Send Orders for Reprints to reprints@benthamscience.ae

The Open Cybernetics & Systemics Journal, 2015, *9,* 1045-1050

Open Access

Research on Trust Evaluation Access Control Model Based on Dynamic Bayesian Network in Trusted Domain

Guo Lei* and Shimin Meng

Mathematics and Computer Science School of Wuyi University, Wuyishan, Fujian 354300

Abstract: Aiming at solving the difficulties of interaction synergism and insecurity of the multi-agent system, a trusted evaluation access control model based on dynamic Bayesian network is proposed in this paper. The model establishes trust domains according to the interaction records of agent itself and the history. The influences of time and interactive behavior on trust evaluation are also considered. Historical interactive records, trust decay control factor and punish factor etc. are introduced. And the sensitivity and accuracy of dynamic interactions are thus improved as well as the safety of the access process is enhanced.

Keywords: Access control, dynamic Bayesian network, intelligent agent, trust evaluation.

1. INTRODUCTION

With the rapid development of wireless networks and pervasive computing technology, intelligent services in the unit of digital community, such as intelligent transportation, intelligent firefighting, smart homes, etc. are also booming. At the same time, due to the uncertainty, heterogeneity, dynamic nature and other characteristics of the complex networks, how to assess the credibility of objects and conduct effective access control has become a new hot spot of next generation network research.

Multi-agent system (MAS) based on the agent is currently a good choice. As the agent has characteristics of autonomy, mobility, initiative, etc., each agent can achieve rich and seamless collaboration in the MAS, providing a good solution for large-scale complex problems. Currently there are a variety of MAS, such as community computing [1] and pervasive information community organization [2] etc. In MAS, in order to complete a task, multiple interactions and dynamic collaboration are required between agents. Agents are typically strange to each other. How to prevent illegal access of unauthorized agents and ensure effective use of resources by legitimate agents is the key issue to guarantee MAS security.

Currently combining the sociological theory of interpersonal trust with the access control to improve the access control capability of unfamiliar subjects in large-scale complex systems is the current hot topic of study. A lot of scholars have analyzed and made modeling for the assessment method of trust evaluation, mainly including fuzzy-based theory [3], information entropy-based theory [4], theory based on statistical evidence and probability [5] and other theories. In 1994, MARSH [6] proposed the mathematical model of trust evaluation for the first time. In 1997, ABDULRAHMAN [7] proposed the concept of using recommendation mechanism to resolve trust control in the context. In recent years, a large number of scholars have used different mathematical models for the trust evaluation study. In literature [8], a simplified model based on Kalman approach is proposed. This model is based on Bayesian network and the attenuation mechanism is also introduced into it. However, the model has the shortages of time continuity and fails to adapt to the complicated network environment. In literature [9], a trust management model is proposed, which has the incentive effect in the distributed P2P environment. However, the model ignores factors of time and dynamic environment. In literature [10], the modeling is made based on evidence theory and the applied trustis probability-weighted average. The shortage of the model is containing a greater amount of subjective assumptions and the lack of flexibility. Kamvar *et al.* proposed the global trust management model Eigen Trust [11]. This model is based on trust transitivity and calculates the global credibility for each user. It also conductsiterative calculation based on mutual feedback of adjacent nodes, truly reflecting node situation. However, this model has high communication cost and the capacity to defect against malicious attacks is poor. In [12], Power Trust model is proposed on the basis of Eigen Trust. This model presents an algorithm of dynamically selecting significantly trusted nodes, improving the aggregate data and accuracy of the global trust. But the model uses the aggregate feedback and the power law for collection, increasing the calculation cost. Li Xiaoyong *et al.* proposed the trust evaluation model [13] based on multiple decision property under trusted network environment, which introduces multiple decision properties to assess the relationship of trust and is an effective solution to the problem of insufficient adaptability to dynamic environment in traditional models.

These research results have effectively promoted the development of trust evaluation model. However, in the MAS with much interaction, there are still deficiencies in dynamic adaptability and timeliness of trust evaluation, mainly reflected as below:

1874-110X/15

1) Only consider the dynamic nature of entity interaction, but not adequately consider the dynamic adaptability with the change of context and the timeliness of interaction.

2) There are many subjective assumptions in the process of modeling, affecting the accuracy and scientificity of models.

3) Lack the consideration of malicious deception and attacks presented on the network and insufficient safety of the model.

To solve the above problems, a trusted domain dynamic Bayesian network trust evaluation access control model (TDBTBAC) is proposed in this paper.

2. TDBTBAC MODEL

2.1. Definition of TDBTBAC Model

In this model, applications are described as a MAS and services are provided to users interact through interaction of agent inside the MAS. In this process, the system needs to pre-build agents suitable to applications, and thus build trust domains with agents. After the application is ended, the corresponding trust domain will also be ended and the agent is released. In order to conduct effective access control of each agent, it is required to control the trust of agent. First of all, it is necessary to increase the level of trust, so that trust of each agent can be dynamically adjusted in the interactive process; secondly, the level of trust is the key factor to determine whether the access shall be activated; and finally, trust of agent shall be global, which means it is not only effective in a service, but also able to support the role of interaction across services. The formalized description of TDBTBAC model is as below:

Definition 1: TDBTBAC model: main elements of the model are as follows:

1) A: the set of all agents in the MAS, a A, the basic unit of the MAS. It can be added to one or more trust domains according to the demand.

2) R: the set of all roles in the MAS.

3) Session: indicating interaction between related agents. Agents are able to reach trust domain *via* session and initiate interactions.

4) Tlevel: the trust evaluation grade of agent made by MAS. Access assigned by the credibility, the credibility of the amount depending on the context, history, behavior dynamically adjusted.

5) Object: the passive entity which is accessed by subject in the constraint of access control decision, referred to as OB. The object can be resource, role, and task in the MAS.

6) Operation: represent the smallest action that can be performed, abbreviated as OP.

7) P: the set of all access that authorize roles in the MAS, $P=2^{OB}$

8) AR⊆A × R: represent the mapping relationship between the agent and the role. The mapping shall meet the threshold requirement of the trust evaluation.

PR⊆P×Rrepresents the mapping relationship between the access and the role.

9) $AgentSess\ (a:A) \rightarrow 2^{SESSION}$ represents the mapping of agent in some reply.

10) $SessR(s:SESS) \rightarrow 2^{R}$represents the mapping between the reply and the role.

STL⊆Session×Tlevel: The mapping between the session and the trust evaluation level. This mapping is a several-for-one mapping.

PTL⊆P×Tlevel: Reflect the relationship between the access and the trust evaluation level. Only agents that have reached the corresponding level can activate the access of corresponding roles.

In order to control the access control process more flexibly and effectively, this model also defines some relevant constraints.

Definition 2: Static separation of duties (SsoD): SsoD⊆2^R × N, mainly consisting of two sorts: the first one is constraint of mutually exclusive roles assignment, which means mutually exclusive roles cannot be assigned to the same user; the second one is the constraint of role number, indicating that it is forbidden to activate roles of agent more than n simultaneously.

Definition 3: Dynamic separation of duties (DsoD): DsoD⊆2^R × N, containing two aspects: if the role $r^1 \in R$ is activated by a in a session, then the corresponding mutually exclusive roles $r^2 \in R$ cannot be activated; in addition, in a session, the agent cannot activate roles more than n.

2.2. Authorization Framework of TDBTBAC Model

The authorization framework of access control in the TDBTBAC model is shown in Fig. (**1**):

First of all, the agent needs to evaluate the trust of the subject, and build trust domains as appropriate. It may issue trust certificates depending on the context, the history of each subject, etc., realizing the automatic registry of trust threshold in the trust domain and establishing roles through AR. The process meets requirements of the static separation of duties and the dynamic separation of duties.

2.3. Calculation of Trust Evaluation Based on Dynamic Bayesian Network

2.3.1. Dynamic Bayesian Network Model

At present, there are three trust evaluation modeling methods: the method based on the theory of probability and statistics, the method based on multi-attribute decision theory and the method based on the fuzzy set theory. These three methods have advantages and disadvantages respectively. The method based on probability and statistics applies statistical methods to analyze the real history records and uses probability to describe trust level. This method is more mature compared to the other two methods and has a better

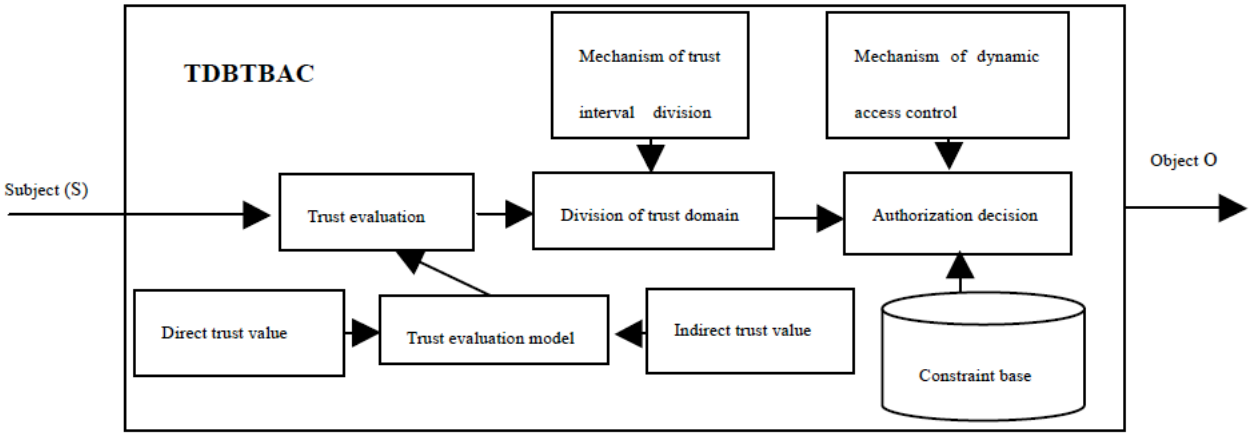

Fig. (1). Procedure chart of TDBTBAC authorization.

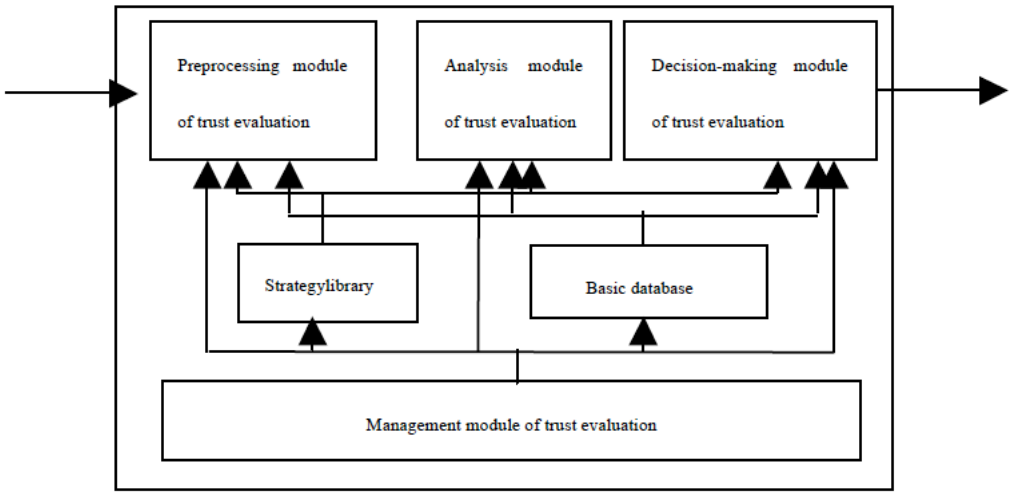

Fig. (2). Calculation model of trust evaluation.

mathematical basis, but it cannot eliminate the impact of malicious recommendation on trust evaluation. The method based on multi-attribute decision theory takes the context information and attributes the decision-making process concerns into overall account to determine the trust level. However, it fails to reflect the blur characteristic and uncertainty of confidence. The method based on fuzzy set theory describes and expands confidence through the fuzzy set theory, but it cannot describe the randomness of trust evaluation. This model uses the method based on dynamic Bayesian network, which is capable of expressing the evolving process of a random variable with time passing. It also takes into account of the interdependence and mutual impression between randomness and random variables of network behaviors, capable of enhancing accuracy of confidence while reflecting characteristics of randomness and fuzziness.

The theoretical basis of dynamic Bayesian network is Bayes theorem and Bayes formula, which combining the timing information with the traditional Bayesian network to reflect the impact of time onevent probability. Dynamic Bayesian network updates the network configuration, conditional probability and experience distribution according to the collected sample information and applies network topology to reflect the change of dependencies between variables over time. It can also reflecta variety of incidence relations between variables by change of topological structures or change of variables. It has good scalability and flexibility. In addition, the inference process of dynamic Bayesian network has strong continuity. Using probabilistic methods to measure confidence provides it with the time decay characteristic and makes it more in line with the reasoning process of the objective world.

2.3.2. Calculation Model of Trust Evaluation

The calculation model of trust evaluation mainly consists of the strategy library, the basic database, preprocessing module of trust evaluation, analysis module of trust evaluation, decision-making module of trust evaluation and management module of trust evaluation. The structure is shown in Fig. (**2**):

① Preprocessing module of trust evaluation: used for interactive data collection, information processing, data association, feature disjunction, grading and standardization, etc.

② Analysis module of trust evaluation: core module of the model, mainly used for direct confidence calculation, indirect confidence calculation and comprehensive confidence calculation, and the sole basis used by the model to judge the agent.

③ Decision-making module of trust evaluation: mainly used for the maintenance and diffusion of trust list and isolation of entities lower than the metric threshold.

④ Strategy library: used to store and update the prior knowledge and strategies of trust evaluation.

⑤ Basic database: the basis of trust evaluation calculation and it can be used to store the preprocessed valid data.

Trust is the relationship established between the agent and the system OB and the dynamic variable interacted by the agent. Trust evaluation concerned in this paper includes the direct confidence, indirect confidence and comprehensive confidence. The comprehensive confidence will eventually be implemented in the access control decision.

1) Direct confidence calculation

Definition 3: Assume HIR (History Interactive recording) is the history interactive recording, *t* is the current time, and C (HIR, t) is the context of occurring history recording at *t.*

Definition 4: Assume any entity x_i and y_i, call*DTn* (x_i, y_i, *t, C (hir, t))* as the direct confidence of x_i in$y_i$at *t* in the context interaction condition of*C (hir, t)*, so

$$DT_n(x_i y_i,t,C(hir,t))=$$

$$\begin{cases} \left(\frac{1}{n},\frac{1}{n},\dots\frac{1}{n}\right), t=0 \\ DT_n\left(x_i,\ y_i, t-1, C(hir,t-1)\right)\cdot\alpha(t), \Delta C=\emptyset \\ DT\left(x_i,y_i,t,C(hir,t)\right)\cdot\beta,\ others \end{cases}$$

where ΔC=*C(hir,t)-C(hir,t-1),*$\alpha(t)$ is time factor and its calculation formula is

$$\alpha(t)=1-\frac{\Delta t\times\omega}{t-t_0}$$

$\omega\in(0,1)$ is confidence attenuation adjustment factor; the greater the $\omega$is, the faster confidence decays, whereas the slower it decays. *t* is the current time and Δt is the time difference between the two calculations.

$\beta\in(0,1)$ is punishment factor and its formula is

$$\beta=\begin{cases} 1,\ \Delta DT\geq 0 \\ 0<\beta<1,\ \Delta DT<0 \end{cases}$$

where ΔDT*= DT (t) -DT (t-1).* This factor is mainly used for confidence punishment when entities provide malicious recommendation, spoof, etc, making the confidence of corresponding entity decline rapidly; the greater $\beta$is, the faster the confidence declines, whereas it declines slower.

It can be seen from the above definition that the initial value of the direct confidence of entity is equally divided with equal probability and is compared at time *t* and time *t-1*. If interaction history recording exists in the context, the confidence is evaluated on the basis of the recording; if no interaction exists in the context, the confidence is decayed on the basis of time.

2) Indirect confidence calculation

Definition 4: Assume any entity x_i and y_i and call ST_n *(*(x_i, y_i,*t, C (hir, t))* as the indirect confidence of x_i in y_i at *t* in the context interaction condition of *C (hir, t)*, so

$$ST_n(x_i,y_i,t,C(hir,t))=$$

$$\begin{cases} \left(\frac{1}{n},\frac{1}{n},\dots\frac{1}{n}\right), t=0 \\ ST_n\left(x_i,\ y_i, t-1, C(\hbar ir,t-1)\right)\cdot\alpha(t), \Delta C=\emptyset \\ \beta\cdot\frac{\sum_{O\in X} DT_n\left(x_i,\ y_k,t-1,C(\hbar ir,t-1)\right)\times MT_n\left(x_k,\ y_j,t-1,C(\hbar ir,t-1)\right)}{\sum_{O\in X} DT_n\left(x_i,\ y_i,t-1,C(\hbar ir,t-1)\right)},\ others \end{cases}$$

In the formula, O represents the set of entities that have interaction with the target entity. The model is initialized and the probability of indirect confidence between entities is equally shared. If no confidence recommendation exists when compared at time *t* and time *t-1*,the indirect confidence decays with time passing by; if recommendation exists, the indirect confidence is updated according to interaction records in the context, the comprehensive confidence of the recommended entity, etc.

3) Comprehensive confidence calculation

Definition 5: Assume any entity x_i and y_i and call MT_n((x_i, y_i, *t,C (hir, t)*) as the comprehensive confidence of x_i in y_i at *t* in the context interaction condition of *C (hir, t)*, so

$$MT_n\ ((x_i y_i,t,C(hir,t))=$$

$$\begin{cases} ST_n\left(x_i,\ y_i,t,C(\hbar ir,t)\right),\ C(hir,t)=\emptyset \\ DT_n\left(x_i,\ y_k,t,C(\hbar ir,t)\right),\ C(hir,t)=C(HIR,t) \\ MT_n\left(x_i,\ y_k,t-1,C(\hbar ir,t-1)\right),\ \Delta C=\emptyset \\ \beta\left[\theta\cdot DT_n\left(x_i,\ y_k,t,C(\hbar ir,t)\right)+(1-\beta)\cdot ST_n\left(x_i,\ y_i,t,C(\hbar ir,t)\right)\right],\ C(hir,t), \text{ others} \end{cases}$$

Where θ is weight regulatory factor, reflecting the weight relationship between the direct and indirect confidence, and the formula is:

$$\theta=\frac{HIR+hir}{2HIR}$$

HIR represents the effective interaction history records and *hir* is the historical interaction records between x_i and y_i. In order to ensure the judgment of confidence is focused on direct confidence, value interval of θ is generally set as (0.5, 1).

As a major judging factor of equity authority management in the process of access control, comprehensive confidence is updated using the method of continuous iterative in the process of confidence calculation and has high sensitivity and accuracy to the dynamic interaction process between agents. When the effective interaction history records increase, by the way of dynamic Bayesian network inference, the comprehensive confidence of the evaluated object will continues to increase, which is consistent with human's social behavior.

3. ANALYSIS OF SIMULATION

3.1. Setting of Experimental Environment

To test the performance of the model, simulation of TDBTBAC model is conducted in this paper. The experimental environment includes: Windows7, 4GB of memory and Matlab7.1. The simulation parameters are set so that there are 1200 entries of history interaction records, of which 150 entries are related to the target entity. The interaction records are divided into high, medium and low levels. The number of entities that are next to the target entity is 10 and the number of iterative simulation process is 10 times.

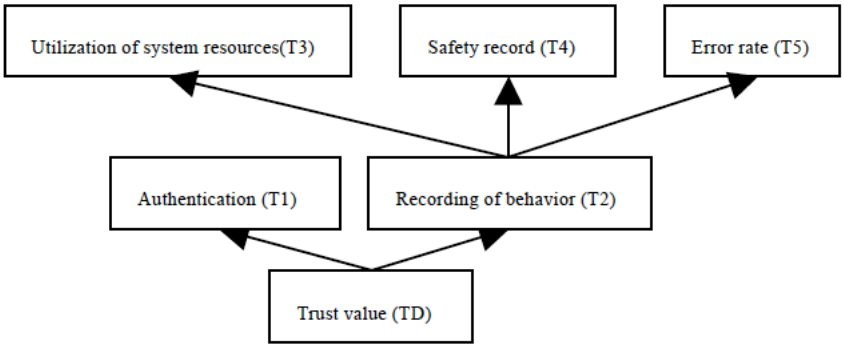

Fig. (3). Dependencies between variables.

Table 1. Probability distribution of dependent conditions for each variable at initial status.

P(A/B)	P(A=H/B=H)	P(A=H/B=M)	P(A=H/B=L)	P(A=M/B=H)	P(A=M/B=M)	P(A=M/B=L)	P(A=L/B=H)	P(A=L/B=M)	P(A=L/B=L)
P(T1/TD)	0.8	0.35	0.1	0.1	0.45	0.3	0	0.1	0.7
P(T2/TD)	0.8	0.4	0.1	0.15	0.45	0.3	0.05	0.1	0.65
P(T3/T2)	0.8	0.5	0.15	0.1	0.35	0.25	0	0.05	0.5
P(T4/T2)	0.85	0.5	0.1	0.1	0.4	0.25	0.05	0.05	0.5
P(T5/T2)	0.8	0.5	0.15	0.1	0.35	0.3	0.05	0.1	0.5

The simulation has set six variables, including trust value (TD), authentication (T1), recording of behavior (T2), and utilization of system resources (T3), safety record (T4) and error rate (T5). The dependencies between variables are as shown in Fig. (**3**):

In the model initialization phase, the conditional probability value of dependency between variables can be set based on expert knowledge and interaction history. Although there is some subjectivity, with the supplementing and update of interaction records while the system is running, the conditional probability value will continue to be adjusted and thus become closer to the real situation. When the dependency between variables is set with initial status, the distribution of conditional probability is as shown in Table **1**, where P (A / B) is the probability of dependent conditions of event A to event B. Its value is as follows:

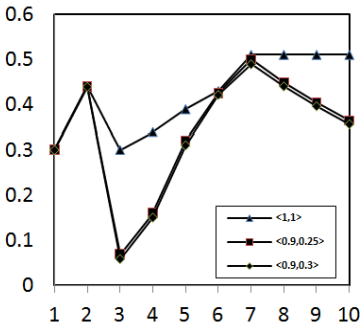

Fig. (4). Simulation results.

3.2. Experimental Analysis

For comparison, the values of (ω, β) are set to (0.9,0.25), (1,1) and (0.9,0.3) respectively in the simulation process, in which the line connected by triangle represents the value of (1,1), the one connected by squares represents the value of (0.9,0.25), and the one connected by diamond represents the value of (0.9,0.3). The levels of the target interaction records are H, H, L, M, H, H, H,∅,∅ and ∅. The simulation results of 10-step size are shown in Fig. (**4**):

It can be seen from the simulation results that at T = 1,2, the value of target trust evaluation continues to increase because the record level is H; at T=3, the record level of L occurs, which indicates except the triangle, the confidence of all other curves declines; at T = 4,5,6,7, the confidence gradually improves; at T = 8,9,10, since no new record appears, the confidence of the triangular curve keeps unchanged, while the confidence of other curves decreases gradually over time. It can be seen from the above simulation result that due to the introduction of trust attenuation regulatory factor and the punishment factor, the model is able to handle anomalies fast and responsively, thus effectively preventing the threat of malicious entities. At the same time, the decline of confidence over time is also in line with cognitive habits of human beings. What's more, it can also be seen from the figure that with the increase of interaction records, the trust evaluation of the target entity has become increasingly clear, which is also consistent with cognitive behaviors of human beings.

CONCLUSION

An important prerequisite to improve the MAS service is to enhance interaction security of each agent in MAS and provide an efficient, accurate and dynamic access control model for MAS. For this end, the TDBTBA model is proposed in this paper. First of all, the current access control modes are improved. Trust evaluation is selected as an im-

portant judging factor for authority management and carrying out access control management, effectively solving the difficulties of interactions between numbers of objects, especially interaction between unfamiliar objects. Secondly, a mechanism for dynamically adjusting the level of trust is proposed. In each session, changes in direct and indirect confidences are taken into consideration to draw the comprehensive confidence, achieving the dynamic adjustment of trust evaluation. Finally, full consideration has been given to the timeliness of interaction record in the paper. The calculation of trust evaluation is performed on the basis of dynamic Bayesian network. The historical interaction record, trust attenuation regulatory factor, the punishment factor, etc. are introduced to the calculation process, in such a manner to sensitively reflect the dynamic changes of confidence of related subject while accurately calculating trust evaluation of each subject. The next step in the author schedule will be further improving the model, studying the connecting of trust evaluation, designing appropriate management functions, and conducting performance evaluation on the TDBTBAC model.

CONFLICT OF INTEREST

The authors confirm that this article content has no conflict of interest.

ACKNOWLEDGEMENTS

Declared none.

REFERENCES

[1] KUMAR M, SHIRAZI B A, DAS S K, et al, "PICO: a middleware framework for pervasive computing," IEEE Pervasive Computing, vol. 2, pp.72-79, Mar. 2003.

[2] JUNG Y,JOSHI J B D, "CRIBAC: community –centric role interaction based access control model," Computer & Security, vol. 31, pp.497-523, Apr. 2012. [3] BHAVNA G, HARMEET K, NAMITA, "Trust based access control for grid resources," International Conference on Communication Systems and Network Technologies, Jammu, India, 2011,pp. 678-682.

[4] SUN Y, YU W,HAN Z, "Information theoretic framework of trust modeling and evaluation for ad hoc networks," IEEE Journal on Selected Areas in Communications, Selected Areas in Communications, vol. 249, pp.305-319,Feb. 2006.

[5] FENG R J,XU X F,ZHOU X, "A trust evaluation a algorithm for wireless sensor networks based on node behaviors and D-S evidence theory," Sensors, vol. 132, pp.1345-1360,Nov. 2011.

[6] BLAZE M,FEIGENBAUM J,LACY J, "Decentralized trust management," Proceedings of the 17th Symposium on Security and Privacy Oakland, Oakland, CA, 1996, pp.164-173.

[7] ABDUL-RAHMAN A,HAILES S, "Using recommendations for managing trust in distributed systems," Proceeding of IEEE Malaysia International Conference on Communication, Kuala Lumpur, Malaysia,1977, pp.1-7.

[8] MELAYE D,DEMAZEAU Y, "Bayesian dynamic trust mode," LNCS3690,Berlin:Springer-Verlag,Germany,2005, pp.480-489.

[9] Hu Jianli, Zhou Bin, Wu Quanyuan, "Dynamic P2P Trust Management with Incentive Mechanismin P2P Networks ," Journal on Communications, vol.32, pp.22-32, May. 2011.

[10] ALMENAREZ F,MARIN A,DIAZ D, "Developing a model for trust management in pervasive devices," Proc of the 3rd IEEE Int'l Workshop on Pervasive Computing and Communication Security (PerSer 2006), Washington DC, USA, 2006 pp.267-272.

[11] Kamvar S D. Schlosser M T. Molina H G, "The EigenTrust algorithm for reputation management in Peer-to-peer networks," Proc of the 12thInt World Wide Web Conf(WWW2003), NewYork:ACM, 2003, pp.640-651.

[12] Zhou R F.Kai H W, "PowerTrust:A robust and scalable reputation system for trusted peer-to-peer computing," IEEE Trans on Parallel and Distributed Systems, vol.18, pp.460-473, Apr. 2007.

[13] Li Xiaoyong, GuiXiaolin, " Trust Quantitative Modelin Trusted Network Based on Multiple Decision," Chinese Journal of Computers, vol. 32, pp. 405-416, Mar. 2009.

Received: September 16, 2014 Revised: December 23, 2014 Accepted: December 31, 2014