Non-interference assessment in bounded Petri nets via Integer Linear Programming

American Control Conference 2018 (ACC 2018)

Francesco Basile and Gianmaria De Tommasi

Milwaukee - 28 June 2018
1 Preliminaries
   - Non-interference in DES context
   - Contribution
   - Notation & definitions

2 Main results
   - Necessary and sufficient condition to check SNNI
   - Necessary and sufficient condition to check BSNNI

3 Example

4 Conclusions
In system security it is important to prevent information leaks.
In system security it is important to prevent information leaks.

Objective: to prevent to an intruder to access to secret information.
In system security it is important to prevent information leaks.

**Objective:** to prevent 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)
In system security it is important to prevent information leaks.

Objective: to prevent 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
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

- Y.-C. Wu and S. Lafortune,
  Comparative analysis of related notions of opacity in centralized and coordinated architectures,

- N. Busi and R. Gorrieri,
  A survey on non-interference with Petri nets,
  *Lectures on Concurrency and Petri Nets*, pp. 328–344, 2004
Two classes of users: **high-level** and **low-level** users
Two classes of users: **high-level** and **low-level** users

A leak of information occurs when a low-level user (the **intruder**) obtains information meant to be visible only to high-level users.
Two classes of users: **high-level** and **low-level** users

A leak of information occurs when a low-level user (the **intruder**) obtains information meant to be visible only to high-level users.

Both high-level and low-level users know the system structure, but they interact with the system in two different ways (**views**).
Two classes of users: **high-level** and **low-level** users

A leak of information occurs when a low-level user (the **intruder**) obtains information meant to be visible only to high-level users

Both high-level and low-level users know the system structure, but they interact with the system in two different ways (**views**)

If the high-level view of the system **interferes** with the low-level one, information leaks may occur
In a **strong non-deterministic non-interference (SNNI)** the firings of a high-level transition cannot enable any *additional* firing of any low-level transition.
In a **strong non-deterministic non-interference (SNNI)** the firings of a high-level transition cannot enable any *additional* firing of any low-level transition.

In a **Bisimulation SNNI (BSNNI)** the firing of a low-level transition cannot disable the firing of any high-level transition.
Non-interference properties

- In a **strong non-deterministic non-interference (SNNI)** the firings of a high-level transition cannot enable any *additional* firing of any low-level transition.

- In a **Bisimulation SNNI (BSNNI)** the firing of a low-level transition cannot disable the firing of any high-level transition.

- More restrictive non-interference properties exist:
  - Bisimulation non-deducibility on composition (BNDC)
  - Place-based non-interference (PBNI)
Two necessary and sufficient conditions are provided
Two necessary and sufficient conditions are provided
- to check SNNI in bounded PNs
- to check BSNNI in bounded PNs
Two necessary and sufficient conditions are provided:
- to check SNNI in bounded PNs
- to check BSNNI in bounded PNs

The proposed approach relies on the algebraic representation of the PN dynamic.

The proposed conditions are based on the solution of Integer Linear Programming (ILP) problems.
Two necessary and sufficient conditions are provided
  - to check SNNI in bounded PNs
  - to check BSNNI in bounded PNs

The proposed approach relies on the algebraic representation of the PN 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)
Main assumptions

- The net system is bounded
Main assumptions

- The net system is bounded
- The low-level subnet (subnet induced by the low-level transitions) is acyclic
Main assumptions

- **Main assumptions**
  - The net system is **bounded**
  - The *low-level* subnet (subnet *induced* by the low-level transitions) is **acyclic**

- **Unnecessary assumptions**
  - the net does not need to belong to any special class (ordinary or safe)
Notation

- The P/T net: \( N = (P, L, H, \text{Pre}, \text{Post}) \), with \( L \cap H = \emptyset \)
- The incidence matrix: \( C = \text{Post} - \text{Pre} \)
- The net system \( S = \langle N, m_0 \rangle \)
- Projection of a string on the set of low-view transitions \( L \)
  - \( \text{Pr}_L(\varepsilon) = \varepsilon \)
  - \( \text{Pr}_L(\sigma t) = \begin{cases} 
  \text{Pr}_L(\sigma)t & \text{if } t \in L \\
  \text{Pr}_L(\sigma) & \text{otherwise}
  \end{cases} \)
The P/T net: $N = (P, L, H, \text{Pre}, \text{Post})$, with $L \cap H = \emptyset$

The incidence matrix: $C = \text{Post} - \text{Pre}$

The net system $S = \langle N, m_0 \rangle$

Projection of a string on the set of low-view transitions $L$

- $Pr_L(\varepsilon) = \varepsilon$
- $Pr_L(\sigma t) = \begin{cases} Pr_L(\sigma) t & \text{if } t \in L \\ Pr_L(\sigma) & \text{otherwise} \end{cases}$

The projection $Pr_L(\cdot)$ can be extended in the usual way to sets of sequences, i.e., if $\Sigma \subseteq (L \cup H)^*$ then

$$Pr_L(\Sigma) = \{ Pr_L(\sigma) \mid \sigma \in \Sigma \}.$$
Low-view trace equivalence

Two net systems $S_1$ and $S_2$ are said to be **low-view trace equivalent**, denoting it by

$$S_1 \approx_{tr} S_2,$$

if and only if

$$Pr_{L_1}(\mathcal{L}(N_1, m_{0_1})) = Pr_{L_2}(\mathcal{L}(N_2, m_{0_2})),$$

where $\mathcal{L}(N_i, m_{0_i})$ is the language generated by the $i$-th net system.
Let $S = \langle N, m_0 \rangle$ be a net system and $S_L = \langle N_L, m_0 \rangle$ the system defined on the corresponding low-level subnet $N_L$. $S$ is said to be **strong non-deterministic non-interference** if and only if

$$S \stackrel{Pr}{\approx} tr S_L.$$
Let $S = \langle N, m_0 \rangle$ be a net system and $S_L = \langle N_L, m_0 \rangle$ the system defined on the corresponding low-level subnet $N_L$. $S$ is said to be **strong non-deterministic non-interference** if and only if

$$S \approx_{tr} S_L.$$ 

In a SNNI system, the firings of a high-level transition cannot enable any *additional* firing of any low-level transition.
Low-view bisimilarity

Let $S_1$ and $S_2$ be two net systems. A *low-view bisimulation* from $S_1$ to $S_2$ is a relation $\mathcal{R}$ on $R(N_1, m_{01}) \times R(N_2, m_{02})$ such that if $(m_1, m_2) \in \mathcal{R}$, then for all $t \in \bigcup_{i=1,2} L_i \cup H_i$ it is:

1. If $m_1[t] \mathcal{M}_1$ then there exist $\tau$ and $m'_2$ such that $m_2[\tau] \mathcal{M}_2$, with $Pr_{L_1}(t) = Pr_{L_2}(\tau)$ and $(m'_1, m'_2) \in \mathcal{R}$;

2. If $m_2[t] \mathcal{M}_2$ then there exist $\tau$ and $m'_1$ such that $m_1[\tau] \mathcal{M}_1$, with $Pr_{L_2}(t) = Pr_{L_1}(\tau)$ and $(m'_1, m'_2) \in \mathcal{R}$.

$S_1$ and $S_2$ are said to be **low-view bisimilar**, denoting it by

$$S_1 \Pr \approx_{\text{bis}} S_2,$$

if and only if there exists a low-level bisimulation $\mathcal{R}$ from $S_1$ and $S_2$ such that $(m_{01}, m_{02}) \in \mathcal{R}$. 
BSNNI

Let \( S = \langle N, m_0 \rangle \) be a net system and \( S_L = \langle N_L, m_0 \rangle \) the system defined on the corresponding low-level subnet \( N_L \). \( S \) is said to be \textbf{bisimulation strong non-deterministic non-interference} if and only if

\[
S \Pr \approx_{\text{bis}} S_L.
\]
BSNNI

Let $S = \langle N, m_0 \rangle$ be a net system and $S_L = \langle N_L, m_0 \rangle$ the system defined on the corresponding low-level subnet $N_L$. $S$ is said to be **bisimulation strong non-deterministic non-interference** if and only if

$$S \Pr \approx_{\text{bis}} S_L.$$ 

- The class of SNNI systems includes the class of BSNNI systems, but the two classes are not equivalent.
- In a BSNNI system the firing of a low-level transition cannot disable the firing of any high-level transition.
A bounded net system \( S = \langle N, m_0 \rangle \) is SNNI if and only if the set of constraints

\[
\begin{align*}
m_0 + C_L \cdot \hat{\sigma} & \geq \text{Pre} \cdot s_1 \\
m_0 + C_L \cdot \hat{\sigma} + C \cdot s_1 & \geq \text{Pre} \cdot s_2 \\
& \vdots \\
m_0 + C_L \cdot \hat{\sigma} + C \cdot \sum_{i=1}^{J-1} s_i & \geq \text{Pre} \cdot s_J \\
m_0 + C_L \cdot \hat{\sigma} + C \cdot \sum_{i=1}^{J} s_i & \geq 0 \\
\sum_{i=1}^{J} s_i(t) & = 1
\end{align*}
\]

(1)

does not admit any solution \( s_1, \ldots, s_J \in \mathbb{N}^{n_L+n_H} \) for all \( t \in L \), with \( J \geq J_{\text{min}} \) and \( \hat{\sigma} \) being equal to the solution of the ILP problem

\[
\max \sigma(t) \\
\text{s.t.} \\
\begin{align*}
m_0 + C_L \cdot \sigma & \geq 0 \\
\sigma & \in \mathbb{N}^{n_L}
\end{align*}
\]

(2)
BSNNI for bounded net systems

A SNNI bounded net system \( S = (N, m_0) \) is BSNNI if and only if the set of constraints

\[
\begin{align*}
    m_0 &\geq \text{Pre} \cdot s_1 \\
    m_0 + C \cdot s_1 &\geq \text{Pre} \cdot s_2 \\
    &\vdots \\
    m_0 + C \cdot \sum_{i=1}^{J-1} s_i &\geq \text{Pre} \cdot s_J \\
    m_0 + C \cdot \sum_{i=1}^{J} s_i &\geq 0 \\
    \sum_{i=1}^{J} s_i(t_L) &= \hat{\sigma}(t_L) \\
    \sum_{i=1}^{J} s_i(t_H) &= \sum_{i=1}^{J} \bar{\sigma}_i(t_H)
\end{align*}
\]  

admits a solution \( s_1, \ldots, s_J \in \mathbb{N}^{n_L+n_H} \) for all \( t_L \in L \) and \( t_H \in H \), with \( J \geq J_{\min} \), \( \hat{\sigma} \) being equal to the solution of (2), and \( \bar{\sigma}_1, \ldots, \bar{\sigma}_J \) equal to the solution of the ILP problem

\[
\max \sum_{i=1}^{J} \sigma_i(t_H) \\
\text{s.t.} \begin{align*}
    m_0 &\geq \text{Pre} \cdot \sigma_1 \\
    m_0 + C \cdot \sigma_1 &\geq \text{Pre} \cdot \sigma_2 \\
    &\vdots \\
    m_0 + C \cdot \sum_{i=1}^{J-1} \sigma_i &\geq \text{Pre} \cdot \sigma_J \\
    m_0 + C \cdot \sum_{i=1}^{J} \sigma_i &\geq 0 \\
    \sigma_i &\in \mathbb{N}^{n_L+n_H}, \quad i = 1, 2, \ldots, J
\end{align*}
\]
By setting $J = 5$, the solution of (2) for the transition $l_1 \in L$ returns $\hat{\sigma}(l_1) = 1$

- Given the solution $\hat{\sigma}$, also the feasibility problem (1) admits a solution

- The net system is NOT SNNI

- The time needed to solve a single instance of the ILP problem (2) and of the feasibility problem (1) is less than 500 $\mu$s using GLPK on a MacBook Pro equipped with an Intel® i5 at 3.1 GHz and with 16 GB of RAM
Example (II)

By setting $J = 5$, in this case (1) does not admit any solution for any $t \in L$,

- The net system is SNNI

- The feasibility problem (3) does not admit a solution as well

- The firing of $l$ prevents the firing of the two high level transitions

- The net system is NOT BSNNI

- About 2 ms are needed to check both SNNI and BSNNI on the considered hardware
The mathematical representation of Petri nets has been exploited to provide necessary and sufficient conditions to check both SNNI and BSNNI in bounded systems.
The mathematical representation of Petri nets has been exploited to provide necessary and sufficient conditions to check both SNNI and BSNNI in bounded systems.

Possible extensions:
- Relaxation of the acyclicity assumption on the low-level subnet (submitted to the next CDC)
- Labeled net systems
- Non-interference enforcing (submitted to the next CDC)
Conclusions

- The mathematical representation of Petri nets has been exploited to provide necessary and sufficient conditions to check both SNNI and BSNNI in bounded systems.

- Possible extensions:
  - relaxation of the acyclicity assumption on the low-level subnet (submitted to the next CDC)
  - labeled net systems
  - non-interference enforcing (submitted to the next CDC)
  - algebraic characterization of opacity in PNs (WODES 2018)

F. Basile and G. De Tommasi,
An algebraic characterization of language-based opacity in labeled Petri nets,
WODES’18, Sorrento Coast, Italy, May 2018
Questions?