计算机科学2002Vol. 29№. 10

访问授权任务依赖关系及其 Petri 网分析*)

The Dependent Relationships of Access Authorization Tasks and its Timed Color Petri Net Analysis Model

王小明[1,3] 赵宗涛[1,2] 冯德民[3]

(西北大学计算机系 西安710069)[1] (第二炮兵工程学院计算机与指挥自动化系 西安710025)[2]

(陕西师范大学计算机科学学院 西安710062)[3]

Abstract Supporting the separation of duties is one of the security strategies that must be achieved in any one of access control methods. However, the facts that the same user is not allowed to hold some permissions at a certain time (static permission exclusion) and that the same user is not allowed to activate some permissions at a certain time (dynamic permission exclusion) are only realized in existing authorization models, that is, these models only support a user-level separation of duties. But under the environment of network and distribution, there exists separation of duties in authorization tasks themselves. That is, whether some authorization tasks have been or should be carried out is the prerequisite that other some authorization tasks are carried out, whereas this very important problem is not discussed in existing authorization models such that it is very difficult to model access authorization task execution in network and distribution environments. Thus the novel notions of authorization task dependencies and the new concepts of separation of duties and cooperation of duties are present in this paper, and their formal descriptions also are given. With the mutual exclusion and cooperation relationships of authorization tasks, a system-level authorization separation of duties may be achieved. Finally, a timed color Petri net model used to analyse the dependent relationship consistency among authorization tasks is discussed.

Keywords Authorization, Task dependency, Separation of duties, Cooperation of duties, TCPN

1 引言

访问授权是信息系统安全最重要的措施之一。支持访问授权职责分离原则是评价访问授权模型的重要技术指标[1,5]。但是，现有的访问授权模型仅支持用户级授权职责分离，即不允许同一用户同时拥有某些访问权限(权限静态互斥)[4,5]，或者不允许同一用户在一次用户访问会话(进程)中激活其所拥有的某些访问权限(权限动态互斥)[4,5]，而对访问授权任务本身存在的互斥关系在目前的相关文献中讨论很少。然而，授权任务本身应具有职责分离特性(系统级职责分离)同样是实际需要的，对网络和分布式环境下实现协同安全授权策略具有十分重要的意义[5,8]。研究表明，由授权者错误(或超越授权职责)执行授权任务造成的系统安全危害与隐患远远大于用户对系统安全造成的危害。在协同授权策略中，授权任务之间具有复杂的相互依赖性，正确处理这些制约关系，才能确保授权任务执行的安全性，从而在根本上保证系统访问的安全性。即某一授权任务的实施需要以其它一些授权任务预先实施或未实施为前提条件。例如，假定一个银行金库管理安全授权系统由三个权限组成：现金入库权限(add)，记帐权限(account)，现金出库权限(move)。现金入库审计权限(addaudit)和现金出库审计权限(moveaudit)，其授权策略为：①授予某人 add 的前提条件是此人当前没有 account；②授权任务执行者不能是权限接受者的亲属；③account 和 move 的授权任务执行者不能是同一个人(或同一部门内的人)；④move 需要属于两个不同组织的不同的授权任务者分别执行各自的授权操作后才能完成授权任务；⑤addaudit 和 moveaudit 的授权任务执行者不能是同一个人(或同一部门内的人)；⑥add 和 addaudit 必须同时执行，move 和 moveaudit 必须同时执行。显然，完成这种授权任务既需要用户级权限互斥约束，又需要系统级授权任务执行互斥与协同约束，即授权模型需要支持授权任务本身应具有的职责分离。但是，现有的授权模型均不支持这种极其重要的职责分离，使得网络和分布式环境下实现安全访问授权策略十分困难。为此，我们提出了新的访问授权任务依赖和访问授权任务职责分离与职责协同新概念及其形式化描述，使得访问授权模型通过授权任务互斥与协同关系实现系统级授权职责分离与职责协同，从而降低网络和分布式环境下协同授权建模的复杂性，进一步提高授权安全性。建立了一种访问授权任务依赖关系一致性分析的时间着色 Petri 网(TCPN)模型，实现了协同授权仿真与授权冲突可视化分析。

2 访问授权任务依赖关系

设 T 为时间集，$[\tau_b,\tau_e]\in T\times T$ 是时间闭区间，$\tau_b\leqslant\tau_e$。N 为自然数集。序偶(uid，l_{uid})和(oid，l_{oid})分别表示用户和访问对象，其中 uid，l_{uid}，oid，$l_{oid}\in$N 分别为用户标识，用户级别，对象标识和对象级别，U 和 O 分别为用户集和对象集。F 为级别函数，对$\forall$ u$\in$U，$F(u)=l_{uid}$，$\forall$ o$\in$O，$F(o)=l_{oid}$。P 为用户操作权限集。

定义1 授权任务是一个五元组 gt=(op，IN，OUT，$[\tau_x,\tau_y]$，g)。其中 op$\in$｛grant，revoke，block｝是授权任务操作。$[\tau_x,\tau_y]$是授权任务执行的时间区间。g$\in$U 是授权任务执行者。IN 和 OUT 分别为前提条件授权集和授权任务执行所产生的授权集，IN$\subseteq$｛(u，p，o，$[\tau_g,\tau_r]$，g')|$\forall$ u，g'$\in$U，$\forall$ p$\in$P，$\forall$ o$\in$O：$F(g')\geqslant\max(F(u),F(o))$｝，OUT$\subseteq$｛(u，p，o，$[\tau_g,\tau_r]$，g)|$\forall$ u，g$\in$U，$\forall$ p$\in$P，$\forall$ o$\in$O：F(g)$\geqslant\max(F(u),F(o))$｝，τ_g 为 u 获得 o 上的权限 p 的时刻，τ_r 为此权限被收回的时刻。

*)国防预研基金项目(C³I)资助。王小明 博士研究生，副教授，主要研究领域为数据库与知识库，信息系统。赵宗涛 教授，博士生导师，主要研究领域为数据库与知识库，决策支持系统。冯德民 教授，主要研究领域为计算机算法与操作系统。

设 GT 是授权任务集，X，Y⊆GT，如果执行 Y 的前提条件是执行 X，则称 Y 依赖于 X，并称 X 为 Y 的前提条件任务，记作 X→Y。否则称 Y 不依赖于 X，记作 X↛Y。若 X→Y，并且 Y⊆X，则称 Y 平凡依赖于 X；若 X→Y，并且 X∩Y=∅，则称 Y 非平凡依赖于 X。显然，平凡依赖在授权语义上会造成"某些授权任务的执行以其自身预先执行为前提条件"的谬论，因此本文不予讨论，以下依赖均指非平凡依赖。

定义2 设 GT 是授权任务集，X，Y⊆GT，定义：

(1)若 X→Y，X∩Y=∅，并且∄ X'⊂X，使得 X'→Y，则称 Y 对 X 完全任务依赖，记作 $X \xrightarrow{F} Y$；

(2)若 X→Y，X∩Y=∅，并且∃ X'⊂X，使得 X'→Y，则称 Y 对 X 部分任务依赖，记作 $X \xrightarrow{P} Y$；

(3)若 X→Y，Z⊆GT，X∩Y=Z∩Y=X∩Z=∅，Y→X，并且 Y→Z，则 X→Z，称 Z 对 X 传递任务依赖，记作 $X \xrightarrow{T} Y$；

(4)若完成 X 的同时完成 Y，则称 X 与 Y 同步任务依赖，记作 $X \xrightarrow{S} Y$；

(5)若完成 Y 需要曾经完成 X，则称 Y 对 X 历史任务依赖，记作 $X \xrightarrow{H} Y$；

(6)若完成 Y 需要 X 在将来完成，则称 Y 对 X 将来任务依赖，记作 $X \xrightarrow{W} Y$。

定义2表明，授权任务之间存在错综复杂的相互依赖关系。正是由于这种相互制约才保证了授权任务执行的安全性。我们把所有授权任务依赖构成的集合记作 D。为了使授权任务执行控制最大化，避免造成错误的授权语义，需要对授权任务依赖集 D 进行约简。我们把既不包含平凡授权任务依赖，也不包含部分授权任务依赖的授权任务依赖集称为约简集，记作 D_{NF}。如果已知 D，则 D_{NF} 可按公式(1)求得：

$$D_{NF}=\{X\to Y \mid \forall X,Y\subseteq GT,\nexists X'\subset X: X\cap Y=\varnothing \wedge X\to Y\in D\wedge X'\to Y\in D\} \quad (1)$$

存在依赖的授权任务在其执行过程中还可能存在一定的序关系，这种序关系刻画了授权任务执行的有序性。

定义3 对∀ gt_i，$gt_j\in GT$，若 gt_i 必须在 gt_j 之前执行，则称 gt_i 与 gt_j 之间存在执行顺序关系，记作 $gt_i \prec^{\Delta t} gt_j$，其中 Δt 为 gt_i 领先 gt_j 执行的时间。若 gt_i 必须与 gt_j 同时执行，则称 gt_i 与 gt_j 之间存在执行并发关系，记作 $gt_i \prec^{0} gt_j$。若 gt_i 与 gt_j 的执行顺序无关，则称 gt_i 与 gt_j 之间不可比较，记作 $gt_i \not\prec gt_j$。

在上述概念基础上，下面讨论几种特殊的授权任务依赖：授权任务静态和动态互斥与协同。

定义4 设 *EXE* 为授权任务执行函数，$\pi_g(gt_i)$ 表示 gt_i 的执行者。对∀ gt_i，$gt_j\in GT$，若下列断言之一为真，则称 gt_i 与 gt_j 静态互斥，记作 $gt_i \ominus' gt_j$。

(1)$\pi_g(gt_i)=g_r\to\pi_g(gt_j)\neq g_r \vee \pi_g(gt_j)=g_r\to\pi_g(gt_i)\neq g_r$。即这两个授权任务不能由同一个任务执行者完成。

(2)$EXE(gt_i)\to\neg EXE(gt_j)$。即如果已执行 gt_i，则禁止执行 gt_j。

性质1 二元关系 $\ominus'$ 是反自反的，传递的。

授权任务是通过任务会话 gs 完成的。一个 gs 只对应一个任务执行者，但可以对应一个或多个任务。任务静态互斥是对授权任务执行的一种强约束。有时候，需要把这种约束要求降低以完成授权任务。于是，我们给出动态任务互斥概念，并称其为授权任务执行的一种弱约束。

定义5 设 *Gsession* 为授权任务会话函数，*Gsession*(gs_k) 表示 gs_k 对应的授权任务集。对∀ gt_i，$gt_j\in GT$，若 $gt_i\in Gsession(gs_k)\Rightarrow gt_j\notin Gsession(gs_k) \vee gt_j\in Gsession(gs_k)\Rightarrow gt_i\notin Gsession(gs_k)$，则称 gt_i 与 gt_j 动态互斥，记作 $gt_i\ominus^d gt_j$。

性质2 二元关系 $\ominus^d$ 是反自反的，对称的，传递的，即是偏序关系。

授权任务之间除了可能存在互斥关系之外，还可能存在协同关系。

定义6 对∀ gt_i，$gt_j\in GT$，若下列断言之一为真，则称 gt_i 与 gt_j 静态协同，记作 $gt_i\oplus' gt_j$。

(1)$\pi_g(gt_i)=g_r\to\pi_g(gt_j)=g_r \vee \pi_g(gt_j)=g_r\to\pi_g(gt_i)=g_r$。即这两个授权任务必须由同一个任务执行者完成。

(2)$EXE(gt_i)\to EXE(gtj)$。即如果执行 gt_i，则必须执行 gtj。

性质3 二元关系 $\oplus'$ 是自反的，传递的。

定义7 设 GS 为授权任务会话集，对∀ gt_i，$gt_j\in GT$，∃ $gs_k\in GS$，若 $gt_i\in Gsession(gs_k)\Rightarrow gt_j\in Gsession(gs_k) \vee gt_j\in Gsession(gs_k)\Rightarrow gt_i\in Gsession(gs_k)$，则称 gt_i 与 gt_j 动态协同，记作 $gt_i\oplus^d gt_j$。

性质4 二元关系 $\oplus^d$ 是自反的，对称的，传递的，即是一个等价关系。

根据定义7很容易证明性质1～4。我们用 S_{ex}，D_{ex}，S_{co}，D_{co} 分别表示所有授权任务静态互斥偶对，动态互斥偶对，静态协同偶对，动态协同偶对构成的集合。传统的访问授权理论要求授予用户访问权限过程中应遵循用户职责分离原则，主要通过权限互斥实现[1,5]。相似地，我们通过授权任务互斥能够实现授权任务执行过程中的系统级职责分离，而且通过授权任务协同能够实现网络和分布式环境下复杂的授权策略——授权任务职责协同。事实上，授权任务职责分离可以看作为授权任务职责协同的特例。为了对授权任务职责协同(分离)一致性进行有效分析，我们可以把授权任务依赖关系用图表示。

定义8 授权任务依赖关系图 H(V，E)，其顶点 V={X，Y | ∀ X，Y⊆GT：X→Y∈D_{NF}}表示授权任务子集，弧 E={(X，Y) | ∀ X，Y∈V：X→Y∈D_{NF}}表示任务之间的依赖关系，弧上的标记表示任务间的依赖类型。

显然，授权任务依赖关系图 H(V，E)中不存在有向环。否则会造成某一授权任务的实施以其自身首先实施为前提条件，这是荒谬的。访问授权任务依赖关系的图表示是比较复杂的。造成这种复杂性的原因在于有些访问授权任务执行的前提条件中存在一个以上的授权任务。在授权任务依赖图上表现为图的某些结点包含多个原子任务，我们称这类结点为复合结点，把只包含一个原子任务的结点称为单结点。为了方便研究与实现，通过引入辅助结点消除 H(V，E)的所有复合结点和复合结点到其它结点的弧，使其转化为访问授权任务依赖关系简单图 $G(V_s,E_s)$。为此，先证明以下命题：

命题1 对∀ X→Y∈D_{NF}，X，Y 总可以表示为原子授权任务 gt_i，$gt'_j\in GT$ 的析取范式，即

$$X\to Y\equiv(gt_1\wedge\cdots\wedge gt_n)\to(gt'_1\wedge\cdots\wedge gt'_r)\vee\cdots\vee(gt'_{i+r}\wedge\cdots\wedge gt'_m)$$

其中 ∧ 和 ∨ 分别为"并且"、"或者"连接符，对∀ $gt_i\in X$，∀ $gt'_j\in Y$，$gt_i\neq gt'_j$。

证明 对∀ X→Y∈D_{NF}，根据 X→Y 的定义，X 中所包含的原子授权任务必须全部执行，才能够执行 Y 包含的全部或部分原子授权任务。假设 X 包含 n 个原子授权任务，Y 包含

m 个原子授权任务，则 X 总可以表示为 $gt_1 \wedge \cdots \wedge gt_n$，Y 总可以表示为 $(gt'_1 \wedge \cdots \wedge gt'_i) \vee \cdots \vee (gt'_{i+r} \wedge \cdots \wedge gt'_m)$。假设 $\exists\, gt_i \in X, \exists\, gt'_j \in Y, gt_i = gt'_j$，则造成 gt'_j 的执行需要与其等价的 gt_i 预先执行为前提条件，这是荒谬的，因此 $gt_i \neq gt'_j$。(证毕)

定义9 已知 H(V,E)，与 H(V,E)对应的 G(V,,E,)是按如下规则消去 H(V,E)的复合结点和复合结点到其它结点的弧之后所产生的有向图，其中 x' 为引入的辅助结点。

(1)如果 $X \rightarrow Y \equiv (gt_1 \wedge \cdots \wedge gt_n) \rightarrow (gt'_1 \wedge \cdots \wedge gt'_m)$，则用图1(a)表示；

(2)如果 $X \rightarrow Y \equiv (gt_1 \wedge \cdots \wedge gt_n) \rightarrow (gt'_1 \vee \cdots \vee gt'_m)$，则用图1(b)表示。

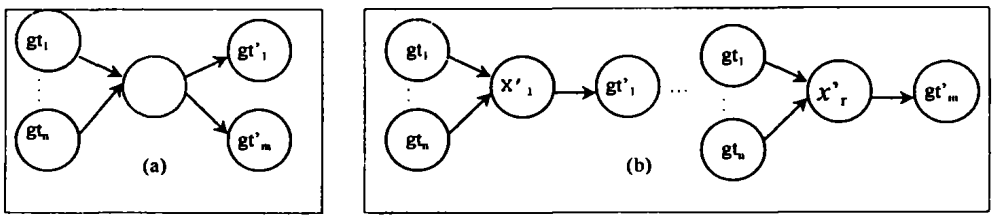

图1 访问授权任务依赖关系简单图表示

对 H(V,E)的每一个结点按定义9进行转化即可得到其所对应的授权任务依赖关系简单图 G(V,,E,)。

已知访问授权任务依赖关系集 $D_{NF} = \{gt_1 \rightarrow gt_2, gt_1 \rightarrow gt_4, gt_3 \rightarrow gt_4, (gt_2 \prec^{\Delta t} gt_3) \rightarrow gt_5, \}$，其等价集为 $D_{NF}' = \{gt_1 \rightarrow gt_2, gt_1 \rightarrow gt_4, gt_3 \rightarrow gt_4, (gt_2 \wedge gt_3) \rightarrow gt_5, gt_2 \prec^{\Delta t} gt_3\}$，其图形表示如图2所示。按定义9对图2进行转化所得的 G(V,,E,)如图3所示。

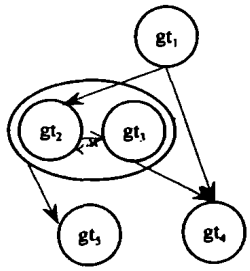

图2 访问授权任务依赖关系图

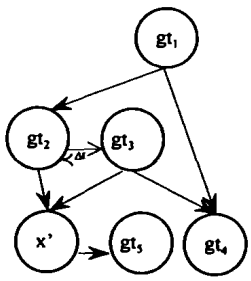

图3 访问授权任务依赖关系图转化的简单图

在上述访问授权任务依赖概念基础上，我们提出一种授权任务职责分离与协同新概念。

定义10 对 $\forall\, gt_i, gt_j \in GT, \exists\, gr \in U, \exists\, gs \in GS$，定义：

(1)若 $(\pi_g(gt_i) = g_r \wedge \pi_g(gt_j) = gr) \Rightarrow (gt_i, gt_j) \notin S_{ex}$，则称该访问授权系统具有静态职责分离性。

(2)若 $(gt_i \in Gsession(gs_k) \wedge gt_j \in Gsession(gs_k)) \Rightarrow (gt_i, gt_j) \notin D_{ex}$，则称该访问授权系统具有动态职责分离性。

(3)若 $(\pi_g(gt_i) = g_r \wedge \pi_g(gt_j) = g_r) \vee (EXE(gt_i) \rightarrow EXE(gt_j)) \Rightarrow (gt_i, gt_j) \in S_{co}$，则称该访问授权系统具有静态职责协同性。

(4)若 $gt_i \in Gsession(gs_k) \wedge gt_j \in Gsession(gs_k) \Rightarrow (gt_i, gt_j) \in D_{co}$，则称则称该访问授权系统具有动态职责协同性。

3 访问授权任务依赖关系时间着色 Petri 网表示

现有的授权模型绝大多数采用子句逻辑程序语言[4](clauses in a logic program)表达访问授权需求，采用访问授权状态图(state chart)或计算树逻辑(computational tree logic)对访问授权一致性进行分析。但是，这几种方法都不同时具有严格的数学基础、直观的图形表达和可视化动态仿真分析功能。Petri 网作为动态系统建模、验证与分析的有效方法，同时兼有上述特点，而且已有丰富的软件分析工具被广泛使用。作为一种高级 Petri 网——时间着色 Petri 网(timeed colored petri nets，TCPN)，其丰富的颜色信息和时间约束表达能力、高度抽象性，使得 TCPN 比普通 Petri 网(OPN)所建模型规模小，能够提供更简洁的系统概念视图。授权任务依赖关系是一种复杂的动态关系，某一授权任务是否可执行不仅与时间有关，而且与其它授权任务状态、用户授权约束等因素相关。因此 TCPN 是一种有效的访问授权任务依赖关系建模方法。

3.1 时间着色 PETRI 网 TCPN

定义11 基本 Petri 网(OPN)是一个四元组，PN＝(P，T，ARC，M)，其中，P 是库所有限集，T 是转移有限集，ARC $\subseteq (P \times T) \cup (T \times P)$ 是弧有限集，$P \cap T = \varnothing$，$P \cup T \neq \varnothing$，$M: P \rightarrow N$，是库所标识，N 为自然数。

定义12 时间着色 Petri 网是一个十元组 TCPN＝(PN，$^\bullet t$，$t^\bullet$，S_c，F_c，F_{arc}，F_t，C_t，F_D，F_{tu})，其中，PN＝(P，T，ARC，M)是一个基本 Petri 网，m(p)是 p 的标记，它是 p 的托肯关于不同颜色的多重集。$^\bullet t = \{p \mid \forall\, p \in P: (p,t) \in ARC\}$ 是转移 t 的输入库所。$t^\bullet = \{p \mid \forall\, p (P: (t,p) \in ARC\}$ 是转移 t 的输出库所。S_c 是颜色有限集。F_c 是颜色函数，$F_c(p) \subseteq S_c$，并且 $F_c(m(p)) \subseteq F_c(p)$。$F_{arc}$ 是弧函数，使得对 $\forall\, (p,t), (t,p) \in ARC$，$F_{arc}((p,t)) \subseteq F_c(p)_{MS}$，$F_{arc}((t,p)) \subseteq F_c(p)_{MS}$，$F_c(p)_{MS}$ 是所有颜色多重集构成的集合。F_t 是转移 T 上的时间区间函数，对 $\forall\, t \in T$，$F_t: t \rightarrow [\tau_x, \tau_y]$，并且 $\tau_x \leqslant \tau_y$。C_t 是 t 上的约束函数，对 $\forall\, t \in T$，$C_t(t)$ 表示 t 上的约束集。F_D 是库所上的延迟函数，对 $\forall\, p \in P$，$F_D: p \rightarrow [\tau_x^p, \tau_y^p]$，并且时间量 $\tau_x^p \leqslant \tau_y^p$。$F_{tu}$ 是一个时间戳函数，$F_{tu}(m(p)) = \sigma, \sigma \in T$ 是一个时间量，表示 p 的托肯(c，σ)到达 p 的时间，其中 $c \in S_c$。p 的所有托肯构成的集合记作 token(p)。

定义12表明，每一个托肯有一个颜色，每一个库所有一个颜色集 $F_c(p)$，能够进入该库所的托肯所携带的颜色必须属

于 $S_c(p)$。每一条弧(p,t)或(t,p)与一个弧函数 $F_{arc}(p,t)$或 $F_{arc}(t,p)$对应，$F_{arc}(p,t)$或 $F_{arc}(t,p)$是 $F_c(p)$的多重集的子集。当某一转移点火时，可能发生颜色转换。转移点火由点火规则和弧函数 $F_{arc}(p,t)$以及 $F_{arc}(t,p)$决定。

定义13 已知转移 t，$F_t(t)=[\tau_x^t,\tau_y^t]$，$\forall p_i\in {}^\cdot t$，$(c_{i1},\sigma_{i1})$，$(c_{i2},\sigma_{i2})$，…，$(c_{in},\sigma_{in})$是 p_i 的托肯，则以下结论成立：

(1)对$\forall (c_{ij},\sigma_{ij})\in token(p_i)$，如果 $\sigma_{ij}\in[\tau_x^t,\tau_y^t]$，则$(c_{ij},\sigma_{ij})$是可用的；在时间区间$[\tau_x^t+\sigma_{ij},\tau_y^t+\sigma_{ij}]$内是活的。

(2)在时刻 τ，如果 $F_{arc}(p_i,t)\leqslant m(p_i)$，并且对$\forall p_i\in {}^\cdot t$，$\exists (c_{ij},\sigma_{ij})\in token(p_i)$，$(c_{ij},\sigma_{ij})$是活的，则转移 t 是活的。

(3)如果$(MAX\{(\tau_x^t+\sigma_{ij})\mid\forall p_i\in {}^\cdot t:\exists (c_{ij},\sigma_{ij})\in token(p_i)\}\leqslant\tau_y^t)\wedge(MIN\{(\tau_y^t+\sigma_{ij})\mid\forall p_i\in {}^\cdot t:\exists (c_{ij},\sigma_{ij})\in token(p_i)\}\geqslant\tau_x^t)$恒为真(true)，那么转移 t 在点火时间区间$[\tau_x^t,\tau_y^t]$内是可以点火的。

(4)假设转移 t 在时刻 τ 点火，则产生一个新的标记 $m'(p_h)=m(p_h)+F_{arc}(t,p_h)$，$m'(p_i)=m(p_i)-F_{arc}(p_i,t)$。其中，+、−是关于颜色的多项式加减运算。

3.2 访问授权任务依赖关系的 TCPN 表示

访问授权任务依赖关系的 TCPN 表示就是把一个访问授权任务依赖关系简单图 $G(V_s,E_s)$转换为一个 TCPN，并给出 TCPN 各组成元素的相关语义。我们给出一个转换算法如下：

算法1 访问授权任务依赖关系简单图 $G(V_s,E_s)$转换为 TCPN。

输入：一个 $G(V_s,E_s)$，$SUB=\{x_i'\mid\forall x_i'$：$x_i'$ 是 G 的辅助结点$\}$。

输出：一个与 $G(V_s,E_s)$对应的 TCPN。

BEGIN

①对$\forall x\in V_s-SUB$，把 x 表示为 TCPN 的一个库所 p。x 的前提条件析取式中的所有析取元构成 p 的颜色集 $F_c(p)$。p 的托肯是一个二元序偶(c,σ)，其中 $c\in F_c(p)$是托肯的颜色，$\sigma\in T$ 是一个时间戳，表示托肯(c,σ)到达 p 的时刻，p 的所有托肯构成的集合称为 p 的托肯集，记作 token(p)。定义 P 的时间延迟 $F_D(p)=[\tau_x^p,\tau_y^p]$。其中，$\tau_x^p\leqslant\tau_y^p$，表示 p 上的访问授权任务能够作为其它访问授权任务执行的前提条件的有效时间范围。

②对$\forall x'\in V_s$，如果 $x'\in SUB$，则把 x' 表示为 TCPN 的一个转移 t 表示授权任务执行。给每个转移 t 定义一个可点火时间区间 $F_t(t)=[\tau_x^t,\tau_y^t]=[\tau_x,\tau_y]$，表示授权任务执行的时间区间。定义 $C_t(t)$为 t 上的授权约束集[2]。

③对$\forall x,y\in V_s-SUB$：$\exists (x,y)\in E_s$，则在结点 x，y 之间创建转移 t，创建弧(x,t)和(t,y)，删除弧(x,y)。$Ft(t)$和 $C_t(t)$同②。

④对$\forall (p_i,t),(t,p_i)\in ARC$，弧函数 $F_{arc}(p_i,t)\subseteq F_c(p_i)_{MS}$，$F_{arc}(t,p_i)=c_1+\cdots+c_n$，其中，$1\leqslant k\leqslant n$，$c_k\in\bigcup_{p\in {}^\cdot t}F_{arc}(p,t)$。

//＊＋表示关于颜色的多项式加法运算＊//

⑤对$\forall p\in P$，$m(p)$为 p 上访问授权任务能够作为其它访问授权任务前提的最大数。

⑥对$\forall x,y\in V_s-SUB$，如果 x，y 之间存在 $x\prec^{\Delta t}y$，则对应的 p_i 到 p_j 之间用一时延弧连接。

END

由于上述算法中的所有集合均为有限集，因此算法1是可终止的。下面给出授权任务执行定义。

定义14 授权任务是可执行的，当且仅当 t 是可点火的，并且 $C_t(t)$中的每一个约束被满足。

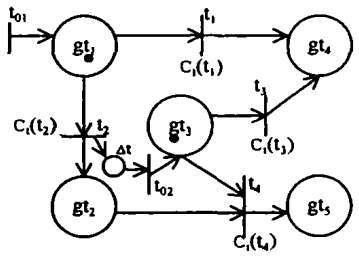

图4 图3转换的 TCPN

应用算法1对访问授权任务依赖关系简单图3进行转换所得 TCPN 如图4所示。

访问授权任务依赖关系的一致性是指在任一时刻 t 访问授权任务依赖关系简单图 $G(V_s,E_s)$中不存在有向环。使用 TCPN 表示访问授权任务依赖关系之后，访问授权任务依赖关系的一致性分析等价于对 TCPN 的可达性分析。TCPN 可达性分析方法参见文[9]。

结束语 本文以实现访问授权任务本身的职责分离与协同为目的，讨论了访问授权任务依赖的若干性质。访问授权任务互斥与协同关系不仅能够在系统级实现访问授权任务职责分离，而且能够实现访问授权任务职责协同。特别是在网络和分布式环境下，访问授权任务互斥与协同关系能够有效实现多个授权者协同完成授权任务，从而更有效地保证了访问授权任务执行的安全性。访问授权任务依赖关系时间着色 Petri 网原形实验表明，TCPN 模型能够有效地实现访问授权一致性动态可视化分析。引入访问授权任务互斥与协同机制之后，需要建立新的系统全局授权任务执行日志，以便对访问授权任务执行情况进行检索、跟踪和审计；高效的授权任务执行冲突消解算法也需要进一步研究。

参 考 文 献

1 Department of Defence (USA). Department of Defense Trusted Computer system evaluation criteria [R], DoD 5200-78-STD, DoD, 1985

2 Sandhu R, Ferraiolo D, KuhnR. The NIST model for role-based access control: towards a unified standard. In: Proc. of 5th ACM Workshop on Role-Based Access Control[C]. ACM, Berlin, Germany, July, 2000

3 Sandhu R, et al. Role-baseed access control model[J]. IEEE Computer, 1996, 29(2)

4 Woo T Y C, Lam S S. Authorization in distributed system: A new approach[J]. Journal of computer security, 1993, 2(3)

5 Sandhu R. Separation of duties in computerized Information Systems[M]. InSushil Jajodia and Carl Landwehr, editor, Database Security, IV: Status and Prospects, North Holland, 1991. 179～180

6 Sandhu R, Samarati P. Access control principlesand practice[J]. IEEE Comm., sept. 1999. 40～48

7 LiuHi Huiri. Role-based access control: A natural approach[C]. In: Proc. of the 1st ACM Workshop on Role-Based Access Control. ACM, 1997

8 LIU Qi-Yuan, LIU Yi. Database and information security[M]. publishing huose of science, 2000

9 W. M. P. van der Aalst. Timed colored petri nets and their application to logistics. PhD thesis, Eindhoven University of Technology, Eindhoven, 1992

10 YUAN Chong-Yi. Petri nets principle[M]. Publishing house of electronics industry, 1998(袁崇义. Petri 网原理. 电子工业出版社, 1998.)

11 Abrames M D, et al. A generalized framework for access control: A informal description. In: Proc of 13th national computer security conf. 1990