一种新的 RBAC 角色协同关系及其 Petri 网模型

王小明[1,2],赵宗涛[1],马建峰[3]

(1. 西北大学计算机科学系,陕西西安 710069;2. 陕西师范大学计算机科学学院,陕西西安 710062;
3. 西安电子科技大学计算机网络与信息安全教育部重点实验室,陕西西安 710071)

摘 要: 角色授权约束是 RBAC 研究的重要内容. 有效表达多角色授权和激活的序约束是一个难点问题. 提出了新的角色授权协同及其序关系,扩展了现有的角色关系概念,使 RBAC 能够表达复杂的角色授权和激活序约束. 其次,提出了角色授权协同及其序关系一致性分析和模拟的时间 Petri 网方法.

关键词: RBAC; 授权协同关系; 激活协同关系; 序关系; 时间 Petri 网

中图分类号: TP309.2 **文献标识码**: A **文章编号**: 0372-2112 (2003) 02-0225-03

A Novel Role Coordination Relation of RBAC and Its Petri Net Model

WANG Xiao-ming[1,2], ZHAO Zong-tao[1], MA Jian-feng[3]

(1. *Department of Computer Science, NorthWest University, Xi'an, Shaanxi* 710069, *China*;
2. *School of Computer Science, Shaanxi Normal university, Xi'an, Shaanxi* 710062, *China*;
3. *The Ministry of Education Key Lab for Computer Networks and Information Security, Xidian University, Xi'an, Shannxi* 710071, *China*)

Abstract: Role authorization constraint is one of focal points of RBAC research. It is a difficult problem to effectively represent the authorization and activation order constraints of multiple roles. Novel role authorization coordination relations were presented and coordination order relations such that existing role relation concepts are expanded. It is able to make RBAC represent complex order constraints when granting or activating multiple roles. The new Petri Net to analyze and simulate the consistence of role authorization coordination as well as its order relation is proposed.

Key words: RBAC; authorization coordination relation; activation coordination relation; order relation; timed Petri nets

1 引言

近年来,基于角色的访问控制(RBAC)研究异常活跃,并取得了丰硕成果[1]. 角色授权约束在 RBAC 中具有十分重要的作用. 有效表达多角色授权或多用户并发激活多角色的序关系约束一直是角色关系研究的一个难点[1,2]. 例如,假定实时银行会计审计系统(简称会计审计系统)由会计(accountant)和审计(auditor)角色组成. 其部分安全策略为: ①审计角色授予先于会计角色授予,会计角色收回先于审计角色收回; ②审计角色激活先于会计角色激活,会计角色休眠先于审计角色休眠,以免造成审计遗漏现象. 但是现有的 RBAC 仅有角色继承和互斥关系,无法表达上述安全策略,即角色授予和激活的协同关系及其协同序关系约束. 文献[1,2,5]分别对角色互斥与继承,权限互斥,用户互斥等关系进行了深入研究,但均未讨论角色授权协同及其序关系. 随着分布式应用快速发展,角色授权协同及其序关系在跨组织应用中愈来愈普遍,迫切需要 RBAC 能够表达类似上述授权约束. 因此,本文引入角色授权模式新概念,提出角色授权协同关系和协同序关系,使得 RBAC 能够表达复杂的授权约束,并给出一种角色授权协同及其序关系一致性分析和模拟的 Petri 网方法.

2 角色授权协同及其序关系定义

为定义角色授权协同及其序关系,首先给出相关的 RBAC 函数. 设 U 为用户集, R 为角色集, P 为权限集, S 为激活角色的会话集. 定义下列 RBAC 函数:

定义 1[1] $RUA: R \to 2^U$ 为角色集 R 到用户幂集 2^U 上的函数映射, $RUA(r)$ 表示角色 r 的用户集. $URA: U \to 2^R$ 为用户集 U 到角色幂集 2^R 上的函数映射, $URA(u)$ 表示用户 u 的角色集. $SUA: S \to U$ 为会话集 S 到用户集 U 上的函数映射, $SUA(s)$ 表示会话 s 对应的用户 u. $SRA: S \to 2^R$ 为会话集 S 到角色幂集 2^R 上的函数映射, $SRA(s)$ 表示会话 s 能够激活的角色集.

RBAC 函数除上述之外,还有权限函数,其与本文的讨论无关,所以被省略.

定义 2 角色授权模式是一个三元组 $RS = (userid, roleid, mark)$. 其中 $userid$ 是用户唯一标识, $roleid$ 是角色唯一标识, $mark \in \{1, 0\}$ 是授予或收回用户 $userid$ 角色 $roleid$ 的标志.

角色授权模式的实例是角色授权(以下授权均指角色授权). 例如,授权$\langle u_1, auditor, 1\rangle$表示授予用户 u_1 角色 $auditor$, $\langle u_2, accountant, 0\rangle$表示收回用户 u_2 角色 $accountant$. 在某一时刻,RBAC 系统的所有授权集记作 Γ. 第 1 节给出的会计审计系统中,假定授予用户 u_1 角色 $auditor$, u_2 角色 $accountant$,则授权集 $\Gamma = \{\langle u_1, director, 1\rangle, \langle u_2, accountant, 1\rangle\}$.

在分布式环境下,对某些角色的授予或收回往往需要"要么全授予,要么全收回",才能保证安全策略语义完整性. 即授权之间可能存在静态协同关系,其形式定义如下:

定义 3 设授权$\langle u_1, r_1, m_1\rangle, \langle u_2, r_2, m_2\rangle \in \Gamma$. 如果对其

收稿日期:2002-03-21;修回日期:2002-09-27
基金项目:国家自然科学基金(No. 69973003);国家"863"计划(No. 2002AA143021);国防预研 C³I 基金(No. EP99027)

实施授予或收回操作,必须要么全部实施,要么全部不实施,才能保证安全策略语义完整性,则称两者之间存在静态授权协同关系,记作$\langle u_1, r_1, m_1\rangle \Theta \langle u_2, r_2, m_2\rangle$. 即$\langle u_1, r_1, m_1\rangle \Theta \langle u_2, r_2, m_2\rangle \Rightarrow u_1, u_2 \in U, r_1, r_2 \in R: (m_1 = 1 \rightarrow u_1 \in RUA(r_1)) \vee m_1 = 0 \rightarrow u_1 \notin RUA(r_1)) \wedge (m_2 = 1 \rightarrow u_2 \in RUA(r_2)) \vee m_2 = 0 \rightarrow u_2 \notin RUA(r_2))$.

但是,授予用户静态协同角色过程中可能还存在一定的序关系. 例如,第 1 节的会计审计系统安全策略 ①的授权要求.

定义 4 已知静态授权协同关系$\langle u_1, r_1, m_1\rangle \Theta \langle u_2, r_2, m_2\rangle$. 如果授予$\langle u_1, r_1, m_1\rangle$并经过 $\Delta\tau$时间之后必须授予$\langle u_2, r_2, m_2\rangle$,则称两者之间存在静态授权协同顺序关系,记作$\langle u_1, r_1, m_1\rangle \vdash\!\!\!\rightarrow^{s.\Delta\tau} \langle u_2, r_2, m_2\rangle$. 即$\langle u_1, r_1, m_1\rangle \vdash\!\!\!\rightarrow^{s.\Delta\tau} \langle u_2, r_2, m_2\rangle \Rightarrow \langle u_1, r_1, m_1\rangle \Theta \langle u_2, r_2, m_2\rangle \wedge execute(\langle u_1, r_1, m_1\rangle, \tau_1) \wedge execute(\langle u_2, r_2, m_2\rangle, \tau_2) \wedge (\tau_1 - \tau_2 = \Delta\tau)$. 其中, $execute(\langle u, r, m\rangle, \tau)$是授予角色谓词, τ是授予完成时刻. 静态授权协同顺序关系集记作 D_s.

如果$\langle u_1, r_1, 1\rangle \Theta \langle u_2, r_2, 1\rangle$,并且两者之间不存在静态协同顺序关系,则它们的授予是可以并发的. 如果$\langle u, r, m\rangle$的授予不需要任何前提条件,则记作 $\vdash\!\!\!\rightarrow \langle u, r, m\rangle$. 在 RBAC 中,用户拥有角色仅仅表明该用户获得了使用该角色的资格. 只有当关联用户和用户拥有的角色的会话(实时映射)激活角色后,用户才能使用该角色包含的权限以完成特定的工作任务. 在多用户环境下,角色激活也可能存在协同关系. 例如,会计审计系统中规定只有当审计角色被激活之后. 才允许激活会计角色. 银行金库门锁的打开需要多个金库管理员(角色)按一定的先后次序执行各自的开锁操作. 由此可见,用户拥有的角色在激活过程中不仅存在动态协同关系,而且存在一定的协同序关系.

定义 5 设授权$\langle u_1, r_1, 1\rangle, \langle u_2, r_2, 1\rangle \in \Gamma$. 如果对它们的激活必须要么全部激活,要么全部不激活,才能保证安全策略的语义完整性,则称它们之间存在角色动态协同关系,记作$\langle u_1, r_1, 1\rangle \Theta^j \langle u_2, r_2, 1\rangle$. 即$\langle u_1, r_1, 1\rangle \Theta^j \langle u_2, r_2, 1\rangle \Rightarrow u_1, u_2 \in U, r_1, r_2 \in R, \exists s_1, s_2 \in S: u_1 \in RUA(r_1) \wedge u_2 \in RUA(r_2) \wedge SUA(s_1) = u_1 \wedge SUA(s_2) = u_2 \wedge r_1 \in SRA(s_1) \wedge r_2 \in SRA(s_2)) \vee (u_1, u_2 \in U, r_1, r_2 \in R, \nexists s_1, s_2 \in S: u_1 \in RUA(r_1) \wedge u_2 \in RUA(r_2) \wedge SUA(s_1) = u_1 \wedge SUA(s_2) = u_2 \wedge r_1 \in SRA(s_1) \wedge r_2 \in SRA(s_2))$.

定义 6 设$\langle u_1, r_1, 1\rangle \Theta^j \langle u_2, r_2, 1\rangle$. 如果激活$\langle u_2, r_2, 1\rangle$并经过 $\Delta\tau$时间后必须激活$\langle u_1, r_1, 1\rangle$,则称$\langle u_1, r_1, 1\rangle$与$\langle u_2, r_2, 1\rangle$之间存在激活顺序关系,并称$\langle u_1, r_1, 1\rangle$激活为$\langle u_2, r_2, 1\rangle$激活的前提条件,记作$\langle u_1, r_1, 1\rangle \vdash\!\!\!\rightarrow^{d.\Delta\tau} (\langle u_2, r_2, 1\rangle$. 即$\langle u_1, r_1, 1\rangle \vdash\!\!\!\rightarrow^{d.\Delta\tau} \langle u_2, r_2, 1\rangle \Rightarrow \langle u_1, r_1, 1\rangle \Theta^j \langle u_2, r_2, 1\rangle \wedge activate(\langle u_1, r_1, 1\rangle, \tau_1) \wedge activate(\langle u_2, r_2, 1\rangle, \tau_2) \wedge (\tau_1 - \tau_2 = \Delta\tau)$. 其中, $activate(\langle u, r, m\rangle, \tau)$是激活角色谓词, τ是激活时刻. 动态授权协同顺序关系集记作 D_d.

如果$\langle u_1, r_1, 1\rangle$和$\langle u_2, r_2, 1\rangle$之间不存在激活顺序关系,则其激活是可以并发的. 如果$\langle u, r, 1\rangle$的激活不需要任何前提条件,则记作 $\vdash\!\!\!\rightarrow^{d} \langle u, r, 1\rangle$. 如果激活$\langle u_1, r_1, 1\rangle$和$\langle u_2, r_2, 1\rangle$并经过 $\Delta\tau_1$ 时间后激活$\langle u_3, r_3, 1\rangle$,再经过 $\Delta\tau_2$ 时间后激活$\langle u_4, r_4, 1\rangle$,则记作$\langle u_1, r_1, 1\rangle \wedge \langle u_2, r_2, 1\rangle \vdash\!\!\!\rightarrow^{d.\Delta\tau_1} \langle u_3, r_3, 1\rangle \vdash\!\!\!\rightarrow^{d.\Delta\tau_2} \langle u_4, r_4, 1\rangle$. 根据上述定义很容易给出两个以上授权协同及其序关系表达式.

3 角色协同关系的性质

关系 Θ, Θ^j, $\vdash\!\!\!\rightarrow^{s.\Delta\tau}$和 $\vdash\!\!\!\rightarrow^{d.\Delta\tau}$具有下列性质.

性质 1 关系 Θ 是反自反的,对称的.

性质 2 关系 Θ^j 是反自反的,对称的.

关系 Θ 和 Θ^j 的反自反性是显然的,因为任何授权与其自身协同在授权语义上是毫无意义的. 由定义 3 和定义 5 可以直接得出 Θ 和 Θ^j 分别是对称的.

性质 3 关系 $\vdash\!\!\!\rightarrow^{s.\Delta\tau}$是反自反的,反对称的.

证明: ①二元关系关系 $\vdash\!\!\!\rightarrow^{s.\Delta\tau}$的反自反性是显然的. 因为对同一用户任何角色的授予或收回不能以其自身首先授予或收回为前提条件. ②用反证法证明二元关系 $\vdash\!\!\!\rightarrow^{s.\Delta\tau}$具有反对称性. 假设对 $\forall\langle u_1, r_1, 1\rangle, \langle u_2, r_2, 1\rangle \in \Gamma, \langle u_1, r_1, 1\rangle \vdash\!\!\!\rightarrow^{s.\Delta\tau} \langle u_2, r_2, 1\rangle$并且$\langle u_2, r_2, 1\rangle \vdash\!\!\!\rightarrow^{s.\Delta\tau} \langle u_1, r_1, 1\rangle$,则其授权语义为两个角色的授予分别以对方首先授予为前提条件,这就造成了角色授予的相互无限期等待状态,是毫无意义的. 因此关系 $\vdash\!\!\!\rightarrow^{s.\Delta\tau}$具有反对称性.

同理可以得出关系 $\vdash\!\!\!\rightarrow^{d.\Delta\tau}$的性质.

性质 4 关系 $\vdash\!\!\!\rightarrow^{d.\Delta\tau}$是反自反的,反对称的.

传统的角色互斥关系是指如果授予同一用户两个不同的角色或者同一会话激活两个不同的角色会违反安全策略,则称前两个角色之间存在静态互斥关系,后两个角色之间存在动态互斥关系. 即角色互斥限定在同一用户或会话内讨论. 深入分析定义 3 - 6,可以把收回角色看作为授予角色的否定,即 $\neg\langle u_1, r_1, 1\rangle = \langle u_1, r_1, 0\rangle$;把激活角色看作为休眠角色的否定,即 $activate(\langle u_1, r_1, 1\rangle, \tau_1) = \neg(deactivate(\langle u1, r1, 1\rangle, \tau_1)$,能够得出重要结论:静态角色互斥关系是静态角色协同关系的特例;动态角色互斥关系是动态角色协同关系的特例.

角色协同关系推广了传统的角色关系概念,使得静态角色互斥不仅仅局限于同一用户,动态角色互斥也不仅仅局限于同一会话,从而既能实现授权职责分离[1]又能实现职责协同. 尤其在分布式 RBAC 授权管理中有重要意义.

4 授权协同及其序关系 Petri 网模型

授权关系一致性分析是 RBAC 研究的重要内容. 授权协同关系既有动态、并发性,又有静态、冲突性,对其进行一致性分析与模拟能够有效避免授予或激活角色过程中可能产生的授权语义冲突或不完整. Petri 网(PN)是动态系统建模的强有力工具,它有良好的并发、异步和冲突消解等特点,适合角色协同关系建模. 由于授权协同及其序关系与时间延迟有关,而基本 PN 不支持时间概念,现有的时间 PN (TPN)又过于复杂[4]. 因此定义一种新的适合授权协同及其序关系建模而且简单易用的时间 PN 是很有必要的.

定义 7 基本 PN 结构是一个四元组 $PN = (P, T; F, M_0)$. 其中, P 是库所有限集, T 是转移有限集, $F \subseteq (P \times T) \cup$

$(T \times P)$ 是弧有限集, $P \cap T = \emptyset$, $P \cup T \neq \emptyset$, $M: P \to N$ 是库所标识, N 为自然数, M_0 是初始标识, $m(p)$ 表示 p 的标识(token)数.

在基本 PN 结构基础上引入一种时间延迟库所和相应的语义定义新的时间 PN($nTPN$)如下:

定义 8　nTPN 结构是一个五元组 $nTPN = (P \cup \underline{P}, T; F, f, M_0)$. 其中 P, T 意义同定义 7, $\underline{P}$ 是时间延迟库所有限集. $P \cap \underline{P} = \emptyset$, $(P \cup \underline{P}) \cap T = \emptyset$, $P \cup \underline{P} \cup T \neq \emptyset$ $F \subseteq ((P \cup \underline{P}) \times T) \cup (T \times (P \cup \underline{P}))$ 是弧有限集. 对 $\forall \underline{p} \in \underline{P}$, $\exists \triangle\tau \in \mathbf{T}: f(\underline{p}) = \triangle\tau$, 表示到达 $\underline{p}$ 的托肯经过 $\triangle\tau$ 时间延迟后才是有效的(p 的托肯一旦到达即是有效的), 其中 $\mathbf{T} = \{\triangle\tau_0, \triangle\tau_1, \cdots\}$ 是时间量集合. $M: P \cup \underline{P} \to N$ 是库所标识, N 为自然数, M_0 是初始标识, 对 $\forall p \in (P \cup \underline{P})$, $m(p)$ 表示 p 的标识数. ${}^*t = \{p \mid \forall p \in P \cup \underline{P}: (p, t) \in F\}$ 是转移 t 的输入库所. $t^* = \{p \mid \forall p \in P \cup \underline{P}: (t, p) \in F\}$ 是转移 t 的输出库所.

nTPN 的动态行为由其转移发生规则描述, 定义如下:

定义 9　在时间 τ, 对 $\forall t \in T$, $\forall p_i \in {}^*t$, 如果 p_i 中存在有效托肯, 那么 t 是活的, 并且是可以发生的. t 发生后产生新的标识 m': $\forall p_i \in {}^*t$, $\forall p_j \in t^*: m'(p_i) = m(p_i) - 1 \wedge m'(p_j) = m(p_j) + 1$.

在授权协同及其序关系建模中, 授权管理员执行授权任务与会话激活角色原理相似, 因此只给出授权管理员执行授权任务的 nTPN 相关语义. 库所集 P 表示角色授权集, 库所集 $\underline{P}$ 表示时间延迟控制结点集. 转移集 T 表示授权管理员的授权活动集, t 发生表示授权活动执行. 转移 t 的输入库所表示角色得以授予的前提条件, 输出库所表示授权活动完成后产生的授权结果. 弧集 F 表示授权协同关系集. 第 2 节的授权协同及其序关系的 nTPN 表示如图 1(a) - (d)所示. 其中无色圆圈表示角色授权, 阴影圆圈表示时间延迟.

设静态授权协同关系集为 Γ, 静态授权协同序关系集为 D_s, 则其 nTPN 构造算法如下:

Step1　$P = \emptyset, \underline{P} = \emptyset, T = \emptyset, F = \emptyset$

Step2　若 $\Gamma = \emptyset$, 则转 3, 否则, 从 Γ 中取出一个角色授权$\langle u, r, m\rangle$, 创建与其对应的库所 p, 令 $P \leftarrow P \cup \{p\}$, $\Gamma \leftarrow \Gamma - \{\langle u, r, m\rangle\}$, 转 Step2.

Step3　若 $D_s = \emptyset$, 则转 4, 否则, 从 D_s 中取出一个关系, 按照图 1 创建对应的转移, 延迟库所和弧, 定义对应的延迟库所函数值, 并把创建的转移并入 T, 延迟库所并入 $\underline{P}$, 弧并入 F, 从 D_s 中删除该关系, 转 Step3.

Step4　停止

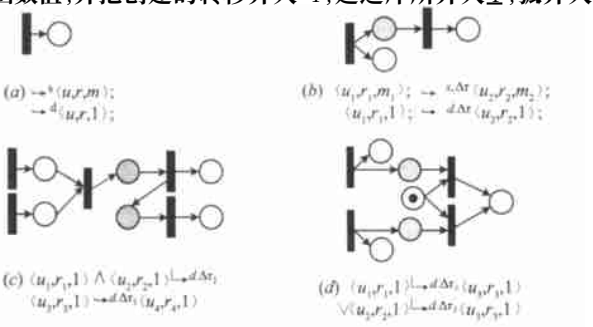

图 1　授权协同及其序关系 nTPN 表示

动态授权协同关系的 nTPN 构造算法与上述算法类似. 授权协同关系的性质决定了使用上述算法构造的 nTPN 是无环的. 按照定义 9 的转移发生规则, 可以执行所建立的 nTPN 以实现授权协同关系一致性分析与模拟. 显然, 使用授权协同及其序关系和 nTPN 建模方法很容易表达第 1 节的会计审计系统角色授予与收回约束, 如图 2 所示. 其中 t_1 发生使 u_1 获得 auditor, t_2 发生使 u_2 获得 accountant, t_3 发生时收回 u_2 的 accountant, t_4 发生时收回 u_1 的 auditor. p_1, p_3 分别表示 u_1 获得授权和被收回授权状态, p_2, p_5 分别表示 u_2 获得授权和被收回授权状态.

图 2　会计审计系统授权与收权 $nTPN$

5　结束语

本文提出的角色授权协同及其序关系扩展了现有 RBAC 的角色关系概念, 能够表达复杂的角色授权(激活)协同及其序关系约束, 尤其在分布式 RBAC 授权管理中有重要意义. 根据本文结果设计的银行会计审计系统 RBAC 授权服务器原形实验表明, nTPN 能够有效表达角色授权协同及其序关系约束.

参考文献:

[1] Sandhu D Ferraiolo, R Kuhn. The NIST model for role-based access control: towards a unified standdard [A]. In the Proceedings of 5th ACM Workshop on Role-based Access Control [C]. USA: ACM, 2000. 60 - 110.

[2] D Richard kuhn. Mutual exclusion of roles as a means of implementing separation of duty in role-based access controlsystems [A]. In the Proceedings of the Second ACM Workshop on Role-based Access Control [C]. USA: ACM, 1997. 240 - 252.

[3] R Sandhu, P Samarati. Access control principles and practice [J]. IEEE Comm, 1999: 40 - 48.

[4] 刘婷, 林闯, 刘卫东. 基于时间 Petri 网的工作流系统模型的线性推理[J]. 电子学报, 2002, 30(2): 245 - 248.

[5] 王小明, 赵宗涛, 冯德民. 一种动态角色委托授权模型[J]. 计算机科学, 2002, 29(2): 66 - 68.

作者简介:

王小明　男, 1964 年 12 月生于甘肃省天水市, 博士生, 副教授, 主要研究方向是信息系统安全, 访问控制与数据库. Email: wangxm@snnu.edu.cn.

赵宗涛　男, 1945 年出生于江苏省徐州市, 教授, 博士生导师, 主要研究方向是信息系统安全, 数据库与知识库.

马建峰　男, 1964 年出生于陕西省西安市, 教授, 博士生导师, 主要研究领域为信息安全与计算机网络, 密码学.