# On Applied Research of Super Trust Model in P2P Networks

Zhike KUANG
Hunan City University, Yiyang, Hunan, 413000, CHINA

**Abstract:** In order to solve the trust problem between nodes in P2P network, it proposes the P2P network trust model Super Trust based on super-peer. In Super Trust, for the trust calculation of ordinary nodes within the same group, it uses the local trust information of the node and the recommendation trust information of owning group to determine the trust value of the target node. The trust evaluation of super node uses the global trust way of the super node within the group computational nodes. Also it puts forward noisy feedback information filtering algorithm to filter the false or unjust evaluation which provided by malicious node. Experimental results show that: This model overcomes some of the limitations of existing models, which can effectively deal with malicious attacks, slander, fraud, conspiracy.

**Keywords:** P2P network; Node trust; Information filtering; Node mapping

## 1. Introduction

In recent years, the rapid application development of P2P networks has become one of the important technologies of affecting the future development of the Internet. The distributed architecture of P2P made it has good scalability and flexibility, but its open, anonymous and self-organizing properties provide a way for the spread of viruses and junk data, and the safety problems caused widespread concern. Blaze, who for the first time the concept of "trust management", the introduction of network services in 1996 [1]. Subsequently, researchers P2P network based on trust management model has been extensively studied.

Depending on the structure of the current P2P networks, trust models into a centralized trust model and distributed trust model. Centralized trust model is equipped with a central server which is responsible for managing the trust of all the nodes, such as PKI-based trust model [2]. Distributed Trust Model has no central server, to determine the trust of nodes evaluated by collecting trust other nodes on the target node. Distributed trust model was classified into global trust model and local trust model in accordance with the trust's search. Processing to obtain global trust model need to find a trusted node in the network of all transactions with the target node over node testimony [3]. The commonly used methods are iterative and feedback entire network. Iterative algorithm iterative global trust value of each node in the network updated until the trust values of all nodes to stabilize based on the trading results over time. The more famous algorithm had early Eigen Rep algorithm model, and model the dynamic Peer Trust TVM algorithm. Convergence of the algorithm and iterative overhead in large-scale network, it has been a major factor restricting the development of this model [4]. After the model-based feedback of each transaction, the transaction client node evaluations will feedback directly to the service node. Typical algorithms have TBRM algorithms and dynamic models Peer Trust PSM algorithm. When this method of calculating the trust is less overhead, the larger scope of malicious attack was being dishonest feedback. How to distinguish between honest and dishonest feedback has been facing challenges such models.

The characteristics of global trust model is that, the system will compute a global trust value for the node base on the historical acts of upload files in each node, and request node to select download source base on global trust values. As global trust model ignores the private characteristics of trust, for a particular node, the trust of other nodes to him are the same values. Therefore, in the large-scale P2P network, whether it is necessary to calculate the global trust value of each node remains to be further studied.

In dynamic adaptive capacity of enhancing trust model, Lee proposed a fully distributed way to store reputation information of a user's. Different with other trusted system, in the NICE system, the trust information stored in node $i$ is the satisfied feedback to the provided services from other nodes, so the nodes have motivated stored trust information [5-7]. In the local trust model based on sharing information, the getting of sharing information generally request for flooding trust from other nodes, such as XREP, in large-scale P2P network has poor scalability. Furthermore, such local trust model based on sharing information is not suitable for the local part of a distributed P2P network.

## 2. The P2P Trust Model

There are four P2P trust model, a trust model is based on super nodes. These models are based mainly on a small number of super nodes in the network to obtain the trust value, such as the common PKI-based trust model. In such models, there are a small number of central node is responsible for overseeing the entire network, the legality of the notice of violation nodes periodically, the central node of the certificates issued by CA to be guaranteed, as long as the individual holding the CA that issued the certificate is considered to be letter. The second is the recommended model based on trust, the trust of the value of the trust model based on recommendation is mainly based on the node to other nodes on the transaction evaluation, in 2003 Kamvar made famous Eigen-Rep global trust model, which is based on transaction history node trust local, consider recommendation trust relationship between nodes, calculate unique global trust value for each node in the network through an iterative degree of mutual trust between neighbors.

In Super Trust, it makes all nodes in the group as a unit to be divided, and each group has only one super-node. Simplicity, Super Trust assume that, each node (if not specifically stated herein "node" refers to common node) belongs to only one group (for a node belonging to a plurality of groups which can be seen as the node in each group there are different identities). Figure 1 is the P2P network structure with a super node, the figure shows the four connections between groups, $S_p$ represents super node. The figure shows three kinds of trust type, in the group $s_1$, setting the relationship between super node $S_p1$ and node $p_2$, and the relationship between $p_2$ and $p_3$ as direct trust relationship, and setting the relationship between $S_p1$ and $p_3$ as the recommended trust relationship. The relationship between $p_2$ and $p_4$ represents the trust relationship between the ordinary nodes in different groups, meanwhile, we characterized the trust relationship between the super nodes $S_p1$ and $S_p3$.

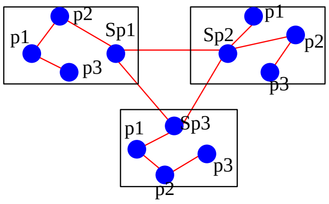

**Figure 1. The P2P network structure with super nodes**

The basic idea of Super Trust is that, the nodes establish local trust relationship to target node according to the transaction. If the target node (for example, $p_3$) is in the same group, the node ($p_2$) will store the transactions of the target node in the local. If the target node (such as $p_4$) is in other groups, then the node ($p_2$) will feedback the outcome of the transaction to its super-group node (SP1). The super node $S_p1$ establishes the trust relationship of super node $S_p2$ in the group of node $p_4$ according to the feedback of node $p_2$. When the node assesses the trust value of other node within the same group, it will calculate the trust value of the node in accordance with the group's reputation-based trust mechanism. The trust value of super nodes is calculated by the global trust in the group with all of its nodes. In the following, it first describes the calculating way of trust between nodes within the same group.

### 2.1. Trust calculating of nodes within the same group

First, it studies the trust computational problems of ordinary nodes in the same group. In Super Trust, the nodes trust calculation is carrying out based on the trust computer system of reputation. To this end, we first give the definition of local trust.

Definition 1 If the node $d_t$ and $d_h$ transacts $d_j$ times throughout the trading period, the local trust (directed trust) of node $d_t$ to $d_j$ is:

$$d(t)=\sum_{i=1}^{N} f(d_i(t)) \tag{1}$$

Where Satmj expresses the number of transactions with satisfaction, UnSatmj expresses the number of transactions with dissatisfaction. We require that if there is no interaction history between both of them, the local trust is 0.

*1) Credibility*

Partial trust is only the limited trust relationships between two nodes after the directly transaction, it is insufficient to fully but accurately evaluate a node. The trust mechanism based on reputation is proved to be a good reflection of trust relationship between nodes in P2P networks. Because we are creating a group in accordance with similar hobbies and aggregation nodes, then the node interaction within the same group is more frequent than the node interaction in ordinary network topology, so it can quickly establish credibility, which can effectively evaluate a node relying on the credibility.

There are various methods of calculating the node credibility. We propose a method of evaluating recommended node trust information by using credibility.

Definition 2 the credibility of Node m means the trust level of node $i$ to the recommended information which expressed by Crim. Credibility has two main characteristics: dynamics and private characteristics. Dynamic change refers to that, the credits changes with the increasing of evaluated times of other nodes provided by node m to node $i$, the private characterize means the reliability of node $i$ is proprietary and not shared for the evaluation of the other nodes.

Node i pooled the trust information of recommended nodes which can be obtained credibility node j. Credibility is the subjective assessment of the cumulative interaction fact of all nodes interacted with node j which reflects the quality conditions of a long historical behavior of $j$.

In Super Trust, we use the requesting node $i$ to weighting its recommendation information through the credibility of all recommended nodes, it was evaluated reputation value of node $j$ after synthesis. Therefore, the credibility of j which calculated by node i is:

$$B_{yij} = \sum_{m\in I(j)} \frac{B_{yj} ar_{im}}{\sum_{m\in I(j)} ar_{im}} \qquad (2)$$

Where, $B_{yij}$ is the credibility of node $j$ after aggregating recommended information by node $i$, $B_{yj}$ is the partial trust from node m to node $j$, $ar_{im}$ is the credibility from node $i$ to recommended node m, I(j) is the recommended collection of node $j$. From (2) it can be seen that, the node $i$ gives a higher weight to local evaluation of nodes with a high reliability.

*2) Calculation of Reliability*

In Super Trust, it requests the node to locally evaluate the recommended node according to the credibility of the recommended nodes. Specifically: after the node $i$ calculated the credibility of node $j$, the recommendation of node m is judged as follows: if the evaluation provided by the node is the same as the comprehensive evaluation of other nodes (i.e., degree of credibility $j$) to a certain extent consistent, which is considered to be correct, then its reliability on the basis of the increase in the original. If the given evaluation is inconsistent with the comprehensive evaluation of other nodes, then its credibility will be reduced based on the original, which then will be on the recommendation of the credibility of the evaluators have a weakening effect.

Wherein, the parameter $0 \prec \varphi \prec \eta \prec 1$, k is an integer as the credibility of node $i$ to node m after $L_{-th}$ recommended. The meaning of formula (5) is that, when the degree of local trust of recommended node m to evaluated node j and the credibility of node $j$ is less than the average deviation of the feedback information provided by all recommended nodes. It is considered the recommendation is credible, the credibility is updated on the basis of the original has a smaller amplitude increase (specific amplitude $\varphi$ (1) (1-RTDim)). Conversely, if the degree of approximation between the two nodes is greater than all the recommended feedback information provided by the average deviation, then the recommendation is credible, credibility is based on the original with a more substantial decline, and we assuming the initial node as recommended credibility of 0.6.

*3) Calculation of Node Trust*

First, it gives the calculation methods of trust between ordinary nodes within the same group. We have the trust between ordinary nodes within the same group:

$$Tr_{ij} = \lambda \times R_{ij} + (1-\lambda)\mathrm{Re}_{ij} \qquad (3)$$

Where $\eta$ is a direct trust confidence factor, $\eta$ values and interaction related to the number, the more the number of interactions larger the value of $\eta$, $0 \le \eta \le 1$. We can take $\eta = h / HLmt$, where h is the node $i$ and node $j$, the number of interactions between, $HL_{mt}$ to set the threshold number of interactions herein value is 20.

## 2.2. Trust calculation of super nodes

In Super Trust, we assume that the initial network joining the P2P network nodes are trusted in the initial stage, which can be used as super-node, because as a whole P2P network builder and the original user, there is no ulterior motive to destroy this network. Meanwhile, we entrust super node the following functions: involved in the transaction, to safeguard their trading results; maintenance group's node management; in addition, super-node also stores the trust information across the node group transactions.

The trust from the node to super node of the group is changing. In Super Trust, the trust calculation of the node to super node is in accordance with global trust calculation, that

$$Trsp_i = \sum_{k\in I(G_i)} (R_{ik} R_{KSP_i}) \qquad (4)$$

Where $Trsp_i$ expressed the trust of super node $sp_i$, $I(G_i)$ is a collection of nodes within the group $sp_i$, $R_{ik}$ represents the partial trust of node $i$.

Thus, to the entire group at a certain moment, the trust of super node is unique, rather than a specific evaluation node itself. Because trust is determined by the interaction result and affected by that, after a certain period of time, there are changes in the node trust. Thus, the entire group of nodes can periodically participate in the assess of the trust. The super nodes which falls below a certain threshold can be replaced with the backup super node replace this super-node, so you can avoid malicious nodes camouflage identity spoofing. The selection of backup super node is decided based on the stability and overall performance of all members.

For the new added ordinary node, we require full trust at the beginning of the super node within the group, with the deepening of their interaction, and gradually adjust to this super node trust relationship. Thus, in Super Trust, the degree trust of node $i$ to super node $sp_i$ is,

$$Trisp_i = \begin{cases} 1, n = 1 \\ \theta Trisp_i, n > 1 \end{cases} \quad (5)$$

Where n is the number of transactions, θ range changes as follows:

$$\Psi^{|R_{ISPi}-s|} \le \theta \le 1-(1-\Psi)\,|\,R_{ISP_i} - s\,| \quad (6)$$

In the above equation, $\psi$ is a constant and $0 \prec \psi \prec 1$, $R_{ISP_i}$ is the direct trust of node i to super node $sp_i$, s is the trust evaluation standard deviation of the set of nodes to super node. In the simulation, $\psi = 1-(1-\psi).\left|R_i sp_{i-s}\right|$.

The trust between super node $sp_i$ and $sp_j$ is established rely on the overall trust evaluation of nodes in $sp_i$ group to $sp_j$ group. The definition is as follows.

When $Sat_{G_iG_j} + UNTrsp_j sp_i = 0$, if there is trust path between $sp_i$ and $sp_j$, then it will calculate the recommended trust $Trsp_j sp_i$ of $sp_i$ to $sp_j$ in accordance with the principle of the strongest path.

The trust $Trsp_j sp_i$ of super node $sp_i$ to $sp_j$ stored in the local cache $sp_i$ (also the preservation of the local intergroup transactions), and has obvious timeliness, because $Trsp_j sp_i$ group nodes based on changes in the number of transactions, as long as the change in the number of transactions, the $Trsp_j sp_i$ of certain changes; and according to formula (10) to be updated.

For the trust path between super node $sp_i$ and $sp_j$, the strongest trust path means the trust path from the most trusted group in $sp_i$ to $sp_j$. Making the smallest trust on the path to be the recommended trust which the trust path identified $sp_i$, then the $Trsp_j sp_i$ will be the strongest recommended trust. If there are many strongest trust paths, then the $Trsp_j sp_i$ will be the average of the recommended trust. As shown in figure 2, there are two strongest trust paths from group A to group B, i.e. “A>G>D>B” and “A>F>H->B”. The recommended trust respectively is 0.4 and 0.2, so, the trust $Trsp_j sp_i$ between groups A to B is $0.4$.

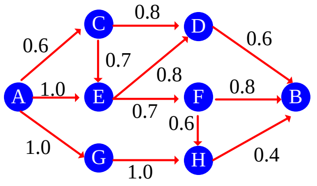

**Figure 2. Example Figure of the Strongest Trust Path**

### 2.3. Trust calculation between nodes

Making $Tr_{ij}$ be the trust of node $i$ to node $j$, if $i$ and $j$ belong to the same group, then calculates $Tr_{ij}$ based on formula (6). No matter the node $i$ is an ordinary node or a super node, since super node participate in the business as the other nodes, so it is also a node of the group.

If $i$ and j don’t belong to the same group, then we will make the trust $Tr_{ij}$ of node $i$ to node $j$ be:

$$Tr_{ij} = \min\left\{Trisp_i, Trsp_i sp_j, Trsp_j j\right\} \quad (7)$$

It is the smallest value among the three. Where, $Trsp_j$ is the trust of super node $sp_j$ which in the same group as node $j$ to super node $j$. As known from the above definitions, the trust range is [-1, 1]. Making 0 as the cutoff point, the greater the trust value of the node is, the more trustworthy it will be. The smaller the value is, the more credible the node is.

## 3. Experimental Simulation and Analysis

### 3.1. Experimental environment and setting

In order to compare with PD Trust, the simulation network uses some of the distributed structure. In Super Trust and RB Trust systems, nodes can save 10 local trust information of nodes, the node or group of trust request message sent TTL of five. In the simulation, assuming that each file system has been own by at least a cooperative node.

Our network environment of simulation is: a total of 1000 nodes, wherein the proportion of malicious nodes is [0.2 ~ 0.6], the number of groups is 20, nodes are randomly distributed to each group, and the number of each group of neighbors is 3 to 5. Better kinds of malicious nodes and good nodes are 100% in active state, and send file requests at a 100% active state. Assuming a simple ratio of 40% malicious nodes provide credible documents, conspiracy to internal node, 100% to provide credible documents, 100% of external un-trusted file number is 10000, the file type is 100, and the file is uniformly distributed on each node. The simulation period is 100, the simulation times are 3, and the results of simulation are average values. Also, assuming that the system can successfully locate all files, and each file of the system is owned by at least one good node. Other parameters are shown as Table 1.

**Table 1. Simulation parameters**

| Parameters | Value |
|---|---|
| $\eta$ | 0.3 |
| $\psi$ | 0.9 |
| $\theta$ | 0.7 |
| $\delta$ | 5 |

First, the simulation experiments detect the anti-attack model. we compared the transaction situation (The successful Transaction Rate, STR) of the three trust mechanism of Super-Trust, PD Trust and RB Trust under the four kinds scenes of SM, DM, CM and CF. The successful transaction rate STR is the proportion of the number of successful trading throughout the all transactions in the network. The successful trading refers to the requesting node accurately downloaded from the response to the desired file; otherwise it will be a failure transaction.

### 3.2. Anti-attack Capability

*1) Simple malicious nodes (SM)*

To the simulation, we assume that the cooperation node provide a credible probability of documents to 0.98, so when the system does not have malicious node, the node's successful request for cooperation was 0 .98. It knows from Figure 3, when the malicious nodes provide only un-trusted files, Super Trust and PD Trust can effectively identify malicious nodes in small proportion of malicious nodes, so the success of co-operative nodes transaction rate decreases slowly as the increase in the proportion of malicious nodes. But with the increase of the proportion of malicious nodes, the Super -Trust system performance indicates a significant advantage. The RB Trust system success rate of requests significantly reduce with the increase proportion of malicious nodes, which is because in the RB Trust system, the node information or the use of local trusted friends and their friend's recommendation to determine the value of the given node's trust. And therefore cannot trust effective access to information for all nodes. Additionally, in our simulation, cooperative nodes may provide un-trusted files because of an error, while malicious nodes in order hide its malicious behavior and provide credible documents with a certain probability, therefore, in RB Trust, nodes may incorrectly assess the credibility of the other nodes, resulting in successful transaction rate.

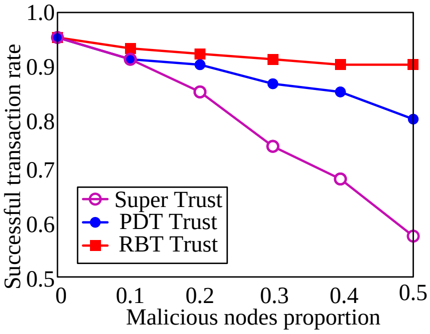

**Figure 3. Comparison of successful transaction rate under SM**

Figure 4 is the rate changes with the successful transaction of the three types of system simulation cycle of Super Trust, PD Trust and RB Trust in the proportion of malicious nodes 0.6. It can be seen, Super-Trust optimal system performance, PD Trust second, RB Trust worst, these show the strong ability to resist attacks of malicious nodes of Super Trust.

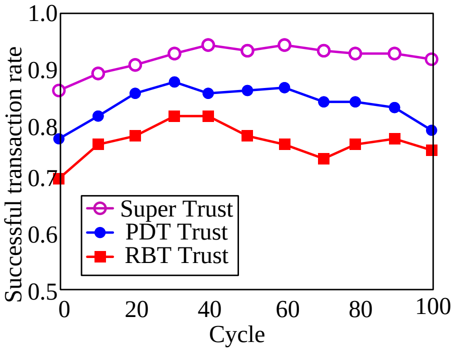

**Figure 4. Changes of successful transaction rate with the period**

*2) Slander Node (DM)*

Figure 5 is the comparison of successful transaction rate of the three systems of Super Trust, PD Trust and RB Trust under the attack of malicious slander node.

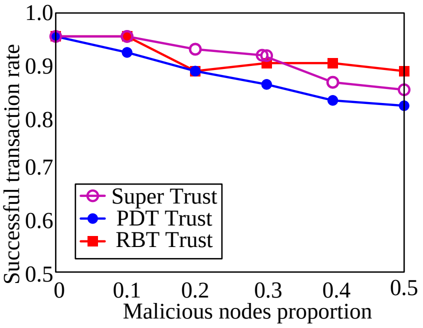

**Figure 5. The comparison of successful transaction under DM**

As can be seen from Figure 5, when the proportion of malicious nodes in system is small, the system successful transaction rate of three mechanisms has little difference, But with the increase in the proportion of malicious nodes, the Super Trust system performance indicates a significant advantage, which because we propose feedback filtering algorithm to filter out the cooperative node slander published injustice information, so Super Trust can effectively identify slander node, leaving most of the attacks ineffective, so when the proportion of malicious nodes reaches 0.6, it also has a higher successful transaction rate. The successful trading rate of RB Trust system decrease rapidly with an increase in the proportion of malicious nodes slander, this is because when there are many slander nodes, the untrue and misleading information of recommended information becomes available, the system can not effectively distinguish these information, the node trust judgment error is large, and therefore can not effectively choose to download the source resulting in successful transaction rate.

Figure 6 is the changes of the three systems successful transaction rate of Super Trust, PD Trust and RB Trust with simulation cycle. It can be seen that, the system successful trading rate of Super Trust rapidly increase with simulation cycle, and ultimately remained relatively stable, and it is always higher than the other two in the entire transaction cycle, showing the strong slander effectiveness of Super Trust against attack.

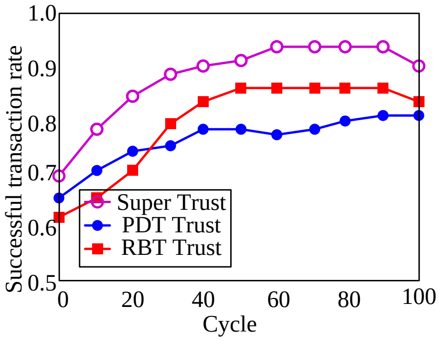

**Figure 6. Changes of the successful transaction rate under DM with the period**

*3) Collusive Fraud (CM)*

Figure 7 is the comparison situation of successful transaction rate of the three systems Super Trust, PD Trust and RB of the malicious nodes.

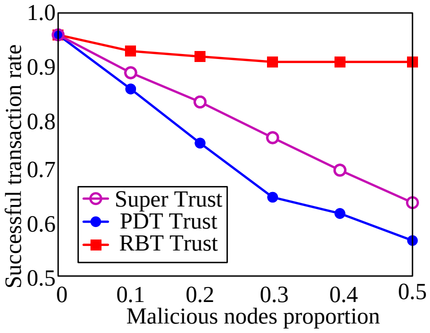

**Figure 7. The comparison of successfully request rate of collusive fraud**

In Super Trust and PD Trust system, a malicious node is associated with a transaction cooperative nodes negative feedback , while there have been transactions with similar nodes provide a high positive feedback . Additionally, malicious nodes may collude with each other frequently submitted for each other high positive feedback. In RB Trust , assuming a malicious node receives another node recommendation trust request, if the inquiry is similar malicious node recommendation trust is given a value of 1 ; otherwise , it is -1.

As can be seen from the figure, with the increase in the proportion of malicious nodes, the successful trading rate of cooperative nodes of Super Trust is much higher than PD Trust and RB Trust system, this is because in the Super Trust, the feedback of information filtering algorithm can filter the most unjust feedback so that when the proportion of malicious nodes is 0.6, the system which can be maintained in successful transaction rate is still close to 0.92. While in PD Trust, the directed update of trusted information allows malicious nodes to give positive feedback and have a high trust value through mutual. Accordingly, in PD Trust, with the increase in the proportion of malicious nodes, the success rate of requests declined sharply in RB Trust, the node cannot be trusted to accurately assess the value of another node, and these assessment malicious inaccuracies node collusion attack is more serious fraud. Thus, in RB Trust, the node can not identify cooperating nodes and malicious nodes, the system's success transaction rate decreased rapidly with the increase in the proportion of malicious nodes.

Figure 8 shows the case of fraud in the collusion, when the proportion of malicious nodes is 0.6, the changes situation of successful trading rate of the three types of system with the simulation period. It can be seen that, the system successful trading rate of Super Trust rapidly increase and eventually remain relatively stable with the simulation cycle. PD Trust and RB Trust system has declined with increased system performance, and the overall performance of PD Trust than RB Trust, because the feedback information directly PD Trust simple summation of the system calculated for each node in the global trust value, when a high proportion of malicious nodes, the system performance is completely controlled by malicious nodes. To the RB Trust, the credibility of information can determine the credibility of a given node according to the local node, so the performance is better than PD Trust.

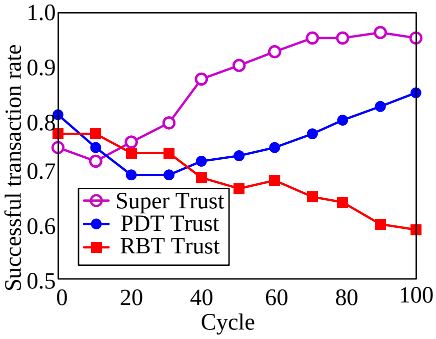

**Figure 8. The changes of successful transaction rate under fraudulent collusion with cycle**

*4) The Collusive Fraud With a Front-end Node*

In the simulation experiments, we assume that the entire front-end node is a proportion of 21% of malicious nodes. In figure 9, we give the successful trading rate of cooperate nodes in Super Trust, PD Trust and RB Trust system with a front-end node under fraudulent collusion attack. While with the various systems malicious nodes under attack fraud conspiracy case were compared.

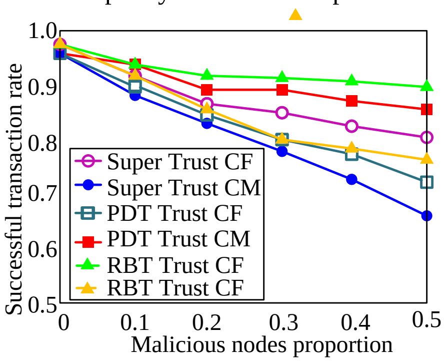

**Figure 9. The comparison of successful transaction rate under CF**

Under the attack of collusion fraud with a front-end node, as the same as in the fraudulent conspiracy of malicious nodes under attack, the successful transaction rate of Super Trust is better than that of PD Trust and RB Trust. But the difference is that, in Super Trust system, the rate of successful trading system under attack in the CM attack is better than the CF, while in PD Trust and opposite RB Trust systems. This is because in the simulation, we set the node Super Trust as long as the number of nodes in the cluster are similar, that all nodes in the cluster as a whole is similar to the attack of CF, malicious concealment of front-end node behavior makes it similar to the node with the increased possibility of cooperation, and to become members of the cluster evaluation, which submitted a highly malicious nodes positive comments in PD Trust and RB Trust systems, the proportion of malicious nodes in the same circumstances, under the attack of CF, the CM system has more nodes to provide valid documents, so the system successful trading has higher attack rate in the CF.

Figure 10 is the comparison between collusion with fraud and conspiracy to fraud under the attack of contrast under the three systems of Super Trust, PD Trust and RB Trust while a malicious node ratio is 0.5. The system performance under the collusion attack has a front end node collusion fraud reasons as described above, however, PD Trust and RB Trust opposite two mechanisms, transaction success rate of the system has a front end node of collusion fraud under all the above. It is because the front end node in the sake of providing effective document, but PD Trust in collusion attack, the system front-end node of the highest reputation, and with the increase of the simulation period, front-end node enhanced ability to provide services, so there cannot be effective from the start node to identify malicious front-end node capabilities, the system performance has the upward trend.

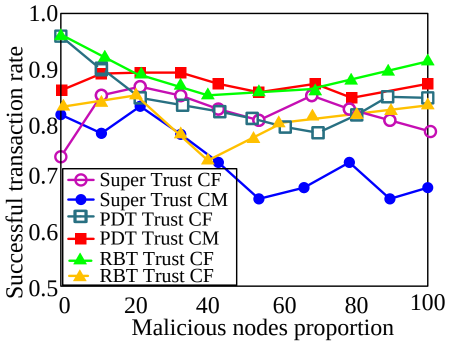

**Figure 10. The changes of successful transaction rate under CF with cycle**

*5) Ratio of Malicious Nodes Affecting the Success Rate for the Download*

In the file download process, malicious nodes percentage success rate for the download has some influence, as shown in Figure 9, because Super Trust for identifying malicious nodes reasonable and effective, and to identify a high success rate, so in this model, the ratio of malicious nodes success rate for download to reduce the influence of some. Super Trust and PD Trust, RB Trust compared to download the success rate has greatly improved, and with the larger ratio of malicious nodes, download success rate declined. Experimental results show that, Super Trust has a stronger ability to resist risks in response to changes in the proportion of malicious nodes.

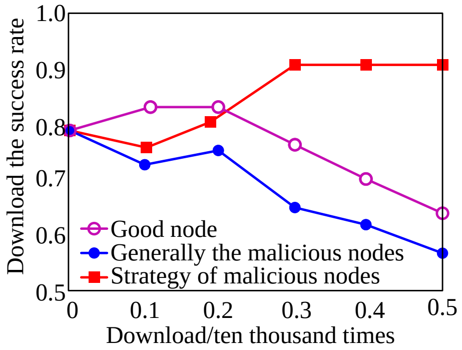

**Figure 11. Downloads affect the success rate of download**

## 4. Conclusion

For the issue of trust between the nodes in P2P networks, this paper presents a P2P network trust model based on super nodes Super Trust. The model for trust ordinary nodes within the same group calculated using the node information and the use of local trust group belongs to recommendation trust information to determine the value of the target node's trust. Trust evaluation super node mode using the global trust group all nodes in the calculation of super nodes.

## References

[1] Raul Medina-Mora, Kelly W. Cartron. ActionWorkflow in Use: Clark County Department of Business License. In Proceedings of the Twelfth International Conference on Data Engineering, IEEE Computer Society Washington, DC, USA, 1996: 288-294.

[2] Jian Yun, Xiaotong Li, Chunxia Wang. Simulation of Conducting Early-warning to the Endangered State of Language. Journal of Multimedia, Vol 8, No 5 (2013), 475-480.

[3] Edward A,Stohr J, Loan Zhao. Workflow Automation: Overview and Research Issuse, Information Systems Frontiers, 2010, 3(3): 281-296.

[4] Y Yang. An Architecture and the Related Mechanisms for Web-based Global Cooperative Teamwork Support. International Journal of Computer Information, 2000, 24(1): 13-19.

[5] Fei Liu, Guangzhou Zeng. A Multiagent Cooperative Learning Algorithm. Lecture Notes in Computer Science, 2007,4402: 739-750.

[6] Benatalhth B,Sheng Q Z,Dumas M. The Self-serv Environment for Web Services Composition. IEEE Internet Computing, 2013, 7(1); 40-48.

[7] J. Yan, Y Yang, G K. Raikundalia. SwinDeW-A P2P-Based Decentralized Workflow Management System. IEEE Transactions on Systems, Man and Cybernetics, Part A: Systems and Humans, 2012, 36(5): 922-935.