A P2P-based Trust Model for E-Commerce

Cheng Su, Hong Zhang, Fang-ming Bi
School of Computer Science and Technology,
China University of Mining and Technology, Xuzhou 221008, China
{sucheng, hongzh, bfm}@cumt.edu.cn l

Abstract

In an open distributed environment, traditional centralized trust mechanism for e-commerce becomes difficult to adapt to it. The existing P2P trust models are propitious to this environment, but they can not directly be used in e-commerce as taking no consideration for characteristics of e-commerce. This paper combines P2P trust model and e-transaction characteristics, presents a new P2P-based trust model for e-commerce. By computing interactive experiences, recommendations of other peers, risk factors and the transaction context, the model evaluates every peer's globe trustworthiness in order to guide transaction participants. Results of Simulation experiments show that, compared with some current trust models, the new model is effective against malicious behavior.

1. Introduction

With the development of growing number e-commerce, transaction risks go with bargainers all along, therefore online trust has become a crucial issue. Over the internet, both seller and buyer may be unfamiliar, thus they have to cope with much higher risk such as uncertainty and fraud. The situation of information asymmetry may give rise to opportunistic behavior. In a used-car market, for example, the seller knows the quality of the car while the buyer does not. The seller can try to exploit this information asymmetry by claiming a higher than actual quality and thus asking a higher price. It may be noted in that traditional transactions, the notion of *seeing is believing* plays a vital role. However, in an e-transaction environment, this is not the case. There is rarely any kind of real life relationship among the participants before they meet each other online, therefore trust plays a crucial role in e-commerce.

Many companies, including eBay, Amazon and uBid, now offer e-transaction evaluation platforms to facilitate e-transactions. A business or enterprise must have an effective reputation system to help users locate trustworthy partners and exchange commodities securely with confidence. Online reputation systems give a solution to the above-mentioned problem by facilitating trust and reducing risks through reputations. A reputation system's effectiveness depends on the trust model adapted. Traditionally trust models can be classified as two types [8]. One is the Central model (CM) which has a central trust point. Every entity in the Central model has the same opinion as what the central trust point has. Reputation-based systems, e.g., eBay, are the typical examples of the CM model. The other model is Transitive model (TM) which has a transitive trust chain. In TM, the recommendation from the recommender is highly emphasized for the trustworthiness. Collusion and wrong recommendations threaten the TM model, whereas making use of the recommendation is also the merit for the TM model when the recommendation is good, which is helpful to discover the quality of other peers even without any mutual interaction.

The current trust models have drawbacks as follow:

- Most existing trust models are developed for general-purpose P2P applications that emphasize distributed file-sharing. Little work has been done in establishing trust in e-commerce applications. Thereby, a lot of important information (such as the amount and value of transaction) has been ignored.
- Traditional trust models only consider the reputation accumulated by entity's long-term behaviors, and it is not adapt to dynamics of the behaviors.
- Traditional trust models have poor ability to cope with malicious behavior such as puffery and slandering attack.

In this paper, we focus on P2P-based trust model for e-commerce suitable for C2C or B2B transactions. The rest of the paper is organized as follows: The second section described some basic concepts used in our model. In third section, we set forth our approach and trust model in detail. Simulation and results are

IEEE International Conference on e-Business Engineering (ICEBE'06)
0-7695-2645-4/06 $20.00 © 2006 IEEE

discussed in section 4. Analysis of existing trust model and related works are outlined in section 5. At last we give a summarization for the paper.

2. Concepts and Definitions

When designing our trust model, we accepted some basic principles [8] as follows.

- A peer's trustworthiness value depends upon its good behavior, and it enhances slowly, however it drops faster while he/she had a bad behavior.
- When a peer often behaves badly and the trustworthiness value reduces to the threshold, it will be unauthentic.
- The calculations of the trustworthiness values include participants' direct interactions experiences and recommendations from others. The latter obtain more weight when no direct interactions experiences before.

In our model, we identify some basic metrics as trust parameter:

Feedback score. Reputation-based systems rely upon feedback to evaluate participant's trustworthiness. For instance, in eBay system, buyers and sellers rate each other after their transaction, the user's reputation is summed by all ratings (positive or negative). However, this approach is rough and is not well-function, as it does not consider various aspects of the participant's service quality such as merchandise price, delivery time etc.. Thus, Instead of a scalar value, we may use a vector composed of attribute factors to represent the participant's reputation value. Let RE(x,y) denotes an evaluation given by participant x for participant y at a transaction, and a_1, a_2, ... , a_n denote reputation attribute factors, then RE(x,y) can be computed as

$$RE(x,y) = (r_{a1}(x,y), r_{a2}(x,y),..., r_{an}(x,y)),$$

where $r_{ai}(x,y) \in [-1,1]$ denotes the feedback score given by x for y about attribute a_i.

Risk factor. Reputation on the valuee reflects an accumulative assessment value of the long-term behavior. However, it is not sensitive enough to perceive the suddenly spoiling peer because it needs time to decrease the accumulative score. Therefore we use risk evaluation to address this problem. Contrast to current reputation-based trust model, our model consists of both reputation and risk. Every peer has its own personalized views (such as transaction amount, recent behavior of the partner, etc.) about others and evaluates risk value itself. For example, one buyer may define risk as the ratio of his anticipative loss over profit.

Decay factor. Trustworthiness is not always remain the same value, because a partner's behavior maybe changed, or with the time going his trustworthiness value fallen off. There are two solutions to solve this problem. The first method is using damping function, that is assigning more weight to recent rating than old one. However it is difficult to choose a unique decay function for all peers, because different peers have different behavior patterns. Another is employing risk window to calculate the risk value. Only the behaviors of the valuee inside the window are taken into consideration, for example, if the size of risk window is five, then the last five transactions can affect the trustworthiness value. With the window shifting forward, the risk value reflects the fresh statistics of the valuee's recent behaviors. The smaller the window size is, the more the shorter-term assessment is favorite by the trustworthiness calculation.

Reliability of valuator. The valuator's reliability is important for a user to decide whether accept the reputation value of a peer or not. If the valuator has high reliability, his evaluation or recommendation will be trustworthy. Contrarily, if the valuator has low reliability, his evaluation or recommendation will be discounted or ignored. By introducing this parameter, a peer can avoid itself suffering from bad peer's attacks in some extent.

Value of transaction. In e-bay's feedback system, a user may gain good evaluation from a transaction cost 1$, and another user spends 10000$ to get the same reputation, this is unreasonable and it results in opportunistic behavior. Accordingly, value of transaction is taken into consideration in our trust model.

3. Design of Trust Model

In our trust model, we calculate a peer's trustworthiness by three steps: calculate direct reputation, assesses recommendation reputation and determine global reputation.

3.1 Calculates direct reputation

The direction reputation is derived from a peer's all direct transaction experience. The transaction satisfaction degree, transaction date and the transaction amount are main factors. Let T_d denotes the peer's direct reputation, S_i denotes the satisfaction value at a past transaction, γ denotes decay quotiety (for example γ=0.95) which reflecting the older transaction will gain the smaller weighs of ratings. Date and Trans_date represent current date and transaction date; we only select the transactions within a period(such as 100 days). Trans_value denotes the transaction value at a transaction, and Norm_value means the value in generally, for example, eBay given the norm value is

200$. Thus, we can use the following algorithm to calculate direction reputation.

Algorithm calc_direct_repu
$T_d \leftarrow 0$
$i \leftarrow 1$
while (i < n) and (Date - Trans_date <= 100)
if (Trans_value > Norm_value)
then
$T_d \leftarrow \gamma * T_d + S_i$
else
$T_d \leftarrow \gamma * T_d + (Trans\_value/Norm\_value) * S_i$
endif
$i \leftarrow i+1$
end while

After calculating the direct reputation, we compute the recommendation reputation.

3.2 Assesses recommendation reputation

In a fully distributed P2P system, peers rely on collective opinions from other peers. Let Tr denotes the recommendation reputation of peer i, S is the set of peers with whom peer i has conducted transactions, t_{ji} is the local trust score of peer i rated by peer j, and w_j is the aggregation weight of t_{ji}. We use the formula below to assess recommendation reputation of peer i.

$$T_r = \frac{\sum_{j \in S} W_j t_{ji}}{\sum_{j \in S} W_j} \qquad W_j > W_{th} \quad (1)$$

Where W_{th} denotes the trustworthiness threshold. In order to decrease the time consuming on the recommendation reputation aggregation, the system only queries qualified peers whose reputation is great than the threshold. For example, if the threshold is defined as 0.7, then the peer whose global_repu<0.7 will be disqualified from participating in the evaluation process.

We designed the prototype system on a DHT-based P2P overlay network which architecture similar to that of FuzzyTrust [10]. The DHT ring can provide fast message transmission and trust computation. In our model, each peer maintains two tables:

- **Transaction Record Table.** The table includes such fields: Peer_ID, Peer_score, trans_value, trans_date, global_repu. It maintains transaction records with remote peers.
- **Local Score Table.** This table contains two fields: Peer_ID and local_score. It maintains remote peers' evaluated trust scores. When performing global reputation aggregation, each peer queries the trust scores from remote peers.

3.3 Determines global reputation

The final step is aggregating the global reputation. Let T denote the global reputation of u to v, T_d is the direct reputation of u to v, T_r is the recommendation reputation of u to v. The values of T_d and T_r have been calculated in §3.1 and §3.2.

$T=\lambda * T_d + (1-\lambda) * T_r$ (2)

Where, the quotiety λ reflects weights of direct reputation and recommendation reputation, λ□[0,1], if peer u highly believes his experiences about peer v, λ value may be large than 0.5, otherwise small than 0.5.

4. Simulation and results

In this section, we will evaluate the performance our trust model. To validate our proposed trust model, we carried out simulation systems experiments with Java language. For comparison purpose, we also simulated other two trust models: eBay feedback system and Eigen model. Selcuk [9] sorted malicious behaviors as four: naïve, hypocritical, collaborative and pseudospoofing. Actually, the hypocritical peer is especially difficult to be identified and quite harmful, therefore we simulated this scenario. In distributed e-commerce environment, an important issue is increasing the ratio of successful transaction, so we attend to compare our model with the other two models against malicious attacks.

Experiment settings. Before the experiment begins, each peer will be assigned a random place, and the trust relationships between them will also be initialized randomly. During experiment, peers will interact with each other for specific times. We simulated 100 peers, which are honest or malicious, the ratios of malicious peers vary from 0% to 50%. Every malicious peer provides bad service at random. Each peer has 5 transactions at least. Other settings: Threshold Value=0.7, λ=0.5, γ=0.95.

Definition: Let TSR denotes transaction successful ratio, N represents the total transaction, N_s denotes successful transaction number, then

$$TSR = \frac{N_s}{N} \quad (3)$$

We use this metric to estimate the effectiveness of trust models against the behavior of malicious peer. The greater TSR is, the more effective the model is.

Figure 1 shows the simulation results. From the figure, we can see that when malicious peers are less than 10%, all the models have good performance. However, with the increase of malicious peers, TSR of eBay model reduces quickly. As in eBay system, the participants' trustworthiness is simply calculated by

the average value of evaluation, so it has no ability to stand against malicious peers. The Eigen model contains global trustworthiness factors, thus its performance is better than eBay system. Our model has a better performance than both other models, since it has the mechanism of punishment for malicious participants and considering the transaction metric, thus it can decrease malicious behavior influence.

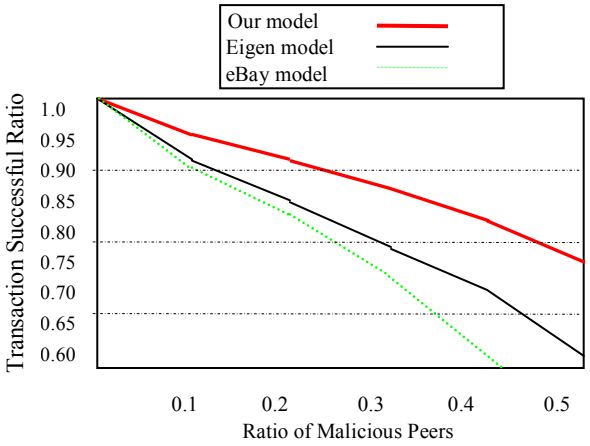

Fig. 1 Successful ratio at different malicious peers

5. Related work

Our work is benefit from a number of previous works for reputation-based system and P2P trust management system. Let us see several prominent trust models.

Centralized reputation systems are a very hot topic and have been widely deployed in e-commerce [1], [2]. EBay [3] is a Web online auctions site, its reputation system is called "eBay Feedback System" . Buyers and sellers can rate each other based on their past transactions, the rating may be positive, neutral, or negative. Sum all the point values of a member's transactions will obtain that member's reputation. Unfortunately, eBay's Feedback System can be compromised in several ways. For example, a seller (a malicious peer) may gain a high reputation score by filling many small orders (thereby attracting more buyers to his items for sale) but then collect money for a larger order and fail to deliver on the order. March's trust model [4] improves eBay Feedback System, but it had trouble when disposing negative trust and trust spreading mechanism. W. Zhang et al [5] present a C2C auction trust model with five basic parameters, Zacharia et al [6] propose an improved eBay-like trust model. But above two calculations are too complicated and the decision of quotiety value is at will. Recently, many decentralized reputation management occurred in the P2P domain, such as EigenTrust [7]. EigenTrust assumes that trust is transitive and addresses the weakness of the assumption and the collusion problem by assuming there are pre-trusted nodes in the system. EigenTrust is intended to decrease the number of downloads of non-authentic files in a P2P file-sharing network using a reputation model. In this scheme, each peer is assigned a unique global trust value, based on the peer's history of uploads. By having peers use these global trust values to choose the peers from whom they download, the network effectively identifies malicious peers and isolates them from the network. Liang et al [8] present a trust model, using the risk as the opinion of short-term trustworthiness and combining with traditional reputation evaluation to derive the trustworthiness. Song et al [10] present a new P2P reputation system based on fuzzy logic inferences, which can better handle uncertainty, fuzziness, and incomplete information in peer trust reports. PeerTrust [11] developed a P2P trust model so peers can quantify and compare the trustworthiness of other peers and perform trusted interactions based on their past interaction histories without trusted third parties. This model has three basic trust parameters and two adaptive factors in computing trustworthiness of peers.

6. Conclusion

In this paper, we try to introduce a P2P-based trust model into e-commerce. It brings a new decentralized approach to solve e-commerce safety issues. As consider of P2P technology and e-transaction characteristics, the model's performance has superiority than the other two trust model. In order to implement and test easily, we simplify the simulation experiment for our model and make comparison and analysis partially. In the future, we need more comprehensive test and evaluation on our trust model.

We anticipate combining several methods to improve the performance of the model, such as: using complex feedback rating vector, fuzzy inference, trust negotiations and so on.

References

[1] P. Resnick, R. Zeckhauser, E. Friedman, and K. Kuwabara. Reputation systems. Communications of the ACM 43(12), 2001.

[2] K. Aberer and Z. Despotovic. Managing trust in peer-to-peer information systems. Proceedings of the 10th International Conference on Information and Knowledge Management (CIKM'01), 2001.

[3] http://www.ebay.com.
[4] S. Marsh. Formalising Trust as a Computational Concept. Ph.D. thesis, University of Stirling, 1994.
[5] Wei Zhang, Lu Liu, Yanchun Zhu, A Computational Trust Model for C2C Auctions, Proceedings of ICSSSM 2005.
[6] G. Zacharia, A. Moukas and P. Maes, Collaborative Reputation Mechanisms in Electronic Marketplaces. Proceedings of the 32nd Hawaii International Conference on System Sciences, 1999.
[7] S. Kamvar, M. T. Schlosser, and H. Gacia-Molina. The eigentrust algorithm for reputation management in P2P networks. Proceedings of the 12th International World Wide Web Conference, 2003.
[8] Z. Liang, W. Shi, PET: A PErsonlized Trust Model with Reputation and Risk Evaluation for P2P Resource Sharing, Proceedings of the 38th Hawaii International Conference on System Sciences, 2005.
[9] A. A. Selcuk, E. Uzun, M. R. Pariente, A Reputation-Based Trust Management System for P2P networks. http://www.cs.bilkent.edu.tr/~selcuk/publications/CCGRID04.pdf
[10] Shanshan Song, etc. Trusted P2P transactions with fuzzy reputation aggregation. IEEE Internet computing, 2005(11-12).
[11] Li Xiong, Ling Liu. A reputation-based trust model for peer-to-peer ecommerce communities. Proceedings of the IEEE Conference on ECommerce, June 2003.