网格计算中基于信任度的动态角色访问控制的研究

邓 勇 张 琳 王汝传 张 梅
(南京邮电大学计算机学院 南京 210003)

摘 要 在网格计算中,资源或服务使用者和提供者之间的信任关系是安全通信的前提。由于网格计算环境的分布特性和动态特性,像传统计算那样预先建立信任关系是不现实的。为了解决这个问题,在研究中发现,可以将信任机制融入网格社区授权服务中的基于角色的访问控制中,对基于角色的访问控制策略做一定的改进,根据信任度评估算法算出网格实体的信任度,CAS服务器能依据实体的信任度动态改变实体的角色。通过基于信任度的动态角色访问控制可以在一定程度上实现网格访问控制的动态性,同时避免实体的欺骗行为,可以有效地达到在网格社区中对客户端进行访问控制的目的。

关键词 网格计算,信任,基于角色的访问控制
中图法分类号 TP393 **文献标识码** A

Research on Dynamic Role-based Access Control Based on Trust Mechanism in Grid Environment

DENG Yong ZHANG Lin WANG Ru-chuan ZHANG Mei
(College of Computer, Nanjing University of Posts and Telecommunications, Nanjing 210003, China)

Abstract In grid computing system, the trust relation between resource vendor and resource user is the premise of safe communication, for the traits on distribution and dynamic, the trust between each other in advance is impossible, however, it can be resolved by importing trust mechanism to RBAC in Grid community, the trust degree of each Grid entity can be counted based on the feedback from other entities, and then their roles are changed based on their trust degrees. Using this policy, the dynamic trait can be realized in Grid and the cheat behavior of Grid entity also can be avoided.

Keywords Grid, Trust mechanism, Role-based access control

1 引言

网格计算通过利用众多服务器和PC机的合力来作为一个大型系统,运行各种应用和服务,多年来一直在学术和研究机构中被用来运行计算密集型应用。网格提供的良好的资源利用率和计算能力已引起了各国企业界的注意,但由于网格计算系统自身的特点,使得安全问题成为其得到普遍使用的一大障碍。随着网格已经从实验和科研阶段进入商业领域,理解并解决网格计算的安全问题已经成为当务之急。

访问控制机制是任何一个安全系统必须考虑的问题,主要通过访问授权约束实现组织安全政策,使获得权限的用户在满足所有约束前提下执行相应的操作。对于网格计算系统这样一个分布式的并且动态变化的系统,提供一种完善的访问机制,是保护资源提供者和资源消费者权利的重要措施。

基于角色的访问控制机制(RBAC)是目前最流行的访问控制方法,已经广泛应用于企业、组织间协作授权、医疗信息系统等领域中。但传统的任何一种访问控制技术,包括RBAC都是静态的,而网格计算系统最主要的特征之一就是其动态性。若将RBAC直接应用于网格计算环境,只会导致整个访问控制机制的僵化。因此,迫切需要引入新的机制来解决网格访问控制的动态性问题,并利用实体的信任度来动态改变实体的角色。为解决这一问题,提供了一种新的思路。本文的重点是将信任机制融入社区授权服务中的RBAC,提出了基于信任度的动态角色访问控制的基本思想及其安全架构,并给出其具体实现的流程和详细说明了基于信任度的动态角色访问控制中实体的信任度评估包含的两大算法,最后给出了其有效性分析。

2 基于信任度的动态角色访问控制的思想和架构

2.1 基于角色的访问控制

基于角色的访问控制(RBAC, Role-Based Access Control)是近年来在信息安全领域访问控制方面的研究热点和重点。它和DAC,MAC称为3大访问控制策略。

随着时间的推移,越来越多的商业用户意识到DAC和

到稿日期:2009-02-13 返修日期:2009-04-20 本文受国家自然科学基金(60573141,60773041),江苏省自然科学基金(BK2008451),国家高科技863项目(2007AA01Z404,2007AA01Z478),现代通信国家重点实验室基金(9140C1105040805),江苏省计算机信息处理技术重点实验室基金(kjs06006)和江苏高校科技创新计划项目(CX08B-085Z,CX08B-086Z)资助。

邓 勇(1975-),男,博士研究生,主要研究方向为计算机网络和网格技术、信息安全和移动代理技术等,E-mail:wangrc@njupt.edu.cn;张 琳(1980-),女,博士,主要研究方向为网格技术、信息安全等;王汝传(1943-),男,教授,博士生导师,主要研究方向为计算机软件、计算机网络、信息安全、移动代理和虚拟现实技术等;张 梅(1983-),女,硕士研究生,主要研究方向为计算机软件、网格安全。

MAC在商业领域中并不十分有效。而同时期Clark-Wilson通过大量商业安全的实际系统形式化出与DAC和MAC完全不同的一套访问控制模型，并第一次提出了职责分离(SoD,Separation of Duty)[1]的概念。

RBAC研究的最初学术论文是1994年美国NIST研究人员David Ferraiolo和Richard Kuhn发表的"Role-Based Access Control"。国内最早的相关学术论文是1994年华中理工大学马建平的硕士学位论文《一种无干扰的访问控制模型》。在RBAC研究历程中，1996年美国George Mansion Univ. Ravi S. Sandhu教授在"IEEE Computer"上发表了一篇学术论文"Role-Based Access Control"，该文中Sandhu教授正式提出了RBAC96[2]模型家族，它为进一步深入研究RBAC奠定了基础。此后国内外研究者在RBAC96模型家族的基础上提出了许多扩展模型。

RBAC模型的基本思想是将访问许可权分配给一定的角色，用户通过饰演不同的角色获得角色所拥有的访问许可权[3,4]。这是因为在很多实际应用中，用户并不是可以访问的客体信息资源的所有者(这些信息属于企业或公司)，这样，访问控制应该基于员工的职务，即访问控制是由各个用户在部门中所担任的角色来确定的。例如，公司根据需要可能创建一个称为销售经理的角色，当雇佣销售经理时，就给他们分派销售经理角色，而他们可以立即具有这份工作所需要的全部权限。他们离开销售经理的职位后，就会从销售经理角色中删除，并且不再具有销售经理的访问权限。

RBAC从控制主体的角度出发，根据管理中相对稳定的职权和责任来划分角色，将访问权限与角色相联系，这点与传统的MAC和DAC将权限直接授予用户的方式不同；通过给用户分配合适的角色，让用户与访问权限相联系。角色成为访问控制中访问主体和受控对象之间的一座桥梁。RBAC用角色表示访问主体具有的职权和责任，灵活地表达和实现了企业的安全策略，使系统权限管理在企业的组织视图这个较高的抽象集上进行，从而简化了权限设置的管理。从这个角度看，RBAC很好地解决了企业管理信息系统中用户数量多、变动频繁的问题。研究表明，角色/权限之间的变化比角色/用户关系之间的变化相对要慢得多，并且委派用户到角色不需要很多技术，可以由行政管理人员来执行。而配置权限到角色的工作比较复杂，需要一定的技术，可以由专门的技术人员来承担。但是不给他们委派用户的权限，这与现实中的情况正好一致。

2.2 基于信任度的动态角色访问控制的流程

与网格中传统的社区授权服务不同，基于信任度的动态角色访问控制方法的特点主要体现在增加了信任度管理单元和仲裁模块[5-7]。

信任度管理单元(TMU,Trust-level Management Unit)包括信任度管理服务器(TMS,Trust-level Management Sever)和信任度管理数据库(TMD,Trust-level Management Database)两个部分。

信任度管理服务器是一个通过信任度评估算法计算实体信任度的控制部分。根据实体的表现改变实体的信任度，以此来保证网格的安全性。

信任度管理数据库用来存储相互交互的实体之间的所有评价和网格社区中实体的当前信任度。每当网格社区中一次作业结束后，根据信任度管理服务器对实体的信任度计算，信任度管理数据库中存储的实体信任度会及时更新，体现了网格的动态性。

为了防止恶意评价，引入了评价准确度的概念。评价准确度是衡量一个实体对其他实体的评价的诚实度。仲裁模块是实现这一功能的功能模块，它将该实体对其他实体的评价准确度和该实体自身的可信任度相关联，准确度太低的评价会降低该实体自身的信任度，从而防止了恶意评价，确保了评价的公正性。

网格实体的信任度以及评价准确度的更新周期均为一个网格作业，即它们的更新是在每次网格作业结束后进行的。

一次动态角色访问控制流程的分解步骤如下。

步骤1　用户实体首先得到一个标准的用户证书，然后向CAS服务器提交证书和声明所需的资源，请求授权；

步骤2　CAS服务器访问CAS数据库，确定用户实体的角色，以判断用户有无权限访问资源；

步骤3　若网格用户有权限访问资源，则CAS服务器用其私钥签署一个授权策略声明返回给用户；

步骤4　用户将声明和资源请求提交给要使用的资源服务器；

步骤5　通过本地策略，资源服务器判断是否提供资源给用户；

步骤6　若资源服务器响应用户，则本次网格作业运行，作业结束后，产生过交互的网格实体给对方做相应的评价；

步骤7　所有的评价都被提交到信任度管理数据库；

步骤8　信任度管理服务器提取信任度管理数据库中的数据，准备对评价客体 n 进行信任度计算；

步骤9　信任度管理服务器判断评价客体 n 是用户或是资源；

步骤10　如果评价客体 n 是用户，查询得到评价客体 n 的全部〈资源，用户〉链路；如果评价客体 n 是资源，查询得到评价客体 n 的全部〈资源，资源〉链路和其唯一的〈用户，资源〉链路；

步骤11　查询所有对评价客体 n 作过评价的实体的评价准确度；

步骤12　计算得到实体 n 的最终信任度，即本次网格作业结束后实体 n 的最新的信任度；

步骤13　信任度管理服务器将数据传回给信任度管理数据库，并更新其中的实体信任度纪录；

步骤14　更新信任度管理数据库中所有做过评价的实体的评价准确度；

步骤15　实体的信任度被提交到CAS数据库；

步骤16　CAS服务器根据实体信任度确定其角色。

3 基于信任度的动态角色访问控制的具体实现

3.1 基于信任度的动态角色访问控制的信任度评估模型

网格社区的信任度评估模型如图1所示。模型使用链路来表示实体的评价行为，即若实体间进行了一次评价，就可以视作在这两个实体之间建立了一条链路。链路是有向的，其方向表示评价的方向，即从评价主体指向评价客体。链路的数学表达形式是〈A,B〉，其中前项 A 是评价主体，后项 B 是评价客体。根据链路的数学表达式可以看出两个实体之间的

链路最多存在两条，即 A 评价 B 和 B 对 A 的评价。这样实体评价行为便映射为链路形成的网格社区信任度评估模型。

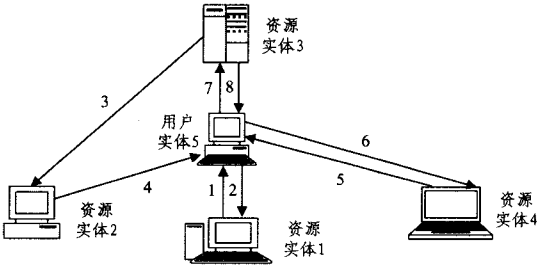

图 1　网格社区的信任度评估模型

以图 1 为例，如果实体 1 要对实体 5 进行信任度评价，那么实体 1 为评价主体，实体 5 为评价客体。假设实体 5 为用户，实体 1、实体 2、实体 3、实体 4 为资源，那么链路 1,4,5,8 属于〈资源，用户〉链路，链路 2,6,7 属于〈用户，资源〉链路，链路 3 属于〈资源，资源〉链路。

链路的权值是实体对某次交互对端实体的行为质量的评价。为简化模型，权值取值为区间[−1,1]之内的几个离散值，如表 1 所列。

表 1　链路权值取值

链路权值	对应评价
−1.00	行为质量很差
−0.33	行为质量较差
0.33	行为质量较好
1.00	行为质量很好

信任度评估模型中的实体信任度等级所对应的信任度区间如表 2 所列。

表 2　信任度等级与信任度区间对照表

信任度等级	区间	描述
较差	[−1,−0.33]	信任度较差，建议不可信
普通	(−0.33,0.33)	信任度一般，可信任
较好	[0.33,1]	信任度较好，值得信任

为简化模型，在本网格环境中角色根据信任度等级划分为 3 种：

角色 1：信任度等级“较好”，对应信任度区间为[0.33,1]，能够提交作业和资源。

角色 2：信任度等级“普通”，对应信任度区间为(−0.33,0.33)，能够提交资源，但不能提交作业。

角色 3：信任度等级“较差”，对应信任度区间为[−1,−0.33]，既不能提交作业也不能提交资源，只能浏览。

当一个实体新注册到网格社区时，为使其在一开始就能作为用户提交作业，实体的信任度被初始化为 0.33，作为“较好”的信任度等级。它的角色为角色 1，既能提交资源，也能提交作业。如果其在使用其他资源的过程中表现良好或者其提交的资源为其他用户提供了良好的服务，得到了较高的评价，那么它的信任度会较高，从而维持角色 1 的状态；反之，如果得到了较差的评价，那么它有可能被降级为角色 2 或者角色 3，不再具有提交作业甚至提交资源的权利。这种信任机制基本保证了每次网格实体行为的可靠性，因为参与网格作业的实体的信任度在每次作业结束后都会根据其表现被更新，如果想获得并一直保持角色 1，那么它只能在网格中维持一个良好的表现。

一旦实体被降级为角色 3，那么它只能浏览，连资源都被禁止提交，这样它对自己的信任度提高就变得无能为力了，只能一直维持角色 3 的状态。为避免这种情况的发生，系统中存在相应的恢复机制。当一个实体的信任度长时间(例如一周)处于角色 3 的范围内，需要人为地为其做一个恢复，通常由 CAS 服务器恢复其初始值；同时，服务器记录该实体已经被恢复的次数，当恢复次数达到一定数量时，可认为该实体为恶意实体，从此不再对其进行恢复。

当然，上述模型中的角色划分相对现实网格环境是比较简单的，在此只是借助这种简单的角色划分来介绍基于信任的动态角色访问控制。在现实网格系统中，各种角色应该根据不同的社区类型及其需要来划分。

3.2　基于信任度的动态角色访问控制的信任度评估算法

信任度评估模型中用到两个算法，分别是信任度管理服务器中使用的实体信任度算法和仲裁模块中使用的评价准确度算法。

(1)实体信任度算法

由于实体被分为用户实体和资源实体，实体信任度算法相应地也分为两种形式。信任度管理服务器首先判断评价客体 n 是用户实体还是资源实体。

如果评价客体 n 是用户，信任度管理服务器向信任度管理数据库查询得到评价客体 n 的全部〈资源，用户〉链路，其权值记为 $l(i,u,n)$，其中 i 为链路编号，u 为评价用户的资源实体。所有评价用户的资源实体构成评价主体集合，记 R，n 为作为评价客体的用户，链路集合记为 D，链路数量表示为 $S(D)$。

信任度管理服务器向信任度管理数据库查询得到所有评价主体的评价准确度，评价主体 u 的评价准确度记为 $A(u)$。

当评价客体 n 是用户时，实体信任度算法为：

$$T(n)=\frac{\sum_{i\in D\wedge u\in R} l(i,u,n)*A(u)}{S(D)} \tag{1}$$

如果评价客体 n 是资源，信任度管理服务器向信任度管理数据库查询得到评价客体 n 的全部〈资源，资源〉链路，其权值记为 $l(i,u,n)$，其中 i 为链路编号，u 为作为评价主体的资源实体，所有作为评价主体的资源实体构成的集合记为 R，n 为作为评价客体的资源实体，〈资源，资源〉链路集合记为 D，链路数量表示为 $S(D)$，评价主体 u 的评价准确度记为 $A(u)$。并且评价客体 n 最多存在一条〈用户，资源〉链路(假设模型中用户的唯一性)，该〈用户，资源〉链路的权值记为 m，用户的评价准确度记为 f。

当评价客体 n 是资源时，实体信任度算法为：

$$T(n)=\alpha*\frac{\sum_{i\in D\wedge u\in R} l(i,u,n)*A(u)}{S(D)}+\beta*m*f \tag{2}$$

式中，α 和 β 是权重因子，算法使用它们来调节用户和其他资源在资源实体信任度计算中的比重，$0<\alpha,\beta<1$，且 $\alpha+\beta=1$。

一般来说，鉴于用户评价的重要性，用户的评价应该占有较大的权重，可以将用户的权重 β 置为 0.8，其他资源的权重 α 置为 0.2。但如果不希望对此进行区别，只需要令 $\alpha=\beta=0.5$ 即可。

(2)评价准确度算法

评价准确度是衡量一个实体对其他实体的评价的诚实度。在本信任度评估模型中引入评价准确度的目的，是建立一个仲裁模块。

这个仲裁模块的作用是降低实体欺骗行为的发生概率，确保评价的公正性。如果一个实体经常做出和其他实体大相径庭的评价，那么它的可信任度就会大大降低，从而失去网格中其他实体的信任。

信任度管理数据库中维护着一张实体评价准确度表，评价准确度范围为[0,1]。所有实体的评价准确度初始值设为1，即假设每个实体的初始评价都是可信的，以后根据实体的行为不断更新其评价准确度。

当一次网格作业结束后，信任度管理服务器计算得出所有参与网格合作的实体信任度，根据实体的最终信任度来更新所有作过评价的实体的评价准确度。

假设评价主体是 m，评价客体是 n，则需要评价主体 m 的评价准确度。

仲裁模块向信任度管理数据库查询得到全部〈m,n〉链路，链路的权值记为 $l(i,m,n)$，其中 i 为链路编号，m 为评价主体，n 为被 m 评价过的评价客体，所有评价客体 n 构成评价客体集合，记为 R。链路集合记为 D，链路数量表示为 $S(D)$。

仲裁模块中使用的评价准确度为：

$$A_n=1-\frac{\sum_{i\in D\wedge n\in R}|l(i,m,n)-T(n)|}{\frac{T_{best}-T_{worst}}{S(D)}} \tag{3}$$

式中，$T(n)$是评价客体 n 的真实信任度，是由信任度管理服务器根据信任度算法计算得出的；T_{best} 和 T_{worst} 分别为最高信任度和最低信任度，$T_{best}=1$，$T_{worst}=-1$。

3.3 基于信任度的动态角色访问控制在网格案例中的分析

下面以一个案例来说明信任度评估算法的具体实现。仍以图1所示的网格社区的信任度评估模型为例，假设实体5作为用户实体提交一次网格作业结束后，实体间相互评价产生了8条链路，这些链路及其权值保存在信任度管理数据库中，链路的权值即相互之间的评价值如表3所列。

表3 链路的权值

链路编号	链路权值
1	0.33
2	1
3	−0.33
4	−0.33
5	−0.33
6	0.33
7	−1
8	−1

假设表4所列为信任度管理数据库中维护的实体评价准确度表。

表4 实体评价准确度表

实体编号	评价准确度
1	1
2	0.8
3	0
4	0.7
5	0.9

信任度管理服务器提取信任度管理数据库中表3和表4的数据，应用实体信任度算法式(1)，可以计算出用户实体5的信任度为0.01375。根据信任度等级与信任度区间对照表可以判断出实体5的信任度等级为“普通”，则角色会动态地从角色1能提交作业改变成角色2只能提交资源。

应用实体信任度算法式(2)(令 $\alpha=0.2$，$\beta=0.8$)，可以计算出各个资源实体的信任度。

接着，信任度管理服务器将数据传回给信任度管理数据库，并更新其中的实体信任度纪录。本例中所有实体的信任度及角色对照表如表5所列。

表5 实体信任度及角色对照表

实体编号	信任度	角色
1	0.72	1
2	0	2
3	−0.72	3
4	0.2376	2
5	0.01375	2

下一步，根据实体的最终信任度，即表5中更新过的信任度数据来计算所有做过评价的实体的评价准确度。应用评价准确度算法式(3)可以计算出各个实体的评价准确度，并对表4做相应的更新。表6为更新过的实体评价准确度表。

表6 更新后的实体评价准确度表

实体编号	原始评价准确度	更新后评价准确度
1	1	0.841875
2	0.8	0.828125
3	0	0.664063
4	0.7	0.828125
5	0.9	0.891267

3.4 网格环境下应用动态角色访问控制的有效性分析

基于信任的动态角色访问控制是一种针对网格社区环境下的高效便捷的访问控制方法，主要用于解决网格社区中对客户端进行访问控制的问题，可以避免实体欺骗行为和实现动态性，可以有效地达到网格社区中对客户端的访问控制的目的。下面给出其有效性的具体说明。

动态性：根据信任度评估算法算出实体的信任度，CAS服务器能依据实体信任度动态实时地改变网格实体的角色。

可信任性：基于信任的动态角色访问控制使用的信任模型是可靠的，可以防止实体欺骗行为的发生。在本模型中，只有来自信任度高的实体的正面评价才能提高对端实体的信任度，信任度一般的实体对端实体的信任度几乎没有影响。

合理性：当一个实体新注册到网格社区时，为使其在一开始就能作为用户提交作业，实体的初始信任度设为0.33，它的角色为角色1，既能提交资源，也能提交作业。并且，为避免实体的信任度长时间(例如一周)处在角色3的范围内，系统中存在恢复机制，可以人为地为其做恢复，这样使系统的行为更加合理。

准确性：本方法中不仅考虑到实体欺骗行为的可能性，而且加入了惩罚欺骗行为的仲裁模块，增加了系统的准确度。在引入反馈信息时，不但将正面评价和负面评价均引入信任模型，而且考虑到反馈信息提供者的可信任度，使得反馈信息更加准确。

结束语 网格计算的安全问题是网格计算的关键技术问题之一，研究网格计算的安全策略目前还处于初级阶段，其研究的深度和广度还亟需加强。本文在重点研究基于RBAC的网格社区授权服务的基础上，针对网格计算系统的动态性的特点，将传统安全研究中尤其是安全授权机制研究中隐含的信任概念抽取出来融入RBAC，提出了基于信任度的动态

(下转第107页)

够适用于大规模的网络，其可扩展性较 CBCB 算法明显增强。

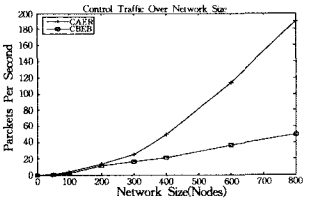

图 10　可扩展性对比

结束语　在基于内容的发布/订阅研究领域中，现有的路由算法缺少对订阅动态变化的支持。针对以上缺陷提出了基于内容的自适应事件路由算法 CAER。该算法通过在基于内容的路由表中将订阅与订阅源结点相绑定的方式来支持订阅的更新，提高事件的分发效率。实验证明该算法既减少了假阳性(即传给结点其并不感兴趣的事件数)的比率，又提高了事件分发的准确性，而且相对于已有的路由算法显著减少了控制信息的通讯开销，具有良好的可扩展性。

参 考 文 献

[1] Eugster P T, Felber P A, Guerraoui R, et al. The Many Faces of Publish/Subscribe[J]. ACM Computing Surveys, 2003, 35(2): 114-131

[2] Fiege L, Muhl G, Buchmann A. An Architectural Framework for Electronic Commerce Applications[C]// Annual Conference of the German Computer Society. New York: IEEE, 2001

[3] Fiege L, Muhl G. Rebeca: Event-Based Electronic Commerce Architecture[EB/OL]. http://www.gkec.informatik.tu-darmstadt.de/rebeca

[4] Perry T S. In Search of the Future of Air Traffic Control[J]. IEEE Spectrum, 1997, 34(8): 18-35

[5] Bornhovd C, Cilia M, Liebig C, et al. An infrastructure for meta-auctions[C]// Second International Workshop on Advance Issues of E-Commerce and Web-based Information Systems (WECWIS'00). New York: IEEE, 2000: 21-30

[6] Casanova H. Distributed Computing Research Issues in Grid Computing[J]. ACM SIGACT News, 2002, 33(3)

[7] Segall B, Arnold D. Elvin Has Left the Building: A Publish/Subscribe Notification Service with Quenching[C]// Proceedings of the Australian UNIX and Open Systems User Group Conference (AUUG'97). 1997

[8] Gryphon. Http://www.research.ibm.com/gryphon/

[9] SIENA. Http://www.cs.colorado.edu/users/carzanig/siena/

[10] Cugola G, Nitto E D, Fuggetta A. The JEDI event-based infrastructure and its application to the development of the OPSS WFMS[J]. IEEE Trans. on Software Engineering, 2001, 27(9): 827-850

[11] Banavar G, Chandra T, Mukherjee B, et al. An Efficient Multicast Protocol for Content-based Publish-Subscribe Systems[C]// Proceedings of IEEE International Conference on Distributed Computing Systems'99. New York: IEEE, 1999: 262-272

[12] Ganguly S, Bhatnagar S, Saxena A, et al. A Fast Content-based Data Distribution Infrastructure[C]// Proceedings of IEEE INFOCOM'06. New York: IEEE, 2006: 1-13

[13] Carzaniga A, Rutherford M J, Wolf A L. A routing scheme for content-based networking[C]// Proceedings of IEEE INFOCOM'04. New York: IEEE, 2004

[14] Castelli S, Costa P, Picco G P. HyperCBR: Large-scale Content-based Routing in a Multidimensional Space[C]// Proceedings of IEEE INFOCOM'08. Phoenix, AZ, USA: IEEE, 2008

[15] PeerSim. http://lists.sourceforge.net/lists/listinfo/peersim

(上接第 54 页)

角色访问控制机制，在解决网格社区中访问控制动态性问题的同时也有效地避免了网格实体欺骗行为的发生。下一步的工作是在网格社区访问控制的基础上提出域间访问控制的解决方案。

参 考 文 献

[1] Clark D D, Wilson D R. A Comparison of Commercial and Military Computer Security Policies[C]// IEEE Symposium on Security and Privacy. Oakland, April 1987: 184-194

[2] Sandhu R S, Coyne E J, Feinstein H L, et al. Role-based access control models[J]. Computer, 1996, 29(2): 38-47

[3] Hildmann T, Barholdt J. Managing Trust between Collaborating Companies Using Outsourced Role Based Access Control[C]// Proceedings of the Fourth ACM Workshop on Role-based Access Control: 105-111

[4] 徐京京，代红雷，查礼，等. 基于社区的服务网格多粒度授权与访问控制研究[J]. 计算机应用研究，2006，7：199-203

[5] 王莉苹，杨寿保. 网格环境中的一种信任模型[J]. 计算机工程与应用，2004，40(23)：50-53

[6] 高承实，张栋，田磊. 网格环境下基于实体行为的动态信任评估模型[J]. 微计算机信息(管控一体化)，2006，22(8-3)：199-201

[7] 郑彦，王汝传，张奇，等. 复合模式的网格系统信任授权模型[J]. 计算机工程与设计，2006，27(13)：2311-2313