CSCanada
Canadian Social Science
Vol. 12, No. 4, 2016, pp. 40-45
DOI:10.3968/8325

ISSN 1712-8056[Print]
ISSN 1923-6697[Online]
www.cscanada.net
www.cscanada.org

An Analysis of a New P2P Trust Control Model

WU Zhijun[a],* ; TANG Jing[a]

[a]Guangdong University of Foreign Studies, Guangzhou, China.
*Corresponding author.

Supported by Education Ministry Youth Foundation Project "Research on the Influence and Mechanism of Political Gene on the Rent-Seeking Behavior of Enterprises" (15YJC630137); Guangdong Natural Science Fund "Political Connection on the Relationship Between Managerial Discretion and Perquisite"
*Corresponding author.

Received 5 January 2016; accepted 14 March 2016
Published online 26 April 2016

Abstract
In order to monitor efficiently the selfish behavior on networks, form reliable relations and prevent problems such as the single point of failure or bottleneck effect in traditional client-server environments, we adopt a novel P2P trust arithmetic-P-Trust referring to the social people trust relation mechanism. The direct trust arithmetic and the recommend trust arithmetic are particularly described. The P-Trust integrates the direct trust value and recommend trust value to create the final trust value. Simulations prove the P-Trust arithmetic can tackle the P2P trust problem in a simple and efficient way.

Key words: IT governance; P2P networks; Trust recommend; Nodes

Wu, Z. J., & Tang, J. (2016). An Analysis of a New P2P Trust Control Model. *Canadian Social Science, 12*(4), 40-45. Available from: http://www.cscanada.net/index.php/css/article/view/8325
DOI: http://dx.doi.org/10.3968/8325

INTRODUCTION
IT governance is a combination of management, accountability system and supervision, aiming to improve a company's competitiveness and financial performance. In a P2P network, since resources sharing is a voluntary act of all nodes, it is impossible to guarantee the quality of services, which can be illustrated by frauds and selfish behaviors. If a company doesn't understand the setting of a P2P network, it is highly possible that data such as hard drive accounts and peers information got leaked without any notice. Take Genutella as an example, in a P2P network, 25% nodes provide fake documents while 10% nodes provide 87% resources of the whole network and 20% nodes supply 98% resources. And most nodes would terminate the sharing files randomly. In order to enhance governance, such selfish behaviors must be supervised and punished. Therefore, it is imperative to establish a thorough node trust mechanism to insure the quality of services. When peers visit sharing resources, services would be first provided by nodes with high trust value.

1. CURRENT TRUST MODELS
Models used in current P2P network can be divided into following types.

1.1 Trust Models Based on PKI
In these systems, there are few central nodes, whose legitimacy is guaranteed by CA certificates. Those central nodes are also in charge of determining the trust value of other nodes. In these systems, single point of failure is more likely to occur due to the dependence of central nodes, which can be demonstrated by the example of on Sale Exchange and Donkey, etc..

1.2 Trust Models Based on Local Recommend
In these systems, peers could visit limited nodes to get the trust value of target nodes, which are usually local and one-sided, through local broadcasting. This point can be implied by the example of Cornelli's improvement proposals to Gnutella.

1.3 Trust Models of Digital Signatures
This method calculates the trust value of data instead of trust values of nodes. When nodes obtain sharing date, they would judge the authenticity of those data. If

those data are approved, then they would get the digital signatures. The more signatures they get, the more trustworthy they are. However, this method can be only used on applications with sharing data and cannot prevent collective frauds. So far Kazza, a popular file sharing application, uses this kind method.

1.4 Trust Models of Global Confidence

This kind of model, which is used by EigenRep of Stanford University, would acquire the reliability of global nodes by iterating the mutual satisfaction of neighboring nodes. Nonetheless, this model does not take punishment into consideration. Meanwhile, the protocol implementation of this model does not consider the performance overhead of the network. Hence, there would be iterations in the whole network every time transaction occurs, which means this model is lack of feasibility on the engineering level.

All trust models above have their strengths and weaknesses. Under this circumstance, this paper adopts a novel trust value arithmetic, which is proved to be more simple and effective. Through observing the trust relations between people, we notice two interesting facts. First, during the establishment of trust, it is easy to build the initial trust and trust value would have a relatively rapid increase during this period. When the trust value reaches a certain level, the growth of trust would slow down. Meanwhile, compared with the rise of trust, the trust would fall faster. In other words, it is easier to lose trust than to gain. It is indeed true that the possibility of nodes that provide successful services in the first time to continue their services is much lower than the possibility of nodes that provide failure services the first time to keep their failure. Second, trust can be recommended. In a sense, trust value among individuals is determined by others recommendation. Besides, the reliability of those recommended would affect the credibility of people he recommends. In fact, this co-depended relationship forms a so called web of trust. In this web of trust, credibility of any individual is not completely reliable. But it could be used as a reference to others' interactions. Furthermore, there is a major similarity between P2P systems based on web of trust and social network.

This paper generates an unstructured P2P network through the observation of social trust relationship and tests the model via simulations. The simulation results suggest that P-Trust model could perfectly improve the services in a P2P network and effectively punish frauds.

2. THE ARITHMETIC ANALYSIS OF P-TRUST MODEL

2.1 The Core Concept of This Arithmetic

The trust value generated by P-Trust model is actually a comprehensive trust value, which contains two aspects, that is, direct trust value and recommend trust value. The direct trust value comes from the evaluation of sharing nodes' trust value. It is based on the visit history of a certain node to the sharing nodes. The recommend trust value comes from the recommendation of neighboring nodes. When calculating the comprehensive trust value, the model first computes the recommend trust value of target nodes from neighboring nodes, then takes trust value of neighboring nodes to get recommend trust value. Eventually this model combines those two types of trust value to generate final trust value.

2.2 The Definition of Direct Trust Value (T_{ij})

The direct trust value suggests the trust value of node *i* to node *j* on the basis of the visit history of node *i*. This direct trust value is also known as T_{ij}.

This paper considers the particularity of building trust, which is that it is relatively easier to gain a relatively low trust value of a stranger. However, after reaching a certain threshold, keep rising the trust would be harder. Meanwhile, trust would fall really fast. Even one mistake could cost all the trust. Thus, the authors design a special arithmetic to simulate the calculation of trust value. This arithmetic could be demonstrated by the following four points, that is, low starting value, exponential increase, twofold decrease and plus-one-per-time increase.

The first step is low starting value. The trust value of node *i* to node *j* starts with a low number, which is TS_{ij}. For each strange node, that is, the node that never been visited before, TD_{ij} equals TS_{ij}, which is 1.

The second step is an exponential increase. After the first visit of a node *i* to node *j*, the trust value would witness an exponential increase. The first time node i having a successful visit to node *j*, the trust value becomes 2. The second time is 4 while the third time comes to 8 and so forth. When the trust values reaching the threshold, it would increase 1 per time. It is indeed true because one's trust of a stranger might rapidly rise along with some successful contacts. However, when the trust gets to a certain point, it would be much harder to keep such growth.

The third step is twofold decrease. When frauds occur, trust value would decrease. After several continuous successful visit, one failed visit to node *j*, which means node *j* provides fake data, would be regarded as a fraud. The trust value would have a dramatic reduce after the fraud to half of the former value, that is, TD_{ij} equals $TD_{ij/2}$.

The forth step is plus-one-per-time increase. There are two different conditions. The first is when the trust value achieves a certain threshold, even though the number would keep rising along with successful visits, the increase ratio would fall down to 1 per time, which can be demonstrated as $TD_{ij}=TD_{ij}+1$. The second is after the reduction of trust value due to frauds, one successful visit would increase the trust value by one per time, that is, $TD_{ij}=TD_{ij}+1$.

2.3 The Definition of Recommend Trust Value (TR_{ij})

There might be some special cases when calculating the recommend trust value of node *i* to node *j*. For example, if node *i* just join a P2P network, then it would not possess any trust value about other nodes because it has not visit any of them. In this situation, node *i* owns the same trust value, which is 1, to any other node. However, the fact is that the existing network already has a relatively clear trust value of node *j*. This means that other nodes have already visited node *j*. Thus, node *i* could obtain trust value towards node *j* by consulting other neighboring nodes.

There is a certain range when computing the recommend trust value. This paper uses a tree structure to implicit the topology structure between node *i* and its neighboring nodes. The author regards node *i* as the root and neighboring nodes as intermediate nodes or leaf nodes. The distance between the leaf nodes and the root is *K*, which can also be regarded as the radius of the computing range. Using breadth first method, this paper applies random walk into the calculation of trust value. Graph 1 shows the search and calculation of recommend trust value.

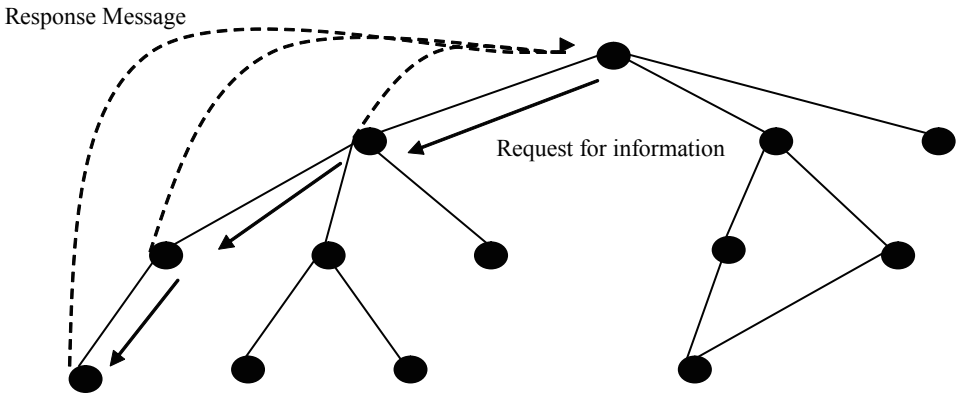

Figure 1
The Search and Calculation of Recommend Trust Value

First node *i* sends request for information to other child nodes. Those child nodes would sent node *i* the trust value of node *j* according to their own trust value of node *j*. Meanwhile, those child nodes would transmit this request to their sub-nodes. The transition contains the node that initially make the request, which is the root node. These sub-nodes would search their trust value of node *j* and send these information directly to root node *i* and so on until the search depth reaches *K*. This procedure calculates a local recommend trust value because searching the recommend trust value of the whole network would cost a lot. Besides, the trust value between nodes could be illustrated by limited local trust values.

After getting the trust value of node *j* from intermediate nodes or leaf nodes, node i would compute the trust value of node *j* according to Formula (1). The arithmetic regards that trust values from each neighboring nodes own the same value and computes the arithmetic mean.

$$TR_{ij}=(TD_{kj}+TD_{mj}+TD_{nj}+\ldots+TD_{pj})/N. \quad (1)$$

Among the formula, TD_{xj} represents the direct trust value of node *x* to node *j*, generated by the arithmetic in 2.3.

Along with the increasing number of visits to other nodes, node *i* would gradually build the direct trust values towards other nodes on the basis of the visit results. Furthermore, node i could determine which node is reliable and which is not based on those trust values. At this time, node *i* would not treat all the other neighboring nodes equally. Those nodes with higher direct trust values would get higher recommend trust values. On the other hand, those nodes that are not so reliable would have relatively lower recommend trust values. This phenomenon is consistent with real life, where one would trust a person recommended by a reliable friend more than the one recommended by a less trustable one. Thus, there would be a new formula to compute the recommend trust value.

$$TD_i=TD_{ik}+TD_{im}+TD_{in}+\ldots+TD_{ip},$$

$$TR_{ij} = \frac{TD_{ik}}{TD_i}TD_{kj} + \frac{TD_{im}}{TD_i}TD_{mj} + \frac{TD_{in}}{TD_i}TD_{nj} + \cdots + \frac{TD_{ip}}{TD_i}TD_{pj}. \quad (2)$$

Among the formula, TD_i represents the sum of direct trust value of node *i* to other intermediate nodes and leaf nodes. In Formula (2), the weight of different nodes could be illustrated by the ratio of different direct trust values on the total values.

2.4 The Definition of the Comprehensive Trust Value (T_{ij})

The trust value of node *i* to node *j* is eventually determined by the following two kinds of trust value. The first one is trust values generated by the interaction between node *i* and node *j*, which is TD_{ij}. The second one is the recommend trust values from neighboring nodes

using random walks with K as the radius, which is TR_{ij}. The value of these two could be computed by Formulas (1) and (2) respectively. This paper combines TD_{ij} and TR_{ij} by using linear technique and gets the final trust value of node i towards node j. The formula is as follows:

$$T_{ij}=aTD_{ij}+(1-a)TR_{ij}(0\leq a\geq 1). \quad (3)$$

The number a MERGEFORMAT is a constant and suppose to balance the direct trust value and the recommend value. This number also determines the weight of those two types of trust values in the final trust value and suggests how much does a peer believe the assessment of the trust value. If a peer trust the appraise more, then a should be relatively higher, vice versa. Meanwhile, a should be lower when node i just joins a P2P network because trust values of node i towards other nodes are completely determined by the recommend trust values from its neighboring nodes. After joining a P2P network for a while, a should be higher since node i already get acquainted with the network.

3. SOME KEY ISSUES IN THE MODEL

3.1 The Setting of the Initial Direct Trust Value of Node *I* Towards Node *J*

The initial direct trust value TS_{ij} should be reasonable. Because if it is too high, then it is not consistent with reality since the trust towards strangers would not be that high. If it is too small then the growth of trust value would be too slow. The value of TS_{ij} in this paper is 1.

3.2 The Threshold of Direct Trust Value

The setting of threshold should obey the following rules. First, threshold should not be too high. If it is too high, then the rise of direct trust value would be too fast. Second, threshold cannot be too low because that would lead to the limitation of the growth of direct trust value.

3.3 The Punishment of Frauds

In this paper, the trust value of nodes that provide fake information would reduce half of their former value. Considering the trust value would only increase 1 for each successful visit, this method would effectively punish nodes with frauds.

3.4 The Value of *K*

This paper uses random walks with K as the radius when searching recommendd trust value. In P2P networks, the value of K is decided by the scale of the whole network. The value of K would be higher if there is a larger network, vice versa.

3.5 The Value of *a*

The constant a is supposed to balance the weight of direct trust value and recommend trust value. Thus, the reality of those two kinds of trust values and peers' preference should be considered when determining the value of a.

3.6 The Issues About Service Hotspot

In this trust model, the author randomly selects a node in the range of [maxT_{ij}, maxT_{ij}/2] as the service node to balance the workload. The graph below shows the random picking.

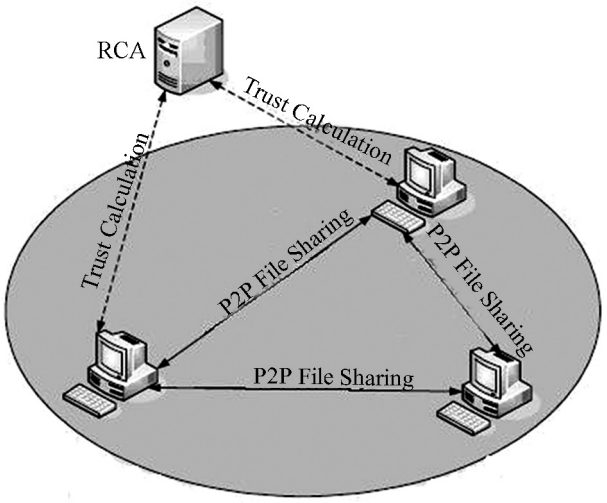

Figure 2
Random Picking of Service Node

4. SIMULATION EXPERIMENTS AND RESULTS ANALYSIS

There are two main targets of simulation experiments in this paper. The first one is the pattern of visiting rate and rate of successful visits to cheating nodes, which are nodes that provide fake information. The simulation experiments tests whether the system could effectively punish the cheating nodes and raise the rate of successful visits rapidly. The second is about service hotspots. This paper compares the arithmetic that selects the node with the highest trust value with the method of service hotspots which simulates the arithmetic above, analyzing whether the arithmetic achieves load balancing.

4.1 Rate of Successful Visits

The simulation experiments provide files to download. There are 1,000 nodes in the simulated networks, sharing 10,000 documents, which are randomly distributed to real nodes. A node would own as well as share a document after downloading it. Under this circumstance, the copy of real sharing files would gradually increase. If the document is fake, the node would delete it and search and download new documents again after evaluating the trust values.

This experiment simulates the situation where fake nodes take up half of nodes and tests the trend of the rate of fraud visits and the pattern of the rate of successful visits. In the experiment, the author uses both P-Trust arithmetic and regular arithmetic to simulate the downloading of documents and compares the results. The experiment downloads 1,000 files overall and assume that threshold equals 16, K equals 3 and a equals 0.5.

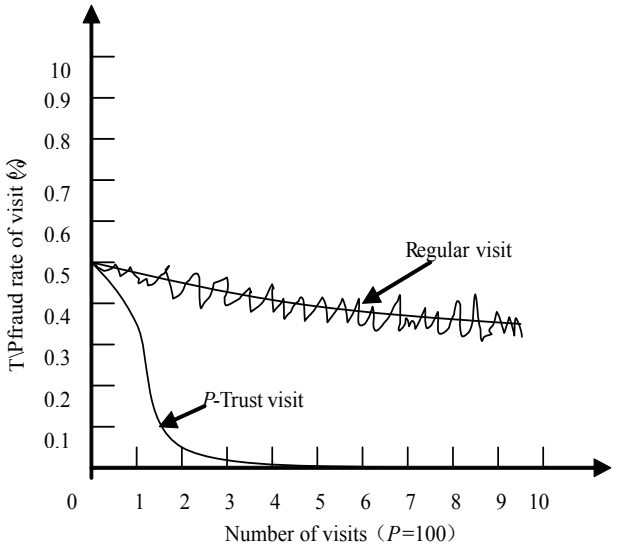

Figure 3
Fraud Rate of Visits

This paper assume that the number of all visits is *a* and the number of visits that have documents is *b*, among which the number of fraud is *c* and the number of successful visits is *d*. Therefore, the rate of fraud AC equals *c*/*b*, the rate of successful visits AS equals *d*/*a*. Graph 3 shows the pattern of the rate of fraud, while graph 4 suggests the law of the rate of successful visits. Those smooth curves are the results of smooth processing of real curves.

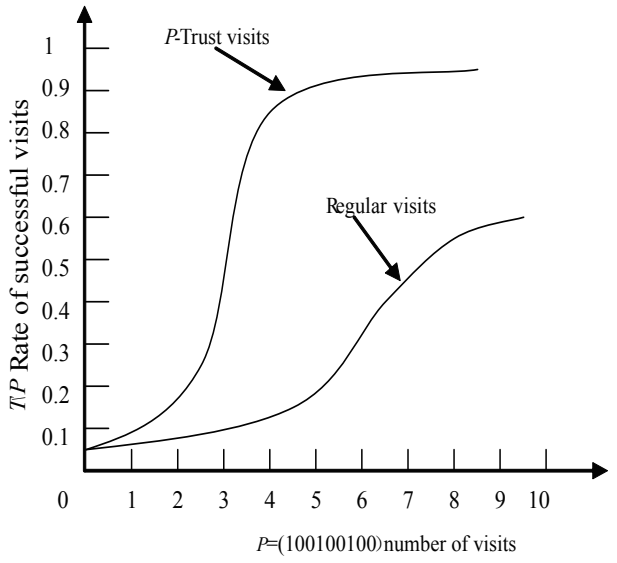

Figure 4
Rate of Successful Visits

The experiment finds that the rate of fraud reduces really fast under the *P*-Trust arithmetic. That means there would soon be no cheating nodes because the trust value of cheating nodes decreases really fast while the trust value of successful nodes has a rapid growth. Whereas, rate of fraud would not have a noticeable reduction owing to the same trust value of all nodes using regular arithmetic. As for the rate of successful visits, the results of *P*-Trust arithmetic witnessed a fast rise and reaches 1 at last. Meanwhile, the rate would grow slowly through regular arithmetic.

4.2 Service Hotspots

This paper simulates the arithmetic that select the node with the highest trust value with the *P*-Trust arithmetic of service hotspots, testing the performance of *P*-Trust arithmetic. To simplify the experiment, this paper selects 10 nodes and shares 1 document with these 10 nodes, which are all real. Each node would download the file for 100 times.

Figure 5 implies the test results, which are that the *P*-Trust arithmetic could effectively eliminate problems of service hotspots and achieve load balancing.

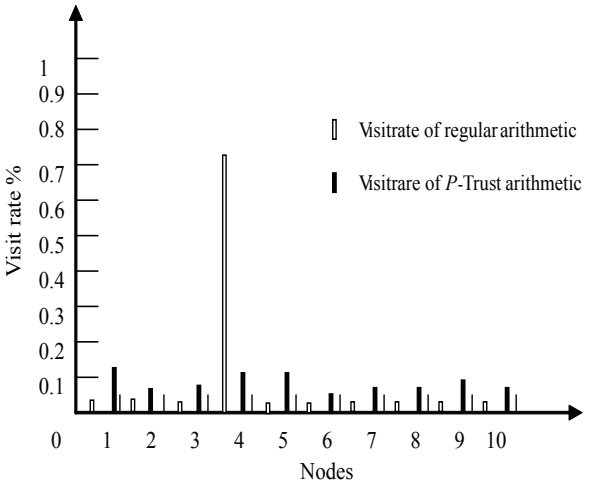

Figure 5
Visit Rate of Regular Arithmetic and *P*-Trust Arithmetic

5. FURTHER RESEARCH

In P2P networks, the application of *P*-Trust arithmetic could dramatically raise the rate of successful visits, punish cheating nodes and balance system's workload. However, current models only consider two types of situations when visiting sharing resources, which success and failure. The fact is that in P2P networks, there are many sharing resources that partially meet the visiting request. Thus, the further research would be easing restricted conditions and combining semantic analysis so that the system would fit the requests of real P2P networks better.

CONCLUSION

a) This paper adopts the *P*-Trust arithmetic, which is generated on the basis of observation of social relationship.

b) The trust value computed by *P*-Trust arithmetic is actually a comprehensive trust value, which contains two aspects: Direct trust value and recommend trust value.

c) As for the rate of successful visits, the results of *P*-Trust arithmetic witnessed a fast rise and reaches 1 at last. Meanwhile, the rate would grow slowly through regular arithmetic. Furthermore, *P*-Trust arithmetic could effectively eliminate problems of service hotspots and achieve load balancing.

REFERENCES

Abdul-Rahman, A., & Hailes, S. (1997). *A distributed trust model* (pp.48-60). Proceedings of the 1997 New Security Paradigms Workshop, USA: ACM Press.

Caronni, G. (2000). *Walking the Web of trust* (pp.153-159). Proceedings of the IEEE 9th International Workshops on Enabling Technologis. Infrastructures for Collaborative Enterprises IEEE Press.

Cornelli, F., Damiani, E. S., & De Capitani di Vimercati, et al. (2002). *Choosing reputable servents in a P2P net work* (pp.376-386). Proceedings of the 11th International World Wide Web Conference. USA: ACM Press.

Dou, W., Wang, H. M., & Jia, Y., et al. (2004). A recommendation based peer-to-peer trust model. *Journal of Software, 15*(4), 571-583.

Fabrizo, C., Ernesto, D., & De Capitani Di Vinercati, S., et al. (2002). Choosing reputable servents in a P2P network (pp.376-386). Proceedings of the 11th International World Wide Web Conference Hawaii ACM Press.

Kamvar, S. D., Schlosser, M. T. (2003). *EigenRep: Reputation management in P2P net works* (pp.123-134). Proceedings of the 12th Int' l World Wide Web Conference. USA: ACM Press.

Khambattim, Dasg Upt A P, Ryu Kd. (2004). A role—based trust model for peer to peer communities and dynamiccoalitions Second IEEE International Information As 2 Surance Workshop, Charlotte, NC.

Khare, R., & Rifkin, A. (1997). Weaving a Web of trust. *World Wide Web, 2*(3), 77-112.

Oram, A. (2001). *Peer to peer: Harnessing the power of disruptive technologies* (pp.135-154). New York: O'Reilly & Associates.

Seluck, A., Uzun, E., & Par Ientem, R. (2004). *A reputation 2 based trust management system for P2P net works*. Proceedings of 4th IEEE /ACM International Symposium on Cluster Computing and the Grid. Chicago: Illinois: 2512258.