Computational model based on the reputation incentive and punishment mechanism in P2P environments

Sun Hua[1*], Yu Jiong[1], Zhang Zhenyu[2], Jiang Hong[1]

[1]*School of Software, Xinjiang University, Urumqi 830008, China*

[2]*School of Information Science and Engineering, Xinjiang University, Urumqi 830046, China*

Received 1 October 2014, www.cmnt.lv

Abstract

Rating reputation of the peers is a key problem in P2P environments, a computational reputation model based on incentive and punishment mechanism is proposed. This model considers both direct and indirect transactions with target peers before their next transactions. The mechanism puts different weights to get the value of reputation, and the model incents the good behaviours and punishes the bad ones through adjustment factor. Through experiment, the model can hold back malicious peers and ensure higher success transaction rate.

Keywords: P2P, reputation, incentive, punishment

1 Introduction

With the development of P2P development of network applications, more and more transactions take place between unfamiliar individual, also distributed P2P network have the characteristic of open anonymous, propagation, the malicious nodes are easy to perform malicious information such as viruses, Trojans, Troy [1]. Therefore, the entities need to establish credit mechanism to resist malicious nodes [2, 3]. But how to deal with the trust relationship between the strangers [4], so that the transaction between them can be carried out smoothly is a problem worthy of study. At present, the method of trust and reputation systems [5] can improve the success rate of the transaction because both parties are not willing to be deceived, so a lot of trust and reputation model [6, 7] has been proposed as an effective method to evaluate the credibility of the counterparty. In P2P network, a node's reputation is computed by the other nodes which have had the transaction with it. The node get reputation through query and these queries will cause the system overhead larger. Therefore, how to effectively use the other nodes have the reputation of the target query is a problem worthy of study [8-11].

Typically, each node is expected to confirm each other's reputation in the trade[12], even though there have been trading experience, in order to fully understand the counterparty reputation, trade both sides still need to query to other nodes. The query message transmission can be used as the Gnutella [13] query mode, although this method can fully obtain the target node's reputation, but will cause a large number of query messages in the network. If a node and a destination node have been trading history, then the node before the transaction is used to search the target node's credibility, it can be the direct trading experience and results obtained after the query as the response data. According to the credibility of each query node's response data and given different weights, the query node combines with the query node and a destination node (or may not) has trading experience to comprehensively calculate the target node's reputation. The reputation value, as the nodes trading conditions, is set up by their own corresponding threshold value. If the counterparty credit value can satisfy the transaction value, then the two sides traded. After completion of the transaction, the node, according to the circumstances of the transaction, assess counterparty credit. The credit value is stored in the database for reputation using as the transaction reputation computation or being recommended to other nodes [14].

In view of the above situation, this paper proposes a reputation computation model, considering not only the node transaction histories, and considering the recommendation of other nodes factors. According to credible recommender and giving each weight factor, the calculation of relative reward or punishment factor to join the new credit to encourage honest nodes to provide honest services and punish the malicious nodes to reduce its credibility and avoid the other node from possible attack.

2 Related work

One of online reputation system known as anybody is eBay reputation feedback Forum (the Feedback Forum), it uses the simple reputation computing mode, each time after the transaction, the seller and the buyer respectively set -1, 0, 1 Evaluate transactions each other, which represent negative, neutral and positive evaluation. Positive evaluation system statistics for each user and the number of negative number, difference then as the user reputation. This intuitive reputation can clearly show the user's credibility, other users are also very easy to understand, but it is too simple statistical methods, and it is difficult to analyze the network with all kinds of complicated situations. Moreover, the system is no incentive and punishment mechanism corresponding in this way to promote the healthy development of system.

[*] ***Corresponding author's*** e-mail: xj_sh@163.com

EigenRep [15] is a P2P file sharing network algorithm proposed by Kamvar. The algorithm uploads history behaviour of nodes in the network, giving to each node reputation, and the distributed security iteration method to calculate the global reputation. Other nodes can choice available to download files according to the node global reputation, EigenRep can effectively identify the malicious nodes, and they are isolated in the network. But there is no corresponding incentive and punishment mechanism. Dou Wen [16] proposed the improvement on EigenRep, and the correlation analysis and the distributed computing protocol is given.

RRM (Resilient Reputation Model) [17] reputation model is an elastic; the main goal is to encourage users to provide good service and promote good trading results. At the same time, malicious nodes try to manipulate the system of punishment or damage to other nodes. Compared with other similar models, RRM mainly on node continuous honest behaviour was analyzed, using LCTGS (Latest Continuous Times of Good Service, recently for the provision of quality service times) to analyze the behaviour of users, better motivate the user behaviour.

Considering the credibility assessment of each node, a node according to the corresponding behaviour encouragement or punishment, on the other hand, in combination with other nodes of the recommendations and their trading experience, calculates the comprehensive reputation.

3 Calculation model

3.1 FUNCTIONAL STRUCTURE DESIGN

Each node in the network follows the two principles:

1) At each node receives the other node reputation request, will actively respond to the query request;

2) Each node can truly evaluate counterparty credit according to the business situation, and can query with real data response.

A malicious node in this paper does not provide high quality service and cause damage to other nodes, but does not make malicious evaluation and malicious response.

In the reputation calculation model, the input data for the reputation calculation includes direct experience and recommended information from other target node having trading experiences, the recommendation nodes included: direct transaction recommended node experience and recommendation node before trading on the target node of the query data. Shown as Figure 1, each node for the credibility of the calculated data is the main source of direct transaction evaluation database (DDB, Direct Database) and recommend evaluation database (RDB, Recommendation Database). Data in DDB is the node itself involved in trading on the assessment of counterparty does, RDB is recommended for evaluation of other nodes in each other's transaction database, query nodes renew and maintain RDB after each time credit counterparty, insert the recommended new record, or delete the earlier data record or reputation value lower nodes recommended data. Due to the different nodes, the recommended focus may be different, so they need to deal with later for reputation computation (process is not in the scope of this study). Stored in the DDB and RDB data, not only for the node reputation computation, but also provide credit data recommended for other nodes. After the credit calculation model calculated data, stored in the database for the credibility, reputation make decision, reach the trade credit threshold trade only. After the transaction counterparty, needs assessment, evaluation and the results stored in DDB, for the next computation credit use, or recommend to other nodes.

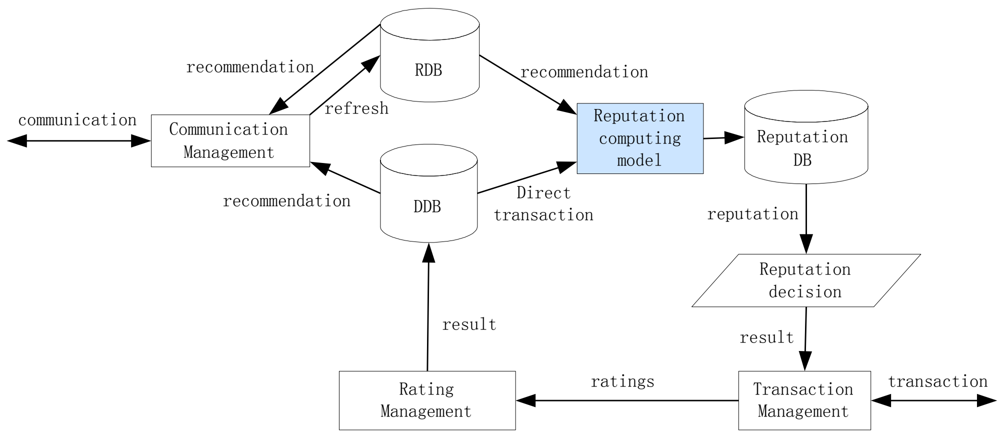

FIGURE 1 Node credit calculation model

3.2 MODEL DESIGN

3.2.1 Direct exchange of experience

If node i and node j direct transaction times is n ($n \geq 0$). Every time after the transaction, nodes need to calculate counterparty credit. The N transaction, credit evaluation node i to node j is $r_{i,j}^{(n)}$, comprehensive credit before the N deal evaluation is $T_{i,j}^{(n)}$. Were given historical transaction evaluation and the current transaction evaluation of different weights:

$$\begin{cases} T_{i,j}^{(n)} = \beta \times T_{i,j}^{(n-1)} + (1-\beta) \times r_{i,j}^{(n)} \times F_{i,j}^{(n)}(T_{i,j}^{(n-1)}), n \geq 1 \\ T_{i,j}^{(0)} = 0.5, n = 0 \end{cases}, \quad (1)$$

where $F_{i,j}^{(n)}(T_{i,j}^{(n-1)})$ as the adjustment factor of incentive and punishment (see section 3.2.3). β as historical factors, ranging from [0,1], by adjusting β value adjustment transaction history and current trade calculation process in the proportion of credit. As shown in Figure 2 $T_{i,j}^{(n)}$ on the effect of β.

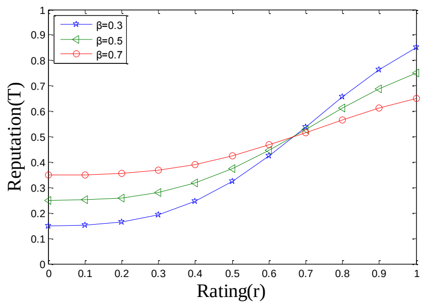

FIGURE 2 Influence of historical factor β on T reputation and evaluation R

3.2.2 Recommendation

In addition to the direct trading experience, in order to obtain the counterparty comprehensive credit information, the node will query other nodes before transaction. As shown in Figure 3.

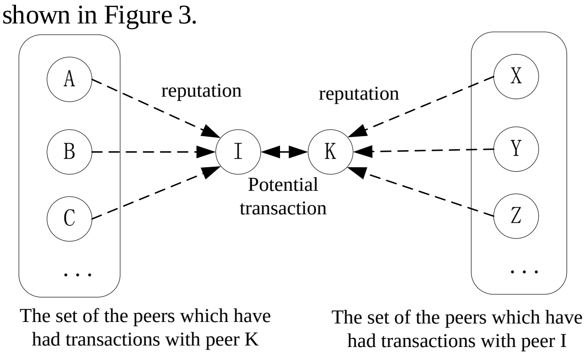

FIGURE 3 Recommendation of reputation between peers

The node i and node j is two nodes to deal, where nodes A, B, C is a set of nodes having trade experience with j. Because the node of the set and node j maybe have had transactions before and also query reputation of j, therefore, node i query node j reputation, will recommend all their trading experience and query result node j once to a node i, node i considering the believable degree of each node, then statistical analysis these information recommendation. The process is the same as the node j.

There are M nodes (hypothesis are node 1 to node m, hereinafter referred to as the node of the K) response of query nodes i for j reputation request, node i statistical analysis recommended information about node j (Recommendation), set, then:

$$R_{i,j} = \frac{\sum_{k=1}^{M} (T_{k,j}^{(S_K)} + R_{k,j}) \times \alpha_k}{2 \times M}. \quad (2)$$

From above formula, $T_{k,j}^{(S_k)}$ is the node k and node j having $S_k(S_k \geq 0)$ transactions take it as a part of the recommendation reputation. $R_{k,j}$ is the recommendation reputation on node j evaluated by other node K, an average of the two recommendation credibility (or set different weights) as recommendation reputation data to the node i. α_k is the recommended weight node k, the node or nodes with high credibility friend, recommended weight setting higher. If recommended information to some node is not available (for example, not online), the system may contain redundant information corresponding to recommendation information of other nodes get recommended comprehensive information.

If node i and node j has been trading n (n≥1) times, when need transaction once again, if the pre transaction time is $Time_{i,j}^{(n+1)}$, corresponding to the last transaction time is $Time_{i,j}^{(n)}$, and τ is interval threshold which need to set for node i to query the credibility of the. If $Time_{i,j}^{(n+1)} - Time_{i,j}^{(n)} < \tau$, then, the node i doesn't query nodes for J's reputation again, and it can use the last query results.

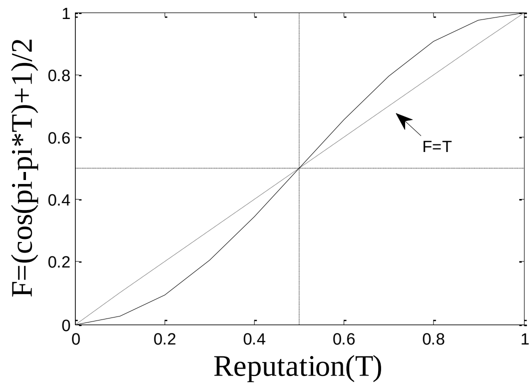

FIGURE 4 The relationship between reputation and incentive penalty adjustment factor

3.2.3 Incentive and punishment

In order to encourage honest node behavior and punish the behaviour of malicious nodes, set $F_{i,j}^{(n)}$ as incentive and penalty factor (AF, Adjustment, Factor) and credit evaluation, i.e. $F_{i,j}^{(n)}(T_{i,j}^{(n-1)})$, the range is [0,1], and which can use a cosine function:

$$F_{i,j}^{(n)}(T_{i,j}^{(n-1)}) = \frac{\cos(\pi - \pi \times T_{i,j}^{(n-1)}) + 1}{2}. \quad (3)$$

From the reference line in Figure 4 shows F = T, when $T_{i,j}^{(n-1)}$ less than 0.5, $F_{i,j}^{(n)}$ less than $T_{i,j}^{(n-1)}$, when $T_{i,j}^{(n-1)}$ more than 0.5, $F_{i,j}^{(n)}$ more than $T_{i,j}^{(n-1)}$.

According to the different functional relationship that $F_{i,j}^{(n)}$ will set the incentive and punishment, the incentive strength is more than punishment, or vice versa, penalties are larger, such as Equation (4), $r_{i,j}^{(n)}$ for the credibility of evaluation node i to node j (Rating).

$$F_{i,j}^{(n)}(x) = \begin{cases} e_{i,j}^{(n)}(x), & 0.5 \le r_{i,j}^{(n)} \le 1 \\ p_{i,j}^{(n)}(x), & 0 \le r_{i,j}^{(n)} < 0.5 \end{cases}, \tag{4}$$

where $e_{i,j}^{(n)}$ are the motivation factors (EF, Encouragement Factor transaction), incentive nodes maintain good behavior; $p_{i,j}^{(n)}$ as the penalty factor transaction (PF, Punishment Factor). The unified EF and PF expresses the adjustment factor AF is incentive, as $F_{i,j}^{(n)}$.

The calculation model of the final evaluation credibility node is described in this paper,. This is the analysis and evaluation system on eBay measures. In the evaluation system of eBay, evaluation of the buyer to the seller's account for only 51.7%, evaluation of buyer seller accounted for 60.6%. In all of the evaluation, less than 1% negative evaluation, less than 0.5% neutral, nearly 99% are affirmative evaluation [7]. According to the above data, we adjusted the evaluation information. Because of incentive cut amplitude smaller than punishment downward, so has the relative effect of incentive and punishment. As shown in Figure 5, credit evaluation is adjusted the incentive strength and penalties.

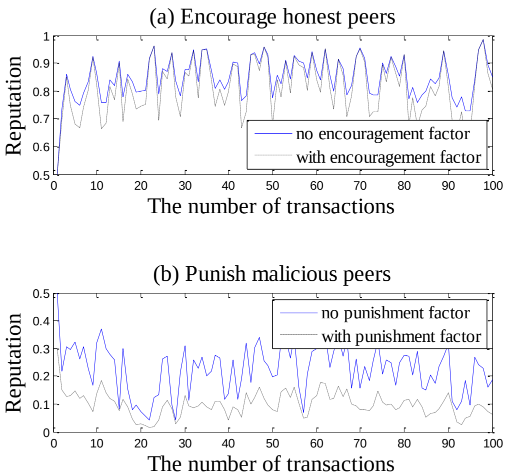

FIGURE 5 The incentive effect of the credibility of the adjustment factor

If the node from the reputation with high into a low evaluation, or vice versa, then in the calculation of the model, will soon be displayed, as shown in Figure 6, the nodes in a honest behavior, started in the malicious behavior, or vice versa, gradual process reputation.

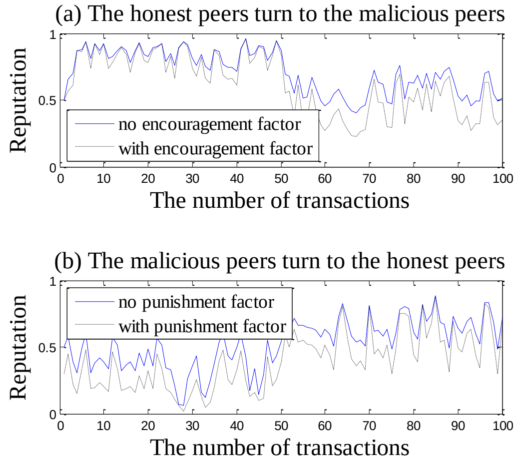

FIGURE 6 Impact on the credibility of the honest nodes and malicious nodes

3.3 CALCULATION MODEL

In summary, comprehensive evaluation of credibility for the node i to the node j is divided into two parts: the direct trading experience and recommendation. Direct trading has a relatively high credibility, set the weight γ for the direct reputation, combined with the Equations (1)-(3), launched a comprehensive credit evaluation $T_{i,j}$:

$$T_{i,j} = \gamma \times T_{i,j}^{(n)} + (1-\gamma) \times R_{i,j} =$$
$$\gamma \times (\beta \times T_{i,j}^{(n-1)} + (1-\beta) \times r_{i,j}^{(n)} \times F_{i,j}^{(n)}(T_{i,j}^{(n-1)})) +$$
$$(1-\gamma) \times \frac{\sum_{k=1}^{M} (T_{k,j}^{(S_k)} + R_{k,j}) \times \alpha_k}{2 \times M}, \tag{5}$$

The set of β =0.3, γ =0.7 respectively, can be shown as in Figure 7. Because of the direct transaction experience is the proportion of relatively large, so the end result is close to the direct exchange of evaluation results.

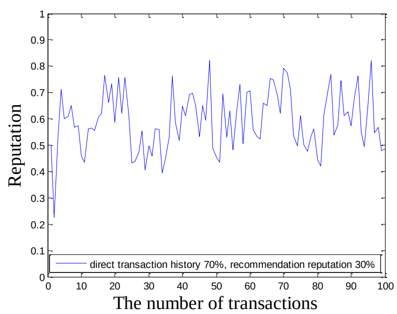

FIGURE 7 Comprehensive direct trading experiences and recommend comprehensive reputation

Node i according $T_{i,j}$ to decide whether to have a transaction with node j, assume node i set transaction threshold ω_i, so when $T_{i,j} > \omega_i$, said node j has reached the credibility of the transaction threshold, so the node i and node j transactions, otherwise, the node i refuse to have transactions with node j.

4 The performance analysis

The results in this paper were compared with several other credit computational model: EigenRep[15], RRM[17_ENREF_17], eBay through analysis of the change of the success of the transaction. The proportion of the experimental hypothesis of honest nodes varies from 20% to 80%. The probability of each node trading is 75%, there are 200 nodes involved in the transaction, the transaction number is 1000, ratio of engaging in honest behaviour of honest nodes is 90%, the malicious nodes in the malicious behaviours of the ratio is 80%. As can be seen from Figure 8, the calculation model of the successful rate of the transaction, contain malicious nodes with EigenRep and RRM are better, because the honest nodes cannot completely guarantee 100 percent satisfied with the service for each other, when the honest node is 80%, transaction success rate is at around 90% however, eBay is relatively low, the transaction success rate is less than 25%. If every node in the network can be honest transactions, namely honest nodes ratio is relatively high, and then various methods can achieve a higher rate of successful transaction. But the actual network, there are a variety of non honest nodes, so it is necessary to analyze each node of the network credit to resist malicious nodes effectively and inspirit honest nodes. As can be seen from Figure 8, in addition to eBay other methods can resist malicious nodes in a certain degree. Because the only relatively inspiriting honest nodes and relative to punish the malicious nodes, while the RRM method with the LCTGS inspiriting honest nodes, so when the honest nodes ratio is very high, the transaction success rate is slightly lower than RRM.

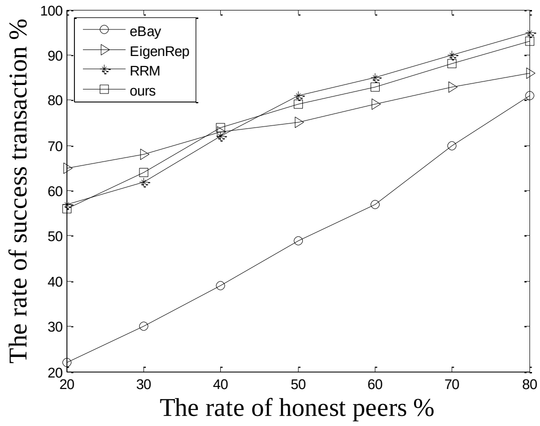

FIGURE 8 Relationship between the rate of successful transactions and honest node ratio

5 Conclusion

Through the calculation and data analysis of the credibility of P2P network, a model of computation with the incentive and punishment mechanism reputation is proposed. This model is not only used the trading experience, but also make use of other node before query reputation and their direct trading experience. By different weights on these data, get a comprehensive credit. Experimental results show that the credit calculation model can get a better transaction success rate.

Based on the design model, we set two assumptions, but in real network environment, these assumptions are not valid. In the cancellation of these conditions, we will focus on how to calculate counterparty credit and make the credit calculation model more perfect and play a greater role in the P2P network, not only can ensure the transaction success rate, but also can effectively prevent the malicious nodes other and avoid some unsafe factors, all of these need more thorough research.

Acknowledgments

The work has been cooperatively supported by the projects as follows:
- PhD Startup Fund of Xinjiang University under grants No. BS120134
- Project of Xinjiang Province Higher Educational Science and Technology Program under grant No. XJEDU2013S08
- The National Nature Science Foundation of China under grants No. 61262088 , 61262089 and 61262087.

References

[1] Cornellu F, Damiani E, di Vimercati SDC, Parboschi S, Samarati P 2002 *Proceedings of the 11th International World Wide Web Conference* New York ACM Press Honolulu HI USA 376-386
[2] Hua S, Hui-Gun Y, Nianhua Y 2011 *Acta Electronica Sinica* **39** 104
[3] Xiaohui L.,Jingsha H.,Ting Z. 2012 Hzlg,
[4] Resnick P., Zeckhauser R. 2002 Elsevier Science, Amsterdam,
[5] Sabater J., Sierra C. 2005 Artificial Intelligence Review, 24, 33
[6] Wang Y., Lin K.-J., S.Wong D., Varadharajan V 2009, *SOCA*. Springer-Verlag London, p. 129
[7] Josang A., Ismail R., Boyd C. 2007 Dec Supp Syst, 43, 618
[8] Chong S.-K., Abawajy J.H., Dew R.A., July 11-13 2007, *6th IEEE/ACIS International Conference on Computer and Information Science (ICIS 2007)*. Melbourne, Australia p. 776
[9] Sun H., Huiqun Y., Nianhua Y., Li L., April, 2011 *2011 International Conference on Computer, Electrical, and Systems Sciences, and Engineering*. Information Engineering Research Institute, Wuhan, China, p. 485
[10] Udoh E., 2013, Information Science Reference, Hershey, PA
[11] Rodriguez-Perez M., Esparza O., Muñoz J.L., March 16-20,2008, *Proceedings of the 2008 ACM symposium on Applied computing Fortaleza*, Ceará, Brazil, p. 2019
[12] Shelton T., 2013, John Wiley & Sons, Hoboken, N.J.

[13] T.Klingberg, R.Manfredi, June 2002.
[14] Winai W., Liberal Rocha F., Moorsel A.v. 2013 Newcastle University, Newcastle upon Tyne
[15] Kamvar S.D., Schlosser M.T., Garcia-Molina H. *2003 Proceedings of the 12th International World Wide Web Conference (WWW 2003)*. New York: ACM Press, Budapest, Hungary, p. 123
[16] Wen D., Huaimin W., Yan J, Peng Z 2004 *Journal of software*, 15, 571
[17] Hong Z., HaiXin D., Wu L. 2008 *Science in China Series F: Information Sciences*, 51, 1871

Authors

Sun Hua, November, 1977, Xinjiang

Current position, grades: associate professor.
University studies: East China University of Science and Technology.
Scientific interests: information security and reputation management.
Publications: 20.
Experience: working experience of 14 years, more than 10 scientific research projects.

Yu Jiong, September, 1964, Xinjiang

Current position, grades: professor at the School of software at Xinjiang University. Senior member of the IEEE and CCF, a member of the ACM.
University studies: Beijing Institute of Technology.
Scientific interests: software architecture and computer network.
Publications: 60 papers.
Experience: Awarded three National Natural Science Foundation research grants and several grants from other sources.

Zhang Zhenyu, February, 1964, Xinjiang

Current position, grades: associate professor.
University studies: University of Electronic Science and Technology.
Scientific interests: opportunistic computing, and social network.
Publications: 40 papers.
Experience: working experience of more than 20 years, many research projects.

Jiang Hong, December, 1976, Xinjiang

Current position, grades: associate professor.
University studies: Xinjiang University
Scientific interests: digitized manufacture
Publications: more than 30 papers published in various journals
Experience: working experience of 14 years, more than 10 scientific research projects.