基于角色权限分配的协同电子政务访问控制模型研究

赵再军
(浙江大学电气工程学院 杭州 310027)

摘 要 首先分析了电子政务的协同性特点,阐述了多域协同工作环境下电子政务系统面临的安全问题。借鉴基于角色的访问控制思想,提出了基于用户、角色和权限分配的电子政务访问控制模型,通过引入权限期和作用域的概念,建立了角色和权限分配机制,描述了模型的运行机制,并就发生访问冲突情况下的调停问题给出了算法实现思想。最后以一项典型的政务活动——文件流转会签为例,具体说明了模型的使用方法,有效地解决了多域环境下电子政务的系统安全和信息保密问题。

关键词 电子政务,协同,角色,权限,访问冲突

Research on Collaborative E-government Model of Access Control Based on the Distribution of Role and Authority

ZHAO Zai-jun
(School of Electrical Engineering, Zhejiang University, Hangzhou 310027, China)

Abstract This paper first analyzed the collaborative characteristics of e-government, described the security problem e-government system facing in the environment of multi-domain collaborative work. To draw on the experience of role-based access control thought, we advanced the access control model of e-government based on the distribution of user, role and authority, through introducing the concept of authority period and effect scope, we established the distribution mechanism of role and authority, described the operating mechanism of model, and gave the thought of algorithm realization for conciliation problem in the situation of occurring access violation. Finally we gave a typical administrative activities-documents circulation countersigning for example, concretely specified the application method of model, effectively solved the problem of system security and information confidentiality for e-government in the multi-domain environment.

Keywords E-government, Collaboration, Role, Authority, Access violation

政府机构的工作性质决定了其所涉及的信息很多都带有机密性,尽管政府部门都是为国家工作的,但他们相互之间还有一个信息保密的问题。比如一个文件还在酝酿讨论过程中,就不可能对外发布或让其他部门知道。最典型的例子就是,国家在出台一项法规政策前,会经过多轮的征求意见阶段。可能会征求同级横向部门的意见,也可能征求下级纵向部门的意见。文件在征求意见阶段应该是处于保密状态的,除了直接当事人之外不能透露给别人,这就是政务活动中的信息保密问题。但在现实中,文件通过电子政务系统在这么多部门之间流转时很可能发生失泄密事件。如果泄密给内部人员也许不会造成太大损失,而一旦敏感信息泄露到外面或是被敌对分子掌握,就可能产生无法估量的负面影响。因此,协同电子政务中的信息安全和保密问题至关重要。

1 电子政务的协同性

电子政务是政府机构运用现代计算机技术和网络技术,将其管理和服务的职能转移到网络上完成,同时实现政府组织结构和工作流程的重组优化,超越时间、空间和部门分隔的制约,向全社会提供高效、优质、规范、透明和全方位的管理与服务。电子政务作为国家信息化建设的重点工程,充分利用现代网络技术,突破部门和区域限制,对于提高政府办公效率,增加政府办公透明度具有重要作用。而协同是不同组织的协作统一,步调一致,围绕同一任务进行高效的业务操作。从国家现实的政治生活来看,越来越多的政务活动无法在同一部门内完成,而是需要多个部门的协调配合。例如在当前国际金融危机的背景下,国家想要对某个行业(如交通运输业)进行基础设施投资,首先要通过国务院投资主管部门下达投资计划,再由行业主管部门具体落实投资和安排项目建设。投资主管部门在下达计划前必须事先与行业主管部门沟通协商,达成一致意见后才能落实这项工作。这就是两个部门之间的协同工作问题,这在政府机关中有一个标准称谓:会签。当然,一些更加复杂的政务活动可能需要多个部门共同会签来完成。在这样的背景下,我们完全可以把协同的思想应用到电子政务领域,将各个孤立的部门信息系统连通起来,将分散的数据资源整合起来,这就产生了协同电子政务。协同电子政务通过系统应用、部门流程再造以及信息的协同互动,可

到稿日期:2009-09-12 返修日期:2009-12-19
赵再军(1966—),男,硕士,高级工程师,主要研究方向为微机、单片机控制与逻辑电路设计。

以更大程度地发挥电子政务的优势和作用，是一种提供服务的崭新方式，它强调以政府工作人员的协作为核心，强化政府信息资源的共享、政府工作流程的优化以及政府信息化系统应用的集成，各种信息系统都与协同平台相互连接，以协同平台作为枢纽，形成紧密联系的整体，从而大大提升电子政务的整体效能。

2 电子政务系统的多域协同工作

为表述方便，将不同政府部门称为不同的“域”或“管理域”。随着政务活动的日益复杂化，电子政务系统间的互操作成为组织合作的一种重要形式，工作环境逐渐由单一管理域向多管理域转变，即所谓的协同工作。而不同管理域的安全策略各异，即不同政府部门都有自己的电子政务安全架构。图1是一典型的多域协同工作环境，其中涉及 A，B 和 C 3个域，每个域都有自己的安全策略，负责的工作内容也各不相同，他们之间又有合作关系。在方框所示的协同工作中，有一个子任务（虚线方框）涉及到不同管理域的用户，系统之间就需要进行互操作。与常规电子政务系统应用环境不同，协同工作环境为电子政务系统带来了新的安全挑战：如何进行有效的权限分配，使不同域在协同工作时既能够给正确的对方用户以相应权限，又能够保护与该项工作无关的信息不被对方用户获取，使系统在提供共享服务的同时有效地保护自己的资源？这个问题的核心是平衡资源保护与协同工作的矛盾，构架安全互信的协同工作环境。

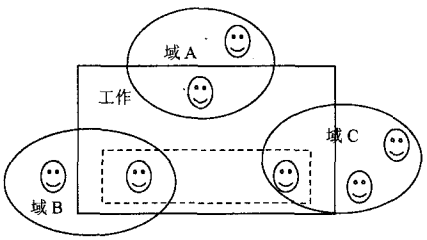

图1 多域协同工作环境示意图

目前，政府网络应用环境纷乱复杂，既有自动办公系统、文件流转系统、内部邮件等应用服务，又有众多面向下属单位、同级机构的对外应用。政府部门中的工作人员显然就是电子政务系统的用户，任何一个用户登录到系统以后，他们可以浏览的信息、可以进行的操作将完全被控制在他们的职权范围内，以保证政府信息不会被滥用。在政府机构中，用户的工作权限会随着工作任务的变化而变化，人员的流动也会造成信息系统用户的不断变化。在变化中，相对固定的是某个职位。当用户担任了一个新的职位，他就会负责相应的工作，拥有相应的权限。电子政务系统中可以把职位抽象为“角色”，这样对角色所拥有的权限也容易随时进行调整。对于部门人员发生调整、岗位出现变动等情况，电子政务系统也应具有相应的灵活的应对机制，要既能够保证不随原来人员的离去而带走权限，又能够使岗位继任者迅速取得相应权限。基于角色的访问控制方法恰好具有这种特性，即可以实现角色与权限的分离。我们完全可以借鉴这种基于角色的访问控制方法，解决协同电子政务中的信息安全问题。

3 协同工作环境下电子政务系统的访问控制模型

3.1 角色和权限分配

在多域协同工作环境下，电子政务系统的管理域分为3个层次，即用户层、角色层和权限层。以国家级政府机构为例，电子政务系统的用户（User，U）一般分为如下几类：部长级、司局长级、处长级、科员级。他们都是电子政务系统的用户，根据工作职责的不同和职位的高低具有不同的系统访问和操作权限。如某些机密或核心信息必须限定知晓范围，即仅由关键的几个核心成员知道；或者具有某项特殊工作职责的用户才能看到某些信息，如某司局的秘书才能知道部委领导的当日工作日程。角色层是对用户的抽象，即对于某一项具体的协同工作任务，来自不同管理域的用户分别在其中承担不同的角色（Role，R）。在权限（Authority，A）层，引入生存期（Time，T）和作用域（Domain，D）的概念。生存期即指该项权限存续的时间，一般以任务完成为终结。作用域是指权限的主体许可范围，对于特定的权限，限定只有作用域中的主体才能拥有和激活权限。生存期是从时间角度规定了角色的权限，而作用域则从空间角度规定了角色的权限。这样，一项权限分配过程就可以描述为：

$$A(T,D)\rightarrow R$$

该式描述了某个角色所拥有的权限及其时间和空间作用范围。相应地，一项协同工作 CT 可以用一个二元组表示为：

$$CT=\langle U,R,A(T,D)\rangle$$

式中，U，R 分别代表要完成这项协同工作拟参与的用户集及其角色，$A(T,D)$ 代表对每个角色权限的详细规定，即权限期和作用域集。此外，在角色和权限分配过程中还要注意以下原则：（1）对用户进行最小权限控制，即用户被分配的权限不能超过完成其职责所需的最小权限；（2）进行互斥角色的约束性监测，以保证一个用户最多只能属于一组互斥角色中的某一个，否则会破坏职责分离原则。权限分配也有互斥约束，同一权限只能授予互斥角色中的某一个；（3）对角色容量的限定，即一个角色对应的用户数目也要根据角色本身的特点进行限定。

3.2 访问控制模型

在定义角色和权限分配机制的基础上，借鉴基于角色的访问控制（RBAC）原理，本文提出了一种支持多域协同工作的电子政务访问控制模型，如图2所示。该模型以一项需要两个域的不同用户完成的协同工作为例。首先由该项协同工作的管理者完成把用户委派给角色的过程，例如，工作管理者根据工作任务需求对域 A 的用户进行角色定义，用户取得相应角色1；对域 B 的用户进行角色定义，用户取得相应角色2。再由技术人员完成配置权限到角色的过程，即由电子政务系统的技术管理者为角色1分配权限1，对角色2分配权限2，使二者获得可进行相应操作的权限，然后允许其进入电子政务系统进行相应操作。对于需要多个域的用户共同完成的协同工作与此类同。该模型有两个优点：一是分配机制灵活。通常在一个具体的系统中，角色/权限之间的变化比角色/用户之间的变化慢得多。如果业务管理者临时决定由另一个人进行这项工作，那么就可以取消对原用户的角色定义，转而将用户 B 定义为角色1，而技术管理者不必重新进行权限分配，事实上，技术管理者并不关心谁是角色1，他的职责就是为角色1分配正确的角色，这样就实现了用户与权限之间的独立，从而大大提高了系统运行效率。二是提高了系统运行的安全性。用户角色和权限的不同主要是因为在整个工作流程中用

户所处的工作任务的不同。换言之，在工作流程中若存在着互斥的工作任务，则将直接决定处理这些任务的用户角色的互斥。这种访问控制机制使业务领域的角色分配与技术领域的权限分配完全隔离开来，可有效防止电子政务系统由于权限被滥用而引发的信息泄露问题。

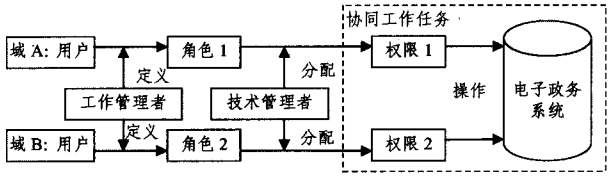

图 2　协同工作环境的访问控制模型

3.3　访问冲突调停

在多域环境中，用户可能来自不同的管理域，跨域用户的授权不仅受指派角色的影响，还受权限的作用域和生存期限制，只有用户在权限的作用域且权限处在合适的时间阶段中，用户才能使用其指派角色拥有的权限。本文提出的访问控制模型就是通过对权限存续时间 T 以及作用范围 D 的有效控制来达到对用户及角色的控制，从而控制信息的知悉范围。举个例子，要起草一份综合性文件稿，涉及到 3 个部门的职责，一般做法是有一个主办部门执笔，另外两个部门提供基础资料。主办部门初稿完成后要征求其他两个部门的意见，达成一致后报各自部门领导会签，然后进入发文程序。在这项协同工作中，有 3 个用户即主办部门负责这项工作的个体或群体，以及另外两个部门参与这项工作的个体或群体。相应的有两类角色，即起草者角色和征求意见者角色。这两类角色的权限是不同的，起草者角色可以对文稿通篇进行修改，而征求意见者角色只有权对他所负责的部分内容进行修改，即这两类角色的作用域不同。如果征求意见阶段已过，再有意见也无法对文件稿进行修改了，也就是征求意见者角色所拥有的权限已经失去了生存期，无法再进入系统进行操作。

但实际运行中可能发生这样的现象，即文件尚未流转到某用户，但他提前进入了系统想进行操作。而这时文件可能正由别的用户操作，因此就发生了所谓的访问冲突。一个健壮的电子政务系统必须具有这种访问冲突调停机制。下面给出本文提出的访问控制模型的冲突检测与调停算法思想。

输入：某项授权 a(t,d)及协同工作的完整信息 CT=〈U,R,A(T,D)〉
输出：判断结果或调停结果

```
For every a 属于 A
    If t 不属于 T then
      终止对 a 的权限期授权；
      提示“未到或已过授权期!”；
    Elseif
      Next t；
    Endif
    If d 不属于 D then
      终止对 a 的作用域授权；
      提示“不具有操作权限!”；
    Elseif
      Next t；
    Endif
Endfor
```

4　实例应用——以文件流转会签为例

文件会签是公文流转的重要内容，也是政务活动的重要内容之一。电子政务系统一般都包括这项功能。本文以一项需要在多个部委之间会签的文件流转工作为例说明模型的运转方式。文件会签通常需要多个岗位、多个人对同一份文件进行处理，这就是一项协同工作。在文件以电子文件形式流转过程中，必须防止用户的恶意篡改或窃取文件的内容，知悉范围要严格限定在规定的范围之内。由于文件需在不同的岗位之间流动，使得对文件的跟踪和监控变得非常困难。

一项典型会签工作的流程是：首先由域 A 的起草人在起草公文后提交处长（副处长）审签。处长察看文档后，一般情况是填写处室意见，然后可以提交下一位处长或者提交给本域领导，不同意则返回。域 A 领导察看文档后，一般情况是填写领导意见，然后可以提交下一位领导或交办公室走会签程序，不同意则返回给前一位处理人。办公室收到经过本域领导审定的文件后按顺序将文件流转到其他域会签，同时对其他域进行权限分配。会签流程如图 3 所示。

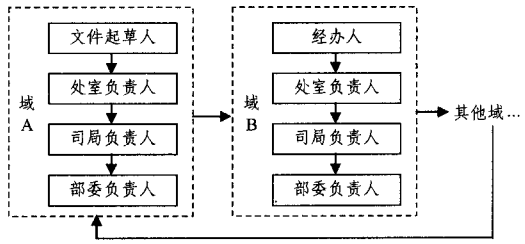

图 3　会签工作流程示意图

(1)角色设计。上述会签工作流程需要设置 3 个角色：起草角色、审核角色和会签角色，其中，起草角色和审核角色在同一域中，而会签角色则分布于其他域中（一个或多个，视该文件需要会签的域而定）。

(2)权限分配。当一个文件开始进入系统后，负责文件运转的工作管理者（可以是部门或个人）将该文件拟经过的用户及其权限一并封装在工作中。该管理者不需了解文件的具体内容，而只需知道当前状态下的公文应由谁处理，具有什么处理权限。这也从一定程度上防止了文件信息的泄密。

(3)在用户访问文件之前，技术管理者对用户的角色和权限进行判断，只有通过认证的用户才能访问文件。步骤如下：

①由已赋予角色的用户输入用户名和密码；

②检测用户名和密码，确认用户的合法身份。如果用户身份合法，则从数据库中获取该用户的角色集和用户的权限集，否则退出，提示用户非法；

③根据用户权限集，在系统菜单列表中查找出菜单类型的权限，形成菜单列表，并将菜单列表显示到客户端。

(4)在用户处理文件的过程中，系统对用户的行为进行实时的监控。处理完毕后，系统可根据用户的需要调用相应的签名机制对用户所做的处理部分进行签名，使用户对文件的修改具有不可否认性。工作步骤如下：

①根据该用户的角色信息，查找该用户的任务信息和基于任务的权限信息；

②按照任务信息的流程号，形成一个完整的工作流程；

③根据工作流程，执行流程上的有执行权限的任务。

(5)会签完毕的文件最终要回到域 A，因为作为文件的始作俑者，域 A 对该文件负有发文义务。

参 考 文 献

[1]　文家福，王嘉祯，刘爱珍. 基于角色的属性证书及其权限认证策略[J]. 科学技术与工程，2006(16)

（下转第 250 页）

Step7　$n=n+1$，进一步减小搜索空间，转 Step4；

Step8　停止搜索，比较所有的综合性能函数值，得出 J 的最小值，其对应权参数值为当前最优的$\hat{Q}^*$，$\hat{R}^*$。

3.2　二级倒立摆实时控制

实际系统中，将表 1 中的参数代入二级倒立摆线性化模型式(2)。取采样周期为 0.05s，式(12)中 $\beta_0=0.5$，其终止条件取 $\beta_n\leqslant10^{-3}$，$\gamma=0.002$，综合性能式(8)中 $a=0.2$，$b=0.3$，$c=0.5$；给定各输出：摆 1 为 $\theta_1=-3.14(rad)$，摆 2 为 $\theta_2=-3.14(rad)$，小车位移 $r=0(m)$。混沌细搜索共进行 6213 步，在 158 步得到系统全局最优的权矩阵 Q，R，进而得到系统的最佳动态性能的负反馈增益矩阵 K：

$K=[17.3312\quad 116.5826\quad -194.6134\quad 18.5759$

$3.5457\quad -31.4390]$

使用以上混沌优化权矩阵参数的 LQ 控制器。

通过搭建二级倒立摆控制系统的模块，选择采样时间 5ms，实现了直线式二级倒立摆系统的稳定控制。二级倒立摆系统 LQ 实时控制结果如图 2－图 4 所示。

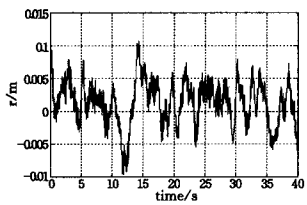

图 2　小车位置的实时控制曲线

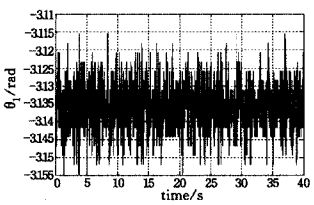

图 3　摆 1 角度的实时控制曲线

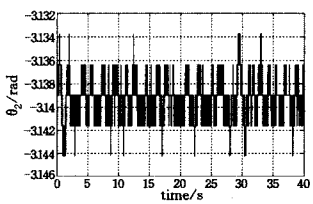

图 4　摆 2 角度的实时控制曲线

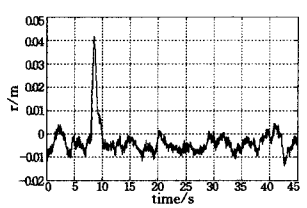

图 5　加扰动后小车位移曲线

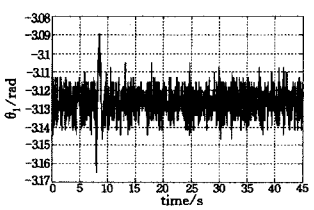

图 6　加扰动后摆 1 角度曲线

试验中，等待系统稳定以后，在大约 8s 给摆 2 摆杆加一个接近 8°的扰动，二级摆杆角度偏差在 2s 左右恢复到垂直状态，小车位移也很快回到零位置如图 5－图 7 所示。结果证明，文中所提的控制策略不仅能稳定控制二级倒立摆系统，而且具有很强的抗干扰能力。

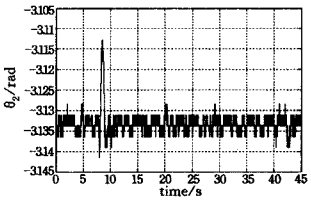

图 7　加扰动后摆 2 角度曲线

结束语　(1) 本文在综合考虑小车位移、下摆角度、上摆角度的重要程度，引入一种与系统动态性能、稳定性密切相关的性能指标基础上，采用混沌全局粗搜索和局部细搜索相结合优化 LQ 控制器，实现了二级倒立摆的实时控制。(2) 它不但使系统具有良好的稳定性，而且抗干扰能力强，为具有快速、强非线性、绝对不稳定系统的控制问题提供通用的方法。

参 考 文 献

[1] 张葛祥，金炜东，胡来招. 多变量系统控制器的参数满意优化设计[J]. 控制理论与应用，2004，21(3)：362-366

[2] 刘丽，何华灿. 倒立摆系统稳定控制之研究[J]. 计算机科学，2007，33(5)：214-219

[3] Rubi J，Rubio A，Avello A. Swing-up control problem for a selferecting double inverted pendulum[J]. IEE Proceedings-control Theory and Application，2002，142(2)：167-175

[4] 岳大志，吴刚. 基于视频的倒立摆摆起控制[J]. 计算机科学，2007，34(7)：214-216

[5] Cheng F Y，ZHong G M，Li Y S. Fuzzy control of a double inverted pendulum[J]. Fuzzy Set and Systems，1996，76(3)：315-321

[6] 李明爱，阮晓刚. 基于连续 Hopfield 网络的多变量时变系统最优控制[J]. 控制与决策，2005，20(9)：1038-1044

[7] 王仲民，孙建军，岳宏. 基于 LQR 的倒立摆最优控制系统研究[J]. 工业仪表与自动化装置，2005，3：6-8

[8] 黄卫忠，高国琴. 基于遗传算法的最优控制加权阵的设计[J]. 计算机测量与控制，2003，11(10)：761-763

[9] 邓莉，鲁瑞华. 一种改进的抑制早熟的模糊遗传算法[J]. 计算机科学，2007，34(11)：150-153

[10] 李献礼. 利用遗产算法解决非线性系统优化问题[J]. 计算机科学，2003，34(10)：217-219

[11] 李生权，张绍德. 基于混沌变量的 LQR 控制器权矩阵优化设计[J]. 传感器与微系统，2007，12(26)：88-90

[12] http://www.googoltech.com.cn/Web/chi/main.jsp#

(上接第 145 页)

[2] 张远林. 论中国电子政务的发展[D]. 武汉：华中师范大学，2004

[3] 王西点，吴琦. 电子政务中实现授权及访问控制的研究[J]. 计算机与通信，2004(7)

[4] 李成锴，詹永照，茅兵，等. 基于角色的 CSCW 系统访问控制模型[J]. 软件学报，2004，11(7)：931-937

[5] 刘婷婷，王惠芬，张友良. 支持授权的基于角色的访问控制模型及实现[J]. 计算机辅助设计与图形学学报，2004(4)：39-41

[6] 于森，王延章. 基于角色网络模型的电子政务系统框架的研究与实现[J]. 计算机工程与应用，2003，12(31)：31-35

[7] 蔡立辉. 电子政务：信息时代的政府再造[M]. 北京：中国社会科学出版社，2004：56-57

[8] 林培光，徐如志. 一种新的电子政务“一站式服务”框架[J]. 微电子与计算机，2008(6)：119-122

[9] Wilikens M，Feriti S，Sanna A，et al. A context-related authorization and access control method based on RBAC[C]// Seventh AMC Symposium on Access Control Models and Technologies. Monterey，California，2002：117-124

[10] 向宏，艾鹏，刘嘉伟. 电子政务系统安全域的划分与等级保护[J]. 重庆工学院学报：自然科学版，2008，22(2)：99-103