IEICE TRANS. INF. & SYST., VOL.E93–D, NO.3 MARCH 2010

PAPER Special Section on Trust, Security and Privacy for Pervasive Applications

A Trust Management Model Based on Bi-evaluation in P2P Networks**

Jingyu FENG[†], **Yuqing ZHANG**[††*a)], ***Nonmembers***, ***and*** **Hong WANG**[†††], ***Member***

SUMMARY The security of P2P networks depends on building trust management among peers. However, current trust management models focus on preventing untrustworthy resources from spreading by malicious providers, but have few effects on reducing denial-of-service attacks of malicious consumers and free riding of selfish peers. Pointing to these problems, a bi-evaluation*** trust management model, called BiTrust, is proposed. In this model, the trustworthiness of a peer is divided into service and request trustworthiness. Service trustworthiness shows the resources reliability of providers, and request trustworthiness is used to deal with requests from consumers, which can keep away malicious consumers and encourage selfish peers to share resources. A generic method for evaluating service and request trustworthiness is described. Furthermore, the implementation strategies of the model are also depicted in this paper. The following analysis and simulation show that BiTrust is more effective on enhancing high-quality resources sharing among peers and more advanced in successful exchanges rate.

key words: *P2P, file-sharing, trust, bidirectional*

1. Introduction

In recent years, P2P file-sharing has gained wide applications, such as Maze, Gnutella, Naspter and BitTorrent. The application of these file-sharing systems composes of a series of P2P networks, where a peer can perform as a provider of resources or a consumer. Despite the autonomous and open nature of P2P networks facilitate peer activities, it also makes P2P networks very vulnerable to abuse by malicious peers [1]. For example, VBS.Gnutella [2] can spread in Gnutella. It is necessary to find an efficient way to prevent virtues from spreading in resource exchanges among peers.

To enhance the security among peers, trust management theories in social networks are introduced to construct trust models, which can effectively suppress malicious behaviors, such as resource-abusing, fraud, and so on [3]. In most trust models, trustworthiness of peers is used to prevent untrustworthy resources from spreading by malicious providers [4].

However, this approach has some effects on the simple identifying of malicious providers, but has few effects on coping with denial-of-service attacks of malicious consumers and free riding of selfish peers. For example, the request resolution of consuming resources may tend to exhaust the provider's serving capabilities (like processing capacity and bandwidth) [5]. One of the simplest attacks of malicious consumers could be achieved by bombarding a provider with lots of requests so as to reduce its capabilities to respond to other normal requests and provide resources, resulting in denial-of-service attacks. Furthermore, free riding may lead to degradation of the network performance. It has been established that nearly 70% of Gnutella users share no files, and nearly 50% of all responses are returned by the top 1% of sharing hosts [6]. Consequently, malicious behaviors and free riding, which are very unfavorable to the survival and development of P2P networks, must be suppressed. In order to make the P2P networks secure, the availability of trust management theories is necessary to apply in the existing access control mechanism [7]. A provider should classify consumers and assign different access rights to each consumer, even if the consumers were previously unknown [8]. In conclusion, the trust relationship among peers should be bidirectional evaluation. While consumers guard against malicious providers, providers must also provide resources selectively.

With these research problems in mind, we develop BiTrust, a P2P trust model using bidirectional evaluation. This model utilizes service and request trustworthiness to implement the bidirectional evaluation of trust relationship in the initialization of an exchange. ST (Service Trustworthiness) shows the service of reliability of providers. RT (Request Trustworthiness) reflects the right that consumers obtain resources. According to their own trust beliefs, both of the participants will observe the trustworthiness of the other party to decide whether to perform the exchange after the initialization or not. Should ST show that the provider is malicious, the consumer may give up the provider and find a new one instead. Should RT show that the consumer is malicious, the provider may refuse to respond to the exchange request so as to guard against denial-of-service attacks from malicious consumers. Thus, malicious peers who can nei-

Manuscript received July 1, 2009.
Manuscript revised October 7, 2009.

[†]The author is with Key Lab of Computer Networks and Information Security of Ministry of Education, Xidian University, Xi'an 710071, China.
[††]The author is with National Computer Network Intrusion Protection Center, GUCAS, Beijing 100043, China.
[†††]The author is with the Department of Computer Science and Technology, Huaibei Coal Normal College, Huaibei 235000, Anhui, China.
[*]Corresponding author.

**This work is supported by the National Natural Science Foundation of China under Grant No.60773135, No.60970140, No.90718007 and No.60773121, as well as the High Technology Research and Development Program of China (863 Program) under Grant No.2007AA01Z427 and No.2007AA01Z450.

a) E-mail: zhangyq@gucas.ac.cn

DOI: 10.1587/transinf.E93.D.466

***Bi-evaluation is the abbreviation of bidirectional evaluation.

ther provide untrustworthy resources nor obtain resources from other peers could be isolated from P2P networks. At the same time, the result that RT restricts the right of selfish peers to obtain resources would make them share resources actively to improve their RT.

The rest of the paper is organized as follows: In Sect. 2, related work is briefly introduced. We present the approach of evaluating ST and RT in Sect. 3. Section 4 describes implementation strategies of BiTrust, including trust-based exchange selection scheme and performing algorithms for the model. Section 5 simulates our model. Finally, we conclude in Sect. 6.

2. Related Work

In an open P2P network, there is no centralized authority for maintaining and distributing trustworthiness data. With a trust management model, a peer in a P2P network can evaluate each other's trustworthiness. Some of previous studies are related on trust management in P2P networks.

EigenTrust [3] aggregated trustworthiness scores by a weighted sum of all raw trust recommendations, and assumes pre-trust peers and uses majority voting to check faulty recommendations reported. Wang et al. [9] designed the incentive-compatible trustworthiness feedback scheme based on well-known economic model, and characterized the social features of trust network in terms of efficiency and cost. Wang's model could combat the selfish and malicious peer behaviors, and could efficiently increase successful exchange rate. PowerTrust [10] dynamically selected small number of power peers that are most credible using a distributed ranking mechanism to improve aggregation speed. GossipTrust [11] offered the very first attempt to extend the gossip protocol for trustworthiness aggregation in P2P networks without any structured overlay support.

However, these traditional models have few effects in suppressing malicious consumers and selfish peers. It is available to build trust management using bi-evaluation to suppress selfish peers, malicious providers and consumers simultaneously. The study of bi-evaluation first appeared in trust management model for e-Commerce. Participants at eBay's auctions rate each other after each transaction, and use completely centralized mechanisms for storing and exploring trustworthiness data [12]. Mul et al. [13] described the relationship between trust and reciprocity, and encouraged two concerned agents to cooperate.

Typical issues in using bi-evaluation in trust management for P2P networks include the measure of finding providers with high-quality resources and responding to requests from consumers. Some of analogous models have been proposed, which assign each user different access rights on the basis of isolating untrustworthy resources. L. Wang et al. [7] presented a recommendation trust model and described some access policies based on trust, in which the peers with higher trust level can get higher access authority. But the model only evaluates consumers' trustworthiness to assign them access rights. Tran et al. [8] proposed a trust based access control framework, in which the procedure in a typical interaction between a consumer and a provider is presented. But the access values they evaluate are used to select credible providers. William et al. [14] proposed a decentralized access control system that implements sociological trust constructs in a quantitative system to evaluate interaction partners. However, there are no effective trust metric and no experimental results to validate their approach. Above all, these models can not bi-evaluate the trustworthiness of both the participates completely.

The trustworthiness of a peer is divided into service and request trustworthiness in this paper. Participates in an exchange then evaluate each other with the help of the two metrics. Specially, our model which integrates trustworthiness, access authority and trust-based exchange selection scheme leads to several advantages in a P2P network. In our model, a peer who wants to obtain more resources has to firstly supply other peers with high-quality resources. Also, peers who provide corrupted resources could be isolated and their access requests would be refused. Thus, a peer has to actively share resources to get enough access authorities that make it obtain their desired resources.

3. The Bi-evaluation of Trustworthiness

P2P networks are formed by the topology among peers joining P2P file-sharing systems, where peers communicate with each other and exchange resources. With trust management theories, consumers obtain reliable resources and providers receive the evaluation of its credible behavior after an exchange. However, it is not enough to suppress malicious consumers and selfish peers. This problem can be solved by introducing ST and RT to implement bi-evaluation among peers. In this section, we formalize the two trust metrics and explain how to evaluate them.

3.1 Evaluating Service Trustworthiness

In order to obtain reliable resources, peer i firstly sends some requests to the network and then finds a credible provider among the set of responding providers in the light of ST. Let peer j denote the provider and ST_{ij} denote the service trust value from peer i to peer j. ST_{ij} is defined in Eq. (1).

$$ST_{ij} = \alpha DST_{ij} + \beta IST_{ij}, \alpha + \beta = 1 \tag{1}$$

where DST_{ij} is the direct service trust value from peer i to peer j and IST_{ij} is the indirect service trust value. α and β denote the normalized weight factors for DST_{ij} and IST_{ij}, respectively. The calculation of α is in Eq. (2).

$$\alpha = \frac{1}{N(j)}\left(1 - \frac{1}{N(ij) + M(ij)}\right) \tag{2}$$

Obviously, α is proportional to $N(ij)$ and $M(ij)$, and inversely proportional to $N(j)$. The three parameters will be explained in the subsection.

Table 1 The numerical description of S_r.

S_1	S_2	S_3	S_4	S_5
$0 \le S_1 < 0.2$	$0.2 \le S_2 < 0.4$	$0.4 \le S_3 < 0.6$	$0.6 \le S_4 < 0.8$	$0.8 \le S_5 < 1$

3.1.1 Direct Service Trustworthiness

DST (Direct Service Trustworthiness) is the direct credible opinions from one peer to another peer. The calculation of DST_{ij} mainly depends on the satisfaction that peer i obtains resources from peer j.

With respect to the satisfaction of resources, there are five kinds of situation that should be taken into account. [15]: S_1 (There are malicious resources such as Trojan Horses and viruses.), S_2 (False resources), S_3 (No response or rejecting exchange), S_4 (The quality of resources is general), S_5 (The quality of resources is good). The numerical description of this partition is shown in Table 1.

In addition, the calculation of DST_{ij} is also affected by other parameters. Given a recent time window, let $N(ij)$ denote the total number of exchanges performed by peer i with peer j, m_k denote the magnitude of resources peer i receiving from peer j in their kth exchange, $M(ij)$ denote the total magnitude of resources received by peer i among $N(ij)$ exchanges, f_k denote the time recessionary index in the kth exchange. DST_{ij} is defined in Eq. (3).

$$DST_{ij} = \sum_{k=1}^{N(ij)} S_k m_k f_k \Big/ M(ij) \sum_{k=1}^{N(ij)} f_k \tag{3}$$

where we define $M(ij) = \sum_{k=1}^{N(ij)} m_k$ and $f_k = e^{k-N(ij)}$.

3.1.2 Indirect Service Trustworthiness

IST (Indirect Service Trustworthiness) is the indirect credible opinions from one peer to another peer through other peers' recommendations. If peer i is not sure about the DST of peer j, it would ask the other peers to make recommendations for peer j. These recommendations are used to formalize the evaluation of IST from peer i to peer j in succession. Let Ψ denote the set of recommending peers, peer w denote one of them. DST_{ij} is defined in Eq. (4).

$$IST_{ij} = \sum_{w \in \Psi} L_{wj} * C_w \tag{4}$$

C_w is the credibility of w'recommendation. Without the factor, some of malicious peers would submit dishonest recommendation and collude with each other to boost their own ratings or bad-mouth other peers [16]. Different approaches are used to determine the factor. One way is to use the DST of a recommending peer as its credibility factor. However, it is possible (though not common) that a peer may maintain a good reputation by performing high quality services, but send malicious feedback to its competitors [17]. Using DST to approximate the credibility of recommendations would generate errors. Moreover, it is impossible to use a personalized similarity measure to rate the credibility factor of peer w through i's personalized experience, as finding the common set of peers that have interacted with both peer i and w will make trustworthiness evaluation more complex.

The best measure is to quantify the similarity between w's recommendation L_{wj} and the mean of these $C_w = \mid L_{wj} - \lambda \mid$ recommendations. Here, we can define $\lambda = \frac{1}{N(j)} \sum_{w \in \Psi} L_{wj}$.

For each $C_w \sim 1$, there is a collusive group. Then peer i should find new recommending peers instead.

3.2 Evaluating Request Trustworthiness

As the credential of a consumer to obtain resources, its RT (Request Trustworthiness) is utilized by the provider to provide resources selectively. The evaluation of RT corresponds with the past behaviors when the consumer was a provider. For example, the RT of peer i would be enhanced by its past active behaviors, and vice verse. In other words, the evaluation of i's RT is affected by its past binary behaviors. Consequently, our model uses the Bayesian probability to represent the RT from peer j to peer i. Bayesian systems take binary ratings as input, namely, positive and negative.

Given a recent time window, let pos and neg represent the amount of positive and negative ratings respectively. These binary ratings about peer i come from peer j itself or other peers' recommendations. It is reasonable to expect that the greater the number of peers that peer i has interacted with by active behaviors, the more the amount of pos it would have. And then the beta PDF denoted by $beta(pos, neg)$ can be expressed with the gamma function:

$$beta(pos, neg) = \frac{\Gamma(pos + neg)}{\Gamma(pos)\Gamma(neg)} \theta^{pos-1}(1-\theta)^{neg-1} \tag{5}$$

where $0 \le \theta < 1, pos, neg > 1$.

By observing the amount of positive and negative ratings, the RT of peer i maintained at peer j is given by: $RT_{ji} = beta(pos + 1, neg + 1)$, which is related to the probability that peer i cooperates with peer j in next exchange. Otherwise, the probability expectation value of the beta distribution is given by: $E[beta(pos, neg)] = pos/(pos + neg)$ [18]. Thus, RT_{ji} can be further described is as follows:

$$RT_{ji} = \frac{pos + 1}{pos + neg + 2} \tag{6}$$

4. Implementation Strategies

The effectiveness of supporting a trust model depends not only on the parameters and metrics for evaluating trustworthiness, but also on the implementation of the trust model in a P2P network. Typical issues in implementing a trust model such as BiTrust in a P2P network include trust-based exchange selection scheme and its performing algorithms for the model.

4.1 Trust-Based Exchange Selection Scheme

As a peer has two kinds of identity, a malicious peer also

has two kinds of identity: malicious provider and malicious consumer. Without centralized control in P2P networks, it is difficult to suppress malicious providers and malicious consumers synchronously. Thus, a key objective of trust-based exchange selection scheme is to select a credible consumer and provider. The ST and RT produced by bidirectional evaluation give a secure platform for the exchanging peers. In the subsection, let peer i also represent a consumer, peer j represent a provider.

While an exchange is initialized, ST plays an important role in the process of i's selecting a credible provider. With ST, peer i estimates on trust relationship about peer j to determine whether to perform an exchange. A decision rule for peer i to form a trust action on peer j is described as $ST_{ij} > ST_{threshhold(i)}$, where $ST_{threshhold(i)}$ is the ST threshold for peer i to trust another peer. By doing so, it reduces the risk of obtaining inauthentic or corrupted resources from malicious providers. On being selected as the provider, peer j will receive an access request from peer i. Subsequently, peer j decides how to respond to the request.

To identify malicious peers and selfish peers, peer j must supply different peers with different authorities. Generally speaking, good peers have higher authority than the other two kinds of peers. This would inspire peers to perform active behaviors and increase their RT, such as providing high-quality resources. Peers who provide low-quality resources will get lower RT, and then will have very limited authorities while accessing other peers.

Let $R = \{0, common, priority\}$ denote the set of peer j's access authorities, $RT_{threshhold1(j)}$ and $RT_{threshhold2(j)}$ denote two types of RT threshold for peer j to provide resources selectively. By comparing the two types of threshold, peer j gives peer i the access authority r:

- **Prior access authority:**
  For $RT_{ji} > RT_{threshhold2}(j) \rightarrow r = priority$, peer i is a good peer. Thus, peer j gives peer i the prior access authority and feedback tuple $(priority, RT_{ji})$. While several peers sent access requests, peer j would respond to these requests from high to low.
- **Common access authority:**
  For $RT_{ji} \in [RT_{threshhold1}(j), RT_{threshhold2}(j)] \rightarrow r = common$, peer i is a selfish peer. Thus, peer j gives peer i the common access authority and feedback tuple $(common, RT_{ji})$. The function of this authority is to reduce the chance that selfish peers get their desired resources. It makes peers believe that active participation in P2P networks means better chance to obtain the desired resources.
- **Zero access authority:**
  For $RT_{ji} < RT_{threshhold1}(j) \rightarrow r = 0$, peer i is a malicious peer. As a result, peer j gives peer i the zero access authority and feedback tuple $(0, RT_{ji})$. The function of this authority is to suppress malicious consumers and abolish their right of obtaining resources.

4.2 Performing Algorithm

Our model is performed in the following two phases: 1) Initializing an exchange; 2) Updating the provider' trustworthiness at the end of an exchange. The first step is that the consumer selects the provider and sends an access request in the initialization of an exchange, which can be achieved by Algorithm 1. The provider responds to the request and feedbacks tuple (r, RT_{ji}) is the second step, which can be achieved by Algorithm 2.

Algorithm 1. SendingRequest(i, Φ)
Input: i, Φ the set of providers
Output: Req
for $i \in \Phi$ do
/* Peer i select peer j as the provider */
  $ST_{ij} \leftarrow Eq.(1)$.
  if $(ST_{ij} > ST_{threshhold}(i))$ do
    $Req \leftarrow 1$;
/* Peer i sends Req that is the access request */
  else
    $Req \leftarrow 0$;
    $Provider \leftarrow \Phi$;
/* Peer i selects a new provider again */
    end if
end for

Algorithm 2. ProcessingRequest(i, j)
Input: i, j
Output: Ack
$RT_{ji} \leftarrow Eq.(6)$.
if $(RT_{ji} > RT_{threshhold2}(j))$ do
  $Ack \leftarrow (priority, RT_{ji})$;
/* Peer j feedbacks Ack */
else if $(RT\,ji \in [RT_{threshhold1}(j), RT_{threshhold2}(j)])$
    $Ack \leftarrow (common, RT_{ji})$;
  else if $(RT_{ji} < RT_{threshhold1}(j))$
      $Ack \leftarrow (0, RT_{ji})$;
    end if
  end if
end if

Finally, the consumer must rate the provider's behavior at the end of an exchange. During this period, the DST of the provider will be updated. Besides, pos and neg corresponding to the provider's behavior will be recorded.

Algorithm 3. RatingProvider(i, j)
Input: i, j
Output: DST_{ij}, pos and neg
$S_k \leftarrow$rating peer i;
/* Peer i rates j's behavior */
$DST_{ij} \leftarrow Eq.(6)$. ;
/* Updating DST_{ij} */
if $(S_k < 0.6)$ do
/* Updating pos and neg */
  $pos \leftarrow 0$;
  $neg \leftarrow 1$;
else
  $pos \leftarrow 1$;

Table 2 Description of simulation elements.

	Description	Default
Environment Setting	Number of peers in the network	100
	Percentage of malicious peers	10%-50%
	Percentage of selfish peers	20%
	Percentage of good peers	40%
Behavior Patterns	Malicious peers provide inauthentic or corrupted resources and attack other peers by denial-of-service. Selfish peers do not share resources without incentive measures. Good peers execute active behavior and provide high-quality resources.	
Trustworthiness Threshold	$ST_{threshhold}(i)$	0.4
	$RT_{threshhold1}(j)$	0.4
	$RT_{threshhold2}(j)$	0.6

$neg \leftarrow 0$;
else if

5. Experimental Analysis

We performed three simulations to validate the BiTrust approach, and show its effectiveness and robustness. The first one validates effect of BiTrust in terms of its reducing malicious query responses. The second one validates effect of BiTrust in terms of its suppressing selfish peers. Last, by comparing BiTrust with EigenTrust, Wang's model [9] and Random[†], we analyze the successful exchanges rate of these models vary with the percentage of malicious peers.

5.1 Simulation Setup

We implemented these simulations through QueryCycle developed by Stanford University [19]. In this subsection, we describe the general simulation setup, including the environment setting, behavior patterns and trustworthiness threshold.

The simulation setting includes three types of peers: malicious peers, selfish peers and good peers, and their behavior patterns are given in Table 2. The experiments initiates as peers perform random exchanges with each others. After a few exchanges, a trusted network topology is gradually formed by trust management. The participating peers then use the trusted-based exchange selection scheme and algorithms to select the provider or consumer with high trustworthiness to perform an exchange, and update DST, *pos* and *neg* on related peers.

5.2 Simulation Results

In the first and second simulation, we validate the effectiveness of BiTrust in terms of comparing BiTrust with Baseline which is an unidirectional trust model with only considering ST. By doing so, we can test that BiTrust based on bi-evaluation is more effective than unidirectional trust model to suppress two types of peers. To ensure the authenticity of simulating the effectiveness of BiTrust, the two simulations are performed in the case of the percentage of malicious peers by 40%. Finally, we validate the robustness of BiTrust.

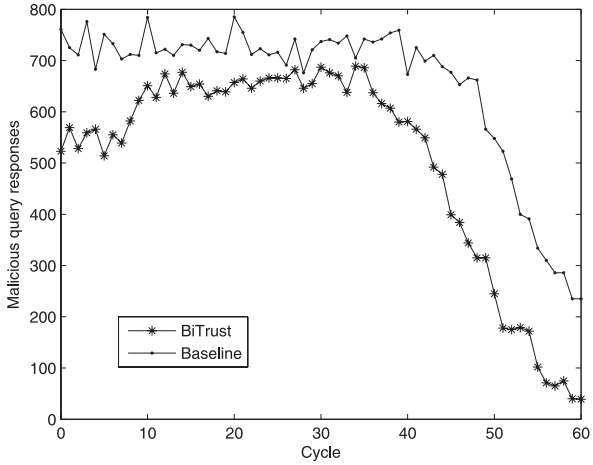

Fig. 1 Reducing malicious query responses.

Simulation 1. Figure 1 shows the effectiveness of reducing malicious query responses. Malicious peers provide inauthentic or corrupted resources and attack other peers by denial-of-service, which generates a large amount of malicious query responses. So, the best measure to suppress malicious peers is to reduce the number of malicious query responses. As shown in Fig. 1, the curve of BiTrust is lower than that of Baseline. Baseline makes a consumer only abandon a malicious provider by its ST and pick up a new provider on the basis of Algorithm 1, wherease BiTrust can further utilize Algorithm 2 to make a provider feedback the zero access authority to a malicious consumer by its ST. As a result, malicious peers in BiTrust can neither obtain resources nor provide resources, which will make them lose the ability to survive in the network. Consequently, the function of BiTrust's suppressing malicious peers is better than Baseline.

Simulation 2. Figure 2 shows the effectiveness of suppressing selfish peers. These peers become leeches and drain resources from the network [20]. With an incentive measure, selfish peers can be transformed into good peers. As shown in Fig. 2, the rate of selfish peers decreases gradually by 250 cycles, and the curve of BiTrust is lower than that of Baesline. The reason is that BiTrust makes a few selfish peers change their past behaviors to share resources on the basis of Algorithm 3, which enhance their ST and RT. Then, these peers are transformed into good peers. However, Baseline only inspires selfish peers to improve their ST by active behaviors. Without RT, selfish peers are insufficiently encouraged to share more resources in the unidirectional trust model. Thus, BiTrust is more effective than Baseline to suppress selfish peers.

Simulation 3. Figure 3 shows successful exchanges rate vs. the percentage of malicious peers. An exchange is

[†]Random is the case when there is no trust management in a P2P network.

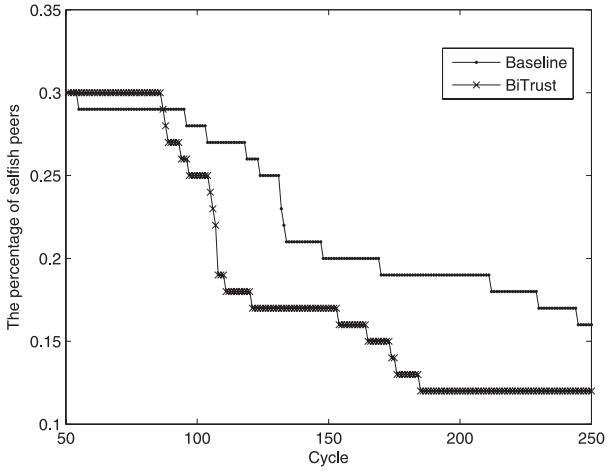

Fig. 2 Suppressing selfish peers.

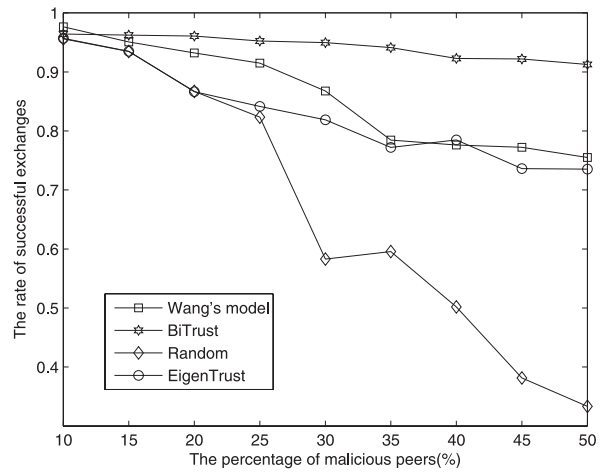

Fig. 3 The rate of successful exchanges vs. the percentage of malicious peers.

considered to be successful if both of the participants cooperate. A successful exchange rate is defined as the ratio of the number of successful exchanges over the total number of exchanges in a P2P network up to a certain time [9]. Specially, the successful exchanges rate of a trust model reflect its robustness, namely, the ability of the model to prevent malicious attacks.

To ensure the accuracy of the simulation results, each trust model is implemented 60 cycles. Besides, we gather data for every cycle and calculate their mean. As shown in Fig. 3, the successful exchanges rate of Random descends quickly. This is because the network might not prevent malicious peers without a trust model. Compared with traditional trust model EigenTrust and Wang's model, the curve slop of BiTrust is much slower as it can suppress malicious consumers and providers simultaneously. In conclusion, BiTrust can reduce the total number of unsuccessful exchanges through suppressing malicious peers, and enhance the total number of successful exchanges through suppressing selfish peers. So its successful exchanges rate is better than other models.

6. Conclusion

We have presented a bi-evaluation trust model to suppress malicious peers and selfish peers for P2P networks. The trustworthiness of a peer consists of ST and RT, which are used to evaluate the trust relationship between the participants of an exchange. Also, we have described the implementation strategies of BiTrust. While a consumer selects a credible provider by its ST, the selected provider establishes the consumer's access authority. Simulation results show that our model can suppress malicious peers and selfish peers effectively, and has much better successful exchanges rate than other models. Furthermore, the detailed threat analysis in P2P networks and the detailed bi-evaluation of trust relationship among peers under large scale network environment remain for further studies.

References

[1] E. Sit and R. Morris, "Security considerations for P2P distributed hash tables," Proc. Int'l Workshop Peer-to-Peer Systems (IPTPS '02), pp.261–269, March 2003.
[2] "Vbs.gnutella worm," http://securityresponse.symantec.com/avcenter/venc/data/vbs.gnutella.html
[3] S. Kamvar, M. Schlosser, and H. Garcia-Molina, "The eigentrust algorithm for reputation management in P2P Networks," Proc. 12th International World Wide Web Conference, pp.640–651, May 2003.
[4] O.H. Kwon, S.Y. Lee, and J. Kim, "FileTrust: Reputation management for reliable resource sharing in structured peer-to-peer networks," IEICE Trans. Commun., vol.E90-B, no.4, pp.826–835, April 2007.
[5] A. Gummadi and J. Yoon, "Modeling group trust for peer-to-peer access control," Proc. 15th Int'l Workshop on Database and Expert Systems Applications, pp.971–978, 2004.
[6] E. Adar and B. Huberman, "Freeriding on gnutella," First -Monday, vol.5, no.2, pp.42–68, 2000.
[7] L. Wang, Y.Q. Zhu, L.F. Jin, and X.Z. Luo, "Trust mechanism in distributed access control model of P2P networks," 17th IEEE/ACIS International Conference on Computer and Information Science, pp.19–24, 2008.
[8] H. Tran, M. Hitchens, V. Varadharajan, and P. Watters, "A trust based access control framework for P2P file-sharing systems," Proc. 38th Hawaii International Conference on System Sciences, pp.1–10, 2005.
[9] Y.F. Wang, Y. Hori, and K. Sakiurai, "Characterizing economic and social properties of trust and reputation systems in P2P environment," J. Computer Science and Technology, vol.23, no.1, pp.129–140, Jan. 2008.
[10] R.F. Zhou and K. Hwang, "PowerTrust: A robust and scalable reputation system for trusted P2P computing," IEEE Trans. Parallel Distrib. Syst., vol.18, no.7, pp.460–473, April 2007.
[11] R.F. Zhou and K. Hwang, "Gossip for fast reputation aggregation in peer-to-peer networks," IEEE Trans. Knowl. Data Eng., vol.20, no.9, pp.1282–1295, Sept. 2008.
[12] K. Aberer and Z. Despotovice, "Managing trust in a peer-to-peer information system," Proc. ACM 10th International Conference. Information and Knowledge Management (CIKM), pp.310–317, 2001.
[13] L. Mui, M. Mohtashemi, and A. Halberstadt, "A computational model for trust and reputation," Proc. 35th Hawaii Int'l Conf on System Sciences, pp.2431–2439, Hawaii, 2002.
[14] J. William and I. Davis, "Toward a decentralized trust-based access control system for dynamic collaboration," Proc. IEEE Workshop on

Information Assurance and Security, pp.317–324, 2005.
[15] C.Q. Tian, S.H. Zhou, W.D. Wang, and S.D. Cheng, "Trust model based on reputation for peer-to-peer networks," Journal on Communication, vol.29, no.3, pp.63–70, April 2008.
[16] K.W. Wang, K.Q. Li, W.Y. Qu, and Y. Xian, "A time-decay based P2P trust model," 2009 Inernational Conference on Networ-ks Security, Wireless Communications and Trusted Computing, pp.235–238, 2009.
[17] L. Xiong and L. Liu, "PeerTrust: Supporting reputation-based trust for peer-to-peer electronic communities," IEEE Trans. Knowl. Data Eng., vol.16, no.7, pp.843–857, July 2004.
[18] A. Jϕsang and R. Ismail, "The beta reputation system," Proc. 15th Bled Electronic Commence Conference, pp.1–14, June 2002.
[19] "The stanford P2P sociology project," http://p2p.standford.edu/www/demos.htm/, May 2003.
[20] J.L. Hu, Q.Y. Wu, and B. Zhou, "TTEM: An effective trust-based topology evolution mechanism for P2P networks," Journal of Communications, vol.3, no.7, pp.3–10, 2008.

Jingyu Feng received the B.Sc in electrical information science and technology from Lanzhou University of Technology, China, in 2006. He has joined in 2006 for his M.Sc and Ph.D. in Xidian University. His current research interests include trust management and P2P security.

Yuqing Zhang is a professor and supervisor of Ph.D. students of Graduate University of Chinese Academy of Sciences. He received his B.Sc and M.Sc in computer science from Xidian University, China, in 1987 and 1990 respectively. He received his Ph.D. degree in Cryptography from Xidian University in 2000. His research interests include cryptography, wireless security and trust management.

Hong Wang received his B.S. degree in applied mathematics in 1994 and the M.S. degree in Cryptography in 1998, both from Zhengzhou Information Engineering University, Henan, China. He received his Ph.D. degree in Cryptography in 2001 from Xidian University, Xi'an, China. He is currently a professor of the Department of Computer Science and Technology at the Huaibei Coal Normal College, Anhui, China. His current research interests include computer cryptography, network security, and digital right management.