Assessment of Multilevel Intransitive Non-Interference for Discrete Event Systems

60th Conference on Decision and Control (CDC 2021)

Francesco Basile and Gianmaria De Tommasi

Virtual Edition - 17 Dec 2021

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

Outline

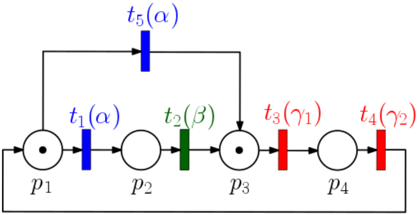
1. Preliminaries
   - Non-interference in DES context
   - Contribution
2. INI assessment through solution of optimization problems
   - Notation and assumptions
   - Main idea
   - Necessary and sufficient condition
3. Example
4. Conclusions

Non-interference

- In system security it is important **to prevent information leaks**
- **Objective:** to prevent to an **intruder** to access to *secret* information
- DES have been used to model different information flow properties
  - Opacity (the secret is a state or a sequence)
  - **Non-Interference**
- The *simplest scenario* for non-interference includes two security levels (*domains*)
  - high, i.e. confidential
  - low, i.e. public

  information is allowed to flow from low to high, but not vice-versa.
- **Intransitive Multilevel Non-Interference (INI)** enables the modelling of more complex scenarios where direct flow between two security levels is forbidden, while a flow *mediated* through a third level is admitted
  - INI enables the modelling of declassification or downgrading of confidential information

INI in PN systems



- Three domains: **A**, **B** and **C**
- $A \nrightarrow C$ although $A \rightarrow B \rightarrow C$
- Information leak from A to C may occur through the firing of t_5

Contribution of this work

- **A necessary and sufficient condition** to assess INI in DES modeled with **bounded labeled** PNs
- The approach relies on the algebraic representation of the PN dynamic
- The condition is based on the solution of Integer Linear Programming (ILP) problems
  - Efficient *off-the-shelf* commercial software available (e.g., CPLEX, FICO-Xpress)

Notation & main assumption

- Labeled PNs
  - The P/T net $N = (P, T, \mathbf{Pre}, \mathbf{Post})$
  - The incidence matrix $\boldsymbol{C} = \mathbf{Post} - \mathbf{Pre}$
  - The set of events E and the labeling function $\ell : T \mapsto E$
  - The labeled net system $\mathcal{S} = \langle N, \boldsymbol{m}_0, \ell \rangle$
  - Given a sequence $\sigma \in T^*$, $|\sigma|$ is its length and $\boldsymbol{\sigma} = \pi(\sigma)$ is the corresponding firing count vector
- Non-interference
  - Set of security domains $\mathbb{D}$
  - Domain mapping function $\mathrm{dom} : E \mapsto \mathbb{D}$
- The net system is bounded (i.e., bounded state space)

Preliminary result

Necessary and sufficient condition that must be fulfilled by every sequence with finite length enabled under the marking $\boldsymbol{m}_0$ (Garcia Vallès, 1999)

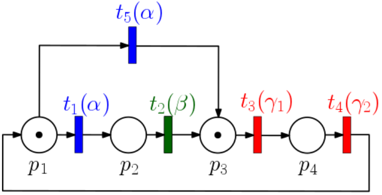
There exists J integer vectors $\boldsymbol{s}_1, \ldots, \boldsymbol{s}_J \in \mathbb{N}^n$ with $J \leq |\sigma|$ such that the following linear constraints are *fulfilled*

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

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

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

Main idea



- $E = \{\alpha, \beta, \gamma_1, \gamma_2\}$ and $\mathbb{D} = \{A, B, C\}$
- $\mathrm{dom}(\alpha) = A, \mathrm{dom}(\beta) = B, \mathrm{dom}(\gamma_1) = \mathrm{dom}(\gamma_2) = C$
- $A \nrightarrow C$
- Given a bounded net, the reachability set can be described by means of $J \geq \mathcal{J}_{\min}$ inequality constraints (1a)

Main idea

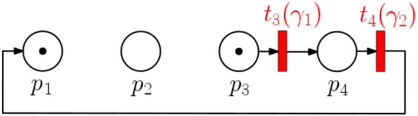


Figure: Net system induced by the C domain.

- For a given $J \geq \mathcal{J}_{\text{min}}$, it is possible to compute the maximum number of occurrences of each event e of a given domain, when all the other domains are *disabled*

Main idea

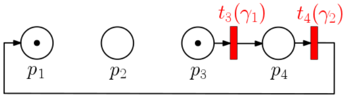


Figure: Net system induced by the C domain.

- These maxima can be computed by solving ILP problems on the net system *induced* by the given domain. For example, for γ_1 with $\mathrm{dom}(\gamma_1) = C$, it is

$$\max \sum_{i=1}^{J} \boldsymbol{s}_i(t_3)$$

subject to the constraints (1a) specified on the induced system reported in the figure

- If $J = 4$ it is $\max \gamma_1 = \max t_3 = 1$ and $\max \gamma_2 = \max t_4 = 1$

Main idea

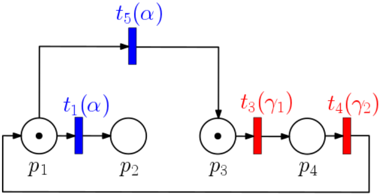


Figure: Net induced by the domains A and C, with $A \nrightarrow C$.

- Given the J constraints (1a), if the number of occurrences in presence of the *non-interfering domains* **exceeds** the maximum occurrences computed in absence of such domain, then the system is not INI
- In the considered case, for $J = 4$, these new maxima are $\max \gamma_1 = \max t_3 = 2$ and $\max \gamma_2 = \max t_4 = 2$
- The system is not INI

Main result

- Given a k-bounded net system $\mathcal{S} = (N, \boldsymbol{m}_0, \ell)$, a set of security domains $\mathbb{D}$ on which an intransitive interference relationship $\rightsquigarrow$ is defined, and an integer $J \geq \mathcal{J}_{\text{min}}$
- For a given domain $U \in \mathbb{D}$
  - for a given event $e \in E_U$, let φ_e be the maximum number of occurrences of event e for the given J
  - $\mathcal{P}$ is the set of domains that cannot interfere with U
  - $\mathcal{Q}$ is the set of domains that can interfere with U
  - $\bar{\mathcal{Q}} = U \cup \mathcal{P}$

Main results (cont'd)

$$\min \sum_{i=1}^{J} \sum_{t_p \in T^{E_{\mathcal{P}}}} \boldsymbol{x}_i(t_p) \tag{2}$$

$$\begin{cases} \boldsymbol{m}_0 \geq \mathbf{Pre}_{T^{E_{\bar{\mathcal{Q}}}}} \cdot \boldsymbol{x}_1 \\ \boldsymbol{m}_0 + \boldsymbol{C}_{T^{E_{\bar{\mathcal{Q}}}}} \cdot \boldsymbol{x}_1 \geq \mathbf{Pre}_{T^{E_{\bar{\mathcal{Q}}}}} \cdot \boldsymbol{x}_2 \\ \dots \\ \boldsymbol{m}_0 + \boldsymbol{C}_{T^{E_{\bar{\mathcal{Q}}}}} \cdot \sum_{i=1}^{J-1} \boldsymbol{x}_i \geq \mathbf{Pre}_{T^{E_{\bar{\mathcal{Q}}}}} \cdot \boldsymbol{x}_J \\ \boldsymbol{m}_0 + \boldsymbol{C}_{T^{E_{\bar{\mathcal{Q}}}}} \cdot \sum_{i=1}^{J} \boldsymbol{x}_i \geq \mathbf{0} & (3a) \\ \sum_{t \in T^e} \sum_{i=1}^{J} \boldsymbol{x}_i(t) \geq \varphi_e + 1 & (3b) \\ \boldsymbol{x}_i \in \mathbb{N}^{\mu}, \quad i = 1, 2, \dots, J & (3c) \end{cases}$$

$$\min \left[\sum_{i=1}^{J} \sum_{t_u \in T^{E_U}} \boldsymbol{y}_i(t_u) + \kappa \sum_{i=1}^{J} \sum_{t_p \in T^{E_{\mathcal{P}}}} \boldsymbol{y}_i(t_p) \right] \tag{4}$$

$$\begin{cases} \boldsymbol{m}_0 \geq \mathbf{Pre}_{T^{E_{\bar{\mathcal{Q}}}}} \cdot \boldsymbol{y}_1 \\ \boldsymbol{m}_0 + \boldsymbol{C}_{T^{E_{\bar{\mathcal{Q}}}}} \cdot \boldsymbol{y}_1 \geq \mathbf{Pre}_{T^{E_{\bar{\mathcal{Q}}}}} \cdot \boldsymbol{y}_2 \\ \dots \\ \boldsymbol{m}_0 + \boldsymbol{C}_{T^{E_{\bar{\mathcal{Q}}}}} \cdot \sum_{i=1}^{J-1} \boldsymbol{y}_i \geq \mathbf{Pre}_{T^{E_{\bar{\mathcal{Q}}}}} \cdot \boldsymbol{y}_J \\ \boldsymbol{m}_0 + \boldsymbol{C}_{T^{E_{\bar{\mathcal{Q}}}}} \cdot \sum_{i=1}^{J} \boldsymbol{y}_i \geq \mathbf{0} & (5a) \\ \sum_{t \in T^e} \sum_{i=1}^{J} \boldsymbol{y}_i(t) = \varphi_e & (5b) \\ \boldsymbol{y}_i \in \mathbb{N}^{\mu}, \quad i = 1, 2, \dots, J & (5c) \end{cases}$$

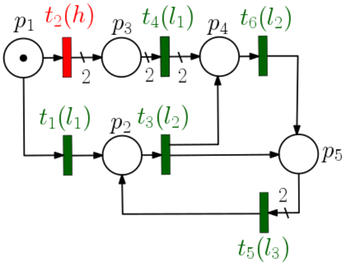
with κ small

Main result (cont'd)

System $\mathcal{S}$ is INI *if and only if* the following two conditions hold $\forall\, U \in \mathbb{D}$ and $\forall\, e \in E_U$

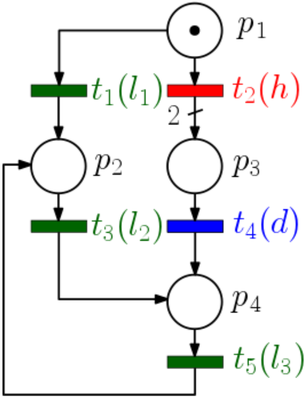
1) the ILP problem (2)-(3) does not admit a solution;
2) being $\tilde{\boldsymbol{y}}_1, \ldots, \tilde{\boldsymbol{y}}_J \in \mathbb{N}^{\mu}$ the solution of the ILP problem (4)-(5), it is $\sum_{i=1}^{J} \sum_{t_p \in T^{E_{\mathcal{P}}}} \tilde{\boldsymbol{y}}_j(t_p) = 0$.

Two domains non-interferent labeled system



- $H \not\rightarrow L$
- When $U = L$, by setting $J = 5$ it is $\varphi_{l_1} = \varphi_{l_3} = 1$ and $\varphi_{l_2} = 3$, and the necessary and sufficient conditions are satisfied
- When $U = H$, the net induced by $E_{\bar{Q}}$ coincides with the one induced by E_H $\Rightarrow$ also in this case the conditions are satisfied
- The net system is non interferent

Non-interferent system with encryption



- $H \not\rightarrow L$ but $H \rightarrow D \rightarrow L$
- Also in this case the necessary and sufficient conditions are satisfied
- The ILP problems for the considered this example include ∼20 optimization variables and ∼20 constraints, and their solution with the GLPK (non commercial) took about 200 μs on a MacBook Pro

Conclusions

- A necessary and sufficient condition to assess multi-level INI in labeled net systems has been presented
- The proposed approach is based on the algebraic representation of PNs, and requires the solution of optimization problems (ILP ones) and
  - is more general with respect to the structural one proposed by Gorrieri and Vernali in 2001, and to the unfolding approach proposed by Baldan and Beggiato in 2018 (it does not require the net to be safe)
  - efficiently scales up with the net marking, especially for nets with high level of parallelism
- Future research will focus on the exploitation of these results to compute a supervisory control law to enforce multi-level INI

Questions?