An efficient approach for on-line diagnosis of discrete event systems

F. Basile[1] P. Chiacchio[1] G. De Tommasi[2]

[1]Università di Salerno, Italy
[2]Università di Napoli "Federico II", Italy

MED Conference 2007, Athens, Greece, 27-29 June 2007

Motivations - 1

- Safety issue plays an important role for the reliability of complex systems
- Fault detection is crucial for the safety systems and operators
- When a fault is detected and identified, the control law can be modified in order to continue the operations (increasing the *robustness* of the control systems)
- Fault detection for DES has been issued since the mid 80s, and it is still an *hot topic*
- The standard approach is based on the *diagnoser* automata (Sampath et al., IEEE Trans. Aut. Contr., 1995)
- All possible unobservable events that may occur from a given state have to be considered

Motivations - 1

- Safety issue plays an important role for the reliability of complex systems
- Fault detection is crucial for the safety systems and operators
- When a fault is detected and identified, the control law can be modified in order to continue the operations (increasing the *robustness* of the control systems)
- Fault detection for DES has been issued since the mid 80s, and it is still an *hot topic*
- The standard approach is based on the *diagnoser* automata (Sampath et al., IEEE Trans. Aut. Contr., 1995)
- All possible unobservable events that may occur from a given state have to be considered

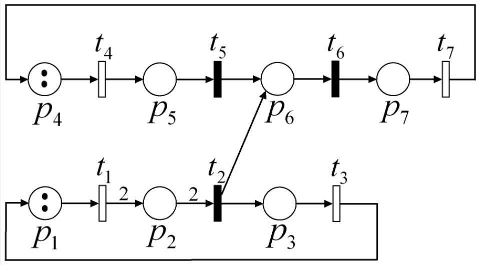
Motivations - 2

- A number of approaches based on a Petri net model of the plant have been proposed
- Faults are associated to unobservable transitions
- These approaches need to estimate the current state of the net
- Explosion of the state space estimation

Motivations - 2

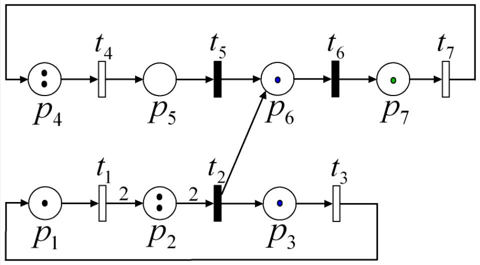
- A number of approaches based on a Petri net model of the plant have been proposed
- Faults are associated to unobservable transitions
- These approaches need to estimate the current state of the net
- Explosion of the state space estimation

Explosion of the state space estimation



$\mathbf{m}_0 = \begin{bmatrix} 2 & 0 & 0 & 2 & 0 & 0 & 0 \end{bmatrix}^{\mathrm{T}}$ - t_1 fires.

Explosion of the state space estimation



$\mathbf{m}_1 = \begin{bmatrix} 1 & 2 & 0 & 2 & 0 & 0 & 0 \end{bmatrix}^{\mathrm{T}}$

$\mathbf{m}_2 = \begin{bmatrix} 1 & 0 & 1 & 2 & 0 & 1 & 0 \end{bmatrix}^{\mathrm{T}}$ - if t_2 has fired

$\mathbf{m}_3 = \begin{bmatrix} 1 & 0 & 1 & 2 & 0 & 0 & 1 \end{bmatrix}^{\mathrm{T}}$ - if t_2 and t_6 have fired

Contribution

In order to cope with the problems related with the state space estimation explosion:

- we propose a fault detection algorithm based on the on-line solution of programming problems
- the proposed approach is based on the new concept of *generalized marking* of a P/T net
- at each step the estimated generalized marking is always unique
- the proposed approach is very efficient in terms of requested memory

Outline

Place/Transition nets - 1

P/T net

A *Place/Transition* net is a 4-tuple $N = (P, T, \mathbf{Pre}, \mathbf{Post})$.

Marking of a net

$$\mathbf{m} : P \rightarrow \mathbb{N}$$

It is usually represented with a vector $\mathbf{m} \in \mathbb{N}^m$.

Enabling and firing of a transition

- A transition $t \in T$ is enabled at $\mathbf{m}$ iff $\mathbf{m} \geq \mathbf{Pre}(\cdot, t)$ and it is denoted as $\mathbf{m}[t\rangle$.
- An enabled transition t may fire yielding the marking $\mathbf{m}' = \mathbf{m} + \mathbf{C}(\cdot, t)$ and this is denoted as $\mathbf{m}[t\rangle\mathbf{m}'$.

Place/Transition nets - 2

Firing sequences and firing vectors

Given a firing sequence $\sigma = t_1 \dots t_k$, the function

$$\boldsymbol{\sigma} : T \to \mathbb{N} \,,$$

is called *firing count vector* of the fireable sequence σ.

State equation

If $\mathbf{m}_0[\sigma\rangle\mathbf{m}$, then it is possible to write in vector form

$$\mathbf{m} = \mathbf{m}_0 + \mathbf{C} \cdot \boldsymbol{\sigma} \,.$$

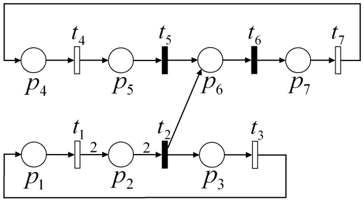
Induced subnets

T'-Induced subnet

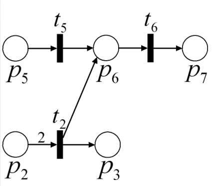
Given a net $N = (P, T, \mathbf{Pre}, \mathbf{Post})$, and a subset $T' \subseteq T$, the T'-induced subnet on N, denoted with $N' \prec_{T'} N$, is the 4-tuple $N' = (P', T', \mathbf{Pre}', \mathbf{Post}')$, where $P' = {}^{\bullet}T' \cup T'^{\bullet}$, while $\mathbf{Pre}'$ and $\mathbf{Post}'$ are the restrictions of $\mathbf{Pre}$ and $\mathbf{Post}$ to P' and T'.

The subnet $N' \prec_{T'} N$ can be obtained from N removing all the places which are not connected with any transition in T', and all the transitions in $T \setminus T'$.

Induced subnets - Example



(a) A net N.



(b) The $N_{uo} \prec_{T_{uo}} N$ subnet.

Figure: Example of induced subnet.

Assumptions

1. Each transition is associated to an event and two different transitions cannot share the same event.
2. The net N has $T = T_o \cup T_{uo}$, with $T_o \cap T_{uo} = \emptyset$, and $T_f \subseteq T_{uo}$.
3. $N_{uo} \quad \prec_{T_{uo}} \quad N$ is *acyclic*.

Generalized marking μ

A *generalized marking* is a function

$$\boldsymbol{\mu} : P \to \mathbb{Z}$$

A transition t is enabled at $\boldsymbol{\mu}$ iff:

ia) $t \in T_o$,

iia) $t \in T_{uo}$ and $\exists\ \sigma \in T_{uo}^*$ s.t. $\boldsymbol{\mu}' = \boldsymbol{\mu} + \mathbf{C}\boldsymbol{\sigma} \geq \mathbf{0}$, $t \in \sigma$, with $\boldsymbol{\sigma} = \pi(\sigma)$.

The notation $\boldsymbol{\mu}[t\rangle$ denotes that t is enabled at $\boldsymbol{\mu}$.
A transition t may fire if:

ib) $t \in T_o$ is enabled and its firing has been observed.

iib) $t \in T_{uo}$ is enabled,

When a transition t fires, it yields the generalized marking $\boldsymbol{\mu}' = \boldsymbol{\mu} + \mathbf{C}(\cdot, t)$, this is denoted as $\boldsymbol{\mu}[t\rangle\boldsymbol{\mu}'$.

Negative markings

- The negative components of μ represent the tokens that are needed to explain:
  - the firing of an observed transition;
  - the firing of an unobservable transition that must have fired.
- As far as the fault diagnosis is concerned, μ allows to store in a compact way all the needed information about the state space estimation.

Unobservable explanations

Given a generalized marking $\boldsymbol{\mu} \in \mathbb{Z}^m$

$$\Sigma(N, \boldsymbol{\mu}) = \{\sigma \in T_{uo}^* \mid \boldsymbol{\mu}[\sigma\rangle\boldsymbol{\mu}' \text{ s.t. } \boldsymbol{\mu}' \geq 0\}$$

is the set of all the *unobservable explanations* enabled at $\boldsymbol{\mu}$ and

$$\Sigma_f(N, \boldsymbol{\mu}, t_f) = \{\sigma \in T_{uo}^* \mid \boldsymbol{\mu}[\sigma\rangle\boldsymbol{\mu}' \text{ s.t. } \boldsymbol{\mu}' \geq 0 \\ \text{and } \boldsymbol{\sigma}(t_f) \neq 0\,, \text{ with } \boldsymbol{\sigma} = \pi(\sigma)\}$$

is the set of all the *faulty unobservable explanations* which includes the fault t_f enabled at $\boldsymbol{\mu}$.

The sets

$$\boldsymbol{\Sigma}(N, \boldsymbol{\mu}) = \{\boldsymbol{\sigma} \in \mathbb{N}^n \mid \exists\, \sigma \in \Sigma(N, \boldsymbol{\mu}) \text{ s.t. } \pi(\sigma) = \boldsymbol{\sigma}\}$$

and

$$\boldsymbol{\Sigma}_f(N, \boldsymbol{\mu}, t_f) = \{\boldsymbol{\sigma} \in \mathbb{N}^n \mid \exists\, \sigma \in \Sigma_f(N, \boldsymbol{\mu}, t_f) \\ \text{s.t. } \pi(\sigma) = \boldsymbol{\sigma}\}$$

are the corresponding set of firing count vectors.

Unobservable explanations - Results 1

Theorem 1

Given a net N with $T = T_o \cup T_{uo}$. Let $\boldsymbol{\mu}$ be a generalized marking, $t_f \in T_f \subseteq T_{uo}$ a fault transition, then

$$|\boldsymbol{\Sigma}(N,\boldsymbol{\mu})| = |\boldsymbol{\Sigma}_f(N,\boldsymbol{\mu},t_f)| \iff \min_{\boldsymbol{\sigma}\in\boldsymbol{\Sigma}(N,\boldsymbol{\mu})} \boldsymbol{\sigma}(t_f) \neq 0 \,.$$

Corollary 1

Given a net N with $T = T_o \cup T_{uo}$. Let $\boldsymbol{\mu}$ be a generalized marking, $t_f \in T_f \subseteq T_{uo}$ a fault transition, then

$$|\boldsymbol{\Sigma}(N,\boldsymbol{\mu})| = |\boldsymbol{\Sigma}_f(N,\boldsymbol{\mu},t_f)| \iff \begin{array}{l} \forall\ \boldsymbol{\sigma} \in \boldsymbol{\Sigma}(N,\boldsymbol{\mu})\,, \\ \boldsymbol{\sigma}(t_f) \neq 0 \,. \end{array}$$

Unobservable explanations - Results 2

Theorem 2

Given a net N with $T = T_o \cup T_{uo}$. Let $\boldsymbol{\mu}$ be a generalized marking, $t_f \in T_f \subseteq T_{uo}$ a fault transition, then

$$|\boldsymbol{\Sigma}_f(N, \boldsymbol{\mu}, t_f)| \neq 0 \iff \max_{\boldsymbol{\sigma} \in \boldsymbol{\Sigma}(N, \boldsymbol{\mu})} \boldsymbol{\sigma}(t_f) \neq 0\,.$$

Corollary 2

Given a net N with $T = T_o \cup T_{uo}$. Let $\boldsymbol{\mu}$ be a generalized marking, $t_f \in T_f \subseteq T_{uo}$ a fault transition, then

$$|\boldsymbol{\Sigma}_f(N, \boldsymbol{\mu}, t_f)| \neq 0 \iff \exists\, \boldsymbol{\sigma} \in \boldsymbol{\Sigma}(N, \boldsymbol{\mu})\,,\ \boldsymbol{\sigma}(t_f) \neq 0\,,$$

and

$$|\boldsymbol{\Sigma}_f(N, \boldsymbol{\mu}, t_f)| = 0 \iff \forall\, \boldsymbol{\sigma} \in \boldsymbol{\Sigma}(N, \boldsymbol{\mu})\,,\ \boldsymbol{\sigma}(t_f) = 0\,.$$

Fault detection algorithm - 1

Given a net N with $T = T_o \cup T_{uo}$. Let $t_f \in T_f \subseteq T_{uo}$ and $\boldsymbol{\mu}$ a generalized markings. As far as the detection of t_f is concerned, the following three conditions have to be checked:

1a) $|\boldsymbol{\Sigma}(N, \boldsymbol{\mu})| = |\boldsymbol{\Sigma}_f(N, \boldsymbol{\mu}, t_f)| \iff t_f$ has occurred

2a) $|\boldsymbol{\Sigma}_f(N, \boldsymbol{\mu}, t_f)| = 0 \iff t_f$ has not occurred

3a) $|\boldsymbol{\Sigma}_f(N, \boldsymbol{\mu}, t_f)| \neq 0 \iff t_f$ may be occurred

The three conditions listed above are equivalent to:

1b) $\min_{\boldsymbol{\sigma} \in \boldsymbol{\Sigma}(N,\boldsymbol{\mu})} \boldsymbol{\sigma}(t_f) \neq 0 \iff t_f$ has occurred

2b) $\max_{\boldsymbol{\sigma} \in \boldsymbol{\Sigma}(N,\boldsymbol{\mu})} \boldsymbol{\sigma}(t_f) = 0 \iff t_f$ has not occurred

3b) $\max_{\boldsymbol{\sigma} \in \boldsymbol{\Sigma}(N,\boldsymbol{\mu})} \boldsymbol{\sigma}(t_f) \neq 0 \iff t_f$ may be occurred

Fault detection algorithm - 2

1 $\boldsymbol{\mu} = \boldsymbol{\mu}_0 = \mathbf{m}_0$ (* Initialization *)

2 **for all** $t_{f_i} \in T_f$ **do**

- 2.1 **if** $\min_{\boldsymbol{\sigma} \in \boldsymbol{\Sigma}(N,\boldsymbol{\mu})} \boldsymbol{\sigma}(t_{f_i}) = F \neq 0$,
  then (* t_{f_i} has occurred F times *)
  - 2.1.1 report that t_{f_i} **has occurred**
  - 2.1.2 $\boldsymbol{\mu}_{|P_{uo}} = \boldsymbol{\mu}_{|P_{uo}} + \mathbf{C}_{uo}(\cdot, t_{f_i})F$ (* Update $\boldsymbol{\mu}$ *)
  - 2.1.3 **go to** Step **2** (* Restart the **for** cycle *)
- 2.2 **if** $\max_{\boldsymbol{\sigma} \in \boldsymbol{\Sigma}(N,\boldsymbol{\mu})} \boldsymbol{\sigma}(t_{f_i}) = G \neq 0$,
  then report that t_{f_i} **may be occurred**
  (* t_{f_i} may be occurred G times *)
- 2.3 **else** report that t_{f_i} **has not occurred yet**

3 **end for**

4 **if** $\mathbf{C}_{uo}\boldsymbol{\sigma}_{|T_{uo}} \geq -\boldsymbol{\mu}_{|P_{uo}}$ admits only one solution $\boldsymbol{\sigma}^*_{|T_{uo}}$,
then $\boldsymbol{\mu}_{|P_{uo}} = \boldsymbol{\mu}_{|P_{uo}} + \mathbf{C}_{uo}\boldsymbol{\sigma}^*_{|T_{uo}}$ (* Update $\boldsymbol{\mu}$ *)

5 **wait for** a new observed transition $\bar{t} \in T_o$

6 $\boldsymbol{\mu} = \boldsymbol{\mu} + \mathbf{C}(\cdot, \bar{t})$ (* Update $\boldsymbol{\mu}$ *)

7 **go to** Step **2**

Compute min and max - 1

Since $N_{uo} \prec_{T_{uo}} N$ is *acyclic*, then:

$$\boldsymbol{\Sigma}(N, \boldsymbol{\mu}) = \{\boldsymbol{\sigma} \in \mathbb{N}^n \mid \mathbf{C}_{uo}\boldsymbol{\sigma}_{|T_{uo}} \geq -\boldsymbol{\mu}_{|P_{uo}} \text{ and } \boldsymbol{\sigma}_{|T_o} = \mathbf{0}\},$$

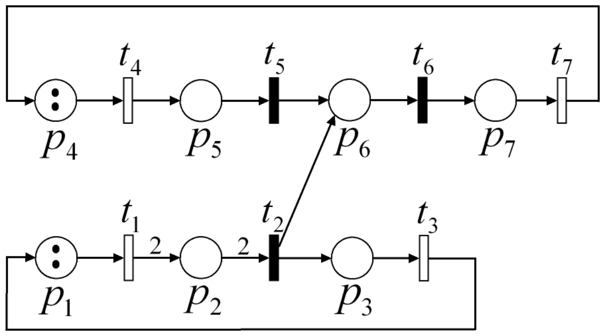
thus $\min_{\boldsymbol{\sigma}\in\boldsymbol{\Sigma}(N,\boldsymbol{\mu})} \boldsymbol{\sigma}(t_f)$ and $\max_{\boldsymbol{\sigma}\in\boldsymbol{\Sigma}(N,\boldsymbol{\mu})} \boldsymbol{\sigma}(t_f)$ can be computed by solving an Integer Linear Programming (ILP) problem.

Compute min and max - 2

ILP problems have NP-hard complexity, but:

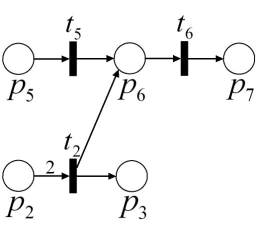
1. If $N_{uo} \prec_{T_{uo}} N$ is TS1 or TS2 then the calculation of $\min_{\boldsymbol{\sigma} \in \boldsymbol{\Sigma}(N,\boldsymbol{\mu})} \boldsymbol{\sigma}(t_f)$ and $\max_{\boldsymbol{\sigma} \in \boldsymbol{\Sigma}(N,\boldsymbol{\mu})} \boldsymbol{\sigma}(t_f)$ to the evaluation of algebraic functions of net generalized marking (see Li and Wonham, Trans. Autom. Contr., 1994).
2. If $\mathbf{C}_{uo}$ is totally unimodular, then $\min_{\boldsymbol{\sigma} \in \boldsymbol{\Sigma}(N,\boldsymbol{\mu})} \boldsymbol{\sigma}(t_f)$ and $\max_{\boldsymbol{\sigma} \in \boldsymbol{\Sigma}(N,\boldsymbol{\mu})} \boldsymbol{\sigma}(t_f)$ are solutions of a *linear programming problem*, which has polynomial complexity. If $N_{uo} \prec_{T_{uo}} N$ is a *Marked Graph*, then $\mathbf{C}_{uo}$ is totally unimodular.
3. ...

Example



Let $\mu_0 = \left[2\ 0\ 0\ 2\ 0\ 0\ 0\right]^{\mathrm{T}}$, and $T_f = \{t_5\}$.

Example



The $N_{uo} \prec_{T_{uo}} N$ subnet is TS2, thus the ILP problems $\min_{\sigma \in \Sigma(N,\mu)} \sigma(t_5)$ and $\max_{\sigma \in \Sigma(N,\mu)} \sigma(t_5)$ admit the following closed - form solutions:

$$\min_{\sigma \in \Sigma(N,\mu)} \sigma(t_5) = \max\left(-\mu_{|p_6} - \mu_{|p_7} - \left\lfloor \frac{\mu_{|p_2}}{2} \right\rfloor, 0 \right),$$

$$\max_{\sigma \in \Sigma(N,\mu)} \sigma(t_5) = \mu_{|p_5} .$$

Example

Action	$\boldsymbol{\mu}$	$\min_{\boldsymbol{\sigma} \in \boldsymbol{\Sigma}(N,\boldsymbol{\mu})} \boldsymbol{\sigma}(t_5)$	$\max_{\boldsymbol{\sigma} \in \boldsymbol{\Sigma}(N,\boldsymbol{\mu})} \boldsymbol{\sigma}(t_5)$
Initialization	$[2\ 0\ 0\ 2\ 0\ 0\ 0]^T$	0	0
t_1 fires	$[1\ 2\ 0\ 2\ 0\ 0\ 0]^T$	0	0
t_4 fires	$[1\ 2\ 0\ 1\ 1\ 0\ 0]^T$	0	1
t_7 fires	$[1\ 2\ 0\ 2\ 1\ 0\ -1]^T$	0	1
t_7 fires	$[1\ 2\ 0\ 3\ 1\ 0\ -2]^T$	1	1
Update $\boldsymbol{\mu}$ (Step **2.1.2**)	$[1\ 2\ 0\ 3\ 0\ 1\ -2]^T$	0	0
Update $\boldsymbol{\mu}$ (Step **4**)	$[1\ 0\ 1\ 3\ 0\ 0\ 0]^T$	0	0

Conclusion & future works

- Generalized markings have been introduced and used to perform fault diagnosis of DES modeled as Petri nets.
- The estimated generalized marking is always unique.
- Efficient on-line implementation in terms of memory request.
- In general the proposed approach request the resolution of ILP problems.

Future works

- Further research is ongoing to rewrite ILP problems into an equivalent one, which are formulated only on the subnets that influence the occurrence of the observed event.
- Add timing information to improve fault diagnosis (paper submitted to IEEE CASE 2007)

Conclusion & future works

- Generalized markings have been introduced and used to perform fault diagnosis of DES modeled as Petri nets.
- The estimated generalized marking is always unique.
- Efficient on-line implementation in terms of memory request.
- In general the proposed approach request the resolution of ILP problems.

Future works

- Further research is ongoing to rewrite ILP problems into an equivalent one, which are formulated only on the subnets that influence the occurrence of the observed event.
- Add timing information to improve fault diagnosis (paper submitted to IEEE CASE 2007)

. . . The End

Thank you!