Trusted Decision Mechanism Based on Fuzzy Logic for Open Network

Zhang Lin, Wang Ruchuan, Wang Haiyan
College of Computer, Nanjing University of Posts and Telecommunications, Nanjing, China
Email:cumt-zhanglin@163.com

Wang Ruchuan
State Key Laboratory for Novel Software Technology, Nanjing University, Nanjing, China
Email:wangrc@njupt.edu.cn

***Abstract*—Trust mechanism will be an important trend in the field of security for open network. But, as an important factor risk is little considered in trust model. In this paper, Further works are done in trust and risk separately. In course of trust propagation, direct interaction information of the middle recommendation node is presented, which expresses the importance of subjective factor. About risk mechanism, two important factors are considered to improve the corresponding algorithms: length-limit of the risk propagation path and pre-operation process before integrating these paths. With the help of fuzzy logic technology, the trusted decision mechanism is presented which is based on trust and risk. Experimental results and some cases show that the new trusted decision mechanism is reasonable and high-powered.**

***Index Terms*—trust model, risk propagation, trusted decision, fuzzy logic**

I. INTRODUCTION

There are extensive application-formats in open network, such as grid, P2P, Ad hoc network and so on, with the rapid development of computer and network technology. The trend is that nodes in this system are abundant, distributed, dynamic and independent in a large degree. Traditional security schemes have not met the needs of open network. Because the existing secure techniques[1,2], such as authentication, encryption, access control and other mechanisms, are mostly based on identities and credentials and are lack of the subjective evaluation factors. It is necessary for us to integrate trust into open network.

The subject is sponsored by National Natural Science Foundation of P. R. China (No. 60573141 & 60773041), National 863 High Technology Research Program of China (No.2006AA01Z201, 2006AA01Z439, 2007AA01Z478 & 2007AA01Z404), Natural Science Foundation of Jiangsu Province (BK2008451), High Technology Research Program of Jiangsu Province (No.BG2006001), Foundation of National Laboratory for Modern Communications (9140C1101010603), key Laboratory of Information Technology processing of Jiangsu Province .(kjs06006), Jiangsu provincial research scheme of natural science for higher education institutions (07KJB520083).

Trust is a social phenomenon. Any model of trust must be based on how trust works between people in society. It is a complex problem relating to a firm belief in attributes such as reliability, honesty and competence of the trusted entity. Until now there is not a uniform definition.

Here, we pay attention to its study contents: trust modeling, the quantitative measurement mechanism, type definition, the initial trust value establishment, trust storing, trust propagation, trust synthesizing, trust renewal etc. Among these, trust propagation is an important problem. If it is not exact and reasonable, the trust value coming from trust synthesizing will not be useful. Many trust models [3,4] have studied this problem, but most of them can not avoid from the malicious attacks better. In this paper, we will make a further study in trust propagation by integrating global reputation and the subjective trust concept of each recommender in a transitive path into synthesizing trust evaluation.

As we known, trust is used to evaluate the trustworthiness of the node behaviors in open network. But it can guarantee that the process of interaction among nodes is virtuous. This work must be done by risk. Thus, in order to gain the trusted decision in open network, it is nothing to do but integrating trust and risk mechanisms.

Until now, little literature has considered the relationship of trust and risk in trust model or in risk model. This research is young. Even though there's a report on their relationship, it is disposed by the simple addition-summarizing. In this paper, we will consider human's history experience in making trusted decision and apply fuzzy logic technology to solve this problem, which fits the factual cognizing habit of human well. In addition, Reports on risk propagation are lacked. But it is very important and can not be ignored in open network environment. Zhang [5] presents a risk propagation model and some correlative algorithms. This report gives us a new opinion. We will make a further improvement on it in order to enhance the performance of risk evaluation in open network.

The remainder of this paper is organized as follows. Section 2 presents a brief review of related work. Section 3 is the keystone of this paper. About trust propagation

and risk propagation, we have made the corresponding improvements separately. On the basis of these, trusted decision is exhibited by using fuzzy logic technology. Section 4 presents the experimental investigations and case illustration. Section 5 provides future results. And section 6 gives the conclusions.

II. Related Works

A. Trust Model

Ref. [6] presents the Beth model, which gives a differentiation between direct trust and recommendation trust. On the basis of positive experiments and negative ones, it computes the successful probability of the task implementation of each entity and regards it as the trust degree. Moreover, it gives the rules of trust deducing and synthesizing, and the computing methods of the trust degree. But, this model is modeled on the probability statistics theory, which can not describe the intrinsic uncertain properties of trust. In the process of trust synthesizing, a simple average is used, which can not resist the malicious attack.

Ref. [7,8] present the Jøsang model, which is based on the subjective logic. By introducing the notion of evidence space and opinion space, it gives the description of the trust relationship. In virtue of the Beta distribution function of the binary events, it gains the trust degree of each event. In addition, a group of logic operators are offered in order to computing trust value. Though this model considers the uncertain factors of trust, it's also modeled on statistics theory and has made the confusion between subjectivity and randomicity.

As a cognitive process, trust is fuzzy. That is, for a special context, we can not easily make a decision about whether to trust an entity or distrust it. Ref. [9] proposes a trust model by combining with the fuzzy set theory, which has created a new research way in trust. There is an important significance in the proper description of subjectivity. The trust measurement mechanism is expressed by the vectors of the membership functions, which can accord with the factual situations better. For the sake of getting a good grain in trust model, it provides a notion of trust tree. Another contribution of this literature is that it presents the formalization expression of trust and the deducing rules including deduction and consensus.

B. Risk Management

Ref. [10] proposed the approach: a decision tree is first established from vulnerabilities of information systems, then the residual risk of each vulnerability is calculated, finally, the expectation cost of loss is calculated in terms of the residual risk and cost of investment of information systems.

From the perspective of economics, Ref. [11] presented an econometric model of the security risk from remote attacks. The model analyzes the cost of detecting vulnerabilities by means of regression analysis, then predicts the probability of detecting a new vulnerability at a given cost in a given period of time.

Fault tree analysis[12] is a deduction method to decompose the total risk situation of information systems which is considered as the root of the fault tree (top event). The reasons caused top event are analyzed and the relations between those reasons are constructed for the fault tree first, then the probability of occurrence of the top event is calculated.

III. Trust Model Based on Trust And Risk

A. Trust Propagation for Open Network

Trust value of a node in network can be obtained through direct trust and recommendation. In this paper we introduce global reputation evaluation which provides the trust value of a node by synthesizing other nodes' evaluations in the whole open network. Here, we must emphasize the difference between recommendation and global reputation. One is built on the acquaintance mechanism derived from their own history information. The length of the transitive path must be less than a threshold, which dooms that the evolvement of recommendation is not global. But, the other is built on the global information. Thus, it is essential for us to integrate global reputation into the computing of the final trust. Especially, when a new node joins the open network, it has no direct trust or recommendation information. At this time, global reputation is very important for it to decide which node is trustworthy.

Our model assumes that the interaction happens for a special context c at a given time t. Let $T(node_i, node_j, c, t)$ be the final trust of $node_j$ received and integrated by $node_i$. $D(node_i, node_j, c, t)$ be direct trust and $R(node_i, node_j, c, t)$ be recommendation trust. $GR(node_j)$ be global reputation of $node_j$. α, β, γ is the weighting factor of the three aspects separately and $\alpha + \beta + \gamma = 1$. Then,

$$T(node_i, node_j, c, t) = \alpha \times D(node_i, node_j, c, t) + \beta \times R(node_i, node_j, c, t) + \gamma \times GR(node_j) \quad (1)$$

Here, the three aspects need not appear at the same time, that is, each of them can be selected according to system user's requirements and the fact at that time.

$$D(node_i, node_j, c, t) = accuracy_{node_i}(node_j, c, t_{accuracy}) \times \Psi(t - t_{accuracy}, c) \quad (2)$$

$accuracy_{node_i}(node_j, c, t_{accuracy})$ is the direct trust of $node_j$ gained by $node_i$ at the time $t_{accuracy}$. $\Psi(t - t_{accuracy}, c)$ is the time decay function.

$$R(node_i, node_j, c, t) = \left(\sum_{k=1}^{n} honesty_{node_i}(node_k, c, t_{honesty}) \times \Psi(t - t_{honesty}, c) \times Tr(node_k, node_j, c, t)\right) / \left(\sum_{k=1}^{n} honesty_{node_i}(node_k, c, t_{honesty}) \times \Psi(t - t_{honesty}, c)\right) \quad (3)$$

Suppose there are n independent recommendation paths. $node_k$ is the last recommender of the *k-th* path. $honesty_{node_i}(node_k, c, t_{honesty})$ is the $node_k$'s recommender trust factor gained by $node_i$ at the time $t_{honesty}$. $Tr(node_k, node_j, c, t)$ is recommendation trust value of $node_j$ integrated by the *k-th* path, which is transferred to $node_i$ by $node_k$ immediately. As shown in fig.1, there are *h* recommenders in the *k-th* path. And *h* must be less than a threshold.

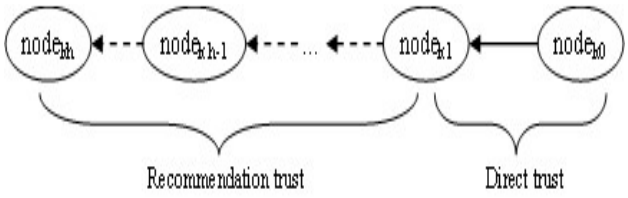

Figure 1. The k-th recommendation path between $node_j$ and $node_k$

Where, $node_{kh}$ is equal to $node_k$ and $node_{k0}$ is equal to $node_j$ .Then,

$$\begin{aligned} &Tr_f(node_{kf}, node_j, c, t) = \\ &\delta_{kf} \times accuracy_{node_{kf}}(node_j, c, t_{accuracy}) \times \Psi(t - t_{accuracy}, c) \\ &+(1-\delta_{kf}) \times Tr_{f-1}(node_{k\ f-1}, node_j, c, t) \times \\ &honesty_{node_{kf}}(node_{k\ f-1}, c, t_{honesty}) \times \Psi(t - t_{honesty}, c) \\ &(2 \le f \le h) \end{aligned} \quad . \quad (4)$$

We will apply the recursive method to give a definition of recommendation trust information in the *k-th* path. $Tr_f(node_{kf}, node_j, c, t)$ is recommendation trust value of $node_j$ provided by $node_{kf}$, which is the f *-th* recommender in the *k-th* path, to the next recommender $node_{k\ f+1}$. Here we emphasize the subjective concept of each recommender about $node_j$ because trust is a cognitive process. When $node_{kf}$ receives the $node_j$'s trust value offered by $node_{k\ f-1}$, he needs to make a colligation between his direct trust value about $node_j$ (namely $accuracy_{node_{kf}}(node_j, c, t_{accuracy})$) and recommendation trust value about $node_j$ offered by his front recommender $node_{k\ f-1}$ (namely $Tr_{f-1}(node_{k\ f-1}, node_j, c, t)$), that is ,there is a weighted sum between the direct trust and recommendation trust. In addition, δ_{kf} is the weighting factor between the two factors. Then he transfers the integrated recommendation trust value to $node_{k\ f+1}$ in order to continue propagation. $honesty_{node_{kf}}(node_{k\ f-1}, c, t_{honesty})$ is the recommender trust factor of $node_{k\ f-1}$ gained by $node_{kf}$ at the time $t_{honesty}$. Where,

$$Tr(node_k, node_j, c, t) = Tr_h(node_{kh}, node_j, c, t) . \quad (5)$$

$$Tr_1(node_{k\ 1}, node_j, c, t) = accuracy_{node_{k\ 1}}(node_j, c, t_{accuracy}) . \quad (6)$$

About $GR(node_j)$, we will apply statistic theory to gain global reputation value of each node by virtue of the successful and failing times. Then,

$$GR(node_j) = \frac{success}{success + failure} . \quad (7)$$

In our model, trust value belongs to the interval [0,1] continuously, with 0 representing distrust and 1 representing trust. The same is recommender trust factor.

B. Risk Propagation for Open Network

Trust and risk play the same important role in the field of trusted decision. One is used to evaluate which nodes are trustworthy in open network, the other will evaluate the security of the interaction process between trustor and trustee. Thus, trusted decision will depend on both trust and risk. At present, some risk models have been provided. But most of them are done by summarizing the risk values which come from the deferent vulnerabilities separately. The propagation of risk is ignored. Ref. [5] gives a model of risk propagation, which presents a novel opinion in this field.. In this model, three algorithms (RH , RH_1 and RH_2) describe the rules of risk propagation. Here, as the atomic algorithm of risk independence propagation, RH_1 applies the recursive method to search risk propagation path coming from a vulnerable resource. Two attribute sets(PS and Q)are used to record the searching path in no time and must be updated at the same time. Otherwise, the result of researching will be wrong. In RH_1 , the cutting-tail operation of Q is done, but PS is neglected. Additionally, the more longer is the risk propagation path, the more smaller is the probability of risk-happening. This path plays a little role in computing the integrated risk value, but it will expend the large costs of open network. Thus, in the searching process it is important for us to avoid finding the long path. Before describing our improved algorithm, we must give the concept: limit value of the path length, noted $Length_{\max}$. That is, when the length of path($Length$)is less than $Length_{\max}$,this path is valid and it can be continued. The improved algorithm RH_1' is given as follows:

Input: Subject $\boldsymbol{C_{mi}}$, character string ***Pstr*** , subject set $\boldsymbol{Q}$.

Output: null.

(1) If($Length > Length_{\max}$) then searching the next subject;

(2) Else for every $e(mi, nj) \in E$

{

(3) if $C_{nj} \in Q$, then doing the operating: “break”;

(4) else putting the string $"Pstr \times e(mi, nj).P"$ into $n.j.PS$ and C_{nj} into Q , $Length++$;

(5) $RH_1'(C_{nj}, "Pstr \times e(mi, nj).P", Q)$;

(6) cutting C_{nj} from Q , cutting $e(mi, nj).P$ from string, $Length--$;

}

In RH_2 , the method of extracting the common right factor is applied to integrate the absolute risk propagation path. If there are the two paths: $1\to 4\to 2\to 3$ and $5\to 2\to 3$ .The result will be $\{1\to 4,5\}\to 2\to 3$. But it will do nothing for this two paths like $1\to 4\to 2\to 3$ and $1\to 4\to 3$. In fact, if an attacker has breached the vulnerability of $node_1$, it will intrude $node_4$ by virtue of the legal authorized trust relationship from $node_1$ to $node_4$. In order to intrude $node_3$ successfully, the attacker would rather assault $node_3$ directly than do it through $node_2$ again in the same safe conditions. That is, the path $1\to 4\to 2\to 3$ is invalid in computing the final risk value of $node_3$ .Thus, we should adding a new pre-operation before algorithm RH_2 to meet the needs of actual conditions. Then, the pre-operation process is expressed:

If there are the risk propagation paths like "$\cdots\to Pleft\to\{null, Pcenter_i\}\to Pright\to\cdots$", that is, There lie no(*null*) or some($Pcenter_i$) middle propagation nodes between the same left atomic character-strings(*Pleft*)and the same right atomic character-strings(*Pright*). We will note the path"$\cdots\to Pleft\to Pcenter_i\to Pright\to\cdots$" as an invalid risk propagation path, which includes the atomic character-string " $Pcenter_i$ ", and only keep the path "$\cdots\to Pleft\to Pright\to\cdots$"as the valid path which will take part in computing the final risk evaluation value of the end node.

C. Trusted Decision Using Fuzzy Logic

Fig.2 shows the trusted decision model based on trust and risk. Here, By balancing the relationship of trust and risk, model will make a logical decision, which may not be the most excellent but a safe selection among the nodes in open network.

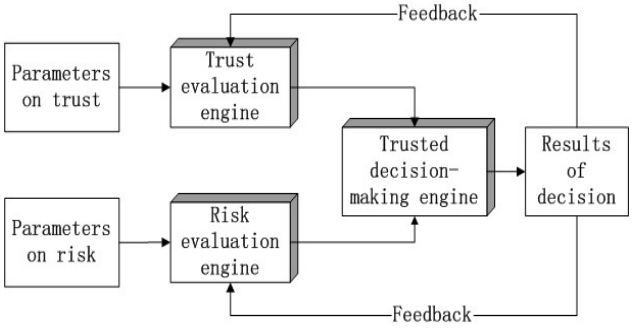

Figure 2. Trusted decision model based on trust and risk

Trust evaluation engine — It is an implementing result with a concrete trust model. By evaluating the parameters on trust, the engine gains the trust values and sends them to trusted decision engine.

Risk evaluation engine — It is used to evaluate the risk value of nodes based on the parameters on risk by using some evaluating methods. Then it also sends them to trusted decision engine.

Trusted decision engine —It is the core subject in this trust model. Some pivotal policies will be applied to assist the model to make the logical decisions. Results of decision will be fed back to trust evaluation engine and risk evaluation engine separately for updating the system information in no time.

Fuzzy logic can express the fuzzy information and human's experience, it has been widely used in decision field. In this paper, we will use this theory to integrate trust and risk into trusted decision value. For trust variable, it is easy to work out the membership function whose universe in $[0,1]$. But, for risk variable its universe is often designed in $[0,+\infty]$. It is hard for us to define its membership function. In order to resolve this problem better, we need to make a normalization-disposal for trust value and risk value.

Make $Trust=(trust_1,trust_2,...,trust_n)$ be trust vector of resource nodes in open network and $Risk=(risk_1,risk_2,...,risk_n)$ be risk value vector. Here, n is the number of the nodes for open network. Then,

$$Trust'=(trust_1',trust_2',...,trust_n')=\left(trust_1\Big/\sum_{i=1}^{n}trust_i,\ trust_2\Big/\sum_{i=1}^{n}trust_i,\ ...,\ trust_n\Big/\sum_{i=1}^{n}trust_i\right). \quad (8)$$

$$Risk'=(risk_1',risk_2',...,risk_n')=\left(risk_1\Big/\sum_{i=1}^{n}risk_i,\ risk_2\Big/\sum_{i=1}^{n}risk_i,\ ...,\ risk_n\Big/\sum_{i=1}^{n}risk_i\right). \quad (9)$$

$Trust'$ and $Risk'$ is the normalization results and will be the input-parameters in trusted decision mechanism.

Take risk for example, when $Risk=(risk_1,risk_2,...,risk_4)=(1.6000,1.4266,3.0682,2.2244)$, then, the normalized result will be $\left(\frac{1.6}{8.3192},\frac{1.4266}{8.3192},\frac{3.0682}{8.3192},\frac{2.2244}{8.3192}\right)=(0.19,0.17,0.37,0.27)$.

In our fuzzy inference system(FIS), trust is designed 4 level (entire distrust, little distrust, little trust, entire trust), risk is done 3 level (low, medium and high) and the trusted decision is the same as trust.

For trust variable, parameter designs of the 4 membership functions are described in the underside.

- MF1='entiredistrust':'gauss2mf',[0.1132 -0.03333 0.1132 0.03333]
- MF2='littledistrust':'gauss2mf',[0.1132 0.3 0.1133 0.3666]
- MF3='littletrust':'gauss2mf',[0.1133 0.6334 0.1132 0.7]
- MF4='entiretrust':'gauss2mf',[0.1132 0.9667 0.1131 1.033]

Fig.3 shows the membership function of trust.

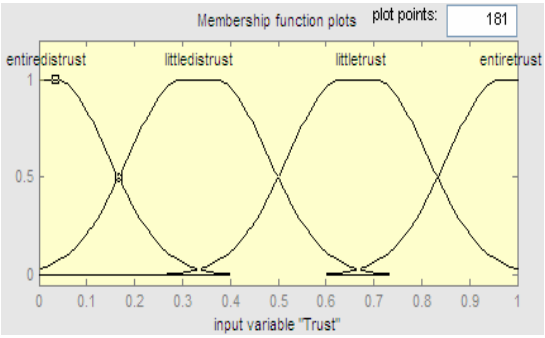

Figure 3. Membership of trust variable

For risk variable, there is the following expression.

- MF1='low':'gauss2mf',[0.1037 -0.08075 0.1037 0.07523]
- MF2='medium':'gauss2mf',[0.1359 0.46 0.1359 0.54]
- MF3='high':'gauss2mf',[0.1359 0.96 0.1359 1.04]

Fig.4 shows the membership function of risk.

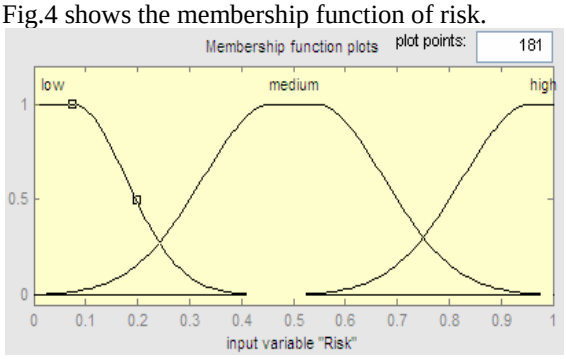

Figure 4. Membership of risk variable

The design of membership function affects the capability of FIS strictly. When the shape of membership function is narrow, it belongs to high resolving power. That is, system is very sensitive. Otherwise, it is blunt. Usually, when the error is big, it is perfect to select the fuzzy set with high resolving power.

The 12 rules are designed as follows:

(1) If (Trust is entire distrust) and (Risk is low) then (Decision is entire distrust) (1)
(2) If (Trust is entire distrust) and (Risk is medium) then (Decision is entire distrust) (1)
(3) If (Trust is entire distrust) and (Risk is high) then (Decision is entire distrust) (1)
(4) If (Trust is little distrust) and (Risk is low) then (Decision is little distrust) (1)
(5) If (Trust is little distrust) and (Risk is medium) then (Decision is entire distrust) (1)
(6) If (Trust is little distrust) and (Risk is high) then (Decision is entire distrust) (1)
(7) If (Trust is little trust) and (Risk is low) then (Decision is little trust) (1)
(8) If (Trust is little trust) and (Risk is medium) then (Decision is little distrust) (1)
(9) If (Trust is little trust) and (Risk is high) then (Decision is entire distrust) (1)
(10) If (Trust is entire trust) and (Risk is low) then (Decision is entire trust) (1)
(11) If (Trust is entire trust) and (Risk is medium) then (Decision is little trust) (1)
(12) If (Trust is entire trust) and (Risk is high) then (Decision is little distrust) (1)

Firstly, we analyze the differentiation between two-valued logic and fuzzy logic.

In two-valued logic, the rule of "if-then" is very simple. If the condition is true, the result is also true. But, in fuzzy logic, if the condition is true to some extent, the result is the same. That is,

Two-valued logic: $p \rightarrow q$

Fuzzy logic: $0.5p \rightarrow 0.5q$

In these rules, there are two conditions. So "and" operation is used to solve this composing problem. That is,

$$T_i(t,r) = E_{1i}(t)E_{2j}(r) = \mu_{E_1 \times E_2}(t,r) = \min\left\{\mu_{E_1}(t), \mu_{E_2}(r)\right\}, (i = 1,2,3,4;\ j = 1,2,3) \quad (10)$$

Here, $E_{1i}(t)$ expresses the membership degree of trust value t, evaluated by requestor, to the corresponding fuzzy subset E_{1i}. In the same way, $E_{2j}(r)$ is the membership degree of risk value r to the fuzzy subset E_{2j}. And $T_i(t,r)$ denotes the membership degree of trusted-decision value to fuzzy subset T_i ,after the two factors work together.

Among these rules, there is the "also" relation. Make the weight of every rule in the system be 1, that is , each rule is equal in trusted decision. "Max" operation is applied to do this work. Make V be the output value of every rule and $\mu_i(V)$ be the membership degree of V to a certain fuzzy subset under the action of rule $i (i \in (1,12))$. With the 12 rules the final membership degree $T(V)$ will be described as follows:

$$T(V) = \max\left\{\mu_1(V), \mu_2(V), ..., \mu_i(V), ..., \mu_{12}(V)\right\}. \quad (11)$$

There may be many valid rules in the face of the same input parameter. Thus the conclusion of many rules may locate in the same fuzzy subset. In this condition, the maximal membership degree value will be selected as the final value.

IV. Simulation Analysis And Case Illustration

A. Simulation on Trust Propagation

Here, we take into account the influence of global reputation on the final trust evaluation and make a comparing between traditional trust model and the new one.

Suppose $node_i$ is the trustor and $node_j$ is the trustee, the initial trust value of $node_j$ is 0.5, there is only a recommender in the transitive path from $node_i$ to $node_j$ and $node_i$ has no direct trust information about $node_j$. 10 times experiments have been done separately in our simulation. In each experiment there lie 50 interaction evaluation results about $node_j$ in

the global scope. The success probability of $node_j$ follows $N(0.7,0.05)$. If the recommender is malicious, let his recommendation value about $node_j$ follows $N(0.6,0.05)$. In addition, $\alpha=0;\beta=0.4;\gamma=0.6$. Experiment results have been shown in Fig.5.

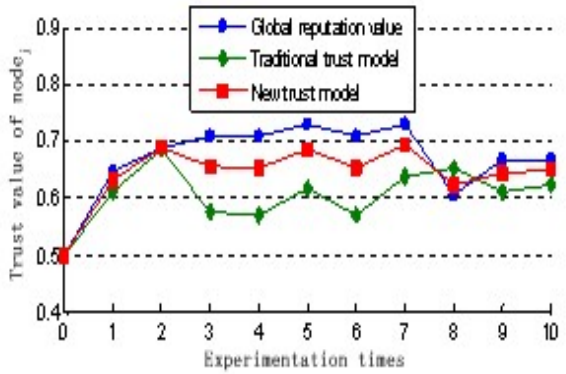

Figure 5. Trust propagation simulation

Without global reputation the recommender is easy to make a malicious recommendation, the new trust model can prevent from the malicious attack better with the help of global reputation and the final trust value tends to 0.7.

B. Case of Risk Propagation

As shown in Fig.6, There are 4 nodes in the risk network, in which $node_2$ has no vulnerability; $node_1$ has two subjects(1 and 2) and two vulnerabilities ($1.1.V_1, 1.2.V_2$); $node_3$ has one subject and two vulnerabilities ($3.1.V_4, 3.1.V_5$); $node_4$ has one vulnerability ($4.1.V_3$); $E_{1\sim6}$ are the six legal authorized trust relationship among the four nodes in network.

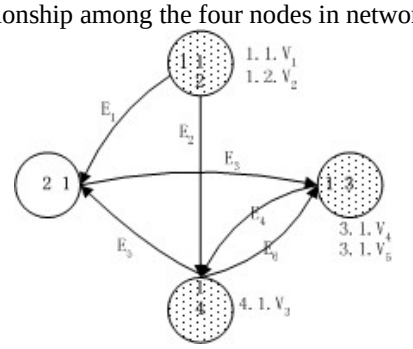

Figure 6. Risk network graph of the case

Fig.7 describes all risk propagation paths coming from vulnerabilities in the network by implementing the algorithm RH_1'. Because the number of the nodes in the network is little and the length of the risk propagation path is short: $Length \le 3$, the factor of $Length_{\max}$ will not be considered in this case. Here, for $node_1$ there are two separate risk propagation path like a tree with two breaches by virtue of its two vulnerabilities: $1.1.V_1, 1.2.V_2$; The mark"×" indicates that the algorithm has inspected the circled path and the corresponding propagation path will be stopped, then it will continue searching the next valid path; Additionally, there is not any risk propagation path form $node_2$,because of no vulnerability.

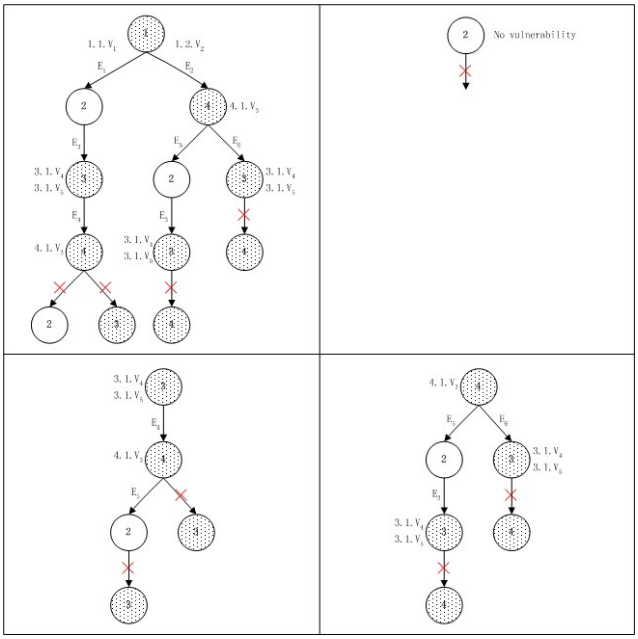

Figure 7. Risk propagation path

Fig.8 shows us the pre-operation process of risk propagation path for $node_3$ before algorithm RH_2. Without this process, the integrated result of these paths will be expressed as the left side of Fig.8. That is, there will be the two paths "$1\to4\to2\to3$"and "$1\to4\to3$" by extracting the common right factor at the same time. It is clear that if an attacker will intrude $node_3$ from the vulnerability $1.2.V_2$, it will select the path "$1\to4\to3$" not "$1\to4\to2\to3$" in the same safe condition. Thus, the path "$1\to4\to2\to3$" will be removed in computing the integrated risk value of $node_3$. After our pre-operation process, the results will be presented as the right side of Fig.8.

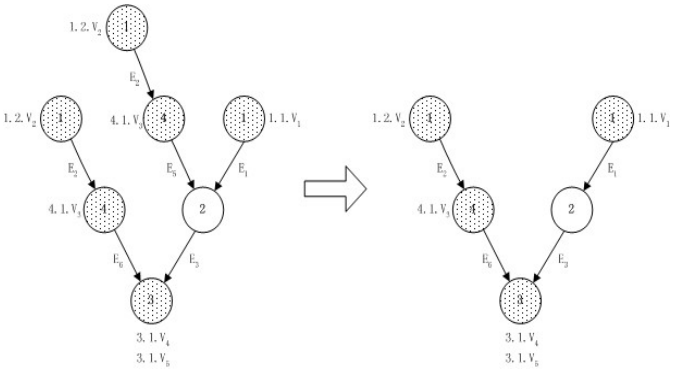

Figure 8. Pre-operation process of node$_3$

Fig.9 shows the synthesizing results of valid risk propagation paths when $node_1 \sim node_3$ as the object of propagation.

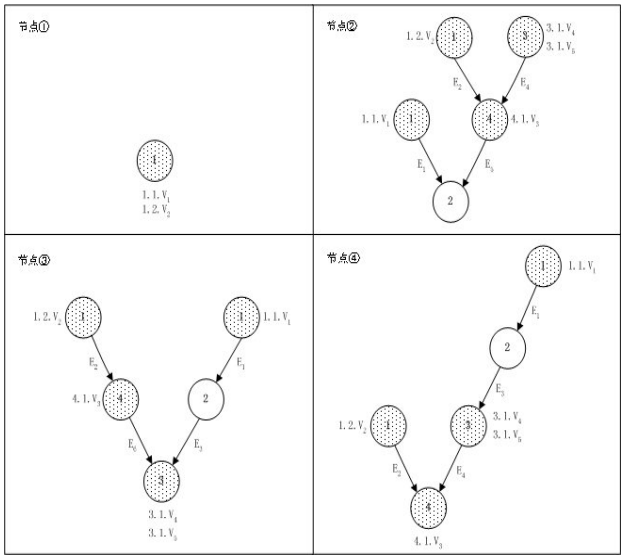

Figure 9. Synthesizing results of valid risk propagation paths

C. Simulation on Trusted Decision Mechanism

As we known, trust is used to evaluate trustworthy ends in open network, and risk will evaluate the security of the interaction process among nodes. They are integrated by some policies in FIS, which is called inference rules. Human's experience is just expressed on these rules. In our opinion, Risk represents the malicious behaviors. Once it is integrated into trusted decision, the trust value must be lower than ago. About the degree of descending, it is rules' duty. If the value of risk is high, the final trust value will be very low clearly.

Fig.10 gives an example of FIS.

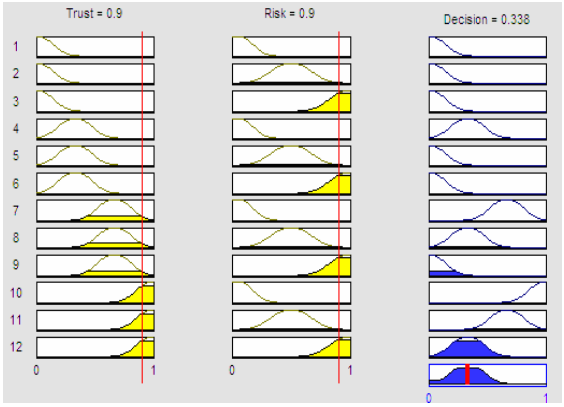

Figure 10. An example: The results of FIS

Here, $Trust = 0.9$, $Risk = 0.9$ and the final trusted decision value is equal to 0.338. That is, Before considering the factor of risk, the trust model can compute the trust value 0.9. But, the new trusted decision model works out the value $Decision = 0.338$ after introducing the risk mechanism. It is easy to see that the back trust value is largely lower than the fore one. In other words, the fore trust level is "entire trust". But, the back trust level may be "little distrust" by using our trusted decision mechanism for the same node in open network. The key problem is that this node is detected with high risk($Risk = 0.9$) in the process of interacting with other nodes. The final trusted decision value will be at a high discount. So the new trust mechanism fits with the factual conditions well for having considered plenty of factors. That is, our new trust model is feasible.

Fig.11 shows another example of FIS under the same implementation environment.

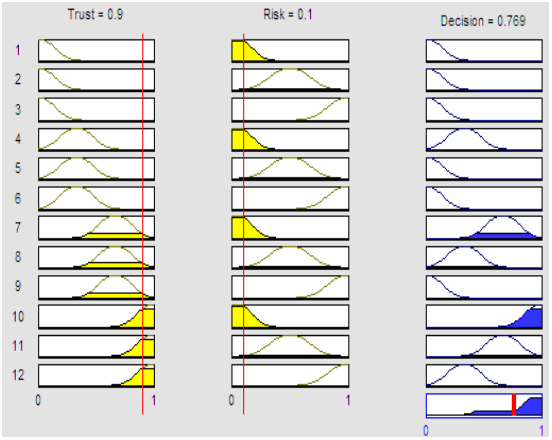

Figure 11. Another example of FIS

In this example, $Trust = 0.9$ and $Risk = 0.1$. That is, trust value is immovable, but risk value reduces to 0.1. In other words, the evaluated node in open network is in a low risk state. The final trusted decision value is equal to 0.769 through the implementation of the new model, which has a little difference with the traditional trust value 0.9. Experimental results show this node is still trustworthy.

Fig.12 show us the input-output view of trust, risk and decision.

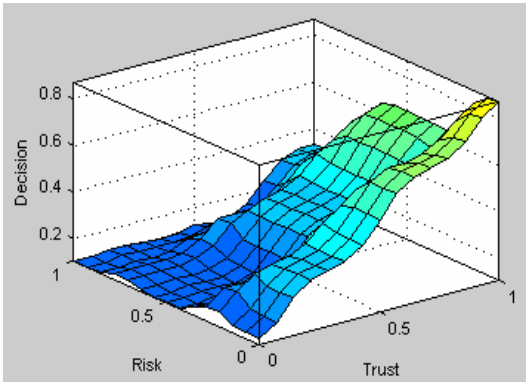

Figure 12. View of FIS about inputs and output

Here, For considering the factor of risk, decision value is lower than trust value in the whole time. And, when trust value is stable, decision value also decreases with the ascending of risk value. These show us the important influence of risk to trusted decision system.

V. FUTURE RESULTS

There are other works to be done for us continuatively. As we known, recent trust models have been built on different mathematics theories, such as probability statistics, D-S evidential theory, the fuzzy set theory and

so on. It is necessary for us to think out the effective methods to solve this aggregation problem among these different models. Additionally, fuzzy rules are very important factors for FIS. We need to learn a lesson in actual implementations and integrate useful experiences into rules' design to make FIS more accurate.

VI. CONCLUSIONS

There are a lot of mature secure mechanisms including authentication, access control, authorization and so on, which have been applied into many fields like grid computing, P2P, wireless sensor network etc. But these can not make an evaluation about entity's behavior. As a cognitive process, trust has been highly paid attention by plenty of researchers at present. Trust and risk are two important factors in trusted decision. In this paper, we make a further study on trust propagation and risk propagation separately. To trust propagation, we further emphasize the subjective factor of the middle recommendation node in the propagation paths. To risk mechanism, new methods are presented to improve the exiting algorithms. Finally, trust model is provided by integrating trust and risk into trusted decision.

ACKNOWLEDGMENT

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

REFERENCES

[1] H.Y. Wang, R.C. Wang, "CPK-based grid authentication: a step forward," The Journal of China Universities of Posts and Telecommunications, vol.14, 2007, pp.26-31.
[2] J.G. Chen, R.C. Wang, H.Y. Wang, "The extended RBAC model based on grid computing," The Journal of China Universities of Posts and Telecommunications, vol.13, 2006, pp. 93-97.
[3] F. Azzedin, M. Maheswaran, "A trust brokering system and its application to resource management in public-resource grids," Parallel and Distributed Processing Symposium, Proceedings. 18th International 2004, 2004, pp.22-32.
[4] Y. Wang, J. Lü, F. Xu, L. Zhang, "A trust measurement and evolution model for internetware," Journal of Software, vol.17, 2006, pp. 682-690.
[5] Y.Z. Zhang, B.X. Fang, Y. Chi, X.C. Yun, "Risk propagation model for assessing network information systems," Journal of Software, vol.18, 2007, pp.137-145.
[6] T. Beth, M. Borcherding, B. Klein, "Valuation of trust in open networks," Proceedings of the European Symposium on Research in Security (ESORICS), Brighton: Springer-Verlag, 1994, PP.3-18.
[7] Jøsang A, Knapskog SJ. A metric for trust systems. In: Global IT Security. Wien: Austrian Computer Society,1998.541-549.
[8] A. Jøsang, "A logic for uncertain probabilities," International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, vol.9, 2001, pp. 279-311.
[9] W. Tang, Z. Chen, "Research of subjective trust management model based on the fuzzy set theory," Journal of Software, vol.14, 2003, pp. 1401-1408.
[10] S. Mehmet, "Security Meter: A Practical Decision-Tree Model to Quantify Risk," IEEE Security & Privacy, May/June 2005, pp.14-24.
[11] S.E. Schechter, "Toward Econometric Models of the Security Risk from Remote Attacks," IEEE Security & Privacy, January/February 2005, pp.40-44.
[12] X. Hong, J.B. Dugan, "Combining Dynamic Fault Trees and Event Trees for Probabilistic Risk Assessment," Proceedings of the 2004 Annual Symposium Reliability and Maintainability, 2004, pp.214–219.

Zhang Lin(1980-), from Jiangsu province of China, doctorial candidate in Nanjing University of Posts and Telecommunications, China, majoring in grid computing, the security of network and trustworthy computing.

She has published some high-quality papers in books, such as Acta Electronica Sinica(Beijing, China: Chinese Institute of Electronics, 2008), China University of Posts and Telecommunications(Beijing, China: Editorial Department of The Journal of China University of Posts and Telecommunications, 2007) and so on.

Wang Ruchuan(1943-), from Anhui province of China, Professor, Supervisor of Doctorial Graduate, Nanjing University of Posts and Telecommunications, China, majoring in the security of network and Mobile agent technology, computer network , grid computing and sensor network.

Wang Haiyan(1974-), from Jiangsu province of China, Associate professor, Supervisor of Graduate, Nanjing University of Posts and Telecommunications, China, majoring in computer software, mobile agent technology, grid computing technology and information security.