Research and Application of Trust Management System

Fengyin Li and Peiyu Liu

Abstract Trust status of a service provider is critically important to potential buyers in electronic commerce (e-commerce), particularly when they are unknown to each other, while trust establishment and trust accumulation are still key problems need to be solved. By defining new trust architecture and introducing new concepts of trades' turnover and trust decline, a trust management model was proposed in this paper. In the new architecture, events were divided into two categories and rules were predefined to determine which formula to use according to the feature of the events occurred during the electronic transaction. In the new trust calculation method, the concepts of trades' turnover and trust decline were first introduced to further depict the dynamic feature of trust status. Further, to adapt to different application domains, formulae with variable parameters were adopted. Simulation results show that the proposed model precisely implements the long and incremental characteristics of trust establishment process.

Keywords Trust management · Trust evaluation · Electronic commerce

1 Introduction

The concept of trust management was proposed by Blaze in 1996 [1]. It aimed to solve the security problems in Internet applications and provided a security policy framework adapted to open and dynamic network application systems. In

F. Li (✉) · P. Liu
School of Information Science and Engineering, Shandong Normal University, Jinan, China
e-mail: lfyin318@126.com

P. Liu
e-mail: liupy@sdnu.edu.cn

F. Li
School of Computer Science, Qufu Normal University, Rizhao, China

S. Patnaik and X. Li (eds.), *Proceedings of International Conference on Soft Computing Techniques and Engineering Application*, Advances in Intelligent Systems and Computing 250, DOI: 10.1007/978-81-322-1695-7_15, © Springer India 2014

electronic commerce (e-commerce), a variety of electronic transactions (e-transactions) are implemented in a loosely coupled network environment. In most cases, both sides of the e-transaction do not know each other, neither of them is willing to be cheated, and this makes trust management a very challenging and critical issue.

In e-transaction, the dynamic trust status of a seller always plays a decisive role in real-time e-transaction systems, and more factors (such as trades' turnover, trust decline, and goods types) should be considered to precisely reflect the latest trust status of each seller. Furthermore, a better incentive mechanism should be studied to better reflect the evolution of trust values. In trust evolution, positive events and negative events play completely different roles. So, not only incentive rules but also punishment rules should be included in the incentive mechanism. Further, the incentive scale and the penalty scale should vary from event to event and from domain to domain. The most important is that trust establishment is a long and incremental process. Even if a "good" service provider behaves very well, it takes an enough long time for him to obtain a high reputation value.

To solve the problems discussed above, a trust management model for e-commerce applications was proposed in this paper. The new model was composed of a centralized trust management architecture and a trust calculation method. In the new architecture, events were divided into two categories and rules were predefined to determine which formula to use and what arguments to use according to the events occurred during the e-transaction. By first introducing the concepts of trades' turnover and trust decline, based on formulae, a new trust calculation method was proposed. The used formulae were designed to adapt to different application domains by revising corresponding arguments. Simulation results show that the proposed model addresses the long and incremental characteristics of trust establishment process.

The rest of this paper was organized as follows. In Sect. 2, we presented the rule-based and event-driven trust management architecture. In Sect. 3, the formula-based trust computation method was proposed. Some empirical study results were illustrated in Sect. 4. In Sect. 5, we concluded our work.

2 Trust Management Architecture

Centralized trust management architecture (like eBay) for e-commerce applications was proposed in this section (Fig. 1). The trust management server was responsible for the storage and management of all trust data and other related information. System clients (buyers or sellers) reported the rating of the other side of the transaction to the trust management server after every transaction.

We assumed the centralized trust management server was independent of any system client. This makes it feasible to apply the unified evaluation approach to the same domain of applications. In addition, it ensures that the trust computation could be completed on relatively complete trust data, which is difficult in a decentralized architecture. Certainly, the centralized architecture is vulnerable to a

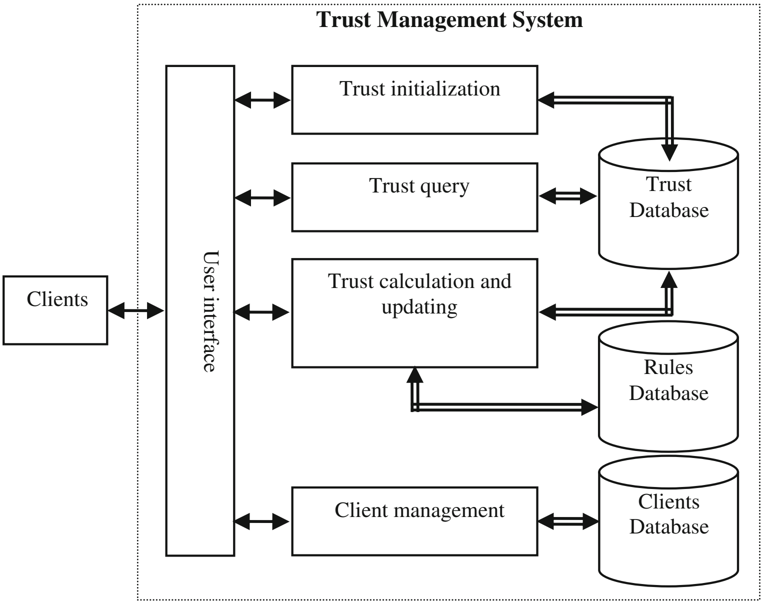


Fig. 1 Trust management architecture

single point failure due to the scale expansion problem, which is less risky in the decentralized environment.

In Fig. 1, all clients' requests were sent to the user interface module, which would distribute the requests to the trust initialization module, the trust query module, the trust calculation, and updating module or the client management module according to the feature of each request. The trust initialization module was in charge of the allocation of an ignorance trust value (e.g., 0.1) to each new comer. The final trust value of each new comer depended on its subsequent behavior performance. The trust query module mainly responded the trust requests by querying the trust database. The trust calculation and updating module afresh calculated and updates the trust value of a client as long as a new valid rating of that client was produced. When positive cases or negative cases happened, the incentive or punishment rules could be used to reward or punish a client during the trust calculation process. The incentive scale and penalizing scale were also predefined as variable parameters.

3 Trust Evaluation Method

In this section, a formula-based trust calculation method was proposed. In the new trust calculation method, the concepts of trades' turnover and trust decline were first introduced into trust management to depict the dynamic feature of trust status.

In different domains, there may be different policies for trust evaluation. The used formulae could be applied into different domains by setting different arguments. In addition, in the case of penalty, the decrement was determined by arguments, which were selected according to the nature of negative events.

Definition 1 Let T_i^x denote the trust value of target service provider x at current time period t_i, R_{i+1}^x be the rating of x at time period t_{i+1}, and $\Delta = R_{i+1}^x - T_i^x$. The trust value of x at time period t_{i+1} was defined in Eq. (1).

$$T_{i+1}^x = \begin{cases} \min\left(1, T_i^x + \lambda_+ \cdot \theta \cdot \Delta\right) & \text{if } \Delta \geq 0 \\ \max\left(0, T_i^x + \lambda_- \cdot \theta \cdot \Delta\right) & \text{if } \Delta < 0 \end{cases} \tag{1}$$

where $0 \leq \theta < 1$ was the impact factor function determining the impact of recent change (i.e., Δ) on trust calculation, and $\lambda_+ \leq 1$ (or $\lambda_- \geq 1$) factor determining the incentive (penalty) scale of trust change. From the arguments, we can see that the penalty scale is no less than the incentive scale. That is, the improvement of trust value is more difficult than the drop of it.

Formula (1) yielded a value in the range of [0, 1]. To obtain the trust value in period t_{i+1}, the trust value in period t_i and the latest rating value were used.

We assumed that in time period t_i the service provider x received such valid rating values as $R_{i_1}^x, R_{i_2}^x, \ldots, R_{i_m}^x$ and the corresponding transaction prices as $P_{i_1}^x, P_{i_2}^x, \ldots, P_{i_m}^x$, and then the ultimate rating R_i^x of x in period t_i could be obtained as Eq. (2).

$$R_i^x = \sum\nolimits_{j=1}^{m} \left(R_{i_j}^x \cdot P_{i_j}^x / \sum\nolimits_{k=1}^{m} P_{i_k}^x \right) \tag{2}$$

That is, we used the rating value and the corresponding trades' turnover of each transaction to calculate the ultimate trades rating in every time period. In this way, we first considered price feature in trust calculation to promote the accuracy of trust evaluation system.

According to trust principles, the impact factor function should be a decreasing function whose decrement is decreasing. There may be more than one function to depict the feature, and we just selected a simple one of them.

The impact factor function was defined as follows.

Definition 2 If the current trust value was T_i^x, the *impact factor function* was defined in Eq. (3).

$$\theta\left(T_i^x\right) = C/(T_i^x + C)^2 \tag{3}$$

where $C > 0$ is a constant parameter affecting the curve shape of function θ.

Based on the same principles, we selected a decreasing function whose decrement was increasing as our trust decline function, which was defined as Eq. (4).

Definition 3 If a service provider got no valid rating values after time period t_i, the trust value decline function was defined as Eq. (4).

$$T(t) = T(t-1) - (t - t_i)/D \tag{4}$$

where t stands for time, and D is a constant parameter.

From the above discussion, we can see that, when $\Delta \geq 0$, according to formulae (1)–(3), there would be an increment in the trust calculation, namely $T_{i+1}^{x} \geq T_{i}^{x}$. In this case, we set $\lambda_{+} = 0.9$. Thus, the increment would be $\lambda_{+} \cdot \theta(T_{i}^{x}) \cdot \Delta$. When $\Delta < 0$, there would be a decrement in the trust calculation. By definition, we set $\lambda_{-} = 1$. As $\lambda_{+} \leq \lambda_{-}$, assuming the same $|\Delta|$ and T_{i}^{x}, the decrement $\lambda_{-} \cdot \theta(T_{i}^{x}) \cdot |\Delta|$ was no less than the increment $\lambda_{+} \cdot \theta(T_{i}^{x}) \cdot \Delta$. This indicates that it is not easier to improve the trust value than to worsen it. Therefore, generally it takes longer time to reach a high-level trust value (e.g., 0.98) than to drop from a high level to a low level. The value of λ_{+} (or λ_{-}) was determined by the predefined rules in different applications. In addition, if a severely negative event happened, λ_{-} would be applied for decrement cases. This also results a harder trust improvement process.

4 Simulation and Application

To further study the properties of our proposed approaches, a set of empirical studies were conducted in this section, and the results were illustrated and analyzed. For trust computation, the formulae discussed in Sect. 3 were adopted.

4.1 A Simulation

In this section, we compared the trust establishment process of several service providers with different system entry periods and different trust levels, and we aimed to compare their reputation levels delivered by the proposed model. We studied the trust establish process of new service providers and the trust accumulating process of old service providers. To avoid the whitewashing behaviors, the initial trust value was set to $T_0 = 0.1$, an ignorance initial value. We assumed that there were 5 service providers and they were marked as S_1, S_2, S_3, S_4, and S_5. In each time round, S_1 got a static rating of 0.95. S_2 got a static rating of 0.9 in the former 149 rounds, and at round 150 it got a rating of 0.2 due to an extremely negative case, and then, its ratings stayed at 0.6. S_3 got a static rating of 0.8 in the former 100 rounds, but at the following rounds, its trust value decayed based on the formula (4) due to lacking of valid ratings, while S_4 and S_5 attended at round 150 and got their static ratings of 0.95 and 0.7.

The simulation curve with above 5 service providers is shown in Fig. 2, and Fig. 3 shows the same simulation curve with a rating deviation of $|\varepsilon| \leq 0.1$. In the above figures, we obtained the curves by setting the arguments $\lambda_{+} = 0.9$, $\lambda_{-} = 2$, and $C = 20$.

Fig. 2 Simulation curves

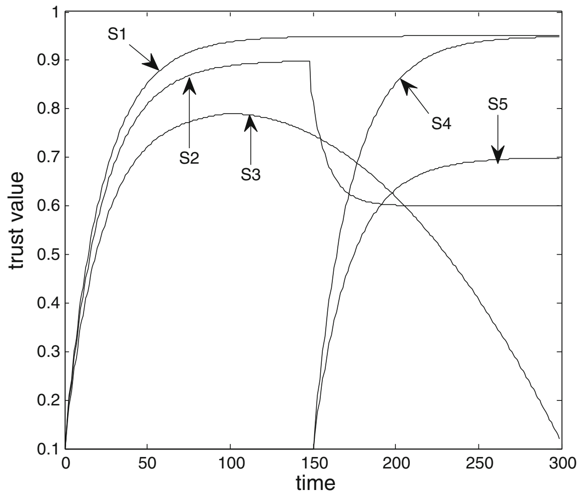
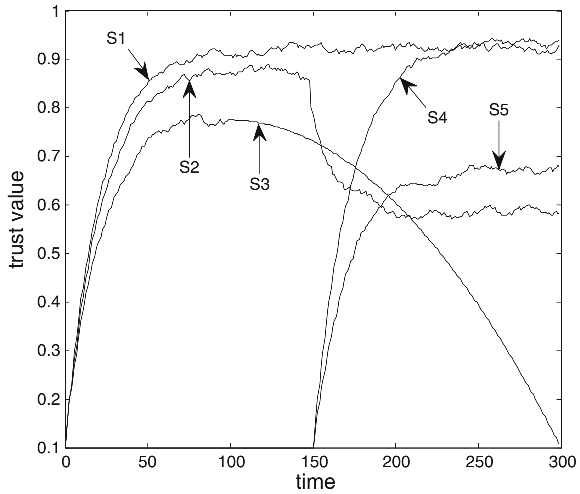


Fig. 3 Simulation curves with R deviation $|\varepsilon| \leq 0.1$



From the simulation curves, we can see that the trust curves could depict the dynamic trust status of every service provider, that is, the service providers with the same trust values have the same trust levels. Obviously, our trust model could accurately depict the trust changes in different situations.

4.2 Performance Discussion

Compared with trust evaluation method in the literature [2–4], the proposed trust evaluation method could differentiate positive events and negative events by set scale control factors λ_+ and λ_-, and further the scale control factors could vary from domain to domain by setting different parameters. Compared with the trust management model in the literature [5–7], the new trust model introduced such factors as trades' turnover, incentive scale, penalty scale, and trust decline into trust evaluation process and could more precisely depict the trust establishment process. Compared with the scheme in the literature [8–10], the new trust model selected a simple function with variables to avoid the hyperbolic tangent transformation and so greatly improved the efficiency of trust evolution. By setting different variable parameters, the proposed trust evaluation method could be applied into different fields. Furthermore, the new trust model implemented the long-term and incremental trust establishment process and could solve the open trust problems discussed above.

In the new trust model, due to the implement of the long-term and incremental process of trust establishment and accumulation process, the trust value of each client precisely depicted its trust status. That is, the service providers with the same trust value must have the same trust reputation level, and vice versa. And so in the new trust model, we do not need to differentiate the clients with the same trust values and the above trust issues has been completely solved.

5 Conclusions and Future Work

In this paper, a trust management architecture and a trust evaluation method were proposed. The new trust model has some advances in the following aspects. The features of the new model are critically important to a trust management service authority with a large pool of system clients.

1. It is incentive to good service providers with good service quality for a long service period.
2. It is incentive to new service providers.
3. It penalizes service providers with poor service quality.
4. For service providers who are not active, their trust values will decay in a special way, until eventually into zero or a valid rating is obtained.

All these properties aim to provide clearer information to service clients and prevent some service providers from cheating clients after obtaining a good reputation rank.

For future work, more impact factors (e.g., the varieties and properties of different goods) will be studied in trust management model. The distributed trust management architecture for e-commerce applications will also be studied. In addition, in order to better ensure the fairness of the trust model, the trust status of service clients (buyers) will be further studied in e-commerce applications.

Acknowledgments This work is partially supported by National Nature Science Foundation of China (61373148), National Social Science Foundation of China (12BXW040), Nature Science Foundation of Shandong Province of China (ZR2012FM038), and Science & Technology

Foundation planning Project of Colleges and Universities of Shandong Province of China (J12LN07). The authors also gratefully acknowledge the helpful comments and suggestions of the reviewers, which have improved the presentation.

References

1. Blaze M., Feigenbaum Jand Lacy, J.: Decentralized trust management. In: Proceedings of the 17th Symposium on Security and Privacy, pp. 164–173. IEEE Computer Society Press, Oakland (1996)
2. Qureshi, B., Min, G., Kouvatsos, D.: A distributed reputation and trust management scheme for mobile peer-to-peer networks. Comput. Commun. **35**(5), 608–618 (2012)
3. Denko, M.K., Sun, T., Woungang, I.: Trust management in ubiquitous computing: a Bayesian approach. Comput. Commun. **34**(3), 398–406 (2011)
4. Omar, M., Challal, Y., Bouabdallah, A.: Certification-based trust models in mobile ad hoc networks: a survey and taxonomy. J. Netw. Comput. Appl. **35**(1), 268–286 (2012)
5. Cho, J.H., Swami, A., Chen, I.R.: Modeling and analysis of trust management with trust chain optimization in mobile ad hoc networks. J. Netw. Comput. Appl. **35**(3), 1001–1012 (2012)
6. Manzanares-Lopez, P., Malgosa-Sanahuja, J., Muñoz-Gea, J.P.: The importance of considering unauthentic transactions in trust management systems. J. Parallel Distrib. Comput. **72**(6), 809–818 (2012)
7. Sun, J., Sun, Z., Li, Y., et al.: A strategic model of trust management in web services. Phys. Procedia **24**(B), 1560–1566 (2012)
8. Wang, Y., Varadharajan, V.: Interaction trust evaluation in decentralized environments. In: Proceedings of the 5th International Conference on Electronic Commerce and Web Technologies (EC-Web'04). Lecture notes in Computer Science, vol. 3182, pp. 144–153. Zaragoza, Spain (2004)
9. Zacharia, G., Maes, P.: Trust management through reputation mechanisms. Appl. Artif. Intell. **14**(9), 881–908 (2000)
10. Wang, Y., Lin, K.J., Wong, D., et al.: Trust management towards service-oriented applications. SOCA **3**(2), 129–146 (2009)