# One improved P2P electronic commerce trust model

**Xue Zhao**

*International Education College, Nanyang Institute of Technology, Nanyang, 473004, China*

*Corresponding author's e-mail: 89061028@qq.com*

*Received 01 March 2013, www.cmnt.lv*

**Abstract**

To effectively solve the security problem in P2P electronic commerce trading, this paper analyses the existing trust model and proposes an improved trust model. The trading sum, trading evaluation, trading time and trading time are introduced into the direct trust computing to prevent against malicious cheat of nodes. The punishment factor suppresses the cheat behaviour of nodes and effectively prevents the malicious nodes from cheating at certain frequently. When recommendations from other nodes are combined, the weighted averaging method and trust of the recommendation nodes are used to effectively prevent malicious nodes from providing malicious recommendation. The simulation experiment indicates that this mode can effectively beat the malicious nodes, protect the honest nodes, enhance security of the P2P electronic commerce nodes, and reduce the trading risks.

*Keywords:* electronic commerce, trust model, trust evaluation, network security

## 1 Introduction

P2P (peer-to-peer) [1] technology can provide direct communication, resource sharing or collaborative work between nodes in the network and have low computing cost. The trading information between companies or traders is directly transmitted in a peer-to-peer manner in the electronic commerce model based on P2P network, which simplifies the trading flow and reduces the trading cost. Both trading parties do not know each other due to high anonymity and flexibility of P2P network, so it is highly risky.

Research on security of P2P technology is popular all the time and the trust mechanism is important to secure P2P network. The trust model is an advanced component in the trust mechanism, can restrict behaviours in the network to some extent, and reduce security risk, so it can improve availability of P2P network and make P2P network further evolve better. This paper proposes to compute the trust value of a node according to the past trading history information of this node and provide a reliable trust mode based on this value. This method can improve success rate of trading much and effectively solve weaknesses in the existing model.

## 2 Trust and trust evaluation

Trust [2] indicates to evaluate identify and behaviour confidence of an entity and is related to reliability, credit and performance of this entity. It is a subjective concept and depends on experiences. Generally the trust value is used to represent trust level. The trust will dynamically change with behaviours of an entity. Trust is a bilateral relation and is respectively called as the trust subject and trust object. Generally the buyer is thought as a party which is susceptible to harm in the electronic commerce and is the trust subject. The seller is a trust object and has an opportunity to utilize the weaknesses of the trust subject.

The trust value is the quantitative representation of the trust degree of an entity to another entity. Generally the trust degree is represented as a real number interval, so the probability theory is used to establish a trust model. The trust will continuously change with time and entity behaviours. The trust value will change with behaviours of this entity and evaluation of other entities to this entity. The quality of the service provided by this entity in the network can be quantified by establishing a trust model, so reliability of the service provided by this entity in future can be predicted based on the computed trust degree.

Trust to a person or an entity in a realistic society is from direct intercourse experiences in the past or recommendation from others. This case is similar in the network. Trust between entities can be divided into direct trust and recommended trust (or indirect rust).

Definition 1: the direct trust is a direct mutual experience of two entities which directly trade with each other in the past based on trading information.

Definition 2: the recommended trust is established via recommendation from other entities when two entities have no direct trading experiences with each other or have few experiences. The recommended trust is from the evaluation results of other entities and is obtained via central computing, reliable third-party computing or independent computing of disperse entities. The nodes with direct trust relation are very limited in P2P distributed network, so the recommended trust is very important for driving of EC.

## 3 Trust mode

For the trust model proposed in this paper, before the node a gets the trading application from the node b or is ready to interact with the node in whole trading flow, it will first find the local history records to get direct trust value based on the direct intercourse with the node b. Based on this value, the node a checks if trading is performed. If no trading history is available and the trading time of the node b is 0, it indicates that the node b is a new node. The node a should leverage advantages and disadvantages to determine trading.

If no trading experiences are available and the trading time of the node b is 0, the node a will send the query request to the related nodes. The nodes receiving the requests will return the local related history records to the node a. The node a will compute the recommended trust of the node b according to the collected information on the node b and determines to trade with the node or not. If the node a agrees to trade with the node b, the trading will start. After trading ends, both nodes will submit mutual evaluation and update their total trading time and successful trading time according to the evaluation of both parties.

## 3.1 DIRECT TRUST

### *3.1.1 Initial trust*

When a node b joins in an EC system for the first time and has no trading experiences. When it requests to trade with other node a, the node a will check the trading history. If no trading history is available, it will have no direct trust. The node a will send the request to other nodes and can not get response from any node, so the new node has no trading opportunity and affects normal operation of the EC. a reasonable initial trust is very important for security of EC system.

Definition 3: the triad (T(a,b), N(b), Ns(b)) is used to indicate the direct trust.

T(a,b) indicates the direct trust of the node a to the node b, N(b) indicates total trading time of the node b and Ns(b) indicates successful trading time. Total trading time N(b) and successful trading time Ns(b) are stored together with other attributes of the node b. when the node b and a send the requests, it can get two values. The trading time of new node is 0, successful trading time is 0, and T(a,b) is 0. Although the node a gets T(a,b) with the value 0, but it knows that T(a,b) is 0 by checking N(b)=0, which is caused because the node b is a new node and is not caused due to the worse prestige of the node b.

To prevent any node from not trusting the new node and lead to “discrimination” of no trading, the incentive measures are taken in this model. if the node a trades with the new node b, regardless of evaluation of node b to the node a, the node a will be escalated to higher level. if the evaluation is the top level “best”, the successful trading time of the node a will increase by one time.

### *3.1.2 Trust parameters*

The direct trust [3] is the evaluation of both trading parties to peer based on their direct trading experiences. Based on subjectivity, non-symmetry and dynamics of trust, the following parameters are introduced in direct trust computing.

1) History trading time.

Definition 4: N(a,b) indicates the history trading time of the node a and b, N(a) indicates total trading time of the node a and Ns(a) indicates the successful trading time of the node a.

2) Trading sum.

Amount (simplified as A) indicates the trading sum. This model assumes that the history trading evaluation approaching to this trading sum has the biggest influence on this trading. If Anew indicates this trading sum and Aold indicates the history trading sum, smaller |Anew-Aold| indicates that this history trading has bigger influence on this trading. To avoid the case of multiple history trading sums have similar influences on this trading, the trading sum is classified. The trading sum influence at each level is regarded to have same influence effect. The trading sum is divided into the following 10 levels:

(1) Level 0: [0,15)
(2) Level 1: [15,50)
(3) Level 2: [50,100)
(5) Level 3: [100,500)
(5) Level 4: [500,1000)
(6) Level 5: [1000,4000)
(7) Level 6: [4000,10000)
(8) Level 7: [10000,40000)
(9) Level 8: [4000,200000)
(10) Level 10: [200000, ∞)

CAmount indicates the level of a sum. The influence of a history trading on the new trading can be identified according to CAnew-CAold from the view of the trading scale. If CAnew-CAold=Δ, the influence factor of history trading with different trading sum levels can be marked as C(Δ).

Definition 5:

$$C(\Delta)=\begin{cases} 1 & \Delta=0 \\ \left(\dfrac{2.9}{e+e^{-1}}\right)^{\Delta^2} & 0<\Delta<9 \\ \left(\dfrac{2.9}{e+e^{-1}}\right)^{\Delta^2} * 0.15+0.85 & -9<\Delta<0 \end{cases}$$

and $\Delta$ is an integer

When -9<Δ<0, $\left(\dfrac{2.9}{e+e^{-1}}\right)^{\Delta^2}$ ×0.15+0.85, so it can control C(Δ) to be within (0.85, 1) to improve the influence factor of the big sum history trading and weaken the influence of failed big trading on the results.

3) Trading evaluation

Trading evaluation [4] is a subjective parameter and reflects satisfactions of one trading party to different aspects of the trading behaviours of another party. The trading evaluation is divided into five levels in this trust model. The initial values of five levels are 0(or -1), 0.25(or -0.5), 0.5, 0.75 and 1. If a common trading is evaluated as “worse”, the value is 0. If the trading has a big sum and the evaluation is “worse”, the value is -1. The value for “bad” evaluation is same. it aims to increase the influence of the big sum trading.

The trading with trading sum over a is defined as the big sum trading and other trading are common trading. The value of a will differ with the trading market to solve the weakness in the trading history.

Definition 6: the trading evaluation of different node i to the node b for the commodity j is Sj(i,b).

Definition 7: if the trading time Nj(i) of the node b for the commodity j is more than 5, then:

$\frac{\sum_{i=1}^{N_j(i)} S_j(i,b)}{N_j(i)}$ indicates the mean trading evaluation.

Definition 8: if $\left| Sj(a,b) - \frac{\sum_{i=1}^{Nj(i)} Sj(i,b)}{Nj(I)} \right|$ <=0.25, S(a,b)=Sj(a,b).

Otherwise, S(a,b)= Sj(a,b) ± 0.25.

When $S_j(a,b) > \frac{\sum_{i=1}^{N_j(i)} S_j(i,b)}{N_j(i)}$ , S(a,b)= Sj(a,b) -0.25

Otherwise, S(a,b)= Sj(a,b) + 0.25.

When S(a,b)=Sj(a,b), it indicates that the evaluation of the node a to the node b is honesty and trustable. Otherwise, it indicates that the evaluation of the node a is not honesty and the node a gives malicious evaluation to the node b. To punish the malicious node a, the successful trading time of the node a decreases by 1 and the initial evaluation of the node a to the node b increases or decreases by 0.25 to protect the honesty node b.

4) Trading time.

The trading time [5] reflects the elapsed time of the trading from current time. With time elapse, the trading individuals will continuously change. The trust relation between two nodes is continuously changing, which indicates dynamics of the trust, so the recent trading behaviours will have higher reference value on this trading, namely more recent the trading behaviour is, bigger its trading time factor is and bigger the influence on the trust value is.

Definition 9: Tnew indicates the date of this trading, Told indicates the date of history trading, and Δt=Tnew-Told indicates interval days between history trading and this trading.

Definition 10: C(Δt) indicates the time action factor.

$$C(\Delta t) = \begin{cases} 1 - \left( \frac{\Delta t}{366} \right)^2 & \Delta t \le 365 \\ 0.0001 & \Delta t > 365 \end{cases}$$

If one year has 365 days, when the interval between the history trading and this trading is over 1 year, we think that the influence of history trading on this trading is very small and C(Δt)=0.0001.

5) Failure acceleration factor

To make reputation value of the node with failed trading quickly decrease, we introduce the failure acceleration factor. One the node fails in trading, the decreasing speed of the reputation is far higher than its increasing speed, so the loss the malicious behaviours such as cheat will overweight the gain. It will punish the malicious nodes much and warn other nodes.

Definition 11: the acceleration factor is $\frac{1}{1+e^{N-Ns}}$.

N indicates the total trading time of the nodes and Ns indicates the successful trading time of the node.

6) Computing method of direct trust

Definition 12: before the node a performs a new trading with the node, the direct trust value of the node a to the node b is:

$$T(a,b) = \frac{\sum_{i=1}^{N(a,b)} C(\Delta) * S(a,b) * C(\Delta t)}{N(a,b)} - \frac{1}{1+e^{(N-N_s)}}$$

Definition 13: The direct trust is:

$\left( \frac{\sum_{i=1}^{N(a,b)} C(\Delta) * S(a,b) * C(\Delta t)}{N(a,b)} - \frac{1}{1+e^{(N-N_s)}} \right.$, N(b), Ns(b))

## 3.2 RECOMMENDED TRUST

If two entities have no trading with each other, recommendation from other entities is required. Based on their recommended values, we can get a recommended trust value and check if this trading is performed according to the recommended trust value. The recommended trust is obtained from direct trust of other nodes and nodes to trade.

Definition 14: The number of the nodes participating in the recommendation of the node a is I(b).

Definition 15: Direct trust value of the node x to the node b:

$$T(x,b) = \frac{\sum_{i=1}^{N(x,b)} C(\Delta) * S(x,b) * C(\Delta t)}{N(x,b)} - \frac{1}{1+e^{N-N_s}}$$

Definition 16: trust of the node x is

$$D(x) = \frac{Ns(x)}{N(x)}$$

when D(x)<0.8, the recommendation of this node is ignored.

Ns(x) indicates the successful trading time of the node x. N (x) is total trading time of the node x. For recommendation of other nodes, the trust of this recommended node should be also considered to reduce influence of malicious behaviours of some nodes.

Definition 17: Computing method of recommended trust

$$T_b = \frac{\sum_{1}^{I(b)} T(x,b) * D(x)}{I(b)}$$

## 3.3 WEIGHT SELECTION IN TRUST MODEL.

To ensure that the value of the reputation value is always within [0,1], the definition of this model involves several weight parameters:

1) The weights 2.9, 0.85 and 0.15 are used in the definition 5. If the weight is 3, the decreasing speed is too low and the effect is not significant. If the weight is 2.8, the deceleration speed is too quick and the gap is too high, so the weight 2.9 is selected.

For Δ<0, the weight 0.85 and 0.15 are used to increase the influence of the history trading which trading sum is bigger than it of the new trading, so the weight will not decrease to a very small value with decrease of Δ. The weight 0.8 and 0.2 or other values can be used.

2) The weight 5 trading and the weight 0.25 are used in the definition 6, 7 and 8.

The quality of same commodities provided by the seller should be rough same in practice, even if the service and goods transportation have some small problems, it will not lead to big differences between the initial evaluation of the buyers. Based on this condition, we check if the new evaluation is fair.

The trading of one commodity less than 5 times is directly evaluated by the node and is not assessed. The evaluation of the trading of one commodity more than 5 times should be compared with the history mean evaluation to determine if averaging is honesty.

## 4 Analysis on trust model

This trust model proposed in this paper facilitates isolation of malicious nodes, can inspire nodes to provide better service quality and get higher reputation. This model can make users prefer to trading with the nodes with better reputation, so it can suppress the behaviours of the nodes with the worse reputation. The non-honesty recommended nodes will be assigned with the less recommended weights, so the given recommendation has smaller influences on the collaborative decision of the nodes. This mechanism can effectively identity and suppress collaborative cheating and slandering between nodes, and can ensure that the model effectively processes the reputation of the nodes. The nodes in the network can communicate the direct experience evaluation on the target nodes via computing of the indirect trust value in the trust model in order to mark the malicious nodes via the reputation. The nodes with higher regulation have more opportunities to get trading. The trust value should be computed as accurately and practicably as possible. The strict punishment and reward mechanism is introduced to computing of the direct trust in this model, so growth of the trust value will first increase slowly and decrease quickly and resist malicious attacks.

## 5 Test of trust model

This paper simulates a P2P EC community [6], tests the performance of the trust model, checks if the trust model can effectively suppress bad behaviours, punishes behaviours of the malicious nodes, protects the honesty good nodes, and suppresses the malicious trading behaviours and malicious evaluation behaviours.

Assuming that the node b sends the trading request to the node a, the node a searches local trading records and does not find the trading history with the node b, so it requests recommendation to other nodes. it is possible that the malicious nodes can increase the reputation of the partners in recommendation and make it get the trust for trading, or some nodes purposefully slander the node b. E.g. if all nodes are kindly nodes, they recommend and compute the indirect trust value of the target node to get the value 0.4, but some malicious nodes exist in voting in practice, these nodes purposefully improve or reduce the reputation of the target nodes to appraise or slander the target node. When the indirect trust is computed in this model, recommendation value of each node is weighted for averaging. Weights indicate the trust of the node, so the recommendations of not all nodes are regarded equally. They are distinguished. The nodes providing correct recommendation can get more trust, so it can better prevent this attacking mode.

The number of the nodes participating in the recommendation is 10 in this experiment. The number of the malicious nodes is 2, namely node c1 and c2. Their malicious behaviours mainly indicate to provide malicious recommendations. The trust of the node c1 is less than 0.8, so the recommendation of the malicious node c1 is not adopted. The experimental results are shown as the Table 1.

TABLE 1 Trust model test

| | **c1** | **c2** | **c3** | **c4** | **c5** | **c6** | **c7** | **c8** | **c9** | **c10** |
|---|---|---|---|---|---|---|---|---|---|---|
| Recommended value | 0.1 | 0.2 | 0.8 | 0.78 | 0.81 | 0.815 | 0.79 | 0.80 | 0.84 | 0.82 |
| Recommended trust value | | | | | 0.6755 | | | | | |
| Confidence | Not adopted | 0.8 | 1 | 1 | 1 | 1 | 1 | 1 | 0.9 | 1 |
| Recommended trust with confidence | | | | | 0.726 | | | | | |

The recommendations from other nodes are computed by using the weighted averaging method in our model. The confidence of the recommended node is added to effectively prevent the malicious nodes from providing malicious recommendations.

## 6 Conclusions

Based on analysis on the existing trust model, an improved trust model is proposed. The simulation experiment indicates that this model adds the failure factor in computing of direct trust. Once the failure trust value decreases quickly, the successful trading time and failed trading time are not only simply summed in computing of the trust value. Other influence factor is introduced to effectively prevent the malicious nodes from cheating without loss of trust value at certain frequency. The reward mechanism is added in computing of the direct trust value. If a node trades with the new nodes, additional evaluation value is added. This trust model makes EC in P2P network more flexible, secure, stable and robust.

## References

[1] Song S, Hwang K, Zhou R F 2005 Trusted P2P Transactions with Fuzzy Reputation Aggregation *IEEE Internet computing* **9**(6) 24-34

[2] Zhang G, Kang J 2006 A New Kind of Subjective Trust Model *Wuhan University Journal of Natural Sciences* **14**(6) 1457-61

[3] Abdul-Rahman A 2004 A Framework for Decentralised Trust Reasoning *PhD thesis, University of London*

[4] Lorenz E H 1988 Neither Friends nor Strangers: Informal Networks of Subcontracting in French Industry *in Diego Gambetta editor Trust Basil Blackwell* 98-103

[5] Abdul-Rahman A, Hailes S 1997 Using Recommendations for Managing Trust in Distributed Systems *Proceedings of IEEE Malaysia International Conference on Communication '97 (MICC'97) Kuala Lumpur Malaysia* 450-64

[6] Dewan S, Hsu V 2001 Trust in Electronic Markets: Price Discovery in Generalist Versus Specialty Online Auctions http://databases.si.umich.edu/reputations/bib /papers /Dewan&Hsu.doc

## Author

**Xue Zhao, 22.11.1980, Henan Province, China.**

**Current position, grades**: lecture of Management Information System in the IEC of NIT.
**University studies**: BSc of Electronic Commerce, Zhengzhou university, China, MSc of Administration Management, major in E-government, Central China Normal University, China.
**Scientific interest**: E-ecommerce.
**Publications**: 8 papers.