RBAC授权策略在网格环境中的优化

彭 舰，谢 川，廖朝辉

(四川大学计算机学院 成都 610065)

【摘要】分析了网格安全基础设施授权过程和存在的问题，根据网格动态性、自主性与多重管理特点提出了基于角色、能够解决大规模虚拟组织授权问题的方案，实现了虚拟组织用户有效管理与细粒度授权，完善了本地资源授权策略，为虚拟组织的安全运转提供了保障。根据网格体系结构特点，新模型改进当前存在的RBAC授权机制，从整体和局部两个方面完善了系统，为降低网格系统成本、快捷实施、增强安全性提供了一条新的解决方案。

关 键 词 授权策略; 身份管理; 交叉角色; 基于角色的访问控制; 虚拟组织

中图分类号 TP311.52 **文献标识码** A

Research on the Optimization of RBAC Authentication Policy in Grid Environment

PENG Jian, XIE Chuan, and LIAO Chao-hui

(School of Computer Science, Sichuan University Chengdu 610065)

Abstract A new role base access control (RBAC) based authentication model which can resolve virtue organization (VO) authentication problem in large scale is proposed. The new model provides security to grid system in two aspects: firstly it makes user management and authentication more precisely, secondly, it reinforces authentication strategy at local level. According to the characters of VO in the Grid, we need a new solution to relieve burden of security, hence the optimized authentication architecture is built to achieve the better performance as well as reduction of total cost of ownership.

Key words authentication strategy; identity management; intercross role; role-based access control; virtue organization

网格代表了一种先进的技术和基础设施，它是一个集成的计算与资源环境，具有强大的求解问题的能力[1]。虚拟组织(virtue organization，VO)是网格的一个重要概念，它为资源共享的规则提供组织形式，具有共享与分布、动态性与多样性、自治性与管理的多重性[2]等特点。从管理角度看，VO是一种动态的网格协作环境，它包含了许多用户以及由协作伙伴提供的资源[3]。VO定义了资源的共享规则，即资源提供者(resource provider，RP)必须明确和谨慎地定义共享的资源、共享的用户和共享的资源的条件。

本文分析当前网格安全基础设施授权过程中存在的问题，根据网格特征提出了一种新型的基于角色的授权问题的方案，将权限的集中式管理变为分布式管理，从而增强本地资源的自主性和网格系统的敏捷性，为网格的安全、高效率运转提供保障。

1 当前网格授权模式分析

1.1 基于文件的授权

目前网格安全中使用较多的解决方案是美国网格研究项目Globus提出的网格安全基础设施(grid security infrastructure，GSI)，GSI的认证授权主要是基于PKI的公钥认证机制-X.509证书的相关机制[4]。

GSI授权是通过对一个文件的操作实现的，该文件提供全局用户到本地账号的映射关系，通过赋予VO用户对应本地账号的权限实现对资源的操作。

GSI授权是一种静态授权机制，要求每个访问资源的VO用户都要在本地资源服务器上拥有一个自己的账号，根据用户需求为每个账号赋予相应的权限。每个RP都需要维护一个庞大笨拙的全局/本地映

收稿日期：2007 – 07 – 29；修回日期：2007 – 12 – 23
基金项目：四川省科技支撑项目(07GG006-040)
作者简介：彭 舰(1970 –)，男，博士，副教授，主要从事分布式计算、高性能计算等方面的研究.

射表，因此难以扩展到拥有大量资源和用户的VO环境中，并且不能体现网格动态、自主与多重管理性的特征，缺乏基于全局策略且具有良好扩展性的访问控制机制。

1.2　基于角色的授权

虚拟组织中最关键的问题就是安全，它包括鉴别用户以及其行为，社区授权服务(community authorization service，CAS)就是当前一种著名的解决方案[5]。基于角色的访问控制(role base access control，RBAC)模型的基本思想是：通过分配和取消角色来完成用户权限的授予和取消，授权者为用户划分不同的角色，资源访问许可被封装在角色中，用户通过赋予的角色间接地访问系统资源；授权者根据需要定义各种角色，并设置合适的访问权限。整个访问控制过程分成两个部分，即用户与角色关联、角色再与访问权限关联，从而实现用户与访问权限的逻辑分离[3]。

在CAS模型中，当一个VO用户访问RP提供的资源时，由CAS提供授权服务。CAS授权服务的本质是管理用户的角色和权限，由它来决定用户能做什么、不能做什么[4]。CAS授权模型如图1所示。

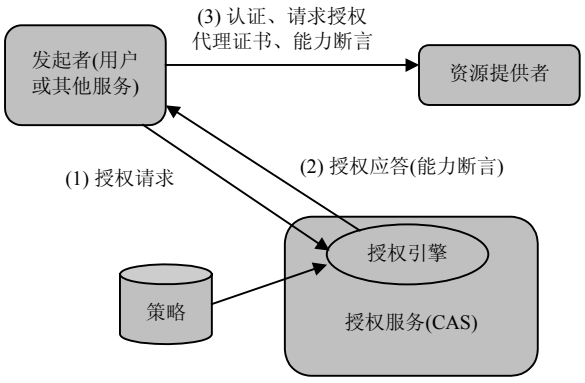

图1　CAS授权模型

CAS虽然解决了在虚拟组织中对资源和数据访问控制的灵活性、可扩展性等问题，但是，也存在着一些弊病。

(1) CAS用静态定义的权限来工作，其能力断言声明直接包含了权限，并不需要由资源提供者来解释权限，资源信息反馈机制没有得到反映[6]，不利于某些消费性资源(如磁盘容量)的合理分配。

(2) VO拥有庞大的用户群，CAS既要管理角色又要管理权限，而RP仅仅执行CAS的决策，工作量主要集中在CAS上，这种集中式管理导致网格系统的权限管理增加了不确定性。

2　RBAC的改进与优化模型

由于虚拟组织共享控制复杂性是由参与协作各方共同引起的[7]，本文提出一种改进的RBAC模型，使其适应网格系统的需要。网格构建最具挑战性的是资源管理，资源管理策略有基于集中式的、分布式的和层次性的，文献[8]提供了不同管理策略的比较。根据VO资源管理的自主性与多重性，本地授权应基于VO与RP之间制定的共享规则。本地授权的依据是用户证书以及VO提供的身份信息。本文引入改进的基于角色的访问控制授权模型，并对VO认证授权过程做了改进。

2.1　分离角色管理与权限管理

在网格资源共享过程中，授权扮演了十分重要的角色[9]。从网格授权的角度看，网格授权是基于RP和VO之间的契约，因此RP与VO在资源管理上扮演了不同的角色，在VO中明确区分二者的职责是十分必要的[10]。为了明晰这种管理上的双重性，本文将授权信息分为两类。

(1) 用户身份信息：描述用户的身份，如用户属于哪些组、扮演的角色等。

(2) 资源授权策略：根据用户身份，决定是否授予以及授予什么本地资源的权限。

本文认为用户身份信息应该由VO管理的服务器保存，资源授权策略则保存在与资源相联系的RP的机器中。改进的授权过程如图2所示。

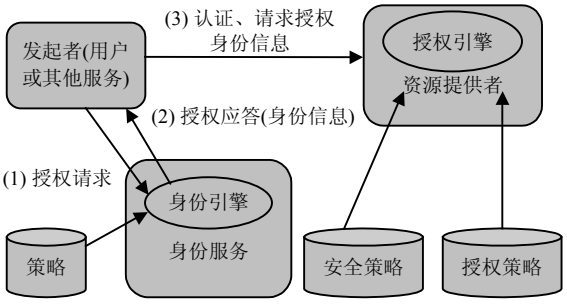

图2　改进的授权过程

当RP将资源共享给VO时，同时也将有权访问这个资源的角色代理给VO，如果用户需要访问某个资源，那么他必须被授予访问该资源的代理角色，还必须根据不同的需求被授予受限的代理角色。

当将具体授权职责从VO授权服务中分离之后，该服务承担的主要职责是管理用户身份服务。VO授权服务的身份声明包含角色或组成员的列表，用户将该身份声明发送给RP，由RP根据本地授权策略来授予用户权限[11]。

2.2 权限管理

虽然本文提供了一种新的角色管理模式，但仍没有从根本上解决角色数量随着使用大量增加的问题以及安全性等问题，所以把用户具体授权工作交给RP，RP根据本地授权策略实现对VO用户的授权，如图3所示。

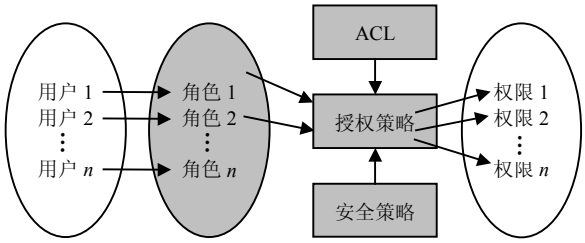

图3 权限管理

本地授权策略中包含对(以ACL等形式的)权限的管理与安全策略。改进的RBAC模型与RBAC基本授权模型的最大区别在于在角色与权限中间增加了授权策略。该环节的作用就是对用户进行准确的细粒度授权，优点是不需增加角色，利用当前已存在的角色就能对用户准确授权，保证了系统的安全结构不随权限的逻辑交叉而变化，并增强了本地资源的自主控制能力。授权策略工作原理是通过用户的角色集合制定用户的权限集合。需要注意的是，用户角色集合中可能存在冗余或矛盾的权限分配，授权策略需要对矛盾和冗余进行处理[12]。

2.3 角色和权限的表示

资源的访问控制是由主体(用户)、客体(资源)和主体对客体的操作组成的，表示为{S, OB, OP}，其中S表示主体；OB表示客体；集合OP表示主体对客体的操作。角色封装了对资源(RE)的操作，即{RE, OP}。权限P是从集合{RE, OP}到集合{ true, false}的一个映射关系，表示为RE×OP→{true, false}。权限P将{RE, OP}中的一个点映射到集合{ true, false}上，对某个资源能(映射为true)或者不能(映射为false)执行某种操作，就是访问控制中的一条权限限制，所有的权限限制便构成了权限集合，表示为P={(RE_i,OP_j,B_k)|$RE_i \in RE$, $OP_j \in OP$, $B_k \in B$={true, false}}，而角色即该权限集合的一个子集。

对RP管理的资源，RP将每个资源针对的角色进行授权。本文采用字符串来表示某个资源对某个角色的权限分配情况，字符串的数据结构为Role|OperationType | Boolean，其含义是授予角色|操作类型|能否操作，操作之间根据不同的需求可以赋予蕴含关系。定义关系C是从集合OP到集合OP的二元关系。下面证明蕴含关系C是集合OP上的偏序关系。

因为 $P_x \in OP$，$(x,x) \in C$，所以关系C是自反的。因为$P_{x,y} \in OP$，若$(x,y) \in C$，且$x \neq y$，则$(y,x) | C$，所以关系C是反对称的。因为$P_{x,y,z} \in OP$，若$(x,y) \in C$, $(y,z) \in C$，则$(x,z) \in C$，所以关系C是传递的。

关系C在集合OP上具有自反性、反对称性和传递性，得证关系C是偏序关系。

角色的继承关系类似操作的蕴含关系，定义为P(RE_i,OP_j,B_k)$\in R_1$，其中$RE_i \in$ Re；$OP_j \in OP$；$B_k \in B$；均有(RE_i,OP_j,B_k)$\in R_2$，即角色R_2继承自角色R_1。继承关系同样是偏序关系，角色继承关系和操作的蕴含关系是角色冗余处理的基础。

2.4 角色矛盾和冗余处理

角色的矛盾与冗余处理以角色的继承关系和操作的蕴含关系两个偏序关系为基础。本文将偏序关系用<以及>符号表示，如RO_1>RO_2表示RO_1继承于RO_2；OP_1> OP_2表示OP_1蕴含OP_2；而继承角色比被继承角色具有更高的权限；同时定义角色的Boolean字段取值false<true，用=表示操作、角色和Boolean字段取值的相等关系。角色的矛盾与冗余处理关系如表1所示。表中序号为3、4的两栏主要用于表示矛盾与冗余处理。

表1 角色矛盾以及冗余处理

序号	条件	结论
1	RO_1>= RO_2，OP_1>= OP_2	B_1和B_2关系任意
2	RO_1< RO_2，OP_1< OP_2	B_1和B_2关系任意
3	RO_1>= RO_2，OP_1< OP_2	B_1>= B_2
4	RO_1< RO_2，OP_1>= OP_2	B_1<= B_2

3 验证与应用

本文模型已经被应用于SCU-GRID系统，如图4所示。运行环境为带有六个节点的Linux集群，节点上安装并配置了Globus4.0。该系统实现了角色和权限的分离管理。每个本地资源只需要定义自身需要的角色-权限列表，并与中央角色池同步，通过本地授权引擎实现交叉角色的授权。当VO用户使用资源时，首先向中央身份服务器请求自己的角色，之后再将角色发送到RP的本地授权服务器，根据RP定义好的权限和安全策略，授予用户对应权限。VO管理员负责维护中央身份-角色数据库以及角色库，RP负责维护自身的角色-权限数据库与安全策略。

本文构造的VO环境下的改进优化的RBAC模型与CAS的集中式模型相比有很多优点：(1) 改进的RBAC模型是一种动态构造模型，结构灵活，扩展性强；(2) 某一节点权限分配不会影响其他节点，可

以更加精确地为某一资源进行授权；(3) 改进的模型使中央服务器所承担的工作量减少，中央服务器的工作是进行角色定义与分配，更加有利于管理员进行维护。

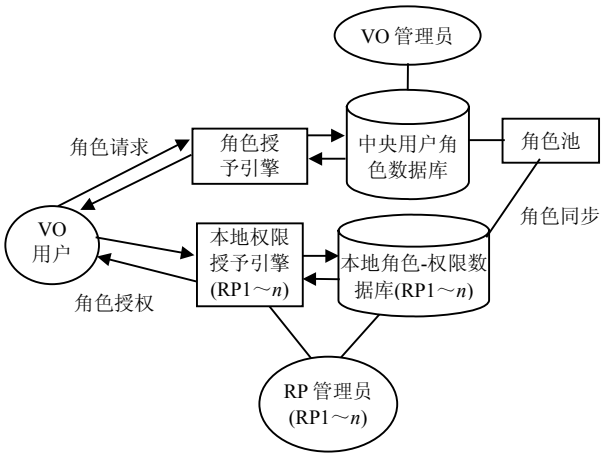

图4　SCU-Grid结构图

4　结 束 语

本文提出了基于RBAC改进的网格虚拟组织授权模型，它提高虚拟组织用户管理管理效率，实现了用户细粒度授权，并加强了本地资源的管理，为虚拟组织的安全运转提供了保障。该模型已经成功应用于SCU-GRID系统。在可以预见的未来，网格应用将更具有动态性，因此需要的授权方案也将更具有动态特性。下一步工作将从动态性着手，进一步完善网格授权策略。

参 考 文 献

[1] JOSHY J, CRAIG F. Grid computing[M]. 北京: 清华大学出版社, 2005.

[2] 李志英, 黄　强, 楼新远, 等. RBAC模型研究、改进与实现[J]. 计算机应用, 2006, 26(12): 50.

[3] ALFIERI R, CECCHINI R, CIASCHINI V. CAS, an authorization system for virtual organizations[C]//Procee -ding in CAS Conference. Berlin: Springer, 2005.

[4] NASSER B, BENZEKRI A, LABORDE R. Access control model for grid virtual organizations[C]//ICEIS Conference Proceeding [S.l.]: INSTICC, 2005.

[5] GLOBUS. GLOBUS toolkit version 4 CAS (community authorization services)[EB/OL]. [2007-05-13]. http://www. 1to2.us/GT4-CAS(Community-Authorization-Services)-a17 2519. htm.

[6] 王　杨, 林　涛, 王汝传. 计算网格中访问控制策略研究与应用[J]. 计算机技术与发展, 2006, 16 (8): 77.

[7] CANNON S, CHAN S, OLSON D, et al. Using CAS to manage role based VO sub-groups[EB/OL]. [2007-10-09] http:// www.globus.org/alliance/publications/papers/CAS-group- CHEP03. pdf.

[8] KRAUTER K, BUYYA R, MAHESWARAN M. A taxonomy and survey of grid resource management systems[D]. Melbourne: University of Monash and Melbourne, 2000.

[9] 吴毓毅, 贺也平. 关于网格计算授权机制的研究[J]. 计算机应用研究, 2006, 22(8): 27.

[10] 刘　妍, 郭　洁. 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): 25.

[11] 王西龙. 基于GLOBUS的网格认证授权模型研究[D]. 南京: 南京工业大学, 2007.

[12] 石稀林, 方　勇. 分布式环境下一种基于角色的访问模型[J]. 四川大学学报(自然科学版), 2007, 44(2):19.

编　辑　熊思亮

(上接第180页)

[5] HIJAZJ S L, NATARAJAN B. Near-optimal multiuser detection in asynchronous MC-CDMA via the ant colony approach[C]//2007 2nd International Symposium on Wireless Pervasive Computing. Piscataway: Institute of Electrical and Electronics Engineers Computer Society, 2007: 274-279.

[6] KENNEDY J, EBERHART R C. A discrete binary version of the particle swarm optimization algorithm[C]//1997 IEEE International Conference on Systems, Man, and Cybernetics. New York, NY, USA: IEEE Service Center, 1997: 4104-4108.

[7] 赵　莹, 郑君里. 采用粒子群算法的DS-CDMA多用户检测[J]. 清华大学学报, 2004, 44(6): 840-842.

[8] 杨红孺, 高洪元, 庞伟正, 等. 基于离散粒子优化算法的多用户检测器[J]. 哈尔滨工业大学学报, 2005, 37(9): 1303-1306.

[9] GUO Zhen-qing, XIAO Yang, LEE M H. Multiuser detection based on particle swarm optimization algorithm[C]//2007 IEEE International Symposium on Circuits and Systems. Piscataway: Institute of Electrical and Electronics Engineers Inc, 2007: 27-30.

[10] SOO K K, SIU Y M, CHAN W S, et al. Particle-swarm-optimization-based multiuser detector for CDMA communications[J]. IEEE Transactions on Vehicular Techno logy, 2007, 56(3): 3006-3013.

[11] MANOLAKOS E S. Hopfield neural network implementation of the optimal CDMA multiuser detector[J]. IEEE Transactions on Neural Networks, 1996, 7(1): 131-141.

编　辑　张　俊