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

F. Basile\textsuperscript{1}    P. Chiacchio\textsuperscript{1}    G. De Tommasi\textsuperscript{2}

\textsuperscript{1}Università di Salerno, Italy
\textsuperscript{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
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
An efficient approach for on-line diagnosis of discrete event systems

Explosion of the state space estimation

\[
\mathbf{m}_0 = \begin{bmatrix} 2 & 0 & 0 & 2 & 0 & 0 & 0 \end{bmatrix}^T - t_1 \text{ fires.}
\]
An efficient approach for on-line diagnosis of discrete event systems

Explosion of the state space estimation

\[ m_1 = \begin{bmatrix} 1 & 2 & 0 & 2 & 0 & 0 & 0 \end{bmatrix}^T \]

\[ m_2 = \begin{bmatrix} 1 & 0 & 1 & 2 & 0 & 1 & 0 \end{bmatrix}^T \quad \text{if } t_2 \text{ has fired} \]

\[ m_3 = \begin{bmatrix} 1 & 0 & 1 & 2 & 0 & 0 & 1 \end{bmatrix}^T \quad \text{if } t_2 \text{ and } t_6 \text{ have fired} \]
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 \textit{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

1. PNs notation
2. Generalized marking
3. Unobservable explanations
4. Fault detection algorithm
5. Example
6. Conclusion & future works
An efficient approach for on-line diagnosis of discrete event systems

PNs notation

Place/Transition nets - 1

**P/T net**

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

**Marking of a net**

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

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

**Enabling and firing of a transition**

- A transition $t \in T$ is enabled at $m$ iff $m \geq \text{Pre}(\cdot, t)$ and it is denoted as $m[t]$.
- An enabled transition $t$ may fire yielding the marking $m' = m + C(\cdot, t)$ and this is denoted as $m[t]m'$. 
Place/Transition nets - 2

Firing sequences and firing vectors
Given a firing sequence $\sigma = t_1 \ldots t_k$, the function

$$\sigma : T \rightarrow \mathbb{N},$$

is called firing count vector of the fireable sequence $\sigma$.

State equation
If $m_0[\sigma]m$, then it is possible to write in vector form

$$m = m_0 + C \cdot \sigma.$$
**Induced subnets**

*\( T' \)-Induced subnet*

Given a net \( N = (P, T, \text{Pre}, \text{Post}) \), and a subset \( T' \subseteq T \), the \( T' \)-induced subnet on \( N \), denoted with \( N' \prec_{T'} N \), is the 4-tuple \( N' = (P', T', \text{Pre}', \text{Post}') \), where \( P' = \bullet T' \cup T'\bullet \), while \( \text{Pre}' \) and \( \text{Post}' \) are the restrictions of \( \text{Pre} \) and \( \text{Post} \) 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. $N_{uo} \prec_{T_{uo}} N$ is acyclic.
Generalized marking $\mu$

A generalized marking is a function

$$\mu : P \rightarrow \mathbb{Z}$$

A transition $t$ is enabled at $\mu$ iff:

ia) $t \in T_o$,

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

The notation $\mu[t]$ denotes that $t$ is enabled at $\mu$.

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 $\mu' = \mu + C(\cdot, t)$, this is denoted as $\mu[t] \mu'$. 
The negative components of $\mu$ 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, $\mu$ allows to store in a compact way all the needed information about the state space estimation.
Unobservable explanations

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

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

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

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

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

The sets

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

and

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

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 $\mu$ be a generalized marking, $t_f \in T_f \subseteq T_{uo}$ a fault transition, then

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

#### Corollary 1

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

$$|\Sigma(N, \mu)| = |\Sigma_f(N, \mu, t_f)| \iff \forall \sigma \in \Sigma(N, \mu), \sigma(t_f) \neq 0.$$
Unobservable explanations - Results 2

Theorem 2

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

\[
|\Sigma_f(N, \mu, t_f)| \neq 0 \iff \max_{\sigma \in \Sigma(N, \mu)} \sigma(t_f) \neq 0.
\]

Corollary 2

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

\[
|\Sigma_f(N, \mu, t_f)| \neq 0 \iff \exists \sigma \in \Sigma(N, \mu), \sigma(t_f) \neq 0,
\]

and

\[
|\Sigma_f(N, \mu, t_f)| = 0 \iff \forall \sigma \in \Sigma(N, \mu), \sigma(t_f) = 0.
\]
Given a net $N$ with $T = T_o \cup T_{uo}$. Let $t_f \in T_f \subseteq T_{uo}$ and $\mu$ a generalized markings. As far as the detection of $t_f$ is concerned, the following three conditions have to be checked:

1a) $|\Sigma(N, \mu)| = |\Sigma_f(N, \mu, t_f)| \iff t_f$ has occurred

2a) $|\Sigma_f(N, \mu, t_f)| = 0 \iff t_f$ has not occurred

3a) $|\Sigma_f(N, \mu, t_f)| \neq 0 \iff t_f$ may be occurred

The three conditions listed above are equivalent to:

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

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

3b) $\max_{\sigma \in \Sigma(N, \mu)} \sigma(t_f) \neq 0 \iff t_f$ may be occurred
Fault detection algorithm - 2

1 \( \mu = \mu_0 = m_0 \) (* Initialization *)
2 for all \( t_{f_i} \in T_f \) do
   2.1 if \( \min_{\sigma \in \Sigma(N, \mu)} \sigma(t_{f_i}) = F \neq 0 \),
       then (* \( t_{f_i} \) has occurred \( F \) times *)
       2.1.1 report that \( t_{f_i} \) has occurred
       2.1.2 \( \mu|_{P_{uo}} = \mu|_{P_{uo}} + C_{uo}(\cdot, t_{f_i})F \) (* Update \( \mu \) *)
       2.1.3 go to Step 2 (* Restart the for cycle *)
   2.2 if \( \max_{\sigma \in \Sigma(N, \mu)} \sigma(t_{f_i}) = G \neq 0 \),
       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 \( C_{uo} \sigma|_{T_{uo}} \geq -\mu|_{P_{uo}} \) admits only one solution \( \sigma^*|_{T_{uo}} \),
   then \( \mu|_{P_{uo}} = \mu|_{P_{uo}} + C_{uo} \sigma^*|_{T_{uo}} \) (* Update \( \mu \) *)
5 wait for a new observed transition \( \bar{t} \in T_o \)
6 \( \mu = \mu + C(\cdot, \bar{t}) \) (* Update \( \mu \) *)
7 go to Step 2
Compute $\min$ and $\max - 1$

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

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

thus $\min_{\sigma \in \Sigma(N, \mu)} \sigma(t_f)$ and $\max_{\sigma \in \Sigma(N, \mu)} \sigma(t_f)$ can be computed by solving an Integer Linear Programming (ILP) problem.
ILP problems have **NP-hard complexity**, but:

1. If $N_{uo} \prec_{T_{uo}} N$ is TS1 or TS2 then the calculation of $\min_{\sigma \in \Sigma(N,\mu)} \sigma(t_f)$ and $\max_{\sigma \in \Sigma(N,\mu)} \sigma(t_f)$ to the evaluation of algebraic functions of net generalized marking (see Li and Wonham, Trans. Autom. Contr., 1994).

2. If $C_{uo}$ is totally unimodular, then $\min_{\sigma \in \Sigma(N,\mu)} \sigma(t_f)$ and $\max_{\sigma \in \Sigma(N,\mu)} \sigma(t_f)$ are solutions of a linear programming problem, which has polynomial complexity. If $N_{uo} \prec_{T_{uo}} N$ is a Marked Graph, then $C_{uo}$ is totally unimodular.

3. ...
Example

Let \( \mu_0 = [2 \ 0 \ 0 \ 2 \ 0 \ 0 \ 0]^T \), and \( T_f = \{t_5\} \).
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

<table>
<thead>
<tr>
<th>Action</th>
<th>( \mu )</th>
<th>( \min_{\sigma \in \Sigma(N, \mu)} \sigma(t_5) )</th>
<th>( \max_{\sigma \in \Sigma(N, \mu)} \sigma(t_5) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initialization</td>
<td>( [2 0 0 2 0 0 0]^T )</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>( t_1 ) fires</td>
<td>( [1 2 0 2 0 0 0]^T )</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>( t_4 ) fires</td>
<td>( [1 2 0 1 1 0 0]^T )</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>( t_7 ) fires</td>
<td>( [1 2 0 2 1 0 \ - \ 1]^T )</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>( t_7 ) fires</td>
<td>( [1 2 0 3 1 0 \ - \ 2]^T )</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Update ( \mu ) (Step 2.1.2)</td>
<td>( [1 2 0 3 0 \ - \ 2]^T )</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Update ( \mu ) (Step 4)</td>
<td>( [1 0 1 3 \ 0 0]^T )</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
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!