Fault Diagnosis in Discrete Event Systems modeled by Petri Nets with Outputs

Yu Ru and C. N. Hadjicostis

Department of Electrical and Computer Engineering
University of Illinois at Urbana-Champaign

May 2008
Fault Diagnosis in Discrete Event Systems – Overview

Fault model

- Faults modeled as unobservable events
- Faults classified into fault types $F_1, F_2, \ldots, F_q$
- Need to identify the occurrence of fault of type $F_i$

Approaches

- Diagnoser approach based on automata (Sampath, 1995)
- Extension of the diagnoser approach to Petri nets (Ushio, 1998; Chung, 2005; Genc, 2007)
- Basis reachability tree approach (Giua, 2005)
- Faults modeled as unobservable events with unknown structure (Cabasino, 2008)
Motivation for Refined Diagnosis Results

Diagnosis results about the occurrence of fault of type $F_i$ traditionally consists of

- ‘$N$’: no fault of type $F_i$ has occurred
- ‘$F_i$’: a fault of type $F_i$ must have occurred
- ‘$A$’: a fault of type $F_i$ may or may not have occurred

The results can be made more precise if likelihood information about events is available

- Refined diagnosis results by introducing the notion of belief
- Belief captures the likelihood of fault types in individual execution paths
Petri Net Notation

- Petri net structure $N = (P, T, F, W)$
  $P = \{p_1, \ldots, p_4\} \& T = \{t_1, \ldots, t_5\}$
- Marking $M : P \leftrightarrow N_0$:
  $M_0 = (2 \ 0 \ 0 \ 0)^T$
- Petri net $G = \langle N, M_0 \rangle$
- $t$ is enabled at $M$ if $M(p) \geq W(p, t)$ for
  $p \in P$ (e.g., $t_2$ is enabled at $M_0$)
- State equation: $M = M_0 + D\sigma$

$$D = (D_{ij}) = (W(t_j, p_i) - W(p_i, t_j)) = \begin{pmatrix}
1 & -1 & 0 & 0 & 0 \\
0 & 1 & -1 & 0 & -1 \\
0 & 0 & 1 & -1 & 0 \\
-1 & 0 & 0 & 1 & 1
\end{pmatrix}$$
Petri Net Notation

Petri Net with Outputs

- Petri net with outputs $Q = (G, \Sigma, L, P_s)$
- $G = \langle N, M_0 \rangle$
- $\Sigma$ is a given alphabet
- Labeling function $L : T \mapsto \Sigma \cup \{\varepsilon\}$
- $P_s \subseteq P$ is a set of places with sensors
- Note: $(G, \Sigma, L)$ is a labeled Petri net

For the above Petri net
- $\Sigma = \{a, b, c\}$
- $L(t_1) = a, L(t_2) = L(t_3) = b, L(t_4) = L(t_5) = \varepsilon$
- $P_s = \{p_2\}$ ($p_2$ is drawn with a red, thick circle)
Outline of the Talk

**Part I**: Fault diagnosis problem formulation in the context of Petri nets with outputs

**Part II**: Definition of belief and online monitor construction to obtain beliefs in the context of labeled Petri nets

**Part III**: Adaptation of the solution from Petri nets with outputs to labeled Petri nets
Part I: Fault diagnosis in Petri nets with outputs
Information from Sensors

- Petri net with outputs $Q = (G, \Sigma, L, P_s)$
- Transition sensors specified by $L$: each transition firing emits a label, except $t_4$ and $t_5$
- $P_s$ includes places with sensors that provide the number of tokens at those places: $P_s = \{p_2\}$ in this case

Assume transition $t_5$ is a fault transition and the (unknown) system trajectory is

$$[2 \ 0 \ 0 \ 0]^T \xrightarrow{t_2} [1 \ 1 \ 0 \ 0]^T \xrightarrow{t_5} [1 \ 0 \ 0 \ 1]^T$$

$\Rightarrow$ The observation from sensors is $[0] \xrightarrow{b} [1] \xrightarrow{} [0]$

$\Rightarrow$ Fault transition $t_5$ must have occurred because of the observation $[1] \xrightarrow{} [0]$
Problem Formulation

Given Information

- System Model: $Q = (G, \Sigma, L, P_s)$ whose unobservable subnet is deadlock structurally bounded, and a given weight function $wt(M, t)$
- Fault Model: $T_{F_i}$ (set of transitions of type $F_i$ for $i = 1, \ldots, q$) such that $T_{F_i} \subseteq T_{uo} := \{ t \in T \mid L(t) = \epsilon \}$ and $T_{F_i} \cap T_{F_j} = \emptyset$ if $i \neq j$
- Observation: $M^0_{P_s} \xrightarrow{d_1} M^1_{P_s} \xrightarrow{d_2} \cdots M^{k-1}_{P_s} \xrightarrow{d_k} M^k_{P_s}$ where $d_i \in \Sigma \cup \{\epsilon\}$ and $M^i_{P_s}$ denotes information from place sensors regarding $M_i$

Goal

- Determine the occurrence of each fault type and its belief

Definitions: Unobservable subnet is obtained by removing observable transitions and related arcs; a Petri net is deadlock structurally bounded if $\exists y$ with positive integer entries such that $y^T D < 0^T_m$ (Ru, 2008)
Part II: Notion of belief and online monitor construction (to obtain beliefs) for labeled Petri nets
Weight Function

\[ wt(M, t) : R(G, M_0) \times T_M \mapsto R_0^+ \]

- \( R(G, M_0) \): set of reachable markings; \( T_M \): set of transitions enabled at \( M \)
- Nonnegative weight can capture, for example, the probability of occurrence of a particular transition at a particular state
- Assume the function can be extended for \( S = t_{s_1} t_{s_2} \cdots t_{s_k} \) enabled at \( M \) by taking the product of the weights of individual transition

Examples of weight functions

- \( wt(M, t) = 1, \forall M \in R(G, M_0), \forall t \in T_M \)
- \( wt(M, t) = \frac{1}{|T_M|}, \forall M \in R(G, M_0), \forall t \in T_M \) (shown in the right figure)

- Weight function can also be defined based on probabilistic models
Given \((G, \Sigma, L)\) and a sequence of observed labels \(\omega\), the belief on the occurrence of fault of type \(F_i\) is

\[
b(\omega, F_i) = \frac{\sum_{S \in S(\omega)} \text{ and } \exists t \in T_{F_i} \text{ appearing in } S \text{ wt}(M_0, S)}{\sum_{S \in S(\omega)} \text{ wt}(M_0, S)}
\]

- \(S(\omega) = \{S | S \in T^* T_0 : M_0[S] \text{ and } L(S) = \omega\}\), where \(T_0 = T \setminus T_{uo}\)
- \(b(\omega, F_i)\) is closer to 1 (or 0), we are more (or less) confident about the occurrence of a fault of type \(F_i\)
- For example, the observation is \(a\) and \(t_f\) is a fault transition of type \(F\) (shown in the right figure)

\[
b(a, F) = \frac{1}{5} \text{ if } \text{ wt}(M, t) = 1
\]

\[
b(a, F) = \frac{1}{3} \text{ if } \text{ wt}(M, t) = \frac{1}{|T_M|}
\]
Recursive Updating of Weight Function: Intuition

**Key Idea**: compute $wt(M_0, S)$ for $S \in S(\omega)$ recursively to calculate $b(\omega, F_i)$

- Given $\omega = e_1 \cdots e_j$ and $\omega' = \omega e_{j+1}$, let $S = t_{s_1} \cdots t_{s_k} \in S(\omega)$ (i.e., $M_0[t_{s_1}]M_1 \cdots [t_{s_k}]M_k$, $t_{s_k}$ is observable and $L(S) = \omega$), and let $S' = St_{s_{k+1}} \cdots t_{s_l} \in S(\omega')$. Then
  
  $$wt(M_0, S') = wt(M_0, S) \times wt(M_k, t_{s_{k+1}}) \times \cdots \times wt(M_{l-1}, t_{s_l})$$

- Store $wt(M_0, S)$ at $M_k \in C(\omega) := \{M | \exists S \in S(\omega) : M_0[S]M\}$

- For example, if $S = \varepsilon$ and $S' = t_1t_2t_3$,
  
  $$wt(M_0, S') = wt(M_0, S) \times wt(M_0, t_1) \times wt(M_{11}, t_2) \times wt(M_2, t_3) = 1 \times \frac{1}{3} \times \frac{1}{2} \times 1$$

- Similarly, if $S'' = t_2t_1t_3$, we can store $wt(M_0, S') + wt(M_0, S'')$ at $M_3$ because $S'$ and $S''$ share the same future behavior.
Monitor Construction

Representation of Weight Function

Structure \((M, K)\) to hold marking and weight function information

- \(M\) is a marking reachable from \(M_0\)
- \(K\) is a \((q + 1)\)-dimensional row vector: i) \(K(i)\) for \(i = 1, \ldots, q\) represents the weighted sum of consistent paths that drive the system from \(M_0\) to \(M\) and also contain faults of type \(F_i\); ii) \(K(q + 1)\) represents the weighted sum of all consistent paths that drive the system from \(M_0\) to \(M\)

Let \(C'(\omega) = \bigcup_{M \in C(\omega)} \{(M, K)\}\), then for \(i = 1, \ldots, q\)

\[
b(\omega, F_i) = \frac{\sum_{(M, K) \in C'(\omega)} K(i)}{\sum_{(M, K) \in C'(\omega)} K(q + 1)}
\]

- To compute \(C'(\omega)\) recursively, we need update each node \((M, K)\) if a fault transition or a normal transition fires; there are four rules (Cases I-IV) on updating node \((M, K)\) (for more details, refer to the paper)
Algorithm

1. \( \omega_0 = \varepsilon, C'(\omega_0) = \{(M_0, K_0)\} \) where \( K_0 = [0_{1 \times q} \ 1] \).
2. Let \( i = 0 \).
3. Wait until a new event \( e \) is observed.
4. Let \( i = i + 1, \omega_i = \omega_{i-1}e, C'(\omega_i) = \emptyset \).
5. Let \( C_{uo} = \bigcup_{(M,K) \in C'(\omega_{i-1})} UR(M,K) \)
6. For all \( (M,K) \in C_{uo} \)
   For all \( t \) such that \( L(t) = e \) and \( M[t) \)
   Compute \( M' = M + D(:,t) \): (i) if \( M' \) does not appear in any node of \( C'(\omega_i) \), calculate \( K' \) using the rules in Cases I-II and add \((M',K')\) into \( C'(\omega_i) \); (ii) if \( M' \) exists in node \((M',K')\) of \( C'(\omega_i) \), update \( K' \) using the rules in Cases III-IV.
7. Output the belief \( b(\omega_i,F_i) \) for \( i = 1, \ldots, q \).

\[ UR(M,K) = \{(M',K') | \exists S = t_{s_1} \cdots t_{s_j} \in T^*, M[S]M' \} \], where \( K' \) is computed using updating rules sequentially to each \( S \) (such that \( M[S]M' \)).
Part III: Transformation from Petri nets with outputs to labeled Petri nets
Intuition via Example

- Firing of $t_2$ generates $(b, 1)$, where 1 is the token change at place $p_2$
- Firing of $t_3$ generates $(b, -1)$
- Firing of $t_4$ does not generate any label or visible token change
- Firing of $t_5$ generates $(\varepsilon, -1)$

- Equivalent labeled Petri net
- The observation

$$0 \xrightarrow{b} 1 \xrightarrow{} 0$$

gets translated into $b_1\varepsilon_1$
Problem Formulation and Basic Idea

Problem

- Given $Q = (G, \Sigma, L, P_s)$ and $M_{P_s}^0 \xrightarrow{d_1} M_{P_s}^1 \xrightarrow{d_2} \cdots M_{P_s}^{k-1} \xrightarrow{d_k} M_{P_s}^k$, construct $(G, \Sigma', L')$ and translate the sequence to $\omega \in \Sigma'^*$ of length $k$ such that the set of states consistent with $Q$ and the observation sequence is the same as the set of states consistent with $(G, \Sigma', L')$ and $\omega$

Basic Idea

- Use token changes of places with sensors to refine transition labels
- An observation unit $x \xrightarrow{e} y$ is translated to a label in $\Sigma'$ based on $e$ and $y - x$
Example: Communication Protocol

- Petri net model is adapted from (Giua, 2005) by adding $t_8$ and related arcs (so that the system is deadlock-free)

- $t_6$ is a fault transition of type $F$; place $p_4$ has a sensor and all other places do not

- Equivalent labeled Petri net model

- $t_4$ becomes observable with label $\varepsilon_1$ but $t_6$ is still unobservable
Assume $wt(M, t) = 1$, $\forall M \in R(G, M_0)$, $\forall t \in T_M$.

Assume the observation is $0 \xrightarrow{a} 0 \rightarrow 1 \rightarrow 2$, which is translated to $\omega = a_1 \epsilon_1 \epsilon_1$.

After observing $a_1$, there is one consistent marking $N_1$ and $K = (0 1 1)$; thus, $b(a_1, F) = 0$.

After observing $\epsilon_1$, the belief $b(a_1 \epsilon_1, F) = 0.4$.

After observing another $\epsilon_1$, the belief $b(a_1 \epsilon_1 \epsilon_1, F) = 1$. 
Conclusions

Fault Diagnosis in DES modeled by Petri nets with outputs

- Beliefs regarding fault types are introduced to enhance diagnosis results and are calculated recursively using online monitor
- Transformation scheme to handle information from place sensors

Future Directions

- Notion of diagnosability for infinite state systems
- Ways to determine the diagnosability of (certain classes of) Petri nets with unobservable transitions
References

