* 1

GSI 的信息栅格授权服务策略

陈　靖，　张水平，　石琢栋，　张凤琴
(空军工程大学　电讯工程学院，陕西　西安　710077)

摘　要：GSI 授权机制过于简单，作为对 GSI 授权机制补充的社区授权服务(CAS)又过于中心化，不适应情报网格信息流授权机制的要求。为此，提出了基于角色访问控制(RBAC)的虚拟组织授权服务(VOAS)策略，允许给用户分配 VO 角色来支持角色分层和限制。通过将 VO 角色映射为本地数据库角色，以及对本地角色委派细粒度权限等工作，既实现 VO 间用户与访问权限的逻辑分离，又杜绝了角色联合权限的方式，使 VO 间的授权管理比较简单灵活。解决了现有信息栅格中 CAS 授权粒度不够细化、可扩展性差等问题。仿真实验表明，该授权策略在不影响系统运行效率的前提下，简化了系统授权和管理的复杂度。

关键词：信息栅格；授权服务策略；角色访问控制；栅格安全基础设施
中图分类号：TP338.8　　**文献标识码**：A　　**文章编号**：1009－3516(2009)02－0071－05

栅格(Grid)为动态变化的多个虚拟组织间实现一致的、柔性的资源共享与协同问题[1]提供了新视角、新理念和新技术。美军的全球信息栅格 (Global Information Grid，GIG)[2-3]是栅格技术在军事运用的第一个实例，其建设与发展给世界新的军事变革带来了深远的影响。将栅格思想应用于雷达情报组网一体化建设方面在情报处理的逻辑层面上采用了传统集中式、紧耦合的静态体系架构，而且该系统的建设没有基于一个通用、标准和开放的安全体系架构，不仅使其它情报系统难以与此系统互联、互通、互操作，而且该系统既有中心节点，各关键节点间又过于紧耦合，使系统的安全性、动态灵活性、可扩展性和抗毁性都受到了极大限制。

为此，我们基于开放网格服务结构(OGSA)和网格中间件、P2P 中间件等技术，通过情报资源组织与发现机制、统一的情报资源描述模型和情报服务组合模式，以及雷达情报仿真系统，构建了雷达情报的信息栅格(Information Grid，IG)[4]资源共享环境，继承了 GSI(Grid Security Infrastructure)[5]的一些设计思想与实现，尤其是通信保护、认证和代理证书机制。但因它的授权机制过于简单[6]，而 CAS (Community Authorization Service)[7]作为 GSI 授权机制的补充，又过于中心化，而且授权单位是一条条的许可，不适应情报网格信息流授权机制的要求。VOMS (Virtual Organization Membership Service)[8]作为欧洲数据网格的虚拟组织授权方式，具备了分布、灵活的特点，本地资源参与授权的思想对情报网格值得借鉴。但它颁发的属性证书没有遵循 Web Service 安全标准，而且解决的是网格环境中文件系统的管理问题。因此，需要扩展适用于 IG 的 GSI 授权策略。

1　IG 的授权策略

传统的访问控制策略[9]可以分为自主访问控制 DAC 和强制性访问控制 MAC 两种。DAC 中用户可以针对被保护对象制定自己的保护策略。由于其易用性与可扩展性，自主访问控制机制经常被用于商业系统，如 UNIX 操作系统就采用了 DAC 访问控制。其特点是配置的粒度小，但是它无法实现动态的和复杂的安全

*　**收稿日期**：2008－07－18
基金项目：陕西省自然科学基金资助项目(2007F43，SJ08－ZT15)；空军工程大学电讯工程学院博士启动基金资助项目(KDYBSJJ402)
作者简介：陈　靖(1963－)，女，山西临汾人，副教授，博士，主要从事分布式计算及信息栅格研究；
E－mail：jingchen@263.net
张水平(1956－)，女，山西新绛人，教授，主要从事网络与分布式数据库研究.

策略。MAC 主要用于多层次安全级别的应用中,用来保护系统确定的对象,用户不能改变它们的安全级别或对象的安全属性。MAC 进行了很强的等级划分,所以经常用在军事系统中。其缺点在于主体访问级别和客体安全级别的划分与现实要求无法一致,在同级别间缺乏控制机制。另外,由于 MAC 过于偏重保密性,对其它方面如系统连续工作能力、授权的可管理性等考虑不足。

DAC 和 MAC 有时会结合使用,例如:系统可能首先执行 MAC 来检查用户是否有权限访问一个文件组,然后再针对该组中的各个文件制定相关的访问控制列表。其特点是配置的粒度大,但是缺乏灵活性。

1.1 社区授权服务 CAS

早期的 GT3 通过 GSI 提供的安全措施重点解决了认证和消息保护问题,但是缺乏基于全局策略的具有良好扩展性的访问控制机制。GT4 的 GSI 通过提供建立在公共密钥确认和授权机制之上的 CAS 体系结构,记录了 VO 的用户群和它们对资源的权限及接入控制策略。需要访问 VO 资源的用户与 CAS 服务器联系,服务器根据用户的请求和用户在 VO 内的责任给用户授权。假定 VO 中的所有成员都信任 CAS 服务器,并将它们资源的部分或全部访问权限由 CAS 来统一管理。在此条件下,一个资源的访问策略分为 2 部分:一部分是 VO 统一管理的策略,有统一的策略表示形式,称之为 VO 的全局策略;另一部分为各站点制定的策略,称为本地策略。只有访问者同时满足 2 部分策略才能获得访问资源的权限。CAS 在 VO 中是一个策略服务中心,发布 VO 的全局策略,其内容包括:VO 中资源的访问控制策略,资源提供者权限、VO 中的成员列表以及 CAS 服务器自己的访问控制策略等。

CAS 的授权策略拥有很多优点,如一个 VO 增加了用户,只需要在 CAS 服务器中存储相关的用户信息就可以了,而不需要每个资源提供者都要将这个用户的信息加入自己的访问控制中。同样,新加入的资源只需要对 CAS 服务器进行授权即可,不需要对庞大的所有用户进行直接授权,这样就保证了授权策略的可扩展性[10]。但在运行 CAS 时,属于多个用户组的用户可以请求并授予组合角色,同时拥有一个或多个用户组的特权。因此,CAS 只能实现一种“多对一”的角色映射,即一个角色可以映射多个用户,而一个用户不能被映射到多个角色。如果某个用户同时映射到 2 个或多个 CAS 上,并且 2 个 CAS 的授权之间出现交集或更复杂的逻辑,则在访问控制时就无法进行处理。此外,如果 CAS 服务器的策略发生改变,必须通知到每一个注册资源进行相应的改变,如果用户的策略发生改变,必须到每一个相应的 CAS 服务器上进行更改或者注销,这些使得资源管理比较复杂,系统可扩展性差;CAS 做为 GSI 授权策略的补充过于中心化,当很多用户同时请求与 CAS 服务器交互时,CAS 服务器可能出现瓶颈,导致性能下降,甚至瘫痪。

1.2 基于 RBAC 的 VOAS 授权策略

本文提出基于角色访问控制 RBAC 的 VOAS 授权策略,允许给用户分配 VO 角色来支持角色分层和限制,并不是使用这些角色联合权限的方式来访问特定角色的资源,而是将 VO 角色映射为本地数据库角色,以及对本地角色委派细粒度的权限等工作,都交给资源提供者和 VO 共同协商解决,既实现 VO 间用户与访问权限的逻辑分离,又使 VO 间的授权管理比较简单灵活。VO 角色以偏序关系(≥)组织,如果 $X \geq Y$,那么 VO 角色 X 就继承了 VO 角色 Y 的权限,意味着 X 的成员也是 Y 的成员。VO 管理可根据 VO 的 Index Service 组织内部的资源权限分类,创建 VO 角色树。

为实现 IG 基于 RBAC 的 CAS 授权管理,需要在 VO 层角色模型中声明 2 类权限:IG 服务权限和 IG 库资源权限,还必须包含使角色易于理解和易于操作的信息,见表 1。

实现 IG 授权的核心模块包括:①VO 端授权管理工具:查询实时的 VO 资源树、VO 角色树,提供 VO 管理者进行角色和授权管理;②VO 授权服务:实现 IG 的 VO 授权协议,发布 VO 角色信息,支持基于 VO 角色的授权;③本地授权服务:实现情报网格本地授权协议,发布共享的情报库用户信息,支持网格用户与情报库用户间映射关系的建立和维护。其关系及交互流程见图 1。

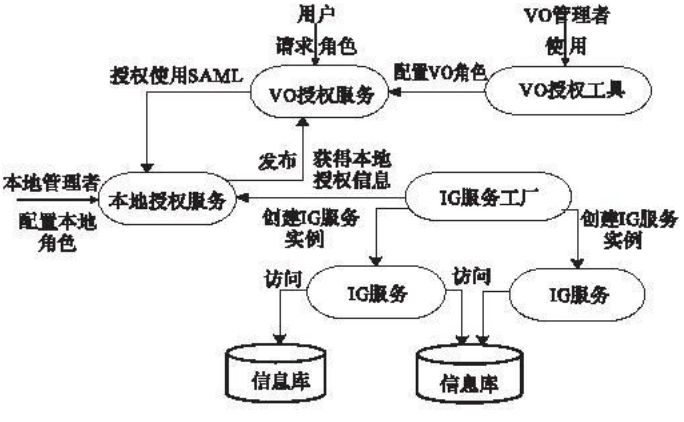

图 1 IG 授权管理交互流程

Fig. 1 Interaction flow of authorization management

表 1　基于 RBAC 的 IG 权限设置

Tab. 1　IG rights settings based on RBAC

角色名称(必须)		角色名
角色权限描述(必须)		角色的大致功能
备注		介绍角色的其他事项
角色层次		有无父角色
父角色名称		父角色名
IG 服务权限(必须:该角色对虚拟组织内部服务的访问权)	服务名称(必须)	IG 服务的名称 ID
	服务功能描述	IG 服务的功能描述
	服务 URI(必须)	IG 服务的 URI
IG 库资源权限(必须:该角色对虚拟组织内部 IG 库资源的访问权)	情报库名称(必须)	IG 库名称 ID
	数据库描述	IG 库简介
	情报库服务名称(必须)	IG 库所对应的 IG 服务的名称 ID
	本地授权服务名称(必须)	IG 库本地授权服务的名称 ID
	本地授权服务 URI(必须)	IG 库本地授权服务的 URI
	IG 库用户名(必须)	该角色对应的本地库用户名
	IG 库用户权限描述(必须)	该角色对应的本地库用户权限描述
	情报库用户访问权限描述	该角色对应的本地库用户建立库连接时的限制;如时段、连接数限制之类
创建时间		创建角色的时间
创建者		创建角色的管理者

在 IG 中支持 RBAC 策略体现出明显的优势:通过在用户和权限之间引入角色的方式,大大降低了系统的复杂度和系统管理员误操作的可能性;角色之间的互斥关系可以很容易地实现任务分离,同时角色访问控制还支持最小权限策略,提高了对系统安全的维护。

2　性能测试与分析

基于 RBAC 的 VOAS 策略系统最主要的改变在于对原有 CAS 策略服务器端的映射和客户端的证书委托,为此需要对客户和服务器的安全进行测试与分析,主要是对提供的签名(Signature)、加密(Encryption)、无安全措施(None)的 3 种栅格服务对系统运行带来的性能影响进行比较。本文为了更加直观显示,分别设计了 IG 使用 VOAS 代理证书的 3 种栅格服务 None With VOAS、Signature With VOAS、Encryption With VOAS,结果分别用 A1、B1、C1 表示;不使用 VOAS 代理证书的 3 种栅格服务 None Without VOAS、Signature Without VOAS、Encryption Without VOAS,结果分别用 A2、B2、C2 表示,并分析和比较了这些服务对性能系统带来的影响。

试验环境部署如下:在 Linux Redhat AS4.0 操作系统下安装了 Globus Toolkit4.0.4;使用 MySQL 作为实验数据库;Intel Pentium 4 处理器,内存为 512 MB。在计时方面,使用 Java 的 SystemCurrentTimeMillis()来获取毫秒级的当前系统时间,在服务器端使用 Apache 的日志操作包 Log4j 组件 loggers,将用时也以毫秒级记录到日志文件。

2.1　客户端安全分析

在客户端使用 VOAS 生成的权能代理证书时,涉及到了创建 VOAS 代理证书的时间花费。因为当客户与 IG 建立安全上下文关系时,会产生一定的时间花费。此时间花费只发生这一次,接下来客户端就可以在代理证书期满之前进行任意次数的访问,因此本文在性能分析中不计算此时间花费带来的额外开销。

在使用 VOAS 的代理证书联系信息栅格服务工厂(Information Grid Server Factory,IGSF)时,IGSF 的 findServiceData 函数可以返回相关数据资源的信息。连续 3 次的执行 findServiceData 函数会依次返回 database schema、activities permitted、product type 这 3 个不同的信息。IG 服务的 perform 函数将 perform 生成的文档(包括查询和返回的结果)传给客户端。IG 的 Secure Conversation 需要在客户和服务器之间首先建立安全的上下文关系。

从图 2 所示客户端通讯耗时可以看出,无论网格服务采用何种安全措施(签名或加密),创建证书的时

间基本是相同的。在无安全措施的情况里,由于不需要使用证书,所以这里的耗时为0。无论在何种安全类型中在第1次执行 findServiceData 数据时 IG 都需要进行初始化,因此执行 findServiceData 函数的时间远比第2、3次用时要多。另外,图2(b)清楚的展示了在客户端的安全措施里并没有作任何改变,只是将用户代理证书换成了 VOAS 代理证书.因此使用 VOAS 代理证书与不使用的耗时基本相同。

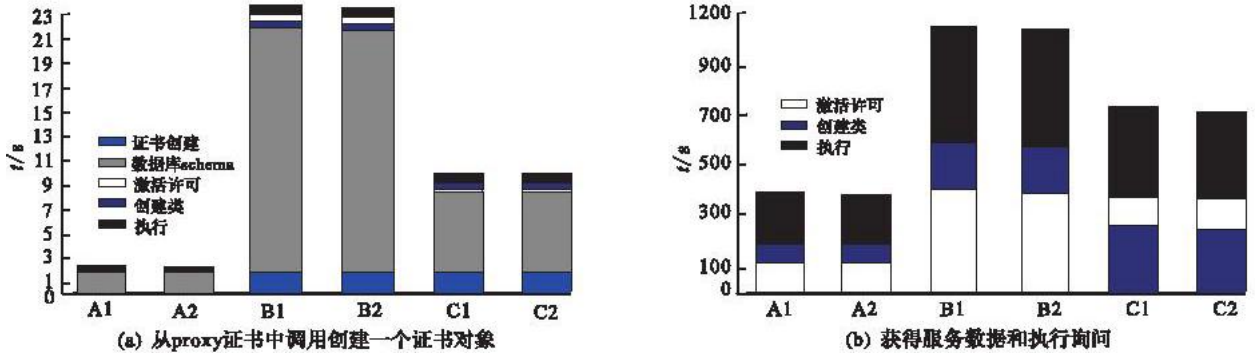

图2 IG 客户端耗时

Fig. 2 IG time in client

2.2 服务器端安全分析

对服务器端的分析应该从以下几个方面进行考虑:对用户证书访问要从证书中提取 VO 角色或栅格实体身份;将用户角色映射为数据库中的用户名和密码并建立 JDBC 连接;perform 函数的执行。

从图3服务器端各种情况耗时比较可以看出:只有当信任证书过程提取完毕后操作才被执行完,结果提取时间不受信任证书使用的类型所影响,执行 perform 函数的耗时基本保持不变,与证书提取时间相比,执行 perform 函数的时间是非常少的。同时也可以看到,映射和建立数据联接的耗时,各种情况下几乎相同。而由于需要从 VOAS 证书中提取角色信息 所以使用新方案的时间比原系统的耗时略为增加 但可忽略不计。

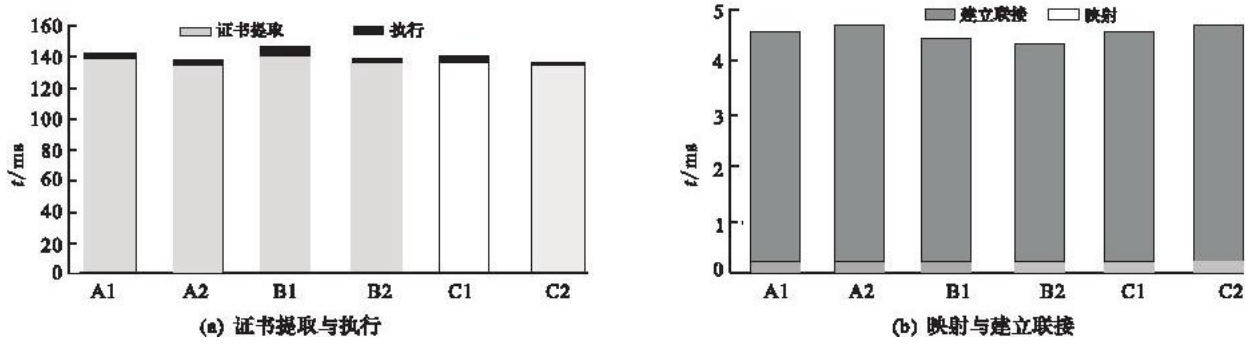

图3 IG 服务器端耗时

Fig. 3 IG time in server

3 结束语

本文针对 IG 环境中资源和用户属于多 VO,以及状态的动态性特点,在深入研究 GSI、网格信任授权模型以及访问控制策略等相关技术的基础上,以 GT4 为系统开发工具,通过 CAS 中引入 RBAC 策略,以及提供本地授权服务、VO 授权服务和授权管理工具,实现了细粒度的授权服务和用户资源共享的高度可控性,并简化了系统授权和管理的复杂度。

参考文献:

[1] Foster I, Kesselman C, Nick J, et al. Grid Services for Distributed Systems Integration [J]. IEEE Computer, 2002, 35 (6): 37-46.

[2] 徐志伟, 冯百明, 李 伟. 网格计算技术[M]. 北京:电子工业出版社, 2004.

XU Zhiwei, FENG Baiming, LI Wei. Grid Computing Technology [M]. Beijing: Electronic Industry Press, 2004. (in Chinese)

[3] 刘　鹏,王立华. 走向军事网格时代[M]. 北京:解放军出版社,2004.
LIU Peng, WANG Lihua. Taking to Time of Military Grid [M]. Beijing: PLA Press, 2004. (in Chinese)

[4] 陈　靖,张水平,殷肖川,等. 雷达情报栅格安全访问控制研究与实现[C]//军事电子信息学术会议论文集. 北京:电子工业出版社,2008:651 - 656.
CHEN Jing, ZHANG Shuiping, YIN Xiaochuan, et al. The Research and Implementation of Safe Access Control For Radar Information Grid [C]//The Conference on Military Electronic Information Proceedings. Beijing: Elctronic Industry Press, 2008: 651 - 656. (in Chinese)

[5] Randy Butler, Von Welch, Douglas Engert. A National - Scale Authentication Infrastructure [J]. IEEE Computer, 2000, 22(4): 13 - 19.

[6] 王　闰. 基于 GSI 的数据库网格安全基础架构[D]. 杭州:浙江大学,2006.
WANG Run. The Basic Architecture of Database Grid Security Based on GSI [D]. Hangzhou: Zhejiang University, 2006. (in Chinese)

[7] Pearlman L, Welch V, Foster I, et al. A Community Authorization Service for Group Collaboration [C]//IEEE Workshop on Policies for Distributed Systems and Networks. [S. l.]: IEEE, 2002: 512 - 518.

[8] Loomis C. The Data Grid Project [EB/OL]. [2004 - 02 - 19]. http://eu - datagrid. web. cern. ch/eu - datagrid/.

[9] 张　亮. 网格安全中信任关系以及访问控制的研究[D]. 合肥:合肥工业大学,2007.
ZHANG Liang. Researching on Trusting and Access Control in Grid Security [D]. Hefei: Hefei Industry University, 2007. (in Chinese)

[10] Cannon S, Chan S, Olson D. Using CAS to Manage Role - Based VO Sub - Groups [C]// Computing in High Energy and Nuclear Physics. California: CHEP, 2003: 231 - 236.

(编辑:田新华)

The Research of Authorization Service Strategy for Information Grid Based on GSI

CHEN Jing, ZHANG Shui - ping, SHI Zhuo - dong, ZHANG Feng - qin
(Telecommunication Engineering Institute, Air Force Engineering University, Xi'an 710077, China)

Abstract: The Information Grid (IG) presented in this article is aimed at providing different units in the multiple virtual organizations (VO) with uniform information safely and rapidly, accurately and reliably. Its security frame takes up the designing idea and implementation of GSI, especially in communication protection, authentication and agency certification mechanisms. Yet the GSI authorization is not suitable for information grid stream as it is too simple and its supplement of the authorization mechanism CAS is too centralized. According to the Role - based Access Control (RBAC), the VO authorization service strategy (VOAS) is presented, by which the problems of the delicate authorization and extensibility of globus are solved. The result of simulations shows that the VOAS strategy will not affect the efficiency of the system, and instead, the complexity of the accessing control is reduced.

Key words: information grid (IG); authorization service strategy; role - based access control; grid security infrastructure (GSI)