DISTRIBUTED TRUST INFERENCE MODEL BASED ON PROBABILITY AND BALANCE THEORY FOR PEER-TO-PEER SYSTEMS

Zhenhua Tan, Guangming Yang*, Wei Cheng
Software College of Northeastern University, MailBox 349#
Shenyang, 110819, China
Emails: tanzh@mail.neu.edu.cn, yanggm@mail.neu.edu.cn, chengw@mail.neu.edu.cn

Submitted: Aug. 1, 2012 ***Accepted: Oct. 30, 2012*** ***Published: Dec. 1, 2012***

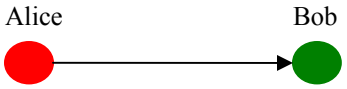
Abstract- Researchers have done much around how to measure trust degrees or levels by local and global style in a given distributed network. However, how to infer trust degree for a strange node efficiently in a large-scale distributed environment was little done. This paper focuses on this problem, and proposes a novel trust model based on balance theory and probability theory. We firstly design a simple direct trust model for evidence computing, then construct trust relations network and trust inference network based on direct trust network. In order to discover trusted evidence chains during complex relations, we design two inference rules and propose mathematics models to infer indirect trust value based on Markov chain theory. Simulations proved the rightness and effectiveness in intensive trust relations environment and intensive distrust environment.

Index terms*: trust model, trust inference, peer-to-peer security, distributed system, trusted evidence chain, trust probability, peer-to-peer network.*

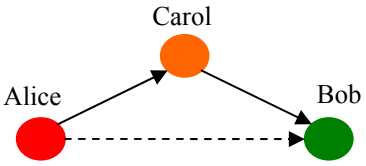
I. INTRODUCTION

As one of the important components of Internet, peer-to-peer networks make a significant impact on Internet Applications, such as P2P community, P2P search engine, P2P files sharing, and P2P media service, due to openness and anonymity. Meanwhile, benefits from principles of P2P networks, P2P E-commerce systems (e.g. eBay) and P2P loan systems (e.g. Zopa.com) are also popular recently. However, some urgent problems regarding the availability and security of P2P networks remain unsolved, such as malicious attacking, team malicious cheating, intellectual property rights, selfish and routing attacking in P2P [1,2,3]. Trust management has been emerging as an essential complementary to security mechanisms of P2P systems. A well-defined trust model can provide meaningful decision support and help customer reduce possible risk during an Internet transaction.

Like trust and reputation in social networks, trust evaluation in P2P systems is based on communication histories. We call these histories trust evidences. Trust models are divided into two categories based on the way evidences are aggregated from an evaluator's perspective [4, 5]. They are local/direct trust model and global/indirect trust model. Local or direct trust models use the firsthand evidences of destination nodes [15, 16], while global or indirect trust models usually come from recommendations or references to destinations [6-14]. As shown in Figure 1. Alice can evaluate Bob's trust probability directly (Figure 1(a)) while there are direct evidences for Bob. In Figure 1(b), Alice can also evaluate indirect trustworthiness of Bob by computing direct trust values of <Alice, Carol> and <Carol, Bob>. Indirect trust models are more complex than direct models usually based on direct trust value.



(a) *Trust Evaluation Directly*



(b) *Trust Evaluation Indirectly*

Figure 1. Trust Evaluation

To compute indirect trust by traditional trust models, a trustor needs to aggregate all of the trustee's trust evidences, and then uses algorithms to compute or infer indirect trust degree.

Aberer and Despotovic [6] proposed a complaint-based trust inference method for a distributed P2P system, due to the lack of incentives for submitting feedbacks. Its complaint-only trust metric runs in few limited cases and is over-sensitive to the skewed distribution of the community and to several misbehaviors of the system. Although this mechanism has some limitations, it is the very early trust model for P2P E-commerce. Kamvar et al. presented the EigenTrust reputation system [7] to infer a unique global trust in a very distributed way by history. Such a global model does not need an administration center, difficult to guarantee a fast and secure convergence when computing the global trust. Nevertheless, it inspires our works. Dou and Wang et al. [8] improved the EigenTrust in computing convergence and model security. However, there remains an efficiency problem and its security mechanism is only from punishment and certification. Xiong and Liu [9] proposed a PeerTrust model with three basic trust parameters and two adaptive factors, and then define a general trust metric to combine them efficiently. Jøsang et al. [10] proposed a trust inference method for simplifying a complex network to express it in a series of parallel network. This solution may lead to the loss of trust information. They proposed an edge splitting method in the further works [11] to address this problem. Nevertheless, this method is valid only on a simple trust network and invalid on complex trust networks.

Gradually, researchers began to infer trust degree with multi-dimensional evidence factors. Wang and Wu [12] proposed a multi-dimensional evidence-based trust management system with multi-trusted paths (MeTrust for short) to conduct trust computation on any arbitrarily complex trusted graph. The trust computation in MeTrust has three tiers, namely, the node tier, the path tier, and the graph tier. It is an excellent trust model. However, it does not provide distributed storage structure for P2P system. Jiang at el. [13] presented a novel reputation-based trust mechanism for P2P e-commerce systems. In this mechanism, one peer has two kinds of reputations, local reputations and global reputations. To compute the local and global reputations precisely and to obtain stronger resistibility to attacks as well, they use many comprehensive factors in computing trust value in the mechanism. Anyway, this model is a comprehensive mechanism. However, its time factor is only linear and there is no clear method to resist team malicious behaviors. Tan and Cheng et al. [14] presented a global trust model with correlation factor based on communication

history, and improved the time factor with exponential equation. It shows a rational history vector and presents three trust models with multi-dimensional trust factors.

However, all of the above trust models face a common problem, that is, models are too difficult or infeasible to compute the indirect trust when no trusted recommendations happen or no (or sparse) common nodes' histories exist between trustor and trustee. Trust chain-based inference is quite a new method for a trustor to compute a trustee's indirect trust only according to the direct local trust relationships. We need to discover trusted evidence chains from trustor to trustee in a direct trust network firstly. There are two kinds of computation method usually used to infer the indirect trust by trusted chains. The first one is based on multiplication, which multiplies all direct trust degrees to obtain the trustee's final trust degree while the second one selects max or min trust value or average trust value from the trusted chain instead. However, the multiplication model will lead the result to be very small; even if the result is within the range of 0 and 1, it is not consistent with objective facts. In contrast, the second method ignores the importance of contribution from trusted nodes that have higher trust degree.

With these research problems in mind, we propose a new trust model based on trust and distrust information. We use a famous social psychological theory named “balance theory” [17] to design inference rules in this paper, and model a series of inference method by probability to compute indirect trust value. During the sparse history situation or between quite strange nodes, the proposed scheme can run well and infer trusted evidence chains relatively rational.

In the remainder of the paper, we will introduce modeling and definitions firstly in the next section. Section III describes the inference algorithms for proposed scheme, while the simulations and results follow in section IV, with conclusions afterwards in section V.

II. MODELING AND DEFINITIONS

a. Direct trust model

In this section, we design a very simple direct trust model by communication history that was presented in our former work [18]. Consider S_{ij} as the successful transactions amount between node <i, j>, while F_{ij} as the failed transactions amount. Then, let

$$dT(i,j)=\begin{cases} S_{ij}/S_{ij}+F_{ij}, i\neq j \\ 1, i=j \end{cases} \quad (1)$$

,

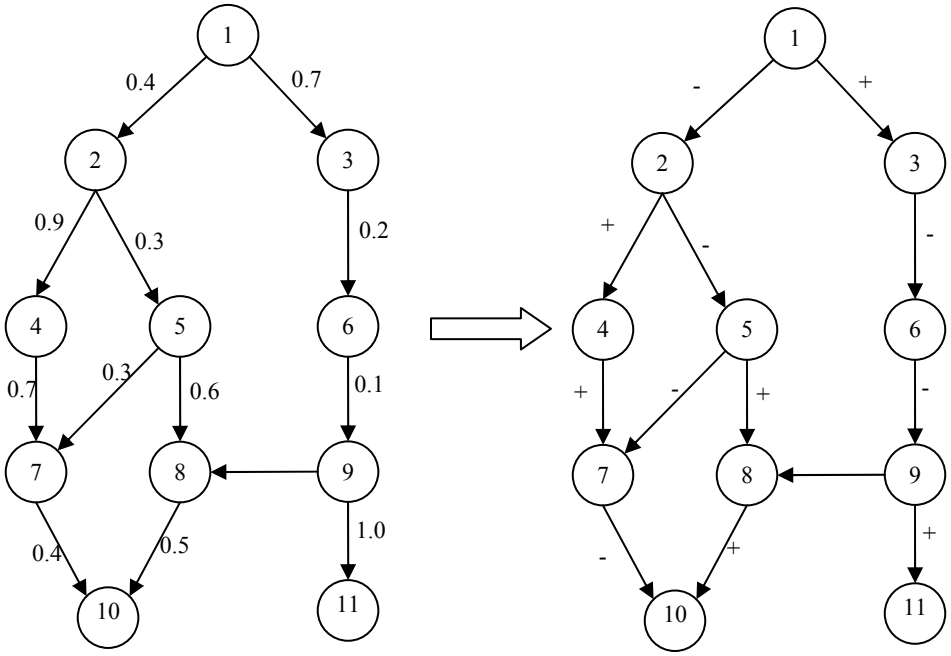
which means the local trust degree of node j from the perspective of node i. By the way, integer number represents node identification in this paper, such as integer i and j.

By the way, although we have proposed more complex trust models in [14] with multi-dimensional factors, we only need a very simple direct trust model here since the purpose of this paper is to design a new inference algorithm for indirect trust.

b. Trust relations network

The above direct trust model could easily compute direct trust value for a node, and a P2P network G=<V, E> with such direct trust degrees would be improved to be a weighted network graph as G=<V, E, W>. We call such a network "trust relations network" in this paper.

Definition 1. A *trust relations network* is a directed graph G_{Trn}=<*V*, *E*, *W*>, where *V* is the set of nodes and *E*={<*i*,*j*>|*i*→*j*} is the set of the directed relations between nodes; let $W=\{dT(i,j)\,|\,dT(i,j)\in[0,1]\wedge i\in V\wedge j\in V\wedge<i,j>\in E\}$. Figure 2(a) shows a simple trust relations network.



(a)Local trust relations network (b)Local trust inference network

Figure 2. A simple trust relations network

Sometimes, we need to focus on relations of only one node. Then, such a relations network is a sub graph of trust relations network.

Definition 2. A *local trust relations network* for a given node i $G_{LTrn}(i)$ is a sub-set of G_{Trn}, where $G_{LTrn}(i) =< V', E', W', i >$. V', E', W' in $G_{LTrn}(i)$ are subsets of V, E, W in G_{Trn} separately. $G_{LTrn}(i)$ represents a directed graph that starts with node i. As it shows, the trust relations network in Figure 2(a) is also a local trust relations network for node 1.

c. Local trust inference network

In practical networks, each node fixes a trust threshold according to its practical requirements. Using $\tau(i)$ to be personalized trust threshold of node *i*, so that node can make sure trustees are trustworthy or not. In order to infer from trust relations network for node i, we should convert the $G_{LTrn}(i)$ into a trust inference network firstly.

Definition 3. A local trust inference network for a given node i is a directed graph to represent trust or distrust relations in $G_{L-TIN}(i)$, that is $G_{L-TIN}(i) =< V', E', Opers, i >$, where $Opers(i, j) = \begin{cases} +, when\ dT(i, j) \geq \tau(i) \\ -, when\ dT(i, j) < \tau(i) \end{cases}$, and "+" means trust while "-" means distrust. Figure 2(b) is a local trust inference network converted from Figure 2(a), assuming that all nodes fix trust threshold as 0.5.

d. Trust inference rules

Balance Theory [17] is a motivational theory of attitude change, proposed by Fritz Heider in 1958. It conceptualizes the cognitive consistency motive as a drive toward psychological balance. The consistency motive is an urge to maintain one's values and beliefs over time. Heider proposed that liking relationships were balanced. As shown in Figure 3, each vertex of the triangle has a positive or negative relationship with the other two vertices. To judge the status of the triangle, we first pick up signs of the three edges (positive be 1, negative be -1), then multiply the three signs. If the result is "1", the triangle is balanced. Otherwise, the triangle is unbalanced. So, triangles with three positive signs (T3) or two negative signs (T1) tend to be balanced. On the contrary, triangles with two positive signs (T2) or three negative signs (T0) tend to be unbalanced. J. Leskovec et al found the universality of T3 and T1 in real trust networks [19].

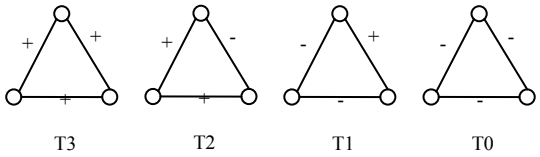
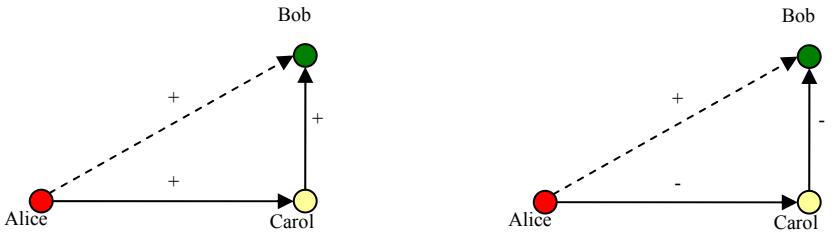


Figure 3. Balance and unbalance relations

According to balance theory, we can indicate that node A trusts node C if node A trusts node B and B trusts C. This result is consistent with case T3 in Figure 3. Another situation is that if A distrusts B, but B distrusts C, we can indicate A trusts C, which is consistent with case T1 in Figure 3. Therefore, we design two important rules for trust inference, just as shown in Figure 4.

$$Rules = \begin{Bmatrix} rule1 : A(+)B \wedge B(+)C \Rightarrow A(+)C \\ rule2 : A(-)B \wedge B(-)C \Rightarrow A(+)C \end{Bmatrix}, \quad (2)$$

where A(+)B means A trusts B and A(-)B means A distrusts B. Rule 1 is usually used to find trusted evidence chains while rule 2 is usually used to get more trusted pairs.



(a) Inference Rule 1 (b) Inference Rule 2

Figure 4. Inference rules

On the basis of the above definitions, we can define how to infer trust value from trust relations networks.

Definition 4. Let $TI(i,j) =< G_{L-TIN}(i), Rules, j >$ be inference process, which means node i can infer trust value of node j in the trust inference network $G_{L-TIN}(i)$, where i is the inference source node while j is the sink node.

Now, we should consider how to evaluate the direct trust degree of Alice to Bob when Alice infers Bob to be a trusted node according to the inference rules. However, we do not consider the situation in rule 1 since we will use probability theory to compute the trust value.

In the situation of rule 2, Alice distrusts Carol while Carol distrusts Bob. We infer that Alice could trust Bob to some extent. Thus, let

$$dT_{r2}(i,--+,j)=\tau(i), \tag{3}$$

where dT_{r2} here means node i could trust node j according to rule 2, and trust degree of node j in perspective of node i is the personalized trust threshold value $\tau(i)$ of node i.

e. Trust inference level

There may be a long distance path from source node to sink node. In order to improve inference efficiency, we design a trust inference level in our scheme.

Definition 5. Let $L(i)$ be the inference deep degree. According to the small world theory "six degrees of separation", that everyone is on average approximately six steps away, by way of introduction, from any other person on earth, so that a chain of "a friend of a friend" statements can be made, on average, to connect any two people in six steps or fewer. So, we assume $L(i)\le 7$ to help the search efficiency. Figure 5 shows the level demo.

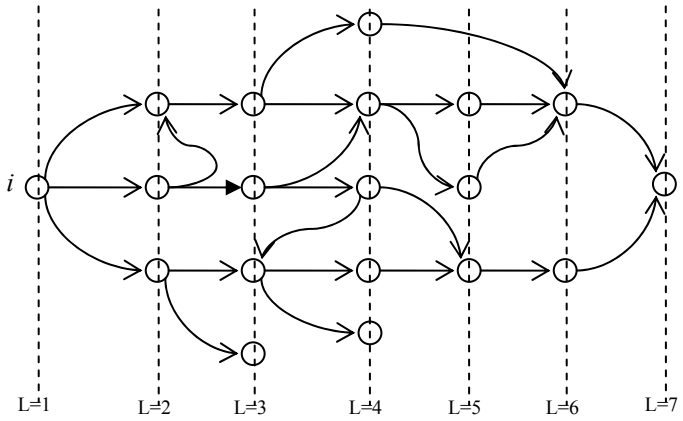


Figure 5. The hierarchy model of trust relations network

In our opinion, any connections are useful for the proposed scheme. Thus, we do not reduce any relations in the trust relations network to provide enough information for trust inference. However, different level would have different impact on the final trust degree, and deeper level should return less impact value. Therefore, we design a level factor.

Definition 6. Let $f_L(x)$ denote level factor with decreasing exponential function, that is

$$f_L(x)=1-e^{x-L(i)-1}, where \quad x\in[1,L(i)], \tag{4}$$

Figure 6 shows the level factor.

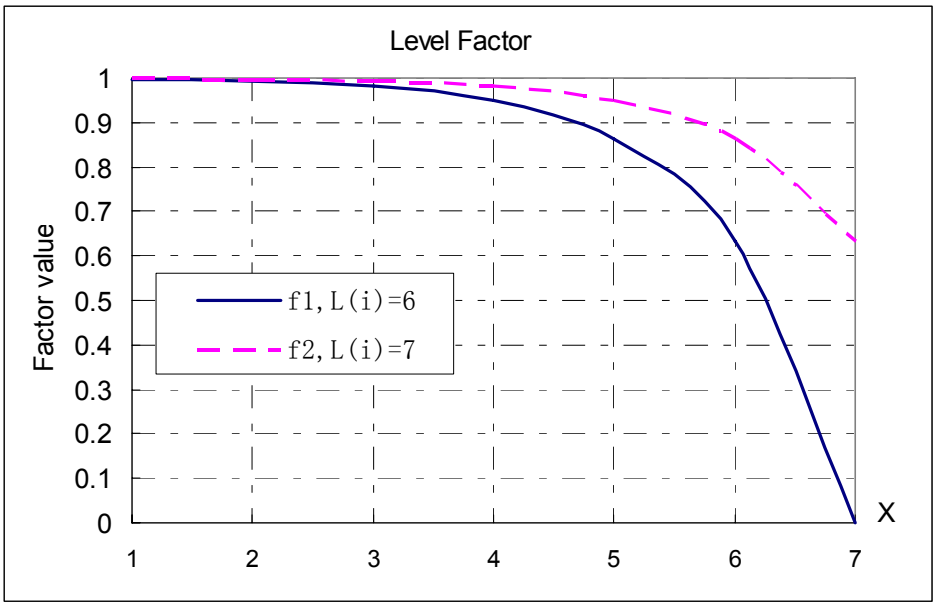


Figure 6. Level factor

Obviously, $f_L(1) > f_L(2) > \ldots > f_L(L(i))$. In addition, the factor decreases drastically when level x≥6.

f. Trusted evidence chain

A trusted evidence chain is a directed chain from source node to sink node, and any previous node trusts its succeeding node in the chain. Trusted evidence chains are basis for trust inference. Let TEC(i, j) be a trusted evidence chain from node i to node j. We design an algorithm to discover TEC (trusted evidence chain) in local trust relations network.

Algorithm 1: program *DiscoverTEC*(*i, j*)

(1)While ($L(i)$ >0)

(2) Converting $G_{LTrn}(i)$ into $G_{LTIN}(i)$ according to each node trust threshold value

(3) L(I) ←$L(i)$+1

(4)End

(5)SPath: Search *path* from node *i* to node *j* in $G_{LTIN}(i)$

(6)*IniTEC[]*← *path*

(7)Goto SPath if more paths exist

(8)For *k*←1 to length(*IniTEC*) do

(9) Convert *IniTEC*[*k*] by rules 1 and rules 2 to a new inference path.

(10) *InferTEC*[]←new inference path from *i* to *j*

(11) End for

(12) For *k*←1 to length(*InferTEC*) do

(13) if relation "+" is mapped from $G_{LTrn}(i)$ directly during path *InferTEC*[*k*] then

(14) update *InferTEC*[*k*] by mapping "+" into the origin direct trust value in $G_{LTrn}(i)$

(15) Else

(16) update *InferTEC*[*k*] by fixing "+" with direct trust value by equation (3)

(17) End if

(18) *TEC*[]←updated *InferTEC*[*k*]

(19) End for

(20) Return *TEC*[]

End.

According to Algorithm 1, we finally get trusted evidence chains with direct trust value. Figure 7 shows the mapping processes with respect to only one TEC.

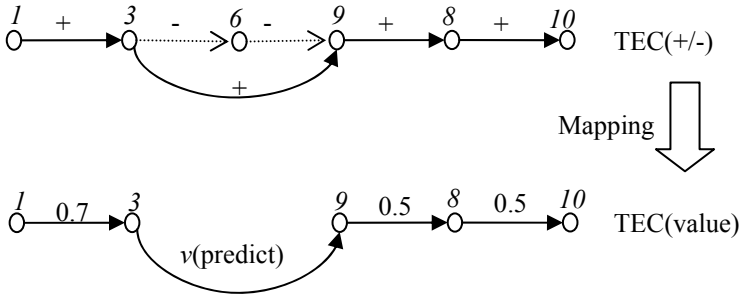


Figure 7. Demo of mapping processes of TEC

III. TRUST INFERENCE WITH PROBABILITY THEORY

a. Trust Inference for single TEC path

Markov chain describes the fact that the current state of the node is just associated with the adjacent node and the trust evidence chain (TEC) is corresponded to this Markov property. In Markov model, the transfer probability of Markov chain has k steps, denoted as $p\{X(n+k)=j \mid X(n)=i\}$, which means that the condition probability in state i to j after k-step. According to Markov model, we could calculate the TEC(i, j) by the following equation,

$$p_{TEC}(i,j) = \prod_{k=1}^{L(i)} p(i+k-1, i+k) \quad (5)$$

However, the above equation will return a very small (even to zero) value to TEC(i,j) because of too many multiplication operations, and it's not objective. Each node should have confidence with its trust evaluation, and different transfer levels should have different level factor, yet the equation (5) does not consider any of them.

Moreover, confidence is the confident level of the trust evaluation value. According to the degree of the confidence, we divide the trust level into three categories, NT(Not very Trust), GT(General Trust) and VT(Very Trust).

Assume $\alpha \in [0,1]$ is the cut-off point of NT and GT while $\beta \in [0,1]$ is the cut-off point of GT and VT. The range of the direct trust values in TEC(i, j) is

$$R_k = P_{(\max)} - P_{(\min)}, \quad (6)$$

where $P_{(\max)}$ is the maximum direct trust value among TEC(i, j), and $P_{(\min)}$ is the minimum. Then,

$$\alpha = P_{(\min)} + R_k / 3, \quad (7)$$

$$\beta = P_{(\max)} - R_k / 3. \quad (8)$$

So, $NT \in (0, \alpha], GT \in (\alpha, \beta]$ and $VT \in (\beta, 1]$.

Let C(i,j) be the confidence of direct trust evaluation from node i to node j, that is,

$$C(i,j) = \begin{cases} \dfrac{1}{1+(\alpha - dT(i,j))} \times \alpha, if\ dT(i,j) \in NT \\ \dfrac{1}{1+(\beta - dT(i,j))} \times \beta, if\ dT(i,j) \in GT \\ \dfrac{1}{1+(P_{(\max)} - dT(i,j))} \times P_{(\max)}, if\ dT(i,j) \in VT \end{cases}, \quad (9)$$

At last, we could adjust the equation (5) with the above analysis as

$$p_{TEC}(i,j) = \frac{\sum_{k=1}^{L(i)} \left(dT(i+k-1, i+k) \times f_L(k) \times C(i+k-1, i+k) \right)}{\sum_{k=1}^{L(i)} \left(dT(i+k-1, i+k) \right)}. \quad (10)$$

b. Trust Inference for multi TEC paths

We can apply equation (10) to compute a single trust evidence chain. However, how to compute TEC when multi-paths exist? Assume there are *m* paths existed between node i and j, let $P'_{TEC}(x,i,j)$ denote trust inference value for the x^{th} path from node i to j according to $P_{TEC}(i,j)$ in equation 10. So, according to total probability we can get

$$\sum_{x=1}^{m}\left(\frac{P'_{TEC}(x,i,j)}{\sum_{y=1}^{m}P'_{TEC}(y,i,j)}\right)=1. \tag{11}$$

In the equation (11), $\frac{P'_{TEC}(x,i,j)}{\sum_{y=1}^{m}P'_{TEC}(y,i,j)}$ means weight of the x^{th} path. Finally, we can obtain the trust inference (node i to node j) method to compute multi-paths TEC as

$$p(i,j)=\sum_{x=1}^{m}\left(\frac{\left(P'_{TEC}(x,i,j)\right)^2}{\sum_{y=1}^{m}P'_{TEC}(y,i,j)}\right). \tag{12}$$

We could apply equation (12) to infer trust probability while there are multi TECs.

IV. SIMULATIONS AND ANALYSIS

In order to verify the rightness of our proposed scheme, we design a simulation platform by C# programming language, and simulate the P2P environment with multi processes and threads. We improve the simulation environment based on our former simulation platform [14] and [18]. In addition, we design three kinds of nodes for simulation. (1) Class A. It denotes normal and 'good' nodes that provide correct appraisals and good services in P2P system. (2) Class B. It denotes independent malicious node in P2P system, providing mendacious service and appraisals. Nevertheless, this kind of node does not work coordination with other malicious nodes. (3) Class C. It denotes cooperative malicious nodes in P2P system, providing dishonest service and giving incorrect appraisals to other nodes except their team members. At the same time, these nodes overstate appraisals to the cooperative nodes. Simulation platform provides trust and distrust

status for each trust relationship. These three kinds of nodes can generate trust relations, and we simulate more than 1,500,000 direct trust relations for 20,000 nodes with equation (1). In simulations, we denote our proposed scheme as "Infer-Trust".

a. Capability to discover TEC

Firstly, we simulate the capability to discover TEC in our proposed scheme. In this paper, let

$$Cap(i,j) = \frac{number\ of\ TEC(i,j)}{Totoal\ \ paths\ between\ i\ and\ \ j}, \qquad (13)$$

which means the capability to discover TEC between node i and j.

In our simulations, we select node pair <i, j> at random and compute the cap(i,j) at the same time. According to the current research articles, we use three kinds of methods to infer trusted evidence chains from i to j in experiments. The first method finds paths with all trusted nodes. The second method treats distrust information as a filter which gives up any node that is evaluated to be distrust (direct trust value less than 0.5). The third one is "Infer-Trust" with inference rule 1 and rule 2. Figure 8 shows the performance to discover TEC.

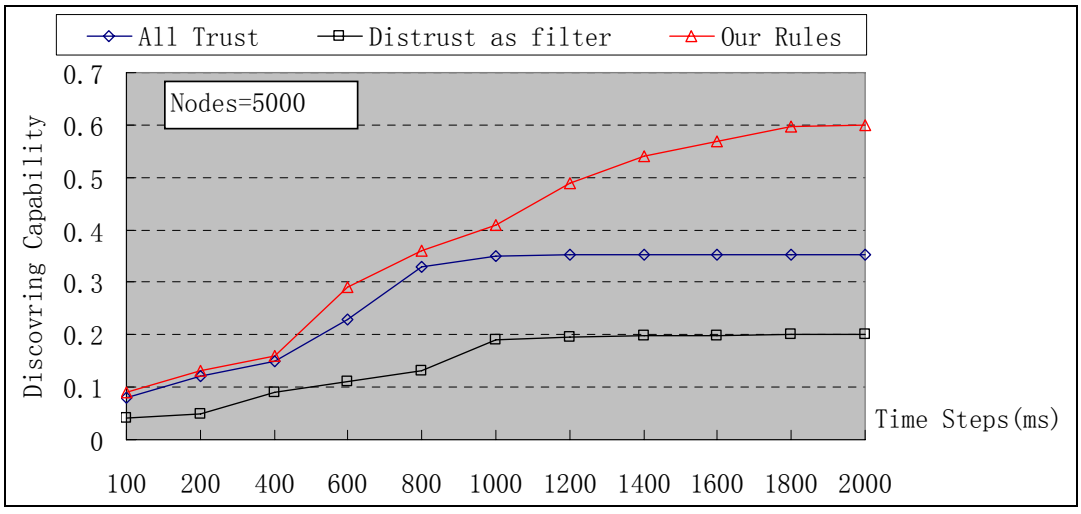


Figure 8. Capability of discovering TEC

In this experiment, three methods are under the same environment with 5000 nodes. From the above chart, we could find easily that the "Infer-Trust" has advantages in capability to discover TEC under the same environment with the time-steps go on. However, our scheme spends more time steps during the processes to finish task while the other two methods could stop within 1000 time steps. Thus, the time performance needs improving in our future work.

b. Trust Inference Performance during intensive trust relations

Simulations are made to compute the indirect trust value via three methods, that is average method in [14], multiplication method in [18] and "Infer-Trust" method in this paper, for the same <i, j> pairs.

We test the rightness of "Infer-Trust" during a simulated dataset with 70% nodes belonging to class A, to get an intensive trust relation environment. We find that the tree methods could return the relatively same results. Figure 9 shows one of the result with marked node pair <i=12, j=253>.

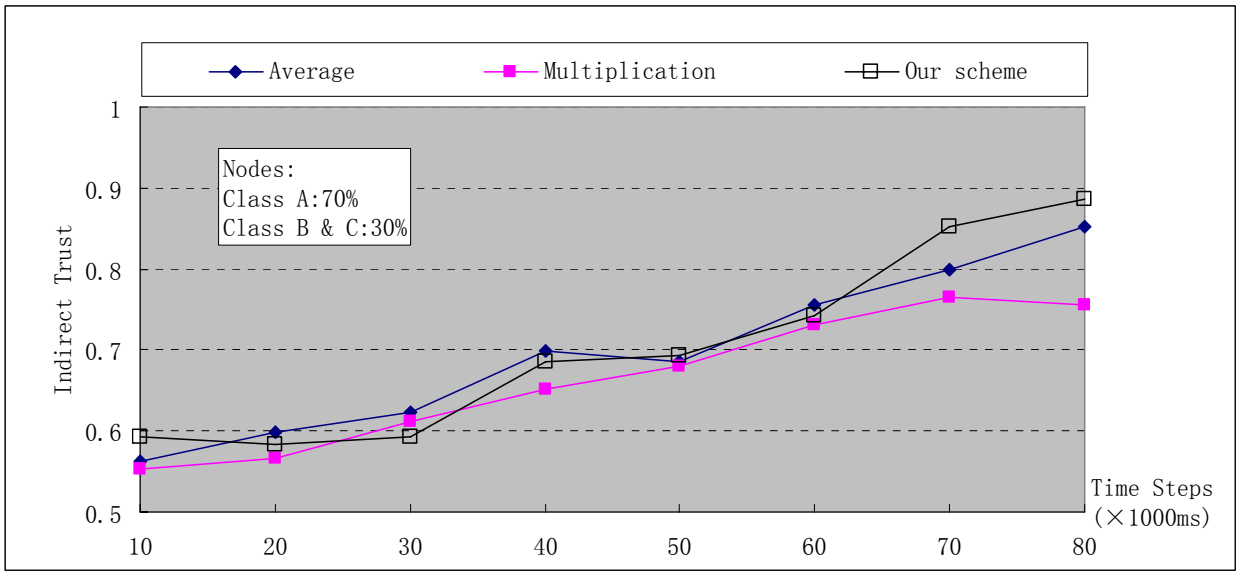


Figure 9. Performance to infer indirect trust for intensive trust relations

In our former works, we have simulated and proved that the other two methods in [14] and [18] are effective to infer trust during intensive trust environment. Now, as we can see from the above results, the "Infer-Trust" could normally infer a rational value, just as the other method. Thus, our scheme has the same capability to compute indirect trust during intensive trust relations environment.

c. Trust Inference Performance during intensive distrust relations

We simulate the intensive distrust relations environment with 40% class A nodes, 30% class B nodes and 30% class C nodes, initialized with 1000 nodes and gradually increasing by running cycles. Figure 10 shows the result.

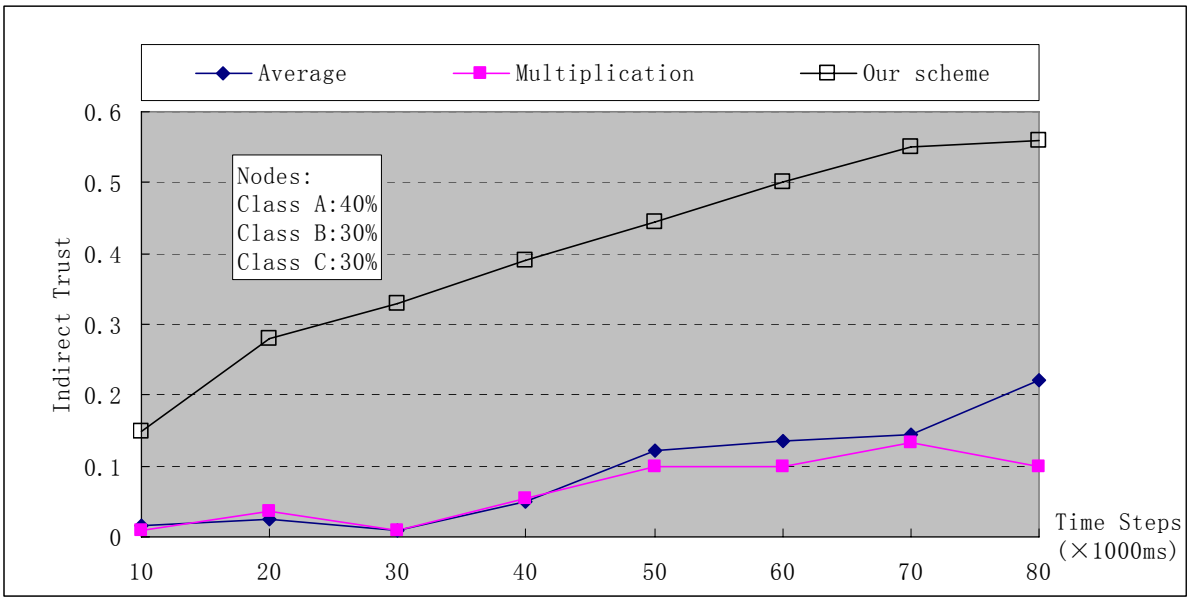


Figure 10. Performance to infer indirect trust for intensive distrust relations

The result proves that our scheme "Infer-Trust" is more efficient to infer trust during the intensive distrust relations environment. In fact, in our works [14] and [18], the other two methods prove to be invalid when trust relations are sparse.

d. Performance to resist malicious download

Assumed *TotalCount* is the total transaction times and *BC_Count* is the total transaction times with B-nodes or C-nodes, which are malicious nodes. Then, the download-resisting performance from malicious nodes is

$$dr = \frac{BC\_Count}{TotalCount}, \tag{14}$$

For example, a node of class A has 100 transactions, and 20 transactions with B-nodes or C-nodes, then the download-resisting performance is dr=20%.

We simulate the download-resisting performance for MDHTrust [14], EigenRep [7], random model and our scheme "Infer-Trust", with 60% nodes of class A, 20% nodes of class B and 20% nodes of class C. We do statistics of the download-resisting performance for these trust models. Figure 11 shows the results.

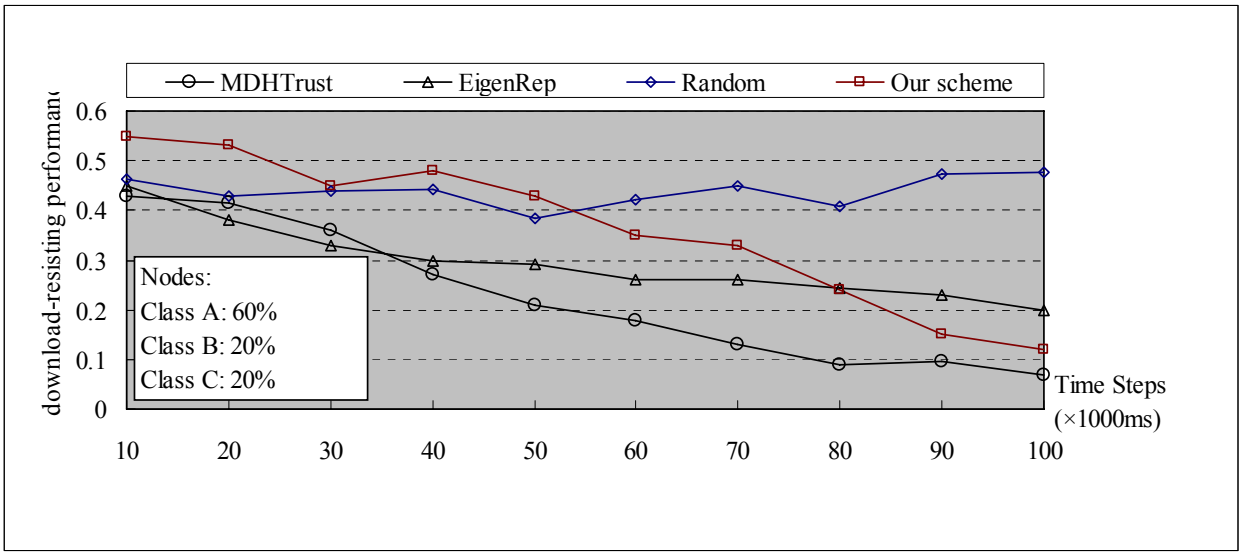


Figure 11. Performance of download-resisting

As we can see, the random model had the worst performance while our scheme had a relatively modest efficiency during resisting malicious download. That proves our scheme is effective.

V. CONCLUSIONS AND FUTURE WORKS

A main security issue in P2P networks is how to discover effective trusted relations between nodes. In our opinion, relations in a completely distributed P2P network are projections of users' behaviors. Therefore, some theory about social network could be adapted to P2P network. In this paper, we present a novel distributed trust model based on balance theory. After modeling a simple direct trust model, we construct trust relations network, trust inference network and trust inference deep level based on direct trust network. Moreover, we design two inference rules to discover trusted evidence chains in trust relations network in order to generate inference graph. At last, this paper proposes mathematics inference models to compute trusted evidence chains by Markov probability theory. We simulate the proposed scheme in distributed environment, and results prove the rightness and effectiveness both in intensive trust relations environment and intensive distrust environment.

However, it will be a long time to study the trust model for a distributed system. There are many problems need improvement, such as how to improve the time performance and how to apply it into existed models.

ACKNOWLEDGEMENT

Thank editors and anonymous reviewers for their careful and constructive suggestions to this paper. This work is supported by the Doctor Program Foundation of Education Ministry of China under Grant No. 20110042120027; China Postdoctoral Science Foundation under Grant No. 2012M511166; the Fundamental Research Funds for the Central Universities of China under Grant No. N110417006 and No. N110204003; the National Natural Science Foundation of China under Grant No. 61070162, No. 71071028 and No. 70931001; the Specialized Research Fund for the Doctoral Program of Higher Education under Grant No. 20100042110025 and No. 20110042110024; the Specialized Development Fund for the Internet of Things from the ministry of industry and information technology of China.

REFERENCES

[1] L. MEKOUAR, Y. IRAQI, and R. BOUTABA, “Peer-to-peer's most wanted: malicious peers”, Computer Networks, Vol. 50, No. 4, 2006, pp. 545-562.

[2] H. Q. Lin, Z. T. Li, and Q. F. Huang, “Multifactor hierarchical fuzzy trust evaluation on peer-to-peer networks”, Peer-to-Peer Network Applications, Vol. 4, 2011, pp. 376–390.

[3] J. Li, “mSSL: A framework for trusted and incentivized peer-to-peer data sharing between distrusted and selfish clients”, Peer-to-Peer Network Applications,Vol. 4, 2011, pp. 325–345.

[4] L. Mui, M. Mohtashemi, and A. Halberstadt, “A Computational Model of Trust and Reputation for E-Businesses”, Proc. 35th Ann. Hawaii Int’l Conf. System Sciences (HICSS ’02), , 2002, pp. 2431-2439.

[5] A. Das, M. M. Islam, “SecuredTrust: A Dynamic Trust Computation Model for Secured Communication in Multiagent Systems”, IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, Vol. 9, No. 2, 2012, pp. 261-274.

[6] K. Aberer, Z. Despotovic, “Managing trust in a peer-to-peer information system”, In proceedings of the 10th International Conference on Information and Knowledge Management, ACM Press, Atlanta, GA, United states, 2001, pp. 1-7.

[7] S. D. Kamvar, M. T. Schlosser, and H. GarciaMolina, “The EigenTrust algorithm for reputation management in P2P networks”, in proceedings of ACM WWW 2003, pp. 640-651.

[8] W. Dou, H. M. Wang, and Y. Jia, “A recommendation-based peer-2-peer trust model”, Journal of Software, Vol.15, no.4, 2004, pp. 571−583.

[9] L. Xiong, L. Liu, “PeerTrust: supporting reputation-based trust for Peer-to-Peer electronic communities”, IEEE Transactions on Knowledge and Data Engineering, Vol.16, no.7, 2004, pp. 843-857.

[10] A. Jøsang, R. Hayward, and S. Pope, “Trust network analysis with subjective logic”, In proceedings of ACSC 2006, pp. 85-94.

[11] A. Jøsang, T. Bhuiyan, “Optimal trust network analysis with subjective logic”, In proceedings of SECURWARE 2008, pp. 179-184.

[12] G. Wang, J. Wu, “Multi-dimensional evidence-based trust management with multi-trusted paths”, Future Generation Computer Systems, Vol. 27, No. 5, 2011, pp.529-538.

[13] S. X. Jiang, J. Z. Li, “A Reputation-Based Trust Mechanism for P2P E-Commerce Systems”, Journal of Software, Vol.18, No.10, 2007, pp. 2551-2563.

[14] Z. H. Tan, X. W. Wang, W. Cheng, G. R. Chang, and Z. L. Zhu, “A Distributed Trust Model for Peer-to-Peer Networks Based on Multi-Dimension-History Vector”, Chinese Journal of Computers, Vol. 33, No. 9, 2010, pp. 1725-1735.

[15] E. Damiani, S. D. C. Vimercati, and S. Paraboschi, “A reputation-based approach for choosing reliable resources in peer-to-peer networks”, the 9th ACM Conference on Computer and Communications Security, Washington, DC, 2002, pp. 207-216.

[16] Z. Despotovic, K. Aberer, “Maximum likelihood estimation of peers’ performance in P2P networks”, the 2nd Workshop on the Economics of Peer-to-Peer Systems, Cambridge, 2004, pp. 1-9.

[17] F. Heider, “The Psychology of Interpersonal Relations”, Wiley, 1958.

[18] Z. H. Tan, H. Wang, W. Cheng, and G. R. Chang, “A distributed Trust Model for P2P overlay networks based on correlativity of communication history”, Journal of Northeastern University (Natural Science), Vol. 30, No.9, 2009, pp. 1245-1248.

[19] J. Leskovec, D. Huttenlocher, and J. Kleinberg,“Signed Networks in Social Media“, 28th ACM Conference on Human Factors in Computing Systems , 2010, pp. 1361-1370.