http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 12 (18): 4776-4782, 2013
ISSN 1812-5638 / DOI: 10.3923/itj.2013.4776.4782

Research of New Real-time Trust Monitoring Model Base on Multiple Behavior Attributes

[1,2,3]Lin Zhang, [1]Zhengbang Liu, [1]Kaili Rao and [1,2,3]Ruchuan Wang
[1]College of Computer, Nanjing University of Posts and Telecommunications, 210003, Nanjing, China
[2]Jiangsu High Technology Research Key Laboratory for Wireless Sensor Networks,
Jiangsu Province, 210003, Nanjing, China
[3]Key Laboratory of Broadband Wireless Communication and Sensor Network Technology,
Nangjing University of Posts and Telecommunications,Ministry of Education Jiangsu Province,
210003, Nangjing, China

Abstract: In order to ensure the reliability and security of working environments under the open network environment dynamically,a fine-grain real-time and dynamic trust monitoring model is proposed which is based on behavior attribute factor, penalty factor of bad frequency, penalty factor of reputation, penalty factor of hazard-warning frequency, union-recommendation trust, etc. Through monitoring the behavior change in the context of service nodes, the calculating method about the behavior risk value is discussed which is based on the degree of damage about bad behaviors. This can provide convenience for making new judgment.When work is completed, the updating method about trust encouragement or punishment is given. Experiment results show that the new real-time trust monitoring model is accurate and effective.

Key words: Open network environment, dynamic trust, trust monitoring, trust updating

INTRODUCTION

The emergence and development of network technology provides a convenient environment for the efficient use and share of global resources. Today, because the network is heterogeneous, dynamic, open and large-scale, the mutual trust relationship between resource providers and resource users is needed, when they want to interact in order to complete a job (Abbadi *et al*., 2011). Open network environment provides a lot of different services for users to choose and apply (Wang, *et al*., 2009), therefor, the user must not only chose service nodes which meet user's requiments in his operation, but also ensure that the job data itself is secure during the whole process of interaction (Blandford, 2011). Based on our previous studies (Li *et al*., 2012) which have provided the dynamic trust mechanism about the user node behaviors, we will do some further researches on how to keep the safety of user nodes with a dynamic and real-time protection method by monitoring the behavior of service nodes in the open network environment. Nowadays, plenty of trust-based security researches have been provided (Akay *et al*., 2012) which can determine a service node reliable or not through calculating its trust value (Lang, 2010). Due to open and dynamic characteristics of current network applications, dynamic trust management technology has been a hot research topic (Shao *et al*., 2012),which has built many valuable models on trust (Li *et al*., 2009). In order to ensure the security of network environments, it is necessary for us to restrict malicious nodes by monitoring their behaviors in Internet (Ren *et al*., 2012).

Currently, scholars have proposed some dynamic trust models, but there are still some shortcomings:

- Although, trust value updating has be given in some models, the real-time and dynamic update effects have not been achieved (Zhang, *et al*., 2009). These models judge and predict trust value of service node based both on the past history behavior and on the condition, in which the interaction job has just been completed. This may not achieve the role of real-time monitoring and updating
- In some monitoring models, the partition granularity of behavior attribute of network nodes is too rough, not refined (Li *et al*., 2009b)
- About the updating of dynamic trust of the service node based on behaviors, the existing literature studies ignore the time factor and the frequency of occurrence of bad behavior. Without considering the time factor and the frequency factor, the model is imperfect

Corresponding Author: Lin Zhang, College of Computer, Nanjing University of Posts and Telecommunications, 210003, Nanjing, China

- Service node can simultaneously provide services for multiple users. In order to ensure the safety of the user node itself, many nodes should form an alliance. members in alliance can provide different recommendation trust values about the same service node and monitor service node behavior together. Existing literatures have not taken this in consideration

In short, the real-time monitoring should be studied during interact operation between the service node and the user one. If bad behaviors of service node are discovered during the process of monitoring, its trust value will be reduced immediately.

DYNAMIC TRUST MONITORING MODEL WITH MULTIPLE ATTRIBUTES

Problem: In open network environment, dynamic trust management is modeled on the multiple attributes of the trust relationship considering various factors of credibility. In the trust evaluation, by collecting the real-time and dynamic changes of network node behavior, the corresponding adjustment will be realized in a timely manner, such as trust computing, trust management and decision making:

- **Definition 1:** Behavior attribute factor: Different types of bad behavior has different destructive degree, so for different bad behavior, there should be a different punishment degree
- **Definition 2:** Service level importance factor: Different service types have different importance degree for the different degree, the loss and damage caused by the emergence of bad behavior is different, so the corresponding punishment should also be differen
- **Definition 3:** Reward and punishment factor of operation time length: The legal interaction time between service nodes and user nodes is meaningful. When bad behavior occurred, the time from the beginning of interaction is punishment factor K, the whole interaction time without bad behavior is reward factor T
- **Definition 4:** Penalty factor of bad frequency: If bad behaviors of a service node are consecutive, it is great possibile that the node is a malicious node and is trying to destroy the user nodes. In order to ensure the safety of the network environment, it is necessary to increase the penalty degree based on the original weight of bad behavior factor
- **Definition 5:** Penalty factor of reputation: For a service node with a high initial trust value, if this node arises bad behaviors in the process of interaction, it should be increased stricter penalty. Because the more credible service node should be more reliable and stable. The probability of appearing bad behavior is very small in the eye of user nodes, the destroy is also far beyond imagination once it happens
- **Definition 6:** Penalty factor of operating frequency: In a period of recent, more frequent user node select a service node, the service node is more credible for the user node. When the service node appears bad behaviors, it will be maken corresponding punishment combined with penalty factor of bad frequency
- **Definition 7:** Penalty factor of hazard-warning frequency: When service node appears a kind of bad behavior in the interactive process and this kind of bad behavior also occurs in the process of interaction with other user nodes, it is needed to increase the punishment of this service node in order to protect users' security
- **Definition 8:** Union-recommendation trust: In the interactive process of user node and service node, we should not only consider the historical trust experience of the service node, but also consider the change of trust evaluation values from the others. In order to form a real-time evaluation system which is more comprehensive and closer to the real trust value of service node, the consideration about online-union is very necessary.

Architecture of monitoring model: Figure 1 is the architecture of a behavior-based, real-time trust monitoring system which reflects the trust interaction process among network entities, network services, support softwares and network resources. The behavior monitoring module always monitors the entity's behaviors, then the monitoring data will be served as a strong evidence to measure and forecast trust value about object.

The steps of this model are as follows:

Step 1: When user node accesses the network environment, it can query history interaction database firstly and search for the nodes which can provide the service function type that user desired, then predict their trust value and find a service node which meets user's needs to began to interact

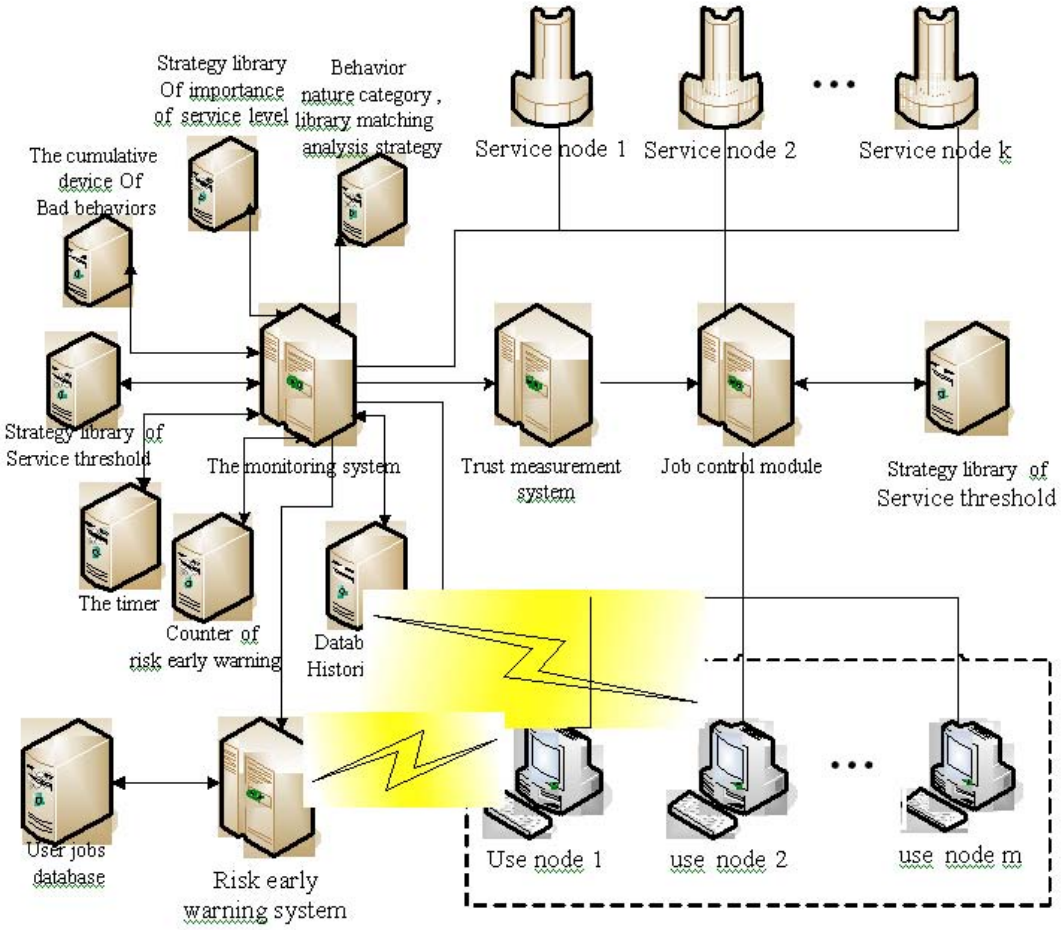

Fig. 1: Architecture of new dynamic trust monitoring model

Step 2: Behavior Monitoring module is always monitoring the interaction behaviors by querying the policy database of service importance level. User node can judge the service node belongs to what level of service and gain the service level importance factor about this service node

Step 3: In the process of interaction, when the bad behavior appears, the monitoring module will send the bad behavior to strategy analysis database in order to gain some behavior factors by been analyzed

Step 4: When the monitoring system detects there is one bad behavior in service node, the information will be sent to the early warning system, this system query the user operation information database, this danger information will be sent to all the user node nodes, which are operating with the current service node, then send out warning

Step 5: When user nodes operate with service nodes, searching the union members, which meet the conditions, as the recommended members of the evaluation service nodes, when a member of the union on the service node's trust value is changed, the current user on the service node trust value of nodes corresponding changes will occur at the same time necessarily, meanwhile, re-select the new nodes as union members

Step 6: Monitoring module submits the service nodes' multiple basic attribute data to the trust measurement module

Step 7: Trust measurement module doing trust updating calculation, as to the service nodes that have bad behaviour, punish the trust value and submit to the job control module timely, then queries the threshold policy repository, control the service nodes' operation ability that is, if the trust value

about the service node has been less than the threshold value,which this type of service should require, disconnect the operation between user nodes and service nodes actively, in order to protect the user nodes

Step 8: When the operation between user nodes and service nodes is accomplished, the service node has updated trust value, the updated trust value is stored in the historical database and can be provided for the next interactive operation

Working principle: Assuming there are m kinds of common behavior types $l_1, l_2,\ldots, l_m$ in the behavior nature classified and the library of matching analysis strategy. The weight values of the penalty are expressed as $\theta_1, \theta_2,..., \theta_m$, each type of behavior $l_i(1 \le i \le m)$ is called a behavioral attribute decision factor. If the degree of the badness of the behavior type $l_1, l_2,\ldots, l_m$ is higher and higher, then the weight values of the penalty will increase successively and:

$$1 \le \theta_i, \sum_{i=1}^{m} \theta_i = N$$

N is a constant.

The weight value of the penalty for service level are recorded as $\alpha_1, \alpha_2,..., \alpha_k$ successively,the weight value of the reward are recorded as $\beta_1, \beta_2,..., \beta_k$. Both of them are Increasing successively and:

$$0 \le \beta_i \le 1, \sum_{i=1}^{k} \beta_i = 1, 1 \le \alpha_i, \sum_{i=1}^{k} \alpha_i = M$$

M is a constant.

Conversely, If there is no any of the above types of malicious behavior, the reward weights are given a constant $h \le 1$.

When user node interacts with the service node for operation, take a recent period of time T_x, get X_m which is the total number of service node to complete the service type work, as well as X_s, the number of the current user has had the service operation:

$$\frac{X_s}{X_m}$$

is operating frequency, X is the operating frequency penalty factor:

$$X = \begin{cases} \sigma + \frac{X_s}{X_m}, & \frac{X_s}{X_m} \ge 0.5 \\ 1, & \frac{X_s}{X_m} < 0.5 \end{cases} \quad (1)$$

Among them, $X_S < X_m$ is a constant called the penalty adjusted figures, in this study σ is recorded as 0.5.

When the ratio between the initial value $\omega(p_s)$ and the service threshold C_i is larger, the user node will more trust this kind of service node, but if it appear bad behavior, the damage to the user node is greater. The ratio between $\omega(p_s)$ and c_i is the service node's credibility penalty factor Y:

$$Y = \frac{\omega(p_s)}{c_i} (\omega(p_s) \ge c_i) \quad (2)$$

When a service node had many bad behaviors to different user nodes in the operation process, this study adopts a linear fashion to increase the penalties for service node trust value, in order to ensure the safety of the user node. This value is called the hazard warning count, denoted by E, warning coefficient is $W = \delta * E + 1$, δ is Constant coefficient of variation.

In the research of the process about user nodes on a service node trust values in the dynamic change, need to regard the user nodes that operate with the same service node as a group and each user node in the organization has his most trusted friend team, through the inquiry about the service node has a user node the most similar evaluation, forming friends team.

When a user node's trust on a service node value is ω, using rating similarity method to obtain the user node union members:

$$1 - \delta \le \frac{\omega_i}{\omega} \le 1 + \delta \quad (3)$$

Among them, ω_i is a value which is currently another user node evaluates the same service node, δ is an adjusted figure greater than zero and less than 1, when the ratio approaches to 1, indicating that the user node and the letter about the service node user nodes as value evaluation closer. Users can choose from node ratio closest to the N user node 1 as their friends team members, thus forming a union.

As a user node establishes his friends team, when one of the members on the service node trust value has changed, the user node trust on the current service node values will also have a corresponding change. The original trust a friend members on the current service node value is ω_i, after the change trust value is ω'_i, a user node has n friends members,at a certain moment, the current user nodeis a time of current user nodes receive recommendation trust value from friends team on the current service node $\Delta\omega_i$ is defined as follows:

$$\Delta\omega_i = \frac{(\frac{\omega_i}{\omega} - 1 - \delta) * (\frac{\omega_i}{\omega} - 1 + \delta)}{\sum_{i=1}^{i=n} (\frac{\omega_i}{\omega} - 1 - \delta) * (\frac{\omega_i}{\omega} - 1 + \delta)} * (\omega_i - \omega'_i) \quad (4)$$

$$\in = \frac{(\frac{\omega_i}{\omega} - 1 - \delta) * (\frac{\omega_i}{\omega} - 1 + \delta)}{\sum_{i=1}^{i=n} (\frac{\omega_i}{\omega} - 1 - \delta) * (\frac{\omega_i}{\omega} - 1 + \delta)} \quad (5)$$

Among them, $\Delta\omega_i$ is a change of the service node trust value, which is the member of the union recommended to the user node, $(\omega_i - \omega'_i)$ is a change of the service node trust value, which is provided by a member of the union, $\in$ is the weight allocated to members of the union.

UPDATE OF TRUST MODEL

Behavioral data is mean basic data, which can be directly obtained under the testing of software and hardware and used for quantitative assessment of the overall evaluation of trust services node. The process of data acquisition needs comprehensive, real-time, real, reliable flow rate and the flow rate will not affect normal network traffic as far as possible.

As to the monitoring module in this article, we can use existing intrusion detection systems, audit tracking system or some special data collection tools, to collect data.

Now, the specific algorithm of trust updating calculation is following.

Definition 9: Behavioral risk value: When services nodes send bad behavior to the user nodes, the degree of damage caused to the users node:

$$R(e) = \begin{cases} \sqrt{\varepsilon' * X * Y * \alpha_j * W * \theta_j * K_j * v} * \partial, & \text{(a)} \\ \partial \times R_{old}(e) + (1-\delta) \times \sqrt{\varepsilon' * X * Y * \alpha_j * W * \theta_j * K_j * v} * \partial, & \text{(b)} \end{cases} \quad (6)$$

(a) **Applicable condition:** User nodes and the service nodes have no historical job interactive experience

(b) **Applicable condition:** User nodes and the service node have historical job interactive experience

Among them α_j is the penalty weight of the d_j level service; θ_j is the penalty weight of the j kind behavior; K_j is the penalty factor of length of time and it is in units of hours, $v = r^2$, r is the penalty factor of frequence,and indicates when service nodes meet consecutive bad behavior, it imposes heavier penalties on the next bad behavior. ∂ is a dimensionless unit value at the given reward and penalty weight. It's called trust reward and penalty units. $\delta \in [0, 1]$ is balance factor of risk.

$R_{old}(e)$ is the risk valve on the services node at the last time, ε' is a correction factor of dangerous value and change itself with $R_{old}(e)$:

$$\varepsilon' = \begin{cases} R_{old}(e), R_{old-1}(e) \neq 0 \\ 1, R_{old-1}(e) = 0 \end{cases} \quad (7)$$

$R_{old-1}(e)$ is the last dangerous value of $R_{old}(e)$. The value changes of ε' reflect the trend of damage of the last bad behavior on the services node.

In the job, if users nodes find bad behavior which is sent by services nodes,it will update the trust value on services nodes in real time. Assumeing $\omega(p_s)_{old}$ is the last trust value of users node on the services node.In a time of job, when the user node detects bad behavior which is from services node, the update the trust value is calculated as:

$$\omega(p_s)_{new\_1} = \gamma \times \omega(p_s)_{old} - (1-\gamma) \times R(e) \quad (8)$$

Among them, R(e) is the dangerous value of the services node behavior when bad behavior occurs, $\gamma \in [0, 1]$ is correction factor of trust, $\gamma = 0.9$.

Similarly, in the job, if received the variation recommendation of the trust value on the services node which is from friends in the league. $\omega(p_s)_{new\_2}$ is the updated values to the trust value of services node, after users node receiving the updating changes of trust of the services node from the union member. And, updating the trust value of users node to services node is calculated as:

$$\omega(p_s)_{new\_2} = \begin{cases} \omega(p_s)_{old} + (1-\varphi)[\omega(p_s)_{new\_1} - \omega(p_s)_{old}] \\ +\varphi \times \Delta\omega, & \text{(a)} \\ \omega(p_s)_{new\_1}, & \text{(b)} \end{cases} \quad (9)$$

(a) **Applicable condition:** The trust value of union member on services node changed

(b) **Applicable condition:** The trust value of union member on services node did not change

Among them φ is vitiating.

This model can continuously monitor job interaction between the services node and user node and update the trust value of services node in real time. This measure can suppress the damage of users node which is caused by services node at the maximum.

ANALYSIS OF SIMULATION

Comparing with the monitoring models which did not distinguish the service level and behavior attributes, the new model is more accuracy and rational in monitoring technology about service node. Some experiments are maken as follows.

Context of this experiment: The network computing environment can provide five service levels, marked as d_1, d_2, d_3, d_4, d_5 which are increasing in turn. The punishment weight in the order is $\alpha_1 = 1$, $\alpha_2 = 1.5$, $\alpha_3 = 2$, $\alpha_4 = 2.5$, $\alpha_5 = 3$. In addition, there are 5 kinds of bad behavior l_1, l_2, l_3, l_4, l_5 in the strategy library of system which are also increasing in turn. The penalty weight of these bad behaviors is $\theta_1 = 1$, $\theta_2 = 1.5$, $\theta_3 = 2$, $\theta_4 = 2.5$, $\theta_5 = 3$. To ensure that the behavior of network node is legitimate, it is necessary to punish bad behaviors and to make a supplement with the reward.

Suppose an initial trust value of a service node is V. The following discussion is how the trust value of service node changes once its behaviors make some varieties.

Analysis of the trust monitoring with multi-dimension attributes: Assume there are user nodes p_{u1}, p_{u2} and p_{u3} are interacting with service node p_3 which provides d_3 level service. The initial trust value of p_3 is 0.8, and its use frequency is 0.6. p_{u1} Uses the new model, p_{u2} and p_{u3} just consider some factors, respectively. Table 1 shows the experiment simulation situation.

This experiment reflects that the real trust value about service node can be easily gained by the multi-dimension, fine-grained factors.

From Fig. 2, It can be seen that p_{u1} does better in protecting his own safety and be more sensitive to bad behaviors of service node, thus it may contain the bad service node better. In this experiment context it will stop the interaction with service node at time 1.8, because the trust value of service node has decreased under 0.7.

Analysis of the affection under different factors: Simulate in the process of operation, service node to the user nodes with different levels of vandalism. e_1, e_2, e_3, e_4, are different user nodes which have considered with different factors. The service node carries dissimilar bad behaviors into the four uses. Table 2 shows another experiment simulation situation.

From Fig. 3, the curved line of e_1 reflects that by introducing penalty factor of bad frequency, bad behaviors happens more posterior in the process of interaction, the the more behind of the bad behavior, the attenuation of trust value about service node is greater. e_2 reflects the affection of reward and punishment factor of operation time lengt. e_3 reflects that bad behavior is more vicious, the degree of punishment is larger. By comparing between $e_1$and e_4, it can been seen that the continuous low damages of bad behaviors are worse than a kind of great damage.

Table 1: A situation of experiment simulation

Time (T) and factor	p_{u1}	p_{u2}	p_{u3}
0.5 and l_i	l_1	l_1	l_1
0.7 andW	1	\	\
1.0 and l_i	l_2	l_2	l_2
1.3 and $\Delta\omega_i$	-0.18	\	\
1.5 and l_i	\	l_5	l_5

Table 2: Another experiment simulation situation

Time (T)	e_1	e_2	e_3	e_4
0.5	l_3	l_2	l_1	l_4
1.0	l_3	l_3	l_2	l_4
1.5	l_2	l_2	l_3	l_5
2.0	l_4	l_4	l_3	\
2.5	l_3	l_3	l_4	\
3.0	l_2	l_2	l_5	\

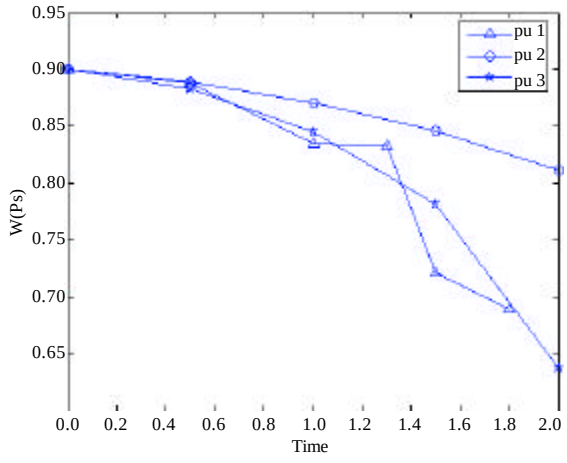

Fig. 2: Analysis of trust monitoring based on multi-dimension factors

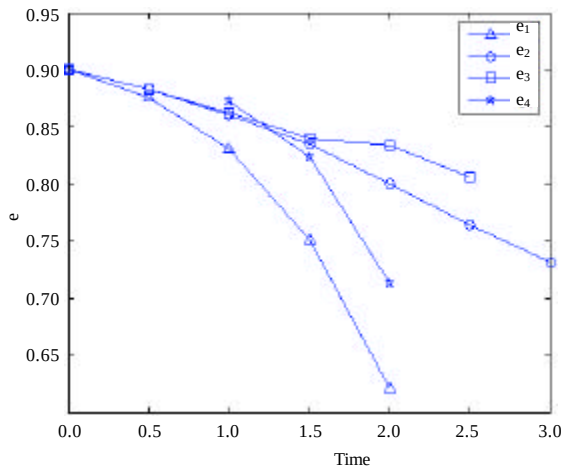

Fig. 3: Affection analysis of different factors

CONCLUSION

In this study, the real-time dynamic update of trust value about service node is proposed by continuously monitoring interaction behaviors between service node and user node in a real-time way. Many factors are introduced in the new model, such as service level importance factor, penalty factor of bad frequency, penalty factor of hazard-warning frequency, union-recommendation trust and so on. These factors are very necessary to be considered because they will produce an effect on the change of trust value about service node. User nodes can dynamically update trust value about service node based on multiple factors so as to ensure the security of the network environment. experimental results show that the new model is in line with the cognitive habits of human society.

ACKNOWLEDGMENTS

The study is subsidized by the National Natural Science Foundation of P. R. China (61170065, 61171053, 61203217, 61103195, 61201163, 61202354); the Natural Science Foundation of Jiangsu Province (BK2011755, BK2011072, BK2012436); Scientific and Technological Support Project (Industry) of Jiangsu Province (BE2011189, BE2012183, BE2012755); Natural Science Fund for Colleges and Universities in Jiangsu Province (13KJB520017); A Project Funded by the Priority Academic Program Development of Jiangsu Higher Education Institutions (PAPD) (yx002001).

REFERENCES

Abbadi, I.M. and A. Martin, 2011. Trust in the cloud [Elektronische versie]. Inform. Security Tech. Rep., 16: 108-114.

Akay, B. and D. Karaboga, 2012. A modified Artificial Bee Colony algorithm for real-parameter optimization. Inform. Sci., 192: 120-142.

Blandford, R., 2011. Information security in the cloud. Network Security, 2011: 15-17.

Lang, B., 2010. Access control oriented quantified trust degree representation model for distributed systems. J. Commun., 31: 45-54.

Li, M.C., B.Yang, W. Zhong, L.L. Tian, H. Jiang and H.G. Hu, 2009. Grid dynamic authorization model based on feedback mechanism. Chinese J. Comput., 32: 2187-2199.

Li, X.Y., X.L. Gui, Q. Mao and D.Q. Leng, 2009b. Adaptive dynamic trust measurement and prediction model based on behavior monitoring. Chinese J. Comput., 32: 664-674.

Li, Z.Y. and R.C. Wang, 2012. A Dynamic Secure Trust Model for Mobile P2P Networks. Acta Electron. Sinica, 1: 1-7.

Ren, W., M. Lei and Y.M. Yang, 2012. Dynami-cal and robust trust model for software service in cloud computing. J. Chinese Comput. Sys., 4: 679-683.

Shao, K., F. Luo, N.X. Mei and Z.T. Liu, 2012. Normal distribution based dynamical recommendation trust model. J. Software, 12: 3130-3148.

Wang, Y., G.P. Dai, Z.T. Jiang, Y.R, Hou, J. Fang and X.T. Ren, 2009. A trust enhanced service compo sition scheduling algorithm. J. Acta Electron. Sinica, 10: 2234-2238.

Zhang, R.L., X.N. Wu, S.Y. Zhou and X.S. Dong, 2009. A trust model based on behaviors risk evaluation. Chinese J. Comput., 4: 688-698.