Robust diagnosability of discrete event systems subject to intermittent sensor failures

Lilian Kawakami Carvalho ∗ Jo˜ao Carlos Basilio ∗
Marcos Vicente Moreira ∗

∗ Federal University of Rio de Janeiro
COPPE - Electrical Engineering Program
21949-900, Rio de Janeiro, R.J., Brasil
(e-mails: lilian@coep.ufrj.br, basilio@dee.ufrj.br, moreira@dee.ufrj.br).

Abstract: The modeling of physical systems using discrete event models assumes that a set of sensors always report the event occurrences correctly. However, bad sensor operation can result in loss of observability of the events associated with the malfunctioning sensors. If one or more sensors fail, it may be possible that either the diagnoser stands still or provide wrong information on the fault occurrence. This paper assumes that intermittent sensor failures may occur and deals with the problem of fault diagnosis in the presence of intermittent sensor failures. To this end, an automaton model for intermittent sensor failures based on a newly proposed language operation (language dilation) is presented in the paper. Necessary and sufficient conditions for robust diagnosability against intermittent sensor failure are also given in the paper. The development of a robust diagnoser that copes with intermittent sensor failures is another contribution of the paper.

Keywords: Discrete event systems, fault diagnosis, intermittent sensor failures, robust diagnosability.

1. INTRODUCTION

Fault diagnosis in discrete event systems (DES) has attracted a lot of attention in the last years (Sampath et al., 1995; Debouk et al., 2000; Boel and van Schuppen, 2002; Tripakis, 2002; Zad et al., 2003; Thorsley and Teneketzis, 2005; Contant et al., 2006; Qiu and Kumar, 2006; Wang et al., 2007; Kumar and Takai, 2009; Athanasopoulou et al., 2010; Moreira et al., 2010). The main objective of a fault diagnosis system is to infer and inform fault occurrences by considering only observed events. This is carried out in practice using a deterministic automaton called a diagnoser.

The modeling of physical systems using discrete event models assumes that a set of sensors always reports the event occurrences correctly. However, bad sensor operation that results from of bad electrical linkage, defective components, circuit heating, measurement noise, etc, may lead to loss of observability of the events associated with the malfunctioning sensors. When sensor failures occur, the diagnoser could get stuck in some states due either to the lack of observed events or to the occurrence of an event that is not in the active event set, issuing therefore incorrect diagnostic decisions.

Recently the problem of “robust” diagnosis has started to gain attention. Basilio and Lafortune (2009) approached the robust codiagnosability problem, i.e., when entire diagnosers may fail and cease to operate. Athanasopoulou et al. (2010) develops a probabilistic methodology for failure diagnosis in finite state machines based on a sequence of unreliable observations. In the context of supervisory control of DES, sensor failures have been considered by Rohloff (2005) and Sanchez and Montoya (2006), where permanent sensor failure is assumed, i.e., once a sensor fails, it never recovers again.

In this paper we address the problem of fault diagnosis of discrete event systems modeled as automata assuming intermittent sensor failures. This is a more general formulation since it includes permanent failures; the latter can be seen as forever lasting intermittent failures. In order to achieve this objective we first derive a model for a given automaton that accounts for intermittent sensor failures. In the sequel we obtain a diagnoser based on this model that can be used either in the verification of robust diagnosability or in run-time to perform the fault diagnosis. We also present necessary and sufficient conditions for diagnosability based on an “indeterminate cycle” test for the property of diagnosability (Sampath et al., 1995).

This paper is structured as follows. In Section 2 we present a background material in discrete event systems that is necessary in the sections that to follow, and in Section 3 we present an example to highlight the need for robust diagnosers. In Section 4 we approach the problem of modeling discrete event systems in order to take intermittent sensor failures into account. In Section 5 we present the definition of robust diagnosability. In Section 6 we show how to build a robust diagnoser starting from the automaton model of the plant and we also present necessary and sufficient conditions for robust diagnosability. Finally, in Section 7 we list the main contributions of the paper.

2. PRELIMINARIES

Let

\[ G = (X, \Sigma, f, \Gamma, x_0) \]

\[ G = (X, \Sigma, f, \Gamma, x_0) \]

denote a deterministic automaton, where \( X \) is the set of states, \( \Sigma \) is the finite set of events, \( f : X \times \Sigma \to X \) is the transition function, partially defined in its domain, \( \Gamma : X \to 2^\Sigma \) is the active event function, and \( x_0 \) is the initial state. Let us partition \( \Sigma \) as \( \Sigma = \Sigma_o \cup \Sigma_{uo} \), where \( \Sigma_o \) and \( \Sigma_{uo} \) denote, respectively, the sets of observable and unobservable events.
Deterministic automata are not able to represent transitions labeled with the same event starting in a state but ending at two different states, and also ε-transitions (transitions associated with the empty trace $\epsilon$). In order to overcome these limitations, nondeterministic automata are deployed, being defined as:

$$G_{nd} = (X, \Sigma \cup \{\epsilon\}, f_{nd}, \Gamma_{nd}, x_0),$$

where $f_{nd} : X \times (\Sigma \cup \{\epsilon\}) \rightarrow 2^X$, and the initial state may itself be a set of states, that is, $x_0 \subseteq X$. The nondeterministic automaton behavior can be represented by an equivalent (in terms of language equivalence) deterministic automaton called an observer, which is denoted as:

$$Obs(G_{nd}, \Sigma) = (X_{obs}, \Sigma, f_{obs}, \Gamma_{obs}, x_{0,obs}).$$

where $Obs(G_{nd}, \Sigma)$ is taken with respect to $\Sigma$. The steps of the algorithm to construct the observer is presented in Cassandras and Lafortune (2007). It is important to remark that $L(Obs(G_{nd}, \Sigma)) = L(G_{nd})$.

Let $G_1 = (X_1, \Sigma_1, f_1, \Gamma_1, x_{0,1})$ and $G_2 = (X_2, \Sigma_2, f_2, \Gamma_2, x_{0,2})$ denote any two automata. The synchronous (or parallel) composition of $G_1$ and $G_2$, denoted by $G_1 \parallel G_2$, is defined as:

$$G_1 \parallel G_2 = Ac(\{X_1 \times X_2, \Sigma_1 \cup \Sigma_2, f_1[2], \Gamma_1[2], (x_{0,1}, x_{0,2})\}),$$

where $\times$ denotes the cartesian product and Ac denotes the accessible part of $G_1 \parallel G_2$. The transition function of $G_1 \parallel G_2$ is defined as:

$$f_{1[2]}((x_1, x_2), \sigma) = \begin{cases} (f_1(x_1, \sigma), f_2(x_2, \sigma)), & \text{if } \sigma \in \Gamma_1(x_1) \cap \Gamma_2(x_2), \\ (f_1(x_1, \sigma), x_2), & \text{if } \sigma \in \Gamma_1(x_1) \setminus \Sigma_2, \\ (x_1, f_2(x_2, \sigma)), & \text{if } \sigma \in \Gamma_2(x_2) \setminus \Sigma_1, \\ \text{undefined, otherwise.} \end{cases}$$

The fault diagnosis problem of discrete event systems consists in identifying the occurrence of a fault event in a system by observing only events in $\Sigma$. Let $\Sigma_f \subseteq \Sigma_{obs}$ denote the set of fault events, and assume, for the sake of simplicity, that there is only one fault event, i.e., $\Sigma_f = \{\sigma_f\}$. The following assumptions are also made:

A1. The language generated by $G$, $L$, is live, i.e., $\Gamma(x_t) \neq \emptyset$ for all $x_t \in X$;

A2. Automaton $G$ has no cycle of unobservable events, i.e., $\forall s \in L \times \Sigma_{obs}, \exists n_0 \in \mathbb{N}$ such that $\|s\| \leq n_0$, where $\|s\|$ denotes the length of trace $s$.

The notations used throughout the paper are as follows:

(i) $s_f$: the last event of $s$;

(ii) $\Psi(\Sigma_f) = \{s \in L : s_f \in \Sigma_f\}$: set of all traces of $L$ that end with the fault event $\sigma_f$;

(iii) $L/s = \{t \in \Sigma^* : st \in L\}$: post-language of $L$ after $s$;

(iv) $P_s : \Sigma^* \rightarrow \Sigma^*$: language projection operation (Ramadge and Wonham, 1989), where $\Sigma^*$ denotes the Kleene closure of $\Sigma$;

(v) $P_{s^{-1}} : \Sigma^* \rightarrow 2^\Sigma^*$: inverse projection;

(vi) for a trace $s \in L$, then $\tau$ denotes the prefix-closure of $s$; thus the membership relation $\Sigma_f \in s$ can be used to denote that $\tau \cap \Psi(\Sigma_f) \neq \emptyset$;

(vii) $L_G(x)$: set of all traces that originate in state $x \in X$.

The diagnosability of a language is defined as follows (SamPATH et al., 1995).

---

**Fig. 1.** Label automaton $A_f$.

**Definition 1.** A prefix-closed and live language $L$ is diagnosable with respect to projection $P_s$ and $\Sigma_f = \{\sigma_f\}$ if the following holds true:

$$(\exists n \in \mathbb{N})(\forall s \in \Psi(\Sigma_f))(\forall t \in L/(s))(\|t\| \geq n \Rightarrow D),$$

where the diagnosability condition is

$$(\forall o \in P_s^{-1}(P_s(xt))) \cap L(\Sigma_f) \in o.$$  

One way to verify the diagnosability of a DES is by using a deterministic automaton called a diagnoser (SamPATH et al., 1995). The diagnoser for $G$, hereafter denoted as $G_d$, is defined as:

$$G_d = (X_d, \Sigma, f_d, \Gamma_d, x_{0,d}),$$

and can be obtained from $Obs(G/A_f, \Sigma)$, where $A_f$ is the two-state label automaton depicted in Figure 1. The diagnoser states are classified according to the presence of $Y$ and $L$ labels (SamPATH et al., 1995). A state $x_d \in X_d$ is called certain (or faulty), if $\ell = Y$ for all $(x, \ell) \in x_d$, and normal (or non-faulty) if $\ell = N$ for all $(x, \ell) \in x_d$. If there exist $(x, \ell), (y, \ell) \in x_d$, $x$ not necessarily distinct from $y$ such that $\ell = Y$ and $\ell = N$, then $x_d$ is called an uncertain state of $G_d$ (SamPATH et al., 1995).

A set of states $\{x_1, x_2, \ldots, x_n\} \subseteq X$ forms a cycle in $G$ if there exists a trace $s = \sigma_1 \sigma_2 \ldots \sigma_k \in L(G, x_1)$ such that $f(x_1, \sigma_1) = x_{i+1}$, $l = 1, \ldots, n - 1$, and $f(x_n, \sigma_n) = x_1$. A set of uncertain states $\{x_{d_1}, x_{d_2}, \ldots, x_{d_p}\} \subseteq X_d$ forms an indeterminate cycle if the following conditions hold true:

C1. $x_{d_1}, x_{d_2}, \ldots, x_{d_p}$ form a cycle in $G_d$;

C2. $(\exists x_i^{b_1}, y_i, x_i^{b_2} \in X_{d_i}, x_i^{b_1} \cdot x_i^{b_2}$ not necessarily distinct from $x_i^{b_1}, l = 1, \ldots, m_i, k_i = 1, \ldots, m_i$, and $r_i = 1, \ldots, m_i$ in such a way that the sequence of states $\{x_i^{b_1}\}, l = 1, \ldots, 0, k_i = 1, \ldots, m_i$ and $\{x_i^{b_2}\}, l = 1, \ldots, 0, r_i = 1, \ldots, m_i$ form cycles in $G$.

Language diagnosability can be stated in terms of the existence of indeterminate cycles in diagnosers, as follows (SamPATH et al., 1995).

**Theorem 1.** The language $L$ generated by automaton $G$ is diagnosable with respect to projection $P_s$ and $\Sigma_f = \{\sigma_f\}$ if, and only if, its diagnoser $G_d$ has no indeterminate cycles.

---

## 3. A MOTIVATING EXAMPLE

Figure 2(a) shows the state transition diagram of an automaton $G$, for which $\Sigma = \{a, b, c, d, e, \sigma_f\}, \Sigma_s = \{a, b, c, d, e\}$, and $\Sigma_f = \{\sigma_f\}$. The corresponding diagnoser $G_d$ is depicted in Figure 2(b). According to Theorem 1, since $G_d$ has no indeterminate cycles, the language generated by $G$ is diagnosable with respect to $P_s$ and $\Sigma_f$.

Assume that trace $s' = c\sigma_1\sigma_2\sigma_3$ $(n \in \mathbb{N})$ has been generated and let us suppose that, due to a sensor malfunction, the occurrence of event $c$ has not been recorded. Since event $c$ has become unobservable, the first event occurrence to be recognized by $G_d$ is $a$, which takes the diagnoser state to $\{5N\}$. The next event of $s'$ is not in the active event set of $\{5N\}$;
thus the diagnoster stands still in a normal state, giving wrong information regarding the fault occurrence. Assume, now, that trace $s^n = c\sigma_fh^n$ ($n \in \mathbb{N}$) has been generated and assume also that event $c$ has become unobservable due to a sensor failure. In this case, $b$ is the first event to be recognized by $G_d$, and since it does not belong to the active event set of $\{1N\}$, $G_d$ remains in the initial state. The next event occurrences $d^n$ also do not belong to the active event set of $\{1N\}$, and thus, the diagnoster stands still in a normal state, and, once again, the diagnoster provides a wrong indication regarding the fault occurrence.

The anomalous behavior of the diagnoster in the example above suggests that diagnosters should be modified in order to account for possible sensor failures.

4. MODELING OF THE OBSERVED BEHAVIOR OF AN AUTOMATON SUBJECT TO INTERMITTENT SENSOR FAILURES

A more general approach to the problem of fault diagnosis in the presence of sensor failure is when intermittent sensor failures are assumed. Such an assumption has the advantage of accounting for both, intermittent and permanent sensor failures, since the latter can be viewed as a forever lasting intermittent failure.

Consider, again, the example presented in section 3. Assuming intermittent sensor failure, the diagnosability problems that result from the failure of the sensor that records event $c$ can be explained as follows. Let us partition $\Sigma_o$ as $\Sigma_o = \Sigma_{sf}\cup\Sigma_{afs}$, where $\Sigma_{sf}$ is the subset of $\Sigma_o$ whose events are associated with intermittent sensor failures and $\Sigma_{afs}$ is the set of events whose sensors are not subject to malfunctioning. Assuming, initially, that $\Sigma_{sf} = \emptyset$, then $L(G) = L(G_o)$ where $L_G = \{a\} \{b\} \{d\}^{*} \cup \{c\} \{a\} \{e\}^{*}$ and the observed language is $P_o[L(G)]$. On the other hand, when $\Sigma_{sf} = \{c\}$, then although the language generated by $G$ remains the same, the observed language is no longer $P_o[L(G)]$, but $P_o[L_{sf}]$, where $L_{sf} = L(G) \cup L_{\alpha}$, with $L_{\alpha} = \{\sigma_f\} \{b\} \{d\}^{*} \cup \{a\} \{e\}^{*}$. The state transition diagram of an automaton that generates $L_{sf}$ is shown in Figure 3.

Based on the explanation above, it is clear that language diagnosability in the presence of intermittent sensor failures should be stated in terms of $L_{sf}$, and therefore, it is necessary to obtain an automaton $G_{sf}$ whose generated language models not only the normal behavior of $G$, i.e., when no sensor failures take place, but also the influence of intermittent sensor failures on $L$. In order to do so, consider the following language operation.

**Definition 2. (Dilation)** Let $\Sigma = \Sigma_{sf}\cup\Sigma_{afs}\cup\Sigma_o$ be a partition of $\Sigma$, where $\Sigma_{sf}$ is the set of events associated with intermittent sensor failures and $\Sigma_{afs}$ denotes the set of observable events associated with sensors that have no failures during the course of work. The dilation $D_{sf}$ is the mapping

$$D_{sf} : \Sigma^{*} \rightarrow 2^{\Sigma^{*}}$$

where

$$D_{sf}(\varepsilon) = \{\varepsilon\},$$

$$D_{sf}(\sigma) = \begin{cases} \{\sigma\}, & \text{if } \sigma \in \Sigma_{sf}, \\ \{\sigma, \varepsilon\}, & \text{if } \sigma \in \Sigma_{afs}, \end{cases}$$

$$D_{sf}(\sigma) = D_{sf}(s)D_{sf}(\sigma), s \in \Sigma, \sigma \in \Sigma.$$

The dilation operation $D_{sf}$ can be extended to languages by applying it to all sequences in the language, that is,

$$D_{sf}(L) = \bigcup_{s \in L} D_{sf}(s).$$

Dilation and projection are language operations that can be interchanged, as shown in the following result.

**Lemma 1.**

A. For any event $\sigma \in \Sigma$, $D_{sf}P_o(\sigma) = P_o[D_{sf}(\sigma)]$.

B. For any language $L$, defined in $\Sigma^{*}$, $D_{sf}P_o(L) = P_o[D_{sf}(L)]$.

**Proof:** The proof for A follows directly from the definitions of dilation and projection, and will therefore be omitted.

The proof for B is by induction on the length of the traces in the two languages.

- The base case is for traces of length 0. For $s = \varepsilon$, we have that, by definition, $D_{sf}(P_o(\varepsilon)) = \varepsilon$ and $P_o[D_{sf}(\varepsilon)] = \varepsilon$.

- The induction hypothesis is that for all traces $s_n \in L$, $|s_n| \leq N$, $D_{sf}(P_o(s_n)) = P_o[D_{sf}(s_n)]$.

- Let us now consider a trace $s_{n+1} = s_n\sigma$, where $\sigma \in \Sigma$. Then
\[ D_{isf}[P_o(s_{N+1})] = D_{isf}[P_o(s_{N} \sigma)] = D_{isf}[P_o(s_{N})P_o(\sigma)] = D_{isf}[P_o(s_{N})]. \]

Let us now build an automaton \( G_{isf} \) from \( G \) as follows.

**Algorithm 1.** Given an automaton \( G = (X, \Sigma, f, \Gamma, x_0) \), perform the following changes:

**Step 1.** To each transition of \( G \) labeled with an event in \( \Sigma_{isf} \), add an \( \varepsilon \)-transition in parallel. This results in the following augmented automaton:

\[ G_A = (X_A, \Sigma_A, f_A, \Gamma_A, x_{0_A}), \]

where \( X_A = X, \Sigma_A = \Sigma \cup \{ \varepsilon \}, x_{0_A} = x_0 \), and \( \Gamma_A(x) = \{ \Gamma(x) \cup \{ \varepsilon \}, \) if \( \Gamma(x) \cap \Sigma_{isf} \neq \emptyset, \)

\[ f_A(x, \sigma) = f(x, \sigma), \]

for all \( \sigma \in \Gamma(x) \) and \( f_A(x, \varepsilon) = f(x, \sigma), \)

for all \( \sigma \in \Gamma(x) \cap \Sigma_{isf}. \)

**Step 2.** Obtain the deterministic automaton \( G_{isf} = \text{Obs}(G_A, \Sigma). \)

The following result shows that \( G_{isf} \) models the observed behavior of \( G \) when subject to intermittent sensor failures.

**Theorem 2.** Let \( G_{isf} \) be a deterministic automaton obtained from \( G \) in accordance with algorithm 1. Then, \( L_{isf} = L(G_{isf}) \) and \( L(G_{isf}) = L_{isf}. \)

**Proof:** The first equality is proved by induction on the length of the traces of \( L \) that originate in \( L_{isf} \) and \( D_{isf}(L). \)

- The base case is for traces of length 0. Note that \( x \in L \) and, by construction, \( \varepsilon \in L_{isf} \). By Definition 2, \( \{ x \} = D_{isf}(x). \)
- The induction hypothesis is that for all traces \( s \in L, \|s\| \leq n, \) there exists a set \( S_{isf} \) formed from \( s \), such that \( S_{isf} \subseteq L_{isf} \) and \( S_{isf} = D_{isf}(s). \)
- We now prove the same for traces \( s \in L, \|s\| = n. \) Note that if \( \sigma \in \Sigma_{isf} \), then \( S_{isf}(\sigma) \subseteq S_{isf} \cap L_{isf} \) and \( S_{isf}(\sigma) \cup S_{isf} = S_{isf}(\sigma, s) \) for all \( \sigma \in \Sigma_{isf}. \) On the other hand, if \( \sigma \notin \Sigma_{isf} \), then \( S_{isf}(\sigma) \subseteq L_{isf} \) and \( S_{isf}(\sigma) = D_{isf}(\sigma). \)

Therefore, \( L_{isf} = \bigcup_{s \in D_{isf}(L)}(s) = D_{isf}(L) \), according to Equation (4).

To prove the second equality, note that the language generated by a nondeterministic automaton with \( \varepsilon \)-transitions is equal to the language generated by its observer. Since \( G_{isf} = \text{Obs}(G_A, \Sigma), L(G_A) = L(G_{isf}) \). In addition, by construction of \( G_A, \) it is easy to see that \( L(G_A) = D_{isf}(L) \). Thus, \( L(G_{isf}) = D_{isf}(L) = L_{isf}. \)

5. ROBUST DIAGNOSABILITY OF DES SUBJECT TO INTERMITTENT SENSOR FAILURES

As we saw in the previous section, although the language generated by an automaton subject to intermittent sensor failures remains unchanged, the observed language dilates. The definition of language diagnosability (Sampath et al., 1995) is expressed in terms of the observed language and thus in order to accommodate intermittent sensor failures, the diagnosability definition must be changed. First, the following assumption is necessary.

A3. Automaton \( G_{isf} \) has no cycle of unobservable events.

This assumption extends Assumption A2 to \( G_{isf} \) in order to avoid cycles of unobservable events due to intermittent sensor failures.

The diagnosability of DES subject to intermittent sensor failures is defined as follows.

**Definition 3.** (Robust diagnosability of DES subject to intermittent sensor failures) A prefix-closed and live language \( L \) generated by an automaton \( G \) is robustly diagnosable with respect to dilation \( D_{isf} \), projection \( P_o \) and \( \Sigma_f = \{ \sigma_f \} \) if the following holds true:

\[ (\exists n \in \mathbb{N}) (\forall s \in \Psi(\Sigma_f))(\forall t \in L/x)(\|t\| \geq n \Rightarrow R_D), \]

where the robust diagnosability condition \( R_D \) is

\[ (\forall o \in P_o^{-1}(P_o(D_{isf}(st))) \cap L_{isf} \})) \in \Sigma_f \in o. \]

**Remark 1.** Note that if \( \Sigma_f = \emptyset \) then \( L_{isf} = L \) and \( D_{isf}(st) = st. \) In this case, Definition 3 reduces to the usual definition of language diagnosability introduced by Sampath et al. (1995).

The following example illustrates the verification of robust diagnosability according to Definition 3.

**Example 1.** Consider automata \( G_1 \) and \( G_2 \) whose state transition diagrams are depicted in Figures 4(a) and 5(a), respectively, and assume, for both automata, that \( \Sigma_f = \{ a, b, c \}, \Sigma_f = \{ b \} \) and \( \Sigma_f = \{ \sigma_f \}. \)

The objective here is to verify if the language generated by \( G_1 \) and \( G_2 \) (\( L_1 \) and \( L_2 \), respectively) are robustly diagnosable with respect to \( D_{isf} \), \( P_o \) and \( \Sigma_f = \{ \sigma_f \}. \)

Consider, initially, automaton \( G_1. \) From Figure 4(a), we see that the faulty trace of \( L_1 \) is given by \( s' = a \sigma_f c^n, n \in \mathbb{N}. \) Following the steps in the robust diagnosability condition \( R_D \), we have:

\[ D_{isf}(s') = \{ a \sigma_f c^n \} \Rightarrow P_o \left[ D_{isf}(s') \right] = \{ ac^n \}. \]

Let \( L_{isf} \) denote the language generated by automaton \( G_{isf}, \) shown in Figure 4(b). It is not difficult to see that:

\[ P_o^{-1}(P_o \left[ D_{isf}(s') \right]) \cap L_{isf} = \{ a \sigma_f c^n \}. \]

Therefore, since \( P_o^{-1}(P_o \left[ D_{isf}(s') \right]) \cap L_{isf} \) has only a fault trace, we may conclude that \( L_1 \) is robustly diagnosable with respect to \( D_{isf}, P_o \) and \( \Sigma_f = \{ \sigma_f \}. \)

Consider, now, automaton \( G_2. \) In this case, the unique faulty trace of \( L_2 \) is \( s'' = \sigma_f abc^n, n \in \mathbb{N}. \) Proceeding according to the robust diagnosability condition \( R_D \), we have:

\[ D_{isf}(s'') = \{ \sigma_f abc^n, \sigma_f ac^n \} \Rightarrow P_o \left[ D_{isf}(s'') \right] = \{ abc^n, ac^n \}. \]
From automaton $G_{2ad}$, shown in Figure 5(b), we can obtain $L_{2ad}$, and therefore:

$$P_n^{-1} \{ p_o \mid D_{isf}(x^n) \} \cap L_{2ad} = \{ \sigma_f ab^n, \sigma_f a^{2n}, a^{3n} \}.$$  

Since there is a normal trace in $P_n^{-1} \{ p_o \mid D_{isf}(x^n) \} \cap L_{2ad}$, we may conclude that $L_2$ is not robustly diagnosable with respect to $D_{isf}$, $P_o$ and $\Sigma_f = \{ \sigma_f \}$.

6. A ROBUST DIAGNOSER FOR DES SUBJECT TO INTERMITTENT SENSOR FAILURES

Apart from the replacement of $L$ with $L_{2ad} = D_{isf}(L)$ and $\sigma$ with $D_{isf}(\sigma)$, Definitions 1 and 3 are the same. This suggests that the diagnosability condition $R_2$ can be expressed in terms of indeterminate cycles in a diagnoser $G_{isf,d}$ associated with $G_{isf}$, as in Theorem 1.

It is not difficult to see that, starting from $G$, two diagnoser candidates to account for intermittent sensor failures can be obtained:

(i) $G'_{isf, d} = \text{Obs} (G_{isf} \mid A_i, \Sigma_o)$;
(ii) $G''_{isf, d} = \text{Obs} (G_A \mid A_i, \Sigma_o)$,

where $A_i$ is the label automaton shown in Figure 1. Since, according to Algorithm 1, $G_{isf} = \text{Obs} (G_A, \Sigma)$, we may state the following result.

Theorem 3. Let $X_{isf, d}$ and $X''_{isf, d}$ denote the state spaces of $G'_{isf, d}$ and $G''_{isf, d}$, respectively. Then $G'_{isf, d}$ and $G''_{isf, d}$ are equal up to the following renaming of states:

$$x'_{isf, d} = \{ x_{isf, \ell_1, x_{isf, \ell_2, \ldots, x_{isf, \ell_p}} } \} \in X'_{isf, d} \Leftrightarrow$$

$$x''_{isf, d} = \{ x_{i, x_{i1, x_{i2, \ldots, x_{i, \ell_q, \ell_p}} } } \} \in X''_{isf, d},$$

where $x_{isf} \in X$, $x_{isf} \in 2^X$, $|x_{isf}| = q_i$, $i = 1, 2, \ldots, p$, $x_{isf} = \{ x_{i1, x_{i2, \ldots, x_{i, \ell_q, \ell_p}} } \}$, and $\ell_i \in \{ Y, N \}$.

Proof: The proof of this theorem follows similar steps as the proof of Theorem 2 of Basilio and Lafonture (2009) and, therefore, be omitted. ■

Example 2. Consider again automaton $G$ of Figure 2. Let $\Sigma_o = \{ a, b, c, d, e \}$, and assume that the sensor that records event $c$ fails intermittently, i.e., $\Sigma_{isf} = \{ c \}$. The two diagnosers $G'_{isf, d}$ and $G''_{isf, d}$ are shown in Figures 6(a) and (b), where it can be seen that the relationships presented in Theorem 3 hold true. □

Although the computation of $G'_{isf, d}$ is performed in a more natural way, i.e., first a model for $G$ that takes into account intermittent sensor failure is derived and, in the sequel, a diagnoser for this model is obtained, the representation of the states of $G''_{isf, d}$ is more convenient for robust diagnosability analysis, since its state components have the same structure as those of Sampath et al. (1995); therefore, avoiding the need for different definitions of certain, uncertain and normal states and indeterminate cycles. As a consequence, the state representation of $G''_{isf, d}$ will be adopted throughout the paper, in spite of the way $G_{isf, d}$ has been computed. We state the following result.

Theorem 4. The language $L$ is robustly diagnosable with respect to $D_{isf}$, $p_o$ and $\Sigma_f$ if, and only if, the robust diagnoser $G_{isf, d}$ has no indeterminate cycles.

Proof: According to Theorem 2, $L_{isf} = D_{isf}(L)$. Thus, the robust diagnosability of $L$ with respect to $D_{isf}$, $P_o$ and $\Sigma_f$ is equivalent to the diagnosability of $L_{isf} = D_{isf}(L)$ with respect to $P_o$ and $\Sigma_f$. The result then follows from Theorem 1 by replacing $L$ with $L_{isf}$.

Remark 2. The robust diagnoser proposed in this paper, not only provides an off-line test for robust diagnosability but also can be used at run-time to perform diagnosis of a DES subject to intermittent sensor failure. This is illustrated in the example that follows.

Example 3. Under the same assumptions as in Example 2, the verification of the robust diagnosability of $L$ with respect to $D_{isf}$, $P_o$ and $\Sigma_f$ is carried out by using the robust diagnoser $G_{isf, d} = G''_{isf, d}$ shown in Figure 6(b). We may then conclude
that, since $G_{isf,d}$ has no indeterminate cycles, $L$ is robustly diagnosable.

Let us now consider the effect of intermittent failure of the sensor associated with event $c$ in online fault detection. We will consider here the same faulty traces used in the motivating example of Section 3.

Consider, initially, the occurrence of the faulty trace $s' = cG_{ate}a^n$. Note that, if the sensor associated with event $c$ fails, then the first event occurrence recognized by $G_{isf,d}$ is $a$, which takes the robust diagnoser to state $\{5N, 7\}$\}. When the next event ($e$) occurs, the robust diagnoser updates its state to $\{7\}$, being, therefore, sure of the fault occurrence. On the other hand, if the sensor associated with event $c$ does not fail, then $c$ is the first event occurrence recognized by $G_{isf,d}$, which takes its state to $\{2N, 3\}'$. When the next observable events in trace $s'$ occurs, the robust diagnoser moves to state $\{7\}$ and remains there; therefore indicating the occurrence of $G_{c}$.

Consider, now, the occurrence of the faulty trace $s'' = cG_{bde}a^n$. When the sensor associated with event $c$ fails, the robust diagnoser of Figure 6 goes to state $\{4\}'$ and remains there; therefore, indicating the fault occurrence. When the sensor associated with event $c$ does not fail, the diagnoser moves first to state $\{2N, 3\}'$ and then goes to state $\{4\}'$, where it remains; again indicating the fault occurrence.

It is important to stress that the robust diagnoser not only succeeded in detecting the fault occurrence in the presence of sensor failures but also has, as part of the state components, indications of the states where $G$ is likely to be after the events in the traces that have occurred, even when a sensor failure takes place.

7. CONCLUSIONS

We have addressed in this paper the problem of fault diagnosis of discrete event systems modeled by automata when subject to intermittent sensor failures. We have introduced a new language operation (dilation) which has allowed us to derive an automaton model that accounts for both, normal behavior (with no intermittent sensor failures) and subject to sensor failures. We have also presented a definition of robust diagnosability and derived a necessary and sufficient condition for robust diagnosability against intermittent sensor failures.

ACKNOWLEDGEMENTS

The authors wish to thank the Brazilian Research Council (CNPq) and the Carlos Chagas Foundation (FAPERJ) for financial support.

REFERENCES


