recommended reputation value $t_d(i)$ of peer i is the aggregation of trust ratings and reputation of those peers that have downloaded files from it, like $t_d(3)$ in Fig. 2.

Definition 2. Recommending reputation value $t_g(i)$ of peer i is the aggregation of self trust recommendations and reputation of the peers from which it has downloaded files, like $t_g(3)$ in Fig. 2.

Therefore, the RDRV and RGRV are defined as

$$t_d(i) = \sum_{j \in I(i)} l_{ji} \cdot t_g(j), \tag{3}$$

$$t_g(i) = \sum_{j \in O(i)} l_{ij} \cdot t_d(j). \tag{4}$$

We can get $t_d(i)$, $t_g(i) \in (0, 1)$ via normalization process in Algorithm 1, let $I(i)$ represent the set of peers which have downloaded files from peer i, and $O(i)$ represent the set of peers from which peer i has downloaded files. The more the peers belonged to $I(i)$, the larger the RDRV, which illuminates peer i can provide more file uploading services, meanwhile, a good peer can give correct recommendation to others. RDRV and RGRV are strongly interrelated and interactive.

However, we should pay more attention to the RDRV while confirming the unique global reputation, because RDRV reflects others' personal trust ratings, which may be more objective and trusted to some extent. Therefore a coefficient α is designed to adjust the proportion weight, and the global reputation value is defined as

$$t(i) = \alpha \cdot t_d(i) + (1 - \alpha) \cdot t_g(i). \tag{5}$$

To get the exact value of α, several simulations are performed in Section 3.3. Experimental results show that the number of successful transactions is largest when α is 0.75 compared with 0.5, 0.65 and 0.85. The results become better with the increase of α, but decrease immediately when α is 0.85, so the most suitable value should be neither too large nor too small.

In distributed P2P networks, the implementation of query and storage on rating information is very crucial and hard. Some of trust mechanisms, such as EigenRep, PeerTrust and PowerTrust [29], are based on a DHT (distributed hash table) to store, search and calculate trust value. However, most of P2P systems deployed on Internet are unstructured [2]. Therefore, in this paper a simple list is designed for each peer to store the rating information to other peers based on the transaction behavior whether the peer got the authentic sources or not.

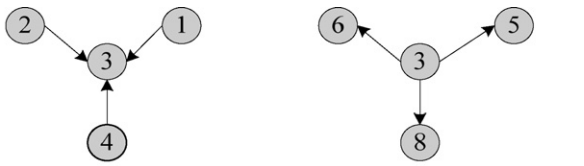
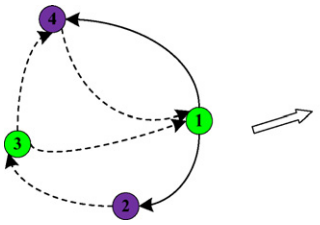


Fig. 2. The expressions of $t_d(3)$ and $t_g(3)$.



j	$succ(i,j)$	$unsucc(i,j)$	$t(j)$
2	10	15	0.223
4	30	22	0.562

Fig. 3. Data list of peer 1.

Algorithm 1 Global reputation value.

Input: personal trust rating $l(i,j)$, initial column vectors v_d and v_g, parameters τ, k and α
Output: global reputation value $t(n)$;
Initiation of RDRV and RGRV line 3–5
for for i from 1 to n **do**
  $t_d(i) \leftarrow v_d$
  $t_g(i) \leftarrow v_g$
end for
Power iteration line 7–25
while $(\delta \succ \tau)$ **do**
  for i from 1 to n **do**
    for j from 1 to n **do**
      $t_d(i) \leftarrow sum\_t_d + l(j,i) \cdot t_g(j)$
      $t_g(i) \leftarrow sum\_t_g + l(i,j) \cdot t_d(j)$
    end for
  end for
  Normalization process line 14–21
  for i from 1 to n **do**
    $sumz\_t_d \leftarrow sumz\_t_d + t_d(i) \cdot t_d(i)$
    $sumz\_t_g \leftarrow sumz\_t_g + t_g(i) \cdot t_g(i)$
  end for
  for i from 1 to n **do**
    $t_d(i) = t_d(i)/sqrt(sumz\_t_d)$
    $t_g(i) = t_g(i)/sqrt(sumz\_t_g)$
  end for
  Condition parameter line 22–24
  for i from 1 to n **do**
    $\delta = |t_d^{(k+1)}(i) - t_d^{(k)}(i)| + |t_g^{(k+1)}(i) - t_g^{(k)}(i)|$;
  end for
end while
Global reputation value line 26–28
for i from 1 to n **do**
  $t(i) = \alpha \cdot t_d(i) + (1-\alpha) \cdot t_g(i)$
end for
Return $t(i)$

As shown in Fig. 3, peer 1 has two transaction partners 2 and 4, and the number of successful transactions with peer 2 is 10, while the unsuccessful number is 15. The last item $t(j)$ represents the partner's global reputation value. This list is updated timely if there exists any change about $succ(i,j)$, $unsucc(i,j)$ and $t(j)$ with the continual transactions. Each peer stores the local information, and simultaneously inquires the partners' rating information from other peers, then, by aggregating all the rating information derived from different peers, the partners' global reputation values can be calculated.

The personal trust rating reflects the historical transaction behavior between a pair of arbitrary peers, which represents a peer has the direct opinion in others; and the global reputation value reflects the aggregated personal trust ratings, which represents the common view of trustworthiness. Algorithm 1 lists the implementation process to calculate the global reputation. Analyzing Algorithm 1, we can get that the time complexity mainly depends on the computation process of t_d and t_g. Each time while calculating the reputation value, each peer always aggregates the others' personal trust ratings on the transaction partners, this process needs $O(n)$ steps, thus, the computation complexity of the total system peers would take $O(n^2)$ steps. Moreover, each peer needs to maintain a local $(n \times n)$-dimensional storage list ($succ(i,j)$ and $unsucc(i,j)$).

2.3. Proof of convergence

Usually, the directed weighted graph can be expressed by using adjacency matrix equal to the personal trust rating matrix l here. In this paper, all the peers' reputation values are viewed as a column vector, and t_d is used to express RDRV

as a column vector, t_g used to express RGRV as a column vector. Thus we can calculate them via power iteration:

$$t_d^{(k+1)} = l^T \cdot t_g^{(k)}, \tag{6}$$

$$t_g^{(k+1)} = l \cdot t_d^{(k)}. \tag{7}$$

Here l^T is the transpose of matrix l, and k is the iteration number. Based on the above formulas, we can transform them into:

$$t_d = l^T \cdot t_g = l^T \cdot l \cdot t_d, \tag{8}$$

$$t_g = l \cdot t_d = l \cdot l^T \cdot t_g. \tag{9}$$

Suppose that $l^T \cdot l = M$, $l \cdot l^T = N$, there will be $M^T = (l^T \cdot l)^T = l^T \cdot l = M$, $N^T = (l \cdot l^T)^T = l \cdot l^T = N$, so both M and N are symmetric Matrices.

Now we introduce three preliminary theorems for the convergence proof of our algorithm:

Theorem 1. *The eigenvalues of symmetric matrices are real.*

Theorem 2. *The eigenvectors of a symmetric matrix M corresponding to different eigenvalues are orthogonal to each other.*

Theorem 3. *If k is a positive integer, λ is an eigenvalue of the matrix M, x is the corresponding eigenvector, then λ^k is an eigenvalue of M^k and x is the corresponding eigenvector.*

Next we prove the convergence in detail.

Theorem 4. *t_d converges to the principal eigenvector of matrix M, and t_g converges to the principal eigenvector of matrix N.*

Proof. The matrix M can be considered as to be composed of a certain number of connected components with no connections between each other according to [30]:

$$M = \begin{bmatrix} M_1 & 0 & \cdots & 0 \\ 0 & M_2 & \cdots & 0 \\ \vdots & & \ddots & \\ 0 & 0 & \cdots & M_m \end{bmatrix}.$$

Each of these matrices $M_1, M_2, \ldots, M_m$ is a real, irreducible and nonnegative symmetric matrix, with real nonnegative eigenvalues, since the eigenvalues of $l^T l$ are real and nonnegative (Theorem 1). The eigenvalues of M are given by the sum of eigenvalues of different matrix M_i, $i = 1, 2, \ldots, m$, and each of them which is different from 0 has a strictly dominant eigenvalue, i.e. an eigenvalue which is strictly greater than all the other eigenvalues of the matrix; moreover, all the entries of its associated eigenvector are greater than 0. We can see that the eigenvectors of matrix M can be obtained from the eigenvectors of the matrices $M_1, M_2, \ldots, M_m$ by just considering 0 the entries corresponding to the other matrices. Suppose that the $\lambda_1 \geqslant \lambda_2 \cdots \lambda_n \geqslant 0$ corresponding to the eigenvectors $x_1, x_2, \ldots, x_n$, each of them is related to the particular diagonal block of above matrix. If more than one matrix M_i has a strictly dominant eigenvalue equal to λ_1. Without loss of generality, we suppose that M has the eigenvalues $\lambda_1 = \lambda_2 = \cdots = \lambda_r > \lambda_{r+1} \geqslant \lambda_{r+2} \geqslant \cdots \geqslant \lambda_n$ with r maximum eigenvalues. The eigenvectors $x_1, x_2, \ldots, x_r$ are related to the r different matrices $M_{h_1}, M_{h_2}, \ldots, M_{h_r}$, so that x_j, $1 \leqslant j \leqslant r$, has positive entries corresponding to the diagonal block M_{h_j}.

Based on the consideration $\aleph = \{x_1, x_2, \ldots, x_n\}$ as an orthonormal basis for $\mathbb{R}^n$ in [30] (Theorem 2), we define an initial vector v to be equal to $t_d^{(0)}$:

$$v = t_d^{(0)} = \alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_r x_r + \cdots + \alpha_n x_n.$$

According to [30], we can get the $\alpha_j > 0$, $j = 1, 2, \ldots, r$, since at least one entry of l^T in each row j corresponding to a row of M_{h_j} in above component matrix must be greater than 0, because M_{h_j} represents a connected graph, thus, in every row it must have at least one entry that is greater than 0. Then we can get the following results:

$$\begin{aligned} t_d^{(1)} &= M \cdot t_d^{(0)} = M \cdot v \\ &= \alpha_1 M x_1 + \alpha_2 M x_2 + \cdots + \alpha_r M x_r + \cdots + \alpha_n M x_n \\ &= \alpha_1 \lambda_1 x_1 + \alpha_2 \lambda_2 x_2 + \cdots + \alpha_r \lambda_r x_r + \cdots + \alpha_n \lambda_n x_n, \end{aligned}$$

$$
\begin{aligned}
t_d^{(2)} &= M \cdot t_d^{(1)} = M^2 \cdot v \\
&= \alpha_1 M^2 x_1 + \alpha_2 M^2 x_2 + \cdots + \alpha_r M^2 x_r + \cdots + \alpha_n M^2 x_n \\
&= \alpha_1 \lambda_1^2 x_1 + \alpha_2 \lambda_2^2 x_2 + \cdots + \alpha_r \lambda_r^2 x_r + \cdots + \alpha_n \lambda_n^2 x_n, \\
&\vdots \\
t_d^{(k)} &= M \cdot t_d^{(k-1)} = M^k \cdot v \\
&= \alpha_1 M^k x_1 + \alpha_2 M^k x_2 + \cdots + \alpha_r M^k x_r + \cdots + \alpha_n M^k x_n \\
&= \alpha_1 \lambda_1^k x_1 + \alpha_2 \lambda_2^k x_2 + \cdots + \alpha_r \lambda_r^k x_r + \cdots + \alpha_n \lambda_n^k x_n.
\end{aligned}
$$

Since $\lambda_1 = \lambda_2 = \cdots = \lambda_r$, then we have

$$
\begin{aligned}
t_d^{(k)} &= \lambda_1^k \left(\alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_r x_r + \cdots + \alpha_n \left(\frac{\lambda_n}{\lambda_1} \right)^k x_n \right) \\
&= \lambda_1^k \left(\alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_r x_r + \sum_{i=r+1}^{n} \alpha_i \left(\frac{\lambda_i}{\lambda_1} \right)^k x_i \right),
\end{aligned}
$$

where $\lim_{k\to\infty} (\frac{\lambda_i}{\lambda_1})^k = 0$, $i = r+1, \ldots, n$, then $t_d^{(k)} = \lambda_1^k (\alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_r x_r)$. Thus t_d converges to the principal eigenvector of matrix M corresponding to the principal eigenvalue λ_1, similarly, t_g converges to principal eigenvector of matrix N. □

2.4. Dual-EigenRep analysis

In our algorithm, each peer possesses rated and recommending features. The rated feature represents the capacity of providing resource for others, which reflects that it is an important downloading source; and the recommending feature represents the capacity of giving correct recommendation to service sources, which reflects that it is a junction center to link good peers together.

After a certain number of mutual transactions, a good peer will provide a large number of authentic resources for other peers and get plenty of positive ratings, thus it must be directed by many other ones like $t_d(5)$ in Fig. 4; meanwhile, a good peer also gives correct self-recommendation to other downloading sources while finishing transactions, thus it will direct many other peers like $t_g(2)$ in Fig. 4. These good peers would be linked together and reinforce each other mutually, which forms an interrelated relationship via our algorithm.

We can explain this phenomenon via trust matrix $M = l^T l$, let $(M)_{ij} = m_{ij}$, then we get: $m_{ij} = \sum_{k=1}^{n} l_{ki} l_{kj}$, since the $(l^T)_{ik} = l_{ki}$, from this formula we see that the generic entry m_{ij} is a nonzero entry if and only if there is at least one peer k with rating information towards peers i and j at the same time. This means that the peer k will play the role as a link junction and drive peers i and j into an interrelated relationship.

Generally speaking, a peer gets positive trust ratings by uploading authentic file resource. However, for a malicious peer, it can still get positive and exaggerated trust ratings from other malicious ones as shown in Fig. 5, in which white and black nodes represent normal and malicious peers respectively. The RDRV of malicious peers may become relatively high by exaggerating personal trust ratings, but their RGRV would be small because of unauthentic or non-recommendation to normal peers, which would decrease the global reputation. For a normal peer, it provides authentic file uploading service, as well as gives authentic personal trust ratings, thus both RDRV and RGRV would be high as shown in Fig. 6.

With the increase of transactions, the normal peers with authentic services will get many positive ratings; and the malicious peers with unauthentic services will get many negative ratings. We would like to illuminate our model via Fig. 7, in which nodes 1, 2, 3, 4, 5, 6 are supposed to serve as normal peers, and the others to serve as different types of malicious peers. Nodes 7, 8, 9, 10, 11 are collective malicious peers; Nodes 12, 13, 14, 15, 16 are disguised malicious peers, and some of them get positive ratings from normal peers by providing authentic files in some cases when selected as downloading sources; Node 17 only recommends peers, and does not provide file uploading service; on the contrary, node 18 only provides file uploading service, and does not give personal trust ratings; and node 19 is a sybil peer with two new

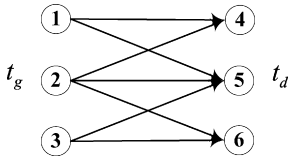


Fig. 4. The interrelated relation between t_d and t_g.

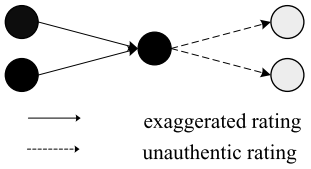


Fig. 5. Behavior of malicious peer.

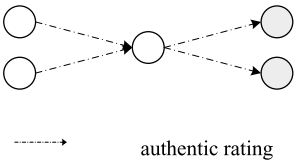


Fig. 6. Behavior of normal peer.

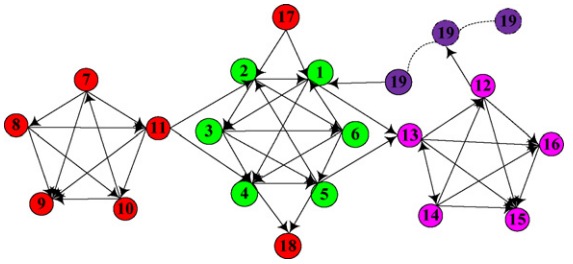


Fig. 7. Interrelated relation among different types of peers.

identities to prevent from gaining negative trust ratings. The details on these different types of peers will be introduced in Section 3.1.

After a certain number of transactions, the entire network will form different trust communities corresponding to different types of peers as shown in Fig. 7. The community composed of the normal peers is trusted, and the members in it are cooperative with each other.

However, there may be some problems worth to be discussed. For instance, if more than 50% collective malicious peers exist and make a collusion threat, can our trust model resist it? According to characteristic of our algorithm, these malicious peers would form a strongly linked transaction relation and get relatively high reputation via exaggerated trust ratings. But we should also focus on the personal trust ratings given by normal peers, which would provide negative ratings and reduce their reputation gradually. Therefore, the malicious peers may have high reputation temporarily, but they cannot keep this situation for a long time. And simulation results in Section 3.5 also confirm the efficiency of our algorithm against collusion threat made by plenty of malicious peers.

3. Experimental results and analysis

3.1. Types of peers

Considering the behavior of peers, we mainly classify them into two types: normal and malicious. The normal peers provide authentic file uploading services, as well as give authentic trust recommendation (personal trust ratings); the malicious peers not only provide unauthentic file uploading services, but also give unauthentic recommendation, even calumniate or pretend to be normal peers. Considering the variability of malicious peers, we define several types of threats as follows:

(1) Individual malicious peers (IMP): this type of malicious peers provides unauthentic file uploading services, as well as gives unauthentic personal trust ratings to others.
(2) Collective malicious peers (CMP): on the one hand these malicious peers provide unauthentic file uploading services, cheat and calumniate normal peers; on the other hand, they give exaggerated personal trust ratings to other malicious ones mutually, which makes a serious collusion threat.
(3) Disguised malicious peers (DMP): these disguised malicious peers provide authentic and popular files to get high reputation in some cases when selected as downloading sources, then, they give high personal trust ratings to other malicious ones. This type of malicious peers has the IMP and CMP characteristics.
(4) Sybil attack: each time one of these malicious peers is selected as a service provider, it provide a bad service. Then, it is replaced with a new identity. This kind of attack might prove quite problematic because it prevents authentic peers from being able to obtain high reputation, since they might not be selected most of the times.
(5) Single recommended-peers (SRDP): these malicious peers only provide unauthentic files uploading services, but do not give any personal trust ratings to others.
(6) Single recommending-peers (SRGP): contrary to SRDP, these malicious peers only negatively recommend other peers, but do not provide file uploading services.

The IMP, CMP, DMP and sybil attack are commonly used threats, and SRDP and SRGP are designed specially for our model to verify the reasonability and correctness that RDRV contributes a little more to the global reputation.

Table 1
Parameter configuration.

Parameter	Value	Parameter	Value
Peers of system	600	Round each cycle	30
Files of system	6000	Simulation operation	10
Types of files	100	Request peers each round	120
Simulation cycles	20	Reputation values initialization	1/600

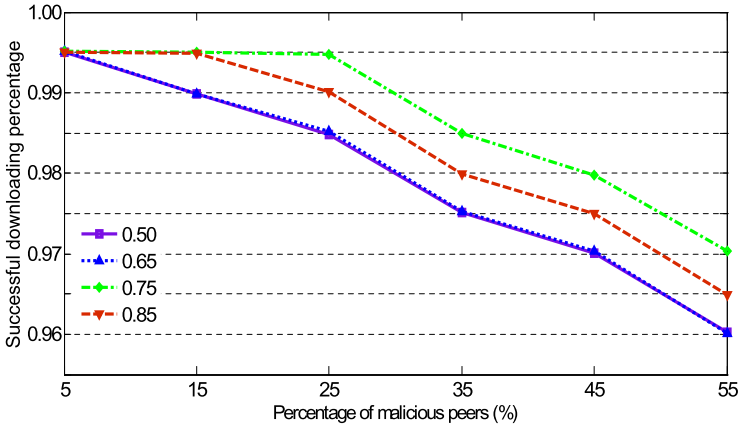


Fig. 8. The SDP with different values of α.

3.2. Experiment configuration and evaluation criterion

Since the similarity between social network and P2P network, we design a power-law P2P network to simulate the different types of threats. During the simulation, some peers are able to issue service requests for downloading files, which are propagated by broadcast through entire network in the usual Gnutella way; meanwhile, other peers are able to respond to these requests. The peers which receive the service requests will check if they have the requested files. There may be two or more peers that have the requested files, then, the requester will select the peer which has the largest global reputation value as downloading source. Table 1 lists the parameter configuration in our simulation.

Seen from the table, our system has 600 peers with 6000 files which are classified into 100 file types, and each peer has 10 files. In each simulation, 20 cycles are included. For each cycle, 120 peers issue 120 file downloading requests randomly, which are performed 30 rounds. In addition, we initialize RDRV and RGRV of each peer as 1/600. In order to get the accurate values, we always perform 10 simulation operations and calculate their average value as the final result.

To evaluate the performance of trust model rationally, we propose successful downloading percentage (SDP) as the measure criterion. Generally speaking, the more the number of successful transactions, the better the performance. So we define the SDP as

$$\varphi = \frac{\sum_i \sum_j succ(i, j)}{\sum_i \sum_j (succ(i, j) + unsucc(i, j))} \tag{10}$$

$succ(i, j)$ and $unsucc(i, j)$ are defined in Section 2.2. It presents the satisfactory transaction percentage in the entire network.

3.3. Proportion coefficient α and iteration number

We deem that RDRV contributes a little more to the global reputation value because of the objective trust ratings given by others, and several simulations are performed while existing different percentages of malicious peers when α are 0.5, 0.65, 0.75 and 0.85. The simulation results show that SDP is best when α is 0.75 as described in Fig. 8. The SDP become better with the increase of α, but it decreases when α is 0.85, so we may select 0.75 as the suitable value.

In EigenRep model, the final reputation value will converge to the principal eigenvector of local trust matrix, similarly, the HopRec model also converges to the principal eigenvector of $[\alpha \cdot RW_{hop} + (1-\alpha) \cdot e \cdot p^T]^T$. According to the convergence proof in Section 2.3, the RDRV and RGRV converge to the principal eigenvectors of matrices M and N respectively. All these algorithms adopt power iteration to calculate the reputation values. As we know, the number of iteration controls the overheads of the algorithm, as well as reflects the convergence rate. Generally speaking, the more the number of iteration is, the higher the precision of calculated reputation values to some extent. As the configuration of increment in HopRec model, we also set conditional increment $\tau = 10^{-4}$ in this paper.

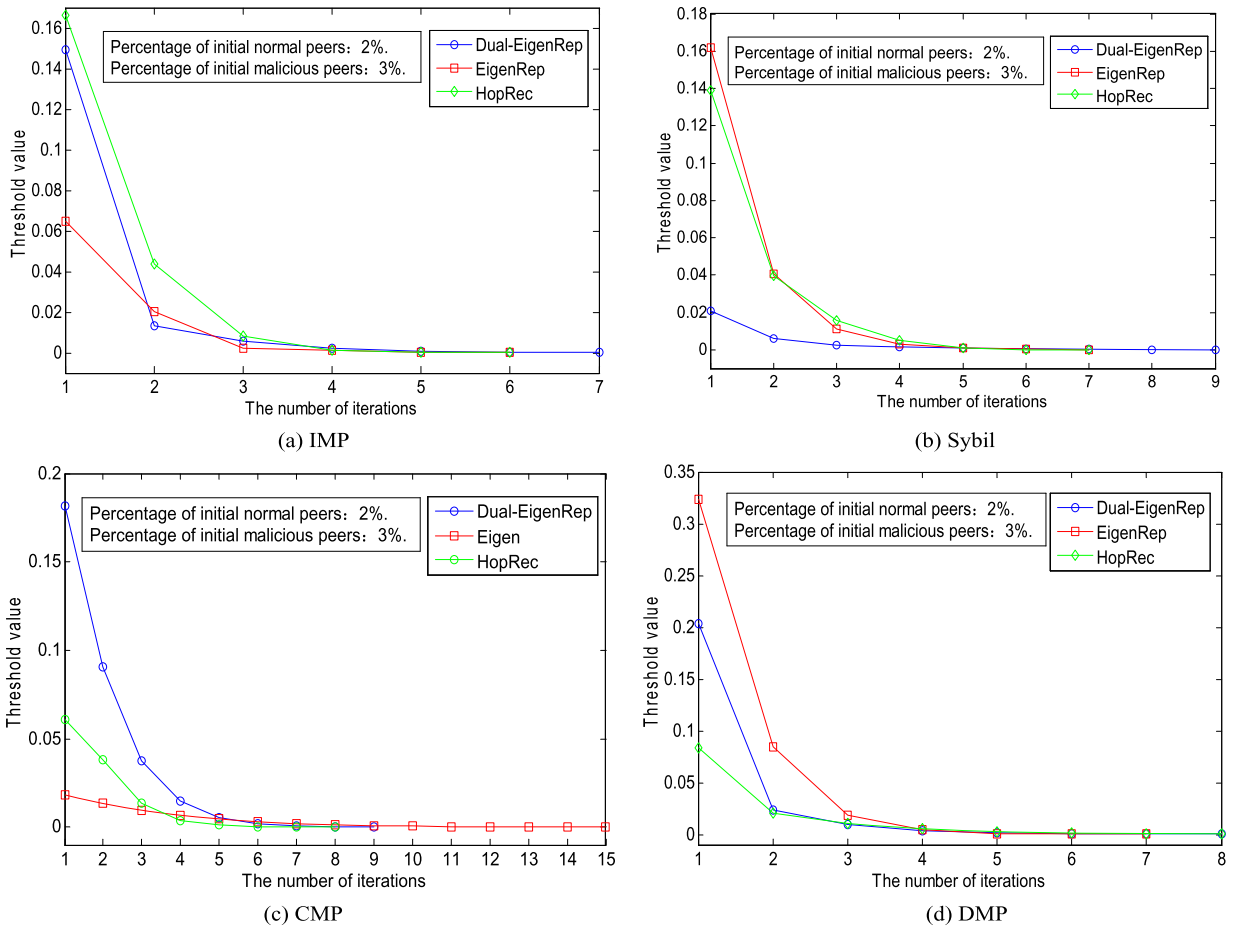


Fig. 9. The comparison of iteration number.

Several simulations on iteration number are performed for IMP, Sybil, CMP and DMP, and the results are presented in Fig. 9. Seen from the curves, the CMP's iteration cycle is relatively longer compared with others, which shows the seriousness of this type of malicious threat and hardness to crawl those pre-trusted peers. In general, these three trust mechanisms almost have a similar convergence rate more or less.

3.4. IMP simulation and analysis

These individual malicious peers cheat independently. They provide unauthentic file uploading services, as well as give unauthentic personal trust ratings. Based on these characteristics, we run simulations with Dual-EigenRep, EigenRep, PathTrust and Random models. In our simulation, the Random model presents that those request peers randomly select another response peer as downloading source without implementing any reputation management. We depict the experimental results in Fig. 10.

Seen from Fig. 10, the performance of Dual-EigenRep is better than other models. Owing to the dual-reputation, the SDP can maintain high level even when the malicious peers are 55%. However, the EigenRep performs well at first because of little blindness resulting from those pre-trusted peers defined previously, but the SDP declines obviously with the increase of malicious peers because of the trust transitivity among plenty of malicious peers. In PathTrust model, it only considers the personal trust values between initiator and candidates as the criterion of selecting downloading source without aggregating complete related trust ratings to the candidates, so its performance is poor. And the curve of Random model decreases almost linearly with the percentage increase of malicious peers, which may meets the property of random selection from the response peers.

3.5. CMP simulation and analysis

This type of malicious peers collaborates with each other and make a serious threat. They always exaggerate the personal trust ratings mutually. In our simulation, we set that a malicious peer will give personal trust ratings to the other

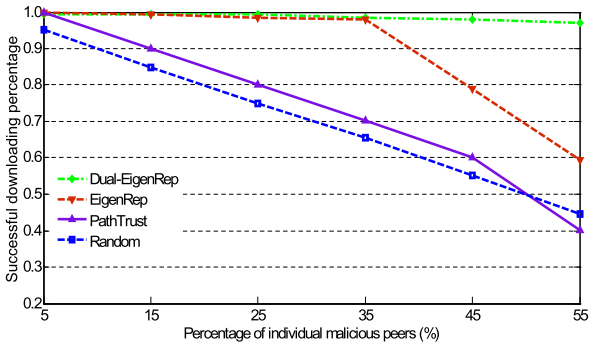


Fig. 10. The SDP with different percentages of IMP.

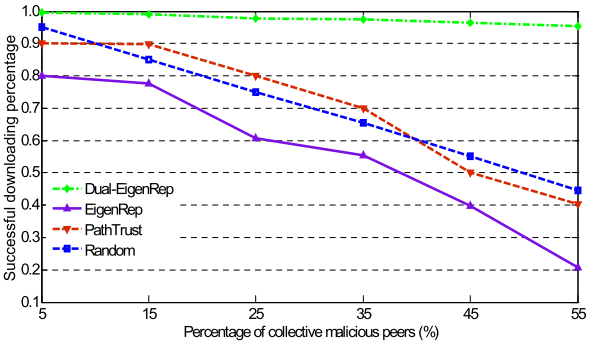


Fig. 11. The SDP with different percentages of CMP.

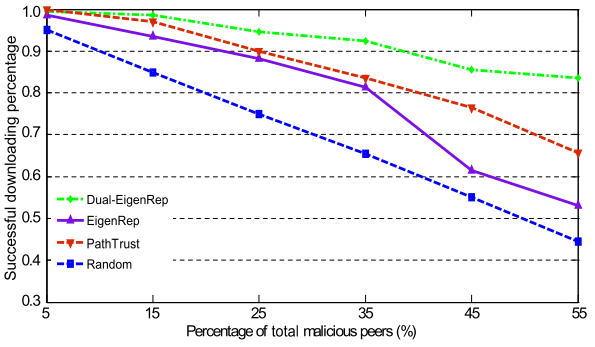


Fig. 12. The SDP with different percentages of TMP.

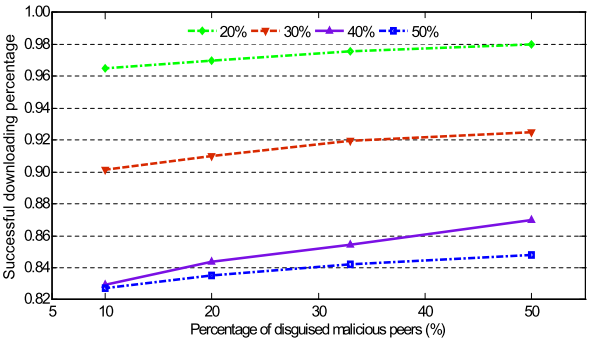


Fig. 13. The SDP with different percentages of DMP.

malicious peers once it has a transaction. Based on these characteristics, we run simulations and the results are described in Fig. 11.

Faced with the collusion threats, Dual-EigenRep performs well compared with other models. EigenRep performs poorly because it cannot identify and isolate those collective malicious peers effectively. With the increase of malicious peers, some of them will get high reputation, then, they in return give high personal trust ratings to other malicious ones under trust transitivity chain. In this way most of these malicious peers get relatively high reputation via mutual exaggeration ratings with each other. However, our model makes those normal peers form a trusted and cooperative community, and the reputation values of normal peers become larger and larger via normalization process, by which the transaction behavior of malicious peers are confined markedly. PathTrust only calculates the personal trust ratings between initiator and candidates, so it can arrest the collusion behavior to some extent, and it performs relatively better than EigenRep. And the Random model is changeless, because it does not refer to any feedback information and reputation dependence.

3.6. DMP simulation and analysis

This type includes individual and disguised malicious peers. The disguised malicious peers are cunning, they provide popular and authentic files for normal peers to get high reputation values in some cases when selected as downloading sources, then give high personal trust ratings to individual malicious peers. The disguised peers are defined as 50% of the total malicious peers (TMP) in our simulation, and the results are shown in Fig. 12.

At first, the performance of EigenRep is good because of the pre-trusted peers which can resist the temptation of those disguised peers. But the SDP declines with the increase of malicious peers. However, in our model, it evaluates the global reputation from two aspects: RDRV and RGRV. For the disguised peers, they can get high trust ratings by providing authentic services, but their RGRV would be low because of no or unauthentic recommendation to the normal ones. So Dual-EigenRep can confine the global reputation values of disguised peers effectively. PathTrust just selects the maximum-weight paths as the trust value between initiator and candidates, and avoid the trust transitivity between disguised peers and those candidates more or less, so the experiment results are a little better than EigenRep. And the Random model is changeless as well.

In addition, if there are more disguised peers while the amount of TMP is certain, the number of successful transactions will be larger because the disguised peers can provide more authentic files for requesters. Therefore we run four simulations with different percentages of disguised peers when the total malicious peers are 20%, 30%, 40% and 50%. And the simulation results also verify our thought as described in Fig. 13.

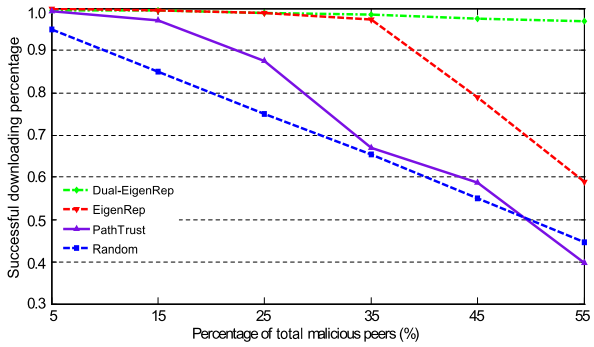


Fig. 14. The SDP with different percentages of sybil peers.

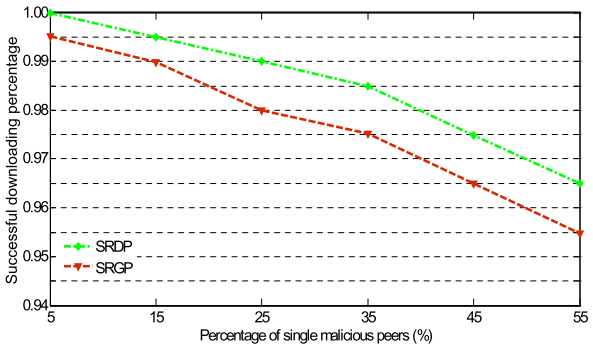


Fig. 15. The SDP with single-behavior malicious peers.

3.7. Sybil simulation and analysis

Providing bad services for other requesters, meanwhile, these malicious peers create many new identities to prevent from being given negative ratings. They not only provide unauthentic file services, but also give negative ratings to others. However, this type of malicious peers does not make a united attack. Based on these characteristics, we run simulations and the results are described in Fig. 14.

Seen from the simulation results, our model can still perform well with the increase of malicious peers. Firstly, the EigenRep model has a good behavior because the high reputation of pre-trusted peers which are selected as the downloading sources, nevertheless, the results become poor with the increase of malicious peers. These malicious peers can create some new identities to avoid negative ratings, but they cannot gain positive ratings from other requesters, besides, they do not give correct ratings to other normal peers, thus both RDRV and RGRV would be small. From the global view, EigenRep aggregates the other peers' personal trust ratings to calculate the unique reputation for each peer, the results may be all-sided to some extent. Different from the EigenRep, PathTrust just regards the personal trust ratings as the selection criterion whether to have a transaction. Because these malicious peers create many new identities, it is difficult to give them negative ratings and decrease the personal trust, so the simulation results are a little poorer than EigenRep.

3.8. SRDP and SRGP simulation and analysis

We specially design two types of extreme peers for our trust mode. The SRDP only provide unauthentic file uploading service for other peers, but do not give personal trust ratings; on the contrary, the SRGP only give unauthentic recommendation to other peers, but do not provide file uploading service. According to these characteristics, we run simulations and the results are shown in Fig. 15.

The results illuminate that they make a weak threat because of lacking collusion. However, the SRDP performs a little better than the SRGP with our trust model, which also explains the rationality and correctness that the RDRV contributes a little more to the global reputation.

3.9. Ranking error ratio

Considering the limited evaluation and comparison to the old trust mechanism EigenTrust, we compare another trust mechanism HopRec, and introduce ranking error ratio as a new evaluation criterion to reflect the performance.

As the definition in [31], the ranking error ratio is $|B|/|A|$, here set A denotes the high reputation-ranking list returned by trust schemes, and set B represents the list of malicious peers included in set A. Moreover, the size of list A equals the number of normal peers in the system. To illuminate the precision of our algorithm, several simulations are performed on ranking error ration based on the proposed types of malicious peers. During the process of simulations, we set the amount of malicious peers as 50% of the system peers while running Sybil, CMP and DMP. However, 25% are set as disguised peers (front peers in [2,28,31]) and the other 25% as ordinary malicious peers, the experimental results are described in Fig. 16.

Seen from the above results, the ranking error ratio of EigenRep obviously performs worse than Dual-EigenRep and HopRec. The reason lies in that EigenRep cannot prevent the malicious peers from propagating their trust values to other malicious ones. On the contrary, the Dual-EigenRep would make the normal peers form a trust community which consists of a large number of normal peers to arrest unauthentic trust ratings. The HopRec could detect the malicious peers, and assign low recommendation ability to those malicious peers. The sybil peers can create many new identification to escape the negative ratings, it is hard to evaluate the RDRV appropriately using Dual-EigenRep mechanism. However, the HopRec can restrict the malicious peers' reputation values by dampening the recommendation ability of recommending peers in the hop to the initial malicious seeds, thus HopRec performs a little better than Dual-EigenRep while facing the sybil malicious peers.

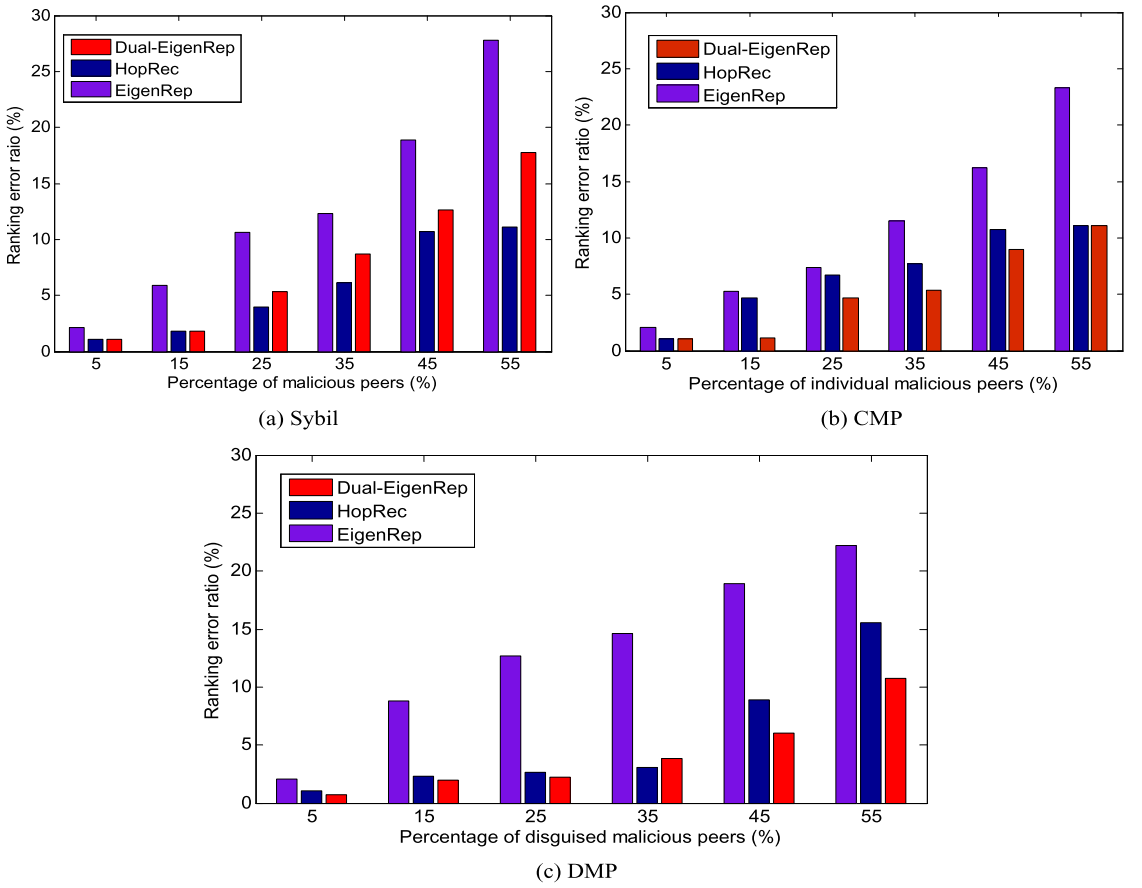


Fig. 16. The comparison of ranking error ratio.

In HopRec mechanism, the recommendation ability can exponentially dampen in the hop to initial malicious peers, and CMP and DMP collaborate with each other and make exaggeration-intensive ratings to other malicious peers, the hop number may be relatively large sometimes (maximal hop numbers is 6 in [28]), the recommendation ability would not be decreased effectively. Nevertheless, Dual-EigenRep makes the normal peers reinforce each other and form a trusted community, which isolates the collusion behavior among CMP and DMP in a valid way. Therefore Dual-EigenRep performs better slightly on the condition of CMP and DMP.

3.10. Discussion

The service and recommendation behaviors are the basis for computing reputation in our paper. We propose these two different behaviors on the condition of considering the two different roles played by each peer. The service behavior reflects the resource providing ability as a server, and recommendation behavior reflects the trust recommendation ability as a client. In literatures [2,28,31], the authors propose recommendation ability to infer more accurate reputation ranking based on logistic model, hop number and disproportional way, which is similar to the recommendation behavior proposed in our paper from the view point that peers with different trusted levels should have different recommendation ranking. But, in fact, another purpose of introducing recommendation behavior in our paper is to link the normal peers together as a junction presented by trust matrix in Section 2.4. Therefore there exists a difference on recommendation behavior between our work and literatures [2,28,31].

4. Conclusion

In this paper, we propose a new trust model Dual-EigenRep adopting the technology to calculate the principal eigenvectors of the behavior matrices. Considering the different transaction behaviors, we define RDRV to reflect the resource service behavior, and RGRV to reflect the trust recommending behavior. Our algorithm makes them rely on each other and establish an interrelated relation. After a certain number of transactions, the entire network forms different trust communities corresponding to different types of peers. Furthermore, we prove the convergence of our algorithm to guarantee the

stability of entire network. Extensive simulation results also show that our model can achieve better against the threats of exaggeration, collusion, disguise, sybil and single-behavior.

References

[1] A. Jøsang, R. Ismail, C. Boyd, A survey of trust and reputation systems for online service provision, Decis. Support Syst. 43 (2) (2007) 618–644.
[2] Y. Wang, A. Nakao, Poisonedwater: An improved approach for accurate reputation ranking in p2p networks, Future Gener. Comput. Syst. 26 (8) (2010) 1317–1326.
[3] P. Resnick, K. Kuwabara, R. Zeckhauser, E. Friedman, Reputation systems, Commun. ACM 43 (12) (2000) 45–48.
[4] S. Song, K. Hwang, R. Zhou, Y. Kwok, Trusted p2p transactions with fuzzy reputation aggregation, IEEE Internet Comput. 9 (6) (2005) 24–34.
[5] A. Tajeddine, A. Kayssi, A. Chehab, H. Artail, Patrol-f-a comprehensive reputation-based trust model with fuzzy subsystems, in: Autonomic and Trusted Computing: Third International Conference, ATC 2006, Wuhan, China, September 3–6, 2006, in: Lecture Notes in Comput. Sci., vol. 4158, Springer-Verlag New York, Inc., 2006, p. 205.
[6] S. Schmidt, R. Steele, T. Dillon, E. Chang, Fuzzy trust evaluation and credibility development in multi-agent systems, Applied Soft Comput. 7 (2) (2007) 492–505.
[7] Y. Wang, V. Cahill, E. Gray, C. Harris, L. Liao, Bayesian network based trust management, in: Autonomic and Trusted Computing: Third International Conference, ATC 2006, Wuhan, China, September 3–6, 2006, in: Lecture Notes in Comput. Sci., vol. 4158, Springer-Verlag New York, Inc., 2006, p. 246.
[8] S. Buchegger, J. Le Boudec, A robust reputation system for mobile ad-hoc networks, in: Proceedings of the Second Workshop Economics of P2P Systems, 2004.
[9] A. Jøsang, A logic for uncertain probabilities, Internat. J. Uncertain. Fuzziness Knowledge-Based Systems 9 (3) (2001) 279–311.
[10] A. Jøsang, R. Ismail, The beta reputation system, in: Proceedings of the 15th Bled Electronic Commerce Conference, vol. 160, 2002.
[11] C. Castelfranchi, R. Falcone, Social trust: A cognitive approach, Trust Deception Virtual Soc. (2001) 55–90.
[12] C. Castelfranchi, R. Falcone, G. Pezzulo, Integrating trustfulness and decision using fuzzy cognitive maps, Lecture Notes in Comput. Sci. 2692 (2003) 195–210.
[13] B. Edmonds, E. Norling, D. Hales, Towards the evolution of social structure, Comput. Math. Organ. Theory 15 (2) (2009) 78–94.
[14] A. Marcozzi, D. Hales, Emergent social rationality in a peer-to-peer system, Adv. Complex Syst. 11 (04) (2008) 581–595.
[15] Y. Ren, M. Li, K. Sakurai, Finetrust: a fine-grained trust model for peer-to-peer networks, Sec. Commun. Networks 4 (1) (2011) 61–69.
[16] Y. Zhang, Y. Fang, A fine-grained reputation system for reliable service selection in peer-to-peer networks, IEEE Trans. Parallel Distributed Syst. (2007) 1134–1145.
[17] C. Dellarocas, Efficiency and robustness of binary feedback mechanisms in trading environments with moral hazard, Working papers.
[18] J. Corbo, D. Parkes, The price of selfish behavior in bilateral network formation, in: Proceedings of the Twenty-Fourth Annual ACM Symposium on Principles of Distributed Computing, ACM, 2005, pp. 99–107.
[19] T. Moscibroda, S. Schmid, R. Wattenhofer, On the topologies formed by selfish peers, in: Proceedings of the Twenty-Fifth Annual ACM Symposium on Principles of Distributed Computing, ACM, 2006, pp. 133–142.
[20] A. Nakao, Y. Wang, On cooperative and efficient overlay network evolution based on a group selection pattern, IEEE Trans. Syst. Man Cyb., Part B, Cyb. 40 (2) (2010) 493.
[21] J. Kleinberg, Authoritative sources in a hyperlinked environment, J. ACM (JACM) 46 (5) (1999) 604–632.
[22] F. Kerschbaum, J. Haller, Y. Karabulut, P. Robinson, Pathtrust: A trust-based reputation service for virtual organization formation, Trust Manag. (2006) 193–205.
[23] S. Kamvar, M. Schlosser, H. Garcia-Molina, The eigentrust algorithm for reputation management in p2p networks, in: Proceedings of the 12th International Conference on World Wide Web, ACM, 2003, pp. 640–651.
[24] L. Xiong, L. Liu, Peertrust: Supporting reputation-based trust for peer-to-peer electronic communities, IEEE Trans. Knowledge Data Engin. 16 (7) (2004) 843–857.
[25] D. Wu, Y. Sun, Cooperation in multi-agent bidding, Decis. Support Syst. 33 (3) (2002) 335–347.
[26] S.M. Allen, G. Colombo, R.M. Whitaker, Cooperation through self-similar social networks, ACM Trans. Auton. Adaptive Syst. 5 (1) (2010) 1–29.
[27] F. Marmol, G. Pérez, Security threats scenarios in trust and reputation models for distributed systems, Comput. Security 28 (7) (2009) 545–556.
[28] Y. Wang, A. Nakao, J. Ma, Hoprec: Hop-based recommendation ability enhanced reputation ranking in p2p networks, IEICE Trans. Inform. Syst. 93 (3) (2010) 438–447.
[29] R. Zhou, K. Hwang, Powertrust: A robust and scalable reputation system for trusted peer-to-peer computing, IEEE Trans. Parallel Distrib. Syst. 18 (4) (2007) 460–473.
[30] A. Maristella, P. Luca, A theoretical study of a generalized version of kleinberg's hits algorithm, Inf. Retr. 8 (2) (2005) 219–243.
[31] Y. Wang, A. Nakao, A. Vasilakos, Doubleface: Robust reputation ranking based on link analysis in p2p networks, Cybernet. Systems 41 (2) (2010) 167–189.