基于策略的自动协商机制在分布委托授权中的应用

武小年[1,2] 张润莲[1] 马春波[1] 周胜源[1,2]
(桂林电子科技大学信息与通信学院 桂林 541004)[1] (现代通信国家重点实验室 成都 610041)[2]

摘 要 网格系统采用委托授权有效地解决了分布状态下的授权问题,但其动态变化将打破委托授权模式下不同安全域间访问权限的全局一致性。为解决该问题,采用了一种基于策略的自动协商机制。为及时发现问题并在相关安全域间快速协商和恢复双方访问权限的全局一致性,该机制定义了一组用于引导协商过程自动进行的策略规则,并给出一个系统必须遵循的协商状态转换图,从而在事件触发器的推动下,自动实施协商过程的状态变换,实现权限协商并重新授权。测试结果表明,与人工协商相比,该自动协商机制提高了解决问题的效率,改善了系统性能,并简化了管理者的安全维护管理工作。

关键词 委托授权,自动协商,策略,状态转换图
中图法分类号 TP393 **文献标识码** A

Application of Automated Negotiation Based on Policy in Delegation Authorization of Distributed Environment

WU Xiao-nian[1,2] ZHANG Run-lian[1] MA Chun-bo[1] ZHOU Sheng-yuan[1,2]
(School of Information and Communication, Guilin University of Electronic Technology, Guilin 541004, China)[1]
(National Laboratory for Modern Communications, Chengdu 610041, China)[2]

Abstract The grid system authorizes in delegation model to adapt well to the distributed environment. But the dynamic change of the grid would break the global consistency of privileges in delegation model between different secure domains. To address the problem, this paper introduced an automated negotiation mechanism based on policies. In order to detect the problem timely and negotiate the privileges quickly and renew the global consistency of privileges between the corresponding secure domains, the mechanism defined a set of policy rules, which would conduct the negotiation process to automate, and presented a state transition diagram that the system should follows. Sequentially, driven by the trigger, the mechanism would implement automatically the negotiation state transition, and enforce the privileges negotiation and reauthorize between negotiation parties. The test result shows that, comparing with negotiation process conducted by people, the automated negotiation mechanism improves the efficiency of the solution to the problem and system performance, and simplifies security administration work of the administrators.

Keywords Delegation, Automated negotiation, Policy, State transition diagram

随着 Internet 的发展,人们开始在这种便利的公共交互平台上从事各种商业活动。为了能够在这种平台上不受人为约束地自由交互(如投标、拍卖、交易等),一种自动协商机制应运而生,并引起了不同学科背景学者的广泛关注,包括社会学、经济学、通信科学等。协商是自主的两方或多方之间为达成某种一致的目的进行交互并决策的一个过程[1]。与人工协商相比,自动协商机制具有如下优势:(1) 自动协商通过交易代理能高效地实现协商过程,不需要协商者随时在线,具有快速响应能力并能够大大拓展协商的应用范围;(2) 基于管理者预先制定的策略,自动协商能以指定方式自动地调用相关服务以执行特定任务,大大简化了管理者的管理工作;(3)自动协商能够不断获取不同管理者的知识而成为领域协商专家,并通过这些知识更好地引导复杂的协商过程,获得比人工协商更好的效果。自动协商机制已被广泛应用到各种分布、开放性系统中。

网格系统以 Internet 为桥梁,在开放的广域网环境中为地理位置分布的个体、机构和资源的动态联合提供一种灵活、安全、对等的资源共享。为解决系统在分布状态下的授权问题,目前的网格授权框架,如 CAS(Community Authorization Service)[2] 等采用委托授权模式[3],即由资源提供者(Resource Provider)为社区(Community)授权并签发属性证书(Attribute Certificate, AC)[3]。社区通过持有资源提供者签发的 AC,保持其对资源提供者中资源的访问权限与资源提供者访问策略中定义的社区访问权限的全局一致性。但这种

到稿日期:2009-04-15 返修日期:2009-07-02 本文受现代通信国家重点实验室基金项目(9140C1101050706)和广西信息与通讯技术重点实验室基金(10908)资助。
武小年(1972—),男,硕士,副教授,主要研究方向为信息安全、网格计算,E-mail:xnwu@guet.edu.cn;张润莲(1974—),女,博士生,副教授,主要研究方向为信息安全、网格计算;马春波(1975—),博士,教授,主要研究方向为公钥密码学、网络安全;周胜源(1974—),男,硕士,副教授,主要研究方向为宽带通信网络。

一致性是静态的。在网格环境中，用户和资源是动态变化的。这种动态变化将导致网格系统相关安全域中访问策略单方面的动态变化，从而破坏在委托授权模式下特定安全域间访问权限的全局一致性。这种不一致的访问权限不仅威胁系统安全，也将因权限的不一致而导致系统中产生大量的最终被拒绝的网格作业，浪费系统资源，且对不一致权限的协商处理使得管理者的安全管理工作更加复杂。在开放的网格环境中，以人工协商方式及时并准确地解决这种因动态变化所引起的权限不一致问题是非常困难的。

目前，人们开始在网格环境中引入自动协商机制，如支持资源的自动管理[4]和授权协商[5,6]。文献[5]提出的 TOWER 是一种用于 CROWN 网格环境的信任协商框架，其借助于基于属性的信任书来支持灵活的委托授权，并基于协商策略在服务请求者和提供者间动态地构造信任链。为了能够让位于网格不同管理域的客户端和服务器间发现彼此的授权策略，文献[6]提出一种策略驱动的授权协商机制，该机制声明了保护其资源的策略。这些声明详细说明了用于协商的约束和能力，识别来自另一方的信任书的需求，并决定被请求的信任书是否能被获得。协商的结果是一个状态：双方满足即将开始的交互的策略约束，或者这样的交互被单方或双方所否决。然而，这些策略协商机制并未考虑和解决委托授权中因系统动态所引起的访问权限全局不一致问题。

针对上述问题，在前期研究的基础上[7]，本文采用一种基于策略的自动协商机制，来维持开放的网格环境中不同安全域间访问权限的全局一致性。在该机制中，定义了一组用于引导协商过程自动进行的策略规则，并给出一个系统必须遵循的协商状态转换图，从而在事件触发器的推动下，实施协商过程的状态变换以执行特定的协商任务，解决在分布委托授权中因系统动态变化所引起的访问权限的全局不一致问题。

1 基于策略的自动协商机制

在网格环境中，资源和用户的动态变化将最终破坏资源提供者和社区间前阶段定义的访问权限的全局一致性。为及时发现并快速解决问题，本文通过触发器实时监控访问策略的动态变化，并引入基于策略的自动协商机制来支持双方访问权限的自动协商。为了自动化一个协商过程，需要完成两个重要的任务：(1)建立一个能够引导协商过程自动执行的策略知识库；(2)明确定义并执行协商过程中的状态变换[1]。因此，基于策略的自动协商机制主要包括两个部分：策略知识库和协商者。其中，协商者包括 4 个功能部件：策略管理、策略协商、策略决策和策略实施。为了能够最终恢复协商双方访问权限的全局一致性，协商者需要调用系统委托授权中的证书管理和访问策略的相关服务。基于策略的自动协商机制的系统结构如图 1 所示。其中，虚线部分为监测并触发一个协商过程自动进行的处理逻辑。

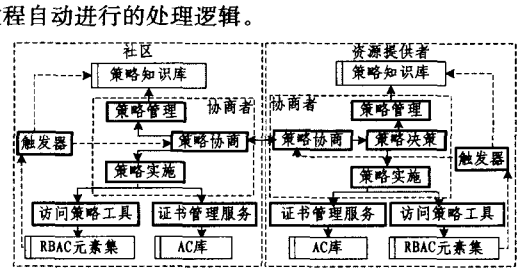

图 1 基于策略的自动协商机制

图 1 中，策略知识库定义一组用于响应资源提供者和社区间访问权限动态变化的基本规则，每个规则阐述了安全域在特定条件下对访问权限的需求或许可。协商者实施协商双方的规则协商，进行协商决策并执行决策结果，维持协商双方访问权限的全局一致性。其 4 个功能部件的功能如下：

策略管理(Policy Administration Point，PAP)通过一个统一的接口，访问并管理策略知识库，实现具体规则的创建、修改和存储。

策略协商(Policy Negotiation Point，PNP)是协商过程中最关键的部分。为了准确地协商各方间的协商请求并进行决策，需要理解协商请求中的相关内容，如协商目的和条件等，并根据自身策略知识库中的协商知识检验协商请求。

策略决策(Policy Decision Point，PDP)根据 PNP 的协定，决定该协商请求是被接受或被拒绝。

策略实施(Policy Enforcement Point，PEP)执行 PDP 的最终决策，恢复协商双方间访问权限的全局一致性。PEP 包括 3 个任务：(1)依据协商的最终决策，PEP 将通过 PAP 更新与协商请求相关的策略规则；(2)根据策略规则中的访问权限变化，通过调用访问策略服务更新访问策略元素集，重新授权；(3)根据更新的授权信息，调用证书管理服务，重新签发包含新访问权限的 AC。

触发器定义了与访问策略相关的事件发生，如进行 insert，update 和 delete 操作，且相关触发条件被满足时，如进行操作的主体和对象符合特定的条件等，应采取的动作。同时，本文也设置一个触发器监测策略知识库，当触发条件被满足，如策略知识库中规则被审计等，将触发启动协商者，开始实施自动协商。

证书管理服务和访问策略工具是系统委托授权的两个功能部件。证书管理服务实施用户标识和 AC 的分发和撤销。依照委托模型，资源提供者作为整个系统授权的最终信任源点(Source Of Authority，SOA)[3]，对整个系统权限的分发负有最终责任。社区作为委托者，将建立授权管理核心服务节点(Attribute Authority，AA)[3]，根据资源提供者的授权信息进行委托授权。访问策略工具定义委托授权中的访问策略基本元素集，本文采用 RBAC 模型[8]定义元素集。

2 策略知识库

为了确保协商双方间的有效交互，协商双方需要在协商过程中交换特定的协商信息。这些信息声明了协商双方的需求、约束、事件或偏好等，成为引导协商过程自动进行的一组必须遵循的规则，并形成协商策略知识。针对上述访问权限的全局不一致问题，协商策略知识侧重声明系统对特定访问权限进行协商处理的规则，包括协商目的和协商条件等。

具体地，协商策略知识库结构包括 4 个部分：(1)协商双方的身份(Identities)，包括授权者(资源提供者)和权限接收者(社区)；(2)协商目的(Purposes)，包括资源对象及指定在该资源对象上进行变更的权限集；(3)协商条件(Obligations)，包括协商权限的变更范围、权限约束和时效性；(4)规则处理状态(States)，包括规则审计状态和协商状态，通过这些状态，系统能够更好地理解规则的当前状态，并方便地依据规则的状态进行特定处理。上述协商策略知识库可通过一个 XML 格式表达如下。其中，在策略规则的角色定义中拥有 depth 标记，表示为此角色能够被委托的深度约束，depth 为 0

时表示不能委托;每当委托一次,depth 自动减 1。

```
〈Policy-Rule〉
 〈Identities〉
  〈Subject〉
   〈provider id =〉〈value〉〈/value〉〈/provider〉
  〈/Subject〉
  〈Recipients〉
   〈community id =〉〈value〉〈/value〉〈/community〉
  〈/Recipients〉
 〈/Identities〉
 〈Purposes〉
  〈principal ref = " " /〉
  〈Object〉
   〈resource id =〉〈value〉〈/value〉〈/resource〉
  〈/Object 〉
  〈Role name = " " depth = " " 〉
   〈attribute name= " "〉〈value〉〈/value〉〈/ attribute〉
  〈/Role〉
 〈/Purposes〉
 〈Obligations〉
  〈principal ref = " " /〉
  〈Max-role name = " " depth = " " 〉
   〈attribute name=" " 〉〈value〉〈/value〉〈/ attribute〉
  〈/Max-role〉
  〈Min-role name = " " depth = " " 〉
   〈attribute name=" " 〉〈value〉〈/value〉〈/ attribute〉
  〈/Min-role〉
  〈Conditions = " " 〉〈value〉〈/value〉〈/Conditions〉
  〈Period = " " 〉〈value〉〈/value〉〈/Period〉
 〈/Obligations〉
 〈States〉
  〈Auditing state〉…〈/Auditing〉
  〈Processing state〉…〈/Processing〉
 〈/States〉
〈/Policy-Rule〉
```

3 协商者

为使协商过程自动化,协商者基于策略知识库的规则,按照特定的状态变换完成协商任务。在协商过程中,协商者将通过图 1 所示的 4 个功能部件执行协商任务,即进行权限协商和重新授权,以恢复协商双方访问权限的全局一致性。一个由社区发起的自动协商过程状态转换图如图 2 所示。

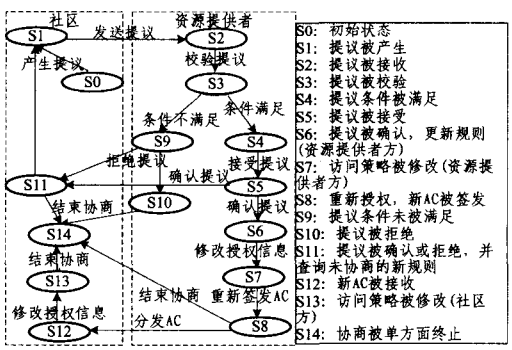

图 2 自动协商状态转换图

图 2 共有 15 种状态。S0 是初始状态,标志着协商过程的开始。根据策略知识库中待协商的规则,社区的协商者由其 PNP 产生一个提议(S0→S1)。提议的数据结构与策略知识库结构相同。资源提供者的 PNP 接收到来自社区的提议后(S1→S2),将学习、理解并校验提议中的信息(S2→S3),这需要其通过 PAP 查询自身策略知识库并进行确认。若条件满足(S3→S4),如提议中请求的权限集及相关约束条件被满足,资源提供者 PDP 将接受该提议(S4→S5);否则(S3→S9),将拒绝该提议(S9→S10)。对提议的最终决策由资源提供者 PDP 决定,这是因为资源提供者需要维持对本域内资源的最终控制权。

若协商提议被资源提供者 PDP 拒绝,资源提供者 PNP 将 PDP 决策结果通告社区 PNP,并等待下一个待协商的问题(S9→S11)。社区 PNP 根据资源提供者 PNP 通告的结果处理与协商提议相关的策略规则,如提议被拒绝,则更新该策略规则中的协商状态,并搜索其策略知识库中与该资源提供者相关的待协商策略规则。若有待协商的规则,社区 PNP 将产生新的提议(S11→S1),并通告资源提供者 PNP 协商进程阻塞等待;否则,社区 PNP 单方面结束协商过程(S11→S14),并通告资源提供者,以结束该协商过程(S10→S14)。

若协商提议被资源提供者 PDP 接受,资源提供者将确认该提议,通过其 PAP 修改自身策略知识库中所对应的规则(S5→S6);同时,资源提供者 PNP 将 PDP 决策结果通告社区 PNP,并等待下一个待协商的问题(S5→S11)。社区 PNP 根据资源提供者 PDP 决策结果修改其策略知识库中所对应的规则,并查询策略知识库中是否有与该资源提供者相关的待协商需求。若有待协商的规则,社区 PNP 将产生新的提议(S11→S1),并通告资源提供者 PNP 协商进程阻塞等待;否则,资源提供者和社区将通过 PEP 执行资源提供者 PDP 的决策结果,重新授权以恢复双方访问权限的全局一致性。

资源提供者 PEP 根据更新的策略规则中的权限变化,通过调用访问策略服务来更新访问策略元素集,为社区重新授权(S6→S7);其后,资源提供者 PEP 根据更新的授权信息,调用证书管理服务为社区重新签发包含新访问权限的 AC(S7→S8)。社区 PNP 接收到资源提供者 PNP 传递的 AC(S8→S12),调用证书管理服务更新其 AC,并根据新 AC 中的授权信息,通过调用访问策略服务来更新其访问策略元素集(S12→S13)。最后,社区 PNP 单方面结束协商过程(S13→S14),并通告资源提供者 PNP 结束协商过程(S8→S14)。

4 实验与分析

本文采用 Java 语言实现了一个系统原型。策略知识库规则存储在 Microsoft SQL 数据库中,并设置相关事件触发器。为了更好地进行交互,协商者的 4 个功能部件被实现在一起,但每个功能部件分别响应特定场景的变化需求。同时,根据 PMI[3]/PKI[9] 标准和 Globus 的安全组件 Java CoG kit[10] 实现了证书管理服务中证书的分发、撤销和检验功能,并根据 RBAC 模型实现了一个 RBAC 工具,用于管理访问策略元素集。访问策略元素集存储在 Microsoft SQL 数据库中,并设置相关事件触发器。

上述原型被引入到校园网格实验平台,解决教务管理子系统中因访问权限的动态变化所引起的权限不一致问题。在教务管理子系统中,教务管理部门负责维护管理教学资源和人员信息,并为各教学单位分配教学任务;各教学单位承担本

部门的教学任务，并将其分配给本部门的相关教师。为实现分布授权，系统采用委托授权模型。其中，教务管理部门作为信任源点(SOA)，对整个系统权限的分发负有最终责任；各教学单位作为委托者(AA)，为本部门教师委托授权。但在系统中，教学资源、教师及其工作职责的动态变化，如电子教案的更新、教师教学任务的调整、学生成绩协同管理中的变化等，极易引起系统中访问权限的不一致，从而使得安全管理者的权限管理工作非常复杂。

在上述实验平台上，测试并比较了采用人工协商和本文的自动协商解决不一致权限问题的时间周期和系统开销。测试环境如下：6 台分布的服务器担当模拟的安全域环境，并通过 100Mbps 交换机连接多台客户机。其中，3 台服务器担当委托者(AA)节点提供服务并为其成员授权，3 台服务器担当信任源点(SOA)节点提供共享的物理资源并为委托者授权。服务器配置为 1.8GH 的 CPU、512MB 的内存和 80GB 的硬盘。

图 3 显示了分别采用人工协商和本文的自动协商解决权限不一致问题的时间周期测试结果。在同样条件下，与人工协商相比，采用自动协商能够更快地解决问题。这是因为自动协商有两方面的优势：(1)触发器能够及时发现问题；(2)服务的自动调用。随着资源、用户动态变化的加剧，这种优势将更加明显。采用自动协商方式，管理员只需预先设置策略知识库，从而大大简化了其日常繁琐的权限维护管理工作。

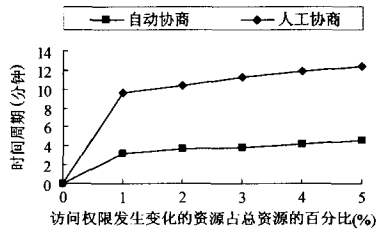

图 3　采用不同方式解决权限不一致问题的时间测试结果

图 4 显示了在同样条件下，分别采用人工协商和本文的自动协商解决不一致权限问题所耗费的系统开销。在人工协商方式中，测试并累计了系统为处理因权限不一致而最终被拒绝的作业所耗费的系统开销；在自动协商方式中，除测试并累计上述系统耗费的开销外，还测试并累计了维持自动协商机制运行的系统开销。图 4 主要测试的是 CPU 时间开销。在实验中，以图 3 所测得的采用人工协商处理少量不一致访问权限所需的 10min 为限，6 台客户机一个接一个提交作业，每分钟有 1 个作业访问存在访问权限全局不一致的资源。由于自动协商方式能够快速恢复权限的全局一致性，使得系统中出现权限不一致作业的数量大大减少，从而避免了系统耗费过多的资源来处理这些作业。从全局来看，采用人工协商解决权限不一致问题需要耗费系统更多的开销。

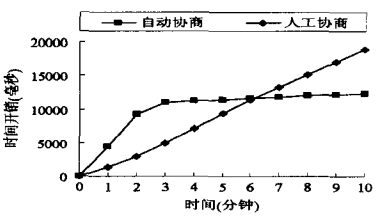

图 4　采用不同方式解决权限不一致问题的开销测试结果

结束语　本文采用一种基于策略的自动协商机制来解决开放网格环境中因动态变化所引起的访问权限全局不一致问题。本机制在触发器的实时监测和推动下，通过预定义的协商策略知识库引导协商，由协商者的 4 个功能部件根据定义的协商状态转换图执行协商过程中的特定任务，维持分布委托授权中系统访问权限的全局一致性。此机制在校园网格实验平台上的应用及测试结果表明，与人工协商相比，自动协商机制大大缩短了解决权限不一致问题的时间，从而减少了因权限变化而最终被系统拒绝的无意义网格作业的数量，避免了系统耗费大量的处理开销，提高了效率和系统性能。同时，机制只需要管理者预先设置策略知识库，大大简化了管理者日常繁琐的权限维护管理工作。

参 考 文 献

[1] Vivying S Y, Cheng, Hung P C K, et al. Enabling Web Services Policy Negotiation with Privacy Preserved using XACML [C]// Proceedings of the 40th Hawaii International Conference on System Sciences. HI, USA: IEEE CS, 2007: 33-43

[2] Pearlman L, Welch V, Foster I, et al. The Community Authorization Service: Status and Futures[C]//Computing in High Energy Physics (CHEP03). La Jolla, California, 2003

[3] Chadwick D. The X.509 Privilege Management Infrastructure [C]// Proceedings of the NATO Advanced Networking Workshop on Advanced Security Technologies in Networking. Bled, Slovenia: IOS Press, 2003: 15-25

[4] Sim Kwang Mong. A Survey of Bargaining Models for Grid Resource Allocation[J]. ACM SIGecom Exchanges, 2006(1): 22-32

[5] Li Jianxin, Huai Jinpeng, Xu Jie, et al. TOWER: Practical Trust Negotiation Framework for Grids[C]// Proceedings of the Second IEEE International Conference on e-Science and Grid Computing (e-Science'06). 2006: 26-33

[6] Constandache I, Olmedilla D, Siebenlist F. Policy-Driven Negotiation for Authorization in the Grid [C] // Proceedings of the Eighth IEEE International Workshop on Policies for Distributed Systems and Networks. June 2007: 211-220

[7] Zhang Runlian, Wu Xiaonian, Dong Xiaoshe, et al. An Authorization Mechanism Based on Privilege Negotiation Policy in Grid [C]// 10th IEEE International Conference on High Performance Computing and Communications (HPCC-08). Dalian, China: IEEE CS, 2008: 720-727

[8] David F, Ferraiolo, Sandhu R, et al. Proposed NIST Standard for Role-based Access Control [J]. ACM Transactions on Information and System Security, 2001, 4(3): 224-274

[9] Tuecke S, von Welch, et al. RFC3820: Internet X.509 Public Key Infrastructure (PKI) Proxy Certificate Profile [EB/OL]. http://www.ietf.org/rfc/rfc3820.txt, 2004

[10] von Laszewski G, Foster I, Gawor J, et al. A Java Commodity Grid Kit [J]. Concurrency and Computation: Practice and Experience, 2001, 13(8/9): 645-662