International Journal of Computational Intelligence Systems, Vol. 5, No. 5 (September, 2012), 905-912

A Complex Estimation Function based on Community Reputation for On-line Transaction Systems

Yu YANG*
Information Security Center, Beijing University of Posts and Telecommunication
National Engineering Laboratory for Disaster Backup and Recovery, Beijing University of Posts and Telecommunications
Beijing, 100876, China

Shang-bao GONG, Yu-cui GUO
School of Science, Beijing University of Posts and Telecommunications
Beijing, 100876, China

Min LEI
Information Security Center, Beijing University of Posts and Telecommunications
Beijing, 100876, China

Yan YANG
State Key Laboratory of Rail Traffic Control and Safety, Beijing Jiaotong University
Beijing, 100044, China

Received 4 November 2011

Accepted 15 June 2012

Abstract

A reputation management system is crucial in online transaction systems, in which a reputation function is its central component. We propose a generalized set-theoretic reputation function in this paper, which can be configured to meet various assessment requirements of a wide range of reputation scenarios encountered in online transaction nowadays. We analyze and verify tolerance of this reputation function against various socio- communal reputation attacks. We find the function to be dynamic, customizable and tolerant against different attacks. As such it can serve well in many online transaction systems such as e-commerce websites, online group activities, and P2P systems.

Keywords: Reputation estimation, Timeliness, Community reputation, Attack tolerance.

1. Introduction

Trust and reputation are both necessary conditions for trustworthy interactions, and also essential for social cooperation and collective actions. Additionally, they are important in peer-to-peer (P2P) networks for transaction, especially in a virtual community and in an on-line transaction system. In a P2P network, peers will cooperate to perform a critical function in a decentralized manner. All peers are both consumers and producers of resources and can interact with each other directly without intermediate peers. Compared with a

*Corresponding author: yangelm@vip.sina.com

centralized system, a P2P system can construct a simple framework to aggregate large amounts of resources in the Internet or Ad-Hoc networks with a low cost. As such, P2P systems have recently attracted much attention from researchers, even though they have certain security problems.

Trust and reputation are related with each other in a network. When an entity without any direct experience about its other side wishes to trade, it normally tends to consider the reputation of the other side seriously through computing its trust values in the network. Interacting with entities having bad reputation would be avoided instinctively. Most of existing reputation management systems utilize information obtained from past transactions. However, these systems often employ some simplistic reputation functions that cannot calculate the reputation of entities accurately because the functions merely aggregate the positive and negative opinions from the past transactions. Therefore these reputation management system tend to be faulty and vulnerable.

In order to address this above problem, we in this paper propose a new reputation management system, which offers a feasible solution to encourage trustworthy behaviors and guarantee security of transactions in P2P networks. Our proposed system is based on two key hypotheses: First, participants of an online transaction system engage in repeated interactions; and second, past transaction information of participants is indicative of their future behaviors. Therefore, we expect that it will enhance the trustworthiness of the participants to collect, arrange, process and disseminate the feedback about the participants' behaviors in the past.

We in this paper describe a practical and efficient reputation system based fuzzy-logic, in which different factors are used to evaluate reputation in various scenarios adaptively, leveraging fuzzy-logic's ability to handle uncertainty, fuzziness and incomplete information. The timeliness of a transaction record is considered in reputation computation as well. Our main goal is to construct a generic system that is dynamic, customizable and simultaneously can stand its ground in face of different types of attacks.

The rest of the paper is organized as follows. Section 2 reviews latest research results of reputation management systems. Section 3 proposes a social-transactional model of a generalized reputation management system framework. Section 4 presents our simulation results. This paper is concluded with a brief summary in Section 5.

2. Related Work

Reputation has long been regarded as a necessary condition in constructing stable social orders since the sixteenth century[1]. Today, the so-called feedback-based reputation systems are widely used in on-line communities, such as Wikipedia, and in P2P systems and e-commerce services such as Yahoo auction, eBay, Amazon, etc. A majority of these reputation systems use only feedbacks from users as a factor to calculate reputation[3]. The reputation is simply measured by the addition of positive and negative feedbacks, i.e., computed by a simple summation equation.

A larger number of improved reputation management systems have been proposed. Many of them were designed specifically for P2P systems[2,6,13-15]. J. I. Khan and S. S Shaikh[2] proposed a generalized set-theoretic phenotype reputation function in which its specific components can be customized to meet different reputation requirements of a wide range of reputation assessment needs encountered in today's online activities. It can resist against various socio-communal reputation attacks such as gang attacks, vendetta and Dr. Jekyll & Mr. Hyde. A fuzzy trust recommendation based on collaborative filtering was proposed in 2009[6]. It stimulated collaboration among distributed computing and communicating nodes, facilitated the detection of untrustworthy nodes, and assisted decision-making in various protocols for MANETs. Its trust model combined direct trust and trust recommendation information based on collaborative filtering to allow nodes to represent and reason with uncertainty and imprecise information regarding other nodes trustworthiness. Simulation results showed that the model was flexible and valid. F G Mármol and G M Pérez[13] presented a pre-standardization approach for trust and/or reputation models in distributed systems. A wide review of them was carried out, extracting common properties and providing some pre-standardization recommendations. A global comparison was performed for the most relevant models against these conditions, and an interface proposal for trust and/or reputation models was proposed. J Lopez, and et al.[14] listed the best practices that we consider are essential for developing a good trust management system for wireless sensor network (WSN) and made an analysis of the state of the art related to these practices. However, for the spectrum of distributed applications, no generic function exists yet that is applicable to the on-line transaction systems. All these existing models consider reputation as a global property. More severely, they all use a single variable that is independent on the context, and do not provide explicit mechanisms to deal with entities providing false information. The last but not the least, they do not take into account the effects and consequences of various attacks that can be launched by a hostile individual or a group[5].

3. Reputation Model Based On Transaction Records

In this section, a social-transactional model of a generalized reputation management system framework is proposed. Any transaction record involves three parties: producer, product, and consumers who provide feedback. However, the components of a product also contribute to reputation, such as the author's reputation, materials and so on. Furthermore, each transaction occurs in a communal context, so the reputation of the community will also affect the peer's reputation. E.g., a particular kind of product is sold repeatedly, but perhaps to different consumers, or perhaps produced by different producers. Similarly, a consumer may buy various products, thus there is a set of consumers, a set of producers and a set of products. The transactions collectively build up a memory about a target individual, which is estimated by target's reputation function, and then its value is useful to establish trust in subsequent transactions involving the target in communities.

A generic reputation function seems to be based on various peers and group properties. However, depending on the environment of deployment, some of the peer and group properties would be included while others omitted when quantifying the reputation of the peer.

There are several factors which potentially contribute to reputation. Here, we mainly adopt the following important factors to compute the reputation of the peer in the community: (1) the opinion about the transaction received from another peer, (2) the total number of transactions/interactions that the peer has performed, (3) the reputation of the opinion provider, (4) the timeliness of the evaluation about the transaction, (5) the community context factor.

3.1. *Transaction Opinion (O)*

In each collaborative community, a feedback is an indicator of how efficiently and honestly a peer carries out its side of a transaction. This is the estimate expressed by one member of the community about another. In many on-line reputation management systems such as eBay, the reputation of a peer is simply an average or summation of the received feedbacks about various transactions, which is denoted by Eq. (1):

$$R = \sum_{j=1}^{n} O_j \qquad (1)$$

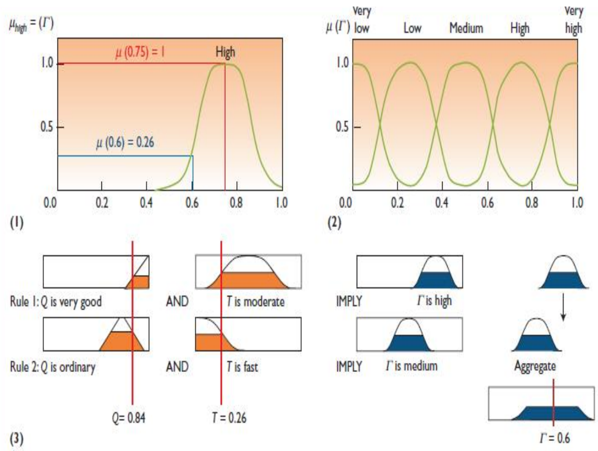

Fig. 1. Fuzzy logic inference and application.

In such a system, the buyer can give a positive (+1), a negative (-1) or a neutral (0) feedback. The reputation of the peer is computed as the sum of these feedbacks. By this equation (Eq. 1), it is hard to distinguish the reputation of a person who has performed 100 good transactions (reputation=100) and the one who has performed 110 good transactions and 10 bad transactions (reputation = 110 – 10 = 100). In our paper, a fuzzy-logic approach is introduced to evaluate the reputation of the peer, for fuzzy theory has demonstrated its power in managing uncertainties and mimicking the human decision-making process. Figure 1 shows how to use the fuzzy logic tools to handle the opinions about the transaction and how to calculate the reputation.

It shows the fuzzy membership functions and the fuzzy reputation aggregation procedure. By Fig. 1, we show (i) the high membership function of a local score (Γ), (ii) five levels of membership functions of Γ, and (iii) the application of two rules to induce the seller's evaluation.

3.2. *Reputation of the Opinion Provider (PR)*

Whenever a peer expresses an opinion, many social scenarios seem to take into account that who exactly is providing this opinion. The opinion from those with higher reputation is often weighted more heavily than those with lower reputation. While some systems, such as most voting systems, do not distinguish between opinion providers.

3.3. *The Timeliness of the Record (T)*

For two entities which have had interactive records in previous time, we suppose that entity *A* saves entity *B*'s set of their interactive record $R_{A\to B}(S,F)$, where *S* is the record set of successful interactions, *F* is the failure set of interactive record. Assuming set $S=(s,\alpha(i,m_k),t_i)$, where s is the number of successful interactions, $\alpha(i,m_k)$ is the successful satisfaction of property m_k on i -*th* interaction, $\alpha(i,m_k)\in[0,1]$, t_i is the time when the i -*th* record of successful interaction occurred. Suppose that set $F=(f,\beta(j,m_k),t_j)$, where f is the number of unsuccessful interactions, and $\beta(j,m_k)$ is the failure of property m_k on j -*th* interaction, $\beta(j,m_k)\in[-1,0]$, t_j is the time when the j -*th* record of failure interaction occurred. Obviously, the interactive record can be considered as the timeliness, namely the last time interaction records can be more indicative. The timeliness of i -*th* successful interactive record is quantified by the formula below:

$$st_i=\begin{cases}\exp(t_i-t_{sys}) & \text{entity A}\in\text{IRset}\\ \dfrac{1}{\ln(t_{sys}-t_i)} & \text{entity A}\in\text{HRset}\end{cases}\qquad(2)$$

The timeliness of j -th failure interactive record is quantified by the following formula:

$$ft_j=\begin{cases}\exp(t_j-t_{sys}) & \text{entity A}\in\text{HRset}\\ \dfrac{1}{\ln(t_{sys}-t_j)} & \text{entity A}\in\text{IRset}\end{cases}\qquad(3)$$

Where t_{sys} denotes the current time of the system. The larger the timeliness is quantified, the newer the record is, which will have the greater influence on the trust calculation. The smaller the timeliness is quantified, the older the record is, thus it will have the less influence on the trust calculation.

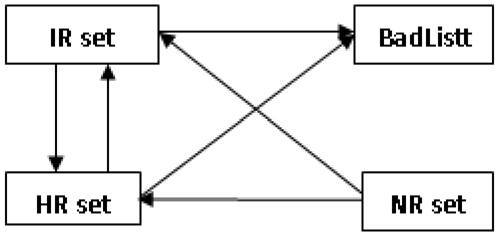

Fig. 2. The transition among entity's HR set, IR set NR set and BadList.

From the sociological viewpoint, different information sources have different credibility, and according to the reputation, the entities can be classified into HonestRater, InteractRater, NewRater and BadList, and so on. For entity i,

HonestRater is defined as *i*'s most trusted entities or recognized honest entities, and friend entities forms the trusted entities set (HR set).

InteractRater is defined as peers who have interactive history with peer *i*, and neighbour entities compose neighbour set (IR set).

NewRater is defined as peers who have not interactive history with peer *i*, and strange entities constitute strange set (NR set).

BadList is a set of malicious entities.

Entities in HR set, IR set and BadList can transform under certain conditions. Fig. 2 shows the transitions among entity's HR set, IR set, NR set and BadList.

3.4. *Number of Transactions (N)*

Generally, the larger the amount of transactions is, the more credible the entity is in the transaction. However, the amount contributes to the reputation in quite complex ways. It seems that at the early count stages, amount tends to play more critical role than at higher count stages. There might be some logarithm normalization involved. Some scenarios tend to ignore the amount at all. Transaction count also contributes to estimating distribution of past outcomes, which is very critical as one of its main usages is to determine the probability of a certain outcome. As we have mentioned earlier the summation of a peer, in this system, a peer can hide his misbehaviors by simply increasing the volume or amount of transactions he involves in. Thus, the total amount of transactions is an important factor in determining the reputations of different peers.

3.5. *The Reputation of the Community (CR)*

A peer with a high individual reputation will usually be associated with a community whose members are also highly reputed. However, when the reputation of a peer in the community increases, it will demand other members in this community to conduct some good behaviors in order to increase their reputations as well. Consequently, community reputation becomes an important factor in our model. The peers who have the same or similar interests form a community, and the average of the reputations of all the members of a community is the community reputation. So it will be an indicator of the credibility of the opinion provider. Since low community reputation affects the good peer, the good peer will have an incentive to encourage the other members to conduct honest transactions. This will have a dual effect. Firstly, the other members will stop misbehaving, and secondly, the good peer will be rewarded for encouraging other members of his community to be honest.

Because the peers in the community have the same or similar interests, we introduce Gauss-bar function to evaluate the similarity. Let $set(i)$ denote the peers in a set that interacts with peer i and let $set(j)$ denote the peers in a set that interact with peer j. For each peer $k \in set(i) \cap set(j)$, we have:

$$\Delta_k = \sum_{n=1}^{N} \omega_{kn} \exp[-\frac{1}{2}(\frac{x_{kn} - \mu_{kn}}{\sigma_{kn}})^2] \quad (4)$$

Where coefficient ω_{kn} is weighted value, and $\sum_{i=1}^{N} \omega_{ki} = 1$, ω_{kn} is set by peers themselves, $\mu_k = (\mu_{k1}, \mu_{k2}, \cdots, \mu_{kN})$ is k^{th} center, which is the k^{th} community's reputation, and will be computed by maximum likelihood estimation[12].

Assuming the service satisfaction provided by peers in $set(j)$ obeys the normal distribution $N(\mu, \sigma^2)$, and the feedback evaluation of $set(j)$ is denoted by $X = (x_{i1}, x_{i2}, \cdots, x_{in})$. The peer i can estimate the parameter μ through the method of maximum likelihood estimation on $set\ X$. The process is as follows:

(1) Randomly choose m elements for $set\ X$, and sort these elements.

(2) Randomly select $x_{i,\lceil ma+1 \rceil}, x_{i,\lceil ma+2 \rceil}, \cdots, x_{i,\lceil ma+m \rceil}$ from a subset of m ordered elements, where $a \in (0, 0.5)$. The likelihood function is denoted in the formula below:

$$\begin{aligned} &L(x_{i,\lceil ma+1 \rceil}, x_{i,\lceil ma+2 \rceil}, \cdots, x_{i,\lceil ma+m \rceil}; \mu, \sigma^2) \\ &= \prod_{i=\lceil ma+1 \rceil}^{\lceil ma+m \rceil} \frac{1}{\sqrt{2\pi\sigma}} \exp(-\frac{(x_i - \mu)^2}{2\sigma^2}) \\ &= (\frac{1}{2\pi\sigma^2})^{\frac{\lceil m+ma \rceil}{2}} \exp[-\frac{1}{2\sigma^2} \sum_{i=\lceil ma+1 \rceil}^{\lceil ma+m \rceil} (x_i - \mu)^2] \end{aligned} \quad (5)$$

Taking the logarithmic operation on formula (5) can calculate the partial derivative operation on the equation above for μ. The estimated feedback evaluation from peer i to peers in $set(j)$ can be denoted by $\hat{\mu}$ in formula (6):

$$\hat{\mu} = \frac{1}{m + 2 * \lceil ma \rceil} \sum_{i=\lceil ma+1 \rceil}^{\lceil ma+m \rceil} x_i \quad (6)$$

By the method above, we can actually compute the community reputation.

3.6. *Complexity function*

To obtain the relationship of the above factors, a complex function has been constructed to compute the reputation of the peer. To describe the direct influences introduced by aforementioned variables, each variable can be quantified by using different methods. Finally, we put all the variables together to form a generic reputation function, which satisfies the requirements discussed in the previous sections and binds them together into a customizable and consistent formula. We call it as "*Complex Reputation Function*".

$$R=\sum_{k=1}^{m}\omega_k\frac{\sum_{i\in Sset(i)}\alpha_i*O_i*T_i*PR_i/CR_i+\sum_{j\in Fset(j)}\beta_j*O_j*T_j*PR_j/CR_j}{N}$$

$$=\sum_{k=1}^{m}\omega_k\frac{\sum_{i=1}^{s}\alpha_i*O_i*st_i*PR_i/CR_i+\sum_{j=1}^{f}\beta_j*O_j*ft_j*PR_j/CR_j}{s+f}$$

Where $Sset(i)$ and $Fset(i)$ denote the peers' set of successful and failure transactions; m is the number of peers who have interacted with it; ω_k expresses the weight.

4. Simulation Results and Analysis

For brevity, each peer in our system plays only one role at a time, either the role of service provider or the role of requester. These peers belong to IR set, NR set, HR set and BadList. At the beginning, peers are separated by their behaviors into good, bad and neutral peers. A good peer will always behave well when serving a request from another peer. A bad peer will provide bad services. A neutral peer will be neutral between providing good and bad service. Recommenders can be separated by their behaviors into honest and malicious peers. The malicious peers include exaggerated, slanderous and collusive peers.

Fig. 3 reflects the changing trend of different services providing peers' global reputation along with the increase of transaction time. Fig. 3 portrays the changing trend of the global reputation of peers of different service types when the proportion of the malicious peers is 50%, the reputation of good peers can be higher than bad peers, and the global reputation of neutral peers at the beginning drops greatly, but with the increase of transactions, its global reputation tends to be lower. When malicious peers become the mainstream, the global reputation of all types of peers degrades. But the good peers' reputations are still higher than those of the bad peers. The bad peers cannot increase their global reputation in this way.

Naturally, the full tolerance of attack can not be achieved just in estimation function. It requires an integrated approach involving other components of on-line transactional system, particularly involving identity management, authentication and non-repudiation process of the overall system. A good reputation function should help with detection. Based on this complex reputation estimation function and reputation management system frame, we prepare to do some simulations which can tolerate the individual or group attacks. Through simulations, we show the behaviors of the functions under various attack signatures.

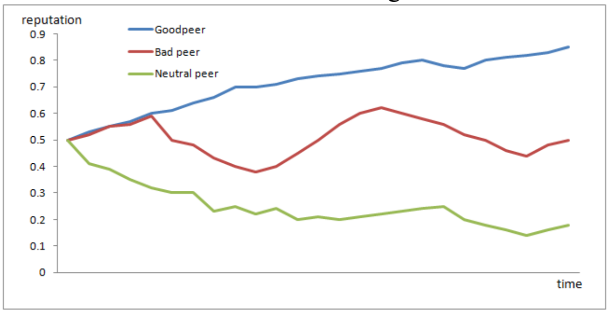

Fig. 3. Trends of reputation when there exist 50% malicious peers.

By changing the ratio of honest and malicious peers among 500 peers, we observe the whole network computing error rate, and the probability of honest service provided after a certain number of transactions. Fig. 3 shows the effect of rate of malicious peers in trust computing phase. Obviously, both PeerTrust and DynamicTrust are efficient when malicious peer ratio is less than 0.4. However, when the ratio exceeds 0.5, trust computation error of PeerTrust is rapidly promoted, while DynamicTrust is relatively steady.

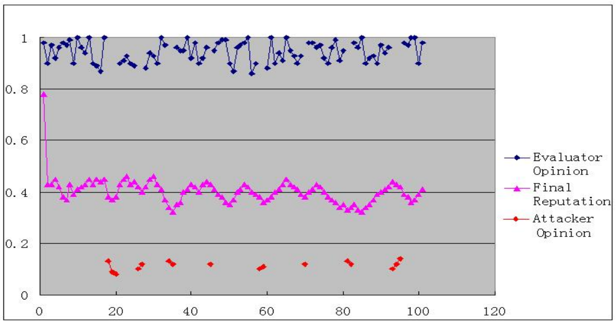

Fig. 4. Behavior of the reputation when the attacker has a random personal reputation.

Fig. 4. shows that the reputation of the peer does not change when the attacker has a random personal reputation. Overall from Fig. 3 we can infer that personal attack has very limited or damaging effect on the target reputation if the attacker frequency is low but can have a considerable impact in case of higher attacker frequency.

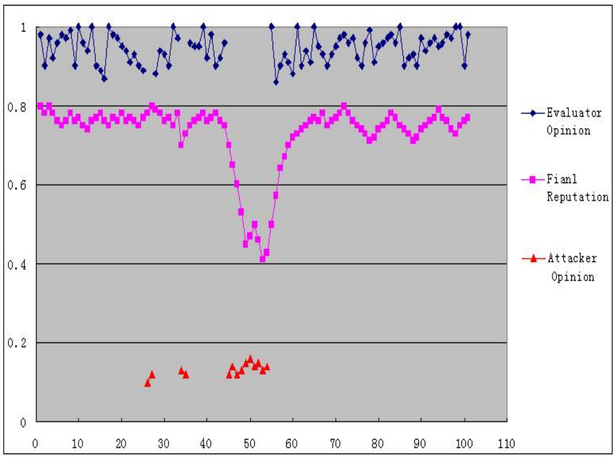

Fig. 5: Behavior of the reputation function the attacking group's members have on random personal reputations.

Fig. 5 denotes the relationship of personal reputation and group's attack, through Fig. 4 we can observe that though the attackers manage to lower the reputation of the target during the attack period, they are not able to inflict permanent damage. The function recovers itself to the original value through the honest opinion expressed by evaluators with high reputation and the age of the opinion variable.

5. Conclusion

Reputation in a society is positively correlated to the variables opinions, the reputation of opinion providers, and timeliness of the opinions. Based on this understanding, we have proposed in this paper a number of methods to quantify these metrics. Each metric has different influences on the reputation and each factor has its independent impact variable. Every factor can affect the process of reputation evaluation differently based on the environment in which the function is deployed. As the deployment environment changes, the influence of each factor may change. Certain factors may be more aggressively involved in the computing process while others not. In contrast to most existing reputation functions in which the factors are static, our model provides a framework in which they may change according to requirements of the context. Thus, our presented complex reputation function can conveniently serve in an e-commerce website or any on-line group activity or P2P systems by only changing a few variables.

Acknowledgements

This work is supported by the National Natural Science Foundation of China under Grant NO 60973146, NO 61170269, NO 61003285, NO 61170272 and the State Key Laboratory of Rail Traffic Control and Safety (Contract No. RCS2010K010), Beijing Jiaotong University.

References

1. Y. Wang amd J. Vassileva, Trust and reputation model in peer-to-peer networks, *Proceeding of the 3rd Int. Conf. on Peer-to-Peer Computing*, eds. N Shahmehri, R L Graham and G Caronni (Linkoping, Sweden, 2003), pp. 150–157.
2. J. I. Khan and S. S Shaikh, A phenotype reputation estimate function and its study of resilience to social attacks, *J. of Network and Computer Applications*, 32(1) (2009) 913–924.
3. Z. Despotovic and K. Aberer. P2P reputation management: probabilistic estimation vs. social networks, J. *Computer Networks*, 50(1) (2006) 485–500.
4. W. W. Yuan, D. H. Guan, Y. K. Lee, S. Y. Lee and S. J. Hur, Improved trust-aware recommender system using small-worldness of trust networks, J. *Knowledge-Based Systems*, 23(1) (2010) 232–238.
5. M. Newman, A. Barabasi and D.J. Watts (eds.), *The structure and dynamics of networks*, first edn. (Princeton University Press, Princeton, 2006).
6. J. H. Luo, X. Liu and M. Y. Fan, A trust model based on fuzzy recommendation for mobile ad-hoc networks, J. *Computer Networks*, 53(14) (2009) 2396–2407.
7. A. Tajeddine, A. Kayssi, A. Chehab and H. Artail, Fuzzy reputation-based trust model, J. *Applied Soft Computing*, 11(1) (2011), 345–355.
8. Z. Shuqin, L. Dongxin and Y. Yongtian, A fuzzy set based trust and reputation model in P2P networks, J. *Lecture Notes in Computer Science*, 3144(1) (2004), 211–217.
9. S. Song, K. Hwang, R. Zhou and Y. K. Kwok, Trusted P2P transactions with fuzzy reputation aggregation, J. *IEEE Internet Computing*, 9(1) (2005) 24–34.
10. H. P. Hu, H. K. Liu, B. H. Huang and R. X. Li, A reputation-based peer-to-peer trust management model, J. *Computer Engineering & Science*, 30(1) (2008) 41–44.
11. S. Marti and H. Garcia-Moline, Taxonomy of trust: Categorizing P2P reputation systems, J. *Computer Networks*, 50(1) (2006) 472–484.
12. L. Tao, S. B. Yang, J. Wang and J. Y. Zhou, Trust model based on similarity measure of vectors in P2P networks. J. *Lecture Notes in Computer Science*, 3795 (2005) 836–847.
13. F. G. Mármol and G. M. Pérez, Towards pre-standardization of trust and reputation models for

distributed and heterogeneous systems, J. *Computer Standards & Interfaces*, 32(4) (2010) 185–196.
14. J. Lopez, R. Roman, I. Agudo, C. Fernandez-Gago, Trust management systems for wireless sensor networks: best practices, J. *Computer Communications*, 33(9) (2010) 1086–1093.
15. J. Fadul, K. Hopkinson, C. Sheffield, J. Moore, and T. Andel, Trust management and security in the future communication-based "smart" electric power grid, in *Proc. 44th Hawaii Int. Conf. on System Sciences,* eds. R H Sprague (Kauai, Hawaii USA, 2011), pp. 1–10.