基于神经网络的访问控制策略优化模型

李肯立 康 强 唐 卓 沙行勉 杨 柳
(湖南大学计算机与通信学院 长沙 410082)

摘 要 访问控制是网络安全防范和保护的主要核心策略,其主要任务是保证网络资源不被非法使用和访问。将风险概念引入访问控制,分析了基于风险的权限委托以及权限再分配的基本性质;基于MUS集合的计算方法,给出了一种基于神经网络的风险评估方法。针对神经网络适合定量数据,而风险因素的指标值具有很大的不易确定性等问题,采用模糊评价法量化信息安全的风险因素指标,对神经网络的输入进行模糊预处理。仿真结果表明,模糊神经网络经过训练,可以实时地估算风险因素的级别。

关键词 访问控制,风险评估,神经网络,模糊神经网络

Access Control Policy Optimization Model Based on Neural Network

LI Ken-li KANG Qiang TANG Zhuo SHA Xing-mian YANG Liu
(School of Computer and Communications, Hunan University, Changsha 410082, China)

Abstract Access control is the main core policy of network security and protection, and its main task is to ensure that network resources are not illegal use and access. Pulling the concept of the risk into access control, analysed delegate permissions based on risk and the basic nature of permissions of redistribution, and the calculation based on MUS collection, proposed a risk assessment based on neural network. Since the neural network is suited for the quantity data processing, and the risk factors are of great uncertainty, the risk factors of information security were quantized by fuzzy evaluation method and the input of neural network was pretreatmented. The simulation results show that the trained neural network can estimate the degree of risk factor real time.

Keywords Access control, Risk assessment, Neural network, Fuzzy neural network

1 引言

访问控制的主要任务是保证网络资源不会被非法使用和访问,它是进行网络安全防范和保护的主要核心策略,也是网络安全最重要的核定策略之一。然而分布式工作流系统、网格计算,乃至当今热门的云计算均具有很大的动态性和不确定等特点,使得系统之间往往有许多个用户、角色、权限之间的指派方案,因此有必要寻找一种最优的访问控制策略的配置方案,使其既能满足最小权限原则,又能有更好的安全性。在动态进行访问控制的时候,将其访问控制的风险[1]这一属性考虑进来,以提高系统的安全性。

Marsh[2]等将经济学中的"效用"这一概念引入访问控制。B. Aziz[3]提出了一种基于风险的访问控制策略调整方法,该调整方法只是提及了降级风险的思路,并没有给出一个具体的调整访问控制策略的方法。

风险这一访问控制因素,它的值具有很大的不易确定性等。风险评估可以采用层次分析法、决策树法以及概率分析法等。它的评估方式分为定性评估方法、定量评估方法和定性与定量相结合的评估方法3大类。风险评估具有复杂性、非线性、不确定性、强实时性等特点,局限性大,而且评估具有很大的主观臆测性等,操作起来也比较复杂。与常规方法相比,人工神经网络方法具有人类智能特性、非线性、自学习和自组织能力,从而可以解决不确定性问题。采用模糊评价法量化访问控制的风险属性,对神经网络的输入进行模糊预处理,可以实时地估算风险属性的级别。

本文使用BP(Back Propagation)网络[4],它是目前应用最广泛的神经网络模型之一,是一种网络拓扑结构,是一种按照误差逆传播算法训练的多层前馈网络,是由Rumelhart等科学家于1986年提出的一种神经网络模型。而由于BP网络模型是由许多神经元组成的一个复杂网络,其非线性关系的能力非常强。也就是说,它能学习和存储大量的输入与输出模式的一种映射关系,而这种映射关系是基于非线性的。在BP网络的训练学习中,基于BP网络的方向传播,使用最速下降法来调整和修正网络的权值或阈值,最后达到网络误差平方和最小。它训练问题的本质是无约束的非线性优化问题。BP神经网络这一拓扑结构由输入层(input)、隐层(hide

到稿日期:2010-12-08 返修日期:2011-05-19 本文受国家自然科学基金项目(90715029,61070057),中国博士后科学基金(20060400845)与中国博士后科学基金面上项目(20100480936)资助。

李肯立 教授,博生生导师,CCF高级会员,主要研究领域为并行计算、DNA计算,E-mail:lkl510@263.com;康 强 硕士生,主要研究领域为信息安全;唐 卓 讲师,主要研究领域为信息安全、云计算;沙行勉 教授,主要研究领域为嵌入式软件和系统、并行机体系结构、传感网络系统、分布式系统、编译器、调度算法、实时系统、操作系统、网络体系结构、计算机和网络安全。

layer)和输出层(output layer)组成,其中隐层有一个或者多个。

针对这一问题,本文将使用访问控制中风险的概念,对风险进行定量计算,根据风险的大小,使得不同风险等级的访问控制策略可以相互比较其安全性的差异[5]。并基于 MUS[6] 集合的计算方法,给出了一种基于神经网络的访问控制策略优化模型,使用户在访问控制权限不变的情况之下,在角色层次中选择一组访问控制策略[7],使用户在执行风险时达到最低。结果表明该方法有效,可操作性强。

2 访问控制和神经网络理论研究现状

RBAC(Role-Based Access Control)[8-10]是一种目前广泛使用的访问控制模型,它在传统的访问控制机制的基础之上,引入了"角色"这一概念。它把角色和权限相关联,用户通过扮演角色来获得相对应的权限。访问客体所具有的权限赋予角色,而不是访问主体。这是对传统访问控制的替代和补充。与传统的访问控制相比,它具有易用和高效的授权方式;在对授权模型的维护上,只需要维护关联模型。主体在进行授权时,只需要对角色进行授权,然后将相应的角色分配给主体即可。上述访问控制模型都是从系统的角度出发保护资源,是一种静态的授权模型,没有将访问控制操作所处的环境考虑在内,容易造成安全隐患。然而随着分布式、网格计算以及数据库等方面的发展,促使我们如何去解决这一静态问题,使得随着任务的执行而进行动态的授权管理。

上述模型是基于主体-客体的一个被动的安全模型。这里被动指的是授权模型是静态的,不能进行动态授权,随着任务的变化而进行动态的授权。这样,系统便有个非安全的因素:主体(用户)在执行某个任务之前,就已经拥有了执行权限;在执行任务之后,由于静态模型,权限依然没有撤销,主体继续拥有。所以,上述静态模型不能满足要求。基于任务的访问控制模型 TBAC[11]解决了上述的静态模型不能解决的问题,它采用任务的观点,动态地授权。这样,授权体依赖 3 个约束:主体、客体和任务。当执行一个任务时,进行授权;当任务挂起或者结束时,撤销权限。这种模型非常适合于工作流系统中。TBAC 也是一种基于实例(instance-based)的访问控制模型,每个任务都是具有时效性的,所以用户对于授予他的权限的使用也是有时效性的[12]。

基于角色的访问控制模型(RBAC),只是把角色和用户、权限关联起来,没有考虑到随着系统上下文环境的变化,或者说随着时间的推移,其用户和权限之间发生变化,是一个被动的安全模型。同样,在上述的 TBAC 模型中,它虽然是一个主动的安全模型,但是没有分离出角色和任务,不能符合被动模型请求。因此,将 RBAC 模型和 TBAC 模型结合,使得模型更加灵活,这就是 TRBAC[13]模型。在这个模型中,角色间具有了 RBAC96 模型的子模型 RBAC1 的特性,即角色的继承。角色和任务之间进行角色分配,而任务和权限之间具有时间约束。文献[14]中,基于 TRBAC 模型提出了 GTRBAC 模型,在角色的基础之上,作者引入了角色的有效(enabled)状态和激活(activated)状态。在文献[15]中,董光宇等提出了带时间特性的角色授权约束,它更侧重于一般的、形式化的表达时间约束,对已有的角色授权模型进行了深入研究和扩展。但是这些模型中,虽然改进了访问控制的安全性,但是没有考虑访问控制的风险问题。

近些年来,在安全领域的恶意或非法行为防范中,越来越多的访问控制研究学者试图借用经济学中的模型来解决此类问题,例如在移动代理平台上基于支出的安全系统[16]和自私的网格计算[17]等。信息安全问题其实是一个关于效用的经济学问题[18]。任何一个绝对安全的系统都是全部限制主体对访问客体,也就是说任何一个系统都不可能达到绝对的安全程度。因此有必要寻找一种最优的访问控制策略,使得用户在执行权限的时候风险最小。

神经网络是一门结合脑科学、神经科学、认知科学、计算机科学、数学和物理学等学科的新兴交叉学科,始于 20 世纪 40 年代,是人类模仿动物的神经特征,是进行智能研究的重要组成部分,以及进行分布式并行信息处理的数学模型。目前,神经网络这一交叉学科的研究已经趋于更加成熟、稳定的发展阶段。其中一个很重要和明显的标志就是越来越多的神经生理学家、心理家、医学家、从事基础科学研究工作的以及计算机科学家等进行合作来开展跨学科的研究,应用神经网络的特性来进行神经网络机理、功能的探讨以及建立相应的算法数学模型。

目前,神经网络的研究已有两大方向和趋势:其一是在理论上,神经网络系统在理论上向更复杂的方向发展,如神经网络动力学、非线性神经场等。它与模糊数学、进化算法、认知科学、生物医学等各方面进行结合。其二是在应用层面上,应用范围随着理论的发展、深入和指导,与多种学科相结合,从而解决了许多传统单一学科所无法解决的难题。它的研究领域包括了模式识别、信号处理、知识工程、优化组合、机器人控制等,对人类认识世界、挖掘未知领域的研究起了极大的促进作用,提高了现代化技术研究水平以及由科技而带动国民经济的增长,是目前世界上公认的前沿科学研究领域之一。

3 概念和属性

3.1 基本概念

基于角色的访问控制,目的在于根据访问主体(如用户等)所授予的角色对所需访问客体(如资源等)进行实时控制,以确保系统的安全性。每一种访问控制策略中的访问权限都有一定的风险,所以可以对风险进行量化,按照风险的大小比较访问控制策略,从而确定最优访问控制策略。访问控制中的主要要素是访问主体和访问客体,所以访问控制权限的风险大小与访问主体的安全级和访问客体的重要程度有密切的关系,也与非授权访问概率(操作失败发生的概率)等有关系。风险是潜在损失及其发生的可能性的度量,表现在访问控制策略上:

$$RB(perm)=a^{OL}\times P=a^{OL}/(1+\exp(-k\times(TI-mid))) \quad (1)$$

通过式(1)[19]就可以计算权限的风险值。风险值越小,系统的安全性越高,访问控制策略更好。所以,通过比较权限之间的风险值,可以为系统制定更好的权限分配策略。

3.2 BP 神经网络基本原理

BP 网络模型处理信息的基本原理[20]是:输入信号 X_i(输

入层),然后通过中间节点(隐层点)进行"黑盒"处理,作用于输出节点。由于神经网络的非线性,使得经过非线性变换,产生输出信号 Y_k(输出层),网络训练的每个样本包括输入向量 X 和期望输出量 t。网络输出值 Y 与期望输出值 t 之间的偏差,通过调整输入节点与隐层节点的联接强度取值 W_{ij} 和隐层节点与输出节点之间的联接强度 T_{jk} 以及阈值,使误差沿梯度方向下降。经过反复学习训练,确定与最小误差相对应的网络参数(权值和阈值),训练即告停止。此时经过训练的神经网络即能对类似样本的输入信息,自行处理输出误差最小的、经过非线性转换的信息。

3.3 基于风险的 BP 神经网络评价模型

如图 1 所示,BP 神经网络是通过对风险属性的样本训练,从而评价风险的级别,它实质上实现了一个从输入到输出的映射功能。数学理论已证明,它具有实现任何复杂非线性映射的功能,神经网络能以任意精度逼近任何非线性连续函数[21]。在建模过程中,许多问题正是具有高度的非线性,使得它特别适合于求解内部机制复杂的问题。将风险的主要因素进行量化,对神经网络的输入进行预处理,可以计算风险的大小,从而确定最优策略。

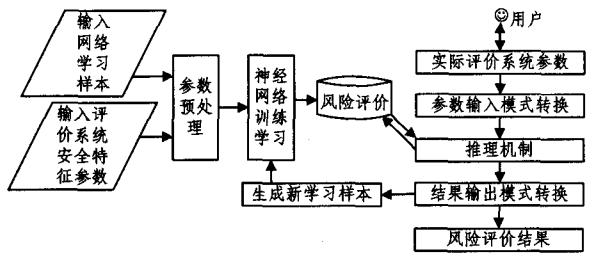

图 1 基于风险的 BP 神经网络评价图

4 用户权限的角色查找

基于角色的访问控制(RBAC)模型[22,23]是一种广泛应用的访问控制机制,它实现了用户与访问权限的逻辑分离,减少了授权管理的复杂性,降低了授权管理开销,达到了系统复杂度和效率的平衡。

在分配权限时,角色是连接用户和权限的桥梁。角色获取相应的权限,主要有两种途径:一种是管理员直接分配权限,或者是通过角色层次间的继承而间接获得;另外一种是通过角色间的委托[24,25]间接获得。但是,对于获取相同权限的情况下,这两种途径都会带来一个问题:给定权限或者权限集相同的情况下,必定至少有一种角色集。一般情况下,对于现在复杂的系统,有多种角色集可以获得相同的指派权限。那么在这多种的角色集中,如何选择最优的角色集合,使得访问控制权限能够在低风险的情况下执行,达到系统的安全性,就需要寻找一种最优的访问控制策略。

图 2 表示的是某个税务系统中的部分角色与权限关系层次树。图 2 中的实线表示角色间的 I-hierarchy 关系,虚线表示角色间的 A-hierarchy 关系,这是一个角色混合层次关系[14]。图中的主要角色有税收征管经理 TCM(Tax Collection Manager)、纳税评估职员 TAC(Tax Assessment Clerk)、税务账单职员 TBC(Tax Billing Clerk)、税收征管职员 TCC(Tax Collection Clerk)、初级税收征管职员 JTCC(Junior Tax Collection Clerk)和财产税职员 PTC(Property Tax Clerk)。图中的权限有 $\{p_2, p_3, p_4\}$。在这个税务系统中,如果在提供权限 $\{p_2, p_3, p_4\}$ 不变的情况下,可以有至少 4 种角色集{{TCC},{TBC,JTCC,PTC},{TCC,PTC},{TCC,JTCC,PTC}}满足权限指派。那么,如何选取一个最优的访问控制策略配置方案,使得此系统的安全性最低呢?这就是本文研究的基于神经网络模型的访问控制策略的主要问题。

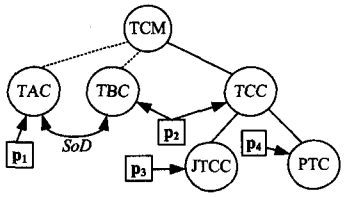

图 2 混合角色层次树的分解

一般来说,不管是被动访问控制模型(传统访问控制),还是主动访问控制模型(RBAC 模型),都缺乏主体和客体之间的访问控制策略优劣性的评价。一旦访问控制策略具有很多时,就无法确定哪种方案更优,这会使系统的安全性更低,不能评估访问控制配置方案给该税务系统带来的风险和隐患。因此,将风险属性作为访问控制,通过定量计算每个策略的风险大小,从而确定最优访问控制策略。所以有必要提出一种方法来评估 4 种配置方案,找出最优的解决方案。

为了寻求混合角色层次树中所有可能的角色集合,下面给出 MUS(MUS 是基于文献[26]提出的 UAS 的一个扩展)的定义。

定义 1(MUS 集合) 定义[6] $H=(ROLE,F)$ 是一个角色层次树,这个树有根节点,其中 $ROLE$ 代表角色集合,F 代表树中节点之间的关系集合。图 2 中的关系图可以用 H 表示为 $ROLE=\{TCM,TAC,TBC,TCC,JTCC,PTC\}$,其中 TCM 是树中的根节点,F 描述了这些节点之间的关系的集合。$MUS(H)=\{ROLE_1, ROLE_2, \cdots, ROLE_n\}$,其中 $\emptyset \subset ROLE_i \subseteq ROLE, i \in \{1,2,\cdots,n\}$。如果给出任何一个权限或者权限集,则必定有一个最小且唯一的角色集合 $ROLE_i$。

5 基于风险属性的策略优化神经网络模型

设神经元有 n 个情况输入,即一个角色 r_j 被指派了权限 $X_{ij}(1), X_{ij}(2), \cdots, X_{ij}(n), \forall X_{ij}(k) \in \{0,1\}$,其中 $k=1,2,\cdots,n$。当第 k 个输入端有输入时,$X_{ij}(k)=1$;无输入时,$X_{ij}(k)=0$。输出 y 也是二值变量,当有输出时,$y=1$,表示角色 r_j 指派了权限 p_k;否则 $y=0$,表示角色 r_j 没有指派权限 p_k。模型如图 3 所示。

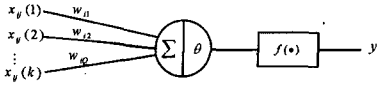

图 3 神经网络优化模型

在不考虑时滞条件下,神经元输入输出间的关系由下述方程描述:

$$y(i)=f(\sum_j w_{ij}X_{ij}(k)-\theta)$$

其中,

$$f(z)=\mathrm{sig}(z)=\begin{cases}1, & z>0\\ 0, & z\leqslant 0\end{cases}$$

$$\theta=\frac{\sum RB(r_{ij},p_k)}{n}$$

$$w_{ij}=\frac{\sum_k RB(r_{ij},p_k)\times SP_{jk}}{Q}$$

通过 Matlab 计算，找出所有 $f(z)=1$ 中最小的 $\sum_j w_{ij}X_{ij}(k)$ 值，即可确定最小的角色集。

图 2 所示的税务系统实例中，对于某个用户 user，策略 $pol_1=\langle$user,TCC$\rangle$、策略 $pol_2=\langle$user,{TBC,JTCC,PTC}$\rangle$、策略 $pol_3=\langle$user,{TCC,PTC}$\rangle$和策略 $pol_4=\langle$user,{TCC,JTCC,PTC}$\rangle$，它们所获得的访问权限是一样的，即{p_2，p_3，p_4}。那么如何在这 4 种策略中选择最优策略，使得访问控制的风险等级最小？在本文应用神经网络模型来寻求最优策略。在此，取 $m=11.0$，$\partial=10.0$，$k=1.0$，$mid=3.0$，$OL=0.6$，利用式(1)，通过 Matlab 计算得表 1－表 4。

表 1　基于神经网络的访问控制{TCC}风险实验数据

MUS 集合角色集	{TCC}		
角色指派关系	(r_{11},p_2)	(r_{11},p_3)	(r_{11},p_4)
主体安全级(SL)	0.99	0.85	0.88
非授权问度量(TI)	0.0392	0.0541	0.0505
非授权访问概率(p)	0.0492	0.0499	0.0498
权限的风险等级 RB	0.1960	0.1988	0.1981
神经元输入	1	1	1

表 2　基于神经网络的访问控制{TBC,JTCC,PTC}风险实验数据

MUS 集合角色集	{TBC,JTCC,PTC}								
角色指派关系	(r_{21},p_2)	(r_{21},p_3)	(r_{21},p_4)	(r_{22},p_2)	(r_{22},p_3)	(r_{22},p_4)	(r_{23},p_2)	(r_{23},p_3)	(r_{23},p_4)
主体安全级(SL)	0.92	0.01	0.05	0.02	0.98	0.03	0.04	0.06	0.98
非授权问度量(TI)	0.0460	0.3741	0.3412	0.3656	0.0401	0.3572	0.3491	0.3334	0.0401
非授权问概率(p)	0.0695	0.0675	0.0654	0.0670	0.0493	0.0664	0.0659	0.0650	0.0493
权限的风险等级 RB	0.1973	0.2687	0.2606	0.2666	0.1962	0.2645	0.2625	0.2587	0.1962
神经元输入	1	0	0	0	1	0	0	0	1

表 3　基于神经网络的访问控制{TCC,PTC}风险实验数据

MUS 集合角色集	{TCC,PTC}					
角色指派关系	(r_{31},p_2)	(r_{31},p_3)	(r_{31},p_4)	(r_{32},p_2)	(r_{32},p_3)	(r_{32},p_4)
主体安全级(SL)	0.99	0.85	0.88	0.04	0.06	0.98
非授权问度量(TI)	0.0392	0.0541	0.0505	0.3491	0.3334	0.0401
非授权问概率(p)	0.0492	0.0499	0.0498	0.0659	0.0650	0.0493
权限的风险等级 RB	0.1960	0.1988	0.1981	0.2625	0.2587	0.1962
神经元输入	1	1	1	0	0	1

表 4　基于神经网络的访问控制{TCC,JTCC,PTC}风险实验数据

MUS 集合角色集	{TCC,JTCC,PTC}								
角色指派关系	(r_{41},p_2)	(r_{41},p_3)	(r_{41},p_4)	(r_{42},p_2)	(r_{42},p_3)	(r_{42},p_4)	(r_{43},p_2)	(r_{43},p_3)	(r_{43},p_4)
主体安全级(SL)	0.99	0.85	0.88	0.02	0.98	0.03	0.04	0.06	0.98
非授权问度量(TI)	0.0392	0.0541	0.0505	0.3656	0.0401	0.3572	0.3491	0.3334	0.0401
非授权问概率(p)	0.0492	0.0499	0.0498	0.0670	0.0493	0.0664	0.0659	0.0650	0.0493
权限的风险等级 RB	0.1960	0.1988	0.1981	0.2666	0.1962	0.2645	0.2625	0.2587	0.1962
神经元输入	1	1	1	0	1	0	0	0	1

图 4 给出神经网络求解 MUS 集合最佳策略算法。

Algorithm1　*ComputerMin*($y(i)$)

Input: m,α,k,mid

Output: Min($y(i)$)

1. #define m,α,k,mid
2. SUM(ij)=0
3. initialize $C(MUS)=Q$ //每个指派方案中有 Q 个角色
4. initialize $C(P)=n$ //用户所获得的权限
5. do{
6. for($j=0;j<Q,j++$)
7. for($k=0;k<n;k++$)
8. $TI=\alpha^{-SL(-OL)}/(m-OL)$
9. $P=1/(1+\exp(-k\times(TI-mid)))$
10. $RB(r_{ij},p_k)=\alpha^{OL}\times P=$
11. SUM(ij)+=$RB(r_{ij},p_k)$
12. $w_{ij}=$SUM(ij)$*SP_{jk}/Q$
13. $\theta=$SUM(ij)$/n$
14. $y(i)=f(\sum_j w_{ij}X_{ij}(k)-\theta)$
15. end for
16. end for
17. $z=\sum_j w_{ij}X_{ij}(k)-\theta$
18. }while($z>0$)
19. if $z>0$
20. $f(z)=$sign(z)$=1$

图 4　神经网络求解 MUS 集合最佳策略算法

由图 5 可以看出，最佳的访问控制策略是 $pol=\langle$user,TCC$\rangle$。也就是说，用户只需指派 TCC 就可以获得相同的权限，且用户执行权限的风险比初始状态小。

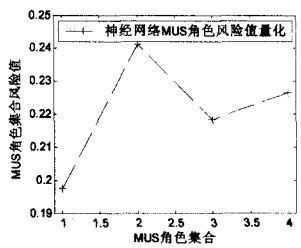

图 5　基于神经网络模型的访问控制策略风险图

本文中的策略优化实际上是在 MUS 集合的基础上获得

访问控制策略的所有角色集合，然后利用神经网络模型，进行策略的优化配置。也就是说，通过重新调整用户的角色指派关系使得用户在执行相同访问权限或权限集的时候，风险最小，同时能够尽量减少用户角色的个数，从而降低系统的风险级。

结束语 在基于角色的访问控制模型中，由于系统的复杂性以及角色之间的层次关系更复杂等，使得访问控制在相同的权限或权限集下，往往具有多个角色集合，即一定的用户权限往往可以通过不同的角色指派方案来获得。如何针对一个用户和角色的指派关系进行优化，在优化策略上，采用了神经网络模型，针对现有的用户角色指派关系来选择一组最优的角色指派给用户，使得用户在执行权限的时候风险达到最低。

参 考 文 献

[1] 唐卓，赵林，李肯立，等. 一种基于风险的多域互操作动态访问控制模型[J]. 计算机研究与发展，2009，43(6)：948-955

[2] Marsh S. Formalising Trust as a Computational Concept[D]. Britain：University of Stirling，1994

[3] Aziz B，Foley S N，Herbert J，et al. Reconfiguring Role-based Access Control Policies Using Risk Semantics[J]. Journal of High Speed Networks，Special issue on Security Policy Management，2006，15(3)：216-273

[4] 郭嗣琮，陈刚. 信息科学中的软计算方法[M]. 沈阳：东北大学出版社，2001

[5] Tang Zhuo，Li Bo，Li Ren-fa，et al. Research on Risk-based Access Control Policy[C]// Proceeding of the 5th International Conference on Management of Innovation and Technology. Singapore：IEEE，June 2010：2-5

[6] Li Rui-xuan，Tang Zhuo，Lu Zheng-ding. A Request-driven Policy Framework for Secure Interoperation in Multi-domain Environment[J]. International Journal of Computer Systems Science & Engineering，2008，23(3)：193-206

[7] Aziz B，Foley S，Herbert J. Reconfiguring role based access control policies using risk sementics[J]. Journal of High Speed Networks，2006，15(3)：216-273

[8] Sandhu R. Issues in RBAC[C]// Proceedings of the ACM RBAC Workshop. ACM Press，1996：21-24

[9] Ferraiolo D，Cugini J，Kuhn D R. Role-based Access Control (RBAC)：Features and Motivations[C]// Proc. of the 1995 Computer Security Applications Conference. December 1995：241-248

[10] Ferraiolo D，Sandhu R，Gavrila S，et al. Proposed NIST Standard for Role-based Access Contro[C]// ACM Transaction on Information and System Security，2001，4(8)：224-274

[11] Thomas R K，Sandhu R S. Towards a task-based paradigm for flexible and adaptable access control in distributed applications [C]// Proceedings of the 1992-1993 ACM SIGSAC New Security Paradigms Workshops. 1993：138-142

[12] 邓集波，洪帆. 基于任务的访问控制模型[J]. 软件学报，2003，14(1)：76-82

[13] Bertino E，Bonatti P A. TRBAC：A Temporal Role-based Access Control Model[J]. ACM Transactions on Information and System Security，2001，4(3)：191-223

[14] James B D，Bertino E. Hybrid role hierarchy for generalized temporal role based access control model[C]// Proceedings of the 26th Annual International Computer Software and Applications Conference(COMPSAC'02). Oxford，England，2002：46-57

[15] 董光宇，卿斯汉，刘克龙. 带时间特性的角色授权约束[J]. 软件学报，2002，13(8)：1521-1527

[16] Sonntag M，Hrmanseder R. Mobile Agent Security Based on Payment[J]. Operating Systems Review，2000，34(4)：48-55

[17] Dimmock N，Bacon J，Ingram D，et al. Risk Models for Trust-based Access Control[C]// Proceedings of the 3rd Annual Conference on Trust Management(iTrust'05). USA：Spinger，Lecture Notes in Computer，2005：364-371

[18] Gordon L，Loeb M，Lucyshyn W. An Economics Perspective on the Sharing of Information Related to Security Breaches[C]// The 1st Workshop on the Economics of Information Security (WEIS'02). Berkeley，CA，2002：1-10

[19] Cheng P C，Rohatgi P，Keser C，et al. Fuzzy Multi-level Security：An Experiment on Quantified Risk- Adaptive Access Control [R]. RC24190. IBM Research Report，2007

[20] Haykin S. 神经网络原理[M]. 叶世伟，史忠植，译. 北京：机械工业出版社，2004

[21] 杨晓帆，陈延槐. 人工神经网络固有的优点和缺点[J]. 计算机科学，1994，21(2)：23-26

[22] Sandhu R，Coyne E J. Role based access control models [J]. IEEE Computer，1996，29(2)：38-47

[23] Ferraiolo D，Sandhu R，Kuhn R. Proposed NIST standard for role-based access control[J]. ACM Transactions on Information and System Security，2001，4(3)：224-274

[24] Barka E，SandhuR. A role-based delegation model and some extensions[C]// Proc of the 23rd National Information Systems Security Conference. Baltimore：NIST，2000：101-114

[25] Zhang X W，Oh S，Sandhu R S. PBDM：a flexible delegation model in RBAC[C]// Proc of the 8th ACM Symp on Access Control Models and Technologies. New York：ACM Press，2003：149-157

[26] Du S，Joshi B D. Supporting authorization query and inter-domain role mapping in presence of hybrid role hierarchy[C]// Proceedings of the Eleventh ACM Symposium on Access Control(SACMAT06). Lake Tahoe，California，USA，2006：47-59