International Journal of Multimedia and Ubiquitous Engineering
Vol. 9, No. 12 (2014), pp. 85-96
http://dx.doi.org/10.14257/ijmue.2014.9.12.08

A Trust Management Model for Mobile P2P Networks based on Multiple-Fuzzy Theory

Meijuan JIA [1,2], Huiqiang WANG [1], Guangsheng FENG [1] and Fangfang GUO [1]

1. College of Computer Science and Technology, Harbin Engineering University, Harbin 150001, China
2. College of Computer Science and Information Technology, Daqing Normal University, Daqing 163712, China
E-mail:jiameijuan@sina.com, wanghuiqiang@hrbeu.edu.cn
fengguangsheng@hrbeu.edu.cn guofangfang@hrbeu.edu.cn

Abstract

The characteristics of dynamic, heterogeneity and limited resources of peers result in the existence of selfish behavior in MP2P network, which affect the network performance. To improve the performance of MP2P, a trust management model for peer reputation is established based on multiple-fuzzy theory in this paper. Direct trust, indirect trust, residual energy and active degree of peers are used as the fundamental variables and their weights are determined by using fuzzy theory, and then the reputation of peers is calculated. Peers with high reputation are allowed to participate in the communication and peers with low reputation are not allowed. The experimental simulation results show that the model not only effectively improve the malicious peer detection rate and the query hit rate but also reduce the Cx of the network.

Keywords: *MP2P networks, trust management model, multiple-fuzzy theory*

1. Introduction

Mobile Peer-to-Peer (MP2P) systems have become very popular, and have been used to provide solutions in areas, such as distributed computation, voiceover IP, and file sharing [1]. MP2P architectures will be very important for future distributed systems and applications.

There are no central administrations and peers are autonomous in many MP2P systems, so peers cannot communicate with each other via well-established infrastructure, which making them inherently insecure and untrustworthy [2]. Due to the limitation of energy, two peers out of communication range require intermediate nodes to transfer messages. Moreover, peers are heterogeneous in providing services and they do not have the same competence of reliability in such networks. Therefore, it is necessary to estimate whether a peer is trustworthy or not for file sharing and other services. In the process of communication, the future behavior of peers can be judged according to the performance and the characteristics [3], which are known as peers' reputation. We can determine peers reputation based on trust management mechanism. Many researchers have proposed some related frameworks and solutions around peers' reputation evaluation mechanisms [4-9]. In the exiting mechanisms, decision factors are often incomplete and lack of rationality and practicality. As a result, they cannot calculate the accurate reputation for each peer. Hence, these mechanisms are ineffective in MP2P trust management.

ISSN: 1975-0080 IJMUE

To solve those problems, we proposed a trust management model based on the Fuzzy Theory for MP2P, which considering the behaviors of the dynamic peer in the open environment and the complete decision factors of peers reputation. We determine reputation not only from direct trust, indirect trust, but also residual energy and active degree based on the Fuzzy Theory. We set threshold value for reputation, when the peer reputation is higher than the threshold value, the peer can be selected as the resource of downloading. On the contrary, when the peer reputation is lower than the threshold, the peer can't be selected.

The rest of the paper is organized as follows. In section 2, we discuss the related work. In section 3, we make some assumptions, definitions and propose a trust management model of peers reputation. Section 4 shows the experiments results and the performance analysis. Finally, section 5 gives the conclusions and the direction for future research.

2. Related Work

Due to the difficulties caused by system mobility and dynamic network topology, MP2P networks pose greater challenges in trust management. There are multiple trust management mechanisms that have been proposed for MP2P networks.

In [4], the fuzzy nature of subjective trust is considered, and a formal model proposed provides a new valuable way for studying subjective trust management in open networks. In this paper, the conceptions of linguistic variable and fuzzy logic are introduced into subjective trust management. A formal trust metric is given at first, and then fuzzy IF-THEN rules are applied in mapping the knowledge and experiences of trust reasoning that humanity uses in everyday life into the formal model of trust management. At last, the reasoning mechanisms of trust vectors are given. But it does not give specific trust calculation methods.

In [5], the author presents an integrated fuzzy-based trustworthiness system for communications in JXTA-overlay P2P platform. This system consists of two Fuzzy Logic Controllers (FLC1 and FLC2). FLC1 has three input parameters: namely Number of Jobs (NJ), Number of Connections (NC) and Connection Lifetime (CL) and its output is Actual Behavioral Criterion (ABC). Then ABC and Reputation (R) are used as input systems for FLC2 and the corresponding output is Peer Reliability (PR).

The method proposed in [6] addresses a super-peer based trust model for Peer-to-Peer (P2P) networks to solve the problem that the trust relation between peers is not sufficiently built due to the difference of peers' interests and low probability of repeated transactions between them. In the model, peers gather in a group according to their interest similarity. Trust relation is categorized into three kinds and subsequently each solution for these kinds is also put forward. Moreover, a feedback filtering algorithm based on peers' similarity is proposed to effectively filter the fake, misleading and unfair feedbacks in the referrals.

Basit Qureshi, *et al.*, [7] propose M-trust model for mobile P2P networks. The new scheme utilizes confidence in reputation, based on interactions among peers, to reduce the computation complexity. Furthermore, distributed algorithms are presented for accurate and reliable trust ratings aggregation and space management.

DTMM is presented in [8]. With DTMM, each moving object within the same group tends to have a high probability of keeping stable distances from each other. The main contribution of this model is to predict the future availability of wireless links and lead to fast generating valid trust evidences.

Ganeriwal, *et al.*, [9] make a trust evaluation model and uncertainty analysis based on Bayes theory. The model regards the subject fuzziness of trust as the randomness and uses pure probability statistic method to assess trustworthiness, which is difficult to obtain prior knowledge from practical application and inevitably result in something unreasonable.

3. The Proposed Trust Management Model

To construct model, we make some necessary assumptions.

Assumption 1 In the network, peers will not report false information to others, and there exists no collusion between peers [10].

Assumption 2 Peers are in promiscuous mode when they are in the network's operation, namely, all peers can monitor the information of other peers within the range of the transmission.

Assumption 3 The network is composed of isomorphic peers. Each peer in the network has the same computing power, storage capacity, communication distance and the initial energy.

Assumption 4 A peer can't complement energy for each other. It will leave from the network while the energy exhausts.

3.1. Calculation of Trust Value

In mobile P2P networks, trust is a relationship between two neighbor peers.

Definition 1 Direct trust (DT): In MP2P networks, peers may rate each other after each transaction. We define the number that peer p_j has downloaded from p_i at t time interval, which is denoted as $DT(p_i, p_j)$, and $0 \le DT(p_i, p_j) \le 1$, as shown in Figure 1.

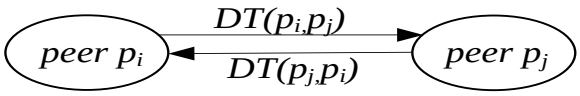

Figure 1. Direct Trust Model

Definition 2 Indirect Trust (IDT) is evaluated by the weighted average of DT which is provided by p_i's neighbors interacting with p_j. It is denoted by $IDT(p_i, p_j)$, as shown in Figure 2.

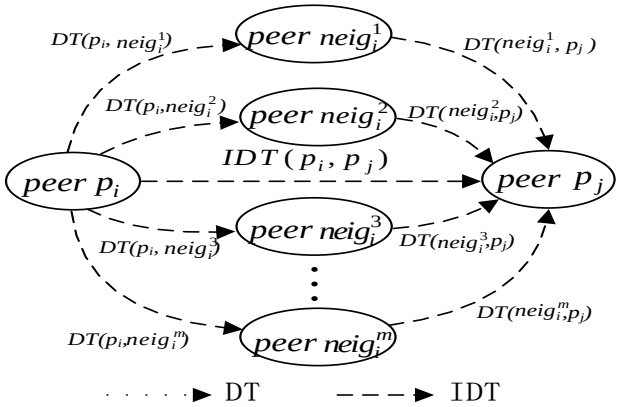

Figure 2. Indirect Trust Model

$IDT(p_i, p_j)$ is defined as follows:

$$IDT(p_i, p_j) = \frac{1}{n}\sum_{m=1}^{n} W_i^m * DT(neig_i^m, p_j) \qquad (1)$$

Where $IDT(p_i, p_j)$ is the indirect trust that peer p_i has about peer p_j .The neighbor number of peer p_i is denoted by n, the m^{th} neighbor of peer p_i is denoted by $neig_i^m$ .The weight of the m^{th} neighbor of peer p_i is denoted by W_i^m, which can be computed by:

$$W_i^m = \frac{DT(p_i, neig_i^m)}{\sum_{m=1}^{n} DT(p_i, neig_i^m)} \qquad (2)$$

The direct trust that peer p_i has about peer $neig_i^m$ is denoted by $DT(p_i, neig_i^m)$.

In a MP2P network, peers join or leave the network frequently, which leads to the dynamic changes in network topology. Due to frequent changes, a trust management mechanism needs to repeatedly revise and update trust value. To determine the latest and the most precise trust value, it is necessary to handle historical trust value and current trust value of peers. Historical Trust Value (HTV) is estimated by the peer's physical neighbors based on historical interaction information before t time interval, and Current Trust Value (CTV) is estimated by the peer's physical neighbors based on DT and IDT at t time interval. They are both calculated by DT and IDT. In our proposed model, $HTV(p_i, p_j)$ can be computed by:

$$HTV(p_i, p_j) = \omega_1 * DT(p_i, p_j) + \omega_2 * IDT(p_i, p_j) \qquad (3)$$

Where ω_i is the weight of two factors, $1 \le i \le 2$, $0 \le \omega_i \le 1$ and $\sum_{i=1}^{2} \omega_i = 1$.

$CTV(p_i, p_j)$ can be computed by:

$$CTV(p_i, p_j) = \omega_3 * DT(p_i, p_j) + \omega_4 * IDT(p_i, p_j) \qquad (4)$$

Where ω_i is the weight of two factors, $3 \le i \le 4$, $0 \le \omega_i \le 1$ and $\sum_{i=3}^{4} \omega_i = 1$.

Trust Value (TV) of a peer can be calculated by HTV and CTV. $TV(p_i, p_j)$ can be computed by:

$$TV(p_i, p_j) = \omega_5 * HTV(p_i, p_j) + \omega_6 * DTV(p_i, p_j) \qquad (5)$$

Where ω_i is the weight of two factors, $5 \le i \le 6$, $0 \le \omega_i \le 1$ and $\sum_{i=5}^{6} \omega_i = 1$

HTV, CTV and TV are calculated based on the Fuzzy Theory [11].The types of trust value transfer process are shown in Figure 3.

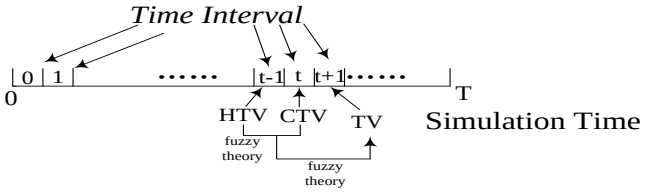

Figure 3. The Types of Trust Value Transfer Graph

3.2. Calculation of Peer Reputation

Reputation is vague and uncertain, so it is very difficult to determine. This vagueness and uncertainty can be handled using the Fuzzy Theory, because it not only can establish relationship between qualitative analysis and quantitative analysis, but also has strong ability of comprehensive judgment.

Reputation of peers (RP) expresses the degree that peers can provide services for others at the next time interval. In MP2P systems, reputation can be useful when there are a large number of peers interacting (*e.g.*, downloading file, knowledge sharing). In proposed model, RP is determined by three decision factors. These factors are trust value, energy and the cumulative number of entities interacting with others.

Definition 5 Residual Energy (RE): In the process of communication, each peer will lose its energy because of providing service for others. Due to the limited energy, the more the peer involved in communications, the more energy will be consumed [12] the residual energy will reduce until it becomes zero. The residual energy is denoted by RE_i and it will determine whether the peer can continue to make communications with others.

Definition 6 Active Degree (AD): We record the cumulative number of entities interacting with an evaluated peer $peer_i$, which is denoted by AD_i .

According to the above analysis, RP can be denoted by:

$$RP_i = \omega_1 * RE_i + \omega_2 * TV(p_i, p_j) + \omega_3 * AD_i \quad (6)$$

Where ω_i is the weight of four factors, $1 \le i \le 3$, $0 < \omega_i \le 1$ and $\sum_{i=1}^{3} \omega_i = 1$

So, the proposed model is shown in Figure 4.

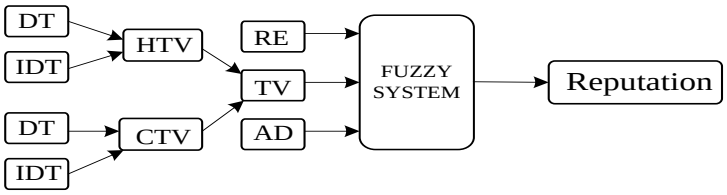

Figure 4. Trust Management Model based on Multiple-fuzzy Theory

Weighted average method (WAM) is very suitable for solving trust evaluation [13], since it is easy to understand and implement. In this paper, with the established factor set, evaluation set and weight set, we can get the result of reputation using WAM and fuzzy arithmetic operators.

Step 1：Confirm the comment set

According to the decision factors, we confirm the comment set $V = \{low(v_1), normal(v_2), high(v_3)\}$, where $low(v_1)$ means that peer reputation is low, $normal(v_2)$ means that the peer reputation is normal and $high(v_3)$ means that the peer reputation is high.

Step 2：Construct the fuzzy comparison matrix

By using TFN [14], the decision factors are required to make pairwise comparisons for the main criteria and sub criteria. A fuzzy comparison matrix A is constructed according to arithmetic mean of pairwise comparisons from decision factors.

Step 3：Determine the weight of factors

The weight of each factor will be determined by normalizing any of the rows or columns of matrix A. By calculating the maximum eigenvalue of the matrix using characteristic root method, we can get $\lambda_{\max}$. After normalization, the weight ω_i can be calculated.

Step 4：Check consistency

The consistency ratio (CR) is calculated in order to control the results of this method. The consistency can be checked by CR, which is used to directly estimate the consistency of pairwise comparisons. CR is computed using equation (7).

$$CR = \frac{CI}{RI} \quad (7)$$

$$CI = \frac{\lambda_{\max} - n}{n-1} \quad (8)$$

Where CI is consistency index. RI is random index, as shown in Table 1 [15] and n is matrix size.

According to this, when $CR < 0.1$, the weight ω_i which is calculated then can be determined.

Table 1. Consistency Checking Table

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
RI	0	0	0.52	0.89	1.12	1.26	1.36	1.41	1.46	1.49	1.52	1.54	1.56	1.58	1.59

Step 5：Determine the reputation of peers

After the weight ω_i is determined, RP can be determined. We set threshold value for RP, when RP is larger than threshold value, peer can be selected as the resource of downloading. On the contrary, the peer can't be selected.

4. Simulation Experiments and Performance Evaluation

In order to evaluate the performance of the proposed trust management model, extensive simulation experiments have been conducted using ns-3 discrete simulator. The network topology structure are generated at random, where peers are deployed every round. The mobility of peers is simulated using random waypoint model: each peer keeps static for a while, and then he or she begins to move towards a set destination. The movement range of peers is confined within 1km× 1km area. The experimental results are averaged from 50 rounds. The parameters in simulation experiments are summarized in Table 2.

Table 2. Parameters setup

Parameter	Value
Peer number	50 to 500
Movement model	Random waypoint model
Mobility speed	1m/s, 2m/s ,3m/s
Deployment area	1km ×1km
Pause time	30s – 2 min
Trust threshold	0.3, 0.5, 0.7
Malicious peer ratio	10%, 20%
Initial energy per peer	1000J

4.1. Initialization of Simulation Experiments

Because no information on trust relationship can be used for either honest peers or malicious peers at the beginning of simulation, their trust values need to be set in the initialization phase. In the simulation experiments, the initial trust values of peers in the

network are set according to normal distribution. The initial trust values of honest peers follow a normal distribution **with means** μ=0.9 and σ^2=0.1 and the initial trust values of malicious peers follow a normal distribution **with means** μ=0.1 and σ^2=0.1. The network traffic follows the Poisson distribution with an arrival rate λ=10-20 requests every minute. In the initialization phase, the indirect trust values of all peers are zero, namely peers can only compute trust value using direct trust values, RE and AD. With the communication among peers, peers can gradually obtain the indirect trust values of non-neighbor peers.

4.2. Metrics

We use the following metrics to evaluate the performance of multiple-fuzzy theory trust management model.

-trust list size (TLS for short in the following paper): the ratio of the number of peers whose trust values is above the trust threshold to the number of all peers of the network. The larger TSL of one peer, the higher the success rate of communication. It is related with the trust threshold. For the same peer, the lower the trust threshold at some time is, the larger the corresponding TLS is.

- congregation state(Cx): Cx for peer *i* is defined as the following formula:

$$Cx_i = \frac{|TLS_i(t)|}{N^2} \quad (9)$$

Where, $TLS_i(t)$ denotes the TSL of peer *i* at time *t*; $|TLS_i(t)|$ denotes the number of $TLS_i(t)$; and N denotes the number of peers in the network. In the simulation, *Cx* is defined as the following:

$$Cx = \frac{1}{N}\sum_{i=1}^{N} Cx_i \quad (10)$$

Cx is the average *Cx* for all peers in the networks. It shows the convergence state of trust value of peers in the network.

-query hit rate is defined as the ratio of the number of the received replies to the number of sent requests. The higher value of query hit rate indicates that the request was fulfilled and further requests are not needed, effectively reducing the overall amount of traffic in the network. So, the higher query hit rate, the reliable multiple-fuzzy theory trust management model.

-malicious peer detection rate is defined as the ratio of the number of detected malicious peers in the simulation to the number of the actual malicious peers in the network. The higher the accuracy, the better the performance of multiple-fuzzy theory trust management model.

4.3. Performance Evaluation

The trust list size vs. time interval is shown in Figure 5. The vertical coordinate of Figure 5 denotes the mean value of peers all over the network, and the trust threshold is set 0.5. It can be seen from Figure 5 that the size of trust list increases with the increase of time interval at the beginning. After 18 time intervals, the size of trust list gradually becomes stable. It is due to the fact that at the beginning of the network every peer only knows the initial trust value about its neighbor peers. In addition, every peer does not know the indirect trust information of other peers and the RE of non-neighbor peers. Finally, few interactions between peers can be made. With the increase of the communication, each peer knows more information on trust of other peers.

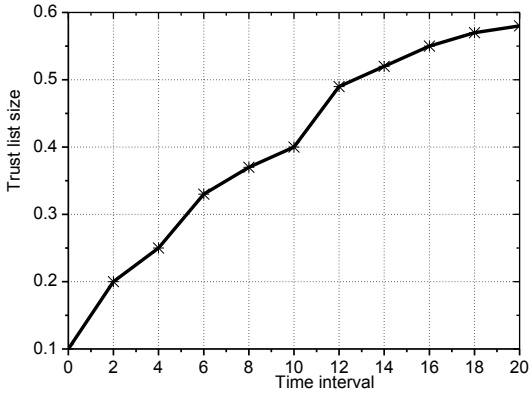

Figure 5. Trust List Size vs. Time Interval

The different trust thresholds have different effects on the performance of the network. The impact of trust threshold on Cx is shown in Figure 6. The Cx degrades sharply with the number of peers increase. The higher the trust threshold is, the fewer peers can be trusted. Therefore, the size of trust list will be reduced with the increase of the trust threshold. Due to the fewer entries in trust list, Cx will gradually decrease with the increase of the trust threshold.

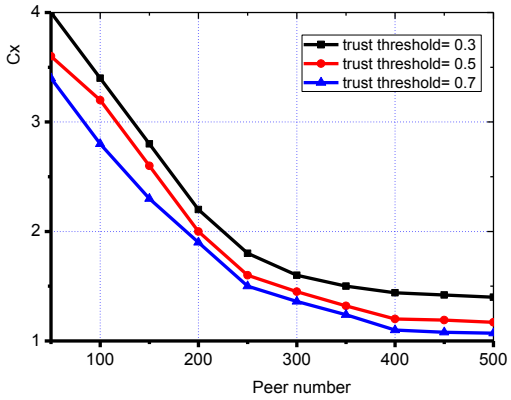

Figure 6. Cx vs. Trust Threshold

The relationship between trust threshold and query hit rate is shown in Figure 7. Along with the increasing of the number of peers, the query hit rate will increase because the number of the received replies will increase. Meanwhile, for the same number of peers, the higher the trust threshold at some time, the larger the query hit rate is.

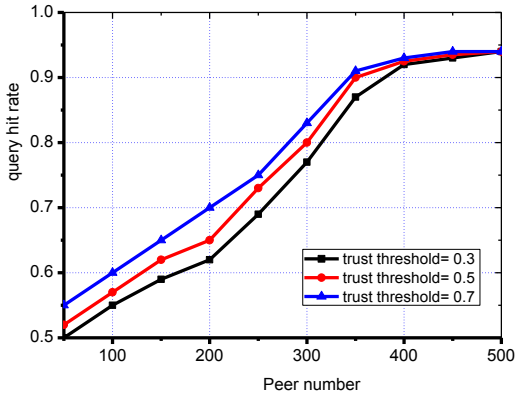

Figure 7. Query Hit Rate vs. Trust Threshold

Figure 8 shows the comparison of the malicious peer detection rate at different trust threshold. The higher the trust threshold, the larger the malicious peer detection rate as the number of malicious peers increases. The reason is that, when the trust threshold is high, the probability of suspect or low trustworthy peers will increase in the network, thus the malicious peer detection rate will increase. At the same time, as the number of peers increases in the network, more and more peers will be detected, which will increase the rate of the malicious peer.

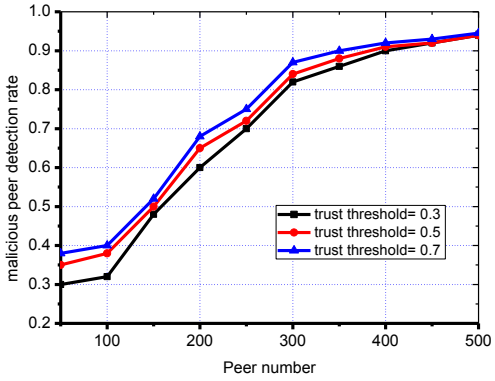

Figure 8. Malicious Peer Detection Rate vs. Trust Threshold

Figure 9 illustrates that the relationship between the malicious peer detection rate and trust threshold with mobility. The peer mobility is set to 1m/s, 2m/s and 3m/s respectively, and the trust threshold is 0.3, 0.5 and 0.7 respectively. It can be seen that the difference of the result is small, and the best malicious peer detection rate is provided when the trust threshold is set to 0.7 and the mobility is 1m/s. This is due to the fact that connectivity will be disrupted frequently with higher mobility and lower trust threshold.

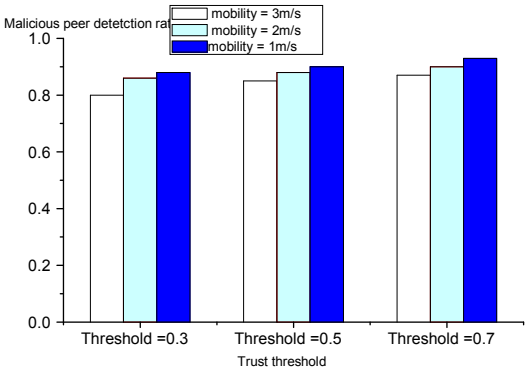

Figure 9. Malicious Peer Detection Rate vs. Mobility

5. Conclusions

This paper presents a novel trust management model for MP2P based on multiple-fuzzy theory. The model relies on history trust and current trust to determine trust value for a peer using fuzzy theory, then the trust value, residual energy and active degree can be used to determine the reputation based on fuzzy theory again. Simulation results demonstrate that the overall performance of the presented model is accurate, reliable and robust for detecting malicious peers in MP2P networks. Especially when peer reputation is high enough, malicious peer detection rate, query hit rate and Cx are good, which is to say that the performance of multiple-fuzzy theory trust management model is better.

In the future research, we will to test our scheme into more real mobile P2P systems and analyze the system performances.

Acknowledgements

This wok was supported by the National Natural Science Foundation of China (61370212), the Research Fund for the Doctoral Program of Higher Education of China (20122304130002), the Natural Science Foundation of Heilongjiang Province (ZD 201102), the Fundamental Research Fund for the Central Universities (HEUCFZ1213, HEUCF100601).

References

[1]. O. Zhong-Hong, S. Mei-Na, Z. Xiao-Su and S. Jun-De, “Key techniques for mobile peer-to-peer networks”, Journal of Software, vol. 2, no. 19, **(2008)**.
[2]. Y. C. Hu, S. M. Das and H. Pucha, “Peer-to-peer overlay abstractions in MANETs in Theoretical and Algorithmic Aspects of Sensor, Ad Hoc Wireless, and Peer-to-Peer Networks”, Edited Jie Wu, CRC Press, Florida, **(2005)**, pp. 857-874.
[3]. A. Josang, R. Ismail and C. Boyd, “A survey of trust and reputation systems for online service provision”, Decision Support Systems, vol. 2, no. 43, **(2007)**.
[4]. T. Wen, H. Jianbin and C. H. Zhong, “Research on a Fuzzy Logic-Based Subjective Trust Management Model”, Journal of Computer Research and Development, vol. 10, no. 42, **(2005)**.
[5]. S. Ganeriwal, L. K. Balzano and M. B. Srivastava, “Reputation-Based Framework for High Integrity Sensor Networks”, ACM Trans. Sens. Netw., vol. 4, **(2008)**.
[6]. T. Chun-qi, J. Jian-hui, H. Zhi-guo and L. Feng, “A novel super-peer based trust model for peer-to-peer networks”, Chinese Journal of Computers, vol. 2, no. 33, **(2010)**.
[7]. B. Qureshi, G. Min and D. D. Kouvatsos, “A distributed reputation and trust management scheme for mobile peer-to-peer networks”, Computer Communications, vol. 35, **(2012)**.
[8]. X. Wu, “A distributed trust management model for mobile P2P networks”, Peer-to-peer Networking and Applications, vol. 5, **(2012)**.

[9]. L. Barolli, E. Spaho, F. Xhafa and M. Younas, "Performance evaluation of an integrated fuzzy-based trustworthiness system for P2P communications in JXTA-overlay", Neuro computing, vol. 122, **(2013)**.
[10]. S. Zhong and F. Wu, "On designing collusion resistant routing schemes for non-cooperative wireless ad hoc networks", Proc. Of the 13th Annual ACM Int'l Conf. on Mobile Computing and Networking (MobiCom). Montreal: ACM Press, **(2007),** pp. 278-289.
[11]. H. Baoqing, Editor, "Fuzzy theory basis (V.2)", Wuhan University Press, Wu Han, **(2010)**.
[12]. W. Jun, "The research of wireless sensor network energy effectiveness", Nanjing: Department of Computer Science and Technology, Nanjing University, **2012**.
[13]. L. YongJun and D. YaFei, "Research on Trust Mechanism for Peer-to-Peer Network", Chinese Journal of Computer, vol. 3, no. 33, **(2010)**.
[14]. T. L. Saaty, Editor, "Fundamentals of Decision Making and Priority Theory (2nd ed.)", RWS Publications, Pittsburgh, **(2000)**.
[15]. X. Jijian and L. Chengping, Editor, "Fuzzy mathematics method and application", Huazhong University of Science and Technology (HUST) PRESS, Wuhan, **(2013).**
[16]. L. Hogie, P. Bouvry and F. Guinand, "The MADHOC simulator." http://www-lih.univ-lehavre.fr /hogie/madhoc.

Authors

Meijuan Jia

She was born in 1976. She received her M.S. degree in Computer Science from Harbin Engineering University. Now she is a PHD candidate at Harbin Engineering University and a lecturer of Daqing Normal University. Her research interests include trusted computing, mobile network, and mobile peer-to-peer.

Email:jiameijuan@sina.com

Huiqiang Wang

He was born in 1960. He is currently a professor of Harbin Engineering University, PhD supervisor and senior member of China Computer Federation. His research interest covers the network technology and information security, trusted computing, automatic computing, cognitive network.

Email: wanghuiqiang@hrbeu.edu.cn

Guangsheng Feng

He was born in 1980. He is a lecturer of Harbin Engineering University. He received his Ph.D. degree in Computer Science from HEU in 2009. His research interests involve cross-layer design, information sensing and wireless channel access control.

Email: fengguangsheng@hrbeu.edu.cn

Fangfang Guo

He was born in 1974. He is an Associate Professor in Harbin Engineering University (HEU). He received his M.S. degree in Computer Science from HEU in 2001 and his Ph.D. degree in Computer Science from HEU in 2006. His research interests include Network and Information Security, Mobile Peer-to-Peer Network, and the Internet of Things.

Email: guofangfang@hrbeu.edu.cn

为方便组委会联系，请提供 2 位作者信息。

论文题目	A Trust Management Model for Mobile P2P Networks based on Multiple-Fuzzy Theory		
所属主题	Mobile Network		
第一作者			
姓名	Meijuan Jia	职称/学位	Lecturer/master
单位	College of Computer Science and Technology, Harbin Engineering University	邮编	150001
地址	NO.145 Nantong Street,Nangang District,Harbin,Heilongjiang		
电话	13936980699	手机	13936980699
Email	jiameijuan@sina.com		
第二作者			
姓名	Huiqiang WANG	职称/学位	Professor/PhD
单位	College of Computer Science and Technology, Harbin Engineering University	邮编	150001
地址	NO.145 Nantong Street,Nangang District,Harbin,Heilongjiang		
电话	0451-82589605	手机	
Email	wanghuiqiang@hrbeu.edu.cn		