An algebraic characterization of language-based opacity in labeled Petri nets

14th Workshop on Discrete Event Systems (WODES 2018)

Francesco Basile and Gianmaria De Tommasi

Sorrento Coast - 31 May 2018

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 *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 system state (initial, current, final)
  - a sequence of events

The *opacity* problem

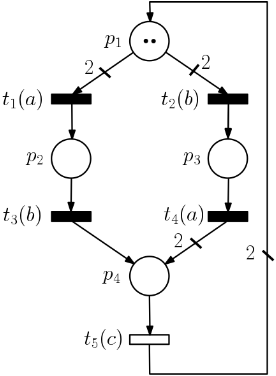
- **Opacity** in DES is related to the possibility of hiding a secret to external observers (the *intruders*)
- The secret can be either
  - a system state (initial, current, final)
  - a sequence of events $\rightarrow$ *Language-based opacity (LBO)*

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 system state (initial, current, final)
  - a sequence of events → *Language-based opacity (LBO)*

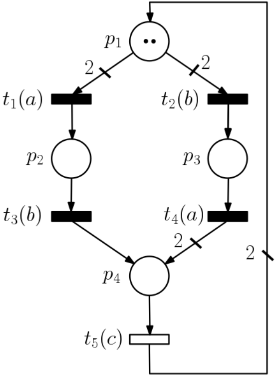
Y.-C. Wu and S. Lafortune,
Comparative analysis of related notions of opacity in centralized and coordinated architectures,
Discrete Event Dyn. Syst., vol. 23, no. 3, pp. 307–339, 2013

Toy example



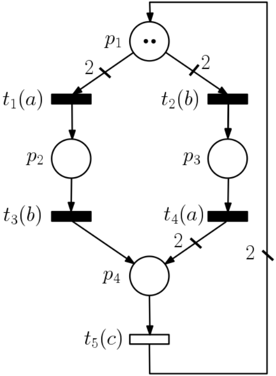
- the secret sequence is *abc*

Toy example



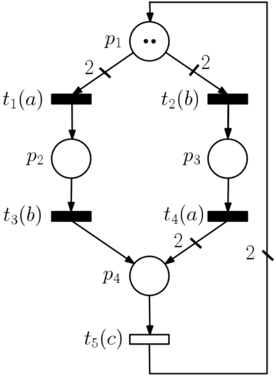
- the secret sequence is *abc*
- *c* is the only observable event (whose occurrence can be directly *measured*)

Toy example



- the secret sequence is *abc*
- *c* is the only observable event (whose occurrence can be directly *measured*)
- observing the single occurrence of *c*, an intruder will never no if either *abc* or *bac* occurred

Toy example



- the secret sequence is *abc*
- *c* is the only observable event (whose occurrence can be directly *measured*)
- observing the single occurrence of *c*, an intruder will never no if either *abc* or *bac* occurred
- the system is said to be opaque

Contribution of this work

- Two conditions to check *language-based opacity* in DES modeled with labeled Petri nets (LPNs)
  - a **necessary and sufficient** one
  - a **sufficient** one (less computationally demanding)

Contribution of this work

- Two conditions to check *language-based opacity* in DES modeled with labeled Petri nets (LPNs)
  - a **necessary and sufficient** one
  - a **sufficient** one (less computationally demanding)
- The proposed approach relies on the algebraic representation of the LPN dynamic
- The proposed conditions are based on the solution of Integer Linear Programming (ILP) problems

Contribution of this work

- Two conditions to check *language-based opacity* in DES modeled with labeled Petri nets (LPNs)
  - a **necessary and sufficient** one
  - a **sufficient** one (less computationally demanding)
- The proposed approach relies on the algebraic representation of the LPN dynamic
- The proposed conditions are based on the solution of Integer Linear Programming (ILP) problems
  - *Off-the-shelf* commercial software can be used (e.g., CPLEX, FICO-Xpress)
  - no need to develop *ad hoc* software tools

Main assumptions

Main assumptions

- The secret language $\mathcal{L}_s$ has finite cardinality

Main assumptions

Main assumptions

- The secret language $\mathcal{L}_s$ has finite cardinality
  - the *non-secret language* is assumed to be equal to $\mathcal{L}_{ns} = \mathcal{L} \setminus \mathcal{L}_s$
- The unobservable subnet is *acyclic* (made also in *Tong et al.*)

Main assumptions

Main assumptions

- The secret language $\mathcal{L}_s$ has finite cardinality
  - the *non-secret language* is assumed to be equal to $\mathcal{L}_{ns} = \mathcal{L} \setminus \mathcal{L}_s$
- The unobservable subnet is *acyclic* (made also in *Tong et al.*)
  - prevents the occurrence of arbitrarily long sequences of unobservable events (which in turn would prevent an intruder to detect the occurrence of a secret for an arbitrarily long period)

Main assumptions

- **Main assumptions**
  - The secret language $\mathcal{L}_s$ has finite cardinality
    - the *non-secret language* is assumed to be equal to $\mathcal{L}_{ns} = \mathcal{L} \setminus \mathcal{L}_s$
  - The unobservable subnet is *acyclic* (made also in *Tong et al.*)
    - prevents the occurrence of arbitrarily long sequences of unobservable events (which in turn would prevent an intruder to detect the occurrence of a secret for an arbitrarily long period)
- *Unnecessary assumptions*
  - the system does not need to be bounded
  - the initial marking is not given ($\boldsymbol{m}_0$ is assumed uncertain, i.e. $\boldsymbol{m}_0$ belongs to a set $\mathcal{M}_0$)

Y. Tong et al.,
Verification of language-based opacity in Petri nets using verifier,
American Control Conference, 2016

Y. Tong et al.,
Verification of state-based opacity using Petri nets,
IEEE Trans. Auto. Contr., vol. 62, no. 6, pp. 2823–2837, 2017

Notation (I)

- The P/T net: $N = (P, T, \mathbf{Pre}, \mathbf{Post})$
- The incidence matrix: $\boldsymbol{C} = \mathbf{Post} - \mathbf{Pre}$
- The labeling function: $\lambda : T \mapsto E$
- Labeled PN system (LPN): $\mathcal{G}\langle N, \mathcal{M}_0, \lambda\rangle$
- Language generated by the LPN: $\mathcal{L}(\mathcal{G}, \mathcal{M}_0)$
- Secret language (assumed *finite*): $\mathcal{L}_s \subset \mathcal{L}(\mathcal{G}, \mathcal{M}_0)$
- Set of transitions associated with the event e:
  $T^e = \{t \in T \mid \lambda(t) = e, \text{with } e \in E\}$
- Length of a word $w \in E^*$: $|w|$
- Occurrences of $e \in E$ in $w \in E^*$:$|w|_e$
- i-th event in the word w: $w[i]$

Notation (II)

- Observable and unobservable events: $E = E_{uo} \cup E_o$, $E_{uo} \cap E_o = \emptyset$
- Natural projection function: $\Pr : E^* \mapsto E_o^*$
- Observable and unobservable transitions:

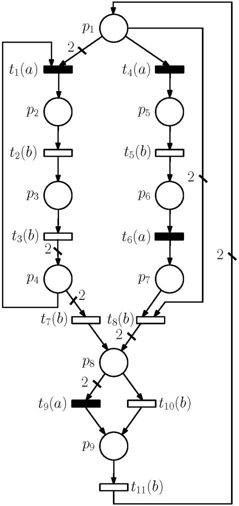
$$T_o = \{t \in T \mid \lambda(t) \in E_o\} \ ,$$
$$T_{uo} = \{t \in T \mid \lambda(t) \in E_{uo}\} \ ,$$

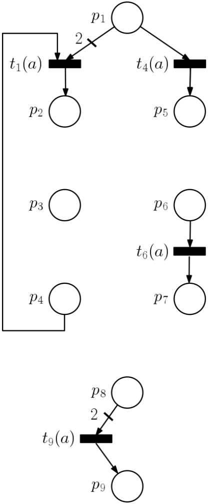
- Given a **firing count vector** $\boldsymbol{\sigma} \in \mathbb{N}^n$, we would like to consider only the firings of either the observable or the unobservable transitions. Hence the following notation is introduced:

$$\boldsymbol{\sigma}_{|T_o} \in \mathbb{N}^n\,, \text{ with } \boldsymbol{\sigma}_{|T_o}(t) = \begin{cases} \boldsymbol{\sigma}(t) & \text{if } t \in T_o \\ 0 & \text{if} t \notin T_o \end{cases}$$

$$\boldsymbol{\sigma}_{|T_{uo}} \in \mathbb{N}^n\,, \text{ with } \boldsymbol{\sigma}_{|T_{uo}}(t) = \begin{cases} \boldsymbol{\sigma}(t) & \text{if } t \in T_{uo} \\ 0 & \text{if} t \notin T_{uo} \end{cases}$$

Unobservable subnet





Language-based opacity

LBO

Given a labeled net system $\mathcal{G} = \langle N, \mathcal{M}_0, \lambda \rangle$, the correspondent natural projection function $\Pr(\cdot)$ and a *secret language* $\mathcal{L}_s \subset \mathcal{L}(\mathcal{G}, \mathcal{M}_0)$, $\mathcal{G}$ is *language-based opaque* (LBO) if for every word $w \in \mathcal{L}_s$, there exists another word $w' \in \mathcal{L}(\mathcal{G}, \mathcal{M}_0) \setminus \mathcal{L}_s$ such that $\Pr(w) = \Pr(w')$.
Equivalently

$$\mathcal{L}_S \subseteq \Pr^{-1}\left[\Pr\left(\mathcal{L}(\mathcal{G}, \mathcal{M}_0) \setminus \mathcal{L}_s\right)\right] .$$

A secret word

$$w \ = \ w_{uo}^1 e_o^1 w_{uo}^2 e_o^2 \cdots w_{uo}^\rho e_o^\rho \,,$$

where:

- $w_o \ = \ \mathrm{Pr}(w) = e_o^1 \cdots e_o^\rho$
- unobservable subwords w_{uo}^i, with $i = 1\,, \ldots\, \rho$, may also be empty.

An algebraic characterization of LBO (I)

$$\boldsymbol{\mu} = \boldsymbol{m}_{0_1} \circ (\mu_1 * \mathbf{1}) + \ldots + \boldsymbol{m}_{0_\mathbf{M}} \circ (\mu_\mathbf{M} * \mathbf{1}) \,, \tag{1}$$

$$\sum_{i=1}^{M} \mu_i = 1 \,, \tag{2}$$

$$\boldsymbol{c}^i = \sum_{t^j \in T^{e_o^i}} \boldsymbol{C}(\cdot\,, t^j) \circ (\gamma_{ij} * \mathbf{1}) \,, \ \forall\, \mathbf{i} = \mathbf{1}\,, \ldots, \rho \,, \tag{3}$$

$$\sum_{j=1}^{\mathrm{card}\left(T^{e_o^i}\right)} \gamma_{ij} = 1 \,, \qquad \forall\, i = 1\,, \ldots, \rho \,, \tag{4}$$

$$\begin{aligned}
&\boldsymbol{\mu} + \boldsymbol{C}_{uo} \cdot \boldsymbol{\sigma}_{1|T_{uo}} \geq \mathbf{0} \,,\\
&\boldsymbol{\mu} + \boldsymbol{C}_{uo} \cdot \boldsymbol{\sigma}_{1|T_{uo}} + \boldsymbol{c}^1 \geq \mathbf{0} \,,\\
&\ldots\\
&\boldsymbol{\mu} + \boldsymbol{C}_{uo} \cdot \sum_{i=1}^{\rho} \boldsymbol{\sigma}_{i|T_{uo}} + \sum_{i=1}^{\rho-1} \boldsymbol{c}^i \geq \mathbf{0} \,,\\
&\boldsymbol{\mu} + \boldsymbol{C}_{uo} \cdot \sum_{i=1}^{\rho} \boldsymbol{\sigma}_{i|T_{uo}} + \sum_{i=1}^{\rho} \boldsymbol{c}^i \geq \mathbf{0} \,,
\end{aligned} \tag{5}$$

- (1) and (2) permit to select one over the *M* possible initial markings
- (3) and (4) associate the firing of single transition for each observable event e_o^i in the secret word *w*
- (5) are the constraints that must be satisfied by the firing count vectors of the *explanations* of $w_o = \Pr(w)$

An algebraic characterization of LBO (II)

$$\sum_{t\in T^{e_{uo_k}}} \sum_{i=1}^{\rho} \boldsymbol{\sigma}_{i_{|T_{uo}}}(t) - |w|_{e_{uo_k}} + 1 \leq B \cdot (1 - \delta_{k1}) \,, \quad \forall\, e_{uo_k} \in E_{uo} \,, \tag{6}$$

$$\sum_{t\in T^{e_{uo_k}}} \sum_{i=1}^{\rho} \boldsymbol{\sigma}_{i_{|T_{uo}}}(t) - |w|_{e_{uo_k}} \geq -B \cdot \delta_{k1} \,, \quad \forall\, e_{uo_k} \in E_{uo} \,, \tag{7}$$

$$-\sum_{t\in T^{e_{uo_k}}} \sum_{i=1}^{\rho} \boldsymbol{\sigma}_{i_{|T_{uo}}}(t) + |w|_{e_{uo_k}} + 1 \leq B \cdot (1 - \delta_{k2}) \,, \quad \forall\, e_{uo_k} \in E_{uo} \,, \,, \tag{8}$$

$$-\sum_{t\in T^{e_{uo_k}}} \sum_{i=1}^{\rho} \boldsymbol{\sigma}_{i_{|T_{uo}}}(t) + |w|_{e_{uo_k}} \geq -B \cdot \delta_{k2} \,, \quad \forall\, e_{uo_k} \in E_{uo} \,, \tag{9}$$

$$\delta_{k1} + \delta_{k2} \leq 1 \,, \qquad \forall\, k = 1, \ldots, \mathrm{card}(E_{uo}) \,, \tag{10}$$

$$\sum_{k=1}^{\mathrm{card}(E_{uo})} (\delta_{k1} + \delta_{k2}) \geq 1 \,. \tag{11}$$

- In order to have opacity, what we want is that $\sum_{t\in T^{e_{uo_k}}} \sum_{i=1}^{\rho} \boldsymbol{\sigma} i_{|T_{uo}}(t)$ is different from $|w|_{e_{uo_k}}$ for at least one unobservable event e_{uo_k}
- Exploiting the technique proposed in Bemporad and Morari 1999, (6)-(11) have been added to force the firing count vectors of the explanations to have at least one component different from the firing count vector of the unobservable substring in the secret

A. Bemporad and M. Morari,
Control of systems integrating logic, dynamics, and constraint,
Automatica, vol. 35, no. 3, pp. 407–427, 1999

A useful lemma

Lemma 3 in the paper

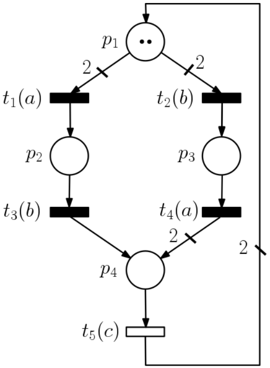
Let $\mathcal{G} = \langle N, \mathcal{M}_0, \lambda \rangle$ be a labeled net system, $w \in \mathcal{L}_S$ a secret word such that $|w_o| = \rho$, with $w_o = \Pr(w) = w_o = e_o^1 \cdots e_o^\rho$, and B be a sufficiently large integer. If the set of constraints (1)–(11) admits a solution, then there exists at least one $w' \in \mathcal{L}(\mathcal{G}, \mathcal{M}_0)$ such that $\Pr(w') = \Pr(w)$.

Sufficient condition

Theorem 3 in the paper

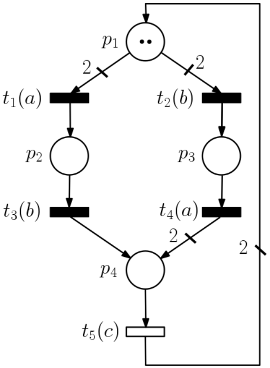
Let $\mathcal{G} = \langle N, \mathcal{M}_0, \lambda \rangle$ be a labeled net system and $\mathcal{L}_s \subseteq \mathcal{L}(\mathcal{G}, \mathcal{M}_0)$ a finite secret language. If for all $w \in \mathcal{L}_s$ the set of constraints (1)–(11) admits a solution, then $\mathcal{G}$ is LBO.

Conservativeness of the sufficient condition



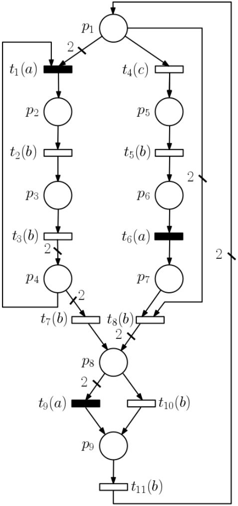
- The proposed sufficient condition cannot take into account the order of the unobservable events in each unobservable subword of the secret

Conservativeness of the sufficient condition



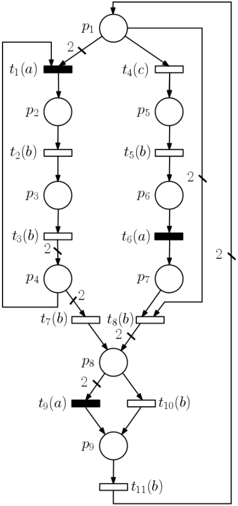
- The proposed sufficient condition cannot take into account the order of the unobservable events in each unobservable subword of the secret
- At the expense of an increase of the number of optimization variable (hence of the computational burden), a necessary and sufficient condition can be derived (Lemma 2 and Theorem 2 in the paper)

Example



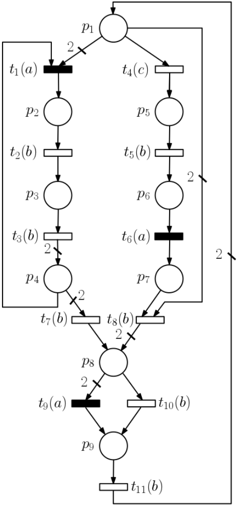
- $\mathcal{L}_s = \{abb\}$
-
$$\mathcal{M}_0'' = \{\boldsymbol{m}_{0_1}'', \boldsymbol{m}_{0_2}''\} = \Big\{(2 \quad 0 \quad 0 \quad 1 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0)^T, \; (2 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 1 \quad 0 \quad 0)^T\Big\}.$$

Example



- $\mathcal{L}_s = \{abb\}$
-
$$\mathcal{M}_0'' = \{\boldsymbol{m}_{0_1}'', \boldsymbol{m}_{0_2}''\} = \left\{\begin{pmatrix}2 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0\end{pmatrix}^T, \begin{pmatrix}2 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0\end{pmatrix}^T\right\}.$$
- Theorem 2 requires to check the feasibility problem only for one word

Example



- $\mathcal{L}_s = \{abb\}$
-
$$\mathcal{M}_0'' = \{\boldsymbol{m}_{0_1}'', \boldsymbol{m}_{0_2}''\} = \Big\{ \begin{pmatrix}2 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0\end{pmatrix}^T, \begin{pmatrix}2 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0\end{pmatrix}^T \Big\}.$$
- Theorem 2 requires to check the feasibility problem only for one word
- GLPK and YALMIP have been used
  - The feasibility problem admits a solution, since *bb* is enabled under $\boldsymbol{m}_0''$

Conclusions

- The mathematical representation of LPN to provide two conditions to check LBO

Conclusions

- The mathematical representation of LPN to provide two conditions to check LBO
- The provided conditions
  - do not require the computation of any kind of reachability graph
  - can be applied also to unbounded LPNs

Conclusions

- The mathematical representation of LPN to provide two conditions to check LBO
- The provided conditions
  - do not require the computation of any kind of reachability graph
  - can be applied also to unbounded LPNs
- The proposed result can be extended along several directions:
  - the possibility of considering the more general case of a non-secret language $\mathcal{L}_{NS} \subseteq \mathcal{L}(\mathcal{G}, \mathcal{M}_0)$
  - the possibility of extend the proposed approach also to *state opacity*
  - the possibility of applying the proposed results to the *synthesis* problem, i.e. the enforcement of opacity in non-opaque systems

Questions?