第34卷 第21期 计 算 机 工 程 2008年11月
Vol.34 No.21 Computer Engineering November 2008
·安全技术· 文章编号：1000—3428(2008)21—0153—04 文献标识码：A 中图分类号：TP393.08

基于信誉担保的网格域动态管理模型

王荣斌[1,2]，陈蜀宇[3]，喻 玲[1]，姬晓波[1]
(1. 重庆大学计算机学院，重庆 400044；2. 重庆高速公路发展有限公司，重庆 400042；3. 重庆大学软件工程学院，重庆 400044)

摘 要：针对目前网格环境下域间管理存在可扩展性、动态适应性差的现状，提出一种基于信誉担保的网格域成员关系管理模型DMRGGD。建立基于信誉值的网格域信誉担保的推荐模型，为新加入的域成员在不依赖中心服务器的情况下建立初始信誉值，在域成员间通过计算直接信任度和多路径间接信任度，实现动态更新信誉值和评估信任关系，通过担保人信誉连带责任制，防止恶意担保。

关键词：网格；信誉值；信任路径；信誉担保；连带责任

Dynamic Management Model Based on Reputation Guarantee in Grid Domains

WANG Rong-bin[1,2], CHEN Shu-yu[3], YU Ling[1], JI Xiao-bo[1]
(1. College of Computer Science, Chongqing University, Chongqing 400044; 2. Chongqing Expressway Development Ltd. Co., Chongqing 400042; 3. College of Software Engineering, Chongqing University, Chongqing 400044)

【Abstract】 To solve the management problem of lacking extensibility and dynamic adaptability in grid domains, this paper puts forward Dynamic Model Based on Reputation-Guarantee in Grid Domains(DMRGGD). In order to join the grid domain and construct the trust with others without the central server for the new domain member, it presents the domain recommendation model based on worthiness. The relations are evaluated and the worthiness is updated for domain members dynamically by computing the direct reputation and indirect reputation of multipath. With the joint responsibility for guarantor, the model is able to prevent malicious guarantee.

【Key words】 grid; worthiness; trust path; reputation guarantee; joint responsibility

1 概述

由于网格具有分布性、异构性、动态演化及广域的特性，因此构建网格安全体系异常困难。如何在网格环境中鉴别用户身份、动态建立动态信任关系，并对用户的访问权限进行动态管理，至今仍未得到很好的解决。目前在网格环境中，域成员之间信任关系的建立大多依靠虚拟组织内的中心服务器，通过其进行身份注册、身份验证、签发身份证书或分配密钥。自治域之间信任管理主要有3种方式：(1)基于中心服务器的集中式管理方式，如CAS[1]；(2)基于中心服务器的层次型管理方式，如Akenti[2]和PERMIS[3]机制；(3)基于多证书的分布式管理方式，如文献[4]提出的基于门限签名算法的投票表决机制，文献[5]提出的基于联合策略的多域信任协商机制，文献[6]讨论了如何基于CAS证书建立网格环境下的信任关系。但都没有结合域间信任关系的动态评估、网格域成员的动态加入和退出机制及初始信任的建立等。

2 基于信誉担保的网格域动态管理模型

2.1 模型概述

本文提出了基于信誉担保的网格域动态管理模型(Dynamic Model Based on Reputation-Guarantee in Grid Domains, DMRGGD)，其结构如图1所示。模型的核心是信誉评估管理器(Reputation Evaluation Manager, REM)和信誉担保管理器(Reputation Guarantee Manager, RGM)，包括信誉评估、关系评估、执行策略、证书存取、证书库及通信接口等模块。REM主要负责对域成员的身份和关系是否可信进行计算和判断，RGM主要对申请加入网格的新成员身份进行鉴别，对域成员的信誉值进行计算，并判断是否有资格承担信誉担保，如有资格，则签发担保证书。信誉评估模块主要对域成员的信誉值进行评估，并计算自身的信誉值，判断是否有资格进行信誉担保以及计算新成员的初始信誉值等。关系评估模块对域成员提供的担保证书或身份证书的CA进行验证，确保来访用户来自于本地域所信任的域。数据库主要存储可信域CA证书、担保证书*Cert_reput*、信誉值及有不良记录域的黑名单。证书库通过更新模块进行及时更新，通过存取模块进行读取和存储。签发担保证书模块对请求信誉担保的管理域身份验证合格后，向请求域签发信任但保证书*Cert_reput*。

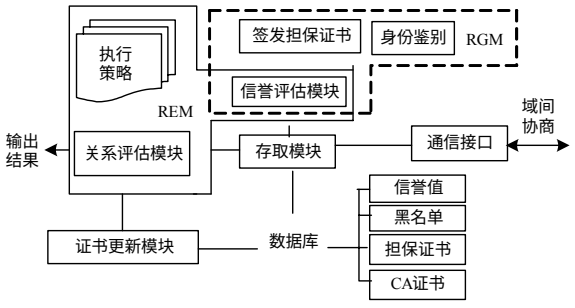


图1 DMRGGD模型结构

基金项目：教育部新世纪优秀人才支持计划基金资助项目(NCET-04-0843)；重庆市自然科学基金资助项目(2005BB2192)
作者简介：王荣斌(1974－)，男，高级工程师、博士研究生，主研方向：网格计算，信息安全；陈蜀宇，教授、博士生导师；喻 玲、姬晓波，博士研究生
收稿日期：2007-12-25 **E-mail**：wangrongbin@vip.163.com

定义 1 基本元素

(1)网格G：$G=\{g_1, g_2,\cdots,g_n\}$，$g_i(i=1,2,\cdots,n)$是网格中同一虚拟组织内的域成员。

(2)网格G^+：$G^+=G\cup g_{n+1}=\{g_1,\cdots,g_n,g_{n+1}\}$表示新域成员$g_{n+1}$加入网格$G$。

(3)网格G^-：$G^-=G-g_n=\{g_1,\cdots,g_{n-2},g_{n-1}\}$表示域成员$g_n$退出网格$G$。

定义 2 信誉担保证书

$Cert\_reput=\{CA\_ID, \{Son\_ID, Son\_p, R_{n+1}, TL, R_i\}, sign\{Son\_ID, Son\_p, R_{n+1}, TL, R_i\}\}$

其中，CA_ID为信誉担保域CA的公开身份；R_{n+1}为信域成员的初始信誉值；Son_ID, Son_p为被担保域的身份信息和公钥；TL为担保证书的生存时间；R_i为担保域的信誉值；$sign\{Son_ID, Son_p, R_{n+1}, TL, R_i\}$为担保域的数字签名，保证担保证书的真实性。

定义 3 信任关系

$A\Rightarrow B$表示 A 完全信任 B，$A\perp B$表示 A 不信任 B，$A\Leftrightarrow B$表示 A 与 B 互相信任；信任担保关系$A\xrightarrow{C}B$表示在 C 作为信任担保人推荐的前提下，A 信任 B。

定义 4 DMRGGD 模型形式化定义

$DMRGGD=\{G, AD, Cert\_reput, LE, RE, RG, ADDM\}$

其中，LE为关系评估；RE为信誉评估；RG为信誉担保；$ADDM$为域成员动态管理。

2.2 模型基本组件

(1)信誉评估

定义 5 直接信任度P_{ij}

P_{ij}代表域j对域i的局部评价，即直接信任度或局部信任度。P_{ij}等于当次交互后的直接信任度与历史交互的评价的加权和。

定义 6 直接信任关系矩阵 $\boldsymbol{P}$

$$\boldsymbol{P}=\left|P_{ij}\right|_n, i,j=1,2,\cdots,n$$

如果以加权有向图 $G(V, E)$表示这种交互关系，则

$$|G|=n,\ V=\{i\mid \exists j, i\xleftarrow{P_{ij}} j\}$$

其中，$i\xleftarrow{P_{ij}} j$ 表示i, j之间存在直接交易，且j对i的评价即直接信任度P_{ij}。在$\boldsymbol{P}$中，如果i, j之间没有直接交互关系，则$P_{ij}=0$。如果$i=j$，则$P_{ij}=1$。

定义 7 间接信任度R_{ij}也称为推荐信任度，即域i, j之间没有直接交互，而是通过中间域推荐：$R_{ij}=\frac{1}{q}\sum_{s=1}^{q}\prod_{l,m\in p_{si}}P_{lm}$，其中，$p_s$是有向图$G(V, E)$上$j$点到达$i$点的第$s$条路径，$p_s$的出发点是$j$，终点是$i$；$l$, m是p_s上的相邻节点，共有q条路径；R_{ij}为路径p_s上节点间的直接信任度P_{lm}之积。

定义 8 全局信任度R_i

$$R_i=\left(\frac{(1-\alpha)}{y}\sum_{k=1}^{y}R_{ik}+\frac{1}{x}\alpha P_{ij}\right),\ k\neq i,j,i=1,2,\cdots,n$$

其中，R_{ik}是k域对i域的推荐信任度；α为直接信任度所占权重；R_i即网格域i的信誉值，任意域的全局可信度为与之发生过交互行为的域对其直接信任度以及间接信任度的加权和；x为直接信任节点数；y为存在间接信任关系的节点数。

定义 9 网格信域值矩阵 $\boldsymbol{R}$

$$\boldsymbol{R}=\left|R_i\right|_n, i=1,2,\cdots,n$$

(2)关系评估

定义 10 在DMRGGD中，域i的信誉值$R_i\geq R_0$时，虽然存在一定风险，但该域在本虚拟组织内是值得信任的；$R_i<R_0$时，该域是不可信的，与其交互将存在较大风险。其中，R_0是虚拟组织内域成员共同商定的一个可信门限值。

定义 11 在DMRGGD中，域j的信誉值$R_j\geq E_0$时，该域在本虚拟组织内有资格进行信成员加入的信誉担保；$R_j<E_0$时，该域没有资格作为新成员推荐人进行信誉担保。其中，E_0是虚拟组织内域成员共同商定的一个担保信誉门限值，一般$E_0>R_0$。可通过下式确定DMRGGD网格中某个域i是否有资格进行信誉担保：

$$F(R_i,E_0)=\begin{cases}1 & R_i\geq E_0\\ 0 & R_i<E_0\end{cases}$$

(3)信誉担保

定义 12 新域成员g_{n+1}的初始信誉值R_{n+1}是指新成员加入网格后被其他网格域成员所信任的程度，是信誉担保人g_i所赋予的，为信誉担保人自身的信誉值与担保人对被担保人的信任程度的乘积：$R_{n+1}=R_i\cdot P_{(n+1)i}$。新成员获得初始信誉值后，在与其他域成员交互时，就有了信任基础，随着交互次数增加，新成员的信誉值逐步更新，与其他域成员之间建立起新的信任关系。

定义 13 担保人g_j的惩罚值Δp_{ij}即对担保人的直接信任度进行扣减的值：

$$\Delta p_{ij}=\beta\cdot(1-R'_{n+1})$$

其中，R'_{n+1}为被担保人在担保有效期内的信誉值；β为连带责任放大系数。惩罚值ΔP_{ij}为在其担保的有效时间内，被担保人g_{n+1}在网格中有严重的不良行为，导致担保人承担连带责任，扣减其直接信任度，并更新担保人的直接信任度为

$$P'_{ij}=P_{ij}-\Delta P_{ij}=P_i-\beta\cdot(1-R'_{n+1})$$

网格域成员将根据信誉评估算法和关系评估算法重新对担保人进行信任评估和关系评估。

(4)域成员的动态管理

1)新域成员的动态加入

如图 2 所示，一个新域成员g_{n+1}的加入需要得到至少一个网格域内R_i较高的成员g_i的推荐，作为g_{n+1}的担保人，要求g_i在网格域G内被其他成员完全信任。

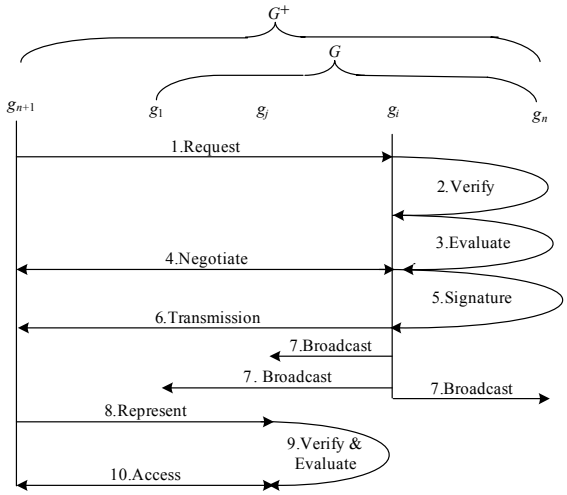


图 2 新域成员加入网格的执行步骤

根据定义 3 知，作为新加入的域成员，

$$\forall g_j\Rightarrow g_i, g_i\Rightarrow g_{n+1}, g_j\xrightarrow{g_i}g_{n+1}$$

在担保人被其他成员都信任的情况下，具有信任传递特性，

其他成员对被担保人有条件信任。

新域成员加入网格步骤如下：

步骤 1 g_{n+1}向其信任的网格成员 g_i发起申请加入网格的申请：

$g_{n+1} \to g_i$：Request for *cert_reput*: *My-ID*, *My_p*, *sign*{*My-ID*, *My_p*}

步骤 2 g_i验证g_{n+1}的身份有效性：

g_i: Verify by *My_p*

如果$sign^{-1}\{sign\{My\text{-}ID, My_p\}\}= My\text{-}ID, My_p$，则验证有效，否则无效，否决担保申请。

步骤 3 g_i对本地域的信誉值进行评估。

g_i: Evaluate the R_i

判断是否有资格进行信誉担保。

步骤 4 g_i与g_{n+1}协商g_{n+1}公钥及身份信息。

步骤 5 g_i为g_{n+1}签发信誉担保证书。

g_i:*Cert_reput*={*CA_ID*,{*Son_ID*,*Son_p*, R_{n+1}, *TL*, R_i}, *sign*{*Son_ID*, *Son_p*, R_{n+1}, *TL*, R_i}}

其中，$g_{n+1} \leftrightarrow g_i$: Negotiate the *Son_p* & *Son_ID*；*CA_ID*, *Son_ID* 分别为g_i, g_{n+1}的身份，其余参数见定义 2。

步骤 6 g_{n+1}向g_i传递信誉担保证书：

$g_i \to g_{n+1}$: Transmission *Cert_reput*

步骤 7 g_i向VO内除本地域之外的所有域成员广播信誉担保证书*Cert_reput*：

$g_i \to g_1, g_2, \cdots, g_{i-1}, g_{i+1}, \cdots, g_n$: Broadcast *Cert_reput*

其他域成员保存该担保证书，G^+刷新成员关系库。

步骤 8 g_{n+1}向g_j申请资源时，出示自己身份证书和信誉担保证书：

$g_{n+1} \to g_j, j = 1,2,\cdots,n$: Represent X.509 & *Cert_reput*

步骤 9 g_j验证g_{n+1}的身份和信誉担保证书的有效性：

g_j:Verify the Validation of ID of g_{n+1} & *Cert_reput* with g_{n+1}

步骤 10 如果g_{n+1}身份或信誉担保证书无效则否决资源请求，如果都有效，则提供资源访问：

$g_{n+1} \leftrightarrow g_j$, j=1,2,$\cdots$,n: Access

2)域成员的动态开除

新域成员的初始信誉值根据定义 12 由担保域成员赋予，当新域成员被其他域成员接受后，其信誉值随着与其他域成员的交互而动态更新。在信任担保证书的生存时间内，如果新成员有超越其权限或恶意攻击、盗取行为，其信誉值将急剧衰减，低于作为可信网格域成员的信誉值后，则被记入黑名单库并开除，此时G^-内域成员进行刷新。同时，担保人将负担连带责任受到惩罚，其信誉值将被扣减，其他域成员对其信任程度会降低，它可能从此不能再进行信誉担保。

2.3 信誉评估算法

在DMRGGD中，每个网格域都存储有一个直接信任关系矩阵库，通过该库计算某域的信誉值R_i，由此可判断该域是否具有信誉担保的资格。域成员之间的直接信任关系P_{ij}通过广播方式传递，因此，可保持在DMRGGD内所有域成员直接信任关系矩阵库的同步。

算法 1 信誉评估算法

输入 信任矩阵 $\boldsymbol{P} = \left|P_{ij}\right|_n$, $i, j = 1,2,\cdots,n$

输出 网格信誉值矩阵 $\boldsymbol{R}$

初始化p[m]=∅, Q=∅, α, E_0, R_0,m=1;

//Q 为与 i 域有直接交互关系的域，即有向图上的相邻节点；//p[m]存储到 i 的路径

for i=1; i<n; i++;

{for j=1; j<n;

{input P[i][j];

if P[i][j]≠0, Q={j，i}j++;

//路径搜索算法，如果 P[i][j]≠0，说明 i, j 之间存在直接信任关//系，记入 Q

else

for l=1;l<n

{if P[j][l]≠0, then p[m]= p[m]∪{ j, l}

//路径搜索算法，从 j 节点开始搜索

//如果 l 正好与 Q 中某域存在直接信任关系，则找到了到 i 的路//由，但仍需重新搜索是否还存在到 i 的其他路由

else j= l

//如果 l 不在 Q 中，则以 l 为起点继续搜索

continue;}

return;

//继续找出与 i 没有直接交互关系的所有其他路由

根据定义 10 计算R_{ij};

计算R_i; }}

3 实现与仿真

为验证本模型的有效性，本文以 8 个网格域为例，相互之间的直接信任关系有向图如图 3 所示，箭头表示出发点对终点的直接信任度，在有向图中，节点代表网格域，有向边代表域之间的直接交互评价的直接信任度，节点 1 与节点 2, 3, 4 有直接交互，节点 2 与节点 1, 5 有直接交互，依次类推，节点 8 与其他节点之间都没有发生过直接交互，因此，称为“孤儿”节点。

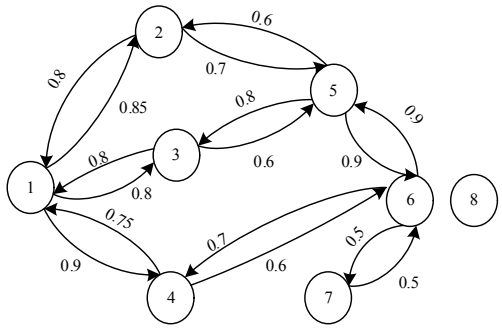


图 3　8 个域成员之间的直接信任关系有向图

根据算法 1 按照以下步骤计算信誉值：

(1)建立直接信任关系矩阵

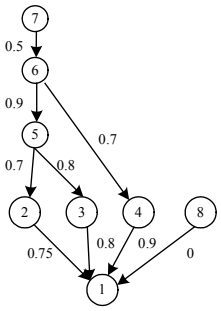
通过有向图$G(V, E)$建立 8 行 8 列的直接信任矩阵，其中，行为被评价域；列为评价域。矩阵的值为直接信任度，0 表示节点之间没有直接信任关系，1 表示完全相信，$i=j$时，P_{ij}=1；$i\neq j$时，0<P_{ij}<1。

$$\boldsymbol{P} = \begin{vmatrix} 1 & 0.8 & 0.8 & 0.75 & 0 & 0 & 0 & 0 \\ 0.85 & 1 & 0 & 0 & 0.6 & 0 & 0 & 0 \\ 0.8 & 0 & 1 & 0 & 0.8 & 0 & 0 & 0 \\ 0.9 & 0 & 0 & 1 & 0 & 0.7 & 0 & 0 \\ 0 & 0.7 & 0.6 & 0 & 1 & 0.9 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0.9 & 1 & 0.5 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0.5 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{vmatrix}$$

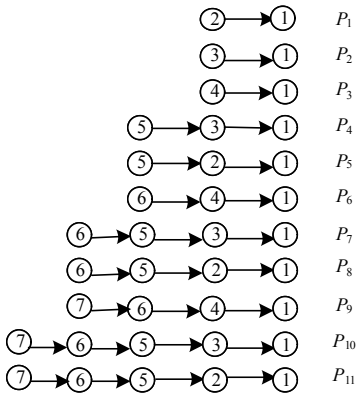
(2)抽象对节点 1 的信任关系路由

如图 4(a)所示，对于节点 1 而言，其信任关系路由图表示出从其余节点到达节点 1 的有向路由，相邻节点之间形成有向边，边上权值为相邻节点之间的直接信任度，其中，节点 8 与其他任何节点都不相连，因此其权值为 0。根据图 4(a)对每个节点到节点 1 的路由进行搜索，路径搜索结果如

图 4(b)，其中，节点 6, 7 到达节点 1 的路径有 3 条，说明节点 6, 7 对节点 1 的推荐信任度经过多路径传播，因此对节点 1 的推荐信任度是这 3 条路径的平均值。



(a)其他域成员对域 1 的全局信任关系路由图



(b)其他域成员对域 1 的全局信任关系路径图

图 4　DMRGGD 信任关系图

其他域成员到域 1 的信任路由及其信任度见表 1。

表 1　其他域成员到域 1 的信任路由及信任度

路径	出发节点	途径节点	信任值	信任方式
P_1＝{2,1}	2		0.8	直接
P_2＝{3,1}	3		0.8	直接
P_3＝{4,1}	4		0.9	直接
P_4={5,3,1}	5	3	0.64	间接
P_5={5,2,1}	5	2	0.525	间接
P_6={6,4,1}	5	4	0.63	间接
P_7={6,5,3,1}	6	5, 3	0.576	间接
P_8={6,5,2,1}	6	5, 2	0.473	间接
P_9={7,6,4,1}	7	6, 4	0.284	间接
P_{10}={7,6,5,3,1}	7	6, 5, 3	0.288	间接
P_{11}={7,6,5,2,1}	7	6, 5, 3	0.237	间接

从表 1 可看出，节点到达路由经过的节点越多，其推荐信任度就越小，这符合常理。

(3)计算间接信任度

根据表 1 和定义 7 的间接信任度计算方法，可计算出各节点对域 1 的推荐信任度。节点 5 对节点 1 的间接信任度为

$$R_{51}=\frac{1}{2}(0.64+0.525)=0.583$$

其余节点计算方法相同，R_{61}＝0.539，R_{71}＝0.267。

(4)计算域 1 的信誉值

通常更重视节点之间直接交互的评价，即直接信誉度，在此取其加权系数 $\alpha=0.7$，计算出域 1 的信誉值为

$$R_1=\frac{1}{3}(0.8+0.8+0.9)\times 0.7+\frac{1}{3}(0.583+0.539+0.267)\times 0.3)=0.722$$

同理可计算出其他节点的信誉值：R_2=0.667，R_3=0.655，R_4=0.689，R_5=0.648，R_6=0.608，R_7=0.475，R_8=0。如图 5 所示，虚线表示有资格进行信誉担保的门限值为 0.65。可以看出，只有域 1~域 4 有资格进行信誉担保，如果设定可信域门限值为 0.5，则域 7 和域 8 是不可信的，将被开除。

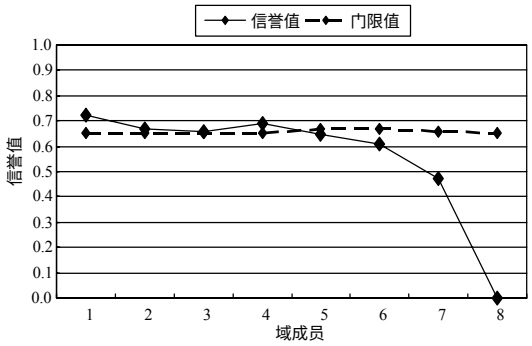


图 5　域间信任仿真结果

4　结束语

本文的 DMRGGD 模型不依赖于中心服务器建立新成员与其他域成员之间的信任关系，而是通过网格内具有高信誉的域成员进行信誉担保推荐。被推荐的新成员在交互过程中有不良行为时会被惩罚，担保人的信誉值也会降低。各域成员根据域间的信任关系评估模型和域成员动态管理机制来动态更新各成员的信誉值。当被推荐域成员的信誉值低于某个门限时，将被强制开除，可以有效防止恶意推荐或重复推荐。由于 DMRGGD 模型不依赖于中心服务器，也不需要其他域成员对该新域成员有足够的先验知识，而是通过值得信赖的域成员推荐来建立信任关系，符合人类社会的认识习惯，因此具有很好的动态适应性和可扩展性，适应网格环境下的应用。本文的信誉评价模型虽结合了直接信任度和间接信任度，但是在多路由情况下，推荐信任度会缓慢下降，建立一种更科学的信誉评价方法将是下一步的研究重点。

参考文献

[1] Pearlman L, Welch V, Foster I, et al. A Community Authorization Service for Group Collaboration[C]//Proceedings of the 3rd International Workshop on Policies for Distributed Systems and Networks. Washington, USA: IEEE Computer Society Press, 2002 .

[2] Thompson M R, Essial A A. Certificate-based Authorization Policy in a PKI Environment[C]//Proc. of TISSEC'03. [S. l.]: ACM Press, 2003.

[3] Chadwick D W, Otenko A. The PERMISX.509 Role-based Privilege Management Infrastructure[C]//Proc. of the 7th ACM Symposium on Access Control Models and Technologies. Monterey, California, USA: ACM Press, 2002.

[4] Qiang Weizhong, Jin Hai, Shi Xuanhua, et al. Joint Management of Authorization for Dynamic Virtual Organization[C]//Proceedings of the 5th International Conference on Computer and Information Technology. [S. l.]: IEEE Press, 2005.

[5] 陈　颖, 杨寿保, 郭磊涛. 网格环境下的一种动态跨域访问控制策略[J]. 计算机研究与发展, 2006, 43(1): 1863-1869.

[6] 刘　妍, 郭　洁, 陈克非. 认证授权技术在网格中的应用与扩展[J]. 计算机工程, 2004, 30(24): 44-46.