# A Peer-to-Peer Game Model using Punishment Strategies

Chunzhi Wang[1], Hongwei Chen[1, 2], Ke Zhou[1], Hui Xu[1], Zhiwei Ye[1]

[1]School of Computer Science and Technology, Hubei University of Technology, Wuhan, China
[2]College of Computer Science & Technology, Huazhong University of Science and Technology, Wuhan, China
Email: chw2001@sina.com, chw75@sohu.com

***Abstract*—Recent years, with the rapid development of P2P networks, the security problem of these networks has become increasingly obvious. According to the behavior of selfishness and betrayal for nodes in P2P networks, this paper analyzes and contrasts the benefits of these nodes, and presents the P2P game model with the penalty factor. The reasonable analysis and simulation by gambit prove that, addition of the penalty factor has certain constraints on the betray nodes and promotes the active cooperation of these nodes, thus improves the security status of P2P networks.**

***Index Terms*—P2P networks, penalty factor, game model, gambit**

## I. INTRODUCTION

Recent years, applications of P2P networks become wider, which include cooperative handling, file sharing and distributed storage etc. P2P networks have become the mainstream development model for future networks. In P2P networks, all nodes are equal, which means that they are both client-side and server-side. Thus these networks have no center, self-organization as well as scalability. However, the nodes in P2P networks behave more selfishness and chase their own networks to maximize revenue [1]. Judging from all that mentioned above, it will cause following issues.

(1) The problem of free-riding. For example, a test [2] obtains the following data, which is that 70% of nodes in the networks do not share any files, and nearly 50% of information search is from only 1% of nodes.

(2) The problem of tragedy of common. As non-exclusive public possessions, the resources in P2P networks are downloaded and used by a majority of uncontrolled nodes in these networks.

Trust exists in the social life, which means that someone believes the future behavior of others. It can also be used to resolve the safety problem in P2P networks. Furthermore, it can resolve the trust problem between nodes. By the game theory hypothesis which is based on the node's entirely rationality, it can make the nodes rational and grasp their mental state among the processes during which they interact with others. For instance, do they trust them; how the nodes will change in strategy selection when their interactive objects betray them. The paper tries to sum up the game processes between the nodes and adjust a number of factors in order to make the nodes tend to trust other nodes.

Some studies indicate that it can establish an effective confidence-building model [3] to resolve such security problems to some extent. Currently, there are some fruitful results about studies on constructing trust models for P2P networks, which are summarized as follows.

(1) Trust models based on Bayesian networks. This kind of models gives a node two trust degrees, derives its certainty factor according to its cooperation in the network and also based on Bayesian networks, thus then it cooperates with other nodes selectively with trust degree as its premise. The weakness of this model is that, the network model considered in this model is too rational, and the nodes are not classified, thus in this case, some "extreme" nodes such as malignant nodes are not further analyzed, lacking corresponding constraint management methods.

(2) Trust models based on PKI. This type of models is supervised by a few leading nodes with CA certificates, which maintain the stability of networks, manage the trust degree, and synchronously notify and penalty offending nodes. But this type of models is maintained by a few nodes, thus is weak in extensibility and may cause the problem of one-node-disability.

(3) Trust models based on Eigen Trust algorithm. This kind of models promotes network nodes deal with each interaction rationally by certainty factors. And the global certainty factor of a node relies on its neighbor nodes and satisfactory degrees of interactive nodes historically. It also has weaknesses, which are the lack of considering the cooperative cheating action of malignant nodes in the network, the problem of deciding the trust degree of new adding node, and the complexity problem.

(4) Trust models based on NICE. In this type of models, nodes interact and create a cookie for other side.

This work was supported by Natural Science Foundation of Hubei Province of China (2009CDB100), and Foundation of Wuhan Twilight Plan Project (201050231084).

© 2010 ACADEMY PUBLISHER
doi:10.4304/jnw.5.11.1357-1364

According to the cookie being positive or negative, other nodes can judge the quality of interacting nodes. However, this type of models still cannot improve the problem of cooperative cheating action of malignant nodes in the network, and control new adding malignant nodes.

(5) Trust models based on RG Trust algorithm. This kind of models is different from methods that centralize trust management or formation of global trust degree by neighbor nodes. This kind of models combines game theory and uses improving policies, which makes the cooperation that is not completed in one interaction realized in multiple repeated interactions. Thus nodes will not choose to betray for only one benefit. This kind of models has problems, which are it can not differentiate penalties for occasional mistakes of gracing nodes and repeating mistakes of malignant nodes, and it has difficulty in holding random probability P.

According to the problems exist in these trust models, this paper combines forecast and Punishment Strategies together, and uses the Markov chain to forecast future multiple time scales for current network running environments, and based on the forecasting results, adopts corresponding Punishment Strategies. In detail, it counts violation actions of network nodes, thus effectively reduces the penalty for occasional mistakes of gracing nodes and deals with new adding nodes equally. Finally it promotes network nodes tend to cooperate in a macro view and maintains the stability for the running of P2P networks.

## II. THE PLIGHT OF THE TRUST GAME

Trust game[7] is applied as a game theory into P2P networks; it treats the node's trust relation as a game. In a simple model of a one-time trust game, it can be supposed that there are two nodes 1 and 2; they are ready to interact and have two strategies to choose cooperation or betrayal. And their choice will not affect others, following the table 1. The model indicated the loss as V (V>0). The communication loss is needed for each node to pay in the interactive process. At the same time, these nodes enjoy the services from the networks. The income is assumed as U, and U>V. Nodes choose different strategies, their revenue will be changed, and the specific distribution of nodes' income is shown in Table 1. It is easy to find that the strategy combination (betray, betray) with the node 1 and 2 is the unique Nash equilibrium[8]. Because any nodes change their strategy from betray to cooperation, this change will make the benefits of the nodes from 0 to –V, these two nodes can not build the trust of one-time game. And the two sides have plunged into "Prisoner's Dilemma" [9]. This is called as the plight of the trust game.

TABLE I. TRUST GAME MODEL

| | | *Node 2* | |
|---|---|---|---|
| | | trust | betray |
| *Node 1* | trust | U-V,U-V | -V ,U |
| | betray | U,-V | 0 , 0 |

Prisoner's Dilemma is used to explain between the best personal income and the best overall income. In real life, many areas appear this contradiction such as battle of the advertisement business, the arms race of the politics, etc. and the "plight" [10] is also appeared in the behavior game of the nodes' interaction in P2P networks.

After analyzing the current trust game models[11] which are proposed by some scholars at home and abroad. The development of trust game model can be summarized as follows.

Reference [12] proposes a management model of nodes' credit in P2P networks by analysis the plight in implementation of individual rationality and collective rationality. This model reduces the time complexity of calculating credit and packet traffic, but the model doesn't consider the nodes' collusion in P2P networks, as well as how to treat the new network nodes differently. Reference [13] is also based on the Prisoner's Dilemma, and it proposes a method to improve the trust relationship between network nodes by adjusting the related factors of the game revenue's mechanism. It solves the trust plight between nodes from the macro level. But more practical issues in P2P networks are not considered, such as how to select the appropriate strategy for nodes of different types in the network, and how to encourage the nodes contribute more resources. The model built by the Reference [14] is based on game theory, with the view of maintaining fairness for nodes. It allocates more bandwidth and incomes for the nodes which contribute more resources. This model sets motivating factors which are the nodes' income and contribution, in order to achieve optimal Pareto about the allocation of bandwidth resources, ultimately maximize social benefits. However, some problems exist in this model; for instance, the model can not treat different between the new nodes and other nodes in existence, and adapt the active state about more frequent entering and exiting by nodes. Reference [15] proposes an incentive scheme which is based on the quality of differential services, but this scheme doesn't consider the nodes' collusion problem in P2P networks, and it doesn't discuss the contribution of the new nodes.

After researching the correlation model, it can be found that the existing and mature trust game models[16] in P2P networks usually gives nodes the trust degree, or regulates the parameters of game mechanism[17], and then the model from this point to inspire nodes being more rational, or more trusted choice. But it always takes

© 2010 ACADEMY PUBLISHER

the appropriate adjustment[18], which aims at the appeared question and does not consider from the forecast point to anticipate the future network environment, and can not take a more active strategy in advance based on predicting network state. This paper just uses this method[19] to take timely punishment strategies for the nodes' behavior in the network, and carry on the constraint, supervision, and maintenance. The proposed method prevents the status of networks moving in disorder, which leads the network environment being more secure and more trustful in advance.

## III. CONSIDER THE PENALY FACTOR OF THE NODE'S GAME MODEL

Through analysis of the trust dilemma above, the model of P2P trust game is proposed, and it is based on punishment strategies. The main idea of this model is that if the nodes take the betrayal strategy when they are trusted by the object, the networks will punish it immediately. This model will make the node rational and choose cooperation rather than betrayal in the coming interactive strategy. After the virtuous circle of this strategy, the node can get rid of the dilemma better and improve the trust problem in P2P networks. Ultimately, the P2P networks are able to be in the state of more cooperation.

### *A. The payoff matrix of different types of nodes*

This paper collects several nodes' interaction and summarizes the node type as follows.

- Trusted nodes ($N_c$): these nodes always actively choose the cooperative strategies when they interact with any node, they rarely betray others, or make mistakes.
- Betrayal nodes ($N_d$): these nodes always want to achieve the biggest gains through the selection strategies. So they choose non-cooperation strategies constantly.
- Free nodes($N_r$): these nodes randomly select the strategy of non-cooperation or cooperation, this paper assumes that the probability for free nodes to choose cooperation strategy is P (0<P<1), the non-cooperation is 1-P.

The gains of different nodes have been summarized after N times game as the following tables.

TABLE II. THE GAINS OF TRUSTED NODES WITH OTHERS

| | | ***Node2*** | |
|---|---|---|---|
| | **Trust** | **Betray** | **Free choose** |
| ***Trusted nodes*** | N(U-V) | N(W-V) | NP(U-V)+N(1-P)(W-V) |
| | N(U-V) | N(U-W) | NP(U-V)+N(1-P)(U-W) |
| | 2N(U-V) | N(U-V) | N(1+P)(U-V) |

TABLE III. THE GAINS OF BETRAYAL NODES WITH OTHERS

| | | ***Node2*** | |
|---|---|---|---|
| | **Trust** | **Betray** | **Free choose** |
| ***Betrayal nodes*** | N(U-W) | 0 | NP(U-W) |
| | N(W-V) | 0 | NP(W-V) |
| | N(U-V) | 0 | NP(U-V) |

TABLE IV. THE GAINS OF FREE NODES WITH OTHERS

| | | ***Node2*** | |
|---|---|---|---|
| | **Trust** | **Betray** | **Free choose** |
| ***Free nodes*** | NP(U-V)+ N(1-P)(U-W) | NP(W-V) | NP2(U-V)+ 1/2NP(1-P)(U-V) |
| | NP(U-V)+ N(1-P)(W-V) | NP(U-W) | NP2(U-V)+ 1/2NP(1-P)(U-V) |
| | N(1+P)(U-V) | NP(U-V) | 2NP2(U-V)+ NP(1-P)(U-V) |

The probability in the t moments that is supposed for the chance when the node encounters the node which chooses the cooperative strategy is P1. So it can be supposed

$$P_1 = \frac{N_c + PN_r}{N_c + N_r + N_d} \tag{1}$$

In the t moments, the probability of the node encountering the betrayal node is P2. So it can be supposed

$$P_2 = \frac{N_c + (1-P)N_r}{N_c + N_r + N_d} \tag{2}$$

Combining with the table 3, it is easily to get the total earnings of $N_c$, $N_r$ , $N_d$ -- $T(N_c)$, $T(N_r)$ and $T(N_d)$ is

$$\begin{aligned} T(N_c) &= (U-V)P_1 + (W-V)P_2 \\ T(N_r) &= (U-V)PP_1 + (U-W)(1-P)P_1 + (W-V)PP_2 \\ T(N_d) &= (U-W)P_1 \end{aligned} \tag{3}$$

A prerequisite as W>V is considered, by the theorem: the sufficient condition satisfies the Nash equilibrium steady state and makes the trusted nodes always get the biggest earnings:

$$T(N_c) > T(N_r) > T(N_d) \tag{4}$$

**Proof:** By the equation (1) , $U > W > V$ , it will get:

$$T(N_c) - T(N_d) = (2U - W - V)P_1 + (W-V)P_2 > 0$$

$$T(N_r) - T(N_d) = (W-V)PP_1 + (W-V)PP_2 > 0$$

© 2010 ACADEMY PUBLISHER

$T(N_c)-T(N_r)=(W-V)(1-P)P_1+(W-V)(1-P)P_2>0$

So it can prove that $T(N_c)>T(N_r)>T(N_d)$.

### B. Establishing the punishment game model

Through analyzing the influence that punishment strategies affect on the income of three types of nodes, this paper constructs the punishment game model of the network nodes in a macro view, expressing as follows.

TABLE V. THE GAME MODEL WHICH HAVE THE PENALTY FACTOR

| | | *Node 2* | |
|---|---|---|---|
| | | trust | betray |
| *Node 1* | trust | U-V, U-V | -V+W, U-W |
| | betray | U-W,-V+W | 0 , 0 |

As shown in table V, it can be found that when the node has betrayed its interactive objects that select trust strategy, the node will be punished and make it pay the value of W, W is the penalty factor set in this paper, and the assumption is W>V, at the same time, the victim node will receive the same benefit as earnings of W. As a result, penalty factor changes the Nash equilibrium point of the payoff matrix. The point in this game is (cooperation, cooperation).

## IV. THE DISCUSSION OF PENALTY FACTOR

Now that the penalty factor is discussed and analyzed, the purpose of advancing the penalty factor is to increase the positivity for the nodes' choice of cooperative strategy, and beating fluke mind of betrayal nodes and guiding the non-cooperative nodes will incline to choose cooperation after repeatedly interacting with other nodes. At the same time, the penalty factor will ensure the stability of the entire P2P networks.

### A. Deduction of penalty factor

In this paper, formula of the penalty factor W is:

$$W=V+\frac{1}{t-t_a}\sum_{k\neq t_0}^{t}D(k)+V[\pi_3+(1-p)\pi_2-\pi_1] \tag{5}$$

The last time when the nodes choose betrayal is $t_a$, D (k) is the number of the nodes chooses non-cooperative strategy when their objects choose cooperative strategy. When D (k) =0 and W=V, from the time $t_0$, when the nodes enter the networks, if the nodes always maintain the cooperation with others, it will not be punished. When the nodes have the fluke mind in the first time at t moment, it betrays others, then in the next moment, the nodes will be punished, and should pay for W. From the causes above, it proves further consequence that the more trust nodes in the network; the less the nodes betray others; the smaller D(k) will be, the farther the time when the nodes betray others than the last time, the smaller $\frac{1}{t-t_0}$ will be, so that the penalty factor will be smaller.

### B. Markov chains forecast function of the model

This paper summarizes the converted trends of three state nodes through counting up the behavior of network nodes, shown as follows.

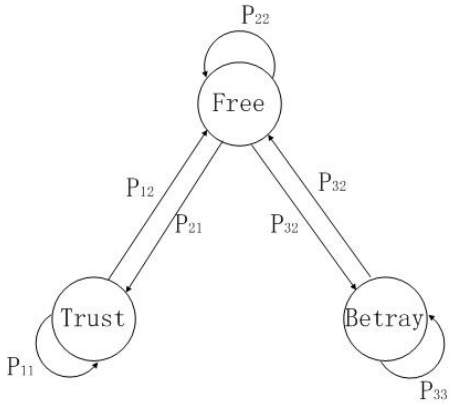


Figure 1. transition diagram of network nodes states

As shown in Figure 1, each node can only transfer to itself or to the adjacent state, and can not stride the transition, for instance, the trustful node can not directly transfer to betrayal node. This transferred trend of states follows the behavioral rule of nodes in the network, that is if the nodes have the fluke mind, through gradual betrayal, their probability of cooperation will decrease, and then their transferred trend of states will follow as: trustful → free → betrayal.

Markov chains[20] are used for forecasting, with the formulas which are commonly used as follows.

If the state space $I$ of Markov chains $\{E_n : n\geq 0\}$ is finite set, and its transition probability matrix $P_{ij}$ satisfies $P_{ij}>0, \forall i,j\in I$, then there exists a only probability distribution $\pi=(\pi_1,\pi_2,\pi_3,...,\pi_n)$ in $I$, and this distribution makes $i,j\in I$ and $\min(Pi_j : i,j\in I)\leq 1/n$ have:

$$1)\ \pi=\pi P$$
$$2)\ \lim_{n\to\infty}P^n=\pi_1^T \tag{6}$$

The mechanism counts the nodes' status in every other t times based on the forecasting methods of Markov chains, supposing in t time, the status of three types of nodes in the network is $E, E\in(En, n=1,2,3)$, the initial distribution of node status is $\pi(0)=(\pi_1(0),\pi_2(0),\pi_3(0))$, the transition probability matrix of nodes status can be built according the condition of nodes' state transition. It can be assumed

© 2010 ACADEMY PUBLISHER

that the number of nodes is $m_i$ in $E_i$ state, the count of the nodes which from $E_i$ state transfer to the $E_j$ state is $m_{ij}$ . The transition probability of states $P_{ij}$ can be obtained, when the network nodes in $E_i$ state transfer to the $E_j$ state, furthermore, $P_{ij} = m_{ij} / m_i$ . Then the transition matrix of three states nodes in network, P can be concluded:

$$p = \begin{bmatrix} p_{11} & p_{12} & p_{13} \\ p_{21} & p_{22} & p_{23} \\ p_{31} & p_{32} & p_{33} \end{bmatrix} \quad (7)$$

The prediction mechanism can get the transfer case of the network nodes' future status at any time, which is based on the transfer matrix of varies states of the nodes. So supposing that in n time, the transfer matrix about any types of the network nodes is $P^{[N]} = P(0).P^n$ , and by $\pi = \pi \cdot P$ , the steady-state distribution vector in regard to the three types of the network nodes(trustful , free , betrayal) is $\pi = [\pi_1, \pi_2, \pi_3]$ .According to the distribution vector on various types of the nodes, this paper concludes the status equation S combines with the network running as follows

$$S = P_3 + (1 - P)P_2 - P_1 \quad (8)$$

### C. The combination of Markov and punishment factor

The management mechanism is installed in P2P networks in order to directly control and constraint the behavior of the network nodes. It can be assumed that the nodes enter the network in the first time, at the time T=$t_0$, combining with the punishment strategies which are designed for the network, the running rules of the management mechanism are as follows.

Step 1 First, the nodes' interaction history in t time is counted, the probability distribution of the three future states of the network nodes can be predicted, is $\pi_0 = [\pi_1^{'}, \pi_2^{'}, \pi_3^{'}]$ , it can make decision that whether choose the punishment strategies or not to node i, and based on the initial conditions of the penalty factor.

Step 2 According to the result of the state equation S, if S>0, it is shown that the network is tend to deterioration, then the management mechanism will take the punishment strategies in the next time. Or if S<0, it can be found that the network in optimum operation, then the management mechanism will enter into step 3.

Step 3 If S<0, the mechanisms will keep supervising the environment of network in the next time, and access to step 1. If the network environment continues to maintain a good running, the mechanism will only be engaged in a supervisory role. However, if the environment is more deteriorative than the predicted result in the last time, the management mechanism will enter into step 2 in time, and takes the punishment strategies to the network nodes.

Step 4 After the management mechanism executed the punishment strategies, it needs to compare the predicted result in last moment with the network future state which is lately used the punishment strategies. If the network state has a good trend, it can be confirmed that this punishment strategy is an effective way for the network, otherwise, the mechanism needs to adjust the parameters of the strategies continually, or to use a more accurate way to predict and to control in advance.

## V. THE SIMULATION AND IMPLEMENTATION

First, this paper makes a pursuant analysis for the game behavior of a single node in P2P networks, and combines the interactional situation of the nodes with the actual and running environment of the network; finally, it simulates the nodes' game behaviors by Gambit. The trend of nodes' behavior selection is compared, which is based on whether the mechanism is carried on, so parameters this paper discussed above are gave real values, in order to have more intuitive analysis of the impact of the penalty factor for the game result of each node and the strategies selection of the nodes.

It can be assumed that when the nodes choose cooperative behavior, they will get the benefit U=9, and they must pay for the loss of network communication, V=4, penalty factor W=6, Figure 2 is the game simulation chart of the P2P nodes which do not execute the management mechanism, however, Figure 3 is the result about the game model simulation after the mechanism is ran. Observing the following two figures, it is clearly found that the nodes will more incline to cooperate with others by restraint and supervision from management mechanism, rather than betray others by a fluke in order to gain a poor income. So it can get the conclusion that the management mechanism have a more positive impact on the behavior choosing of the nodes, it can effectively maintain stability of the network in detail.

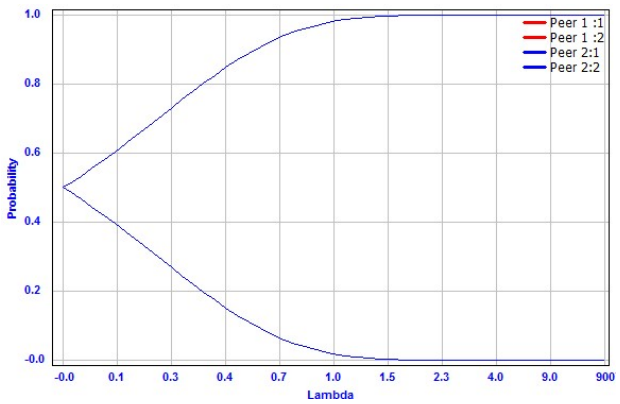


Figure 2. The simulation curve of the nodes' game which is not restricted by the management mechanism

© 2010 ACADEMY PUBLISHER

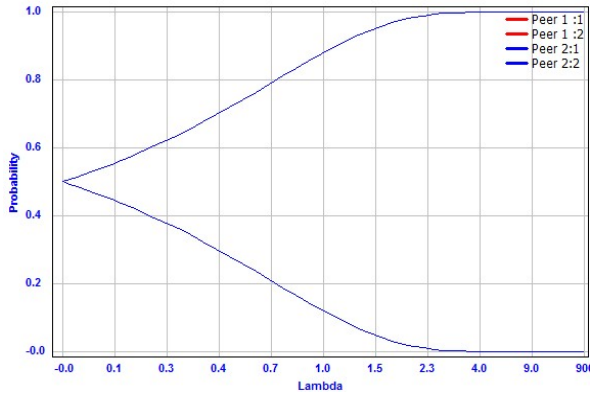


Figure 3. The simulation curve about the nodes' game which is restricted by the management mechanism

Secondly, the thesis simulates the real condition of the P2P network as a whole, obtains the real-time data, and draws a discriminative statistics about the three types of the nodes, before and after the management mechanism is executed. It can count the distribution probability of network nodes by Markov chains, ultimately, the next n-times transferred circs of the nodes are simulated and forecasted by Matlab. The probability distribution about the three types of nodes in the network can be assumed, is $\pi_0 = [1,0,0]$, the transition matrix of the three types nodes' states is $P_1$, which can be obtained based on the real-time data.

This paper predicts that the next 20 times transferred circs of the nodes which are not restricted by the management mechanism, as is shown in Figure 4. Through the graph, it can clearly observe the future trend of three types of the nodes; various nodes are affected by a fluke due to the management mechanism does not supervise and restrain, it leads the nodes take more choice of betrayal. However, the vicious behavior is not got an availably control by punishment, in the end, the operation environment of the network will be deteriorated in the future.

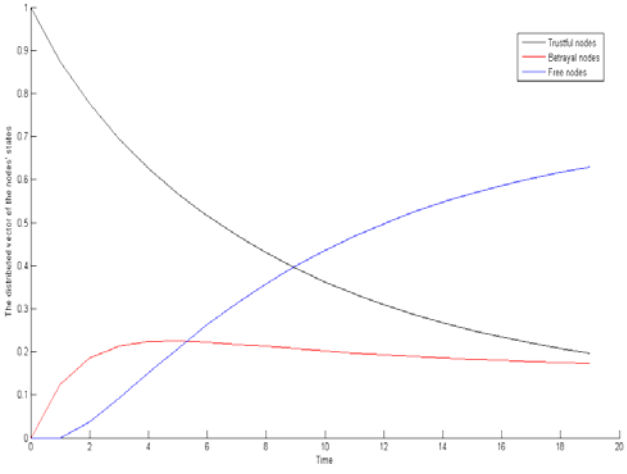


Figure 4. The transferred diagram of the nodes' states out of restriction from the management mechanism.

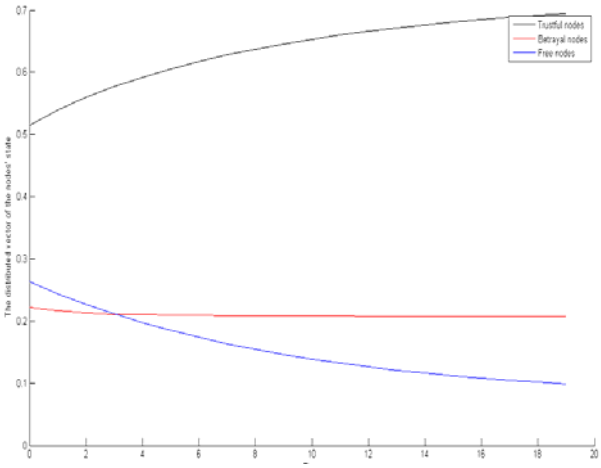


Figure 5. The transferred diagram of the nodes' states by restriction from the management mechanism

Because of the prediction about the transferred trend of the nodes in the future, in t+1 time, this paper installs the management mechanism in the network, and then the mechanism punishes the vicious behavior of the nodes in time, the transferred matrix about the nodes is $p_2$, which will be obtained in the next time by statistics for the transferred situation of the nodes. Now, the mechanism predicts the nodes' transferred situation in next 20 times once again, and Figure 5 shows the simulated result. Compared to Figure 4, it can be clearly observed that the management mechanism has a positive impact on the nodes' transferred situation, as long as the mechanism takes a restrained hand for the nodes' behavior, a slight change will be produced in the nodes' transferred trend, furthermore, the major change will be engendered in the future trend of nodes' behavior in the whole network. It also can be assumed that the existing of the mechanism plays a positive role in punishing the nodes' betrayal and network's stabilization, and it makes accessorial action about the trust between the nodes, and the choice of the cooperation.

This paper also notes that the changes of a single node's behavior selection will play an impact on the network. So the management mechanism is necessary, and it is also needed the mechanism to track and predict for the status of the nodes, in order to prevent the network from paralyzation.

## VI. CONCLUSION

This paper begins with the security issues of the P2P networks and the plight of the node trust game, concludes the deficiency of correlative game model through researches the various types of trust models. Ultimately, the Markov prediction game model which is based on the punishment strategies is proposed. This paper classifies the type of nodes, through comparing with the influence of the game model which execute punishment strategies or not, then sets management mechanism which summarizes the transfer matrix of various types of nodes, and predicts the future state of network development.

© 2010 ACADEMY PUBLISHER

After reasonable arguments and corresponding simulation experiments, it is clearly confirmed that the management mechanism with predictive ability plays a maintainable and preventive role in the network state. And the punishment strategies that are adopted in time by this mechanism, possesses a constrained and punitive action for the betrayal of nodes. Finally, this mechanism plays certain significance for resolving the security problems in P2P networks in a both micro and macro level.

## ACKNOWLEDGMENT

We would like to thank the reviewers and editors for their detailed and valuable comments.

## REFERENCES

[1] Hughes D, Coulson. G, and Walkerdine J, "Riding on Gnutella Revisited: the Bell tolls," *IEEE Distributed Systems Online*, vol. 6, pp. 1–18, Jun 2005.
[2] Hardin G, "The Tragedy of the Commons," *Science*, vol. 162, pp. 1243-1248, March 1968.
[3] Wang Y, Vassileva J, "Bayesian Network-based Trust Model," *Proceedings of the IEEE/WIC International Conference on Web Intelligence(WI'03)*, Halifx, Canada, pp. 372-378, 2004.
[4] Dou Wen, Wang Huai ming, "A recommendation based peer-to-peer trust model," *Journal of Software*, vol. 15, pp. 571-583, Apr 2004.
[5] Sepandar D, Kamvar, Mario T, Schlosser and Hector Garcia Molina, "The Eigen Trust Algorithm for Reputation Management in P2P Network".
[6] Khambatti M, Dasgupta P, Ryu K D, "A role-based trust model for peer-to-peer communities and Dynamic Coalitions," *Proceeding of the Second IEEE International*, Information Assurance Workshop, New York, IEEE Press, pp. 141-154, 2004.
[7] Wang Tao, Lu Xian liang, "A Novel Peer-to-Peer Incentive Mechanism Based on Game Theory," vol. 15, pp. 201-203, Feb 2006.
[8] C. Buragohain, D. Agrawal, S. Suril, "A game theoretic framework for incentives in P2P systems," *In: Proc. 3rd Int'1 Conf. Peer-to-Peer Computing*. Los Alamitos, CA: IEEE Computer Society Press, 2003.
[9] M. L Littman, "Value-function reinforcement learning in Markov games," *j Of Cognitive System Research*, vol. 2, pp. 55-66, 2000.
[10] Myerson R B, "Game theory: analysis of conflict," *Massaehusetts: Harvard University Press*, 1991.
[11] Aberer K, Despotovic Z, "Managing trust in a Peer-to-Peer information system," *International Conference on Information and Knowledge Management*, New York, ACM, pp. 310-317, 2001.
[12] Liu Ye, Yang Peng, "Study of Mechanism of Trust Management to P2P Networks Based on the Repeated Game Theory," *Journal of Computer Research and Development*, vol. 43, pp. 586-593, Apr 2006.
[13] Man Hong fang, Yang Rong rong and Liu Feng ming, "Research of trust evolutionary mechanism based on game theory in P2P networks," *Computer Application*, vol. 27, pp. 2710-2717, Nov 2007.
[14] Xu Hai mei, Zheng Xiang quan, Qi Shou qing and Nie Xiao wen, "Novel incentive based on game theory in P2P networks," *Application Research of Computer*, vol. 25, pp. 2787-2788, Sep 2008.
[15] Chen Zhi qi, Su De fu, "Incentives Model in P2P Network Based on Game Theory," *Computer Engineering*, vol. 31, pp. 118-120, Aug 2005.
[16] Dai Zhan feng, We Qiao yan, Li Xiao biao, "Recommendation Trust Model Scheme for P2P Network Environment," *Journal of Beijing University of Posts and Telecommunications*, vol. 32, pp. 79-72, Mar 2009.
[17] Li Gong, "Peer-to-Peer Networks in Action," *IEEE Internet Computing*, pp. 40-42, May 2002.
[18] Gou Jing, Wu Guo xin, Li Xiang, "Research and Design for Trust Model in P2P Networks," *Computer Technology and Development*, vol. 19, pp. 102-105, Mar 2009.
[19] Joseph D, Grunwald D, "Perfecting Using Markov Predictors," *IEEE Transactions on Computers*, vol. 48, pp. 121-133, Feb 1999.
[20] Jin Shao hua, "A Limit Theorem for Markov Chains," *College Mathematics*, vol. 20, pp. 64-67, Aug 2004.

**Chunzhi Wang**(1963-), femal, from Hubei province of China, Master's degree, Professor of Hubei University of Technology, Dean of School of Computer Science, interested in the security of network and computer network, Computer supported cooperative work. The Chairman of Wuhan of CCF Young Computer Scientists & Engineers Forum(2010).

**Hongwei Chen** (1975-), male, from Hubei Province, PHD, Associate Professor of Hubei University of Technology, interested in Peer-to-Peer, Grid Computing, Information Security, Mobile Agent.

**Ke Zhou**(1987-), master candidate of Hubei University of Technology, interested in Peer-to-Peer.

© 2010 ACADEMY PUBLISHER

**Hui Xu** (1983-), PHD, Lecturer of Hubei University of Technology, interested in network and service management. Since 2006, she has been a certified computer system analyst in P.R. China. In July 2008, her biography was selected for inclusion in the 26th edition (2009) of the Marquis Who's Who in the World, California, USA.

**Zhiwei Ye** (1978-), male, from Hubei Province, PHD, Associate Professor of Hubei University of Technology, interested in Computational Intelligence, Image Processing.

© 2010 ACADEMY PUBLISHER