基于CPN的BPEL活动协同授权一致性检测机制研究

上超望[1,2] 刘清堂[1] 赵 刚[1] 童名文[1]
(华中师范大学教育信息技术学院 武汉 430079)[1]
(青少年网络心理与行为教育部重点实验室 武汉 430079)[2]

摘 要 BPEL访问控制机制是Web服务安全组合研究的重要内容,如何维护活动协同授权的一致性是其中的难点。通过扩展的CPN(有色Petri网)对BPEL活动协同授权执行的动态行为语义进行建模,利用可覆盖树方法分析协同授权模型状态变迁发生的序列,实现活动协同授权约束一致性的动态检测,为组合Web服务中业务流程协同授权约束设计的一致性提供合理的理论基础。最后,通过实例说明了检测机制的有效性。

关键词 BPEL,组合Web服务,活动,协同授权,CPN,一致性检测
中图法分类号 TP393 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2014.07.016

Study on Mechanism of Consistency Detection in BPEL Activities Authorization Coordination Based on CPN

SHANG Chao-wang[1,2] LIU Qing-tang[1] ZHAO Gang[1] TONG Ming-wen[1]
(Department of Information Technology, Central China Normal University, Wuhan 430079, China)[1]
(Key Laboratory of Adolescent Cyberpsychology and Behavior of Ministry of Education, Wuhan 430079, China)[2]

Abstract Mechanism of BPEL access control is one of focal points in Web services secure composition. It is a difficult problem to maintain the activities authorization constraint coordination. With the extended CPN(Colored Petri Nets) for modeling the dynamic behavioral semantics of BPEL activities execution, this paper used the method of coverability tree to analyze the fire sequence of model state transition, and implemented the dynamic consistency detection of activities authorization coordination. The paper provided theoretical foundation for the detection and optimization in the design of BPEL activities authorization coordination. At last, an example proved the efficiency of the mechanism.

Keywords BPEL, Composite Web services, Activity, Authorization coordination, CPN, Consistency detection

1 引言

业务流程执行语言BPEL(Business Process Execution Language)提供了Web服务组合的标准模型[1],它以流程的方式定义了Web服务的协同方式。BPEL活动之间具有分工性、依赖性和交互性的特点,其调用比一个单独Web服务调用需要更多的安全需求,需遵循动态授权、最小权限原则和职责分离原则[2]。合理有效的BPEL访问控制机制可防止用户越权访问对组合服务信息的完整性造成破坏,如何维护活动协同授权的一致性是其中的难点[3]。

目前,BPEL活动授权的一致性检测研究已出现了一些成果,它们各有特点。典型的如文献[4]将活动授权的安全需求表达为施加在用户和角色上的XACML约束向量,并利用约束向量的适配计算对活动协同授权进行一致性分析。然而,这种方法对于流程的任何改变都需要对约束向量进行重新定义,计算量大且正确性难以保证。文献[5]基于BPEL授权树来执行协同授权的冲突发现,不足之处在于没有考虑流程活动之间的安全依赖关系,活动安全交互演算也缺乏直观表示。文献[6]通过协同规则的集合运算来保障协同授权一致性计算目标的完成,但无法准确描述流程执行时的动态行为语义,忽略了流程安全执行过程中的数据与控制驱动问题。文献[7]则基于活动授权数组来简化授权依赖的合理性计算,然而对服务之间存在的各种动态关系缺乏分析,也无法对授权执行状态进行有效监控。文献[8]基于流程授权规则模板图对授权一致合理性检验,但无法描述流程活动授权状态转换的过程和条件。已有研究主要从静态视角进行BPEL活动协同授权的合理性验证,无法刻画流程运行时的动态行为特征,不能满足业务流程活动授权动态协同的一致性检验需求。

本文通过扩展CPN,提出了一种BPEL活动协同授权的一致性检测机制,对BPEL活动协同授权进行了定义,详细论述了基于扩展CPN的活动协同授权建模和一致性检测机制,并在最后通过实例对检测机制进行了验证。

2 BPEL活动协同授权的定义

定义1 授权活动是一个八元组 $aa::=(a,s,o,p,IN,OUT,f_a,l)$。设$U$和$O$分别为用户集和对象集,$actMark$为

到稿日期:2013-04-20 返修日期:2013-05-20 本文受华中师范大学中央高校基本科研业务费项目(CCNU13A05053),教育部人文社科项目(11YJA880163),湖北省教育规划课题(2011B039),武汉市科技计划项目(2014060101010030),国家"十二五"科技支撑计划课题(2012BAD35B02)资助。

上超望(1980—),男,博士,副教授,硕士生导师,主要研究方向为数字版权、服务计算等,E-mail:scw@mail.ccnu.edu.cn;**刘清堂**(1969—),男,博士,教授,博士生导师,主要研究方向为智能服务、数字版权等;**赵 刚**(1982—),男,博士,教授,主要研究方向为知识服务、分布式计算等。

授权活动是否激活的 *Boolean* 型标记函数；a 表示当前活动；$s \in U$ 是授权活动的执行主体，若无用户，则对应 Null；o 是授权活动的执行客体，$o \in O$，对应于与授权活动相关联的 Web 服务，用 Web 服务 *porttype* 来表征；p 是对 Web 服务进行具体访问的许可，对应于 *porttype* 包含的操作 *operation*；映射函数 $f_a: A \rightarrow Type$ 表示原子授权活动所属类型，$Type = \{invoke, receive, pick\}$；$IN$ 和 OUT 分别为前提条件授权集和授权活动执行所产生的授权集，$IN \subseteq \{(u,p,o,l),s') \mid \forall u,s' \in U, \forall p \in P, o \in O: actMark(s') = \text{true}\}$，$OUT \subseteq \{(u,p,o,l),s) \mid \forall u,s \in U, \forall p \in P, o \in O: actMark(s) = \text{true}\}$；$l$ 为授权活动的生存期，一旦 l 终止，授权将被收回。

组合 Web 服务 BPEL 流程活动的授权集记作 Γ，$\Gamma = \{\langle u_i, role_i, a_i, o_i\rangle \mid 1 \leqslant i \leqslant n\}$。

定义 2 BPEL 活动授权状态(Authorization State)表示授权在授权活动生存期内可能经历的状态，记为 AS。业务活动授权有 6 种状态：

(1)睡眠状态(Dormant)，授权还不具备开始执行的先决条件，处于未激活状态；

(2)就绪状态(Ready)，活动授权的合法性条件已经得到满足，并等待调用的状态；

(3)运行状态(Running)，业务活动处于执行中，授权被成功激活，正在使用或消耗有效许可；

(4)挂起状态(Hold)，正处于运行态的授权因授权活动依赖约束或其它原因而强制处于暂停执行状态；

(5)失败状态(Failed)，如果授权执行正常结束前被终止，则授权步进入失败状态，失败状态没有任何后续状态；

(6)完成状态(Completed)，表示授权正确执行完毕。

如图 1 所示，当用户请求执行某个授权活动时，系统首先验证请求是否合法，若是则授权进入“Ready”状态，等待调用；若授权调用的条件完备，则授权将被激活并进入“Running”状态，否则转入“Hold”状态，直到授权调用条件完备恢复授权执行并进入“Running”状态；若授权成功执行完毕便进入“Completed”状态，否则进入“Failed”状态。

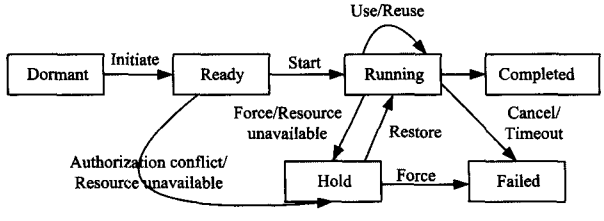


图 1 授权状态迁移图

定义 3 业务流程活动授权关系，表示不同活动授权之间基于依赖的协同关系，任意 3 个授权 $A = \langle u_i, role_i, a_i, o_i\rangle$，$B = \langle u_j, role_j, a_j, o_j\rangle$，$C = \langle u_k, role_k, a_k, o_k\rangle \in \Gamma$，如果 A 的执行受 B 的制约，则称 A 授权依赖于 B，记为 $A \lhd^d B$，业务活动授权关系可分为 4 类：

(1)同步关系：对 A 和 B，B 激活的前提是 A 进入激活状态，反之亦然，记为 $A \leftrightarrow B$。同步关系是一种等价关系，满足自反性、传递性、对称性，若 $A \leftrightarrow B, B \leftrightarrow C$，则 $A \leftrightarrow C$。

(2)顺序关系：对 A 和 B，必须先激活 A，才能激活 B，记为 $A \rightarrow B$。顺序关系满足非自反性、传递性、非对称性，若 $A \rightarrow B, B \rightarrow C$，则 $A \rightarrow C$。

(3)互斥关系：对 A 和 B 不允许同时激活，记为 $A \rightarrow\!\!\!\!\!\!\leftrightarrow B$ 或 $B \rightarrow\!\!\!\!\!\!\leftrightarrow A$。互斥关系满足非自反性、非传递性、对称性。

(4)分权关系：对 A 和 B，必须由不同实体激活，记为 $A \rightleftharpoons B$ 或 $B \rightleftharpoons A$，分权关系满足非自反性、非传递性和对称性。

在这几种业务活动授权关系中，互斥依赖关系和分权依赖关系与当前授权执行上下文无关，是静态关系；同步依赖和顺序依赖取决于权限所处的执行状态，是动态关系。

定义 4 BPEL 活动动态协同授权，安全组合服务调用的一次会话(Session)过程中，存在依赖关系的业务活动授权 A，$B \in \Gamma$，A 和 B 权限的授予或收回，要么全部实施，要么全部不实施，才能保证安全策略的语义完整性，并且在 A 被激活并经过 Δt 时间后必须激活 B，则称 A 与 B 存在动态协同授权关系，记为 $A\Theta^{dc}B$，即 $A\Theta^{dc}B \Rightarrow (A \lhd^d B) \wedge ((Exe(A) \leftrightarrow Exe(B)) \wedge (\neg Exe(A) \leftrightarrow \neg Exe(B)) \wedge ((active(A,t_1) \wedge active(B,t_2)) \wedge (t_1 - t_2 = \Delta t)) \wedge AuS(A,t_1) = AuS(B,t_2) = running \wedge AuS(A,t_2) = completed$，其中，$Exe(a)$ 是 Boolean 型授权实施标识函数，$active(a,t)$ 是授权激活谓词，t 是激活时间点，AuS 是授权的状态函数。业务活动动态协同授权关系集记作 Dc。

定义 5 安全组合 Web 服务 BPEL 流程(Secure Business Process，SBP)是在 BPM 的基础上引入安全规则和约束定义而定义的，记为四元组 $SBP::=\langle \Gamma, E, Dc, aus\rangle$，其中，$\Gamma$ 为活动的授权集，E 为有向边集，Dc 为业务活动动态协同授权关系集，映射函数 $aus: \Gamma \rightarrow AS$ 表示授权活动集 Γ 中每个活动的授权所处的状态。

3 BPEL 活动协同授权建模

3.1 BPEL 活动动态协同授权网

BPEL 活动动态协同授权网基于 CPN[9] 结构来定义。在本文后面的论述中，S_{ms} 表示非空集合 S 上的多重集，$type(v)$ 表示变量 v 的类型，$val(as)$ 表示授权状态变量的取值，$type(expr)$ 表示表达式 $expr$ 的类型，$var(expr)$ 表示表达式 $expr$ 中的变量的集合。

定义 6 形式上，BPEL 活动动态协同授权网 $BACA\_net = (\Sigma, As, P, T, F, C, G_e, E, I, M_0)$ 是一个多元组，其中：

(1)Σ 是非空有限的颜色集，表示活动授权中涉及的数据类型。

(2)As 是授权状态变量有限集，用以表示在安全组合服务调用的一次会话(Session)过程中各活动的授权状态，且 $\forall as \in As, type(as) \in \Sigma$。

(3)P 为库所有限集，T 为变迁有限集，$P \cup T \neq \Phi \wedge P \cap T = \Phi$。

(4)$F \subseteq (P \times T) \cup (T \times P)$ 是有向弧集合，F 称为流关系。

(5)C 是一个数据类型函数，定义为 $C: P \rightarrow \Sigma$，即每个库所中 token 都属于数据类型 $C(p)$。

(6)Ge 是扩展的防卫函数，可以从 T 生成表达式。$Ge = Ge_{pre} \cup Ge_{effc}$，$\forall t \in T, Ge(t) = Ge_{pre}(t)/Ge_{effc}(t)$，$type(Ge_{pre}(t)) = Boolean \wedge type(var(Ge_{effc}(t))) \subseteq As$ 其中，$Ge_{pre}: T \rightarrow$ [*Boolean* 表达式]，$Ge_{effc}: T \rightarrow$ [授权状态变量赋值表达式]，Ge_{pre} 是变迁前提条件函数，指定除输入参数外调用授权活动的许可操作必须满足的条件；Ge_{effc} 是变迁后继效果函数，指定授权活动操作后产生的安全效果。

(7)E 是弧表达式函数，用于表示调用 BPEL 授权活动使能的输入、输出参数，定义为 $E(f)$，满足 $f \in F: type(E(f)) = C(p)_{Ms} \wedge type(var(E(f))) \subseteq \Sigma$，其中 p 为 f 连接的库所。

(8)I 是初始化函数，定义为初始运行时 P 所包含的颜色

集，可表示为 $\forall p\in P: type(I(p))=C(p)_{MS}$，在 BPEL 活动动态协同授权执行过程中，$I$ 对应用户提供的输入参数。

(9)仅存在一个源库所 i 和汇结库所 o，满足 $i,o\in P$，使得 ${}^*i=\Phi\wedge o^*=\Phi$，并且每一个结点 $x\in P\times T$ 都位于从 i 到 o 的一条路径上，若在 T 中添加一个变迁 t^*，并在 F 中加入元素 (i,t^*) 和 (t^*,o) 得 $BACA\_net^*$，则 $BACA\_net^*$ 是强连通的。

(10)M_0 是初始标识，$M_0: P\rightarrow\{0,1,2,\cdots\}$。

定义 6 描述了 $BACA\_net$ 的静态结构，与一般 CPN 相比，对变迁函数进行了扩展，同时增加了一个授权状态变量有限集，使 $BACA\_net$ 能够对 BPEL 活动授权的动态行为进行准确刻画。

3.2 *BACA_net* 动态行为

定义 7 BPEL 活动动态协同授权网标识，令 $CA_n=(\Sigma, As,P,T,F,C,G_e,E,I,M_0)$ 为 $BACA\_net$，则 $M_p: P\rightarrow\{C(p)\}$ 称为 CA_n 的流程业务标识；$M_s: As\rightarrow\{_{x\in As}val(x)\}$ 称为 CA_n 的授权状态标识；$M=M_p+M_s$ 统称为 CA_n 的标识。

根据定义 7，CA_n 的标识由两部分组成，在变迁被激发时，流程业务标识在库所间流动，表示信息空间中数据的传输和处理；授权状态标识则表示当前会话过程中各活动授权所处的状态，它对变迁激发具有约束作用。

定义 8(变迁使能) 变迁 t 在标记 M 下是使能的(enabled)，当且仅当：

(1)$\forall p\in {}^*t, E(p,t)\leqslant M_p(p)$；

(2)在 M_s 下，$Ge_{pre}(t)=\text{true}$。

${}^*t$ 是变迁 t 的前置库所，条件(1)表示使能变迁 t 的所有前置库所的 token 数必须大于弧表达式函数 $E(p,t)$；条件(2)表示变迁 t 应该满足变迁执行的逻辑条件。

定义 9(变迁激发) 当一个变迁 t 在标记 M 下使能时，它可以激发(occur)，若 M' 为 M 的后继状态，记作 $M[t\rangle M'$，$M'=M_p'+M_s'$，则 M' 满足以下条件：

(1)$\forall p\in P, M'(p)=$

$$\begin{cases} M_p(p)-E(p,t), & p\in {}^*t-t^* \\ M_p(p)+E(t,p), & p\in t^*-{}^*t \\ M_p(p)-E(p,t)+E(t,p), & p\in t^*\cap {}^*t \\ M_p(p), & p\in \text{其它} \end{cases}$$

${}^*t$ 与定义 8 中的定义相同，t^* 是变迁 t 的后继库所，满足条件：$t^*=\{p\mid (t,P)\ F\}$。

(2)$x\in As, M_s'(x)=Ge_{effc}(t)(x)$，其中 $Ge_{effc}(t)(x)$ 表示经过变迁 t 后继效果函数计算后，与变迁 t 所关联活动的授权状态变量 x 的新值。

定义 10(CA_n 模型终止) CA_n 模型的终止，意味着一个 token 由源点 i 移到汇点 o，即 $C(o)\neq\Phi$。

CA_n 的动态行为反映了 BPEL 流程中活动授权行为的动态性质，颜色值通过变迁的执行发生变化。模型的实施依赖于防卫函数的运行时解释，通过调整流程控制数据在不同实例中的变化，可以灵活地进行授权活动执行路径选择。

3.3 BPEL 活动动态协同授权建模

BPEL 活动动态协同授权建模包含授权活动建模、协同授权过程建模两个部分。授权活动建模用来分析如何将授权活动映射为 $BACA\_net$，协同授权过程建模则分析如何将 BPEL 活动的动态协同授权关系映射为 $BACA\_net$ 网结构。

3.3.1 授权活动建模

授权活动描述单个服务的一次交互过程，没有子过程，不可再分。授权活动到 $BACA\_net$ 的映射规则如下：

(1)授权活动映射为一个变迁 t，并将 t 命名为授权活动的名称；

(2)授权活动的输入状态映射为包含 token 的库所；

(3)协同授权关系定义了流程活动授权激活的输入条件，映射为变迁 t 的输入弧；

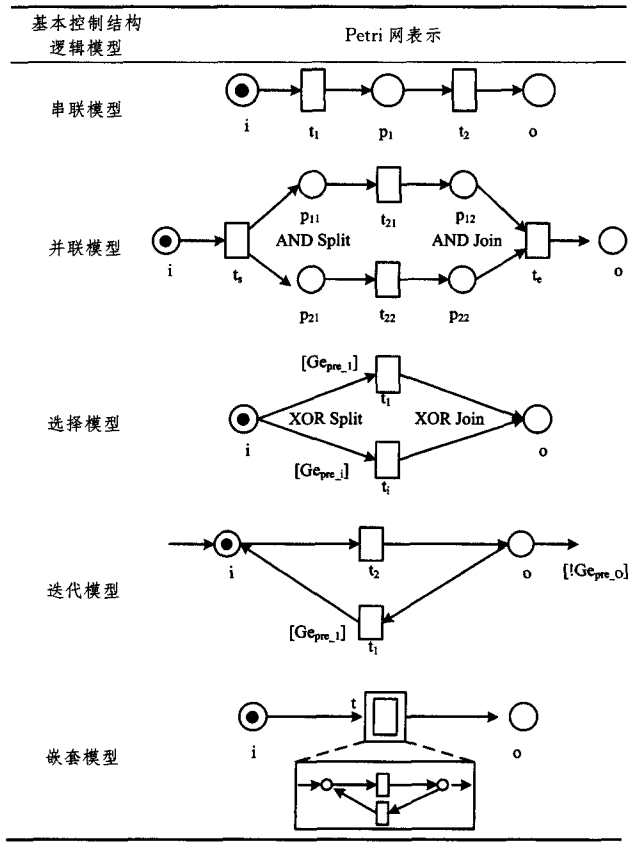
(4)授权活动的输出状态映射为输出弧；

(5)授权活动的执行效果映射为授权活动变迁完成后依据协同关系而定义的输出库所。

3.3.2 协同授权过程到 *BACA_net* 映射

协同授权过程到 $BACA\_net$ 映射可看作由若干原子授权活动通过基本逻辑结构进行动态协同授权关系嵌套建模的过程。如表 1 所列，根据表达语义不同，基本逻辑控制结构模型可分为 5 类。

表 1 基本逻辑控制结构模型的 Petri 网表示



(1)串联模型，后一变迁须等前一变迁顺利执行后才可执行，由 *Sequence* 模式组成；

(2)并联模型，表示并行的两个或多个活动可以任意顺序执行，由 *And Split* 和 *And Join* 两个构造模块组合而成，变迁 t_e 在所有分支都完成后才被激发；

(3)选择模型，表示多个分支只执行其中的一个，由模式 *XOR Split* 和 *XOR Join* 两个构造模块组合而成；变迁 $t_i(1\leqslant i\leqslant n)$ 是否被执行由防卫函数 Ge_{pre_i} 的取值来确定；

(4)迭代模型，当 token 满足某种条件时，t_1 必须多次连续重复执行，由 Iteration 模式组成；

(5)嵌套模型，用包含复合变迁(双线矩形)的结构来表示，嵌套模式可由其它子流程替换和表示，由 *Nesting* 模式组成。

BPEL 活动协同授权的 $BACA\_net$ 模型可按以下步骤递归构建：①按照 3.3.1 节映射规则进行原子授权活动建模；

②对每个基本控制逻辑结构按照相应的优先级和转换规则生成协同授权过程的 *BACA_net* 模型；③将每个基本逻辑控制结构 *BACA_net* 模型视为原子授权活动，再次使用协同授权过程到 *BACA_net* 的映射方法，生成更高一级逻辑控制结构的 *BACA_net* 模型；④重复②和③，直到协同授权业务流程涉及的所有原子授权活动都被包含到 *BACA_net* 模型中为止，得到 BPEL 活动协同授权的 *BACA_net* 模型。

4 BPEL 活动协同授权的一致性检测

4.1 BPEL 活动动态协同授权网分析

定义 11(BPEL 活动动态协同授权网的正确性) 令 M_0 是 *BACA_net* 的初始标识，M_f 是 *BACA_net* 的终止标识，BPEL 活动动态协同授权网模型所描述的协同授权约束一致性是正确合理的，当且仅当：

(1)对于初始标识 M_0 可达的任意标识 M'，存在一个激发序列 $\partial=t_{\partial 1}t_{\partial 2}\cdots t_{\partial n}$，使得标识 M' 可达标识 M_f，即 $\forall M'(M'\in R(M_0))\Rightarrow M'[\partial\rangle M_f$；

(2)标识 M_f(库所 o 包含一个 token 的标识)是从初始标识 M_0 可达的，则 M_f 是唯一满足库所 o 至少包含一个 token 标识，即 $\forall M(M=M_p+M_s\in R(M_0)\wedge M_p(o)\geqslant M_f(o))\Rightarrow(M=M_f)$；

(3) *BACA_net* 中无死变迁，即 $\forall t\in T,\exists M_1,M_2$ 使 $M_1\in R(M_0)\wedge M_1[t\rangle M_2$。

定义中的(1)描述的是从初始标志 M_0 开始，总能达到终止标志 M_f；(2)指的是当库所 o 中存在一个 token 时，其它库所应该为空；(3)表示初始标志中不存在死的变迁。

定义 12(扩展协同授权网) 扩展协同授权网 $\overline{BACA}$ 是在 *BACA_net* 中通过添加一个连接 o 与 i 的变迁 t^* 而得到的，即 $\overline{BACA}=(\Sigma,As,P,T\cup\{t^*\},F\cup\{\langle o,t^*\rangle,\langle t^*,i\rangle\},C,G_e,E,I,M_0)\wedge E(o,t^*)=M_f(o)\wedge E(t^*,i)=M_0(i)$。

定义 11 是 BPEL 活动动态协同授权网过程定义正确合理性的重要理论基础，但是要验证一个模型是否满足正确合理性需要遍历整个模型网的所有结点，过程比较繁琐。协同授权网的正确合理性与 Petri 网的活性和有界性是密切相关的，实际上，它可以通过验证协同授权网的结构特性来获得。文献[10]证明了一个一般业务流程建模的过程正确性的充要条件，可得定理 1。

定理 1 动态协同授权网 *BACA_net* 具有正确性的充要条件是：扩展的协同授权网 $\overline{BACA}$ 是活的并且有界。

4.2 BPEL 活动协同授权的一致性检测

定义 13(BPEL 活动动态协同授权的一致性) 称 BPEL 活动动态协同授权模型 *BACA* 为授权一致的，当且仅当 *BACA* 满足：①在任何可接受的授权状态下，*BACA* 所表示的动态行为过程总能执行完毕；②对于任意 *BACA* 所包含的子流程 sp，总存在合适的初始授权状态，使得 sp 被执行；③*BACA* 模型中不存在某个结点在任何情况下都因不能满足条件而无法执行。

定义 13 从 3 个方面对过程模型进行了约束，在将模型转化为 *BACA_net* 后，这些约束与定义 11 中 *BACA_net* 正确性约束实际上是一致的。基于协同授权模型所对应 *BACA_net* 的正确性计算方法，可以得到组合 Web 服务 BPEL 活动协同授权一致性检测算法，算法描述如下。

算法 1 组合 Web 服务 BPEL 活动协同授权一致性检测算法

输入：安全组合 Web 服务 BPEL 流程 SBP

输出：SBP 动态协同授权的一致性检测结果

Step 1 依据 3.3.1 节内容实现 BPEL 活动授权与协同授权关系到 BACA_net 的映射；

Step 2 依据 3.3.2 节内容构建 BPEL 活动动态协同授权的 BACA_net 模型；

Step 3 依据定义 12 生成 BACA_net 的扩展网 $\overline{BACA}$；

Step 4 根据 Petri 网可覆盖图生成算法生成 $\overline{BACA}$ 的可覆盖图 $CG(\overline{BACA})$，依据定理 1 分析 $\overline{BACA}$ 的活性和有界性，本文中对 Petri 网活性和有界性的判定方法可参见文献[11]中定理 3.2；

(1)如果 $CG(\overline{BACA})$ 中某个结点的标识向量中含有 ω 分量，则 $\overline{BACA}$ 无界，那么 BACA_net 不是正确合理的，返回 False；否则进入(2)；

(2)从 $CG(\overline{BACA})$ 的顶点 M_0 出发，检测 $CG(\overline{BACA})$ 的有向路径，如果当前有向路径中存在一个强连通子图 G[12]，并且 $\overline{BACA}$ 中的每个变迁都至少在 G 中出现一次，则当前有向路径检测通过，继续检测下一条路径，否则返回 False；如果所有有向路径均检测通过，则返回 True；

Step 5 检测完毕。

算法 1 使原本缺乏严格过程动态语义的协同授权模型能通过形式化的方法进行一致性分析和检测，其复杂度主要体现在计算 $\overline{BACA}$ 的活性和有界性上。由于 Step 4 中可覆盖图的创建是可终止的，因此算法 1 也是可终止的，Step 4 的计算复杂度与 BPEL 活动动态协同授权模型中的授权活动成正比。

算法 1 还直接体现了 Petri 网系统的运行机制，可以准确刻画协同授权系统的运行状况，使安全设计者能够快速发现协同授权模型中存在的问题，提高授权一致性的修复和优化的效率。

5 应用实例

我们设计了一个简化的企业原材料采购订单审核 Web 服务组合业务系统，如图 2 所示，系统业务流程采用“参与者 $\xrightarrow{扮演}$ 角色 $\xrightarrow{执行}$ 执行”的三维策略机制，由 6 个授权活动通过串联和选择逻辑结构组合而成。其中，a_1 与订单制订服务关联(执行角色：采购人员)；a_2 与订单校对服务关联(执行角色：采购主管)；a_3 与订单核算服务关联(执行角色：财务人员)；a_4 与订单金额复核服务关联(执行角色：财务人员)，如果订单金额 *VALUE* 小于 1 万元，则订单不需要批准，直接交给采购人员，如果订单金额 *VALUE* 大于 1 万元，则需要采购主管经理批准；a_5 与订单审批服务关联(执行角色：采购主管经理)；a_6 与采购通知单发送服务相关联(执行角色：采购人员)。流程中的权限集合 $P=\{P_1:Create\ Order,P_2:Audit\ Order,P_3:Account\ Order,P_4:Approve\ Order,P_5:Reject\ Order,P_6:Send\ Purchase\ Notification\}$。

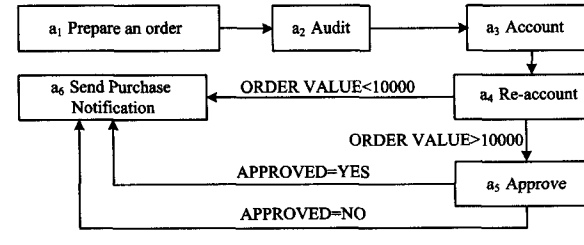


图 2 原材料采购订单审核服务系统业务流程

BACA_net 表示的原材料采购订单审核服务系统业务流程的安全模型如图 3 所示。

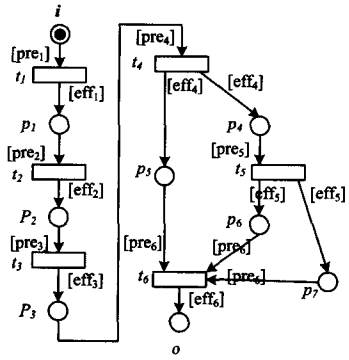


图 3 *BACA_net* 表示的审核服务业务流程

库所及语义描述：i：安全组合服务输入接口；P_1：原材料采购订单；P_2：校对后采购订单；P_3：采购订单金额核算报告；P_4：大额度订单金额复核报告；P_5：小额度订单金额复核报告；P_6：采购主管经理批准报告；P_7：采购主管经理否决报告；o：安全组合服务结束状态（采购通知单）。

变迁及语义描述：t_1，制订原材料采购订单；t_2，校对采购订单；t_3，核算采购订单金额；t_4，复核采购订单金额；t_5，大额度采购订单批准或否决决策；t_6，发送采购通知单。

前提条件及语义描述：前提条件包含两方面内容，前半部分表示授权活动在激发前需要遵循的流程安全策略，确保敏感的活动由不同的用户执行，避免诈骗行为的产生；后半部分要求前趋变迁所关联活动的授权已完成，实现动态授权。设授权活动 a_i 的执行角色用 $R(a_i)$ 表示，a_i 的授权状态用 $AuS(a_i)$ 来表示（$1\leqslant i\leqslant 6$），令 $Ge_{pre\_i}=pre_i$，$Ge_{effc\_i}=eff_i$，前提条件语义描述为：$[pre_1]::=Role(a_1)\neq Role(a_2)$；$[pre_2]::=Role(a_2)\neq Role(a_1)\wedge AuS(a_1)=completed$；$[pre_3]::=Role(a_3)\neq Role(a_4)\wedge AuS(a_2)=completed$；$[pre_4]::=Role(a_4)\neq Role(a_3)\wedge AuS(a_3)=completed$；$[pre_5]::=Role(a_5)\succ Role(a_2)\wedge AuS(a_4)=completed$；$[pre_6]::=Role(a_1)=Role(a_6)\wedge AuS(a_4)=completed\,|\,AuS(a_5)=completed$，其中，$\succ$ 表示角色的偏序关系，$Role(a_5)\succ Role(a_2)$ 表示 $Role(a_5)$ 支配 $Role(a_2)$。

后继效果及语义描述：定义授权活动执行后对授权状态的影响，确保活动执行完成后所有权限被收回，实现最小权限原则，其语义描述为：$[eff_1]::=AuS(a_1)=completed$；$[eff_2]::=AuS(a_2)=completed$；$[eff_3]::=AuS(a_3)=completed$；$[eff_4]::=AuS(a_4)=completed$；$[eff_5]::=AuS(a_5)=completed$；$[eff_6]::=AuS(a_6)=completed$。

利用前面的结果，基于算法 1 对图 3 的协同授权模型进行一致性检测，容易证明模型的扩展网保持活性和有界性，每个变迁都是活的，并且满足可控死锁的性质。因此，实例中原材料采购订单审核服务业务流程在安全协同进程中是授权一致的。

结束语 本文通过扩展 CPN 表达 BPEL 活动授权执行过程的动态行为语义，实现了活动协同授权约束一致性的形式化分析和检测。实例原形实验表明，*BACA_net* 能够有效地描述 BPEL 活动协同授权的状态和行为，降低协同授权建模的复杂性，保证开放环境下 BPEL 活动授权协同执行的安全性。本文对组合 Web 服务 BPEL 活动协同授权一致性检测机制的研究还需要不断完善。建立一套完整的协同授权模型自动生成、性质分析与验证工具，将是下一步主要研究的内容。

参 考 文 献

[1] 宋巍，唐金辉，张功萱，等. WS-BPEL 服务可替换性分析[J]. 中国科学：信息科学，2012，42(3)：264-279

[2] 唐佳俊，黄志球，王进. 一种 Web 服务组合的可信评估方法[J]. 计算机科学，2013，40(2)：163-168

[3] Manuel M，Nicola D. Implementing workflow reconfiguration in WS-BPEL[J]. Journal of Internet Services and Information Security，2012，2(2)：73-92

[4] Bertino E，Martino D L，et al. Security for Web services and service-oriented architectures[M]. Berlin：Springer，2010：170-175

[5] Ahmed A. A compliance management framework for Business Process models[D]. Potsdam：University of Potsdam，2010

[6] Rafael A. An approach to data-driven detective internal controls for process-aware information Systems[C]// Workshop on Data Usage Management on the Web 2012. 2012：20-25

[7] Mohsen R. Security analysis for web services compositions[J]. Journal of Scientific & Engineering Research，2012，3(5)：1-8

[8] Alberto C，Silvio R，et al. Automated validation of security-sensitive Web Services specified in BPEL and RBAC[C]// Proc of the 12th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing. 2010：456-464

[9] Barry D. Policy Driven Development：SOA Evolvability through Late Binding[D]. San Diego：University of California，2013

[10] Karima M. On Transforming Business Patterns to Labeled Petri Nets Using Graph Grammars[J]. Information Technology and Computer Science，2013，20(2)：15-27

[11] 吴哲辉. Petri 网导论[M]. 北京：机械工业出版社，2006：48-49

[12] Agnarsson G，Greenlaw R. Graph Theory：Modeling，Applications，and Algorithms[M]. New York：Prentice Hall Press，2007：89-97

（上接第 80 页）

[7] 朱俊，郭长国，吴泉源. 基于 Petri 网的 Web 服务交互行为一致性检测方法[J]. 计算机工程与科学，2013，35：28-33

[8] Murata T. Petri nets：Properties，analysis and applications[J]. Proceedings of the IEEE，1989，77(4)：541-580

[9] Smirnov S，Weidlich M，Mendling J. Business Process Model Abstraction Based on Synthesis From Well-Structured Behavioral Profiles[J]. Cooperative Information Systems，2012，21(1)：55-83

[10] Weidlich M，Mendling J，Weske M，et al. Causal Behavioural Profiles— Efficient Computation，Applications，and Evaluation [J]. Fundamenta Informaticae：Applications and Theory of Petri Nets and Other Models of Concurrency，2011，113(3/4)：399-435

[11] Koskinen J，Kettunen M，Systa T. Behavioral profiles—a way to model and validate program behavior[J]. Software：Practice & Experience，2010，40(8)：701-733

[12] Du Yu-yue，Jiang Chang-jun. A Formal Approach for Obligation Analysis of E-Commerce[J]. Chinese Journal of Electronics，2008，17(2)：200-204

[13] 钱柱中，陆桑璐，谢立. 基于 Petri 网的 Web 服务自动组合研究[J]. 计算机学报，2006，29(7)：1057-1066

[14] 汤宪飞，蒋昌俊，丁志军. 基于 Petri 网的语义 Web 服务自动组合方法[J]. 软件学报，2007，18(12)：2991-3000

[15] 吴哲辉. Petri 网理论[M]. 北京：机械工业出版社，2006：6-42