Sensors selection for $\mathcal{K}$-diagnosability of Petri nets via Integer Linear Programming

Francesco Basile[1] **G. De Tommasi**[2] C. Sterle[2]

[1]DIEM, Università degli Studi di Salerno, Italy
[2]DIETI, Università degli Studi di Napoli Federico II , Italy

23rd Mediterranean Conference on Control Automaton,
Torremolinos, 2015

Outline

Diagnosability in the DES framework

- Fault detection and diagnosability have been studied in the DES framework since early 90s
- The standard approach to check **diagnosability** is based on the **diagnoser** automata (see the seminal paper by *Sampath et al.*, IEEE TAC-1995)
- In the PNs framework, a possible approach to fault diagnosis provides to associate the faults to unobservable transitions
- A PN system is said to be *diagnosable* if every occurrence of an unobservable fault transition can be detected within a finite number of transition firings
- A number of approaches based on PNs have been proposed (*Cabasino et al.*, IEEE TAC-2012, *Basile et al.*, Automatica-2012)

PN notations

- $\mathcal{S} = \langle N, \mathbf{m}_0 \rangle$ is the net system, where $N = (P, T, \mathbf{Pre}, \mathbf{Post})$
- $T = T_o \cup T_{uo}$, and $T_f \subset T_{uo}$
- 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 explanations

Consider a net system $S = \langle N, \mathbf{m}_0 \rangle$ and a sequence $\sigma \in T^*$ such that $\mathbf{m}_0 [\sigma\rangle$ and

$$\sigma = \sigma_{uo}^1 t_o^1 \sigma_{uo}^2 t_o^2 \ldots \sigma_{uo}^k t_o^k ,$$

with $\sigma_{uo}^i \in T_{uo}^*$ and $t_o^i \in T_o$, $i = 1, \ldots, k$. The following set

$$\Sigma(N, \sigma) \triangleq \Big\{ \bar{\sigma} \in T_{uo}^* \mid \bar{\sigma} = \bar{\sigma}_{uo}^1 \bar{\sigma}_{uo}^2 \ldots \bar{\sigma}_{uo}^{k+1} \text{ and } \mathbf{m}_0 [\bar{\sigma}_{uo}^1 t_o^1 \bar{\sigma}_{uo}^2 t_o^2 \ldots \bar{\sigma}_{uo}^k t_o^k \bar{\sigma}_{uo}^{k+1}\rangle \Big\} ,$$

contains the unobservable explanations of σ.

Diagnosability - Formal definitions 1/2

- $L/u = \{v \in T^* \text{ s.t. } uv \in L\}$, is the post-language of L after the sequence of transitions u.
- $Pr : T^* \mapsto T_o^*$ is the usual projection, which erases the unobservable transitions in a sequence u.
- The inverse projection operator Pr_L^{-1} is defined as

$$Pr_L^{-1}(r) = \{u \in L \text{ s.t. } Pr(u) = r\}$$

- Let $\dot{u}$ be the final transition of sequence u and define

$$\Psi(\hat{t}) = \{u \in L \text{ s.t. } \dot{u} = \hat{t}\}$$

Diagnosability - Formal definitions 2/2

Definition (Diagnosable fault)

A fault transition $t_f \in T_f$ is said to be diagnosable if

$$\exists\ h \in \mathbb{N} \text{ such that } \forall\ u \in \Psi(t_f) \text{ and } \forall\ v \in L/u \text{ with } |v| \geq h\,,$$

it is

$$r \in Pr_L^{-1}\big(Pr(uv)\big) \Rightarrow t_f \in r\,.$$

Definition ($\mathcal{K}$–diagnosable fault)

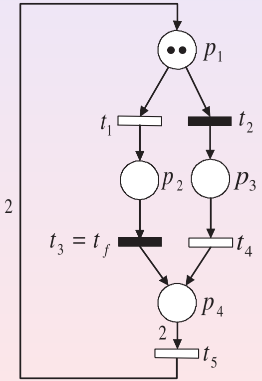
Given $t_f \in T_f$ and $\mathcal{K} \in \mathbb{N}$ (i.e., the maximum length of the postfix is given), t_f is said to be $\mathcal{K}$–diagnosable if

$$\forall\ u \in \Psi(t_f) \text{ and } \forall\ v \in L/u \text{ such that } |v| \geq \mathcal{K}\,,$$

then it is

$$r \in Pr_L^{-1}\big(Pr(uv)\big) \Rightarrow t_f \in r\,.$$

Example



- $T_o = \{t_1, t_4, t_5\}$, $T_{uo} = \{t_2, t_3\}$, $T_f = \{t_3\}$
- Consider the sequence $u = t_1 t_3$, i.e., u is a sequence that ends with the fault transition t_3. It turns out that t_3 is not 1-diagnosable: $v = t_2 t_4$ belongs to the post-language L/u and $t_1 t_2 t_4 \in Pr_L^{-1}\Big(Pr(uv)\Big)$, with $t_3 \notin t_1 t_2 t_4$
- Exploiting similar arguments it readily follows that t_3 is 3-diagnosable, i.e., once t_3 has occurred it is possible to detect it after the firing of three transitions.

- In *Basile et al.*, Automatica-2012 the problem of $\mathcal{K}$-diagnosability has been solved for bounded net systems by
  - exploiting the mathematical representation of PNs
  - using *standard optimization tools* $\rightarrow$ Integer Linear Programming (ILP) problems
- The proposed approach relies on the description (**in terms of linear constraints**) of the following two sets
  - The set of all markings reachable from $\mathbf{m}_0$ that enable t_f (and that are reached by the firing of a sequence that does not contain t_f)

$$\mathcal{M}(t_f) = \left\{ \mathbf{m} \in \mathbb{N}^m \mid \left(\mathbf{m}_0[u\rangle \mathbf{m} \right) \bigwedge \left(t_f \notin u \right) \bigwedge \left(\mathbf{m}[t_f\rangle \right) \right\}.$$

  - The set of all possible continuations of the sequence ut_f, whose postfix contains at least $\mathcal{K}$ firings

$$\mathcal{S}(t_f, \mathcal{K}) = \left\{ \sigma \in T^* \mid \left(\sigma = ut_f v \right) \bigwedge \left(\mathbf{m}_0[\sigma\rangle \right) \right.$$
$$\left. \bigwedge \left(\mathbf{m}_0[u\rangle \mathbf{m} \right) \bigwedge \left(\mathbf{m} \in \mathcal{M}(t_f) \right) \bigwedge \left(|v| \geq \mathcal{K} \right) \right\}.$$

The set of linear constraints describing $\mathcal{S}(t_f, \mathcal{K})$

$\mathcal{F}(\mathbf{m}_0, \hat{t}, \mathcal{J}, \mathcal{K})$:

$$\left\{\begin{array}{l} \mathbf{m}_0 \geq \mathbf{Pre} \cdot \mathbf{u}_1 \\ \mathbf{m}_0 + \mathbf{C} \cdot \mathbf{u}_1 \geq \mathbf{Pre} \cdot \mathbf{u}_2 \\ \dots \\ \mathbf{m}_0 + \mathbf{C} \cdot \displaystyle\sum_{i=1}^{\mathcal{J}-1} \mathbf{u}_i \geq \mathbf{Pre} \cdot \mathbf{u}_{\mathcal{J}} \\ \mathbf{m}_0 + \mathbf{C} \cdot \displaystyle\sum_{i=1}^{\mathcal{J}} \mathbf{u}_i \geq \mathbf{Pre}(\cdot, \hat{t}) \end{array}\right. \qquad \left\{\begin{array}{l} \mathbf{m}_0 + \mathbf{C} \cdot \displaystyle\sum_{i=1}^{\mathcal{J}} \mathbf{u}_i + \mathbf{C}(\cdot, \hat{t}) \geq \mathbf{Pre} \cdot \mathbf{v}_1 \\ \mathbf{m}_0 + \mathbf{C} \cdot \displaystyle\sum_{i=1}^{\mathcal{J}} \mathbf{u}_i + \mathbf{C}(\cdot, \hat{t}) + \mathbf{C} \cdot \mathbf{v}_1 \geq \mathbf{Pre} \cdot \mathbf{v}_2 \\ \dots \\ \mathbf{m}_0 + \mathbf{C} \cdot \displaystyle\sum_{i=1}^{\mathcal{J}} \mathbf{u}_i + \mathbf{C}(\cdot, \hat{t}) + \mathbf{C} \cdot \displaystyle\sum_{j=1}^{\mathcal{K}-1} \mathbf{v}_j \geq \mathbf{Pre} \cdot \mathbf{v}_{\mathcal{K}} \\ \displaystyle\sum_{i=1}^{\mathcal{J}} \mathbf{u}(\hat{t}) = 0 \\ \left\| \displaystyle\sum_{j=1}^{\mathcal{K}} \mathbf{v}_j \right\|_1 \geq \mathcal{K} \end{array}\right.$$

The set of linear constraints for the unobservable explanations of the vectors in $\mathcal{S}(t_f\,,\mathcal{K})$

$\mathcal{E}\left(\mathbf{m}_0\,,\sum_{i=1}^{\mathcal{J}}\mathbf{u}_{i_{|T_o}}+\sum_{j=1}^{\mathcal{K}}\mathbf{v}_{j_{|T_o}}\right)$:

$$
\left\{
\begin{array}{l}
\mathbf{m}_0+\mathbf{C}\cdot\boldsymbol{\epsilon}_{1|T_{uo}}\geq\mathbf{Pre}\cdot\mathbf{s}_{1_{|T_o}}\\
\mathbf{m}_0+\mathbf{C}\cdot\displaystyle\sum_{i=1}^{2}\boldsymbol{\epsilon}_{i_{|T_{uo}}}+\mathbf{C}\cdot\mathbf{s}_{1_{|T_o}}\geq\mathbf{Pre}\cdot\mathbf{s}_{2_{|T_o}}\\
\dots\\
\mathbf{m}_0+\mathbf{C}\cdot\displaystyle\sum_{i=1}^{\mathcal{J}+\mathcal{K}}\boldsymbol{\epsilon}_{i_{|T_{uo}}}+\mathbf{C}\cdot\sum_{j=1}^{\mathcal{J}+\mathcal{K}-1}\mathbf{s}_{j_{|T_o}}\geq\mathbf{Pre}\cdot\mathbf{s}_{\mathcal{J}+\mathcal{K}_{|T_o}}\\
\mathbf{m}_0\geq\mathbf{Pre}\cdot\boldsymbol{\epsilon}_{1_{|T_{uo}}}\\
\mathbf{m}_0+\mathbf{C}\cdot\left(\boldsymbol{\epsilon}_{1_{|T_{uo}}}+\mathbf{s}_{1_{|T_o}}\right)\geq\mathbf{Pre}\cdot\boldsymbol{\epsilon}_{2_{|T_{uo}}}\\
\dots\\
\mathbf{m}_0+\mathbf{C}\cdot\displaystyle\sum_{i=1}^{\mathcal{J}+\mathcal{K}-1}\left(\boldsymbol{\epsilon}_{i_{|T_{uo}}}+\mathbf{s}_{i_{|T_o}}\right)\geq\mathbf{Pre}\cdot\boldsymbol{\epsilon}_{\mathcal{J}+\mathcal{K}_{|T_{uo}}}
\end{array}
\right.
\qquad
\left\{
\begin{array}{l}
\mathbf{s}_{1_{|T_o}}=\mathbf{u}_{1_{|T_o}}\\
\dots\\
\mathbf{s}_{\mathcal{J}_{|T_o}}=\mathbf{u}_{\mathcal{J}_{|T_o}}\\
\mathbf{s}_{\mathcal{J}+1_{|T_o}}=\mathbf{v}_{1_{|T_o}}\\
\dots\\
\mathbf{s}_{\mathcal{J}+\mathcal{K}_{|T_o}}=\mathbf{v}_{\mathcal{K}_{|T_o}}
\end{array}
\right.
$$

Check $\mathcal{K}$-diagnosability via sulution of an ILP problem

Theorem 1

Consider a bounded net system $S = \langle N, \mathbf{m}_0 \rangle$ and a fault transition t_f, let $\mathcal{J}$ be a positive integer such that $\mathcal{J} \geq \mathcal{J}_{\text{min}}$.

Given a positive integer $\mathcal{K}$, t_f is $\mathcal{K}$–diagnosable **if and only if** there exist $3(\mathcal{J} + \mathcal{K})$ vectors $\mathbf{u}_1, \ldots, \mathbf{u}_{\mathcal{J}}, \mathbf{v}_1, \ldots, \mathbf{v}_{\mathcal{K}}$, $\boldsymbol{\epsilon}_1, \ldots, \boldsymbol{\epsilon}_{\mathcal{J}+\mathcal{K}}, \mathbf{s}_1, \ldots, \mathbf{s}_{\mathcal{J}+\mathcal{K}} \in \mathbb{N}^n$ such that

$$\min_{\text{s.t. } \mathcal{F} \cup \mathcal{E}} \sum_{r=1}^{\mathcal{J}+\mathcal{K}} \epsilon_r(t_f) \neq 0 \, .$$

■

Sensors selection for ensuring diagnosability

- The goal is to select a minimal set of sensors to make the system diagnosable $\rightarrow$ *optimal static sensors selection*
- The word *minimal* is used to refer to different objectives
  - select the minimal number of sensors and the transitions/events to ensure diagnosability
  - select the sensors in order to minimize a cost function, which depends on the net transitions/events
- A number of results are available in the context of finite state automata (*Debouk et al.*, DEDS-2002, *Jiang et al.*, IEEE TAC-2003)
- **In the field of PNs, the main contribution is that of Cabasino et al., Automatica-2013, where an approach based on the verifier net allows to tackle the sensors selection problem as a transition relabeling problem**

Main contribution

- The approach *Cabasino et al.*, Automatica-2013 solves the problem in both the bounded and unbounded case
- However, it requires the computation of the reachability/coverability graph of the verified net to analyze its elementary bad paths, being very computation demanding
- We propose an approach based on the solution of ILP problems which exploits the same tools used to check diagnosability (and to perform fault detection $\rightarrow$ see *Basile et al.*, IEEE TAC-2009 and *Dotoli et al.*, Automatica-2009)
- In this preliminary work we propose a technique to compute the minimal number of randomly selected sensors needed to make a net system $\mathcal{K}$-diagnosable
- We also propose a way to further improve this *estimation* by taking into account some elements of the net structures

Problem statement

Problem 1

Given a bounded net system $S = \langle N, \mathbf{m}_0 \rangle$, a fault transition t_f, and a positive integer $\mathcal{K}$, find the integer $\mathbf{Y}^\star$ such that

a) there exists at least one possible choice of observable transitions $T_o^\star$ with $\mathrm{card}\,(T_o^\star) = Y^\star$ such that t_f is $\mathcal{K}$-diagnosable;

b) for all the possible T_o with $\mathrm{card}\,(T_o) < Y^\star$, t_f results $\mathcal{K}$-undiagnosable. ▲

- The solution to Problem 1 can be obtained by checking the condition of Theorem 1 for all the 2^{n-1} possible selections of observable transitions
- In order to avoid this combinatorial explosion, we want exploit the ILP-based formulation of $\mathcal{K}$-diagnosability to obtain an estimation $\hat{\mathbf{Y}} > \mathbf{Y}^\star$

Mimimum number of randomly selected sensors that assure $\mathcal{K}$-diagnosability

Given a bounded net system $S = \langle N, \mathbf{m}_0 \rangle$, a fault transition t_f, and a positive integer $\mathcal{K}$, the minimum number of randomly selected sensors that assure $\mathcal{K}$-diagnosability of t_f is an integer $\widetilde{\mathbf{Y}}$ such that

i) for all the possible choices of observable transitions $\widetilde{T}_o$ such that $\mathrm{card}\left(\widetilde{T}_o\right) = \widetilde{Y}$, t_f is $\mathcal{K}$-diagnosable;

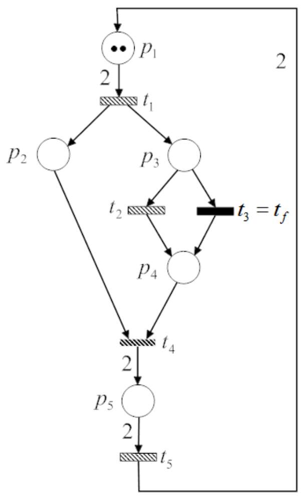
ii) there exist at least one choice of observable transitions T'_o with $\mathrm{card}\,(T'_o) = \widetilde{Y} - 1$ for which t_f results $\mathcal{K}$-undiagnosable.

Proposed approach

- In order to compute $\widetilde{\mathbf{Y}}$ the main ideas exploited by the proposed approach are
  1. To model the possibility of setting the q-th transition observable/unobservable using a binary variable $\hat{s}_{t_q}$
  2. To turn the objective function of Theorem 1 into the constraint

$$\sum_{r=1}^{\mathcal{J}+\mathcal{K}} \epsilon_r(t_f) = 0$$

  3. To maximize $\sum_{q=1}^{n} \hat{s}_{t_q}$



Compute $\widetilde{Y}$ via ILP

Lemma 1

Given a bounded net system $S = \langle N, \mathbf{m}_0 \rangle$, a fault transition t_f, and a positive integer $\mathcal{K}$, let $\mathcal{J} \geq \mathcal{J}_{\text{min}}$ and M be a sufficiently large integer.

The minimum number of randomly selected sensors $\widetilde{Y}$ that assures the $\mathcal{K}$-diagnosability of t_f is given by

$$\widetilde{Y} = \mathcal{Y}_1 + 1 \,,$$

with $\mathcal{Y}_1$ equal to the solution of the following ILP problem

$$\mathcal{Y}_1 = \max_{\text{s.t. } \mathcal{G}} \sum_{q=1}^{n} \hat{s}_{t_q} \,,$$

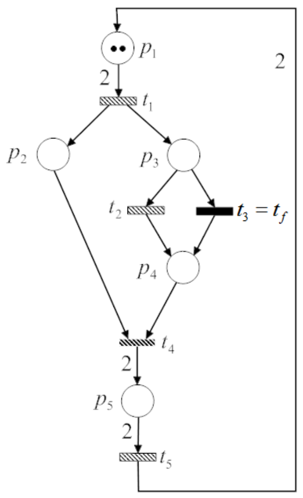
with $\mathcal{G}$ being a *proper* set of constraints ($\rightarrow$ see (7) in the paper) ■

Remarks

- In general Lemma 1 provides a poor estimation of $Y^\star$, that is $\widetilde{Y}$ is overly larger than $Y^\star$
- **Exploiting the knowledge on the net structure** it is possible to improve the estimation of $Y^\star$, i.e. to find an estimation $\hat{\mathbf{Y}}$ such that $\mathbf{Y}^\star \leq \hat{\mathbf{Y}} \leq \widetilde{\mathbf{Y}}$

Sequential paths and generalized diamond structures

- The oriented path $\delta = t^1 p^1 \cdots t^{h-1} p^{h-1} t^h$, with $h \geq 2$, is said to be a **sequential path** if
  - **i)** card $\left({}^\bullet t^1\right) \neq 1$ and card $\left(t^{h\bullet}\right) \neq 1$
  - **ii)** $t^{w\bullet} = \{p^w\}$ for $w = 1, \ldots, h-1$
  - **iii)** $p^{w\bullet} = \left\{t^{w+1}\right\}$ for $w = 1, \ldots, h-1$
- A set of transitions $\gamma = \left\{t^1, \ldots, t^c\right\}$, with $c \geq 2$, is a **generalized diamond structure** if
  - **i)** $t^{1\bullet} = t^{2\bullet} \cdots = t^{c-1\bullet} = t^{c\bullet}$
  - **ii)** ${}^\bullet t^1 = {}^\bullet t^2 \cdots = {}^\bullet t^{c-1} = {}^\bullet t^c$



Improve the estimation of $Y^\star$

Theorem 2

Let $\mathcal{Y}_2$ be the solution of the ILP problem

$$\mathcal{Y}_2 = \max_{\text{s.t. } \mathcal{H}(\mathbf{m}_0, t_f, \mathcal{J}, \mathcal{K})} \sum_{q=1}^{n} \hat{s}_{t_q}, \tag{1}$$

where the constraints $\mathcal{H}\big(\mathbf{m}_0\,, t_f\,, \mathcal{J}\,, \mathcal{K}\big)$ are

$$\begin{cases} \mathcal{G}\big(\mathbf{m}_0\,, t_f\,, \mathcal{J}\,, \mathcal{K}\big) \\ \hat{s}_i = 1\,, \quad \forall\ t_i \in \gamma_{t_f}\,, t_i \neq t_f \\ \displaystyle\sum_{t_i \in \Theta(\delta_j)} \hat{s}_{t_i} \leq 1\,, \quad \forall\ \delta_j \notin \Delta_{t_f} \\ \hat{s}_{t_j} = 1\,, \quad \forall\ \dot{t}_j = \dot{t}(\delta_j)\,, \delta_j \in \Delta_{t_f} \end{cases}$$

Improve the estimation of $Y^\star$ (cont'd)

Theorem 2

1. If (1) is unfeasible, then an estimate of the solution to Problem 1 is given by

$$\hat{Y} = \text{card}\left(\gamma_{t_f}\right) + \text{card}\left(\Delta_{t_f}\right) - 1 \leq \widetilde{Y}\,.$$

   A possible choice for the set of observable transitions that makes t_f $\mathcal{K}$-diagnosable, is to take all the transitions which form a generalized diamond structure with t_f together with $\dot{t}(\delta_j)$ for all $\delta_j \in \Delta_{t_f}$.

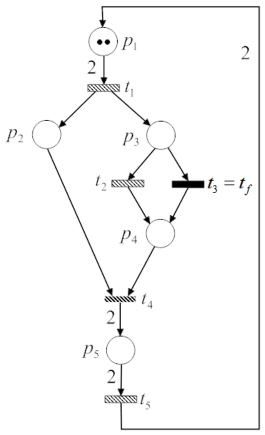
2. If (1) is feasible, an estimation of the solution to Problem 1 is given by

$$\hat{Y} = \mathcal{Y}_2 + 1 \leq \widetilde{Y}\,.$$

Examples 1/2

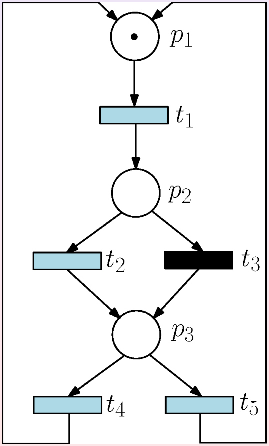
- When $t_f = t_3$ and $\mathcal{K} = 2$, the solution of the ILP problem in Lemma 1 returns $\mathcal{Y}_1 = 3$, which yields $\widetilde{Y} = 4$
- This poor estimation of $Y^\star$, can be easily verified, by checking that there is a choice of three observable transitions that does not include t_2, and which makes the system not 2-diagnosable
- The ILP problem proposed in Theorem 2 constraints
  - t_2 to be observable, since it forms a generalized diamond structure with t_f
  - t_4 to be observable, because $\dot{t}(\delta) = t_4$, with $\delta = \{t_4\,, t_5\,, t_1\}$

  and turns out to be unfeasible. Hence, $\hat{Y} = 2$, and the set of observable transitions $T_o = \{t_2\,, t_4\}$ guarantees the 2-diagnosability of the considered fault.
- In this case, it can be easily verified that $Y^\star = \hat{Y}$, hence Theorem 2 returns the optimal solution to Problem 1



Examples 2/2

- When $t_f = t_3$ and $\mathcal{K} = 3$, Lemma 1 returns $\widetilde{Y} = 4$
- By applying Theorem 2, we obtain $\hat{Y} = 3 < \widetilde{Y}$
- In this case $\hat{Y}$ represents a suboptimal solution to Problem 1, being $Y^{\star} = 2$



Conclusive remarks

- We have proposed an approach to **cast the problem of sensors selection to ensure $\mathcal{K}$-diagnosability in ILP framework**
- This preliminary work allows to compute an estimate (suboptimal) of the optimal solution to the sensor selection problem
- It has been shown how to improve the proposed estimation by exploiting the analysis of some elements of the net structures
- An interesting problem to be explored in the future is the sensors selection when a sensor has an attached cost that depends on the corresponding transition (being such a cost possibly time-varying)

Thank you!