计算机科学 2003Vol. 30№. 7

一种新的安全 Petri 网及其多级安全机制分析*)

王小明[1,2] 赵宗涛[1,3] 袁崇义[4]

(西北大学计算机科学系 西安 710069)[1] (陕西师范大学计算机科学学院 西安 710062)[2]

(第二炮兵工程学院计算机科学系 西安 710025)[3] (北京大学计算机科学技术系 北京 100871)[4]

A Novel Multilevel Security Petri Net and its Security Analysis

WANG Xiao-Ming[1,2] ZHAO Zong-Tao[1,3] YUAN Chong-Yi[4]

(Department of Computer Science, Northwest Univeristy, Xi'an 710069)[1]

(Computer Science College, Shanxi Normal Univeristy, Xi'an 710062)[2]

(Department of Computer Science, the Second Artillery Engnieering College, Xi'an 710025)[3]

(Department of Computer Science and Technology, Peking University, Beijing 100871)[4]

E-mail: yangwr@snnu.edu.cn

Abstract Petri Net(PN) is a very important modeling methodology for dynamic concurrent system. Many PN models are available in existing literature, but a little attention has been paid to such a PN that supports multilevel secure policies. In this paper, a novel PN model, named as multilevel secure PN(MLSPN), is proposed, and its multilevel security mechanism is analysed formally. MLSPN has of a flexible and strong power to support a dynamic time constraint, and the security covert channel can also be eleminated. Therefore MLSPN may have practical application in many areas, such as secure workflow development, secure database design, and secure protocol analysis, etc.

Keywords Mutilevel security policies, MLSPN, Token flow, Token flow channel, Security covert channel

1 引言

Petri 网(PN)是一种重要的动态并发系统建模方法，具有因果相关、支持并发、异步和冲突消解等诸多优点，已广泛应用于复杂动态系统建模与仿真验证[2~5]，例如协议分析、工作流建模、数据库设计等。随着信息安全问题日益突出，迫切需要 PN 支持多级安全策略的系统建模，使得用 PN 建立的模型具有良好的多级安全保护机制。但是，现有的 PN 并不直接支持多级安全系统建模[5,8,9]，而且目前对安全 PN 的研究文献很少。虽然 V. Atluri 和 W. K. Huang 等[9]基于着色时间网(CTPN)提出了一种用于多级安全工作流系统建模的安全 PN，但他们只考虑了变迁之间的控制安全和时间安全约束，而忽略了十分重要的库所及其标识安全。H. Kang 等[8]使用流控制器技术(flow controller)提出了一种多级安全 PN，其基本思想是把一个多级安全系统首先划分为多个单级安全子系统，然后建立各子系统的 PN 子网，最后使用流控制器把多个不同安全级别的子网连接起来，构成一个多级安全 PN。但是，子系统划分往往相当复杂，有时候甚至是不可能的，而且分解后的每个单级安全子系统静态结构和动态行为固定不变，难以满足环境动态变化需要，模型复杂，在实际应用中难于使用。K. Knorr[9]基于基本 PN 提出了一种安全 PN 模型，但该模型只考虑了不同安全级别的变迁依赖，数据流和控制流分开建模，通常所建模型规模庞大，难于把握，而且对时间约束和库所及其标识安全性也未作讨论。更重要的是，上述模型均未对其托肯流安全性进行形式分析，而这一点却是多级安全模型研究必不可少的[12]。

因此，我们提出一种新的支持多级安全策略的 PN 模型(MLSPN)，并对其托肯流安全性进行形式分析，以满足多级安全系统建模需要。通过对经典 PN 的库所(place)、变迁(transition)和托肯(token)赋以不同的安全级和有效性时间约束，使驻留在每一个库所的托肯安全级小于或等于该库所的安全级，并且库所有效时间包含其托肯有效时间，以实现标识安全；通过变迁安全发生规则确保变迁对托肯的接收、处理和发送，满足多级安全原则，而且使托肯只能从低安全级库所向高安全级库所单向流动，从而实现“不可向上读(No-read-up)、不可向下写(No-write-down)”的 BLP 多级安全策略，并且有效消除了多级安全模型普遍难以防止的安全隐通道(convert channel)[1,2]。由于 MLSPN 采用了区间安全级(见第 2 节)，因此它能够克服目前仍然被广泛使用的经典多级安全 Bell-Lapadula(BLP)模型应用于商业系统建模时对主体和客体安全级匹配要求过于严格的缺点，把有效性区间时间作为 MLSPN 的库所、变迁和托肯的基本属性，使得 MLSPN 对动态时间约束的适应性增强，灵活性更大。

本文目的在于提出一种新的多级安全 PN 静态结构和动态行为规则，并对其多级安全机制进行形式分析。关于 MLSPN 的网特性(如可达性、活性等)分析不是本文所要讨论的，可以使用 PN 研究已有的结果对其进行分析，我们将另文介绍。

2 多级安全 PN(MLSPN)

为了定义一种新的多级安全 PN(MLSPN)，我们先给出

*)国家自然科学基金资助项目(No. 69973003, No. 9020402)，陕西师范大学重点科研基金(No. 2002995105)。王小明 博士，副教授，主要研究领域为信息系统安全、访问控制。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、系统安全。袁崇义 教授，博士生导师，主要研究领域为并行计算与 Petri 网、Petri 网理论及应用。

以下基本概念。

定义 1(多重集) 设 S 是非空有限集，N_0 是非负整数集，则函数 $MS: S \to N_0$ 称为 S 上的多重集(bag 或 multi-set)。

如果 $x \in S$，则 $MS(x)$ 表示 x 在多重集 MS 中出现的次数。S 的所有多重集构成的集合记作 S_{MS}。S_{MS} 的子集记作 $2^{S_{MS}}$，它也是多重集集合。多重集与普通集合的区别在于前者允许同一元素多次出现。例如，$\{x,y,y\}=\{x,2y\}$ 是 $\{x,y\}$ 上的多重集构成的集合，$MS(x)=1$，$MS(y)=2$。S 和 S_{MS} 的元素存在关系：$\forall\, x \in S, \forall\, y \in S_{MS}, \exists\,!\ y(x) \in N_0 : y = \sum_{x \in S} y(x) \cdot x$。设 $y_1 = \sum_{x \in S} y_1(x) \cdot x$，$y_2 = \sum_{x \in S} y_2(x) \cdot x$ 为 S 上的两个多重集，多重集上的加法(+)、大小比较(≤)和减法(−)运算定义为：

$$y_1 + y_2 = \sum_{x \in S} (y_1(x) + y_2(x)) \cdot x \tag{1}$$

$$y_1 \leqslant y_2 \equiv \forall\, x \in S : y_1(x) \leqslant y_2(x) \tag{2}$$

如果 $y_1 \leqslant y_2$，则 y_2 与 y_1 之差为：

$$y_2 - y_1 = \sum_{x \in S} (y_2(x) - y_1(x)) \cdot x \tag{3}$$

定义 2(区间安全级) 设 N_0 是非负整数集，N_0 上的闭区间集 $ISC = \{[c_l, c_u] \in N_0 \times N_0 \mid c_l \leqslant c_u\}$ 称之为区间安全级集合。

对 $\forall\, [c_{li}, c_{ui}], [c_{lj}, c_{uj}] \in ISC$：$[c_{li}, c_{ui}] \leqslant [c_{lj}, c_{uj}] \Leftrightarrow c_{li} \leqslant c_{lj} \wedge c_{ui} \leqslant c_{uj} \vee c_{ui} \leqslant c_{lj}$，偏序 $(ISC, \leqslant)$ 是一个格(lattice)。根据格的性质，如果 $\forall\, isc_1, isc_2, isc \in ISC, \exists\, \lambda \in ISC : isc_1 \leqslant \lambda \wedge isc_2 \leqslant \lambda \wedge isc_1 \leqslant isc \wedge isc_2 \leqslant isc \Rightarrow \lambda \leqslant isc$，则称 λ 为 isc_1 和 isc_2 的最小上界，记作 $\lambda = lub(isc_1, isc_2)$。

定义 3(区间时间) 时间点集是可数的时间点的无限集 $\mathscr{T} = \{\tau_0, \tau_1, \tau_2, \cdots,\}$，$[\tau_l, \tau_u] \in \mathscr{T} \times \mathscr{T}$，并且 $\tau_l \leqslant \tau_u$，表示 τ_l 到 τ_u 的时间间隔，称之为区间时间。称 $I\mathscr{T} = \{[\tau_l, \tau_u] \in \mathscr{T} \times \mathscr{T} \mid (\tau_l \leqslant \tau_u)\}$ 为区间时间集。

时间点 τ 是不可再分的最小时间单位，其粒度大小依赖于具体问题。如年、月、日、时、分、秒等。以下把时间点和区间时间通称为时间。对 $\forall\, \tau \in \mathscr{T}, \forall\, [\tau_l, \tau_u] \in I\mathscr{T} : \tau_l \leqslant \tau \wedge \tau \leqslant \tau_u$，则称 $[\tau_l, \tau_u]$ 包含 τ，记作 $\tau \in [\tau_l, \tau_u]$。对 $([\tau_{li}, \tau_{ui}], [\tau_{lj}, \tau_{uj}] \in I\mathscr{T} : \tau_{li} \leqslant \tau_{lj} \wedge \tau_{ui} \leqslant \tau_{uj}$，则称 $[\tau_{lj}, \tau_{uj}]$ 包含 $[\tau_{li}, \tau_{ui}]$，记作 $[\tau_{li}, \tau_{ui}] \Subset [\tau_{lj}, \tau_{uj}]$。$[\tau_{li}, \tau_{ui}]$ 和 $[\tau_{lj}, \tau_{uj}]$ 的重叠部分记作 $[\tau_{li}, \tau_{ui}] \Cap [\tau_{lj}, \tau_{uj}]$，并且

$$[\tau_{li}, \tau_{ui}] \Cap [\tau_{ij}, \tau_{uj}] = \begin{cases} [\max(\tau_{li}, \tau_{lj}), \min(\tau_{ui}, \tau_{uj})], & \text{当 } \tau_{lj} \leqslant \tau_{ui} \leqslant \tau_{uj} \\ \varphi, & \text{否则} \end{cases} \tag{4}$$

其中 φ 表示两个区间时间没有重叠部分。并且，对 $([\tau_{li}, \tau_{ui}] \in I\mathscr{T}, [\tau_{li}, \tau_{ui}] \Cap \phi = \phi$；对 $\forall\, \tau \in \mathscr{T}, \tau \in \phi = \text{false}$。

定义 4(基本 PN 静态结构) PN=(P,T,F,TK,M)，其中 P,T 分别是 PN 的库所和变迁非空有限集，$P \cap T = \varnothing$，$P \cup T \neq \varnothing$。$F \subseteq ((P \times T) \cup (T \times P))$ 是流关系。${}^\bullet t = \{p \mid p \in P, t \in T, (p,t) \in F\}$ 是 t 的输入集。$t^\bullet = \{p \mid p \in P, t \in T, (t,p) \in F\}$ 是 t 的输出集。TK 是托肯集。$M: P \to N_0$ 是 P 的托肯标识，N_0 是非负整数。p 上的托肯集记为 $m(p)$。

定义 5(基本 PN 变迁规则) 设 PN=(P,T,F,TK,M)，其变迁发生规则为 $\forall\, t \in T$，t 在标识 M 下是活的，当且仅当 $\forall\, p \in {}^\bullet t : m(p) > 0$。如果 t 在 M 下是活的，那么 t 是可以发生的。t 发生后产生新的标识 M′ 为 $\forall\, p_i \in {}^\bullet t, \forall\, p_j \in t^\bullet : m'(p_i) = m(p_i) - 1 \wedge m'(p_j) = m(p_j) + 1$。

著名的多级安全策略 BLP 模型的访问控制基本规则是将系统中元素按其特性区分为主体(Subject)与客体(Object)。主体是系统的主动元素，能执行一系列的动作，主要指进程；客体是系统中包含信息的被动元素，主体按照一定的规则访问客体。BLP 模型是基于系统中元素安全密级的，密级用安全级表示。只有当主体的安全级大于或等于客体的安全级时，主体才有权限“读”客体；只有当主体的安全级小于或等于客体的安全级时，该主体才有权限“写”客体。但是，由于 BLP 模型对主、客体安全级匹配的严格约束，从而能够确保军事等安全性要求很高的访问控制安全。不过，它在商用多级安全系统建模中不实用，因为商用系统通常比军事系统安全性要求低，但主体和客体数量庞大，关系复杂。如果采用 BLP 模型的“固定值”安全级，则可能降低系统的可用性，而使用区间安全级能够放松 BLP 模型的安全级匹配约束，使其更符合商用系统的实际需要。使用区间安全级概念的扩展 BLP 模型访问控制基本规则形式定义为：

定义 6 设 S 和 O 分别是系统主体集和客体集，$L: S \cup O \to ISC$ 是主体和客体安全级函数。如果 $\forall\, s \in S, \forall\, o \in O : L(o) \leqslant L(s)$，则 s 对 o 享有“读”权限；如果 $\forall\, s \in S, \forall\, o \in O : L(s) \leqslant L(o)$，则 s 对 o 享有“写”权限。

虽然人们对 BLP 模型已经作了许多改进，但它至今仍然是多级安全系统的基础。为讨论简单，我们把支持扩展 BLP 模型访问控制基本规则的 PN 称之为多级安全 PN(MLSPN)，其中变迁(transition)为主体(subject)，库所(place)和托肯(token)为客体(object)，其静态结构和动态行为形式定义如下：

定义 7 多级安全 PN 的静态结构是一个八元组 MLSPN=(P,T,F,TK,M,FTK,L,Γ)，其中 $P = \{(p, isc, it) \mid p \in P, isc \in ISC, it \in I\mathscr{T}\}$ 是库所集，p 是库所标识，isc 和 it 分别是 p 的区间安全级和有效区间时间。$T = \{(t, isc, it) \mid t \in T, isc \in ISC, it \in I\mathscr{T}\}$ 是变迁集，t 是变迁标识，isc 和 it 分别是 t 的区间安全级和有效时间。$F \subseteq ((P \times T) \cup (T \times P))$ 是流关系。$TK = \{(data, isc, it) \mid data$ 是数据，$isc \in ISC, it \in I\mathscr{T}\}$ 是库所的托肯集，$data$，isc 和 it 分别是托肯携带的数据、区间安全级和有效时间。p 的托肯集记作 $m(pi)$。$M: P \to 2^{TK_{MS}}$ 是 MLSPN 的库所标识，TK_{MS} 是托肯多重集集合，$2^{TK_{MS}}$ 是 TK_{MS} 的幂集合。$FTK = \{ftk_i : (tk_1, tk_2, \cdots, tk_{|{}^\bullet t|}) \mapsto tk \mid t \in T, tk_i \in m(p_i), p_i \in {}^\bullet t, 1 \leqslant i \leqslant |{}^\bullet t|, tk_i \in TK\}$ 是 T 上的输入、输出托肯变换函数集。$L: P \cup T \cup TK \to ISC$，$\Gamma: P \cup T \cup TK \to I\mathscr{T}$ 分别是库所、变迁和托肯的安全级和有效时间函数。并且在任意时间 τ，下列关系成立：

$$\forall\, p_i \in P, \forall\, tk_j \in m(p_i) : L(tk_j) \leqslant L(p_i) \wedge \Gamma(tk_j) \Subset ((p_i) \tag{5}$$

$$\forall\, t_i \in T, \forall\, p_j \in {}^\bullet t_i, \forall\, p_k \in t_i^\bullet : L(p_j) \leqslant L(t_i) \wedge L(t_i) \leqslant L(p_k) \tag{6}$$

$$\forall\, t_i \in T, \forall\, p_j \in {}^\bullet t_i, \forall\, p_k \in t_i^\bullet : \Gamma(p_j) \Cap \Gamma(t_i) \Cap \Gamma(p_k) \neq \phi \tag{7}$$

式(5)、(6)和(7)描述了库所、变迁和托肯的区间安全级(以下简称安全级)和有效性时间之间必须满足的关系。MLSPN 的变迁发生规则定义为：

定义 8 已知 MLSPN=(P,T,F,TK,M,FTK,L,Γ)，在时间 $\tau \in \mathscr{T}$，$\forall\, t_i \in T$，t_i 是安全活的，当且仅当 $\forall\, p_j \in {}^\bullet t_i, \exists\, tk_j \in m(p_j) : \tau \in (\Cap_{1 \leqslant j \leqslant |{}^\bullet t_i|} \Gamma(tk_j)) \Cap \Gamma(p_j) \Cap \Gamma(t_i) \wedge L(tk_j) \leqslant L(t_i)$。如果 t_i 是安全活的，那么 t_i 是可以安全发生的，t_i 发生后产生新的托肯 $tk_u = ftk_u(tk_1, tk_2, \cdots, tk_{|{}^\bullet t_i|})$，并且 $L(tk_u) \geqslant lub(L(t_i), L(tk_1), L(tk_2), \cdots, L(tk_{|{}^\bullet t_i|}))$，$\Gamma(tk_u) = [\tau, \tau_{uu}]$；产生新的标识为：对 $\forall\, p_j \in {}^\bullet t_i, \forall\, tk_j \in p_j, \forall\, p_u \in t_i^\bullet$。如果 $L(tk_u) \leqslant L(p_u)$，并且 $\Gamma(tk_u) \Subset \Gamma(p_u)$，那么 $m'(p_j) = m(p_j) -$

$\{tk_j\}$，并且 $m'(p_x)=m(p_x)+\{tk_x\}$。否则 $m'(p_j)=m(p_j)-\{tk_j\}$，并且 $m'(p_x)=m(p_x)$，其中＋，－为式(1)和(3)定义的多重集运算。

在多级安全环境下，MLSPN 的物理意义为：库所表示客体的"驻留"场所，库所的托肯表示驻留在该库所的客体信息；变迁表示安全事务执行主体，变迁上的托肯变换函数为事务执行函数(规则)；流关系 $f(p,t)$表示变迁 t 上的事务执行前主体需要从库所 p"读"客体，流关系 $f(t,p)$表示变迁 t 上的事务执行完毕之后主体需要向库所 p"写"客体；库所、变迁、托肯的区间安全级(以下简称安全级)和有效时间分别是客体驻留场所、事务执行主体、客体信息的安全级和有效时间约束。

式(5)描述了网的库所与驻留其中的托肯安全级和有效性时间之间必须满足的关系，其语义为：在任何时间驻留在网的每一个库所上的托肯安全级总是小于或等于其驻留的库所安全级，并且托肯有效时间包含于库所有效时间内时，库所上驻留托肯才是安全的。式(6)描述了网的变迁与其输入输出库所安全级之间必须满足的关系，其语义为：每一个变迁的安全级总是大于或等于其输入库所(如果存在)安全级，而小于或等于其输出库所安全级时，网结构才是安全的。式(7)则描述了网的变迁与其输入输出库所有效时间之间必须满足的关系，其语义为：每一个变迁的有效时间与其输入输出库所有效时间之间必须有重叠时，网结构才是有效的。事实上，定义 8 描述的变迁发生规则实现了定义 6 描述的多级安全规则，并支持有效性时间约束。因此，MLSPN 可以用于越来越多的与时间相关的多级安全系统建模。

3 MLSPN 的多级安全机制定义与分析

MLSPN 的多级安全机制是指其托肯存贮、接收、处理和发送均支持多级安全策略。我们把 MLSPN 的托肯存贮、接收、处理和发送所使用的"库所-变迁"构成的交替序列称为托肯流通道，在托肯流通道上移动的托肯称为托肯流。如果 MLSPN 的托肯流通道和托肯流都是安全的，则称 MLSPN 是安全的。以下从托肯流通道和托肯流两方面对 MLSPN 的多级安全机制进行分析。为简化描述，首先定义下列 3 个谓词。在任意时间 $\tau\in\mathscr{T}$，$t\in T$，$p\in P$，$tk\in TK$：

$Sreceive(tk,t,p)=\text{TRUE}\Leftrightarrow p\in {}^\bullet t\wedge tk\in m(p)\wedge L(tk)\leqslant L(p)\wedge L(p)\leqslant L(t)\wedge\tau\in\Gamma(tk)\cap\Gamma(p)\cap\Gamma(t)$

语义：在时间 τ，变迁 t 的输入库所 p 上的托肯安全级不大于 p 的安全级，p 的安全级不大于 t 的安全级，并且 p，tk，t 均处于其有效时间内时，则 t 从 p 上接收托肯才是安全的。

$Sprocess(tk,t)=\text{TRUE}\Leftrightarrow$

$\forall p_i\in {}^\bullet t\exists\ tk\in m(p_i): tk=ftk_i(tk_1,tk_2,\cdots,tk_{|{}^\bullet t|})\wedge L(tk)\geqslant lub(L(t),L(tk_1),\cdots,L(tk_{|{}^\bullet t|}))\wedge\tau\in\Gamma(t)$

语义：在时间 τ，变迁 t 对其安全接收的托肯按预先定义的变换函数 ftk_i 进行处理，产生新的托肯 tk，并且新托肯的安全级不低于输入托肯安全级和 t 的安全级的最小上界，而且在 t 的有效时间内完成托肯变换，则 t 的托肯变换是安全的。

$Ssend(tk,p,t)=\text{TRUE}\Leftrightarrow p\in t^\bullet\wedge L(t)\leqslant L(tk)\wedge L(tk)\leqslant L(p)\wedge\tau\in\Gamma(t)\cap\Gamma(p)\cap\Gamma(tk)\wedge\Gamma(tk)\in\Gamma(p)$

语义：在时间 τ，变迁 t 把安全处理所产生的新托肯向安全级不低于该托肯安全级的输出库所 p 发送，t，p，tk 均处于其有效时间内，并且 tk 的有效时间是 p 的有效时间的子集，则 t 的托肯发送是安全的。

设 M_i 和 M_j 是 MLSPN 的两个标识，如果 M_i 经过一个变迁序列 $s=t_1t_2\cdots t_\kappa$ 到达 M_j，则称 M_i 到 M_j 是可达的，记作 $M_i[s>M_j$；如果存在 $t\in T$，使得 t 在 M_i 发生后产生新的标识 M_j，则称 M_j 从 M_i 是直接可达的，记作 $M_i[t>M_j$。假定 MLSPN 满足 PN 定义下的可达性，则其标识安全和变迁发生(序列)安全概念定义如下：

定义 9 已知 MLSPN＝(P，T，F，TK，M，FTK，L，Γ)，其初始标识为 M_0，可达标识集 $RS(MLSPN)=M\mid M_0[s>M, s=t_1t_2\cdots t_\kappa, |s|\geqslant 0]$，发生序列集 $FS(MLSPN)=\{s\mid M_0[s>M, M\in RS(MLSPN)]$。

定义 10 已知 MLSPN＝(P，T，F，TK，M，FTK，L，Γ)，对∀ $p\in P$，p 的标识是安全的，当且仅当∀ $tk\in m(p): L(tk)\leqslant L(p)\wedge\Gamma(tk)\in\Gamma(p)$为真。

定义 11 已知 MLSPN＝(P，T，F，TK，M，FTK，L，Γ)，$M_i, M_j\in RS(MLSPN)$，$t\in T$，并且 $M_i[t>M_j$，t 在 M_i 发生后产生的托肯 $tk=ftk_i(tk_1,tk_2,\cdots,tk_{|{}^\bullet t|})$，其中 $tk_i\in m(p_i)$，${}^\bullet t=\bigcup_{1\leqslant i\leqslant n}p_i, n=|{}^\bullet t|$。t 发生是安全的，当且仅当∀ $p_i\in {}^\bullet t$，∀ $p_j\in t^\bullet$，∃ $tk_i\in m(p_i)$：$Sreceive(tk_i,t,p_i)\wedge Sprocess(tk,t)\wedge Ssend(tk,p_j,t)$为真。

定义 12 已知 MLSPN＝(P，T，F，TK，M，FTK，ftp)，对∀ $t\in T$，t 是安全的，当且仅当∃ $M\in RS(MLSPN)$，t 在 M 下是安全活的，并且 t 发生是安全的。如果 $M_i[s>M_j$，$s=t_1t_2\cdots t_\kappa$，$\kappa\geqslant 1$，s 是安全的，当且仅当∃ $t\in s$，t 是安全的。

在上述 MLSPN 标识安全、变迁发生(序列)安全概念基础上，我们给出 MLSPN 的托肯流通道安全概念。

定义 13 已知 MLSPN＝(P，T，F，TK，M，FTK，L，Γ)，其托肯流通道是安全的，当且仅当 M_0 是安全的，并且对∀ $s\in FS(MLSPN)$，s 是安全的。

定义 13 没有直接把 MLSPN 的托肯流通道安全性与其可达标识安全性相关联。而验证变迁发生序列安全是比较困难的，但验证标识安全相对比较简单。为了把 MLSPN 的托肯流通道安全性与其可达标识安全性直接关联，以简化托肯流通道安全性验证，我们给出如下定理。

定理 1 已知 MLSPN＝(P，T，F，TK，M，FTK，L，Γ)，如果 MLSPN 的托肯流通道是安全的，那么对∀ $M\in RS(MLSPN)$，M 是安全的。

证明：已知 M_0 是 MLSPN 的初始标识，MLSPN 的托肯流通道是安全的。由定义 13 得 M_0 是安全的，并且对∀ $s\in FS(MLSPN)$，s 是安全的。如果 $RS(MLSPN)=\{M_0\}$，则结论显然成立。现假设 $|RS(MLSPN)|\geqslant 2$，$M_0, M_i\in RS(MLSPN)$，$t\in T$，$M_0[t>M_i$，并且 M_i 是不安全的，则由定义 12 得 t 是不安全的。这个结论蕴涵着∃ $s\in FS(MLSPN)$，$t\in s$，并且 s 是不安全的，与初始假设 MLSPN 是安全的相矛盾。因此，对∀ $M\in RS(MLSPN)$，M 是安全的。

我们把库所和变迁的交替序列称为 MLSPN 的路径 $pa=p_1t_1p_2\cdots t_\kappa p_{\kappa+1}$。对∀ $i\in[1,\kappa]$，$p_i\in {}^\bullet t_i$，并且 $p_{i+1}\in t_i^\bullet$。与 pa 对应的变迁序列 $s(pa)=t_1t_2\cdots t_\kappa$，$\kappa\geqslant 1$。

定义 14 已知 MLSPN＝(P，T，F，TK，M，FTK，L，Γ)，$t_i, t_j\in T$，t_i 和 t_j 之间存在一条托肯流通道，当且仅当存在路径 $pa_{ij}=p_1t_1\cdots p_\kappa t_\kappa p_{\kappa+1}$，使得 $t_i=t_1$，$t_\kappa=t_j$，$\kappa\geqslant 1$，并且∃ $M_i, M_j\in RS(MLSPN)$：$M_i[s>M_j\wedge s(pa_{ij})=t_1t_2\cdots t_\kappa$。

定义 15 已知 MLSPN＝(P，T，F，TK，M，FTK，L，Γ)，$t_i, t_j\in T$，t_i 和 t_j 之间的路径 $pa_{ij}=p_1t_1\cdots p_\kappa t_\kappa p_{\kappa+1}$，$t_i=t_1$，$t_\kappa=t_j$，$t_i$ 与 t_j 之间存在一条托肯流 $info_{ij}$。$info_{ij}$是安全的，当且仅

当存在标识 $M_i, M_j \in RS(MLSPN)$，使得 $M_i[s>M_j, s(pa_{ij})=t_1t_2\cdots t_\kappa, t_r=t_1, t_j=t_\kappa, \kappa\geqslant 1$，并且对$\forall\ t_r \in s, 1\leqslant r\leqslant \kappa, t_r$ 在标识 M_r 下是安全活的，$M_r[t_r>M_{r+1}, t_r$ 发生是安全的。t_i 和 t_j 之间的托肯流是安全的，当且仅当 t_i 与 t_j 之间的每一条路径上的托肯流是安全的。

如果 2 个变迁之间存在一条路径，那么只是为产生托肯流提供了可能性，而托肯流的真正产生还需要存在与这条路径对应的发生序列。为了阐明托肯流安全通道与托肯流安全性之间的关系，我们先给出以下引理。

引理 1 已知 $MLSPN=(P,T,F,TK,M,FTK,L,\Gamma)$，对$\forall\ s\in FS(MLSPN), s$ 是安全的。设 $M_i, M_j \in RS(MLSPN)$，如果 $M_i[s_r>M_j$，那么 s_r 也是安全的。

证明：用反证法。假设 s_r 是不安全的，由定义 12 得，必然存在一个 $t\in s_r$，并且 t 是不安全的。因为 $M_i\in RS(MLSPN)$，所以存在安全变迁序列 $s_i\in FS(MLSPN)$，使得 $M_0[s_i>M_i$。又因为 $M_j\in RS(MLSPN)$，并且 $M_i[s_r>M_j$，则必然存在变迁序列 $s_j\in FS(MLSPN)$，使得 $s_j=s_is_r$，并且 $M_0[s_j>M_j$。由于 $s_j\in FS(MLSPN)$，所以 s_j 是一个安全变迁序列，即对$\forall\ t\in s_j, t$ 是安全的。因此对$\forall\ t\in s_r, t$ 也是安全的，于是由定义 12 得 s_r 是安全的。这个结论与假设相矛盾，所以变迁序列 s_r 是安全的。

使用引理 1，我们可以证明下列 MLSPN 的托肯流通道安全与托肯流安全之间的关系定理。

定理 2 已知 $MLSPN=(P,T,F,TK,M,FTK,L,\Gamma)$，$M_0$ 是其初始标识，对$\forall\ t_i, t_j\in T, t_i$ 和 t_j 之间存在一条托肯流。如果 MLSPN 的托肯流通道是安全的，那么从 t_i 到 t_j 之间的托肯流是安全的。

证明：如果 MLSPN 的托肯流通道是安全的，由定义 13 得 M_0 是安全的，并且对$\forall\ s\in FS(MLSPN), s$ 是安全的。设 pa_{ij} 是从 t_i 到 t_j 之间的任意一条路径，s 是对应于 pa_{ij} 的变迁序列，$\forall\ M_i, M_j\in RS(MLSPN)$，如果 $M_i[s>M_j$，则由引理 1 得 s 是安全的，由定义 12 得 s 包含的每一个变迁 t 是安全的。因此，t 的发生是安全的。由定义 11 得从 t_i 到 t_j 之间沿路径 pa_{ij} 的托肯流必然是安全的。由于 pa_{ij} 是从 t_i 到 t_j 之间的任意路径，因此从 t_i 到 t_j 之间的每一条路径上的托肯流是安全的，于是从 t_i 到 t_j 之间的托肯流是安全的。

定义 16 已知 $MLSPN=(P,T,F,TK,M,FTK,L,\Gamma)$，对$\forall\ t_i, t_j\in T$，如果 t_i 和 t_j 之间的托肯流是安全的，那么 MLSPN 的托肯流是安全的。

在多级安全系统中，信息流安全隐通道（如特洛伊木马等）是指合法的信息访问主体把自己合法拥有的信息发送给不应该得到这些信息的低安全级主体而系统安全机制毫无感知的一种系统安全缺陷[1,2]。信息隐通道是绝大多数多级安全系统中普遍存在而且难于解决的问题，它对系统构成了不可预料的安全隐患，因此有效防止信息隐通道是每一个多级安全系统的主要目标之一[13]。在 PN 模型中，信息流隐通道即指托肯流隐通道，但 MLSPN 中不存在托肯流隐通道，这一点由以下定理 3 给予保证。

定理 3 MLSPN 中不存在托肯流隐通道。

在 MLSPN 中，托肯流隐通道一方面是指变迁把从它的输入库所接收的托肯经过托肯变换函数处理之后，产生的新托肯安全级低于原接收托肯安全级，使得该变迁能够把新托肯合法地发送给安全级低于原托肯的输出库所，造成托肯降级流动，从而违反多级安全原则。由定义 8 的变迁发生规则决定了任意变迁接收的所有托肯经过变换后产生的所有新托肯的安全级不小于原接收的托肯安全级与变迁安全级的最小上界，因此不存在高安全级托肯经过变换处理后变为低安全级托肯的可能性。另一方面是指不存在托肯流通道的 2 个变迁之间非法产生托肯流，从而造成托肯非法流动。定义 8 的变迁发生规则保证了任意 2 个变迁之间如果有托肯流发生，则必然在这 2 个变迁之间存在托肯流通道。换句话说，相互之间不存在托肯流通道的 2 个变迁之间不可能产生托肯流，即 MLSPN 的安全变迁规则使托肯流只能沿托肯流通道从低安全级库所向高安全级库所单向流动。因此，即使某个主体想把自己合法拥有的托肯发送给安全级比托肯安全级低的主体是无法实现的，所以 MLSPN 中不存在托肯流隐通道。

结论和进一步的工作 我们提出的 MLSPN 通过对经典 PN 的库所、变迁和托肯分别赋以区间安全级和有效性区间时间约束，实现了网的标识安全和变迁发生（序列）安全。区间安全级的使用放松了多级安全 BLP 模型的确定值安全级对访问控制十分严格的约束，从而增强了模型对商用系统建模的适应性。把区间时间有效性作为库所，变迁和托肯的基本属性使得 MLSPN 对动态时间约束建模时不必考虑复杂的不确定性事件发生的确切时间或随机时间延迟分布，从而增强了模型对时间约束变化的适应能力。MLSPN 的变迁发生规则使托肯沿托肯流安全通道从低安全级库所向高安全级库所单向流动，从而实现了 BLP 多级安全策略，并有效消除了托肯流隐通道，模型简单，容易使用。

MLSPN 的变迁之间复杂的数据依赖和周期时间约束表达规则是很有意义的研究课题，可以通过在变迁上实施约束规则实现，我们将做进一步研究。其次，MLSPN 的安全性建立在 MLSPN 的可达性基础上，因此我们将使用 PN 已有的研究结果对 MLSPN 的可达性等网特性进行深入分析。一个基于 MLSPN 的多级安全工作流系统原型正在开发之中。实验结果表明，MLSPN 为多级安全环境下的系统建模提供了一种新的途径。

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 Bell D, LaPadula L. The Bell-LaPadula model [J]. Journal of computer security, 1996, 4(2,3): 239～263

3 袁崇义. Petri 网原理. 电子工业出版社, 1998

4 Peterson J L. Petri net theory and modelling of systems [M]. Prentice Hall, 1981

5 Reisig W. Petri nets—An introduction [M]. Springer, 1985

6 Murata T. Petri: properties, analysis and application [C]. Proceedings of the IEEE, 77(4): 541～580

7 Atluri V, Huang Wei-Kuang. Enforcing manadatory and discretionary security in workflow management system [J]. Journal of computer security, 1997, 5: 303～339

8 Kang H, Froscher N. A stragy for a MLS workflow management system [C]. In: Proc. of the 18th IFIP working conf. on database security, Seatle, WA, 1999

9 Knorr K. Multilevel security and information flow in Petri net workflows [J]. Journal of computer security, 2001, 9(2,3): 130～140

10 MacEwen H, Poon V W W, Glasgow J. A model for multilevel security based operator nets [C]. In: Proc. of the1987 IEEE symposium on security and privacy, 1987. 150～160

11 Glasgow J, MacEwen H. The development and proof of a formal specification for a mulilevel secure system [J]. ACM transaction on computer security, 1987, 5(2): 151～184

12 刘启原，刘怡. 数据库与信息系统的安全. 科学出版社, 2000