Noname manuscript No.
(will be inserted by the editor)

Evaluating Transaction Trust and Risk Levels in Peer-to-Peer E-commerce Environments

Yan Wang[1], Duncan S. Wong[2], Kwei-Jay Lin[3], Vijay Varadharajan[4]

[1] Department of Computing
Macquarie University
Sydney, NSW 2109
Australia
yanwang@ics.mq.edu.au

[2] Department of Computer Science
City University of Hong Kong
Hong Kong
duncan@cityu.edu.hk

[3] Department of Electrical Engineering and Computer Science
University of California, Irvine
Irvine, CA 92697
USA
klin@uci.edu

[4] Department of Computing
Macquarie University
Sydney, NSW 2109
Australia
vijay@ics.mq.edu.au

Abstract As it lacks central management in Peer-to-Peer (P2P) e-commerce environments, prior to new transactions with an unknown peer, the trust evaluation is critical, which relies on the transaction history data. Traditionally the evaluation process is based on other peers' recommendations neglecting transaction amounts. This may lead to the bias in the transaction trust evaluation and risk the new transaction, which may occur between unknown peers. The weakness may be utilized by malicious sellers to obtain good transaction reputation by selling cheap goods and then cheat buyers by selling expensive goods. In this paper we present a novel model for transaction trust evaluation, which differentiates transaction amounts and thus computes different impact factors when analyzing old transactions

and computing trust values. As a result, the trust evaluation becomes more accurate, which is dependant on transaction history, the amounts of old transactions, and the amount of the new transaction. Some extensions are also proposed to take the temporal dimension, transaction count and the credibility of responding peers into consideration. Therefore the obtained trust value can reflect the nature of transactions, and the difference of the new transaction and old transactions. Furthermore, the trust value can be taken as the risk indication of the forthcoming transaction and is valuable for the decision-making of the buyers.

1 Introduction

Peer-to-Peer (P2P) network is an infrastructure where each peer can play the role of a client and a service provider at the same time. Meanwhile, P2P e-commerce systems are drawing more and more attention [4][1][15], which let P2P networks go beyond the scope of information sharing systems like Freenet [2] and GNutella [3].

However, as it lacks the central management in most P2P systems, the dynamic status of each peer and the network causes trust evaluation a very important issue. Before interacting with an unknown peer, it is rational to doubt its trustworthiness. Therefore, it makes the new transaction securer by enabling trust evaluation prior to interacting with an unknown peer.

Generally, in Peer-to-Peer (P2P) environments, the trust evaluation on an unknown peer relies on the recommendations of other peers, which have transaction history with the target peer that is being investigated. If the unknown target peer is one of potential sellers, the end-peer (requesting peer) can enquire other peers about the target peer's transaction trust. After having collected the feedback from a set of responding peers, the requesting peer can analyze the data and evaluate the trust status of the target peer [10][14][21].

To evaluate a peer's service quality, some attributes can be considered, such as the price, warranty, and delivery etc. From the point of view of an end-peer, other peers' recommendations outline the transaction history of the target peer providing an indication of the transaction trust status of the target peer, which in some sense indicates the risk level of the new transaction. However the possible new transaction may be different from some previous transactions in terms of transaction amount, which implies these old transactions should not be taken as references equally when analyzing the transaction trust of the target peer. Otherwise, it may lead to a result with bias. This is especially risky for an end-peer, if it has no transaction previously with the target peer.

In this paper, we propose a novel model for evaluating the transaction trust of a target peer taking into account of the transaction amount property. The new method is based on other peers' transaction experience but distinguishes different categories of transaction amounts and determines

different impact factors according to the amount of the new transaction. Meanwhile, the new method also considers the temporal dimension weighing more to fresh transactions. This results in more accurate trust values, which can be taken as the risk indication of the new transaction. With our model, when targeting at a set of potential service providers (peers), the end-peer can investigate their transaction history, analyze the transaction risk, and thus make the decision of selecting the most suitable seller.

This paper extends the work presented in [17] by taking more factors into account when evaluating transaction trust and transaction risk values, such as the transaction count and credibility of responding peers. Thus the evaluation model in this paper is more comprehensive and more objective. Additionally, more examples and experiments are presented to illustrate the properties of the proposed models.

This paper is organized as follows. In section 2, we review some existing studies. Section 3 presents our approach for peer trust evaluation taking transaction amount into account. Section 4 extends the model presented in Section 3 by taking the time dimension, transaction count and the credibility of responding peers into account. Furthermore, Section 5 presents the method of risk evaluation. Two case studies are presented in Section 6 for further illustrating our model. In addition to the case study, an incremental approach is proposed in Section 7 for obtaining good reputation. Finally Section 8 concludes our work.

2 Related Work

eBay [1] is typical Customer-to-Customer (C2C) e-commerce system *with* central management, where peers - buyers or sellers - can evaluate each other based on the service quality or behaviors during transactions. [4] presents a P2P e-commerce system in pervasive environments, where each peer can interact with other peers directly by mobile and handheld devices with wireless network access and Internet access.

Due to the special infrastructure of P2P networks, trust evaluation remains a challengeable issue which draws much attention in the research community.

In [5], Damiani *et al* proposed *XRep*: a reputation-based approach for evaluating the reputation of peers through distributed polling algorithm before downloading any information. The approach adopts a binary rating system and it is based on GNutella [3] query broadcasting method using TTL limit.

EigenTrust [10] collects the *local trust values* of all peers to calculate the *global trust value* of a given peer. Additionally, EigenTrust [10] adopts a binary rating function, interpreted as positive one (representing satisfactory), or zero or negative one (representing unsatisfactory or complaint).

In [14], Marti and Garcia-Molina proposed a voting reputation system aiming at e-commerce applications that collects responses from other peers

on a given peer. The final reputation value is calculated combining the values returned by responding peers and the requesting peer's experience with the given peer. This seems more reasonable than the model in [5]. However, this work and the work in [10] didn't explicitly distinguish transaction reputation and recommendation reputation. This may cause severe bias in reputation evaluation as a peer with good transaction reputation may have a bad recommendation reputation especially when recommending competitors.

In [18], Wang *et al* proposed several trust metrics for the trust evaluation in a decentralized environments (e.g. P2P network) where a trust value is a probabilistic value in the scope of [0, 1]. Prior to the interaction with an unknown peer P_x, the end-peer collects other peers' trust evaluations over P_x. A method has been proposed for trust modification after a series of interactions with P_x that a good value results from the cumulation of constant good behaviors leading to a series of constant good trust values. In [19] the temporal dimension is taken into account in the trust evaluation wherein fresh interactions are weighted more than old ones.

In [22], Yu *et al* proposed the method of exponential averaging taking into account a series of interactions of the requesting peer itself. It is similar to the work in [19]. In [20], Wang *et al* presented $Trust^2$, a model for trust evaluation taking recommendation trust into account. $Trust^2$ also includes a method to measure the recommendation trust, based on the requesting peer's interaction experience with the target peer and the recommendations of responding peers in multiple rounds. For the sake of simplicity, in this paper, recommendation trust is not taken into account. Readers can refer to our work in [20] for the method.

In [12][11], Lin *et al* proposed a method of reputation-based trust evaluation in service-oriented environments based on a novel architecture of distributed trust management brokers.

[9] presented a method for analyzing the gain and lose for different transactions and related them with transaction success probability and decisions which are represented as reliability trust and decision trust.

However, in most existing trust evaluation models, the evaluation is based on transaction history. But the amount of transactions is not taken into account. That implies that all previous transactions are equally evaluated. This may lead to some attacks that may be easily successful in e-commerce environments as different transaction amounts imply different risk levels. For example, buyer A has many successful transactions with seller B. So the trust value of B given by A is always very good. But each time the transaction amount is up to \$100 only. Assume for the next round, the transaction amount is \$1 million. As the new amount is so different from old transactions, previous trust evaluations may not be important references any more. This is because the nature and the risk of the new transaction are definitely different. It is similar to another case, where a new buyer C, to whom seller B is unknown, is going to have a transaction for about \$1 million with B provided the amount of most transactions that B had is

around $100. In this situation, other buyers' experience with the transaction amount around $100 should not be taken as an important reference to C's new transaction. Namely, in the above cases, different nature of transactions implies different situations and experience. Thus it requires different consideration and evaluation methods.

In this paper, we proposed a novel trust evaluation model taking the transaction history, transaction amount, and the temporal dimension into account. As the trust evaluation is based on both old transactions and the new one, the obtained trust value can be taken as an indication of the risk level of the new transaction. This is a subset of the situational trust model proposed by Marsh [13] that trust for similar situations can be considered together. But we further extend the basic idea to the trust evaluation in P2P e-commerce environments.

3 Trust Evaluation

3.1 Local Rating

For each peer P_A, if it has an online interaction with peer P_B in round k at time period t_k, it can give a local trust evaluation $T_{A\to B}^{(k)}$ for the interaction occurred. The value is calculated taking into account of the quality of the service provided by P_B. The quality of the service comes from several aspects (e.g. price, warranty, delivery, etc.) represented by a set of attributes:

$$\bar{A} = \{a_1, a_2, \ldots, a_n\}$$

For example, the end peer may consider some of the follows [19]:

1. is the product the same as the one the buyer paid for?
2. is the warranty the same as claimed?
3. was the delivery as quick as claimed?
4. is the the payment correct for each transaction with the service providing peer?
5. is the service providing peer online most of time?

1. For each attribute a_i, calculate its firing level F_i as:

$$F_i = K_i(a_i)$$

where K_i is the grading function of attributes, which converts the attribute values into the corresponding firing levels. These levels can be represented as linguistic values, such as "very good", "good", "moderate", "poor" or "very poor" for 5 categories.
2. Calculate the scores R_i of each attribute as:

$$R_i = S_i(F_i)$$

where S_i is the score function that maps the attribute score in 5 intervals, i.e. $\{0,\ 0.25,\ 0.5,\ 0.75,\ 1\}$.
3. A crisp evaluation value can be obtained by calculating the overall direct trust value $T_{A\to B}$ of attribute set x as follows:

$$T_{A\to B} = \sum e_{a_i} \cdot R_i \tag{1}$$

where the relative importance assigned to each attribute is modelled as a weight e_{a_i} and $\sum e_{a_i} = 1$. All weights are given by the end-peer (customer).

Thus, each peer maintains a record below of the rating the service quality after a transaction with a seller.

$$< peerID,\ sellerPeerID,\ rating,\ transactionAmount,\ timestamp >$$

This record is local to the record owner but it can be sent to other peers when the owner receives a request for collecting ratings of the seller peer.

3.2 New Transaction and Old Transactions

Now let's assume a requesting peer P_r would like to have a new transaction with a target peer P_x, wherein the transaction amount is about \$10K. If P_r has no transaction with P_x before, it can enquire other peers about their previous transactions with P_x and their trust evaluations over P_x. However, if P_x has a lot of transactions with different transaction amounts, and P_r can collect some of them, as we have analyzed in Section 2, the trust evaluation done by P_r should differentiate transactions with different transaction amounts. If an old transaction has the same transaction amount with the new one, or the two amounts are quite similar to each other, the old transaction information (collected from a responding peer) can be a direct reference for the trust evaluation. However, if the amount of the old transaction is different from the new one, it cannot be taken as a direct reference but is still useful for evaluating the transaction trust.

In this work, we assume that

1. the larger the transaction amount is, the more profit of the seller has, and
2. the more the transaction amount is, the higher risk level is from the perspective of a buyer.

In addition, we assume that each seller peer has enough transactions and obtained enough trust evaluations. Otherwise a seller peer is not comparable to others if it has, say, one evaluation per round no matter how positive the evaluation is.

When evaluating the trust status based on the transaction history and the new transaction, different situations can be further analyzed into 3 cases as follows.

1. The amount of an old transaction is the same as the new one. In this case, the old experience and corresponding trust evaluation can be taken as a *direct reference* for the new transaction.
2. The amount of the old transaction is larger than that of the new one. In this case, the old transaction can be taken as the reference with less impact.
   For instance, assume seller P_x has a lot transactions with some peers, wherein each transaction amount is basically around \$1-2K. Assume the service is good each time. Let C denote the set of corresponding customers. Now P_r is going to buy a product for \$100. If P_r knows that the trust evaluations over P_x given by most peers in C are quite positive, P_r may not worry about the trust of the new transaction as the product to buy is cheaper. However, on the other hand, a situation exists. The gain for selling a cheap product is probably less. Therefore, the seller may not take it seriously. This leads to a worse service quality. Thus, in this case, the old transaction cannot be taken as a direct reference when evaluating the transaction trust relevant to the new transaction. But good trust evaluations from this kind of old transactions should be helpful to give a new and positive trust evaluation relevant to the new transaction.
3. The amount of the old transaction is less than that of the new one. In this case, the old transaction cannot be taken as a direct reference either because it is risky.
   For instance, a seller may be always honest when selling cheap items (say for \$50). However if the new product is quite expensive (say \$10k or more), a fraud is more likely to happen. Due to this reason, after having collected trust evaluations based on transactions with lower transaction amounts, a factor should be determined to scale down the impact of these trust values. The final trust evaluation result should also reflect the risk of the new transaction, wherein the transaction amount is different from most old transactions.

3.3 Impact Factor

To summarize the above analysis, some principles can be listed as follows:

Principle 1 Any old transaction can be taken as a direct reference to a new transaction provided that the old transaction amount is the same as the new one.

Principle 2 Any old transaction with less transaction amount has minor impact to a new transaction with a larger transaction amount. The larger the difference is, the less the impact is.

Principle 3 Any old transaction with larger transaction amount can not be taken as a direct reference to a new transaction with less transaction amount. But it is more important than an old transaction wherein the transaction amount is relatively less than the new one.

Therefore, the trust value of the new transaction results from

1. the transaction amount of the new transaction;
2. the transaction amount of each old transaction;
3. the trust value of each old transaction;
4. the impact factor resulting from the transaction amount difference of the old transaction and the new transaction.

To calculate the impact factor, let's first denote the transaction amount difference as:

$$\Delta = Amount_{new} - Amount_{old}$$

where $Amount_{old}$ denotes the amount of the old transaction and $Amount_{new}$ denotes the amount of the new transaction.

Next, let's design a formula to calculate impact factor θ, which results from Δ.

According to the above analysis, when Δ is 0, θ should be exactly 1 (Principle 1). When Δ is greater than 0, θ should be less than 1 (Principle 2). Therefore, to be consistent to Principle 2, we design a formula as follows using Hyperbolic Secant.

$$\theta = \frac{2}{e^{\Delta * \alpha} + e^{-\Delta * \alpha}} \qquad if\ \Delta \geq 0 \tag{2}$$

where $\alpha \in (0, 1]$ is the *scale control factor*.

Formula (2) is plotted in Figure 1 where $\alpha = 1.0,\ 0.5,\ 0.2$ and 0.05 respectively. From Figure 1, it is easy to see that with the increment of the value of Δ, θ drops but its value is in the scope of $(0, 1]$. When $\Delta = 0$ and $\theta = 1$, with more and more Δ, θ approaches 0, namely, $lim_{\Delta \to \infty} = 0$. In addition, α is used to control the decrement trend. A smaller α (e.g. $\alpha = 0.05$) is more suitable for applications with a large transaction amount scope as θ approaches 0 very slowly. In contrast, a larger α (e.g. $\alpha = 0.5$) is suitable for applications with a smaller transaction amount scope.

Likewise, according to Principle 3, when $\Delta < 0$, the corresponding impact factor θ should be less than 1. Meanwhile, different from case 2, with more and more transaction amount difference Δ, the impact factor θ should be reaching a value greater than a threshold in the scope of (0,1) (e.g. 0.8). Therefore, a formula is designed as follows.

$$\theta = \frac{2}{e^{\Delta * \alpha} + e^{-\Delta * \alpha}} * (1 - \beta) + \beta \qquad if\ \Delta < 0 \tag{3}$$

where $\alpha \in (0, 1]$ and $\beta \in (0,\ 1)$.

Formula (3) is plotted in Figure 2 where threshold $\beta = 0.8$. With more and more $|\Delta|$, θ drops from 1 and approaches β, namely, $lim_{\Delta \to \infty} = \beta$. In formula (3), α is the scale control factor - the same role as in formula (2).

Definition 1: Let $Amount_{old}$ denote the amount of the old transaction and $Amount_{new}$ denote the amount of the new transaction. Let Δ denote the

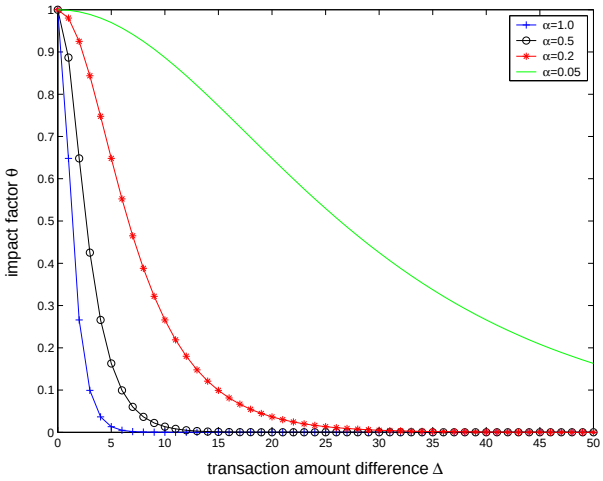

Fig. 1 Impact Factor with Positive Δ

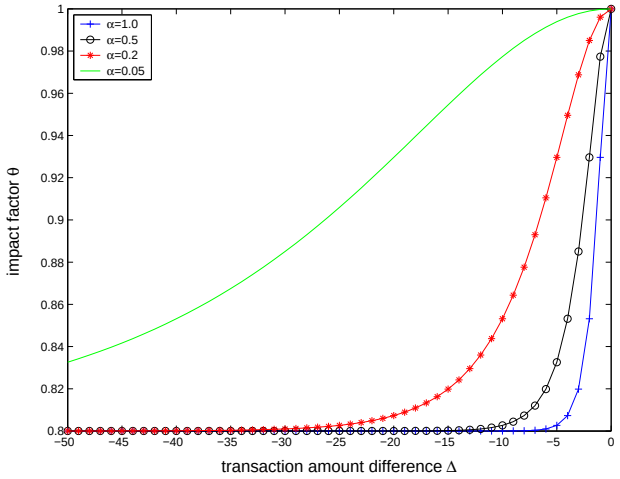

Fig. 2 Impact Factor with Negative Δ ($\beta = 0.8$)

transaction amount difference i.e. $\Delta = Amount_{new} - Amount_{old}$. With Δ, the *impact factor* θ is defined as follows:

$$\theta = \begin{cases} \frac{2}{e^{\Delta * \alpha} + e^{-\Delta * \alpha}} & \text{if } \Delta \geq 0 \\ \frac{2}{e^{\Delta * \alpha} + e^{-\Delta * \alpha}} * (1 - \beta) + \beta & \text{if } \Delta < 0 \end{cases} \tag{4}$$

Formula (4) is plotted in Figure 3.

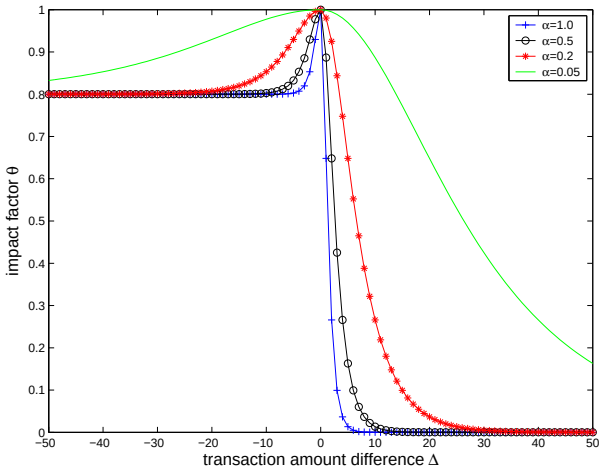

Fig. 3 The Impact Factor Function

3.4 Transaction Amount Category

In the above discussion in section 3.3, impact factor θ results from transaction amount difference Δ. However, how to calculate the transaction amount difference? Is it to directly calculate it as $\Delta = Amount_{new} - Amount_{old}$? That means a transaction for \$10 is definitely different from the one for \$20. But in terms of the nature of transactions, they may be the same.

A more realistic method is to categorize the transaction amount. Transaction amounts in the same category are considered the same.

Here we list an example of transaction amount category as follows where *Amount* denotes the *transaction amount*.

1. *small-* transaction amount category: In this category, $Amount \in [1, 10]$;
2. *small* transaction amount category: In this category, $Amount \in [11, 50]$;
3. *small+* transaction amount category: In this category, $Amount \in [51, 100]$;
4. *medium-* transaction amount category: In this category, $Amount \in [101, 500]$;
5. *medium* transaction amount category: In this category, $Amount \in [501, 1000]$;
6. *medium+* transaction amount category: In this category, $Amount \in [1001, 5000]$;
7. *large-* transaction amount category: In this category, $Amount \in [5001, 10000]$;
8. *large* transaction amount category: In this category, $Amount \in [10001, 30000]$;
9. *large+* transaction amount category: In this category, $Amount \in [30001, 100000]$;

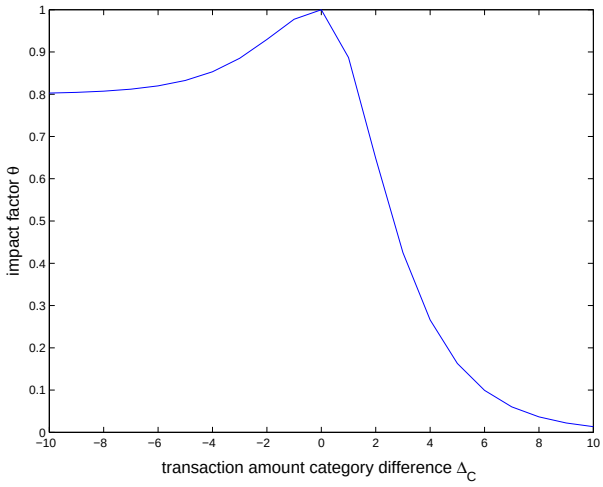

Fig. 4 The Impact Factor Function ($\alpha = 0.5$ $\beta = 0.8$)

10. *huge* transaction amount category: In this category, $Amount > 10K$.

Given a transaction amount $Amount$, if $Amount \in$ category $i \in [1, 10]$, it is denoted as $C(Amount) = i$. For example, if $Amount = 100$, it belongs to category 2 (i.e. $C(100) = 2$).

Based on the above category, when computing the impact factor θ, the transaction amount difference should be replaced with the transaction amount category difference.

Definition 2: If $Amount_{old}$ is the amount of an old transaction, and $Amount_{new}$ is the amount of the new transaction, the *transaction amount category difference* is:

$$\Delta_C = C(Amount_{new}) - C(Amount_{old})$$

With Δ_C, the *impact factor* θ is defined as follows:

$$\theta = \begin{cases} \frac{2}{e^{\Delta_C * \alpha} + e^{-\Delta_C * \alpha}} & \text{if } \Delta_C \geq 0 \\ \frac{2}{e^{\Delta_C * \alpha} + e^{-\Delta_C * \alpha}} * (1 - \beta) + \beta & \text{if } \Delta_C < 0 \end{cases} \quad (5)$$

where $\alpha \in (0, 1]$ and $\beta \in (0, 1)$.

Formula (5) is plotted in Figure 4 where we chose $\alpha = 0.5$ as the transaction amount category difference is $|\Delta_C| \in [0, 9]$.

Moreover, the transaction amount category is domain-dependant. For example, in the property market, a transaction for \$10K is in the "*small+*" transaction amount category as a house is generally worth about \$300K or more. With different transaction amount categories, we can choose different arguments α and β.

3.5 New Transaction Trust Evaluation

In P2P e-commerce environments, as there is no central management mechanism, to obtain the transaction trust status of the target peer P_x, a requesting peer P_r has to enquire other peers who have transactions with P_x.

Definition 3: Assume P_r has collected a set of trust values from a set of intermediate peers $IP = \{P_1,\ P_2,\ \ldots,\ P_n\}$. Let $T_{i\to x} \in [0, 1]$ denote the transaction trust given by a responding peer P_i over target peer P_x. Let $Amount_{old_i}$ denote the old transaction amount between P_x and P_i, and let $Amount_{new}$ denote the amount of the new transaction. θ_i is the impact factor resulting from $\Delta_{C_i} = C(Amount_{new}) - C(Amount_{old_i})$. The *trust value of the new transaction with* P_x is:

$$T_{new_x} = \frac{1}{n}\sum_{i=1}^{n}(\theta_i \cdot T_{i\to x}) \tag{6}$$

According to Definition 3, some features of the new transaction trust value T_{new_x} are as follows.

1. The new trust value T_{new_x} is based on the transaction history between P_x and other (responding) peers, and the new transaction amount $Amount_{new}$;
2. If each $Amount_{old_i}$ and $Amount_{new}$ are in the same category, and T_i is high, T_{new_x} will be a high value;
3. If most $Amount_{old_i}$ values and $Amount_{new}$ are in different categories, it leads to low θ_i values and thus a low new trust value T_{new_x} though each $T_{i\to x}$ may be a high value.

4 Taking More Factors into Account in Trust Evaluation

In the above discussion, we have proposed an approach relating the new transaction amount with the new transaction trust evaluation. However, this base model should be further extended to take more factors into account.

4.1 Adding Temporal Dimension to Trust Evaluation

In the approach proposed in Section 3, the temporal property of a transaction is not taken into account. That means all transactions occurred in different periods are equally evaluated. Nevertheless, this may lead to inaccurate trust values. To reflect more accurate trust situation of a target peer, transactions occurred in different periods should be given different weights, wherein very old transactions should be ignored and fresh transactions should be weighted more as they are more important.

Thus when broadcasting the request, the requesting peer P_r should specify that it is interested in transactions occurred during the period $[t_{start},$

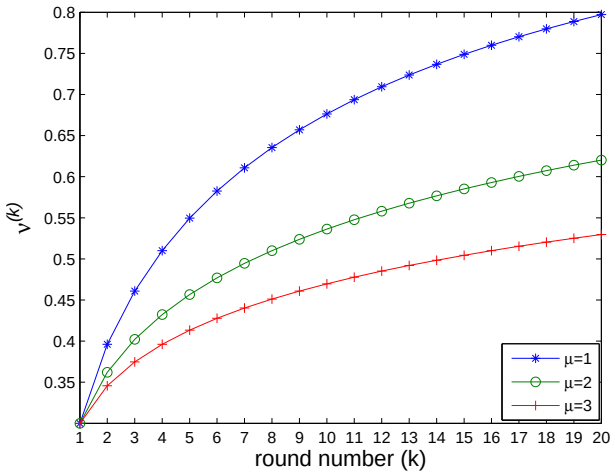

Fig. 5 $\nu^{(k)}$ $(\lambda = 0.7)$

$t_{end}]=\{t_1,\ t_2,\ \ldots,\ t_l\}$ where $t_k < t_{k+1}$ $(1 \le k \le l-1)$ and t_l is the latest period. When calculating the trust value based on the collected data, P_r should also specify a set of weights:

$$W = \{w^{(k)} :\ k = 1,\ \ldots,\ l\} \tag{7}$$

where $w^{(k)} \le w^{(k+1)}$ *and* $\sum_{k=1}^{l} w^{(k)} = 1$

With W, the new trust value can be calculated as follows.

Definition 4: Let $T_{i\to x}^{(k)}$ denote the trust value given by peer P_i over peer P_x for the transaction with the transaction amount $Amount_{old_i}^{(k)}$ occurred at period t_k. The new trust value of peer P_x is:

$$T_{new_x} = \sum_{k=1}^{l} (w^{(k)} \cdot T_x^{(k)}) \tag{8}$$

where

1. $w^{(k)} \le w^{(k+1)}$ *and* $\sum_{k=1}^{l} w^{(k)} = 1$;
2. $T_x^{(k)} = \frac{\sum_{i=1}^{n} (\theta_i^{(k)} \cdot T_{i\to x}^{(k)})}{n}$ is the trust value of P_x in round k;
3. $\theta_i^{(k)}$ results from $C(Amount_{old_i}^{(k)})$ and $C(Amount_{new})$.

Furthermore, to ease the trouble of assigning a set of weights, we adopt a formula with 2 parameters only, which can be employed to generate l weights for period $[t_{start},\ t_{end}]=\{t_1,\ t_2,\ \ldots,\ t_l\}$ where $t_k < t_{k+1}$ $(1 \le k \le l-1)$.

Definition 5: Given parameters λ $(0.5 < \lambda < 1)$ and μ $(\mu \in \{1,\ 2,\ 3, \ldots\})$, *the weight of period* t_k can be calculated as follows:

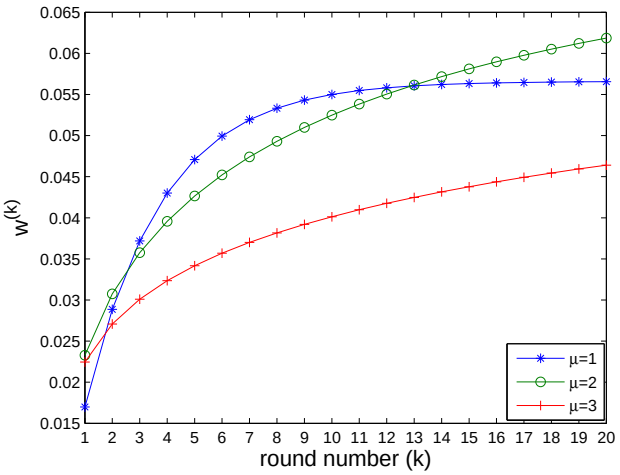

Fig. 6 $w^{(k)}$ $(\lambda = 0.7,\ l = 20)$

$$w^{(k)} = \frac{\nu^{(k)}}{\sum_{i=1}^{l} \nu^{(i)}} \tag{9}$$

where

$$\nu^{(k)} = 1 - \lambda^{k^{\frac{1}{\mu}}},\ 0.5 < \lambda < 1 \textit{ and } \mu \in \{1,\ 2,\ 3, \ldots\} \tag{10}$$

According to Definition 5, given the round number l, parameters λ and μ, each weight factor $\nu^{(k)}$ can be generated. Hereafter each weight $w^{(k)}$ and $W = \{w^{(k)}\}$ can be calculated. For example, if $l = 10$, $\lambda = 0.7$ and $\mu = 2$, then $W = \{0.038797,\ 0.065955,\ 0.084965,\ 0.098273,$
$0.10759,\ 0.11411,\ 0.11867,\ 0.12187,\ 0.1241,\ 0.12567\}$

In formula (10), $\nu^{(1)} = 1 - \lambda$ is the minimal weight factor for period t_1 where $k = 1$. k corresponds to period t_k. Given the same λ and μ, the larger k is, the larger $\nu^{(k)}$ is. This ensures the property $w^{(k)} < w^{(k+1)}$. In addition, the valuation of μ is dependant on applications. For certain applications, k =10 or 20 may mean a high quantity of interactions. In this case, $\mu = 1$ is suitable. For other applications, where 100 means high quantity of interactions, $\mu = 2$ or $\mu = 3$ is more suitable.

$\nu^{(k)}$ is depicted in Figure 5 where $\lambda = 0.7$ and $l = 20$. $w^{(k)}$ is plotted in Figure 9.

4.2 Adding Transaction Count to Trust Evaluation

In Section 3, by default, we assume that each peer has one transaction during each period. But actually a peer can have multiple transactions during one

period. They may belong to different transaction amount categories. Thus, if a buyer peer has several transactions during a period, it can give one rating to the service quality of all transactions in the same amount category in the same period. Thus the number of transactions (transaction count) should also be a factor to be taken into account when evaluating the transaction trust values.

As a result, each peer should maintain a record of the rating as follows. Such a record can be sent to a requesting peer.

$$< peerID,\ sellerPeerID,\ rating,\ transactionAmountCategory,$$
$$transactionCount,\ timePeriod >$$

Thus, a buyer peer can maintain several records for the same period. Each record contains one rating for transactions in the the same transaction amount category and the same round.

Assume P_i has a series of transactions in round k with the amount categories of $C_{i_1}^{(k)}$, $C_{i_2}^{(k)}$, ... Let $N_{i_j}^{(k)} = N(C_{i_j}^{(k)})$ denote the transaction count of transactions in category $C_{i_j}^{(k)}$ in round k.

Definition 6: Assume P_r has collected a set of trust values to seller P_x from a set of intermediate peers $IP = \{P_1,\ P_2,\ \ldots,\ P_n\}$. Each responding peer P_i provides a series of ratings $\{T_{i_j \to x}^{(k)}\}$. Each rating corresponds to the transaction amount in category $C_{i_j}^{(k)}$. Let $C(Amount_{new})$ denote the transaction amount category of the new transaction and let $N_{i_j}^{(k)} = N(C_{i_j}^{(k)})$ denote the transaction count of transactions between P_i and P_x in category C_{i_j} in round k. $\theta_{i_j}^{(k)}$ is the impact factor resulting from $\Delta_{C_{i_j}} = C(Amount_{new}) - C_{i_j}^{(k)}$. The *trust value of the new transaction with* P_x is:

$$T_{new_x} = \sum_{k=1}^{l} w^{(k)} \cdot \frac{\sum_{i=1}^{n} \sum_j (N_{i_j}^{(k)} \cdot \theta_{i_j}^{(k)} \cdot T_{i_j \to x}^{(k)})}{\sum_{i=1}^{n} \sum_j N_{i_j}^{(k)}} \tag{11}$$

4.3 Adding the Credibility of Responding Peers to Trust Evaluation

In formula (11), each trust value $T_{i_j \to x}^{(k)}$ is given by a responding peer. Thus it is local to the responding peer. But when it is sent to the requesting peer, it becomes a recommendation. Thus, the requesting peer may trust it or may not trust it. This is the *recommendation trust* (referred to as *credibility* in [20]) of each responding peer. The credibility value (e.g. in the scope of [0, 1]) of a responding peer results from its recommendation history. It can be determined by the deviations of its recommendations in multiple rounds. Namely, constant high deviations lead to a low credibility level while constant low deviations lead to a high credibility level. Here we would not discuss how to calculate the recommendation trust as it is out of the scope of this paper. However, when calculating the new trust value,

recommendation trust or credibility values of responding peers should be taken into account [21][22][20].

Definition 7: Assume P_r has collected a set of trust values about seller P_x from a set of intermediate peers $IP = \{P_1,\ P_2,\ \ldots,\ P_n\}$. Each responding peer P_i provides a series of ratings $\{T^{(k)}_{i_j \to x}\}$. P_i's recommendation trust (credibility) values are $\{c_i^{(k)} \in [0,1]\}$. The *trust value of the new transaction with* P_x is:

$$T_{new_x} =$$

$$\sum_{k=1}^{l} w^{(k)} \cdot \frac{\sum_{i=1}^{n'} \sum_j (N_{i_j}^{(k)} \cdot \theta_{i_j}^{(k)} \cdot \varpi_i^{(k)} \cdot T_{i_j \to x}^{(k)})}{\sum_{i=1}^{n'} \sum_j N_{i_j}^{(k)} \cdot \varpi_i^{(k)}} \tag{12}$$

where

1. $n' = |IP'|$ $(n' \leq n = |IP|)$ is the size of IP' - the set of 'good' responding peers where each peer's credibility c_i is not worse than a threshold ϵ. Thus 'bad' responding peers whose credibility is worse than ϵ are blacklisted and filtered out;
2. $$\varpi_i^{(k)} = \frac{c_i^{(k)}}{\sum_i^{n'} c_i^{(k)}} \tag{13}$$
   is the weight given to P_i's recommendation in round k with respect to its credibility level among 'good' responding peers.

5 Transaction Risk Evaluation

For each requesting peer P_r, if it can collect the transaction history data from some intermediate peers, the risk of the new transaction can be analyzed as T_{new_x} can be taken as a direct risk indication. The relationship between the trust value and the risk value of the new transaction is as follows.

1. If the trust value of the new transaction is high, the corresponding risk is low;
2. If the trust value of the new transaction is low, the corresponding risk is high.

According to the above properties, we can simply define the computation of risk value r_{new_x} as follows.

Definition 8: If the trust value of a new transaction with peer P_x is T_{new_x}, the *risk value* r_{new_x} of the new transaction is:

$$r_{new_x} = 1 - T_{new_x} \tag{14}$$

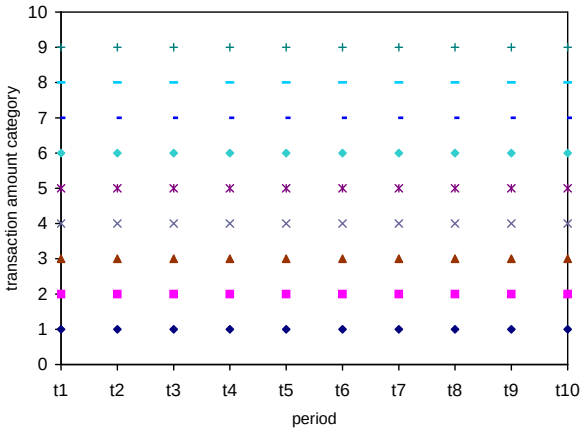

Fig. 7 Transaction History of P_{x_1}

Therefore, if a peer P_r has a set of potential target peers $TP = \{P_{x_1}, P_{x_2}, \ldots, P_{x_m}\}$ to have a new transaction with, it can collect the transaction history data from other peers. Hereafter, P_r can evaluate the risk of the new transaction based on the the new transaction amount, the transaction history of each target peer, and the old transaction amounts. The best target peer is the peer P_{best} with which the corresponding risk value of the new transaction is the minimal.

$$P_{best} = P_i \in TP = \{P_i : \ i = 1, \ldots, \ m\} \tag{15}$$

where $r_{new_i} = min(r_{new_1} : r_{new_m})$

6 Case Studies

6.1 Case Study 1

In this section, we compare 5 seller peers (say P_{x_1}, P_{x_2}, P_{x_3}, P_{x_4} and P_{x_5}) wherein the requesting peer P_r has collected the transaction trust values for the period of $[t_{statrt}, \ t_{end}] = [t_1, t_2, \ldots, t_{10}]$. The transaction history data is plotted in Figures 7, 8, 9, 10 and 11. It is easy to see that peer P_{x_1}'s transaction amounts are in the category scope of $[1, 9]$ (see Figure 7). Peer P_{x_2}'s transaction amounts are in the category scope of $[1, 3]$ (see Figure 8) while P_{x_3}'s are in $[3, 5]$ (see Figure 9). The transaction amounts of P_{x_4} and P_{x_5} 's are in the category scope of $[5, 7]$ and $[7, 9]$ (see Figures 10 and 11) respectively. To compare their transaction trust values and risk values, we assume $C(Amount_{new})$ is 2, 4, 6, 8 or 10 respectively. For the sake of simplicity, the trust value of each transaction is assumed to be 0.95. In this experiment, we set $\alpha = 0.5, \ \beta = 0.8$ and $\mu = 1$.

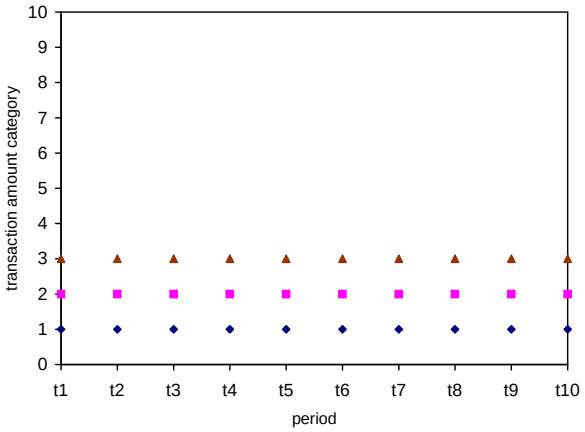

Fig. 8 Transaction History of P_{x_2}

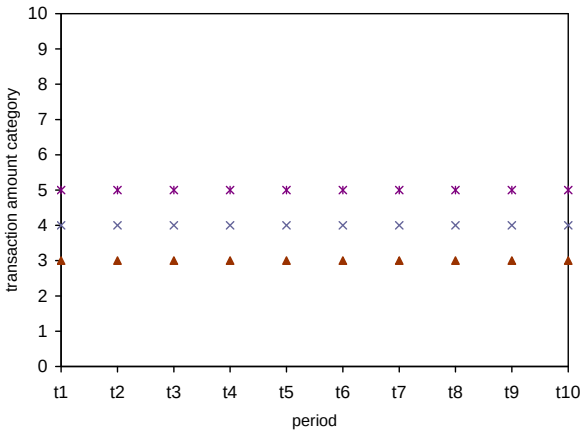

Fig. 9 Transaction History of P_{x_3}

According to formula (6), results are obtained and listed in Table 1. As P_{x_2}'s transactions cover categories 1 to 3, when $C(Amount_{new}) = 2$, its trust value is the maximum. P_{x_2}'s trust value is good too as its transactions cover categories 3 to 5, all of which are very close but higher than category 2. According to formula (5), this leads to the impact factor $\theta \geq \beta$. This is also the reason why P_{x_4} is worse than P_{x_3} and P_{x_5} is worse than P_{x_4}. In these cases, a larger category difference leads to a lower impact factor. When $C(Amount_{new}) = 2$, P_{x_1} is not the best with respect to trust values as it transaction categories cover 1 to 9.

Similarly, when $C(Amount_{new}) = 4$, P_{x_3} becomes the best peer as $C = 4$ is among its transaction categories (refer to Figure 9). P_{x_4} is the second best as it has transactions close to but higher than category 4 (refer to

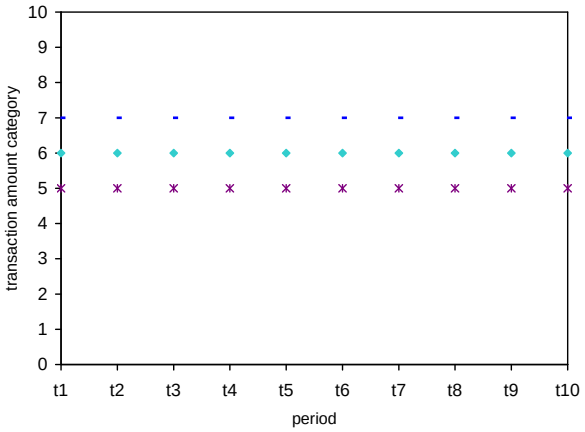

Fig. 10 Transaction History of P_{x_4}

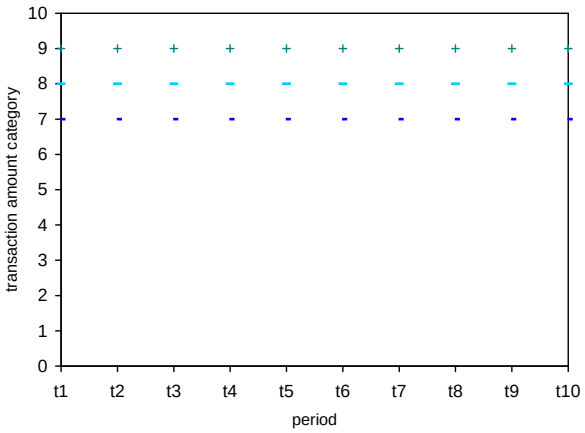

Fig. 11 Transaction History of P_{x_5}

Figure 10). In this case, P_{x_1} is not as good as peer P_{x_3} because it has many transactions in categories 1 to 9. Meanwhile, P_{x_2} is in the worst as its transaction amounts are all lower than $C(Amount_{new}) = 3$. This results in that some impact factors may be approaching 0.

When $C(Amount_{new}) = 6$ or 8, we can see similar result wherein P_{x_4} or P_{x_5} is the best peer respectively in terms of trust value.

When $C(Amount_{new}) = 10$, no peer has any existing transaction in this category. Finally P_{x_5} becomes the best peer as its transactions are in categories 7 to 9, which are very close to category 10. P_{x_1} is the second best as it also has transactions in categories 7 to 9. But it has transactions in categories 2 to 6, which are lower than category 8. Thus P_{x_1}'s trust value

Table 1 Trust Values T_{new}

T_i=0.95	$C_{new} = 2$	$C_{new} = 4$	$C_{new} = 6$	$C_{new} = 8$	$C_{new} = 10$
P_{x_1}	0.844	0.785	0.652	0.478	0.275
P_{x_2}	*0.907*	0.621	0.270	0.102	0.038
P_{x_3}	0.884	*0.907*	0.621	0.270	0.102
P_{x_4}	0.814	0.884	*0.907*	0.621	0.270
P_{x_5}	0.780	0.814	0.884	*0.907*	*0.621*

Table 2 Risk Values r_{new}

T_i=0.95	$C_{new} = 2$	$C_{new} = 4$	$C_{new} = 6$	$C_{new} = 8$	$C_{new} = 10$
P_{x_1}	0.156	0.215	0.348	0.522	0.725
P_{x_2}	*0.093*	0.379	0.730	0.898	0.962
P_{x_3}	0.116	*0.093*	0.379	0.730	0.898
P_{x_4}	0.186	0.116	*0.093*	0.379	0.730
P_{x_5}	0.220	0.186	0.116	*0.093*	*0.379*

is lower than P_{x_5}. P_{x_2} is the worst as its transactions belong to categories 1 to 3, which are too far away from category 10.

Risk values are listed in Table 2. It is easy to see that when $C(Amount_{new})$ =2, the risk of the new transaction with P_{x_2} is the minimum. When $C(Amount_{new})$=8, P_{x_5} is the best. In contrast, the risk of P_{x_2} is the maximum when $C(Amount_{new}) = 10$.

To summarize, from this case study, we can observe that by applying the proposed model, when a seller selling low category goods (e.g. P_{x_2}) wants to sell very high category goods (e.g category 8 or 10), the risk value is very high (e.g. maximum with P_{x_2}) though trust values for low category transactions are always very satisfactory. This can prevent the typical attack mentioned in Section 2 that a malicious seller can obtain good reputation and transaction trust by selling low category goods so as to cheat buyers by selling high category goods.

6.2 Case Study 2

In this section, we conduct the simulation to study the impact of credibility (see formula (12)).

Here we assume that there are 10 responding peers in the peer set $\{P_i\}$ rating target peer P_x. Their credibility values (in the scope of $[0, 1]$) are listed in Table 3. For the sake of simplicity, we assume that each responding peer has one transaction in each period. The trust value of P_x is assumed to be around 0.9. Recommended trust values by responding peers are listed in Table 4.

In this study, we compare three methods. In *Method* 1, no credibility is taken into account. In *Method* 2, the credibility values of all peers are taken

Table 3 Peer Credibility

peers	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9	P_{10}
credibility	0.95	0.98	0.95	0.88	0.95	0.67	0.68	0.75	0.66	0.61

Table 4 Recommended Trust Values

peers	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9	P_{10}
round t_1	0.89	0.91	0.92	0.88	0.90	0.70	0.73	0.78	0.65	0.60
round t_2	0.91	0.90	0.92	0.88	0.90	0.70	0.73	0.79	0.65	0.60
round t_3	0.88	0.92	0.91	0.90	0.89	0.65	0.73	0.80	0.70	0.63
round t_4	0.89	0.91	0.92	0.89	0.90	0.70	0.70	0.78	0.65	0.60
round t_5	0.89	0.91	0.88	0.90	0.92	0.64	0.70	0.67	0.65	0.62
round t_6	0.92	0.89	0.87	0.91	0.90	0.65	0.73	0.75	0.65	0.60
round t_7	0.89	0.91	0.92	0.88	0.90	0.66	0.65	0.80	0.63	0.61
round t_8	0.88	0.89	0.92	0.90	0.91	0.70	0.73	0.81	0.65	0.60
round t_9	0.89	0.92	0.90	0.87	0.91	0.72	0.70	0.69	0.60	0.61
round t_{10}	0.90	0.90	0.92	0.88	0.90	0.70	0.73	0.72	0.65	0.60

into account by normalizing them using formula (13). In *Method* 3, only trust values of good peers with good credibility are taken into account. In this method, the credibility threshold is set to 0.8. Thus peers P_1 to P_5 are taken into account.

As we assume that each responding peer has one transaction in each period, we can compare these strategies by calculating the current trust value by the following formula, which simplifies formula (12).

$$T_{current} = \sum_{k=1}^{l} w^{(k)} \cdot \frac{\sum_{i=1}^{n'} \varpi_i^{(k)} \cdot T_{i \to x}^{(k)}}{n'} \tag{16}$$

In formula (16), $T_{current}$ is fully based on the trust ratings given by responding peers without any relationship with the new transaction.

Table 5 Trust Evaluation

Method	$T_{current}$
Method 1	0.78984
Method 2	0.80956
Method 3	0.90004

The aim of trust evaluation is to obtain accurate trust values. Thus the credibility level of responding peers is important and useful to reduce possible noise. This can be found by comparing the results of different methods in Table 5.

As peers P_6 to P_{10} give low values (see Table 4), this results in a low value in Method 1. In Method 2, though the credibility of each responding peer is taken into account, the final value is less accurate as low trust values from low credibility responding peers are taken into account. The result is improved only when low credibility responding peers are filtered out in Method 3, where the obtained trust value is very close to 0.9 (see Table 5).

Now we assume the above ratings are about peer P_{x_6}, which sells goods in category 2. In Table 6, we list the trust evaluation results based on formula (12) where the new transaction is set to categories 2, 4, 6 and 8 respectively. The result shows that low credibility evaluations lead to low trust values and corresponding high risk values, which are inaccurate. This will affect the decision-making especially when determining the best one from a set of potential sellers.

Table 6 Trust Values T_{new} for Peer P_{x_6}

	C=2	C=4	C=6	C=8
Method 1	0.78984	0.51186	0.13605	0.01351
Method 2	0.80956	0.52464	0.13954	0.01385
Method 3	0.90004	0.58328	0.15504	0.01540

7 An Incremental Approach Towards Good Reputation

From the above example in Section 6.1, it is easy to see that if a seller P_x sells goods in categories 2 and 3 only, it is very hard for it to obtain a good reputation when selling a product in a high category (e.g. category 8) for the first time. In such a case, according to formula (5), the impact factor is 0.1312, which leads to a very high risk value (0.8688 or more). We refer to such a method as *Strategy* 1.

Alternatively, P_x can choose a realistic and incremental strategy (referred to as *Strategy* 2) as follows:

1. If P_x is now selling goods in categories in the scope of $[i, j]$ $(i \leq j)$, it can sell some goods in category $j+1$ and provides good quality services;
2. After obtaining good trust values for selling the goods in category $j+1$, P_x can start selling goods in category $j+2$.

Thus, the seller can add new goods in higher category step by step and earn good reputation. By this strategy, when adding goods in the newest category, the impact factor can be better than *Strategy* 1.

Furthermore, if the final goal of the seller is to sell goods in a high category, he/she can remove the lowest category goods after adding the highest category good (referred to as *Strategy* 3).

The three strategies are compared in Table 7. Here we assume that peer P_x is currently selling goods in categories 2 and 3. P_x's final goal is to sell good in category 8. For the sake of simplicity, we also assume P_x obtains the same good trust value (e.g. 1.0) after each transaction. Thus we can compare the difference of impact factors by different strategies.

From Table 7, it is easy to see that in *Strategy* 2, when adding the newest category goods, the impact factor becomes less and less. But it is in the scope of [0.4257, 0.7675], which is much better than *Strategy* 1. In contrast, *Strategy* 3 leads to the best result where the impact factor is $\theta = 0.7675$.

Table 7 Comparison of Three Strategies

Strategy 1	sell C2 to C3	add C8	θ=0.1312		
action of Strategy 2	sell C2 to C3	sell C2 to C4	sell C2 to C5	sell C2 to C6	sell C2 to C7
	add C4	add C5	add C6	add C7	add C8
θ in Strategy 2	0.7675	0.6533	0.5565	0.491	0.4257
action of Strategy 3	sell C2 to C3	sell C3 to C4	sell C4 to C5	sell C5 to C6	sell C6 to C7
	add C4	add C5	add C6	add C7	add C8
	add C4	remove C2	remove C3	remove C4	remove C5
θ of Strategy 3	0.7675	0.7675	0.7675	0.7675	0.7675

8 Conclusions

In P2P environments, a typical attack is that the attacker can obtain good reputation by selling goods with low price and cheat customers afterwards by selling expensive goods. In this paper, we presented some principles, based on which we proposed a novel formula-based model of transaction trust evaluation taking the transaction amount into account. The trust value results from the transaction history, other peers' evaluation, old transaction amounts and the new transaction amount. This model can depict the trust value of a new transaction and thus indicates the risk level of it, which is especially useful for a buyer peer who intends to have a new transaction with an unknown peer, or useful for the case where the seller peer is known but the new transaction amount is different from some old transactions. The formula-based approach is generic as arguments can be changed according to different transaction amount categories. In this paper, we also proposed various extensions to take the temporal dimension, transaction count and the credibility of responding peers into account. This results in more objective trust evaluations and risk evaluations.

Additionally, the proposed approach can be applied to both decentralized e-commerce environments without a central management server (e.g P2P) and centralized e-commerce environments with a central management server (e.g. eBay [1]). The difference is that if there is no central server, it needs

intensive communication between peers to collect all evaluations for a target peer. If the central server is deployed, these problems will not exist. The server will be in responsible of collecting all evaluations and calculating the current trust value and risk value of a new transaction.

For future work, some directions can be further explored. As the evaluation is based on other peers' experience and recommendations, how to verify the accuracy and the objectivity of recommendations remains a problem. It relies on either security mechanisms or a mechanism checking the deviation of recommendations [20]. In addition, each evaluation may include subjectivity to some extent. How to identify the subjectivity and improve the evaluation accuracy remains challengeable. Another direction is to take other factors into account when evaluating the transaction trust and the transaction risk so that results can reflect more aspects of the nature of transactions [7], such as the social relationship of peers [16]. This is especially important when a peer is a business organization, such as in B2B and B2C environments [6][8].

9 Acknowledgement

We thank anonymous reviewers very much for their valuable suggestions.

References

1. *eBay*. http://www.eBay.com/.
2. *Freenet*. http://freenetproject.org/.
3. *GNutella*. http://www.gnutella.com/.
4. S. Anancha, P. D'souza, F. Perich, A. Joshi, and Y. Yesha. P2P M-commerce in pervasive environments. *ACM SIGecom Exchange*, 3(4):1–9, January 2003.
5. E. Damiani, S. D. C. di Vimercati, S. Paraboschi, P. Samarati, and F. Violante. A reputation based approach for choosing reliable resources in peertopeer networks. In *Proceedings of ACM CCS'02*, pages 207–216, Washington DC, USA, November 2002.
6. J. Franke, T. Stockheim, and W. K?ig. The impact of reputation on supply chains. an analysis of permanent and discounted reputation. *Information Systems and E-Business Management*, 3(4):377–403, December 2005.
7. N. Griffiths. Task delegation using experience-based multidimensional trust. In *Proceedings of the 4th International Joint Conference on Autonomous Agents in Multi-Agent Systems (AAMAS-05)*, pages 489–496, 2005.
8. C. W. Holsapple and S. Sasidharan. The dynamics of trust in B2C e-commerce: a research model and agenda. *Information Systems and E-Business Management*, 3(4):377–403, December 2005.
9. A. Josang and S. L. Presti. Analysing the relationship between risk and trust. In *Proceedings of the Second International Conference on Trust Management (iTrust 2004)*, volume LNCS 2995, Springer-Verlag, pages 135–145, 2004.
10. S. D. Kamvar, M. T. Schlosser, and H. Garcia-Molina. The eigentrust algorithm for reputation management in P2P networks. In *Proceedings of the 12th International WWW Conference*, Budapest, Hungary, May 2003.

11. K.-J. Lin, J. Y. Hsu, Y. Zhang, and T. Yu. A distributed reputation broker framework for web service applications. *Journal of E-Commerce Research*, 7(3), 2006.
12. K.-J. Lin, H. Lu, T. Yu, and C. en Tai. A reputation and trust management broker framework for web applications. In *Proceedings of The 2005 IEEE International Conference on e-Technology, e-Commerce and e-Service (EEE'05)*, pages 262–269, March 2005.
13. S. Marsh. *Formalising Trust as a Computational Concept.* University of Stirling, 1994.
14. S. Marti and H. Garcia-Molina. Limited reputation sharing in P2P systems. In *Proceedings of ACM EC'04*, pages 91–101, New York, USA, May 2004.
15. P2PBazaar, http://www.p2pbazaar.com/index.html/.
16. J. Sabater and C. Sierra. REGRET: A reputation model for gregarious societies. In *Proceedings of the First International Joint Conference on Autonomous Agents in Multi-Agent Systems (AAMAS-02)*, pages 475–482, 2002.
17. Y. Wang and F. Lin. Trust and risk evaluation of transactions with different amounts in peer-to-peer e-commerce environments. In *Proceedings of The IEEE International Conference on e-Business Engineering (ICEBE 2006)*, pages 102–109, Shanghai, China, October 2006. IEEE Computer Society Press.
18. Y. Wang and V. Varadharajan. Interaction trust evaluation in decentralized environments. In K. Bauknecht, M. Bichler, and B. Pröll, editors, *Proceedings of 5th International Conference on Electronic Commerce and Web Technologies (EC-Web?4)*, volume LNCS 3182, Springer-Verlag, pages 144–153, Zaragoza, Spain, August-September 2004.
19. Y. Wang and V. Varadharajan. A time-based peer trust evaluation in P2P e-commerce environments. In *Proceedings of 5th International Conference on Web Information Systems Engineering (WISE'04)*, volume LNCS 3306, Springer-Verlag, pages 730–735, Brisbane, Australia, November 2004.
20. Y. Wang and V. Varadharajan. T*rust*^{2}: Developing trust in peer-to-peer environments. In *Proceedings of 2005 IEEE International Conference on Services Computing (SCC 2005)*, pages 24–31, Orlando, Florida, USA, July 2005.
21. L. Xiong and L. Liu. PeerTrust: Supporting reputation-based trust for peer-to-peer electronic communities. *IEEE Trans. on Knowlege and Data Engineering*, 16(7):843–857, 2004.
22. B. Yu, M. P. Singh, and K. Sycara. Developing trust in large-scale peer-to-peer systems. In *Proceedings of 2004 IEEE First Symposium on Multi-Agent Security and Survivability*, pages 1–10, August 2004.