

# 电子政务系统中角色网络扩展模型研究 \*

彭 友, 王延章, 王 宁, 叶 鑫

(大连理工大学 管理与经济学部, 辽宁 大连 116024)

**摘 要:** 从当前角色网络模型(RNM)所存在的问题入手,通过加入时限约束和解决角色间继承关系上的缺陷对角色网络模型进行改进,并进一步提出基于时限约束的角色网络模型(TRNM)。该模型在继承角色网络模型全部优势的同时,一方面解决了原有 RNM 中角色间继承关系上的缺陷,使高层角色可以部分继承底层角色的权限;另一方面则通过对时限约束特征的定义和分析,给出了在时限约束条件下 TRNM 的组成成员和形式化描述,最后具体给出了 TRNM 的开发方法流程。

**关键词:** 角色网络模型; 基于时限约束的角色网络模型; 信息安全; 电子政务

**中图分类号:** TP311      **文献标志码:** A      **文章编号:** 1001-3695(2012)02-0569-03

doi:10.3969/j.issn.1001-3695.2012.02.044

## Research of role-based network extended model in e-government

PENG You, WANG Yan-zhang, WANG Ning, YE Xin

(Institute of Information Technology & Decision Support, Dalian University of Technology, Liaoning Dalian 116024, China)

**Abstract:** For the purpose of solving the current problems in the role-based network model(RNM), this paper improved RNM from two aspects: time constrained, and the inheritance relationship between roles. And it realized the time constrained role-based network model (TRNM) based on the improved RNM. This model not only inherited all the advantages of RNM, but also provided time constrained and the proper inheritance relationship between roles. This paper specified the development methods about TRNM in the end.

**Key words:** role-based network model(RNM); time-constrained RNM; information security; E-government

## 0 引言

基于角色的访问控制模型(RBAC)的出现,不但改善了传统的访问控制模型中的任意性和强制性(DAC和MAC),而且为解决分布式环境下的访问控制问题提供了便利。电子政务系统作为当前信息化建设中最为重要的领域之一,如何利用RBAC模型以改善自身在权限管理中的不足是目前国内外专家研究工作的重点。通过对电子政务系统长期的开发和研究,作者认为相对于其他信息系统,电子政务系统具有如下特点:

a) 电子政务系统具有强烈的社会科学和自然科学交叉性。相对于其他信息系统单纯在技术层面上的追求,电子政务系统对于其操作主体——人及人所延伸出来的如权利、责任、能力、人与人之间的关系等主观属性的分析和建模同样重视。

b) 电子政务系统业务和服务对象的独特性。相对于其他服务于各大企业的信息系统,电子政务系统并不过分关注于客户的差异和企业的回报,而是强调人的平等权和对整个社会的服务意识,并渗透着对实际业务的深层次分析和对功能的全方位支持。

c) 电子政务系统要具有相当的管理能力、工作流程控制能力和对意外情况的紧急响应能力。由于电子政务系统实际

业务的要求,所以要求其必须在这方面具有比其他信息系统更强的应变处理能力。

基于以上分析,如何针对RBAC模型进行扩展以使其更好地适应电子政务系统自身的特点是笔者研究工作的重点。近年来,王延章等人<sup>[13]</sup>基于系统理论和角色理论提出角色网络模型(role-based network model, RNM),其良好的时空特性既符合电子政务系统自身的特征,也对其业务流程的优化和自主平台的开发提供了支持,因此在很多城市的电子政务系统中得到了广泛的应用。但是通过对具体业务的大量研究,笔者发现当前的RNM主要存在两方面的不足:a) RNM并没有考虑时限约束对其的影响,这样就需要安全管理员根据用户的要求随时地产生和撤销角色,如果不能及时处理,就可能导致权限管理出现混乱;b) RNM在处理角色间的继承关系上还只能做到高层角色对底层角色权限的全部继承,这种单一的继承方式在实际业务的处理上会产生很大的局限性。针对上述问题,本文从上述两个方面对角色网络模型进行了扩展,并提出了基于时限约束的角色网络模型(time constrained RNM, TRNM)。TRNM一方面解决了原有RNM中角色间继承关系上的缺陷,使高层角色可以部分继承底层角色的权限;另一方面则通过对时限约束特征的具体分析和定义,给出了在时限约束条件下TRNM的

**收稿日期:** 2011-08-21; **修回日期:** 2011-09-22      **基金项目:** 国家自然科学基金重点攻关项目(91024029); 国家“十一五”科技支撑计划应急平台重大项目子课题(2006BAK01A)

**作者简介:** 彭友(1981-),男,黑龙江哈尔滨人,博士研究生,主要研究方向为系统工程、复杂信息系统整合、信息安全等(penggote2008@yahoo.cn);王延章(1952-),男,辽宁大连人,教授,博导,博士,主要研究方向为复杂信息系统整合、决策支持、电子政务等;王宁(1973-),男,吉林白城人,副教授,博士,主要研究方向为电子政务、决策支持系统等;叶鑫(1978-),男,辽宁本溪人,副教授,博士,主要研究方向为电子政务、决策支持系统。



2.1 TRNM 的组成成员和形式化描述

首先给出 TRNM 组成成员定义:

定义 4 TRNM 可以表示成一个五元组 (USR,ROL,PER,SESS)。其中各元素分别为下列基本集合:USR (用户集合),ROL (角色集合),PER (业务对象集合),SESS (会话集合)。

定义 5 用户集合 USR,表示系统中用户集合。USR = (ORG,TEAM,INF),其中 ORG 表示用户当前所处的组织,TEAM 表示以任务或者职能来划分的不同职能部门所组成的动态团队,INF 则是用户相关个人信息的集合。

定义 6 角色集合 ROL,表示组织系统中角色的集合。 $ROL = \{rol_1,rol_2,\cdots,rol_n\}$ , $rol_i(i \in \{1,2,\cdots,n\})$  为系统中相应的第  $i$  个角色, $n$  表示系统中的角色总数。角色是构成组织系统的基本要素,是权利和义务的集合体,各种形式的授权最终也是通过角色来实现的。角色与角色之间具有层次结构关系,体现了其组织结构中的职能联系,并基于此构成了一个层次化的角色网络结构。将角色定义为  $ROL = (RIGHT,DUTY,RELATION,TYPE)$ 。其中,RIGHT 表示角色的权限,包括可以执行哪些业务对象,通常是对角色允许发生的特定行为的描述;DUTY 表示角色的义务,包括角色必须执行或者必须禁止执行的某类业务对象,通常是对角色特定行为的描述;角色与角色之间的各种关系是通过 RELATION 来表示的,表 3 给出了角色间常见的七种关系;TYPE 表示角色的类型。

定义 7 业务对象集合,PER = (NAME,PROP,OPERA,RELATION,RULE)。其中,NAME 代表业务对象名称,PROP 是业务对象属性集集合,OPERA 代表业务对象操作集算子集合,RELATION 表示业务对象操作集算子的关系集集合,RULE 表示业务对象操作集算子的规则集集合。

表 3 角色间的七种关系

| 关系类型                                       | 关系表述                                                                                                                                                                                                                                                                                                                                                 |
|--------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 相等关系 EQU:两个角色可以相互替换                        | $(\forall rol_1)(\forall rol_2)(rol_1 \in ROL \wedge rol_2 \in ROL \wedge rol_1 EQU rol_2) \rightarrow rol_2 EQU rol_1$                                                                                                                                                                                                                              |
| 排它关系 EXLD:两个角色互斥,不能在同一用户中存在                | $(\forall rol_1)(\forall rol_2)(rol_1 \in ROL \wedge rol_2 \in ROL \wedge rol_1 EXLD rol_2) \rightarrow rol_2 EXLD rol_1$                                                                                                                                                                                                                            |
| 包容关系 CTN:一个角色涵盖另一个角色                       | $(\forall rol_1)(\forall rol_2)(\forall rol_3)(rol_1 \in ROL \wedge rol_2 \in ROL \wedge rol_3 \in ROL \wedge rol_1 EQU rol_2 \wedge rol_2 CNT rol_3) \rightarrow rol_1 CNT rol_3$                                                                                                                                                                   |
| 重叠关系 OVLP:两个角色存在职责上的交叉                     | $(\forall rol_1)(\forall rol_2)(rol_1 \in ROL \wedge rol_2 \in ROL \wedge rol_1 OVLP rol_2) \rightarrow rol_2 OVLP rol_1$                                                                                                                                                                                                                            |
| 分离关系 SPRT:两个角色毫不相关,不存在职责上的交叉               | $(\forall rol_1)(\forall rol_2)(rol_1 \in ROL \wedge rol_2 \in ROL \wedge rol_1 SPRT rol_2) \rightarrow rol_2 SPRT rol_1$                                                                                                                                                                                                                            |
| 全连通继承方式:高层角色继承底层角色的全部权限                    | $\forall p, \exists (R_x \geq R_y) \wedge can\_be\_acquired(p, R_y, t) \rightarrow can\_be\_acquired(p, R_x, t)$                                                                                                                                                                                                                                     |
| 非连通继承方式:高层角色不继承底层角色的任何权限,但是高层角色的用户可以激活底层角色 | $\forall p, \exists (R_x \geq R_y) \wedge can\_be\_acquire(p, R_y, t) \rightarrow can\_not\_acquire(p, R_x, t)$<br>$\forall u, \exists (R_x \geq R_y) \wedge can\_activate(u, R_x, t) \rightarrow can\_activate(u, R_y, t)$<br>$\forall u, \forall p, can\_activate(u, R_y, t) \wedge u\_assigned(u, R_y, t) \rightarrow can\_acquire(u, R_y, p, t)$ |

TRNM 的形式化描述如下:

- a)  $UAO \subseteq USR \times ROL$ ,用户与角色之间多对多映射关系;
- b)  $RLPR \subseteq ROL \times PER$ ,权限与角色之间多对多映射关系;
- c)  $UAOT \subseteq USR \times ROL \times CONT$ ,在时限约束条件下的用户与初始角色之间的多对多映射关系;
- d)  $RLPRT \subseteq ROL \times PER \times CONT$ ,在时限约束条件下的权

限与角色之间的多对多映射关系;

e)  $USR - (rol,t) = \{u | (\exists r' \geq r)((u,r',cont) \in UAOT) \cap (t \in cont)\}$ ,在时刻  $t$  具有角色  $rol$  的所用用户的集合;

f)  $rol(usr,t) = \{r | u \in USR(r',t), r' \geq r\}$ ,在时刻  $t$  用户  $usr$  所具有的所有角色。

g)  $RH \subseteq rol \times rol$ ,角色层次,定义在角色集上的一种偏序关系,称为角色层次。

2.2 TRNM 的开发方法流程

在网络技术广泛应用和政府组织不断扁平化、网络化的今天,角色网络模型有着天然的优势,特别适用于复杂的组织协作型的电子政务系统。通过归纳,笔者认为 TRNM 的开发方法主要流程包括:

- a) 制定政府组织目标。也就是要根据政府组织的任务以及内外环境条件制定政府的发展目标,然后在此基础上确定政府组织设计的基本思路、组织结构的基本模式,规定设计的主要规则。
- b) 部门划分、职能分解。根据政府组织目标和任务来确定政府组织实现目标的活动,并在此基础上把所有的工作进行分类;然后根据分类来关联职能部门。
- c) 部门职责权限的分配。根据部门的主要职责、权利、条件和关系到部门间的联系,可以自顶向下,也可以自顶向上地配置部门的权限。最后确立政府组织框架(组织图)、组织管理制度文件。
- d) 工作活动的角色逻辑编组。根据部门的职责权利、一系列的相关工作,为了实现专业化和提高效率,需要对工作活动关系进行分组。分组的程序一般为同种、同类划分并计算工作量。

e) 岗位设定与确定用户。根据一组工作量、难易程度设定岗位并配置用户,最后确立岗位任务、工作程序、遵守的规则、工作结果的标准文件。

f) 运行机制与反馈。也就是说,不仅要考虑组织的静态结构,而且要考虑组织的正常、异常运行机制。通过不断地反馈、循环完成电子政务系统的设计过程。

g) 电子政务系统的实施。

TRNM 的开发方法流程如图 2 所示。

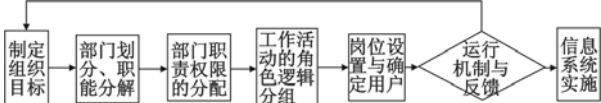


图2 TRNM的开发方法流程

3 结束语

通过 TRNM 的确立,建立了相应电子政务系统的体系结构,并通过它完成了电子政务建设大型项目“辽宁省党政信息网”的主体软件工程部分。目前“辽宁省党政信息网”已正式开通,其软件部分取得了很好的应用效果,得到各方面的好评,并在辽宁省的 14 个地市中推广,推广活动正在顺利进行中。TRNM 充分渗透和体现了对电子政务系统的业务和环境的深层分析,并能适应复杂多变的业务流程,同时还可以对组织中角色进行有效的监控,从而有效提高电子政务系统的管理效率和质量。因此,本文的研究也对构建其他各类信息系统具有一定的现实意义和普遍意义。

b) 对子节点含样本类别数进行判断,所有样本的类别数都不大于 2,则转到步骤 d),否则转到步骤 c)。

c) 对各节点中类别数大于 2 的节点调用遗传粒子群算法聚类分析,转步骤 b)。

d) 结束循环,生成最优二叉树的朴树结构,根据朴树结构训练生成多分类 SVM。

3 实例应用结果与分析

本文所有的实验都是在 PC P4 T2310 1.86 GHz,2 GB RAM, Intel82865G 显卡的计算机上做的实验,利用人造数据进行仿真模拟来验证本文提出算法的有效实用性,通过样本集证明了算法的有效性。本文以桑塔纳轿车为例,采用本文算法对汽车故障进行仿真分析,图 1 给出了按照算法计算的分类精度编号情况,图 2 是本文方法故障特征识别图。从图 2 中可以明显发现,随着汽车故障特征的增加,故障的识别精度也呈递增趋势,这充分说明经本文提出的粒子群分层聚类优化支持向量机算法可以选择较少的故障特征而达到更高的分类精度,算法对汽车故障特征识别能力非常高。

需训练的二分类支持向量机个数为 45 个,测试时需要遍历所有的子分类器,本文方法只需训练 9 个二分类支持向量机,测试时遍历个数不大于 5 个,对训练和分类复杂度比较如表 1、2 所示。

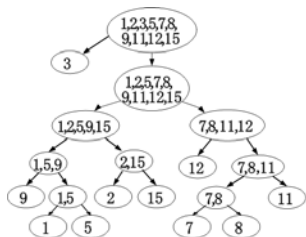


图1 最优决策树

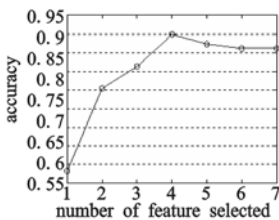


图2 故障特征识别

表 1 训练和分类复杂度比较

| 分类            | 传统算法 | 本文方法 |
|---------------|------|------|
| 需训练 SVM 的数目   | 45   | 9    |
| 分类遍历 SVM 平均数目 | 45   | ≤5   |

表 2 诊断结果

| 分类       | 传统支持向量机 | 本文方法  |
|----------|---------|-------|
| 测试时间/s   | 0.9     | 0.4   |
| 训练正确率/%  | 96.5    | 97    |
| 测试正确率/%  | 96      | 96.5  |
| 样本总正确率/% | 96.25   | 96.75 |

(上接第 571 页)

参考文献:

[1] 于森,王延章.一种基于角色网络模型的电子政务系统框架及其实现研究[J].计算机工程与应用,2003,39(12):31-35.  
[2] 叶鑫,王延章.电子政务的层次角色网络模型研究[J].系统工程学报,2006,22(2):216-220.  
[3] 叶鑫,王延章.基于角色模型的行政事务处理系统建模方法研究[J].计算机应用研究,2005,22(6):44-46.  
[4] 王宁,于森,王延章.面向电子政务领域的角色网络模型[J].系统工程,2007,25(2):7-10.  
[5] 王延章,高国伟,于森,等.信息系统中的角色网络模型和方法研究[J].计算机应用研究,2008,25(10):3116-3118.  
[6] 许永涛,王延章,陈雪龙.基于角色网络理论的政府办公自动化系统开发平台的研究与实现[J].计算机应用研究,2007,24(2):

如表 1、2 所示,本文方法与传统的支持向量机相比,分类正确率相当,诊断时需要遍历的二值 SVM 个数却大大减少,减少了测试时间,提高了测试效率。

4 结束语

本文提出了一种基于粒子群算法优化层次支持向量机汽车故障诊断检测方法。针对分解支持向量机具有测试时间短、结构难以确定的特点,本文利用粒子群算法,依据最大间隔距离原则优化层次支持向量机模型,使每个节点的支持向量机具有最大分类间隔,减少了误差积累,从而优化了多级二叉树结构的 SVM,实现故障的分级诊断。仿真实验结果表明,本文提出的算法在所有参比模型中精度最高,能高效地对汽车系统的故障进行检测与定位,具有较强的泛化能力,同时缩短了故障诊断时间。

参考文献:

[1] 范贵生,虞慧群,陈丽琼,等.基于 Petri 网的服务组合故障诊断与处理[J].软件学报,2010,21(2):231-247.  
[2] 李惠,崔成玲,李新宏.柔性制造系统中 CNC 机床故障诊断机理研究[J].计算机应用研究,2009,26(8):2982-2984.  
[3] 徐滔,王祁.一种神经网络预测器在传感器故障诊断中的应用[J].传感技术学报,2005,18(2):235-236.  
[4] 王源,胡寿松.基于支持向量机的非线性系统故障诊断[J].控制与决策,2001,16(5):617-620.  
[5] 张怡哲,邓建华.舵面损伤在线故障模式预测及故障检测[J].西北工业大学学报,2011,21(3):299-300.  
[6] 王罗,张桂新,陈特效.回归型支持向量机在电机故障诊断中的研究[J].计算机测量与控制,2007,15(12):1691-1694.  
[7] 桑海峰,何大阔,张大鹏.基于支持向量机与遗传算法的发酵过程软测量建模[J].东北大学学报,2010,28(6):781-784.  
[8] LIN C F, WANG S D. Fuzzy support vector machines[J]. IEEE Trans on Neural Networks,2009,13(2):464-471.  
[9] WANG T Y, CHIANG H M. Fuzzy support vector machine for multi-class text categorization[J]. Inform Process Manag,2010,43(4):914-929.  
[10] 刘本德,胡昌华,蔡艳宁.基于聚类和 SVM 多分类的容差模拟电路故障诊断[J].系统仿真学报,2009,21(20):6479-6482.

209-211.  
[7] JOSHI J B D, AREF W G, GHAFOR A, et al. Security models for Web-based applications[J]. Communications of the ACM,2001,44(2):38-72.  
[8] JOSHI J B D, BERTINO E, GHAFOR A. Hybrid temporal role hierarchies in GTRAC[J]. ACM Trans on Information and System Security,1999,2(1):3-33.  
[9] CRAMPTON J, KHAMBHAMMETTU H. Delegation in role-based access control[C]//Proc of the 11th European Symposium on Research in Computer Security. Hamburg: Springer, 2006:174-191.  
[10] WAINER J, KUMAR A. A fine-grained, controllable, user-to-user delegation method in RBAC[C]//Proc of the 10th ACM Symposium on Access Control Models and Technologies. New York: ACM Press, 2005:59-66.