Necessary and Sufficient Condition to Assess Initial-State-Opacity in Live Bounded and Reversible Discrete Event Systems

61st Conference on Decision and Control (CDC 2022)

Francesco Basile, Gianmaria De Tommasi, Carlo Motta, Claudio Sterle

Cancun - 9 Dec 2022

DIETI. UNIVERSITA' DEGLI STUDI DI NAPOLI FEDERICO II
DIPARTIMENTO DI INGEGNERIA ELETTRICA E DELLE TECNOLOGIE DELL'INFORMAZIONE

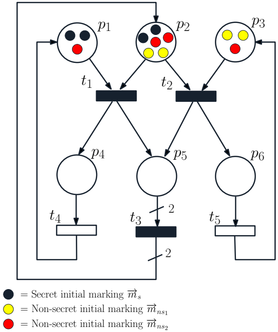
Outline

The *opacity* problem

- **Opacity** in DES is related to the possibility of hiding a secret to external observers (the *intruders*)
- The secret can be either
  - a sequence of events → *Language-based opacity*
  - a system state → *State-based opacity*
    - Initial State Opacity (ISO)
    - Current State Opacity CSO
    - Final State Opacity

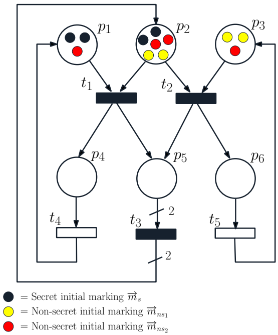
Y.-C. Wu and S. Lafortune,
Comparative analysis of related notions of opacity in centralized and coordinated architectures,
Discrete Event Dyn. Syst., vol. 23, no. 3, pp. 307–339, 2013

Example – 1/2



- Observable (t_4 and t_5) and unobservable (t_1, t_2 and t_3) transitions (associated to events)
- Uncertain initial state (marking)
  - **secret** initial state
    $\vec{m}_s = (2\ 2\ 0\ 0\ 0\ 0)^T$
  - non-secret initial state
    $\vec{m}_{ns_1} = (1\ 2\ 1\ 0\ 0\ 0)^T$
    $\vec{m}_{ns_2} = (0\ 2\ 2\ 0\ 0\ 0)^T$

Example – 2/2



- Starting from $\vec{m}_s$ the only observable transition that can *fire* (i.e. can be observed) is t_4
- The firing of t_4 is always justifiable starting from the non-secret marking $\vec{m}_{ns_2}$
- By observing the fired transitions, under uncertain initial state, an intruder cannot infer if the system *started* from a secret marking $\Rightarrow$ the PN system is ISO

Contribution of this work

- **A necessary and sufficient condition** to assess ISO in DES modeled with PN systems
- The approach relies on both
  - the **algebraic representation of the PN dynamic**. . .
    - $\rightarrow$ enables the use of a standard tool such as ILP problems to check ISO avoiding the computation of graphs whose size is comparable to the one of the reachability graph
  - . . .and **structural representation of the net in terms of T-invariants**
    - $\rightarrow$ allows to represent in a compact way all the possible dynamic evolution in live, bounded and reversible net systems

Contribution (cont'd)

- Only few approaches have been proposed in literature to deal with opacity by exploiting the mathematical representation of PNs to avoid the explicit state space estimation
- In X. Cong *et al.*, Automatica 2018 and ISA Transactions 2019, both ISO and CSO problem are tackled, but a strong assumptions are made
  - secret markings must be modeled by Generalized mutual Exclusion Constraints
  - both the subnets induced by observable and unobservable events need to be acyclic
- Our approach we consider an arbitrary set of uncertain initial markings, that includes both secret and non-secret ones
  - such an assumption is motivated by the fact that the intruder can know the system structure, but not the initial state

Notation & main assumption

Petri net systems

- The P/T net $N = (P, T, \mathbf{Pre}, \mathbf{Post})$
- The incidence matrix $\boldsymbol{C} = \mathbf{Post} - \mathbf{Pre}$
- The net system $\mathcal{S} = \langle N, \boldsymbol{m}_0 \rangle$
- Given a sequence $\sigma \in T^*$, $|\sigma|$ is its length and $\vec{\sigma} = \pi(\sigma)$ is the corresponding firing count vector
- $T = T_o \cup T_{uo}$ and $T_o \cap T_{uo} = \emptyset \rightarrow \mathbf{Pre}_o$ ($\mathbf{Pre}_{uo}$) is the restriction of the **Pre** matrix to the set of observable (unobservable) transitions. The same applies for $\mathbf{Post}_o$ ($\mathbf{Post}_{uo}$) and $\boldsymbol{C}_o$ ($\boldsymbol{C}_{uo}$)

Assumptions

- Boundedness $\rightarrow$ the number of tokens in all places is bounded for all the reachable states
- Liveness $\rightarrow$ any transition can fire an infinite number of times
- Reversibility $\rightarrow$ it is always possible (from any reachable state) to *go back* to the initial state
- Boundedness, liveness and reversibility are three basic properties often fulfilled by engineering-relevant models

Preliminary results – 1/3

Necessary and sufficient condition that must be fulfilled by every sequence with finite length enabled under the marking $\vec{m}_0$ (Garcia Vallès, 1999)
There exists J integer vectors $\vec{s}_1, \ldots, \vec{s}_J \in \mathbb{N}^n$ with $J \leq |\sigma|$ such that the following linear constraints are *fulfilled*

$$
\begin{aligned}
&\vec{m}_0 \geq \mathbf{Pre} \cdot \vec{s}_1 \\
&\vec{m}_0 + \boldsymbol{C} \cdot \vec{s}_1 \geq \mathbf{Pre} \cdot \vec{s}_2 \\
&\ldots \\
&\vec{m}_0 + \boldsymbol{C} \cdot \sum_{i=1}^{J-1} \vec{s}_i \geq \mathbf{Pre} \cdot \vec{s}_J
\end{aligned}
\tag{1a}
$$

$$
\sum_{i=1}^{J} \vec{s}_i = \pi(\sigma) \tag{1b}
$$

iff there exists at least one sequence σ, which is enabled under the marking $\vec{m}_0$

Preliminary results – 2/3

T-invariant

Given a net N, a vector $\overrightarrow{y} \in \mathbb{N}^n$ is called *T-invariant* if $\boldsymbol{C} \cdot \overrightarrow{y} = \overrightarrow{0}$

Support of a T-invariant

$$||\overrightarrow{y}|| = \{t_j \in T \mid \overrightarrow{y}(t_j) > 0\}$$

- A T-invariant $\overrightarrow{y}$ has minimal support if there does not exist another T-invariant $\overrightarrow{y}'$ such that $||\overrightarrow{y}'|| \subset ||\overrightarrow{y}||$
- The set of MS T-invariants $\mathcal{T}(N)$ is finite and constitutes a basis, i.e. any T-invariant can be obtained by linear combination of MS T-invariants

Preliminary results – 2/3

Boundedness, liveness and reversibility for any possible initial state imply that

$$\vec{\sigma} \leq \sum_{\vec{y}_i \in \mathcal{T}(N)} w_i \vec{y}_i$$

with $w_i \in \mathbb{N}$ and $\vec{\sigma}$ the firing count vector of any enabled sequence $\rightarrow$ the net system evolves only along sequences associated to T-invariants

Main result – 1/3

To assess ISO, the following ILP problem must be solved, $\forall\ \vec{m}_s \in \mathcal{M}_s$ and $\forall\ \vec{y} \in \mathcal{T}(N)$,

$$\max \left\{ \sum_{j=1}^{J} \left[(J-j+1) \cdot \sum_{\tau \in \|\vec{y}\|_o} \vec{s}_j(\tau) + B \cdot b_j \right] \right\} \tag{2}$$

Start from a secret marking $\vec{m}_s$, search or the *minimum number* of firing count vectors that cover $\vec{y}$, each holding the maximum number of firings

subject to

$$\begin{cases} \vec{m}_s \geq \mathbf{Pre}_{uo} \cdot \vec{\epsilon}_{s_1} \\ \vec{m}_s + \mathbf{C}_{uo} \cdot \vec{\epsilon}_{s_1} \geq \mathbf{Pre}_o \cdot \vec{s}_1 \\ \vec{m}_s + \mathbf{C}_{uo} \cdot \vec{\epsilon}_{s_1} + \mathbf{C}_o \cdot \vec{s}_1 \geq \mathbf{Pre}_{uo} \cdot \vec{\epsilon}_{s_2} \\ \dots & \text{(3a)} \\ \vec{m}_s + \mathbf{C}_{uo} \cdot \sum_{j=1}^{J} \vec{\epsilon}_{s_j} + \mathbf{C}_o \cdot \sum_{j=1}^{J-1} \vec{s}_j \geq \mathbf{Pre}_o \cdot \vec{s}_J \\ \sum_{j=1}^{J} \vec{s}_j(\tau) \geq \vec{y}(\tau)\,, \quad \forall\ \tau \in T_o & \text{(3b)} \\ \vec{s}_j \leq B(1-b_j) \cdot \vec{1}\,, \quad j = 1, \dots, J & \text{(3c)} \\ \vec{\epsilon}_{s_j}\,,\ \vec{s}_j \in \mathbb{N}^n\,, \quad j = 1, \dots, J & \text{(3d)} \\ b_j \in \{0, 1\}\,, \quad j = 1, \dots, J & \text{(3e)} \end{cases}$$

where $J \geq \mathcal{J}_{\min}$

Main results – 2/3

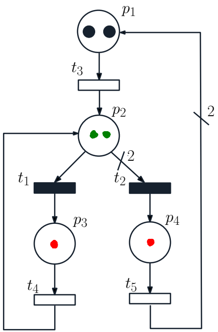
- Let $\vec{s}^{\,\star}_k$ be the not null solution of (2)–(3), with $k = 1, \ldots, K \leq J$
- To assess ISO we seek for possible *unobservable explanations* of $\vec{s}^{\,\star}_k$ starting from any non-secret markings in $\mathcal{M}_{ns}$
  - **If an unobservable explanation EXISTS $\Rightarrow$ the system is ISO**
  - **If an unobservable explanation DOES NOT EXIST $\Rightarrow$ the system is NOT ISO**
- To this aim, the set of optimization vectors $\vec{q}_{k,1}, \ldots, \vec{q}_{k,L_k} \in \mathbb{N}^n$, with $L_k = \|\vec{s}^{\,\star}_k\|_1$, is used to justify each observable occurrence in $\vec{s}^{\,\star}_k$ with a sequence of unobservable transitions

Main result – 3/3

- Let $\mathcal{S} = \langle N, \mathcal{M}_0 \rangle$ be a bounded, live and revirsible net system
- For a given secret marking $\vec{m}_s$ and MS T-invariant $\vec{y}$, let $\vec{s}_1^{\star}, \ldots, \vec{s}_K^{\star}$ be the solution of the ILP problem (2)–(3)
- System $\mathcal{S}$ is ISO *if and only if* the feasibility problem (4) admits a solution $\forall\, \vec{m}_s \in \mathcal{M}_s$ and $\forall\, \vec{y} \in \mathcal{T}(N)$

$$
\begin{cases}
\vec{\mu} \geq \mathbf{Pre}_{uo} \cdot \vec{\epsilon}^{\,1}_{1,1} \\
\ldots \\
\vec{\mu} + \boldsymbol{C}_{uo} \cdot \sum_{k=1}^{K} \sum_{i=1}^{L_k} \sum_{j=1}^{J} \vec{\epsilon}^{\,j}_{k,i} + \boldsymbol{C}_o \cdot \sum_{k=1}^{K-1} \sum_{i=1}^{L_{K-1}} \vec{q}_{k,i} \\
\quad + \boldsymbol{C}_o \cdot \sum_{i=1}^{L_K - 1} \vec{q}_{K,i} \geq \mathbf{Pre}_o \vec{q}_{K,L_K} \\
\sum_{i=1}^{L_k} \vec{q}_{k,i}(\tau) = \vec{s}^{\,\star}_k(\tau), \quad \forall\, \tau \in T_o, \\
\qquad k = 1, \ldots, K, i = 1, \ldots, L_k & \text{(4a)} \\
\vec{\mu} = \sum_{i=1}^{\mathrm{card}(\mathcal{M}_{ns})} \vec{m}_{ns_i} \circ (\mu_i \cdot \vec{1}) & \text{(4b)} \\
\sum_{i=1}^{\mathrm{card}(\mathcal{M}_{ns})} \mu_i = 1 & \text{(4c)} \\
\vec{\epsilon}^{\,j}_{k,i} \in \mathbb{N}^n & \text{(4d)} \\
\vec{q}_{k,i} \in \mathbb{N}^n & \text{(4e)} \\
\mu_i \in \{0, 1\} & \text{(4f)}
\end{cases}
$$

Final example



- $T_o = \{t_3, t_4, t_5\}$ and $T_{uo} = \{t_1, t_2\}$
- MS T-invariants: $\vec{y}_1 = (0\ 1\ 2\ 0 1)^T$ and $\vec{y}_2 = (1\ 0\ 0\ 1\ 0)^T$
- $\vec{m}_{s_1} = (2\ 0\ 0\ 0)^T$
- $\vec{m}_{ns} = (0\ 0\ 1\ 1)^T$ $\rightarrow$ feasibility problem fails for $\vec{y}_1$ $\rightarrow$ NOT ISO
- $\vec{m}_{s_2} = (0\ 2\ 0\ 0)^T$ $\rightarrow$ ISO
- Concerning the computational burden on Intel®Core™ i5 at 2.50 GHz and 8 GB of RAM
  - for $\vec{m}_{s_2}$ and $\vec{y}_1$, the feasibility problem (4) accounts for
    - **23 optimization variables**
    - **64 constraints**
  - the **total time** needed to allocate variables, setup the constraints and solve the feasibility problem in the Matlab environment equals is about **400 ms**

Conclusions

- A necessary and sufficient condition to check ISO in DES modeled as PN system has been presented
- The proposed approach is based on the algebraic representation of PNs, and requires the solution of optimization problems (ILP ones)
  - efficiently scales up with the net marking, especially for nets with high level of parallelism
- The result provided in this work enables to improve privacy of CPSs by enforcing opacity in DES following a supervisory control approach similar to the one proposed

F. Basile, G. De Tommasi, C. Sterle
Non-interference enforcement via supervisory control in bounded Petri nets,
IEEE Trans. Auto. Contr., vol. 66, no. 8, pp. 3653-3666, 2021

- Extend the proposed approach to the case of *labeled* PN systems and to the other state-based opacities

Questions?

UNIVERSITA' DEGLI STUDI DI NAPOLI FEDERICO II
DIPARTIMENTO DI INGEGNERIA ELETTRICA E DELLE TECNOLOGIE DELL'INFORMAZIONE