第33卷 第23期 计 算 机 工 程 2007年12月
Vol.33 No.23 Computer Engineering December 2007
·安全技术· 文章编号：1000—3428(2007)23—0151—03 文献标识码：A 中图分类号：TP309

同步协同应用访问控制

刘婷婷，汪惠芬
(南京理工大学机械工程学院 CIMS 研究所，南京 210094)

摘 要：提出了一个同步协同访问控制结构、协同小组共有权限算法，应用规则资源编码方法进行动态信息的访问控制策略制定，解决了同步协同应用信息共享引起的非法访问问题、访问决策效率问题和协同动态信息访问控制问题。应用表明，同步协同应用访问控制结构能够减少访问控制通信量50%以上，共有权限算法和规则资源编码方法是实用的。

关键词：同步协同应用；访问控制；共有权限

Access Control in Synchro-coroutine

LIU Ting-ting, WANG Hui-fen
(CIMS Institute, Mechanical Engineering School, Nanjing University of Science and Technology, Nanjing 210094)

【Abstract】 An access control scheme for synchro-coroutine, an algorithm to calculating public authorities and an automatic coding method are proposed to resolve the problems resulted from information sharing using synchro-coroutine among cooperant members, including illegitimate access, efficiency problem and the problem of how to control dynamic created information. The application result shows that the access control scheme can reduce the communications traffic to 50 percent and the algorithm is feasible.

【Key words】 synchro-coroutine; access control; public authorities

同步协同应用是指支持多个用户进行同步协同工作的应用程序。随着网络技术的发展，同步协同应用已经应用在很多企业内部部门之间和企业与企业之间的协同工作中，例如设计制造人员在网络化制造系统中对同一个零件的几何模型进行讨论和修改，或是对同一份文档进行编辑等。

同步协同具有共享特性，即同步协同过程中，协作成员之间协作信息共享，这使得同步协同方式能够快捷、方便解决问题的同时，对访问控制的需求区别于一般的个体访问方式。从20世纪90年代开始，同步协同对访问控制的需求已经引起研究人员的关注。

文献[1]对同步协同中权限控制进行了详细的分析并提出了一个面向协作系统的访问控制模型；文献[2]研究协同写作中的版本管理问题，定义了4个角色：编辑(editor)，书写(writer)，浏览(reviewer)和创建者(creator)，并通过定义这些角色在协同写作中具有不同的操作文档的权限来实现协同写作中文档的访问控制。

上述研究关注协作中不同成员对协作文档的操作权限问题，没有解决共享特性可能造成小组成员越权获取到系统资源问题；文献[3]对协同环境中共有资源的权限控制进行研究，基于量化权限的思想，提出细粒度协作访问控制策略，为解决这一问题提供了思路。

本文在分析同步协同应用中存在问题的基础上，对同步协同应用访问控制解决方法进行了研究。

1 问题描述

同步协同应用在网络环境下运行，从逻辑上由系统服务器、小组服务器和小组成员终端构成，其中系统服务器和小组服务器可以是一体的，也可以相互独立，如图1所示。从图中可以看出，小组成员信息交互与共享将造成同步协同应用权限控制等问题。

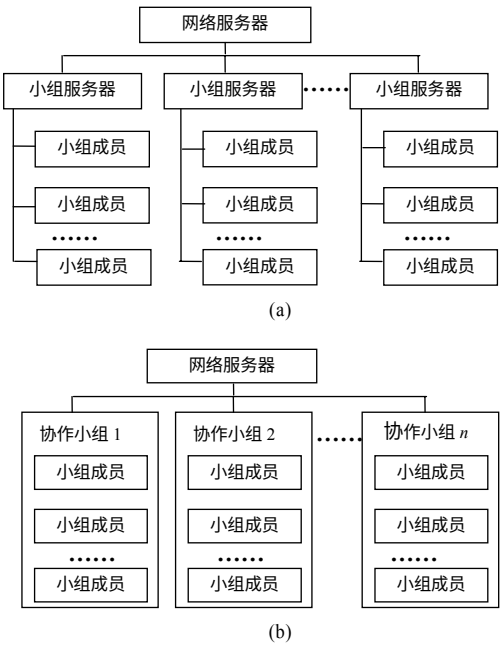


图1 同步协同应用逻辑结构

(1)同步协同应用访问决策效率问题

同步协同应用中，群组通信信息量大，而同步协同应用要求具有实时性，“所见即所得”是同步协同应用的基本要求。因此，如何有效地降低网络通信流量、提升同步速度是同步协同应用访问控制必须解决的问题之一。

基金项目：国家部委“十五”、“十一五”预研基金资助项目
作者简介：刘婷婷(1975－)，女，博士，主研方向：网络化制造，数据安全技术；汪惠芬，博士、副教授
收稿日期：2006-12-10 **E-mail：**liutingtingwy@163.com

(2)同步协同应用权限控制问题

同步协同中，系统资源在小组成员间共享，而协作成员可能是来自多个领域的专家或是多个部门，他们拥有不同的权限，这意味着协作共享特性可能造成小组成员越权获取系统资源。

(3)新产生信息访问控制

同步协同应用中，需要对两种资源进行控制：一是对系统中本就具有的资源的控制；二是对协作中新产生的协作信息、文档的控制。同步协同应用具有动态性，这就要求在协同应用中动态制定新产生信息的访问控制策略，传统的单一的由安全管理员制定安全策略的方法必然难以适应其动态性需求。

2 同步协同应用访问控制结构设计

同步协同应用中，网络通信量大，有效降低访问控制对协同应用实时性的影响是访问控制必须解决的问题。笔者认为，解决问题的最佳办法就是能够在本地进行访问控制决策，为此构建同步协同应用访问控制结构，如图 2 所示(仅给出访问控制相关的模块)，在系统服务器内设置服务器访问控制模块 SA 和全局策略存储器，同步协同成员终端设置小组成员访问控制模块 MA 和局部策略存储器。

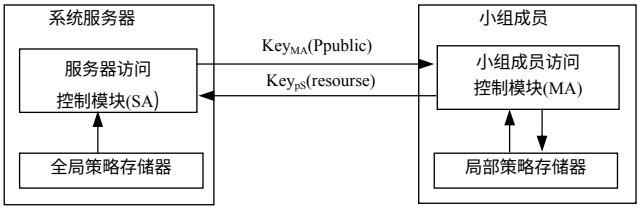


图 2　同步协同应用访问控制

SA 从全局策略存储器提取系统策略并计算协作小组共有策略提供给 MA，MA 将策略存储在局部策略存储器中，并对小组成员的访问请求进行决策，将合法的访问请求提交给 SA。

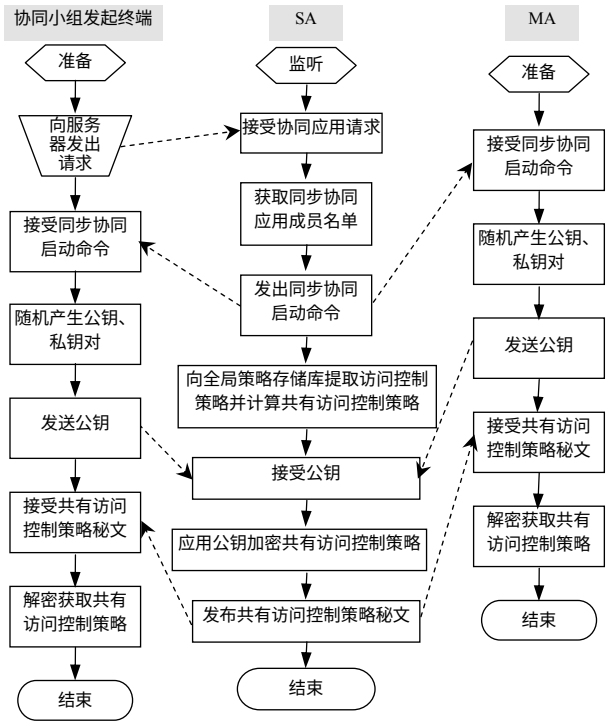


图 3　同步协同应用启动

SA 从全局策略存储器提取系统策略并计算协作小组共有策略提供给 MA 在同步协同应用初始化时进行。以实际应用需求为基础，假设同步协同应用启动前协作小组成员已经定义完成且同步协同应用发起时小组成员均在线，应用一次随机产生公钥、私钥对进行保密传输，设计同步协同应用初始化过程如图 3 所示。如果某小组成员不在线，仅需要服务器记忆非在线成员列表并监测系统用户登录情况，一旦发现系统用户登录且同步协同应用未结束，则可以发出同步协同应用启动命令。

由于应用一次随机生成的密钥对进行保密传输和存储，因此由应用密码学可知，同步协同应用初始化过程的安全性取决于加解密算法的应用和密钥的长度，高强度的算法和长的密钥长度可以保证初始化过程的相对安全性。

上述同步协同应用访问控制结构在 MA 中进行访问控制决策，小组成员发出访问请求，首先在 MA 中进行决策，如果访问请求为非共有权限，则 MA 制止小组成员访问请求；如果是共有权限，则向服务器提交访问请求，这使得与服务器之间的必要交互才执行。

3 共有权限求解算法

同步协同应用中协作小组共享系统资源，这将造成非法访问。解决这一问题的方法有两种：一是向协作小组提供共有权限，即协作小组只能向服务器申请所有成员都有权访问的资源；二是在小组协作中打破共享特性，协作资源仅提供给具有访问权限的成员。后一种方法将造成成员协同不同步现象，因此，使用第 1 种方法是一种相对好的方法。

以目前应用范围最广的基于角色访问控制模型为基础[4~5]，形式化同步协同应用中的访问控制策略，表达为：

$U=\{u_1,u_2,\cdots,u_n\}$　协作小组存在成员

$R=\{r_1,r_2,\cdots,r_m\}$　协同小组所在组织存在角色

$r_i \prec r_j$　r_i是r_j的继承角色，r_i拥有所有r_j的权限

$u_i \in r_j(1\le i\le n,1\le j\le m)$　访问主体u_i属于角色 r_j，拥有角色r_j的权限

$(u,p,object,cons,T)=True$ 主体 u 在约束 $cons$ 下对客体(某类客体)$object$ 具有操作权 p

$(u,p,object,cons,T)=False$ 主体 u 在约束 $cons$ 下对客体(某类客体)$object$ 不具有操作权 p

其中，T 用于区别客体或某类客体，T＝1 表示客体类，T＝0 表示单一客体，客体类是具有类似属性的客体的集合。

同步协同应用访问控制目标是求解共有权限 $P_{\text{public}}=P_{u_1}\wedge P_{u2}\wedge\cdots\wedge P_{u_i}\wedge\cdots\wedge P_{u_n}$，并在协同应用中应用共有权限控制小组成员活动。依据问题描述，本文给出同步协同应用求解算法。本算法依据同步协同应用中的访问控制策略的一般定义，进行用户-角色、用户-访问客体权限遍历，并计算共有角色和共有访问客体，在此基础上计算共有权限。

输入：系统访问控制策略，协作小组成员列表 $U=\{u_1,u_2,\cdots,u_n\}$

输出：协作小组共有权限P_{result}

(1)令$CR_i=\Phi(1\le i\le n)$，$\forall r\in \mathrm{R}$,若$u_i\in r$,计算$CR_i=CR_i\cup\{r\}(1\le i\le n)$；

(2) $\forall r\in CR_i, r\prec r_j$, 计算$CR_i=CR_i\cup\{r_j\}(1\le i\le n)$；

(3) $C_{\text{roles}}=CR_1\cap CR_2\cap\cdots\cap CR_i\cap\cdots\cap CR_n(1\le i\le n)$

(4)令$CP_i=\Phi(1\le i\le n)$, $CL_i=\Phi\ \forall u_i$, $(u_i,p,object,cons,T)=True(1\le i\le n)$,

令$CP_i=CP_i\cup\{(p,T,object,cons)\}(1\le i\le n)$,

$CL_i=CL_i\cup(p,T,object)$；

(5)令$CP=CP_1\cup CP_2\cup\cdots\cup CP_i\cup\cdots\cup CP_n$；

$CL=CL_1\cup CL_2\cup\cdots\cup CL_i\cup\cdots\cup CL_n$；

(6)$C_{\text{permissions1}}=CL_1\cap CL_2\cap\cdots\cap CL_i\cap\cdots\cap CL_n$；

(7)$CL=CL-C_{\text{permissions1}}$；

(8) 令$C_c=\phi,\forall(p,T,object)\in C_{\text{permissions1}},(p',T',object',cons')\in CP,$若$(p=p')\wedge(T=T')\wedge(object=object'),$计算$Cc=Cc\cup cons'$

转换$(p, T, object)$为$(p, T, object, c_1\wedge c_2\wedge\cdots\wedge c_i\wedge\cdots\wedge c_k)$，其中，$c_i\in Cc$；

(9) $\forall(p,0,object)\in CL,object\in object',(p,1,object')$ 在所有$CLi(1\le i\le n)$中共出现的次数为x，$(p, 0, object)$在所有$CLi(1\le i\le n)$中共出现的次数为y且$x+y=n$，则添加元素$(p, 0, object)$到$C_{\text{permissions2}}$；

(10)令 $Cc=\Phi$

$\forall(p,0,object)\in C_{\text{permission2}},(p',T',object',cons')\in CP_i(1\le i\le n),$若$object\in object'',\ (p'=p)\wedge((T'=0\wedge object'=object)\vee(T'=1\wedge object'=object'')),$计算$C_c=C_c\cup cons'$转换元素$(p, 0, object)$为$(p, 0, object, c_1\wedge c_2\wedge\ldots\wedge c_i\wedge\ldots\wedge c_k)$，其中$c_i\in Cc$；

(11) $\forall(u_i,p,object,cons,T)=False(1\le i\le n),$令$CD_i=CD_i\cup(p,T,object,cons)(1\le i\le n)$

(12)$CD=CD_1\cup CD_2\cup\ldots\cup CD_i\cup\ldots\cup CD_n$；

(13)令 $P_{\text{result}}=\phi$， $\forall r\in C_{\text{roles}},$若$(r,p)=True,P_{\text{result}}=P_{\text{result}}\cup p$

$P_{\text{result}}=(P_{\text{result}}\cup C_{\text{permission1}}\cup C_{\text{permission2}})-CD$

4 新产生信息访问控制

同步协同应用中，动态制定新产生信息的访问控制策略需要满足以下要求：(1)不能中断同步协同应用，策略制定方法需要方便、简单、快捷；(2)访问控制策略要合理、安全。

本文提出通过规则资源编码方法实现动态信息的访问控制。规则资源编码通过为新产生信息进行编码，系统依据编码规则自动识别资源并归类为某客体类对其进行控制。一般的编码结构具有 3 种形式，即树式结构、链式结构和混合式结构。树式结构阐述码位之间的隶属关系，重要特点在于能够建立资源之间的从属关系；链式结构为每个码位内的编码设置独立的含义，与前后码位无关，其编码信息量比树式结构少，编码和识别方便，结构简单；混合式结构把树式结构与链式结构融合为一体，兼备两种编码方式的优势。不同企业可以采用不同的编码规则，但为了实现对动态产生资源的控制，同步协同应用中编码规则需要满足以下需求：(1)编码规则应该能够对所有动态产生的系统资源自动命名；(2)通过编码规则，系统能够识别不同编码之间的关系，包括对隶属关系、并列关系的识别。

5 实现

课题组研究开发了网络化制造原型系统，在系统中能够进行小组协同会议，开展网络化协同批注、协同设计、协同装配、协同决策等同步协同应用。数据安全子系统是网络化制造原型系统的一个子系统，具有身份认证、访问控制、保密通信、系统监控等功能。本文提出的基本理论和方法已经在该系统中进行实施，系统在某研究所和企业分别进行了应用验证，并已通过专家组测试、验收和鉴定。

以某雷达产品的协同批注为例，在进行协同批注前，首先进行角色的定义、策略定义。为了进行协同批注，设计人员首先启动会议，会议启动过程中，依据同步协同应用访问控制结构，服务器应用共有权限求解算法计算获得共有权限并发送给所有的协作小组成员，协同客户端对协作成员的信息进行访问控制决策并提交给服务器。若协同客户端决策结果为拒绝资源请求，则系统将发送越权访问信息至服务器。为了防止信息泄漏，客户端不进行用户提示。对通信过程中的通信流量进行分析，结果显示应用本文提出的同步协同应用访问控制结构能够降低访问控制通信量 50%以上。

6 结束语

与一般应用系统不同，同步协同应用中的小组信息共享可能造成非法访问和信息泄漏。本文对同步协同中存在的问题进行了分析，针对同步协同应用中的越权访问问题、访问决策效率和新信息访问控制问题，提出了解决方案。文中提出的方案已在课题组开发的原型系统中实施并在企业中进行了应用和验证。

参考文献

1 Shen Honghai, Prasun D. Access Control for Collaborative Environments[C]//Proc. of Conference on Computer Supported Cooperative Work. 1992: 51-58.

2 Lee B G, Narayanan N H, Chang K H. An Integrated Approach to Distributed Version Management and Role-based Access Control in Computer Supported Collaborative Writing[J]. The Journal of Systems and Software, 2001, 59(2): 119-134.

3 Lei Hao, Huang Jian, Feng Dengguo. A Fine-grained Coalition Access Control Policy for Jointly-owned Resources in Collaborative Environments[J]. Journal of Software, 2005, 16(5): 1000-1011.

4 Sandhu R, Coyne E. Role-based Access Control Models[J]. IEEE Computer, 1996, 29(2): 38-47.

5 刘婷婷, 张友良, 汪惠芬. 语义驱动模式新型访问控制模型[J]. 计算机辅助设计与图形学学报, 2005, 17(9): 2078-2084.

（上接第 150 页）

分配的却是 D 函数的输出字节位这种对数据处理的不对称，因而产生了较好的仿真效果。

4 结束语

本文通过对 CPA 的分析，提出了一个基于 Walsh 谱的功耗分析模型，并通过仿真实验验证了这种模型在小明文样本空间下的的有效性，将 Walsh 谱和功耗分析结合在一起研究功耗分析与加密算法非线性函数的本质联系，证明了加密算法非线性度越高则其防范功耗分析的能力就越弱这个结论。

基于 Walsh 谱的功耗分析模型为对称分组密码系统的功耗分析和防范方法提出了一个新的研究途径。笔者将在如何更为精确地确定 τF 值上下限和证明 ghost peak 现象与加密算法非线性函数的本质联系方面继续展开研究工作。

参考文献

1 Kocher P, Jaffe J, Jun B. Introduction to Differential Power Analysis and Related Attacks[DB/OL]. (1998-08). http: //www. cryptography. com/ dpa/ technical/.

2 Kocher P, Jaffe J, Jun B. Differential Power Analysis[C]//Proc. of Advanced in Cryptology-CRYPTO'99, California, USA. 1999.

3 Brier E, Clavier C, Olivier F. Correlation Power Analysis with a Leakage Model[C]//Proc. of CHES'04. 2004: 16-29.

4 Messerges T S. Using Second-order Power Analysis to Attack DPA Resistant Software[C]//Proc. of CHES'00. 2000: 238-251.

5 Bevan R, Knudsen E. Ways to Enhance Differential Power Analysis[C]//Proc. of ICISC'02. 2002: 327-342.

6 温巧燕, 钮心忻, 杨义先. 现代密码学中的布尔函数[M]. 北京: 科学出版社, 2000: 9-19.