基于矩阵半张量积的信息物理融合系统状态不透明性分析与控制

张志鹏 许 倩 夏承遗*

(天津理工大学智能计算机及软件新技术天津市重点实验室 天津 300384)

(天津理工大学学习型智能系统教育部工程研究中心 天津 300384)

摘 要：状态不透明性作为一种重要的机密属性，能够表征入侵者窃取系统隐私信息的能力。针对带有不可观测事件的信息物理融合系统(CPSs)，该文提出一种基于矩阵半张量积(STP)的代数状态空间方法，并且分析与验证CPSs的状态不透明性。首先利用矩阵STP理论对CPSs的状态演化进行建模，得到系统的动态代数表达式，然后利用STP运算的特性，给出验证系统当前状态不透明性的充分必要代数条件。最后，通过数值仿真算例验证了方法的有效性。该文提出的基于矩阵STP方法为CPSs相关隐私分析与安全控制研究提供了一个新的思路和框架。

关键词：信息物理系统；有限值逻辑系统；矩阵半张量积；当前状态不透明性；有限自动机

中图分类号：TP1 **文献标识码**：A **文章编号**：1009-5896(2021)12-3434-08

DOI: 10.11999/JEIT210492

Semi-tensor Product of Matrices-based Approach to the Opacity Analysis of Cyber Physical Systems

ZHANG Zhipeng XU Qian XIA Chengyi

(*Key Laboratory of Intelligence Computing and Novel Software Technology, Tianjin University of Technology, Tianjin* 300384, *China*)

(*China Engineering Research Center of Learning-Based Intelligent System, Ministry of Education, Tianjin University of Technology, Tianjin* 300384, *China*)

Abstract: As an important confidential attribute, state opacity can characterize the ability of intruders to steal system privacy information. For the Cyber Physical Systems (CPSs) with unobservable events, an algebraic state space method based on the Semi-Tensor Product (STP) of matrices is proposed to analyze and verify the state opacity of CPSs. First, the state evolution of CPSs is modeled by STP of matrices theory, the system dynamics can be obtained as an algebraic expression, and then the characteristics of STP operation are used to give the necessary and sufficient algebraic condition to verify the current state opacity. Finally, the validity of the method is verified by a numerical simulation. The STP of matrices-based method proposed in this paper provides a new idea and framework for privacy analysis and security control of CPSs.

Key words: Cyber Physical Systems(CPSs); Finite value logical systems; Semi-Tensor Product(STP) of matrices; Current state opacity; Finite automata

1 引言

随着信息通信技术的飞速发展和数据处理能力的不断提高，物理系统通过信息通信网络实现互联的趋势日益显著，由此产生了信息物理融合系统(Cyber Physical Systems, CPSs)。同时，为了提高CPSs的智能化和信息化，系统将部分或全部计算和决策上传到云服务器中。此时，物理系统的操作环境变得更加开放，为入侵者窃取隐私和机密信息提供了更多的漏洞。因此，隐私分析与安全控制是CPSs领域一个非常重要的研究方向[1,2]。

不透明性作为一种重要的隐私信息流概念，要求入侵者无法准确地推断出系统的隐私和秘密信息[3,4]。如果一个系统被判定为不透明的，则系统的隐私信息能够得到有效保证。不透明性的分析和控制问题主要集中在两个方面：一个是验证，即判定给定系统是否不透明的；另一个是综合，即如何通过控制策略保证系统的不透明性。具体地，文献[5]首次引入当前状态不透明性的概念，并构建了

收稿日期：2021-06-01；改回日期：2021-10-29；网络出版：2021-11-14
*通信作者： 夏承遗 xialooking@163.com
基金项目：国家自然科学基金(62173247)
Foundation Item: The National Natural Science Foundation of China (62173247)

状态观测器对基于状态的不透明性进行验证；文献[6]通过构造K步时延状态估计器，提出K步不透明性的验证方法；同时，文献[7]分析了无穷状态估计器的性质，证明了无穷步不透明性的验证问题是一个多项式空间难 (Polynomial SPACE hard , PSPACE-hard)问题。除此之外，针对上述状态不透明性的验证问题，学者提出了多种技术方法和算法，比如双向观测器[8]、互模拟法[9]和系统状态变换法[10]。以上工作主要利用形式化方法展开研究，得到了很多非常深刻且有意义的结论。但是，随着传统代数状态空间理论的发展，基于矩阵半张量积(Semi-Tensor Product, STP)的代数方法为不透明性分析、验证与控制提供了非常便捷的工具。STP理论最早是由我国控制科学专家程代展教授及其团队提出的[11–13]，作为常规矩阵乘积的推广，已得到了广泛的应用，包括布尔网络[14–19]、离散事件系统[20–23]、博弈论[24]等多个领域。文献[25]首次将STP应用于有限自动机系统，提出了有限自动机的代数建模以及状态可达性等基本问题；文献[26]基于STP系统地研究了有限自动机的状态反馈镇定和输出反馈镇定问题，并提出相应的镇定充要条件和镇定设计算法；文献[27]利用布尔STP研究了有限状态机在有界通信延迟下的网络化不透明性，给出了在有界通信延迟下的当前状态估计器动力学方程。另外，STP在离散事件系统中其他研究问题可参考相关文献[28–30]。

目前，基于STP理论的CPSs的信息安全与隐私防护研究仍处于起步阶段。本文针对有限自动机建模的CPSs，提出一种新的代数方法来验证系统的状态不透明性。首先，在布尔STP框架下，对CPSs进行代数建模，给出系统动态的代数表达式；其次，假定外部入侵者了解系统结构和状态转移等完全信息，构建了CPSs的当前状态估计器，并提出一个有效的矩阵计算方法；最后，通过引入矩阵的行、列逻辑运算，将系统当前转移状态的估计进行简化，给出判定系统当前状态不透明性的充分必要条件。本文的主要创新点可凝练为以下3点：

(1) 借助矩阵的布尔STP，通过将状态/输入表示为列向量，将有限状态入侵估计器的转移函数表示为状态-转移估计矩阵，进而得到入侵估计器的可观测动态演化代数方程。

(2) 结合布尔STP计算特性，入侵状态-转移估计矩阵将抽象的当前状态不透明性验证问题转化成较为具体的结构矩阵计算和对应元素判断问题。

(3) 利用系统演化代数方程和入侵状态-转移估计矩阵，给出验证带有不可观事件CPSs当前状态不透明性的代数充分必要条件。

本文其余部分组织如下，第2节介绍STP和CPSs的相关预备知识；第3节在STP框架下，建立基于有限自动机的CPSs可观测动力学代数表达式，并提出基于代数状态空间的不透明性验证条件；同时，为便于阅读，针对一些关键结论，通过数值算例进行详细说明。最后，第4节对该文进行总结，并给出后续研究展望。

2　预备知识

本节主要展示了一些常用符号如表1所示，引入了布尔矩阵半张量积的定义、常用性质及具体算例。同时，介绍了本文用到的信息物理系统模型，即带有不可观事件的不确定有限自动机。

2.1　半张量积

近年来，程代展教授及其团队提出的基于STP的代数状态空间方法逐渐发展成为逻辑系统分析和设计有力的工具之一。该方法扩大了矩阵的适用范围，同时，还保持了矩阵普通乘法的所有重要性质。鉴于STP理论的优点，将该方法引入到CPSs的不透明性分析问题中。

首先，给定矩阵$\boldsymbol{A}=(a_{ij})_{a\times b}\in\mathbb{R}^{a\times b}$和$\boldsymbol{B}=b_{ij}{}_{c\times d}\in\mathbb{R}^{c\times d}$，它们的克罗内克积是维度为$ac\times bd$的分块矩阵

$$\boldsymbol{A}\otimes\boldsymbol{B}=\begin{bmatrix} a_{11}\boldsymbol{B} & a_{12}\boldsymbol{B} & \cdots & a_{1b}\boldsymbol{B} \\ a_{21}\boldsymbol{B} & a_{22}\boldsymbol{B} & \cdots & a_{2b}\boldsymbol{B} \\ \vdots & & \ddots & \vdots \\ a_{a1}\boldsymbol{B} & a_{a2}\boldsymbol{B} & \cdots & a_{ab}\boldsymbol{B} \end{bmatrix} \tag{1}$$

定义1[11]　矩阵$\boldsymbol{P}\in\mathbb{R}^{a\times b}$和$\boldsymbol{Q}\in\mathbb{R}^{c\times d}$的STP定义为

表 1　常用符号

概念	定义
$\mathbb{N}^+$	正整数的集合
$\mathbb{R}^n$	维数为n的所有实向量的集合
$\lvert X\rvert=n$	集合X的基数
$\mathbb{R}^{n\times m}$	维数为$n\times m$的实矩阵集
$\mathbb{B}^{n\times m}$	维数为$n\times m$的布尔矩阵集
$\boldsymbol{R}(i,j)$	矩阵$\boldsymbol{R}$的第i行第j列元素
$\mathrm{Col}_i(\boldsymbol{R})$, $\mathrm{Row}_j(\boldsymbol{R})$	分别为矩阵$\boldsymbol{R}$的第i列，第j行
$\mathrm{Col}(\boldsymbol{R})$, $\mathrm{Row}(\boldsymbol{R})$	矩阵$\boldsymbol{R}$的所有列和所有行的集合
$\boldsymbol{I}_n$	维数为n的单位矩阵
δ_n^i	单位矩阵$\boldsymbol{I}_n$的第i列
Δ_n	$\{\delta_n^1,\delta_n^2,\cdots,\delta_n^n\}$
2^X	集合X的幂集合
$\sum_{\mathbb{B}}^{i\in R}\boldsymbol{M}_i$	所有$i\in\boldsymbol{R}$矩阵$\boldsymbol{M}_i$的布尔和

$$\boldsymbol{P}\ltimes\boldsymbol{Q}=\left(\boldsymbol{P}\otimes\boldsymbol{I}_{n/b}\right)\left(\boldsymbol{Q}\otimes\boldsymbol{I}_{n/c}\right)\tag{2}$$

其中，n为b和c的最小公倍数。

例1 考虑两个矩阵

$$\boldsymbol{A}=\begin{bmatrix}1&2\\3&4\end{bmatrix},\ \boldsymbol{B}=\begin{bmatrix}1&1&1\\2&2&2\\3&3&3\end{bmatrix}\tag{3}$$

那么，矩阵$\boldsymbol{A}$和$\boldsymbol{B}$的STP为

$$\begin{aligned}\boldsymbol{A}\ltimes\boldsymbol{B}&=\left(\boldsymbol{A}\otimes\boldsymbol{I}_3\right)\left(\boldsymbol{B}\otimes\boldsymbol{I}_2\right)=\begin{bmatrix}1&0&0&2&0&0\\0&1&0&0&2&0\\0&0&1&0&0&2\\3&0&0&4&0&0\\0&3&0&0&4&0\\0&0&3&0&0&4\end{bmatrix}\\&\cdot\begin{bmatrix}1&0&1&0&1&0\\0&1&0&1&0&1\\2&0&2&0&2&0\\0&2&0&2&0&2\\3&0&3&0&3&0\\0&3&0&3&0&3\end{bmatrix}\\&=\begin{bmatrix}1&4&1&4&1&4\\6&1&6&1&6&1\\2&6&2&6&2&6\\3&8&3&8&3&8\\12&3&12&3&12&3\\6&12&6&12&6&12\end{bmatrix}\end{aligned}\tag{4}$$

在有限逻辑系统中，许多分析和控制问题更关注经过STP运算后矩阵中的元素是“0”还是“1”。以有限自动机的可控性为例，只需要检测初始状态到目标状态是否可达的，不需要知道可达路径的条数。因此，为便于计算和矩阵表示，在矩阵STP中引入布尔运算，得到了布尔STP的定义。

定义2[27] 矩阵$\boldsymbol{P}\in\mathbb{B}^{\alpha+6}$和$\boldsymbol{Q}\in\mathbb{B}^{c\times d}$的布尔STP定义为

$$\boldsymbol{P}\ltimes_{\mathbb{B}}\boldsymbol{Q}=\left(\boldsymbol{P}\otimes_{\mathbb{B}}\boldsymbol{I}_{n/b}\right)\times_{\mathbb{B}}\left(\boldsymbol{Q}\otimes_{\mathbb{B}}\boldsymbol{I}_{n/c}\right)\tag{5}$$

其中，$\otimes_{\mathbb{B}}$是布尔克罗内克积。

备注1 类似于常规的矩阵乘法，布尔STP运算也可以通过迭代的方式扩展到幂运算。记$\ltimes_{\mathbb{B}}\alpha$为布尔STP幂运算的符号。对于任意的$\alpha\in\mathbb{N}^+$，满足

$$\boldsymbol{P}^{\ltimes_{\mathbb{B}}\alpha}=\underbrace{\boldsymbol{P}\ltimes_{\mathbb{B}}\boldsymbol{P}\ltimes_{\mathbb{B}}\cdots\ltimes_{\mathbb{B}}\boldsymbol{P}}_{\alpha}\tag{6}$$

引理1[12] 如果按以下方式构造，矩阵$\boldsymbol{W}_{[b,a]}\in\mathbb{B}^{ab\times ab}$称为交换矩阵，用序号$(11,12,\cdots,1a,\cdots,b1,\cdots,b2,\cdots,ab)$标记矩阵的列，并用序号$(11,21,\cdots,b1,\cdots,1a,\cdots,2a,\cdots,ab)$标记矩阵的行，其$((I,J),(i,j))$位置的元素被赋值为

$$\left(w_{ij}\right)_{((I,J),(i,j))}=\delta_{i,j}^{I,J}=\begin{cases}1,\ I=i\text{和}J=j\\0,\ \text{其他}\end{cases}\tag{7}$$

当$m=n$时，$\boldsymbol{W}_{[a,b]}$可简写为$\boldsymbol{W}_{[a]}$或$\boldsymbol{W}_{[b]}$。

引理2[12] (1) 设$\boldsymbol{X}\in\Delta_m$和$\boldsymbol{Y}\in\Delta_n$是两个列向量，那么$\boldsymbol{W}_{[m,n]}\ltimes\boldsymbol{X}\ltimes\boldsymbol{Y}=\boldsymbol{Y}\ltimes\boldsymbol{X}$和$\boldsymbol{W}_{[n,m]}\ltimes\boldsymbol{Y}\ltimes\boldsymbol{X}=\boldsymbol{X}\ltimes\boldsymbol{Y}$。

(2) 设$\boldsymbol{\sigma}\in\mathbb{R}^n$，对于任意的矩阵$\boldsymbol{A}$满足$\boldsymbol{\sigma}\ltimes\boldsymbol{A}=\left(\boldsymbol{I}_n\otimes\boldsymbol{A}\right)\ltimes\sigma$。

引理3[19] 令$\Delta_{m^\tau}^{\alpha}=\ltimes_{i=1}^{\tau}\delta_m^{j_i}$，可得到$\delta_m^{j_i}=\boldsymbol{A}_i^{\tau}\ltimes\delta_{m^\tau}^{\alpha}\ (i=1,2,\cdots,\tau)$，其中$\boldsymbol{T}_\alpha=[\underbrace{\boldsymbol{I}_m,\cdots,\boldsymbol{I}_m}_{m}]$且满足方程式

$$\left.\begin{aligned}\boldsymbol{A}_1^{\tau}&=\left(\boldsymbol{T}_\alpha\right)^{\tau-1}\ltimes\boldsymbol{W}_{[m,m^{\tau-1}]}\\&\vdots\\\boldsymbol{A}_i^{\tau}&=\left(\boldsymbol{T}_\alpha\right)^{\tau-1}\ltimes\boldsymbol{W}_{[m,m^{\tau-i}]}\\&\vdots\\\boldsymbol{A}_1^{\tau}&=\left(\boldsymbol{T}_\alpha\right)^{\tau-1}\end{aligned}\right\}\tag{8}$$

2.2 基于有限自动机的CPSs与状态不透明性

在现实中，很多CPSs的状态的变迁是由事件驱动的，而且往往会出现同一个事件产生多个不确定的状态转移。针对这些情况，本文引入有限自动机模型对上述现象进行刻画。本节介绍了关于有限状态自动机的基础概念和相关记号。

考虑一个不确定有限自动机(Non-Deterministic Finite mAchine, NDFA)$A=(X,E,E_o,\sigma,x_0)$，其中X表示系统从初始状态$x_0\in X$出发的有限可达状态集，E为有限事件集，E_o为系统可观测事件集，且$E_{uo}:=E/E_o$为系统不可观测事件集。$\sigma:X\times E\to 2^X$代表状态在事件驱动下的状态转移函数，比如，$x_2\in\sigma(x_1,e)$意味着状态x_1在事件e驱动下发生跃迁到达状态x_2。E^*为事件集E上所有的有限字符串集。给定输入事件串$e=e_1e_2\cdots e_s\in E^*$，则转移函数可以推广到$\sigma(x_1,e)=\sigma(\sigma(\cdots\sigma(\sigma(x_1,e_1),e_2)\cdots),e_s)$。换句话说，NDFA在状态$x_1$下读取输入$e_1$并移动到$x'\in\sigma(x,e)$，然后读取输入$e_2$并移动到$x''\in\sigma(x',e)$，以此类推。$P:E\to E_o$表示事件的映射，可以将事件串映射为可观测串，即如果事件$e_i\in E_o$，则$P(e_i)=e_i$，否则$P(e_i)=\varepsilon$。同样，映射P也可以扩展为$E^*\to E_o^*$，即将事件串映射为可观测事件串。从状态x_1出发生成的所有事件串被定义为$\mathcal{L}(A,x_1)=\left\{s\in E^*|\sigma(x_1,s)\neq\varnothing\right\}$。为了简单起见，从初始状态出发生成的事件串集合可简记为$\mathcal{L}(A)$。

基于状态的不透明性描述了系统隐私和秘密状态转换的行为信息流，是信息安全理论和技术的一个重要概念。对于给定的秘密状态集$X_{\text{se}}\subseteq X$和系统生成的任意事件串$\mathcal{L}(A)$，如果外部的恶意入侵者不能确定地推断出系统当前所处状态是否是秘密

状态$x \in X_{\rm se}$，则该系统被认为是状态不透明的。假设入侵者具有以下能力：

(1) 入侵者完全了解系统的结构和事件转换。

(2) 系统A生成的语言是非死锁的，即A中的每个状态都存在一个转移事件。

3 基于STP的当前状态不透明性的分析与验证

3.1 系统入侵下的当前状态估计

给定系统$A=(X,E,E_o,\sigma,x_0)$，其中设定$X=\{x_1,x_2,\cdots,x_n\}$,$E_o=\{e_1,e_2,\cdots,e_{mo}\}$, $E=\{e_1,e_2,\cdots,e_m\}$。在矩阵STP框架下，分别用δ_n^i,δ_m^j等价地表示x_i $(i\in\{1,2,\cdots,n\})$和e_j $(j\in\{1,2,\cdots,m\})$，并称δ_n^i, δ_m^j为x_i和e_j的向量形式。此时，状态集X可表示为$X:=\Delta_n=\{\delta_n^i|i\in\{1,2,\cdots,n\}\}$，同样地，输入事件集可表示为$E:=\Delta_m=\{\delta_m^j|j\in\{1,2,\cdots,m\}\}$。为便于不透明性分析，对系统状态进行适当排列组合，使得非秘密状态集的向量表达式可表示为$X_{\rm nse}:=\Delta_n^{\rm nse}=\{\delta_n^{\rm nse}|i_{\rm nse}\in\{1,2,\cdots,n-|X_{\rm nse}|\}\}$，秘密状态集的向量表达式可表示为$X_{\rm se}:=\Delta_n^{\rm se}=\{\delta_n^{\rm se}|i_{\rm se}\in\{n-|X_{\rm se}|+1,n-|X_{\rm se}|+2,\cdots,n\}\}$。由于不可观测事件集的存在会使得状态转移产生不确定性，为刻画该现象，需要分别构造外部入侵观测条件下的初始状态向量表达式和状态转移结构矩阵。首先，对于任意状态x_i，定义不可观可达状态集为

$$\begin{aligned}{\rm UR}(x_i):=x_i\cup\{x_i'\in X|x_i'\in\sigma(x_i,e_j),\\ \exists j\in\{{\rm mo}+1,{\rm mo}+2,\cdots,m\}\}\end{aligned}\tag{9}$$

进一步，给出入侵观测条件下的初始状态向量表达式为$x(1)$，且满足

$${\rm Row}_i(x(1))=\begin{cases}1,\ x_i\in{\rm UR}(x_0)\\0,\ 其他\end{cases}\tag{10}$$

同样地，利用事件和状态的向量表达式，状态转移函数$x_i\in\sigma(x_j,e_k)$可以等价地表示为$\delta_n^i\in\sigma\left(\delta_n^j,\delta_m^k\right)$。给定可观测事件$e_j$ $(j\in\{1,2,\cdots,{\rm mo}\})$，可确定唯一的状态转移结构子矩阵，记为$S_j\in\mathbb{B}^{n\times n}$，并定义为

$$S_j(i'',i)=\begin{cases}1,\ x_{i''}\in{\rm UR}(x_{i'}),x_{i'}\in\sigma(x_i,e_j)\\0,\ 其他\end{cases}\tag{11}$$

然后，外部入侵者可观测条件下的状态转移结构矩阵可表示为$\boldsymbol{S}=[\boldsymbol{S}_1\ \boldsymbol{S}_2\cdots\boldsymbol{S}_m]\in\mathbb{B}^{n\times nm}$。明显地，一旦状态转移函数$x_i\in\sigma(x_j,e_k)$给定，状态转移结构矩阵$\boldsymbol{S}$可由式(11)唯一确定。

最后，在上述转移结构矩阵$\boldsymbol{S}$和布尔STP框架下，对于入侵条件下系统的动力学可以转换成离散时间双线性表达式，得到如下定理。

定理1　给定系统$A=(X,E,E_o,\sigma,x_0)$，外部入侵条件下的动力学方程可描述为

$$x(t+1)=\boldsymbol{S}\ltimes_{\mathbb{B}}u(t)\ltimes_{\mathbb{B}}x(t)\tag{12}$$

其中，$x(t)$表示从$x(1)$出发在t时刻系统当前状态估计的向量表达式，$u(t)$表示在t时刻可观测事件的向量表示。

证明过程略，可参考文献[25]进行证明。

事实上，上述定理揭示了入侵估计器的动态转换可用代数方程来表示，并且建立了一步可观测事件的动态转移。接下来，通过定理1中矩阵表达式的重复迭代运算，可得到系统从$x(1)$出发在t时刻系统当前状态估计的向量表达式为

$$\left.\begin{aligned}x(2)&=S\ltimes_{\mathbb{B}}W_{[n,m]}\ltimes_{\mathbb{B}}x(1)\ltimes_{\mathbb{B}}u(1)\\&=S\ltimes_{\mathbb{B}}W_{[n,m]}\ltimes_{\mathbb{B}}x(1)\ltimes_{\mathbb{B}}\delta_m^{j_1}\\x(3)&=S\ltimes_{\mathbb{B}}W_{[n,m]}\ltimes_{\mathbb{B}}x(2)\ltimes_{\mathbb{B}}u(2)\\&=\left(S\ltimes_{\mathbb{B}}W_{[n,m]}\right)^{\ltimes_{\mathbb{B}}2}\ltimes_{\mathbb{B}}x(1)\ltimes_{\mathbb{B}}^2{}_{\mu=1}\delta_m^{j_\mu}\\&\vdots\\x(t+1)&=S\ltimes_{\mathbb{B}}W_{[n,m]}\ltimes_{\mathbb{B}}x(t)\ltimes_{\mathbb{B}}u(t)\\&=\left(S\ltimes_{\mathbb{B}}W_{[n,m]}\right)^{\ltimes_{\mathbb{B}}t}\ltimes_{\mathbb{B}}x(1)\ltimes_{\mathbb{B}}^t{}_{\mu=1}\delta_m^{j_\mu}\end{aligned}\right\}\tag{13}$$

作为一般规则，矩阵$\left(S\ltimes_{\mathbb{B}}W_{[n,m]}\right)^{\ltimes_{\mathbb{B}}t}$可简记为$K_t$，且$K_t:=\left[K_t^1,K_t^2,\cdots,K_t^n\right]$，其中$K_t^{i_1}\in\mathbb{B}^{n\times m^t}$ $(i_1\in\{1,2,\cdots,n\})$表示在长度为t的可观测序列下入侵者从初始状态$x(1)$开始，观测到的当前状态估计矩阵。由于不可观测事件集的存在会使得入侵观测条件下的初始状态向量对应多个状态，因此，表达式(13)可以重写为$x(t+1)=\sum_{\mathbb{B}}^{x_{i_1}\in{\rm UR}(x_0)}K_t^{i_1}\ltimes_{\mathbb{B}}^t{}_{\mu=1}\delta_m^{j_\mu}$。通过观察定理1和表达式(13)，可发现入侵条件下系统当前时刻达到的状态集合与矩阵$\sum_{\mathbb{B}}^{x_{i_1}\in{\rm UR}(x_0)}K_t^{i_1}$的元素有关。

例2　给定系统$A=(X,E,E_o,\sigma,x_0)$，如图1所示，其中$X=\{1,2,3,4\}$, $E_o=\{\alpha,\beta\}$, $x_0=\{1\}$，且$X_{\rm se}=\{4\}$。构造外部入侵可观测条件下的初始状态向量表达式和状态转移结构矩阵分别为：$\boldsymbol{x}(0)=[1\ 1\ 0\ 0]^{\rm T}$和

$$\boldsymbol{S}=\begin{bmatrix}0&0&0&0&0&0&0&0\\0&0&0&0&0&0&0&0\\0&0&0&0&0&1&0&0\\0&0&1&1&1&0&0&0\end{bmatrix}\tag{14}$$

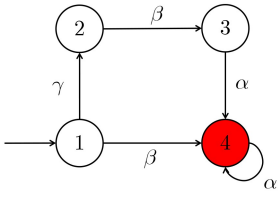

图 1 系统$A=(X,E,E_o,\sigma,x_0)$

当$t=2$时，可得$x(2)=\sum_{\mathbb{B}}^{x_{i_1}\in \mathrm{UR}(1)} \boldsymbol{K}_1^{i_1}\ltimes_{\mathbb{B}}\delta_3^2$，其中

$$\sum_{\mathbb{B}}^{x_{i_1}\in \mathrm{UR}(1)} \boldsymbol{K}_1^{i_1}=\boldsymbol{K}_1^1+\boldsymbol{K}_1^3=\begin{bmatrix}0&0\\0&0\\0&1\\0&1\end{bmatrix} \tag{15}$$

可观察到，$\sum_{\mathbb{B}}^{x_{i_1}\in \mathrm{UR}(1)} \boldsymbol{K}_1^{i_1}(3,2)=1$和$\sum_{\mathbb{B}}^{x_{i_1}\in \mathrm{UR}(1)} \boldsymbol{K}_1^{i_1}(4,2)=1$，这表示入侵者在观察的到事件串$\delta_3^2\sim\beta$时，系统当前时刻的状态估计集合是$\{3,4\}$。

3.2 当前状态不透明的验证

基于上述入侵部分观测条件下的状态估计模型，本节集中对系统的当前状态不透明性进行分析与验证。首先，给出系统当前状态不透明性的定义如下。

定义3 考虑系统$A=(X,E,E_o,\sigma,x_0)$以及秘密状态集$X_{\mathrm{se}}\subseteq X$，

(1) 如果$\sigma(x_0,s)\cap X_{\mathrm{se}}\neq\varnothing$，那么字符串$s\in E^*$是秘密-可达的；

(2) 如果$\sigma(x_0,t)\cap\{X-X_{\mathrm{se}}\}\neq\varnothing$，那么字符串$t\in E^*$是非秘密-可达的；

(3) A称为关于X_{se}不透明的，如果对于任意的秘密-可达串s，总存在另一个非秘密-可达串t使得$P(s)=P(t)$。

值得注意的是，入侵者往往通过系统模型结构和可观事件转移来获得系统的状态估计，根据上述状态不透明性定义，对于任意一个字符串，如果该串验证为秘密-可达的，则至少存在另一个具有相同入侵观测映射的非秘密-可达的字符串，进一步使得入侵者在当前时刻无法判断当前到达的状态是否是秘密状态，此时，具备状态不透明性的系统能够保证入侵者总是不能揭露系统的秘密信息。因此，状态不透明性对于系统信息安全与隐私的分析与控制具有非常重要的意义。

回顾定理1以及式(13)，$x(t+1)=\sum_{\mathbb{B}}^{x_{i_1}\in \mathrm{UR}(x_0)} \boldsymbol{K}_t^{i_1}\ltimes_{\mathbb{B}}\prod_{\mu=1}^{t}\delta_m^{j_\mu}$刻画了在入侵观测初始状态向量条件下具有相同观测映射事件串的当前状态估计。通过观察，发现矩阵$\sum_{\mathbb{B}}^{x_{i_1}\in \mathrm{UR}(x_0)} \boldsymbol{K}_t^{i_1}$是一个包含许多0和1的稀疏矩阵。根据该特点，可将该矩阵的列向量集$\mathrm{Col}\left(\sum_{\mathbb{B}}^{x_{i_1}\in \mathrm{UR}(x_0)} \boldsymbol{K}_t^{i_1}\right)$分为两部分：$\boldsymbol{0}$向量集和非0向量集。如果矩阵的某一列为$\boldsymbol{0}$向量，则该列意味着在对应可观测输入序列下，外界入侵者没有观察到任何信息。明显地，入侵者无法探测到任何秘密状态X_{se}。换句话说，在这些观测序列下，系统总是当前状态不透明的。因此，根据不透明性的定义，将$\mathrm{Col}\left(\sum_{\mathbb{B}}^{x_{i_1}\in \mathrm{UR}(x_0)} \boldsymbol{K}_t^{i_1}\right)$中的0列向量删除，同时，保留其中非0列向量的索引序号，记此序号集合为$\rho_t\in\mathbb{N}^+$，并将属于索引序号集的列向量重构成一个新矩阵，记为$\Theta_{t,\rho_t}\in\mathbb{B}^{n\times|\rho_t|}$。

进一步地，引入布尔矩阵$\boldsymbol{M}\in\mathbb{B}^{n\times m}$的逻辑析取行运算，可实现矩阵所有行的逻辑析取，记为$\mathrm{Row}_\vee(\boldsymbol{M})$，其具体定义为

$$\mathrm{Row}_\vee(\boldsymbol{M}):=\bigvee_{i=1}^{n}\mathrm{Row}_i(\boldsymbol{M}) \tag{16}$$

通过分析定理1中动力学方程和式(12)以及定义的逻辑运算，给出验证当前状态不透明性充分必要代数条件如下。

定理2 给定$A=(X,E,E_o,\sigma,x_0)$和外部入侵条件下的动力学式(12)，则关于秘密状态集X_{se}，系统是当前状态不透明的当且仅当

$$\mathrm{Row}_\vee\left(\bar{\boldsymbol{\Theta}}_{t,\rho_t}\right)=1_{|\rho_t|}^{\mathrm{T}} \tag{17}$$

对于任意的正整数$t\leq n-1$，其中$\bar{\boldsymbol{\Theta}}_{t,\rho_t}\in\mathbb{B}^{(n-|X_{\mathrm{se}}|)\times|\rho_t|}$可通过移除矩阵$\boldsymbol{\Theta}_{t,\rho_t}$的后$|X_{\mathrm{se}}|$行获得。

证明 首先，通过反证法对其充分性进行证明。如果存在某个整数$1\leq t\leq n-1$，使得等式(18)不成立

$$\mathrm{Row}_\vee\left(\bar{\boldsymbol{\Theta}}_{t,\rho_t}\right)=\bigvee_{i=1}^{n-|X_{\mathrm{se}}|}\mathrm{Row}_i\left(\bar{\boldsymbol{\Theta}}_{t,\rho_t}\right)=\boldsymbol{1}_{|\rho_t|}^{\mathrm{T}} \tag{18}$$

这意味着，一定存在某个列索引标号$\lambda\in\rho_t$，使得$\mathrm{Col}_\lambda\left(\bar{\boldsymbol{\Theta}}_{t,\rho_t}\right)=\delta_{n-|X_{\mathrm{se}}|}^0$。同时，$\bar{\boldsymbol{\Theta}}_{t,\rho_t}\in\mathbb{B}^{(n-|X_{\mathrm{se}}|)\times|\rho_t|}$是通过移除非0列向量组成矩阵$\boldsymbol{\Theta}_{t,\rho_t}$的后$|X_{\mathrm{se}}|$行获得的，因此，可推断出“$\boldsymbol{1}$”只能存在于$\mathrm{Col}_\lambda(\boldsymbol{\Theta}_{t,\rho_t})$的后$|X_{\mathrm{se}}|$个元素内。也就是说，通过该观测序列，外部入侵者可确定当前状态属于秘密状态集X_{se}。显然，这与状态不透明性定义相悖。

必要性：如果对于$X_{\mathrm{se}}\subseteq X$，系统是当前状态不透明的，则任何由可观测事件组成的字符串，其从初始状态导出的可达状态集要么为空集，要么至少有一个到达非秘密状态集$X-X_{\mathrm{se}}$。又因为列向量集$\mathrm{Col}(\boldsymbol{\Theta}_{t,\rho_t})$不存在$\boldsymbol{0}$向量且矩阵$\boldsymbol{\Theta}_{t,\rho_t}$的后$|X_{\mathrm{se}}|$行被删除，所以只需要确保矩阵$\boldsymbol{\Theta}_{t,\rho_t}$剩余的每一列中至少包含一个“1”。基于式(16)中行逻辑析取运算，$\mathrm{Row}_\vee\left(\bar{\boldsymbol{\Theta}}_{t,\rho_t}\right)=\boldsymbol{1}_{|\rho_t|}^{\mathrm{T}}$成立。 证毕

为了进一步理解所提方法的计算过程以及提高该文的可读性，算法流程的整体阐述如图2所示。

在实际工程中，设计者往往更关注哪些路径或者转移序列违反了状态不透明性，以便于采取措施进行校正，进而防止隐私信息的泄漏。定理2表明如果系统是当前状态不透明的，当且仅当$\mathrm{Row}_\vee$

$(\bar{\boldsymbol{\Theta}}_{t,\rho_t})=1^{\mathrm{T}}_{|\rho_t|}$不成立，即至少存在一列使得$\mathrm{Col}_\lambda\left(\overline{\boldsymbol{\Theta}}_{t,\rho_t}\right)=\delta^0_{n-|X_{\mathrm{se}}|}$，因此，可定义在$t$步时违反状态不透明性的转移序号为

$$\mathrm{UO}(t):=\{\lambda\in\rho_t|\mathrm{Col}_\lambda\left(\overline{\boldsymbol{\Theta}}_{t,\rho_t}\right)=\delta^0_{n-|X_{\mathrm{se}}|}\}\tag{19}$$

进一步地，根据矩阵STP的运算特性(引理3)，可计算出其对应事件。通过上面定理，可知系统状态不透明性的判定可以转换成逻辑代数的运算，这为更多类型的状态不透明性的验证以及其强化监督控制提供了有效的工具。

备注2　定理2给出了一种基于矩阵的方法来验证有限自动机的当前状态不透明性。相较于现存方法，有以下两方面不同之处：

(1) 在研究问题上，本文提出的代数框架为研究CPS的基于状态的各种不透明属性提供了新的研究思路与视野。

(2) 在研究方法上，矩阵半张量积是我国学者开创性的数学成果，基于此提出验证给定CPS不透明性的方法易计算，同时推广了矩阵半张量积的应用范畴。

本文所提方法具有以下特点：首先，借助矩阵的布尔STP，建立了一种描述入侵估计器动态演化的算法，并基于该代数表达式，简洁明了地导出了不透明性的验证准则，为研究复杂CPSs的分析和控制问题，特别是相关的隐私和安全保护问题提供了新的视角。其次，借助矩阵半张量积Matlab软件包，不透明性的验证问题可以相应地转换成矩阵求解问题。最后，上述结果在未来有望扩展到更复杂的系统[31,32]。

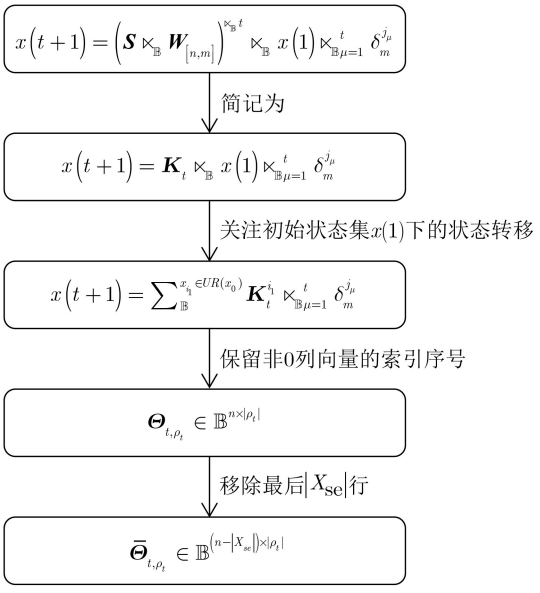

图 2 验证算法的流程图

例3　考虑例2所示的系统$A=(X,E,E_o,\sigma,x_0)$，其中$X_{\mathrm{se}}=\{4\}$是秘密状态集。

当$t=1$时

$$\sum_{\mathbb{B}}^{x_{i_1}\in\mathrm{UR}(1)}\boldsymbol{K}_1^{i_1}=\begin{bmatrix}0&0\\0&0\\0&1\\0&1\end{bmatrix},\bar{\boldsymbol{\Theta}}_{1,\rho_1}=\begin{bmatrix}0\\0\\1\end{bmatrix},$$
$$\mathrm{Row}_\vee\left(\bar{\boldsymbol{\Theta}}_{1,\rho_t}\right)=[1]\tag{20}$$

当$t=2$时

$$\sum_{\mathbb{B}}^{x_{i_1}\in\mathrm{UR}(1)}\boldsymbol{K}_2^{i_1}=\begin{bmatrix}0&0&0&0\\0&0&0&0\\0&0&0&0\\0&0&1&0\end{bmatrix},\bar{\boldsymbol{\Theta}}_{2,\rho_2}=\begin{bmatrix}0\\0\\0\end{bmatrix},$$
$$\mathrm{Row}_\vee\left(\bar{\boldsymbol{\Theta}}_{2,\rho_2}\right)=[0]\tag{21}$$

不满足定理2的条件。然后，系统A关于秘密状态$X_{\mathrm{se}}=\{4\}$不是当前状态不透明的。

4　结束语

本文针对带有不可观测事件的不确定有限自动机建模CPSs，提出一种基于矩阵STP的外部入侵动力学代数方程，并通过矩阵的布尔逻辑运算给出验证当前状态不透明性的充分必要代数条件，为进一步分析其他类型的状态不透明性以及基于状态不透明性强化控制问题提供了一个非常有益的视角。此外，数值算例验证了该方法的有效性。未来的研究方向包括以下两个方面：一方面，当原始系统不是状态不透明时，如何设计一些监控与强化策略来确保不透明性是非常重要的研究问题；另一方面，当前工作假设有限自动机的权重都为1，然而现实系统中事件的转移权重往往是不一样的，因此推广所提方法到加权有限自动机的隐私分析与控制问题具有非常重要的工程意义。

参 考 文 献

[1] 王鹏, 向阳, 宗宇伟, 等. 基于时空π-演算的信息物理融合系统组件可替换性判定[J]. 电子与信息学报, 2012, 34(10): 2494–2500.
WANG Peng, XIANG Yang, ZONG Yuwei, *et al*. Substitution determination of cyber-physical system components via time-space π-calculus[J]. *Journal of Electronics & Information Technology*, 2012, 34(10): 2494–2500.

[2] 汤巍, 景博, 黄以锋. 基于关联图模型的信息物理融合系统感知数据可信性分析[J]. 电子与信息学报, 2015, 37(3): 679–685. doi: 10.11999/JEIT140437.
TANG Wei, JING Bo, and HUANG Yifeng. Creditability analysis of sensor data in the cyber-physical system based on the relationship diagram model[J]. *Journal of Electronics*

& *Information Technology*, 2015, 37(3): 679–685. doi: 10.11999/JEIT140437.

[3] LAFORTUNE S, LIN Feng, and HADJICOSTIS C N. On the history of diagnosability and opacity in discrete event systems[J]. *Annual Reviews in Control*, 2018, 45: 257–266. doi: 10.1016/j.arcontrol.2018.04.002.

[4] JACOB R, LESAGE J J, and FAURE J M. Overview of discrete event systems opacity: Models, validation, and quantification[J]. *Annual Reviews in Control*, 2016, 41: 135–146. doi: 10.1016/j.arcontrol.2016.04.015.

[5] SABOORI A and HADJICOSTIS C N. Notions of security and opacity in discrete event systems[C]. The 2007 46th IEEE Conference on Decision and Control, New Orleans, USA, 2007: 5056–5061.

[6] SABOORI A and HADJICOSTIS C N. Verification of *K*-step opacity and analysis of its complexity[J]. *IEEE Transactions on Automation Science and Engineering*, 2011, 8(3): 549–559. doi: 10.1109/TASE.2011.2106775.

[7] SABOORI A and HADJICOSTIS C N. Verification of infinite-step opacity and complexity considerations[J]. *IEEE Transactions on Automatic Control*, 2012, 57(5): 1265–1269. doi: 10.1109/TAC.2011.2173774.

[8] YIN Xiang and LAFORTUNE S. A new approach for the verification of infinite-step and *K*-step opacity using two-way observers[J]. *Automatica*, 2017, 80: 162–171. doi: 10.1016/j.automatica.2017.02.037.

[9] ZHANG Kuize, YIN Xiang, and ZAMANI M. Opacity of nondeterministic transition systems: A (Bi)simulation relation approach[J]. *IEEE Transactions on Automatic Control*, 2019, 64(12): 5116–5123. doi: 10.1109/TAC.2019.2908726.

[10] MOHAJERAN D and LAFORTUNE S. Transforming opacity verification to nonblocking verification in modular systems[J]. *IEEE Transactions on Automatic Control*, 2020, 65(4): 1739–1746. doi: 10.1109/TAC.2019.2934708.

[11] CHENG Daizhan and QI Hongsheng. A linear representation of dynamics of Boolean networks[J]. *IEEE Transactions on Automatic Control*, 2010, 55(10): 2251–2258. doi: 10.1109/TAC.2010.2043294.

[12] CHENG Daizhan, QI Hongsheng, and LI Zhiqiang. Analysis and Control of Boolean Networks[M]. London: Springer, 2011: 18–22.

[13] CHENG Daizhan and LIU Zequn. Topologies on quotient space of matrices via semi-tensor product[J]. *Asian Journal of Control*, 2019, 21(6): 2614–2623. doi: 10.1002/asjc.2156.

[14] GUO Yuqian, DING Yong, and XIE Dian. Invariant subset and set stability of Boolean networks under arbitrary switching signals[J]. *IEEE Transactions on Automatic Control*, 2017, 62(8): 4209–4214. doi: 10.1109/TAC.2017.2688409.

[15] LI Haitao, XU Xiaojing, and DING Xueying. Finite-time stability analysis of stochastic switched Boolean networks with impulsive effect[J]. *Applied Mathematics and Computation*, 2019, 347: 557–565. doi: 10.1016/j.amc.2018.11.018.

[16] LIANG Jinling, CHEN Hongwei, and LIU Yang. On algorithms for state feedback stabilization of Boolean control networks[J]. *Automatica*, 2017, 84: 10–16. doi: 10.1016/j.automatica.2017.06.040.

[17] FAN Hongbiao, FENG Jun'e, MENG Min, *et al*. General decomposition of fuzzy relations: Semi-tensor product approach[J]. *Fuzzy Sets and Systems*, 2020, 384: 75–90.

[18] FU Shihua, CHENG Daizhan, FENG Jun'e, *et al*. Matrix expression of finite Boolean-type algebras[J]. *Applied Mathematics and Computation*, 2021, 395: 125880. doi: 10.1016/j.amc.2020.125880.

[19] ZHAO Yin, QI Hongsheng, and CHENG Daizhan. Input-state incidence matrix of Boolean control networks and its applications[J]. *Systems & Control Letters*, 2010, 59(12): 767–774.

[20] 韩晓光, 陈增强, 刘忠信, 等. 有界Petri网系统稳定性与镇定性分析的矩阵半张量积方法[J]. 中国科学:信息科学, 2016, 46(11): 1542–1554.
HAN Xiaoguang, CHEN Zengqiang, LIU Zhongxin, *et al*. Semi-tensor product of matrices approach to stability and stabilization analysis of bounded Petri net systems[J]. *Scientia Sinica Informationis*, 2016, 46(11): 1542–1554.

[21] ZHANG Zhipeng, CHEN Zengqiang, HAN Xiaoguang, *et al*. Stabilization of probabilistic finite automata based on semi-tensor product of matrices[J]. *Journal of the Franklin Institute*, 2020, 357(9): 5173–5186.

[22] YUE Jumei, YAN Yongyi, and CHEN Zengqiang. Three matrix conditions for the reduction of finite automata based on the theory of semi-tensor product of matrices[J]. *Science China Information Sciences*, 2020, 63(2): 129203. doi: 10.1007/s11432-018-9739-9.

[23] ZHANG Zhipeng, CHEN Zengqiang, and LIU Zhongxin. Reachability and controllability analysis of probabilistic finite automata via a novel matrix method[J]. *Asian Journal of Control*, 2019, 21(6): 2578–2586. doi: 10.1002/asjc.2160.

[24] CHENG Daizhan, HE Fenghua, QI Hongsheng, *et al*. Modeling, analysis and control of networked evolutionary games[J]. *IEEE Transactions on Automatic Control*, 2015, 60(9): 2402–2415. doi: 10.1109/TAC.2015.2404471.

[25] XU Xiangru and HONG Yiguang. Matrix expression and reachability analysis of finite automata[J]. *Journal of Control Theory and Applications*, 2012, 10(2): 210–215. doi: 10.1007/s11768-012-1178-4.

[26] ZAHNG Zhipeng, XIA Chengyi, and CHEN Zengqiang. On

the stabilization of nondeterministic finite automata via static output feedback[J]. *Applied Mathematics and Computation*, 2020, 365: 124687. doi: 10.1016/j.amc.2019.124687.

[27] ZHANG Zhipeng, SHU Shaolong, and XIA Chengyi. Networked opacity for finite state machine with bounded communication delays[J]. *Information Sciences*, 2021, 572: 57–66. doi: 10.1016/j.ins.2021.04.072.

[28] HAN Xiaoguang, CHEN Zengqiang, and ZHAO Jiemei. Matrix approach to detectability of discrete event systems under partial observation[C]. The 13th IEEE Conference on Automation Science and Engineering, Xi'an, China, 2017: 187–192.

[29] CHEN Zengqiang, ZHOU Yingrui, ZHANG Zhipeng, *et al*. Semi-tensor product of matrices approach to the problem of fault detection for discrete event systems (DESs)[J]. *IEEE Transactions on Circuits and Systems II:Express Briefs*, 2020, 67(12): 3098–3102. doi: 10.1109/TCSII.2020.2967062.

[30] ZAHNG Zhipeng, XIA Chengyi, CHEN Shengyong, *et al*. Reachability analysis of networked finite state machine with communication losses: A switched perspective[J]. *IEEE Journal on Selected Areas in Communications*, 2020, 38(5): 845–853. doi: 10.1109/JSAC.2020.2980920.

[31] 杨卓璇, 马源培, 李慧嘉. 基于DEA模型的中国水行业上市企业的效率和业务类型关系研究[J]. 聊城大学学报:自然科学版, 2020, 33(6): 12–26.
YANG Zhuoxuan, MA Yuanpei, and LI Huijia. The relationship between efficiency and services types of water industry enterprises in China based on DEA model[J]. *Journal of Liaocheng University:Natural Science Edition*, 2020, 33(6): 12–26.

[32] 马源培, 杨卓璇, 李慧嘉. 结合Bass模型和LTV的创新产品扩散预测[J]. 聊城大学学报:自然科学版, 2020, 33(4): 26–32.
MA Yuanpei, YANG Zhuoxuan, and LI Huijia. Innovative product diffusion forecasting combined Bass model and LTV[J]. *Journal of Liaocheng University:Natural Science Edition*, 2020, 33(4): 26–32.

张志鹏：男，1990年生，讲师，研究方向为信息物理系统的隐私分析与安全控制、博弈控制.

许　倩：女，1996年生，硕士生，研究方向为信息物理系统的隐私分析.

夏承遗：男，1976年生，教授，研究方向为复杂网络传播、演化博弈理论、大数据分析和信息安全.

责任编辑：余　蓉