TELKOMNIKA, Vol.11, No.1, January 2013, pp. 417~424
ISSN: 2302-4046

Role-based Trust Management Model in Multi-domain Environment

Xianchen Guo[1,2], Jun Zheng[1*], Qikun Zhang[1], Hongchang Liu[1]
[1]Beijing Key Laboratory of Intelligent Information, School of Computer Science and Technology, Beijing Institute of Technology, Beijing, 100081, China)
[2]The 6th Research Institute of China Electronics Corporation, Beijing, 100081, China
*Corresponding author, e-mail: zhengjun@bit.edu.cn

Abstract

Based on the in-depth analysis of issues in dRBAC model, which include the lack of commission depth control in distributed environment, the inefficiency of cascading revocation of the authorization roles and the incapability of judging whether the commission violates the principles of RBAC model before it is done, this paper proposed MD-dRBAC Model, designed trust management mechanism for MD-dRBAC Model, which was used to control the access, established the credible authority commission tree and finally proposed the detection algorithm for implicit authorities upgrading to avoid violation of the least privilege principle in RBAC model Extensive security and performance analysis show that the proposed schemes are highly efficient and secure.

Keywords*: MD-dRBAC; trust multi-domain; authority commission tree; implicit upgrade*

1. Introduction

With the rapid development of Internet, the form of resource sharing has been greatly changed: from closed, centralized management and relatively static local computing environments, expanded to open, decentralized autonomy and dynamic collaborative inter-domain computing environment. The changes have led to a lot of challenges, mainly in the access progress to shared resource, including the management of user's authentication, the formulation of authorization policies and other trust management tasks1, 2. Thus, the access control of shared resources has become an important research topic in the dynamic collaborative multi-domain environment. Now, a mature way to solve this problem is to use trust management system.

dRBAC (Distributed Role-Based Access Control) model is proposed by Freudenthal, which uses PKI to identify the users' identities and commissioning certificates, in order to control the cross-domain access of shared sources in a dynamic collaborative environment. To a certain cross-domain Internet application system, dRBAC is a scalable, decentralized trust management and access control mechanisms, in which roles defined in a certain domain could be assigned to roles in other domains transitively.

dRBAC model is a distributed trust management and access control mechanism with good scalability, which has the following three features: third-party commission, the value of property, booking of the certificate. However, dRBAC model also has some shortcomings, including the following aspects: ① Lack of control on third-party commission depth; ② Because of the ways of commission management, commission chain may form a ring, but there is no discussion about how to avoid the ring 3; ③ There may be problem of implicit enhancement of roles' authorities, which is contrary to the roles' hierarchical relationships in RBAC model 4, 5; ④ Use RBAC model to manage the domains, but there is no detection for the principle of separation of duties 6, 7.

In this paper, aimed at the above problems, a reasonable solution would be proposed based on the deeply analysis of the current dRBAC technology development, to further explore and to promote dRBAC to safer, more practical direction.

Received August 13, 2012; Revised November 12, 2012; Accepted November 26, 2012

2. Multi Domain-dRBAC model

2.1 MD-dRBAC Trust Model

The Bayesian decision theory: Assuming the overall probability distribution is $f(x,\theta)$, $\theta \in \Theta$ is the unknown parameter, sample drawn from the overall is $X_1,...X_n$, parameter estimation can be derived as follows by using the sample and θ 8.

1) Bayesian Estimation

(a). Take the unknown parameter θ as a random variable (or random vector), and before sampling take the already known information of θ as priori knowledge. Use a certain probability distribution $h(\theta)$ to represent such a priori knowledge, and this probability distribution $h(\theta)$ is called the "priori distribution" of θ. This distribution reflects the probability distribution of the information obtained about the unknown parameter θ before experiment.

(b) Define the distribution function $f(x_1,\theta)...f(x_n,\theta)$ of the sample $X_1,...X_n$, containing the parameter θ as the conditional distribution function of $X_1,...X_n$ on condition of the given θ. So the joint probability density function of $(\theta, X_1,..., X_n)$ is $h(\theta)f(x_1,\theta)...f(x_n,\theta)$, and the marginal probability density of $X_1,...X_n$ is $p(X_i,..., X_n) = \int_{\theta\in\Theta} h(\theta)f(X_1,\theta)...f(X_n,\theta)d\theta$.

(c) Propose the conditional distribution function of θ on condition of the given $X_1,...X_n$ is:

$$h(\theta \mid X_1,..., X_n) = \frac{h(\theta)f(x_1,\theta)...f(x_n,\theta)}{p(X_i,..., X_n)} \quad (1)$$

which is called "posterior probability density" of θ. The function represents the probability distribution of knowledge about θ after obtaining the sample $X_1,..., X_n$; and comprehensively reflects the priori distribution of θ and the information brought by the sample.

(d) Make the inference of θ by $h(\theta \mid X_1,..., X_n)$.

MD-dRBAC Trust Model: In multiple trust domains environment, model of access control mechanism for inter-domain is shown as "Figure 1", each domain has a resource server, a trusted proxy server and multiple local users, resource server provides the service of domain resources, trusted server is set to facilitate the management of trust and the proxy server maintains two trust tables, one of which records the trust of local users and the other records the direct trust values among domains (trust value of direct interaction with this domain). Each local user maintains a record sheet, on which records the trust between the other users in this domain and itself.

2) Trust Calculation

(a) Calculation of direct trust value within domain

Calculate the direct trust within domain by using Bayesian decision theory to estimate the success and failure rate of a certain service.

Assuming the interaction between node *i* and node *j* is random, the evaluation sequence of node *i* to node *j* is $ES_{ij}.Rat = \{es_{ij}^1.Rat, es_{ij}^2.Rat, ..., es_{ij}^N.Rat\}$, $ES_{ij}^+ = \left\{es_{ij}^n \middle| es_{ij}^n \in ES_{ij}^n, es_{ij}^n.rat = 1\right\}$ expresses the positive evaluation sequence set of node *i* to node *j*, $ES_{ij}^+ = \left\{es_{ij}^n \middle| es_{ij}^n \in ES_{ij}^n, es_{ij}^n.rat = 0\right\}$ represents the negative

evaluation sequence set of node *i* to node *j*, supposing the number of positive evaluations is $Z_{ij} = | ES_{ij}^{+} |$ and the number of negative evaluations is $F_{ij} = | ES_{ij}^{-} |$.

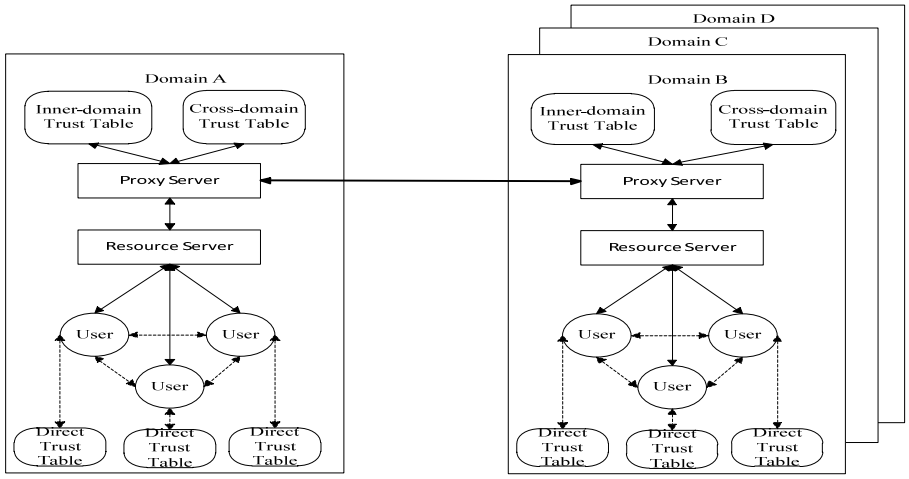

Figure 1. MD-dRBCA trust model

Suppose the probability of successful interactions is p and the failed is q, the Bayesian conditional expectation estimates of p and q will be

$$\tilde{p} = \frac{Z_{ij} + 1}{N_{ij} + 2}, \tilde{q} = \frac{F_{ij} + 1}{N_{ij} + 2}, \tilde{p} + \tilde{q} = 1 \quad (2)$$

Therefore, node *i* can estimate the probability of success of the interaction between node *j* and itself.

Suppose node *i* and node *j* are not connected, $Z_{ij} = | ES_{ij}^{+} | = 0$, and $\alpha = Z_{ij} + 1 = 1$; $F_{ij} = | ES_{ij}^{-} | = 0$, and $\gamma = F_{ij} + 1 = 1$. The original probability density of p is $Beta(\alpha, \gamma) = Beta(1,1)$, which is evenly distributed on [0, 1], therefore $\tilde{p} = \frac{\alpha}{\alpha + \beta} = \frac{1}{2}$. When they are connected, which is to say that $\alpha = 2, \beta = 2$, $\tilde{p} = \frac{2}{2+2} = \frac{1}{2}$. With the increment of evaluation, node i will know more about node j, and p will be more accurate.

Calculation of direct trust: suppose Z_{ij} and F_{ij} each represents the number of positive evaluations and negative evaluations, $\alpha = Z_{ij} + 1$ and $\gamma = F_{ij} + 1$. Suppose p is the probability of successful and q is the probability of failed interactions of node i to node j, $E(h(p \mid \alpha, \gamma))$, $E(h(q \mid \alpha, \gamma))$ each means the mathematical expectation of Bayesian estimation. Then the calculation of direct trust can be as follows:

$$DTV_{ij} = \begin{cases} E(h(p|\alpha,\gamma)) - E(h(q|\alpha,\gamma)) = \frac{\alpha - \gamma}{\alpha + \gamma}, (\alpha > \gamma) \\ 0 \qquad\qquad\qquad\qquad\qquad , others \end{cases} \quad (3)$$

(b) Calculation of recommended trust value within domain

Calculation of recommended trust of node *i* to node *j*: When finding the direct trust table of node *j*, we construct recommendation network by recursively searching node *k* that is directly

interacts with node *j*, calculate the recommended trust through the pass and synthesis relation of trust. In order to avoid finding too deeply, the recursion depth should be limited, so that the influence to calculation from trust path could be ignored at the same time.

Definition1: Rust intensity represents the reliability of trust in progress of recommendation trust delivery; it reflects the main entity's belief degree of direct trust. Use I to represent the trust intensity, and $I \in [0,1]$.

Definition2: Recommendation trust includes the direct trust value of object entity and trust intensity of direct trust value, which is to say that recommendation trust consists of the direct trust value and trust intensity. Recommendation trust is represented as (T, I) and is called recommendation trust vector or trust vector in short.

3) Delivery of trust relation

The recommendation trust will attenuate in progress of trust delivery, performs as the attenuation of trust intensity, as shown in "Figure 2" (a). Suppose the trust value of k to j got from direct experience is T_{kj}, the trust value of i to k is T_{ik}, then the recommendation trust vector that k recommends to i is (T_{kj}, 1), after receiving the recommendation trust from k and the other entities, i synthesizes them and finally get the trust relation. The attenuation formula of trust intensity is: $I_{ij} = T_{ik} I_{kj}$. Then the recommendation trust vector of entity i to entity j is (T_{kj}, T_{ik}), which means that the trust value of k to j get from direct experience is T_{kj}, and we can get T_{ik} as the conclusion of credibility of i to j. When there are multiple intermediate entities, the process is as the same9.

Synthesis of the trust vector

To synthesize the trust vector is to respectively synthesize the direct trust value and trust intensity. Synthesize the direct trust value by taking strength as the weight of trust.

As shown in "Figure 2" (b), according to the attenuation principle in previous section, upon the recommendation of intermediate entities a and b, i can get two recommendation trust vectors (T_{ij1}, I_{ij1}) and (T_{ij2}, I_{ij2}). Then based on the above analysis, the synthetic trust value of i to j is

$$IDTV_{ij} = \frac{I_{ij1}T_{ij1} + I_{ij2}T_{ij2}}{I_{ij1} + I_{ij2}} \tag{4}$$

When there are multiple intermediate recommended entities in parallel, the synthetic trust value of i to j will be:

$$IDTV_{ij} = \frac{\sum_{k=1}^{n} I_{ij_k} T_{ij_k}}{\sum_{k=1}^{n} I_{ij_k}} \tag{5}$$

If the two intermediate recommended entities a and b have the same recommended trust values, I_1 and I_2, which means that there are two evidences to prove that the recommended conclusion is true, and the possibilities are I_1 and I_2, so for comprehensive consideration, the possibility (synthetic trust intensity) that the recommended conclusion is true is:

$$I = 1 - (1 - I_1)(1 - I_2) \tag{6}$$

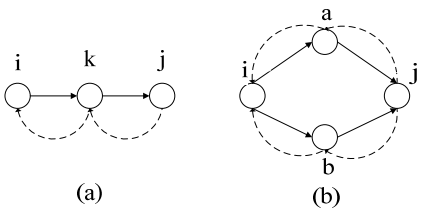

Figure 2. Trust delivery and synthesis

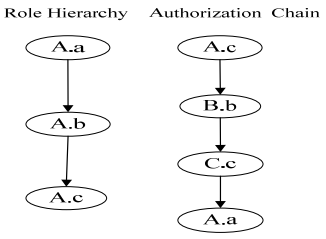

Figure 3. Implicit enhancement of role's authorization

When there are multiple intermediate recommended entities in parallel, the synthetic trust intensity will be:

$$I = 1 - \prod_{k=1}^{n} (1 - I_k) \tag{7}$$

But if the recommended trust values from the intermediate recommended entities are different, we should firstly synthesize the direct trust value and then get the synthetic trust value. In this case, intermediate entities firstly synthesize the direct trust value by the trust values of themselves, and then calculate the synthetic trust value by using the above formula10, 11, 12.

4) Calculation of direct trust value between entities

Calculation of direct trust between entities: By calculating the direct trust value and recommendation trust value, the trust value between entities can be calculated by the formula $TV_{ij} = \beta DTV_{ij} + (1-\beta) IDTV_{ij}, (0 \le \beta \le 1)$ with an appropriate weighting factor β.

5) Calculation of trust value across domains

The calculations of the direct trust value and the recommended trust value across domains are as the same with the calculations within domain. The formula for calculating the cross-domain trust value is

$DOMTV_{ij} = (\beta DOMDTV_{ij} + (1-\beta) DOMIDTV_{ij})\alpha + (1-\alpha)\varphi_i, (0 \le \alpha \le 1), 0 \le \beta \le 1)$, $DOMDTV_{ij}$ means the direct trust values between domains, $DOMIDTV_{ij}$ represents the recommended trust values of a certain domain, φ_i is the trust value of node i got from the trust table kept by proxy server in this domain.

2.2 Detection of implicit enhancement of role's authorization

In dynamic alliance environment each organization manages its access controlling by using the RBAC model. But now there may be some detection that are contrary to the principles of RBAC model, as shown in "Figure 3", role A.a has higher level than A.c, but A.a can be concluded to have the authorities of A.c according to the right authorization chain, which is clearly contrary to the role hierarchies principle of RBAC model.

By using the credibility-authority tree proposed in this paper, we can easily check whether an authorization makes implicit enhance happen. As shown in "Figure 3", suppose authorizations A.c->B.b and C.c->A.a have been done, then B.b->C.c cannot happen because it is contrary to principles of RBAC model. So it's necessary to check the authorization source's authorities and authorized entity's credibility-authority tree before each authorization. Take "Figure 6" for example, by checking the authorization tree of B.b and C.c's authorities we can find that C.c owes authorities of A.a, but A.c is in the authorization tree of B.b and A.c should not have the authorities of A.a, so B.b->C.c is contrary to principles of RBAC model and should be denied 13,14.

Algorithm of detecting implicit enhancement of role's authorization:

```
//Check Whether Certificate c Goes Against Least Privilege Principle
//Input: Certificate c, represented as <sub, obj>, use c.sub and c.obj to represent the
subject and //object of c
```

```
//Output: True/False
Flag
{
If c.sub is an entity Then
Return True           //[sub → obj] Issuer will not violate Least Privilege Principle
Search delegation tree forward      // Search upwards the authorization tree
For each object in c.subject's delegate tree
{
RS = null //RS means the set of Objects that within the same domain of c.obj
For each delegation c' in delegation tree
{
If Domain(c'.obj) = Domain(c.sub) Then RS = RS ∪{c'.obj}
//Domain(x) means to find the name of x's domain
}
Judge(c.sub, RS, RH)   //RH means the Role Hierarchy of c.sub's domain
}
Return Flag
}
Judge(r, R, RH)        //To judge whether there are roles that have higher level than r
in R
//Input: Role r, Roles Set R, Role Hierarchy RH
//Output: True/False
{
Flag = True
For each r'∈R
{
If <r, r'>∈RH Then Flag = False   //There are roles that have higher level than r
}
}
```

3. Simulation and Analysis results of Trust Mechanism

In MD-dRBAC model proposed in this paper, we build both trust relations between entities and domains; take different algorithms to calculate their trust values according to their natures and characteristics, and finally make accurate assessment of their trust relations.

3.1 Simulation Scene

The scenario supposed in this paper is interactions between entities within a domain, in which a user aims to accessing an interested node, and it doesn't matter whether he wants to upload or download a resource he wants or even just a simple accessing. The concerns we care most are whether the source node is being recognized by the target node and the recognition accuracy. Experiment hardware environment: Intel Core i7 870 2.93 Ghz + 4G RAM; software environment: Windows Xp Operation System and MyEclipse. There are totally 40 nodes in this experiment, which is divided into two types: honest nodes, they use services provided by the network safely and rationally, and can accurately rate collaborations between entities; dishonest entities, they use the services unreasonably, and they may even cause threats to the service providers. The weight parameter β in trust formula is set to be 0.9, which means that entities pay more attention to the direct trust value of access nodes rather than indirect values from other entities.

3.2 Experimental results and analysis

Experiment 1: We observe the changes of trust relations between entity i and both honest entities and dishonest entities along with the increase of interactions. It is supposed that honest entities and dishonest entities have the same number in our experiment. Simulation parameters are shown in Table 1.

Table I. Simulation parameters

Total number of entities	40
Honest entities	50%
Dishonest entities	50%
Original direct trust value	0.5
Threshold of trust	0.4
Weight parameter β	0.9

"Figure 4" shows the trend of trust relation changes between entity i and both honest entities and dishonest entities along with the increase of interactions. Since the original direct trust value is 0.5 and it's above the threshold 0.4, so entities at the beginning can access each other. In "Figure 7", horizontal axis represents the times of interactions; vertical axis represents the trust value; red line represents the trend of relations between entity i and honest entities while blue line means trend of dishonest entities'.

As we can see in "Figure 4", along with the increase of interaction times, trust values of honest entities gradually increase while the trend of dishonest entities is decreasing. As a result, the target entity could pre-judge whether the source entity is honest or not and then decide to permit or reject the access.

Experiment 2: Compare the trends of accuracy of detecting malicious behavior in both our model and EigenTrust Model. The simulation parameters are the same as experiment 1, "Figure 5" shows the result:

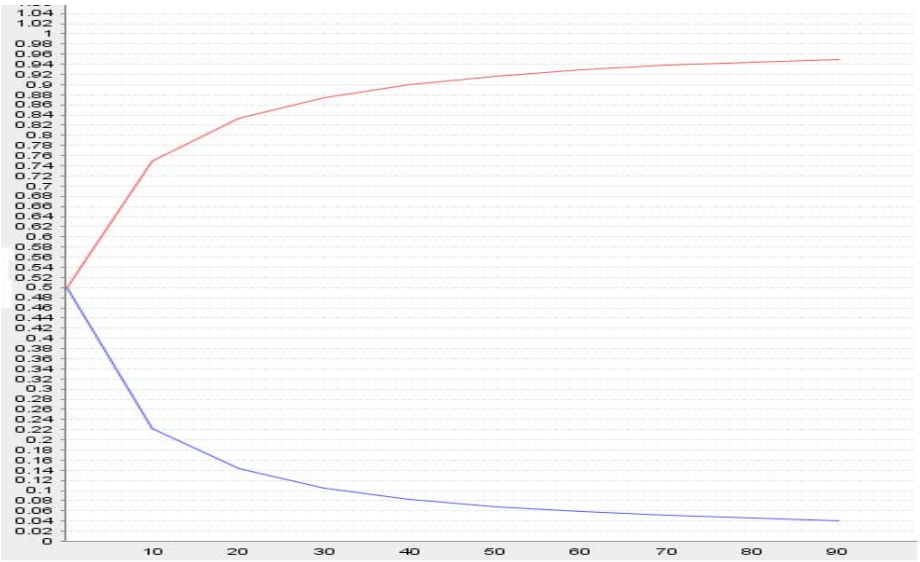

Figure 4. Trend of trust relations along with interactions increase

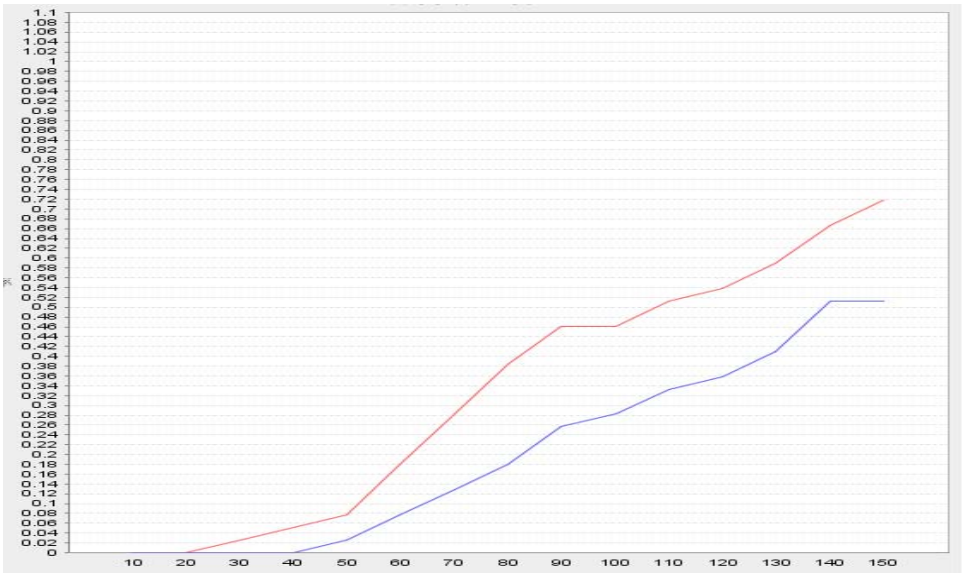

Figure 5. Comparison of malicious behavior detecting accuracies in two models

Red line represents the accuracy of MD-dRBAC Trust Model proposed in this paper, while the blue one means the result of EigenTrust Model. Which is shown in “Figure 8” is that MD-dRBAC Trust Model has faster convergence than EigenTrust Model.

4. Summary

In this paper, we deeply analyzed several issues of dRBAC model, which include the lack of commission control depth in a distributed environment, the inefficiency of cascading revocation of the authorization roles and the incapability of judging whether the commission violated the principle of RBAC model before it is done and so on. To deal with these problems, we proposed MD-dRBAC model, designed trust management mechanism of MD-dRBAC Model, which was used to control the access, established the credible authority commission tree and finally proposed the detection algorithm for implicit upgrade of the role’s authority to avoid violation of the least privilege principle in RBAC model. The experiments and analyses prove the feasibility, effectiveness and safety of MD-dRBAC model.

References

[1] Yu. LN, Gao. WL, Wang. JQ, Yang. KM, Liu. ZL, Wang. Q. Research of a Massive Distributed Remote Sensing Data Resource Sharing Method Under Grid Environment. *SENSOR LETTERS*. 2010; 8(1): 11-15.
[2] Zhang QK, Tan, YA, Zhang L, Wang RF. A Combined Key Management Scheme in Wireless Sensor Networks. *SENSOR LETTERS*. 2011; 9(4): 1501-1506.
[3] R Sandhu, E Coyne, H Feinstein, and C Youman. Role-based Access Control Models. *IEEE Computer*. 1996, 29(2): 3847.
[4] Li Ninghui, William H Winsborough, John C Mitchell. Distributed credential chain discovery in trust management. *Journal of Computer Security*. 2003; 11(1): 35-86.
[5] Chen Ying, Yang Shoubao, Guo Leitao, Liu Pengzhan, Shen Kai. *Design and implementation of Dynamic-Role Based Access Control framework in grid environment*. Int. Conf. Inf. Technol. Coding Comput. Apr. 2005; Vol.2: 758-759.
[6] Baoyi Wang, Shaomin Zhang, Zhilei Zhang. DRBAC based access control method in substation automation system. 2008 *IEEE International Conference on Industrial Technology (ICIT)*. 21-24 April 2008.
[7] Ferraiolo D F, Sandhu R S, Gavrila S. et al. *Proposed NIST standard for role-based access control. ACM Transaction on Information and Systems Security*. 2001; 4(3): 224-274.
[8] Ming Zhimao. Test and Research On Bayes with Dynamic Parameters. *National University of Defense Technology*. 2009.
[9] Yin Gang. Research and Implementation on Authorization Management in Inter-Domain Computing Environment. *National University of Defense Technology*. 2006.
[10] Josang A, Grandison T. Conditional inference in subjective logic. in: Xuezhi Wang ed. Proceedings of the *6th International Conference on Information Fusion*. Cairns, Qld, Australia. 2003. Gallup, NM, USA: Univ. New Mexico. 2003. 635642.
[11] Josang A. A logic for uncertain probabilities. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*. 2001; 9(3): 279311.
[12] Liao Junguo. A Dissertation Submitted to Huazhong University Technology. 2007.
[13] Zhong Hua, Feng Yulin, and Jiang Hongan. Expanded role hierarchy model and its application. *Journal of Software*. 2000: 779-784.
[14] Liao Junguo, Hong Fan, and Yang Qiuwei. Zhang Zhaoli. Safety analysis of dRBAC model. *Journal of Chinese Computer Systems*. 2007; 28 (4): 22-31.