Automatica 79 (2017) 315–325

Contents lists available at ScienceDirect

Automatica

journal homepage: www.elsevier.com/locate/automatica

Diagnosability of intermittent sensor faults in discrete event systems[☆]

Lilian K. Carvalho, Marcos V. Moreira, João Carlos Basilio

Programa de Engenharia Elétrica, Universidade Federal do Rio de Janeiro, Rio de Janeiro, R.J., Brazil

ARTICLE INFO

Article history:
Received 26 April 2015
Received in revised form
16 May 2016
Accepted 10 December 2016

Keywords:
Discrete event system
Automata
Fault diagnosis

ABSTRACT

We address, in this paper, the problem of diagnosing intermittent sensor faults. In order to do so, we employ a model of intermittent loss of observations recently proposed in the literature, and use this model, together with an appropriately modified label automaton, to change the problem of detecting intermittent sensor faults into a problem of diagnosing the language generated by an automaton in the presence of intermittent faults, where the fault event is the unobservable event that models the non-observation of the event whose occurrence is recorded by the sensor subject to intermittent fault. We present necessary and sufficient conditions for diagnosability of intermittent sensor faults and propose two tests to verify intermittent sensor fault diagnosability: the first one based on diagnosers, which can also be used for online diagnosis, and a second one, based on verifiers, which has the advantage of having polynomial time complexity.

1. Introduction

Sensors play a crucial role in the reliability and safety of feedback controlled systems, and their faults have been reported as the cause of several accidents that led to either material or life losses (da Silva, Saxena, Balaban, & Goebel, 2012). It is, therefore, important to find the means to distinguish between sensor malfunction and ordinary (normal) behavior. It is particularly important to check, in practice, if intermittent sensor faults are actually happening with a view to identifying and replacing those sensors that fail frequently (permanently or intermittently) without apparent external causes, and to find out the external causes of the sensor fault (*e.g.*, environmental causes, such as high and low temperatures, pressure, magnetic interference, radiation, *etc.*).

There are basically three main approaches to the problem of detecting incorrect sensor readings (Frank, 1990): (i) simple hardware redundancy with majority voting, (ii) model-based, and (iii) knowledge-based. Hardware redundancy with majority voting is the simplest way to improve sensor reliability; model-based design relies on some model developed for the system under consideration, and the decision regarding the sensor fault occurrence is made based on comparisons between the outputs of the model and of the real system; knowledge-based design employs artificial intelligence techniques such as neural networks and fuzzy logic to develop expert systems. Among the model-based approach, the most relevant works reported in the literature are the incipient work by Clark (1978), who proposed the so-called dedicated observer scheme (DOS), the paper by Frank (1990), which besides presenting a literature survey, also improved the scheme developed by Clark (1978), leading to the so-called generalized observer scheme (GOS), Lunze and Schröder (2004), who proposed a method for the detection and identification of sensor and actuator faults, using discrete event theory, by modeling the plant of the system under consideration as a stochastic automaton, and Ding, Fennel, and Ding (2004), who presented a model-based sensor monitoring scheme for the electronic stability program (ESP) system consisting of an anti-lock break system, a traction control and a yaw torque control. Expert systems were proposed by Athanasopoulou and Chatziathanasiou (2009), who developed an intelligent system for identification and replacement of faulty sensor measurements in thermal power plants, and da Silva et al. (2012), who presented a system for sensor fault diagnosis using neural network approach.

We propose, in this paper, a discrete event approach to the problem of diagnosing intermittent sensor faults by modeling the dynamic system as a deterministic automaton. We assume that the sensor fault diagnosis system is built separately from both the ordinary failure diagnosis and the supervisory control systems, as shown in Fig. 1, and that both the supervisory control and the diagnosis systems can cope with intermittent sensor faults

[☆] The material in this paper was partially presented at the 2013 American Control Conference, June 17–19, 2013, Washington, DC, USA. This paper was recommended for publication in revised form by Associate Editor Jan Komenda under the direction of Editor Christos G. Cassandras.

E-mail addresses: lilian@dee.ufrj.br (L.K. Carvalho), moreira@dee.ufrj.br (M.V. Moreira), basilio@dee.ufrj.br (J.C. Basilio).

http://dx.doi.org/10.1016/j.automatica.2017.01.017
0005-1098/© 2017 Elsevier Ltd. All rights reserved.

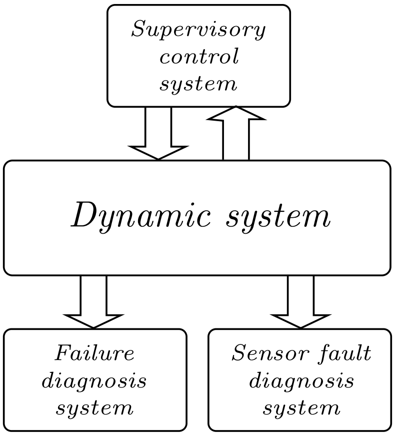


Fig. 1. Schematic diagram showing the supervisory control, the failure diagnosis system, and the fault diagnosis systems.

(Alves, Basilio, da Cunha, Carvalho, & Moreira, 2014; Carvalho, Basilio, & Moreira, 2012). In the proposed structure, the supervisory control and diagnosis systems, being tolerant to intermittent sensor faults, allow the system to continue working properly when such faults occur, whereas the sensor fault diagnosis system detects the occurrence of sensor faults. We employ the model for intermittent loss of observations recently proposed by Carvalho et al. (2012), and convert the problem of detecting intermittent sensor faults into a problem of diagnosing intermittent failure. In this regard, we present necessary and sufficient conditions for intermittent sensor fault diagnosability and propose two tests to verify intermittent sensor fault diagnosability: the first one is based on diagnosers, which can also be used for online diagnosis, and the second one which is based on verifiers has the advantage of having polynomial time complexity. It is worth remarking that, for the sensor fault diagnosis system, any failure event that may appear in the model will be treated as an ordinary unobservable event.

The problem considered in this paper has several differences from that solved by Contant, Lafortune, and Teneketzis (2004), which addressed the problem of diagnosing intermittent failure, namely that: (i) there is no reset event here; (ii) cyclic paths with unobservable events are allowed here, as opposed to Contant et al. (2004), which prevent the existence of cyclic paths. Our approach is also different from that by Thorsley, Yoo, and Garcia (2008), who addressed the problem of stochastic discrete event systems under unreliable observation, and also from that by Ushio and Takai (2009) in the context of supervisory control, which modeled the unreliable observations using masks.

Sensor faults have also been addressed in the context of supervisory control (Alves et al., 2014; Rohloff, 2005; Sanchez & Montoya, 2006; Ushio & Takai, 2009; Xu & Kumar, 2009), and as part of the design requirements of fault diagnosis systems (Carvalho et al., 2012; Carvalho, Moreira, Basilio, & Lafortune, 2013). Differently from the works by Alves et al. (2014), Carvalho et al. (2012, 2013), Rohloff (2005) and Sanchez and Montoya (2006) we are not proposing a system that copes with sensor faults but one that actually detects its malfunction.

This paper is organized as follows. We present in Section 2 a brief review of Discrete Event Systems (DES) theory and review the model for intermittent loss of observations proposed in Carvalho et al. (2012). In Section 3, we convert the problem of sensor fault diagnosis into an equivalent one that consists of diagnosing the language generated by an automaton subject to intermittent sensor faults, where the fault event is the event recorded by the sensor whose malfunction must be diagnosed, and present the definitions of *F*-, *R*-, and *FR*-diagnosability. After that, we present necessary and sufficient conditions for the diagnosis of intermittent faults using diagnosers (Section 4) and verifiers (Section 5). Finally, in Section 6, we remind the main contributions of the paper.

2. Preliminaries

Let $G = (X, \Sigma, f, \Gamma, x_0, X_m)$ be a deterministic automaton, where X denotes the state space, Σ is the finite set of events, $f : X \times \Sigma \to X$ is the state transition function, $\Gamma : X \to 2^{\Sigma}$ is the active event function, where $\Gamma(x) = \{\sigma \in \Sigma : f(x, \sigma) \text{ is defined}\}$, x_0 is the initial state, and X_m is the set of marked states. When the set of marked states is empty, *i.e.*, $X_m = \emptyset$, it will be omitted from G. The Kleene-closure of Σ, Σ^*, is the set of all possible finite length traces that can be formed with the elements of Σ, including the empty trace ϵ. We extend the domain of f to $X \times \Sigma^*$ to define the language generated by G (denoted as $L(G)$, or simply, L) as the set of all traces $s \in \Sigma^*$ for which $f(x_0, s)$ is defined.

The accessible part of G, denoted by $Ac(G)$, is the unary operation that deletes from G the states that are not reachable from x_0 and the transitions attached to these states, *i.e.*, $Ac(G) = (X_{ac}, \Sigma, f_{ac}, \Gamma_{ac}, x_0, X_{ac,m})$, where $X_{ac} = \{x \in X : (\exists s \in \Sigma^*)[f(x_0, s) = x]\}$, $f_{ac} : X_{ac} \times \Sigma \to X_{ac}$, $\Gamma_{ac} : X_{ac} \to 2^{\Sigma}$, and $X_{ac,m} = X_m \cap X_{ac}$. The coaccessible part of G, denoted as $CoAc(G)$, is obtained by deleting all states of G from which it is not possible to reach a marked state and their associated transitions, *i.e.*, $CoAc(G) = (X_{coac}, \Sigma, f_{coac}, \Gamma_{coac}, x_{0,coac}, X_m)$ where $X_{coac} = \{x \in X : (\exists s \in \Sigma^*)[f(x, s) \in X_m]\}$, $f_{coac} : X_{coac} \times \Sigma \to X_{coac}$, with $f_{coac}(x, \sigma) = f(x, \sigma)$, if $x \in X_{coac}$ and $f(x, \sigma) \in X_{coac}$, or undefined, otherwise, and $\Gamma_{coac} : X_{coac} \to 2^{\Sigma}$, with $\Gamma_{coac}(x_{coac}) = \{\sigma : \sigma \in \Sigma, f_{coac}(x, \sigma) \text{ is defined}\}$, and $x_{0,coac} = x_0$, if $x_0 \in X_{coac}$, or undefined, if $x_0 \notin X_{coac}$.

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 two finite state automata. The parallel composition between G_1 and G_2 (denoted as $G_1 \parallel G_2$) is defined as $G_1 \parallel G_2 = (X_1 \times X_2, \Sigma_1 \cup \Sigma_2, f_{1\parallel 2}, \Gamma_{1\parallel 2}, (x_{0,1}, x_{0,2}))$, where $f_{1\parallel 2} : (X_1 \times X_2) \times (\Sigma_1 \cup \Sigma_2) \to (X_1 \times X_2)$ is defined as follows: $f_{1\parallel 2}((x_1, x_2), \sigma) = (f_1(x_1, \sigma), x_2)$ if $\sigma \in \Gamma_1(x_1) \setminus \Sigma_2$; $f_{1\parallel 2}((x_1, x_2), \sigma) = (x_1, f_2(x_2, \sigma))$ if $\sigma \in \Gamma_2(x_2) \setminus \Sigma_1$; $f_{1\parallel 2}((x_1, x_2), \sigma) = (f_1(x_1, \sigma), f_2(x_2, \sigma))$ if $\sigma \in \Gamma_1(x_1) \cap \Gamma_2(x_2)$; and undefined, otherwise; and for all $(x_1, x_2) \in X_1 \times X_2$, $\sigma \in \Sigma_1 \cup \Sigma_2$, $\Gamma_{1\parallel 2}((x_1, x_2)) = (\Gamma_1(x_1) \cap \Gamma_2(x_2)) \cup (\Gamma_1(x_1) \setminus \Sigma_2) \cup (\Gamma_2(x_2) \setminus \Sigma_1)$.

Let $\Sigma = \Sigma_o \dot{\cup} \Sigma_{uo}$ be a partition of Σ, where Σ_o and Σ_{uo} are, respectively, the set of observable and unobservable events. An important language operation is the natural projection $P_o : \Sigma^* \to \Sigma_o^*$ satisfying the following properties (Ramadge & Wonham, 1989): (i) $P_o(\epsilon) = \epsilon$, (ii) $P_o(\sigma) = \sigma$, if $\sigma \in \Sigma_o$, or $P_o(\sigma) = \epsilon$, if $\sigma \in \Sigma_{uo}$ and, $P_o(s\sigma) = P_o(s)P_o(\sigma)$, $s \in \Sigma^*, \sigma \in \Sigma$. The projection operation can be extended to a language L by applying the natural projection to all traces of L. Therefore, if $L \subseteq \Sigma^*$, then $P_o(L) = \{t \in \Sigma_o^* : (\exists s \in L)[P_o(s) = t]\}$. The inverse projection P_o^{-1} is defined as $P_o^{-1}(s) = \{t \in \Sigma^* : P_o(t) = s\}$.

The observed dynamic behavior of a deterministic automaton G with unobservable events, can be described by a deterministic automaton called observer (denoted as Obs (G)), whose event set is the set of observable events of G and the states are estimates of the states of the plant G after the observation of a trace. The language generated by Obs (G) is the projection of the language generated by G over Σ_o^*, *i.e.*, $L(\text{Obs}\,(G)) = P_o[L(G)]$ (Cassandras & Lafortune, 2008).

Let $\Sigma_{isf} \subseteq \Sigma_o$ denote the set of events associated with the sensors that are subject to intermittent faults, and define $\Sigma'_{isf} = \{\sigma' : \sigma \in \Sigma_{isf}\}$ and $\Sigma_{dil} = \Sigma \dot{\cup} \Sigma'_{isf}$. The following language operation can be defined (Carvalho et al., 2012).

Definition 1 (*Dilation*)**.** The dilation D is the mapping $D : \Sigma^* \to 2^{\Sigma_{dil}^*}$, where $D(\epsilon) = \{\epsilon\}$, $D(\sigma) = \{\sigma\}$, if $\sigma \in \Sigma \setminus \Sigma_{isf}$, $D(\sigma) = \{\sigma, \sigma'\}$, if $\sigma \in \Sigma_{isf}$, and $D(s\sigma) = D(s)D(\sigma)$, $s \in \Sigma^*, \sigma \in \Sigma$.

Notice that $D(s), D(\sigma) \subseteq 2^{\Sigma^*_{dil}}$, and thus, $D(s)D(\sigma) = \{uv : u \in D(s), v \in D(\sigma)\}$ is, actually, a concatenation of sets of strings. The dilation operation D can be extended from traces to languages by applying it to all traces of the language, that is, $L_{dil} = D(L) = \bigcup_{s \in L} D(s)$.

Definition 2 (*Path and Cyclic path*). (i) A path in G is a sequence $(x_1, \sigma_1, x_2, \sigma_2, \ldots, \sigma_{n-1}, x_n)$ where $x_i \in X, \sigma_i \in \Sigma, x_{i+1} = f(x_i, \sigma_i)$, $i = 1, 2, \ldots, n-1$; (ii) a path $(x_1, \sigma_1, x_2, \sigma_2, \ldots, \sigma_{n-1}, x_n)$ is cyclic if $x_1 = x_n$.

In Carvalho et al. (2012), we propose the construction of an automaton G_{dil} that takes into account intermittent sensor faults, which is obtained from G by adding transitions labeled with $\sigma' \in \Sigma'_{isf}$ in parallel with all transitions labeled with event $\sigma \in \Sigma_{isf}$, being defined as follows:

$$G_{dil} = (X, \Sigma_{dil}, f_{dil}, \Gamma_{dil}, x_0), \tag{1}$$

where $\Gamma_{dil}(x) = \Gamma(x) \cup \{\sigma' : \sigma \in \Sigma_{isf} \cap \Gamma(x)\}$, $f_{dil}(x, \sigma) = f(x, \sigma), \forall \sigma \in \Gamma(x)$ and $f_{dil}(x, \sigma') = f(x, \sigma), \forall \sigma' \in \Gamma_{dil}(x)$. As proved in Carvalho et al. (2012), the language L_{dil} generated by G_{dil} is $L_{dil} = D(L)$.

3. Diagnosability of intermittent sensor faults

Sensor fault diagnosis is carried out by detecting the occurrence of σ' within a finite number of occurrences of observable events. However, since σ' is not an event of G, sensor fault diagnosability cannot be stated in terms of the diagnosability of L, but in terms of L_{dil}. Notice that, although the model used here to account for sensor fault is a modification of that presented in Carvalho et al. (2012), the definition of sensor fault diagnosability cannot be stated in the same way, since in Carvalho et al. (2012), the objective is to diagnose the occurrence of an unobservable event from a set $\Sigma_f \subseteq \Sigma_{uo}$ assuming intermittent loss of observation of the events in the set $\Sigma_{isf} \subset \Sigma_o$, whereas in this paper the objective is to diagnose the occurrence of the events in Σ'_{isf}.

We make the following assumptions:

A1. The language generated by G is live, *i.e.*, $\Gamma(x_i) \neq \emptyset$ for all $x_i \in X$;
A2. Only one sensor is subject to intermittent malfunction, *i.e.*, $\Sigma_{isf} = \{\sigma\}$ and $\Sigma'_{isf} = \{\sigma'\}$.

Notice that, there is no loss of generality in assuming that $\Sigma_{isf} = \{\sigma\}$, since if more than one of the sensors are subject to intermittent malfunction, the approach presented here is still valid. In this regard, if $\Sigma_{isf} = \{\sigma_1, \sigma_2, \ldots, \sigma_n\}$, then the dilated model G_{dil} is built by adding to G transitions labeled with $\sigma'_i, i = 1, 2, \ldots, n$, in parallel with those labeled by $\sigma_i, i = 1, 2, \ldots, n$. In this case, sensor fault diagnosability will be analyzed in accordance with the approach proposed here for each event $\sigma'_i, i = 1, 2, \ldots, n$, by considering events σ'_j, for $j \neq i$, as ordinary unobservable events (see Yoo & Lafortune, 2002).

Remark 1. An assumption that is made in Contant et al. (2004) and Sampath, Sengupta, Lafortune, Sinnamohideen, and Teneketzis (1995) is that G does not have cyclic paths formed only with unobservable events. We remove this assumption here since even if we preclude G from having cyclic paths formed with unobservable events, such paths could still appear in G_{dil}. This is so because the dilation operation introduces a transition labeled with σ' (which is unobservable) in parallel with σ (which is observable). Notice that, if, for example, there exists a self-loop labeled with σ in a given state of G, then a self-loop labeled with σ' will be introduced in G_{dil}. A consequence of this assumption removal is that all tests proposed in Contant et al. (2004) cannot be applied to the problem considered here.

Let $\Psi(\Sigma'_{isf}) = \{s\sigma' \in L_{dil} : \sigma' \in \Sigma'_{isf}\}$ denote the set of all traces of L_{dil} that end with event σ', and let $L_{dil}/s = \{t \in \Sigma^*_{dil} : st \in L_{dil}\}$ be the language continuation of L_{dil} after trace s. In addition, let $\bar{s}$ denote the prefix closure of s. With a slight abuse of notation, the relationship $\Sigma'_{isf} \in s$ is used to denote that $\bar{s} \cap \Psi(\Sigma'_{isf}) \neq \emptyset$, and we say that a trace $s \in L$ has a sensor fault event if $\Sigma'_{isf} \in s$. We present the following definitions.

Definition 3 (*Normal, Faulty, Recovered, and Unrecovered Faulty Sensor Trace*).

- A normal trace $s_N \in L_{dil}$ is a trace that does not contain the sensor fault event σ', *i.e.*, $\Sigma'_{isf} \notin s_N$.
- A faulty trace $s_{FR} \in L_{dil}$ is a trace that contains the sensor fault event σ', *i.e.*, $\Sigma'_{isf} \in s_{FR}$.
- A recovered faulty sensor trace is a trace $s_R \in L_{dil}$ such that $s_R = s'_R s''_R$ where σ' is the last event of s'_R, and s''_R contains event σ but does not contain event σ', *i.e.*, $s'_R \in \Psi(\Sigma'_{isf})$, $\Sigma_{isf} \in s''_R$ and $\Sigma'_{isf} \notin s''_R$.
- An unrecovered faulty sensor trace is a trace $s_F \in L_{dil}$ such that $s_F = s'_F s''_F$ where σ' is the last event of s'_F, and s''_F does not contain event σ, *i.e.*, $s'_F \in \Psi(\Sigma'_{isf})$, and $\Sigma_{isf} \notin s''_F$.

Definition 4 (*F-Diagnosability, R-Diagnosability and FR-Diagnosability*). Let L_{dil} be the language generated by automaton G_{dil}. We say that:

- L_{dil} is F-diagnosable with respect to projection $P_{dil,o} : \Sigma^*_{dil} \to \Sigma^*_o$ and Σ'_{isf}, if the following holds true:

  $$(\exists n \in \mathbb{N})(\forall s \in \Psi(\Sigma'_{isf}))(\forall t \in L_{dil}/s, \Sigma_{isf} \notin t)$$
  $$(\|t\| \geq n) \Rightarrow D_F,$$

  where the diagnosability condition D_F is

  $$(\forall \omega = \omega'\omega'' \in P^{-1}_{dil,o}(P_{dil,o}(st)) \cap L_{dil})((\omega' \in \Psi(\Sigma'_{isf}))$$
  $$\wedge (\Sigma_{isf} \notin \omega'')).$$

- L_{dil} is R-diagnosable with respect to projection $P_{dil,o} : \Sigma^*_{dil} \to \Sigma^*_o$, Σ'_{isf} and Σ_{isf}, if the following holds true:

  $$(\exists n \in \mathbb{N})(\forall s \in \Psi(\Sigma_{isf}), \Sigma'_{isf} \in s)(\forall t \in L_{dil}/s, \Sigma'_{isf} \notin t)$$
  $$(\|t\| \geq n) \Rightarrow D_R,$$

  where the diagnosability condition D_R is

  $$(\forall \omega = \omega'\omega'' \in P^{-1}_{dil,o}(P_{dil,o}(st)) \cap L_{dil})((\omega' \in \Psi(\Sigma'_{isf}))$$
  $$\wedge (\Sigma'_{isf} \notin \omega'') \wedge (\Sigma_{isf} \in \omega'')).$$

- L_{dil} is FR-diagnosable with respect to projection $P_{dil,o} : \Sigma^*_{dil} \to \Sigma^*_o$ and Σ'_{isf}, if the following holds true:

  $$(\exists n \in \mathbb{N})(\forall s \in \Psi(\Sigma'_{isf}))(\forall t \in L_{dil}/s)(\|t\| \geq n) \Rightarrow D_{FR},$$

  where the diagnosability condition D_{FR} is $(\forall \omega \in P^{-1}_{dil,o}(P_{dil,o}(st)) \cap L_{dil})(\Sigma'_{isf} \in \omega)$.

The idea behind the definitions of F-, R-, and FR-diagnosability are as follows: F-diagnosability accounts for the permanent occurrence of some sensor fault, *i.e.*, if the sensor under consideration has never recovered after the last time it failed; R-diagnosability considers the case when the sensor never fails again after the last time it recovered from failure; and FR-diagnosability attempts to identify if the sensor has failed at some point without concern as to whether or not it will recover from the failure. In this regard, the definition of FR-diagnosability is equivalent to that of failure diagnosability introduced in Sampath et al. (1995).

According to Definition 4, language L_{dil} is not F-diagnosable if there exist an unrecovered faulty sensor trace s_F, with arbitrarily long length after the occurrence of the sensor fault event, and

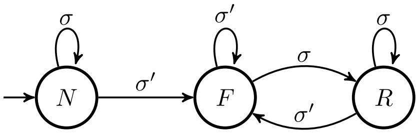


Fig. 2. Automaton A_ℓ that represents the status of the sensor subject to intermittent faults.

either a normal trace s_N or a recovered faulty sensor trace s_R, such that $P_{dil,o}(s_F) = P_{dil,o}(s_N)$ or $P_{dil,o}(s_F) = P_{dil,o}(s_R)$. Language L_{dil} is not R-diagnosable if there exist a recovered faulty sensor trace s_R, with arbitrarily long length after the occurrence of a sensor recovery, and either a normal trace s_N or an unrecovered faulty sensor trace s_F, such that $P_{dil,o}(s_R) = P_{dil,o}(s_N)$ or $P_{dil,o}(s_R) = P_{dil,o}(s_F)$. Finally, L_{dil} is not FR-diagnosable if there exists a faulty trace s_{FR}, with arbitrarily long length after the occurrence of a sensor fault, and a normal trace s_N such that $P_{dil,o}(s_{FR}) = P_{dil,o}(s_N)$.

Remark 2. The definitions of F-diagnosability and R-diagnosability presented here and the definitions of intermittent fault diagnosability presented in Contant et al. (2004) are similar, except that the latter requires, besides a fault event, another unobservable event, the so-called "reset" event, whereas in the former, there is no "reset" event.

4. Verification of diagnosability of intermittent sensor faults using diagnosers

In order to develop a systematic way to verify intermittent sensor fault diagnosability, it is necessary to introduce the label automaton A_ℓ, shown in Fig. 2, whose states correspond to the status of the sensor subject to intermittent faults with respect to the occurrence of the fault and its recovery. In Fig. 2, event $\sigma \in \Sigma_{isf}$ is the event recorded by the sensor whose malfunction we are interested in detecting, and $\sigma' \in \Sigma'_{isf}$ is the corresponding fault event associated with σ. Notice that, as long as the sensor records and communicates correctly the occurrence of σ, the sensor is in normal behavior, which is represented in automaton A_ℓ by state N. However, when a sensor fault occurs, the status of the sensor moves to state F and remains there as long as the sensor is not able to record and communicate the occurrence of the event to the diagnoser. If the sensor starts to work again, *i.e.*, when σ is recorded again, the status of the sensor changes to state R, where it stays while the sensor continues to record and communicate the occurrence of σ. On the other hand, if, at some point, the sensor fails again to record and communicate the event occurrence, the status of the sensor returns to state F.

We will now propose a test to verify the diagnosability of intermittent sensor faults using a diagnoser automaton. Besides its usefulness as a diagnosability test, the proposed diagnoser can also be used for online diagnosis when the sensor fault is diagnosable. Let us first define automaton G^ℓ_{dil} as follows:

$$G^\ell_{dil} = G_{dil} \parallel A_\ell, \tag{2}$$

where A_ℓ is the label automaton shown in Fig. 2. Notice that the states of G^ℓ_{dil} are obtained by adding labels N, F or R to the states of the plant to indicate whether the sensor has not failed, if the sensor has failed, or if the sensor failed and has recovered from the fault. Denoting by $\Sigma_{dil,\ell}$ and $L_{dil,\ell}$ the set of events and the language generated by G^ℓ_{dil}, respectively, it is straightforward to see that $L_{dil,\ell} = L_{dil}$, since $\Sigma_\ell \subset \Sigma_{dil}$, and $L_\ell = \Sigma^*_\ell$, where Σ_ℓ and L_ℓ are, respectively, the event set and the language generated by A_ℓ. We propose the following diagnoser:

$$G^d_{dil} = \mathrm{Obs}\,(G^\ell_{dil}) = (X_d, \Sigma_o, f_d, \Gamma_d, x_{0,d}). \tag{3}$$

Notice that different combinations of labels may appear in the states of G^d_{dil}, which leads to the following state classification.[1]

Definition 5. A state $x_d \in X_d$ is called:

- NF-uncertain, *i.e.*, uncertain if either the sensor has not failed or if the sensor has failed and has not recovered from the fault, if $\exists\ (x, \ell), (y, \tilde{\ell}) \in x_d$, x not necessarily distinct from y such that $\ell = N$ and $\tilde{\ell} = F$;
- NR-uncertain, *i.e.*, uncertain if either the sensor has not failed or if the sensor has failed and recovered from fault, if $\exists\ (x, \ell), (y, \tilde{\ell}) \in x_d$, x not necessarily distinct from y such that $\ell = N$ and $\tilde{\ell} = R$;
- FR-uncertain, *i.e.*, uncertain if either the sensor has failed and not recovered or has failed and recovered from fault, if $\exists\ (x, \ell), (y, \tilde{\ell}) \in x_d$, x not necessarily distinct from y such that $\ell = F$ and $\tilde{\ell} = R$.

According to Definition 5, if there exist $(x, \ell), (y, \tilde{\ell}), (z, \hat{\ell}) \in x_d$, x, y, z not necessarily distinct, such that $\ell = N$, $\tilde{\ell} = F$ and $\hat{\ell} = R$, then x_d is simultaneously NF-, NR- and FR-uncertain, *i.e.*, x_d is uncertain if either the sensor has not failed, or if the sensor has failed and not recovered from fault, or still if the sensor has failed and recovered from fault.

We will now define indeterminate cycles, *i.e.*, cycles that express the diagnoser uncertainty with respect to the traces generated by the plant that can be affected by intermittent sensor faults. Notice that the possibility of appearing cyclic paths of unobservable events requires that not only indeterminate observed cycles but also indeterminate hidden cycles (Basilio & Lafortune, 2009) must be considered.

Definition 6 (*Cycle*). A set of states $\{x_1, x_2, \ldots, x_n\} \subseteq X$ forms a cycle in an automaton $H = (X, \Sigma, f, \Gamma, x_0)$ if there exists in H a cyclic path $(x_1, \sigma_1, x_2, \sigma_2, \ldots, \sigma_{n-1}, x_n)$, where $x_{i+1} = f(x_i, \sigma_i)$, $i = 1, 2, \ldots, n-1$, and $x_1 = x_n$.

Definition 7 (*Indeterminate Observed Cycle*). A set of states $\{x^1_d, x^2_d, \ldots, x^p_d\} \subseteq X_d$ forms an indeterminate observed cycle in G^d_{dil} if the following conditions hold true:

(1) $x^1_d, x^2_d, \ldots, x^p_d$ form a cycle in G^d_{dil};
(2) $\exists (x^i_{k_i}, \ell^i_{k_i}), (\tilde{x}^i_{r_i}, \tilde{\ell}^i_{r_i}) \in x^i_d$, and $x^i_{k_i}$ not necessarily distinct from $\tilde{x}^i_{r_i}$, $i = 1, 2, \ldots, p$, $k_i = 1, 2, \ldots, m_i$, and $r_i = 1, 2, \ldots, \tilde{m}_i$, where $0 < m_i \leq |x^i_d|$ and $0 < \tilde{m}_i \leq |x^i_d|$, such that the state sequences $\{(x^i_{k_i}, \ell^i_{k_i})\}$ (respectively, $\{(\tilde{x}^i_{r_i}, \tilde{\ell}^i_{r_i})\}$), with $i = 1, 2, \ldots, p$, $k_i = 1, 2, \ldots, m_i$, (resp., $i = 1, 2, \ldots, p$, $r_i = 1, 2, \ldots, \tilde{m}_i$) forms a cycle in G^ℓ_{dil}, whose corresponding cyclic paths have sequences s and $\tilde{s}$, respectively, such that $P_{dil,o}(s) = P_{dil,o}(\tilde{s}) = \sigma_1\sigma_2 \ldots \sigma_{p-1}$, where $f(x^i_d, \sigma_i) = x^{i+1}_d$, $i = 1, 2, \ldots, p-1$.

Moreover:

- the cycle is an F-indeterminate observed cycle (F-ioc) if, for all $i = 1, 2, \ldots, p$, $\ell^i_{k_i} = F$, $k_i = 1, 2, \ldots, m_i$, and either $\tilde{\ell}^i_{r_i} = N$ or $\tilde{\ell}^i_{r_i} = R$, $r_i = 1, 2, \ldots, \tilde{m}_i$.
- the cycle is an R-indeterminate observed cycle (R-ioc) if $\ell^i_{k_i} = R$, for all $i = 1, 2, \ldots, p$ and $k_i = 1, 2, \ldots, m_i$, and either $\tilde{\ell}^i_{r_i} = N$, for all $i = 1, 2, \ldots, p$, and $r_i = 1, 2, \ldots, \tilde{m}_i$, or $\tilde{\ell}^i_{r_i} = F$ for at least one $r_i \in \{1, \ldots, \tilde{m}_i\}$.

[1] The state classification introduced here is a natural extension of those originally presented by Sampath et al. (1995).

- the cycle is an *FR*-indeterminate observed cycle (*FR*-ioc) if for all $i = 1, 2, \ldots, p$, $\ell^i_{k_i} \in \{F, R\}$, $k_i = 1, 2, \ldots, m_i$, and $\tilde{\ell}^i_{r_i} = N$, $r_i = 1, 2, \ldots, \tilde{m}_i$.

According to Definition 7, associated with an *R*-indeterminate observed cycle, it is possible to exist cyclic paths in G^{ℓ}_{dil} whose states $(x^i_{k_i}, \ell^i_{k_i})$ are all labeled with *R* and the states $(\tilde{x}^i_{r_i}, \tilde{\ell}^i_{r_i})$ are labeled with *F* and *R*. Thus, we can associate these cyclic paths with an arbitrarily long length recovered faulty trace s, with the same projection as that of an arbitrarily long length faulty trace $\tilde{s}$ which is neither an unrecovered nor a recovered faulty sensor trace.

Definition 8 (*Hidden and Indeterminate Hidden Cycles*). Let $x_d = \{(x_1, \ell_1), (x_2, \ell_2), \ldots, (x_n, \ell_n)\}$ be a state of G^d_{dil}. There exists a hidden cycle in x_d if for some $\{i_1, i_2, \ldots, i_k\} \subseteq \{1, 2, \ldots, n\}$, the following conditions hold true:

(HC.1) $\{(x_{i_1}, \ell_{i_1}), (x_{i_2}, \ell_{i_2}), \ldots, (x_{i_k}, \ell_{i_k})\}$ forms a cycle in G^{ℓ}_{dil};
(HC.2) There exists a set $\{\sigma_{i_1}, \sigma_{i_2}, \ldots, \sigma_{i_k}\} \subseteq \Sigma_{uo} \cup \Sigma'_{isf}$, where $\sigma_{i_1}, \sigma_{i_2}, \ldots, \sigma_{i_k}$ are such that $((x_{i_1}, \ell_{i_1}), \sigma_{i_1}, (x_{i_2}, \ell_{i_2}), \sigma_{i_2}, \ldots, \sigma_{i_k}, (x_{i_k}, \ell_{i_k}))$ forms a cyclic path in G^{ℓ}_{dil}.

If besides conditions HC.1 and HC.2,

- x_d is an *NF*- and/or *FR*-uncertain state of G^d_{dil}, and $\ell_{i_j} = F$, $j = 1, 2, \ldots, k$, then x_d has an *F*-indeterminate hidden cycle (*F*-ihc);
- x_d is an *NR*- and/or *FR*-uncertain state of G^d_{dil}, and $\ell_{i_j} = R$, $j = 1, 2, \ldots, k$, then x_d has an *R*-indeterminate hidden cycle (*R*-ihc);
- x_d is an *NR*- and/or *NF*-uncertain state of G^d_{dil}, and $\ell_{i_j} = R$ or $\ell_{i_j} = F, j = 1, 2, \ldots, k$, then x_d has an *FR*-indeterminate hidden cycle (*FR*-ihc);

Based on Definitions 7 and 8, we state the following theorem.

Theorem 1. *Language L_{dil}, generated by G_{dil} will be F-diagnosable (respectively, R-diagnosable, FR-diagnosable) with respect to projection $P_{dil,o} : \Sigma^*_{dil} \to \Sigma^*_o$ and Σ'_{isf}, if and only if, diagnoser G^d_{dil} has no F-indeterminate (resp., R-indeterminate, FR-indeterminate) cycles (observed or hidden).*

Proof. We will present the proof for *F*-diagnosability, only. The proof of *R*-diagnosability follows the same steps and arguments as those for *F*-diagnosability, and the proof for *FR*-diagnosability has already been presented in Basilio, Lima, Lafortune, and Moreira (2012) and Carvalho et al. (2012).

($\Leftarrow$) Assume that L_{dil} is not *F*-diagnosable with respect to $P_{dil,o}$ and Σ'_{isf}. Therefore, according to Definition 4, there exists a trace $s_F = st \in L_{dil}$, such that $s \in \Psi(\Sigma'_{isf})$, $t \in L_{dil}/s$, and $\Sigma_{isf} \notin t$, and there exists either a normal trace s_N, or a recovered faulty sensor trace s_R, or both, that satisfy the following conditions:

(1) $\Sigma'_{isf} \notin s_N$ and $P_{dil,o}(s_N) = P_{dil,o}(s_F)$;
(2) $s_R = s'_R s''_R$ such that $(s'_R \in \Psi(\Sigma'_{isf})) \wedge (\Sigma_{isf} \in s''_R) \wedge (\Sigma'_{isf} \notin s''_R)$ and $P_{dil,o}(s_R) = P_{dil,o}(s_F)$;

Since G^d_{dil} is a deterministic automaton, for each trace s_F there exist an *NF*- and/or an *FR*-uncertain state such that:

(3) $x_d = f_d(x_{0_d}, P_{dil,o}(s_F)) = f_d(x_{0_d}, P_{dil,o}(s_N))$, if x_d is an *NF*-uncertain state;
(4) $x_d = f_d(x_{0_d}, P_{dil,o}(s_F)) = f_d(x_{0_d}, P_{dil,o}(s_R))$, if x_d is an *FR*-uncertain state.

Notice that although s_F has unbounded length, G_{dil} is allowed to have cyclic paths formed with unobservable events, which implies that $P_{dil,o}(s_F)$ can have bounded length.

Let us consider, initially, the case when $P_{dil,o}(s_F)$ has unbounded length. Therefore, $P_{dil,o}(s_N)$ and $P_{dil,o}(s_R)$ will also have unbounded lengths. Assume that $|X_d| = N_d$, where $|.|$ denotes cardinality. If we make $n > N_d$, there must exist a cyclic path in G^d_{dil} for which at least one event is observable, therefore defining an observed cycle of uncertain states in G^d_{dil}. Notice that this cycle of uncertain states can be associated with two cycles in G^{ℓ}_{dil}, one with states labeled with *F* and another one labeled with *N* or *R*. Thus, the cycle of uncertain states is, according to Definition 7, an *F*-indeterminate observed cycle.

Let us consider now the case when s_F has unbounded length and $P_{dil,o}(s_F)$ has bounded length. Since x_d is an *NF*- and/or *FR*-uncertain state and st has unbounded length, then, according to Definition 8, there exists an *F*-indeterminate hidden cycle in the corresponding uncertain state x_d.

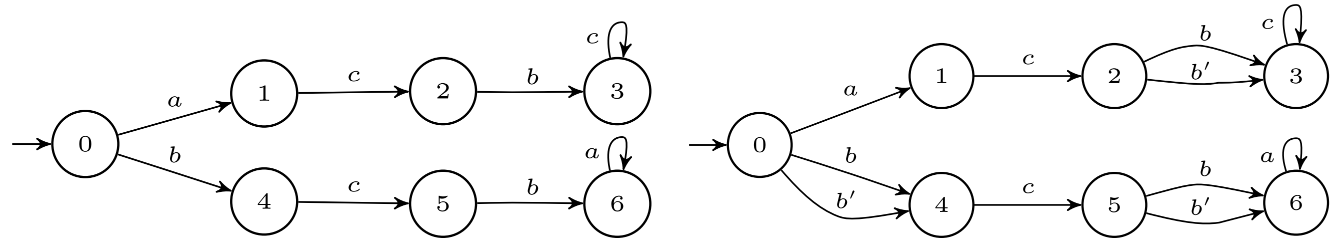
($\Rightarrow$) Let us consider, initially, the case when G^d_{dil} has *F*-indeterminate observed cycles. In this case, according to Definition 7, there exist an unrecovered faulty sensor trace s_F, and a normal trace s_N and/or a recovered faulty sensor trace s_R in L_{dil}, where s_F, s_R and s_N have unbounded length, such that $P_{dil,o}(s_F) = P_{dil,o}(s_N)$ and/or $P_{dil,o}(s_F) = P_{dil,o}(s_R)$. Thus, according to Definition 4, L_{dil} is not *F*-diagnosable with respect to projection $P_{dil,o}$ and Σ'_{isf}.

Finally, let us assume that there exists an *F*-indeterminate hidden cycle in a state $x_d = \{(x_1, \ell_1), (x_2, \ell_2), \ldots, (x_n, \ell_n)\} \in X_d$ of G^d_{dil}, where (x_i, ℓ_i) is a state of G^{ℓ}_{dil}. According to Definition 8, there exists $\{i_1, i_2, \ldots, i_k\} \subseteq \{1, 2, \ldots, n\}$ such that $((x_{i_1}, \ell_{i_1}), (x_{i_2}, \ell_{i_2}), \ldots, (x_{i_k}, \ell_{i_k}))$ forms a cycle in G^{ℓ}_{dil}, where $\ell_{i_j} = F, j = 1, 2, \ldots, k$. Thus, there exists an unrecovered faulty sensor trace s_F with unbounded length, and a normal trace s_N and/or a recovered faulty sensor trace s_R in L_{dil}, with bounded length, such that $P_{dil,o}(s_F) = P_{dil,o}(s_N)$ and/or $P_{dil,o}(s_F) = P_{dil,o}(s_R)$. Thus, according to Definition 4, L_{dil} is not *F*-diagnosable with respect to projection $P_{dil,o}$ and Σ'_{isf}. ■

Example 1. Consider automaton G_1 depicted in Fig. 3(a), where all events are assumed to be observable and let $\Sigma_{isf} = \{b\}$. The corresponding model $G_{dil,1}$ that takes into account possible intermittent faults in b is shown in Fig. 3(b). In order to construct the diagnoser, we must obtain, according to Eq. (2), automaton $G^{\ell}_{dil,1} = G_{dil,1} \parallel A_{\ell}$, which is depicted in Fig. 4(a). The diagnoser is then obtained, according to Eq. (3), as $G^d_{dil,1} = \text{Obs}\,(G^{\ell}_{dil,1})$, whose state transition diagram is shown Fig. 4(b). It is easy to check that $G_{dil,1}$ has neither *F*- nor *R*-indeterminate (observed or hidden) cycles and, thus, the language generated by $G_{dil,1}$ is *F*-diagnosable with respect to projection $P_{dil,o}$ and $\Sigma'_{isf} = \{b'\}$ and *R*-diagnosable with respect to projection $P_{dil,o}$, $\Sigma'_{isf} = \{b'\}$ and $\Sigma_{isf} = \{b\}$.

Example 2. Consider automaton G_2 shown in Fig. 5, and assume that the sets of observable and unobservable events are $\Sigma_o = \{b, c\}$ and $\Sigma_{uo} = \{a\}$, respectively, and that $\Sigma_{isf} = \{b\}$. The corresponding diagnoser $G^d_{dil,2}$ is depicted in Fig. 6, where we can see that there exist both *F*- and *R*-indeterminate (observed and hidden) cycles in $G^d_{dil,2}$. Therefore, according to Theorem 1, the language generated by $G_{dil,2}$ is neither *F*-diagnosable nor *R*-diagnosable with respect to projection $P_{dil,o}$, $\Sigma_{isf} = \{b\}$ and $\Sigma'_{isf} = \{b'\}$. We will show the traces that lead the loss of diagnosability.

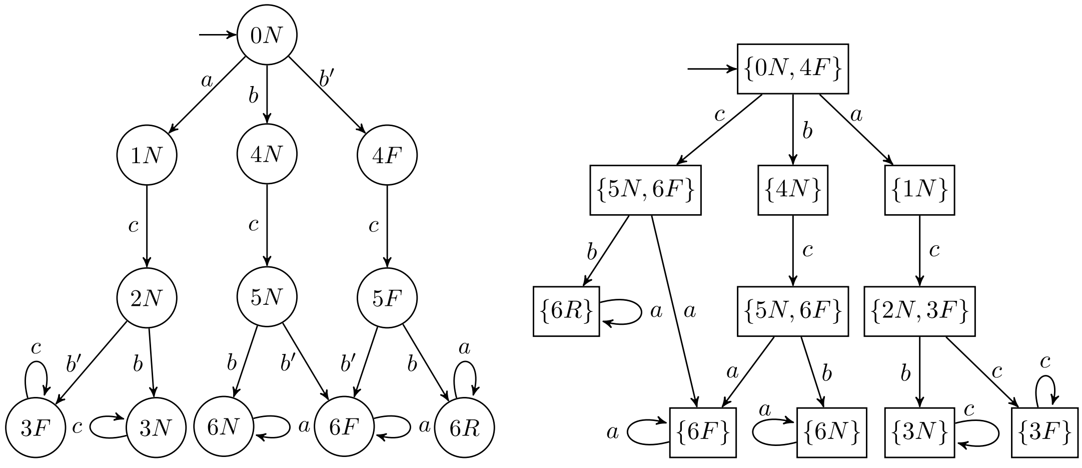
- Let us first consider the *F*-indeterminate hidden cycle in the *NF*-uncertain state $\{2N, 3F, 4F, 7F, 8F\}$. It is not difficult to see that there exist two traces, a faulty trace $s_F = b'acb'a^n$, $n \in \mathbb{N}$, and a normal trace $s_N = ac$, for which, $P_{dil,o}(s_F) = P_{dil,o}(s_N) = c$, which violates the *F*-diagnosability condition.
- Let us now consider the *R*-indeterminate hidden cycles in the *NF*-, *NR*- and *FR*-uncertain state $\{3N, 4F, 4R, 8R\}$. In this case, we can find three traces: a normal trace $s_N = acb$, a faulty trace $s_F = acbb'$ and a recovered faulty sensor trace $s_R = b'acba^n$ with an occurrence of event b after the sensor fault, for which $P_{dil,o}(s_R) = P_{dil,o}(s_N) = P_{dil,o}(s_F) = cb$, which violates the *R*-diagnosability condition.



(a) Automaton G_1.

(b) Automaton $G_{dil,1}$.

Fig. 3. Automata G_1 and $G_{dil,1}$.



(a) $G^{\ell}_{dil,1} = G_{dil,1} \parallel A_{\ell}$.

(b) $G^{d}_{dil,1} = \text{Obs}\,(G^{\ell}_{dil,1})$.

Fig. 4. Automaton $G^{\ell}_{dil,1}$ (a) and its diagnoser $G^{d}_{dil,1}$ (b).

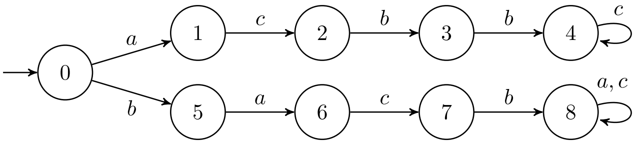


Fig. 5. Automaton G_2.

- Finally, let us consider the F- and R-indeterminate observed cycles formed with state $\{4F, 4R, 8R\}$. In this case, we can identify the existence of a faulty trace $s_F = acbb'c^n$ and two traces with occurrences of event b after the occurrence of b', $s_{R,1} = acb'bc^n$ and $s_{R,2} = b'acbc^n$, $n \in \mathbb{N}$, with the same projection over Σ_o^*, *i.e.*, $P_{dil,o}(s_F) = P_{dil,o}(s_{R,1}) = P_{dil,o}(s_{R,2}) = cbc^n$, which, again, violates both F- and R-diagnosability conditions. Notice that the existence of traces s_F, $s_{R,1}$ and $s_{R,2}$ implies that it is not possible to say whether the sensor has either failed permanently or failed and returned to work.

5. Verification of diagnosability of intermittent sensor faults using verifiers

Another way to verify language diagnosability is by using verifiers (Jiang, Huang, Chandra, & Kumar, 2001; Moreira, Jesus, & Basilio, 2011; Qiu & Kumar, 2006; Yoo & Lafortune, 2002). Although verifiers have the advantage of having polynomial time complexity, they can only be used for diagnosability analysis. Among the existing verifiers, the one proposed by Moreira et al. (2011) has the smallest computational complexity and has a very intuitive construction since only traces that have the same projection are searched. For this reason, we will propose, in this section, verifiers for the analysis of the diagnosability of intermittent sensor fault, inspired by that proposed in Moreira et al. (2011).

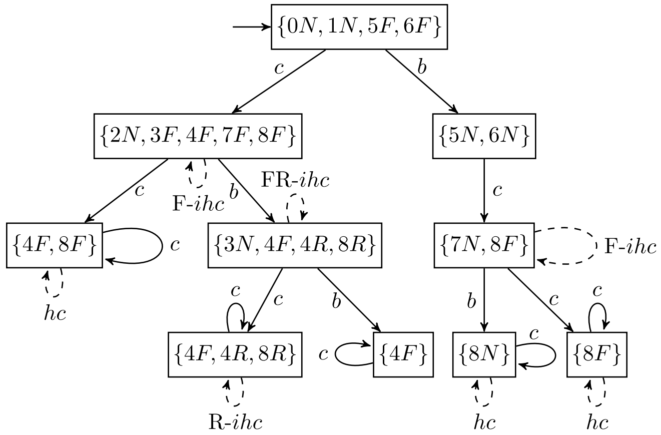


Fig. 6. Diagnoser $G^{d}_{dil,2}$.

The sensor fault diagnosability verification will be based on three verifier automata whose constructions are carried out according as follows.

Algorithm 1.

- Step 1: Compute, according to Eq. (2), automaton $G^{\ell}_{dil} = (X_{\ell}, \Sigma_{\ell}, f_{\ell}, \Gamma_{\ell}, x_{0,\ell})$.
- Step 2: Compute automaton G_N that models the non faulty behavior of G^{ℓ}_{dil}, as follows:
  - · Step 2.1: Mark all states of G^{ℓ}_{dil} whose second component is equal to N. Call the resulting automaton $\hat{G}^{\ell}_{dil}$.
  - · Step 2.2: Compute $G_N = CoAc(\hat{G}^{\ell}_{dil}) = (X_N, \Sigma_{dil}, f_N, \Gamma_N, x_{0,\ell}, X_{m,N})$.

- Step 2.3: Unmark all marked states of G_N, *i.e.*, set $G_N = (X_N, \Sigma_{dil}, f_N, \Gamma_N, x_{0,\ell})$.
- Step 3: Compute automaton G_F that models sensor fault occurrences in G_{dil}^{ℓ}, as follows:
  - Step 3.1: Mark all states of G_{dil}^{ℓ} whose second component is equal to F. Call the resulting automaton $\hat{G}_{dil}^{\ell}$.
  - Step 3.2: Compute the sensor faulty automaton $G_F = CoAc(\hat{G}_{dil}^{\ell}) = (X_F, \Sigma_{dil}, f_F, \Gamma_F, x_{0,\ell}, X_{m,F})$.
  - Step 3.3: Unmark all marked states of G_F, *i.e.*, $G_F = (X_F, \Sigma_{dil}, f_F, \Gamma_F, x_{0,\ell})$.
- Step 4: Compute automaton G_R that models the sensor recovery occurrences of the system, as follows:
  - Step 4.1: Mark all states of G_{dil}^{ℓ} whose second components are equal to R. Call the resulting automaton $\hat{G}_{dil}^{\ell}$.
  - Step 4.2: Compute the sensor recovery automaton $G_R = CoAc(\hat{G}_{dil}^{\ell}) = (X_R, \Sigma_{dil}, f_R, \Gamma_R, x_{0,\ell}, X_{m,R})$.
  - Step 4.3: Unmark all marked states of G_R, *i.e.*, $G_R = (X_R, \Sigma_{dil}, f_R, \Gamma_R, x_{0,\ell})$.
- Step 5: Construct automata $G_N^{\rho} = (X_N, \Sigma_{dil,N}, f_N^{\rho}, \Gamma_N^{\rho}, x_{0,\ell})$ and $G_F^{\rho} = (X_F, \Sigma_{dil,F}, f_F^{\rho}, \Gamma_F^{\rho}, x_{0,\ell})$, where, for $k \in \{N, F\}$, $\Sigma_{dil,k} = \rho_k(\Sigma_{dil})$, $f_k^{\rho}(x_k, \rho_k(\sigma)) = f_k(x_k, \sigma)$, for all $\sigma \in \Sigma_{dil}$, and $\Gamma_k^{\rho}(x_k) = \rho_k(\Gamma_k(x_k))$, with ρ_N and ρ_F being defined as follows:

$$\rho_N : \Sigma_{dil} \mapsto \Sigma_{dil,N}$$
$$\sigma \rightarrow \rho_N(\sigma) = \begin{cases} \sigma, & \text{if } \sigma \in \Sigma_o \\ \sigma_N, & \text{if } \sigma \in \Sigma_{uo} \cup \Sigma'_{isf} \end{cases} \qquad (4)$$

$$\rho_F : \Sigma_{dil} \mapsto \Sigma_{dil,F}$$
$$\sigma \rightarrow \rho_F(\sigma) = \begin{cases} \sigma, & \text{if } \sigma \in \Sigma_o \\ \sigma_F, & \text{if } \sigma \in \Sigma_{uo} \cup \Sigma'_{isf}. \end{cases} \qquad (5)$$

- Step 6: Compute the following verifier automata
$V_{NF} = G_N^{\rho} \parallel G_F = (X_{NF}, \Sigma_{dil,N} \cup \Sigma_{dil}, f_{NF}, x_{0,NF})$,
$V_{NR} = G_N^{\rho} \parallel G_R = (X_{NR}, \Sigma_{dil,N} \cup \Sigma_{dil}, f_{NR}, x_{0,NR})$,
$V_{FR} = G_F^{\rho} \parallel G_R = (X_{FR}, \Sigma_{dil,F} \cup \Sigma_{dil}, f_{FR}, x_{0,FR})$.

A necessary and sufficient condition for intermittent sensor fault based on the verifiers proposed in Algorithm 1 can be obtained in a more straightforward way with the help of the following lemma.

Lemma 1. *Let $G_1 = (X_1, \Sigma_1, f_1, \Gamma_1, x_{0,1})$ and $G_2 = (X_2, \Sigma_2, f_2, \Gamma_2, x_{0,2})$, where $\Sigma_1 = \Sigma_2 = \Sigma$, and let $\Sigma = \Sigma_o \dot{\cup} \Sigma_{uo}$ where Σ_o and Σ_{uo} are, respectively, the set of observable and unobservable events. Define the following renaming function:*

$$\rho(\sigma) = \begin{cases} \sigma, & \text{if } \sigma \in \Sigma_o \\ \sigma_{\rho}, & \text{if } \sigma \in \Sigma_{uo}. \end{cases} \qquad (6)$$

Construct automaton $G_1^{\rho} = (X_1, \Sigma_{1\rho}, f_{1\rho}, \Gamma_{1\rho}, x_{0,1})$, where $\Sigma_{1\rho} = \rho(\Sigma_1)$, $f_{1\rho}(x_1, \rho(\sigma)) = f_1(x_1, \sigma)$, for all $\sigma \in \Sigma_1$, and $\Gamma_{1\rho}(x_1) = \rho(\Gamma_1(x_1))$. Let $V_{12} = G_1^{\rho} \parallel G_2 = (X_v, \Sigma_v, f_v, \Gamma_v, x_{0,v})$ and define the projection $P_o : \Sigma^* \rightarrow \Sigma_o^*$.

Then, for every $v \in L(V_{12})$ there exist $t_1 \in L(G_1)$ and $t_2 \in L(G_2)$, such that $P_o(t_1) = P_o(t_2)$, and conversely.

Proof. Let us define the following projections: (i) $P_{1\rho} : \Sigma_v^* \rightarrow \Sigma_{1\rho}^*$; (ii) $P_2 : \Sigma_v^* \rightarrow \Sigma_2^*$; and (iii) $P_{\rho o} : \rho(\Sigma)^* \rightarrow \Sigma_o^*$.

($\Rightarrow$) Suppose that there exists a sequence $v \in L(V_{12})$, and let $t_{1\rho} = P_{1\rho}(v)$ and $t_2 = P_2(v)$. Since $V_{12} = G_1^{\rho} \parallel G_2$, then $L(V_{12}) = P_{1\rho}^{-1}[L(G_1^{\rho})] \cap P_2^{-1}[L(G_2)]$, which implies that: (a) $v \in P_{1\rho}^{-1}[L(G_1^{\rho})] \rightarrow P_{1\rho}(v) = t_{1\rho} \in L(G_1^{\rho})$; and (b) $v \in P_2^{-1}[L(G_2)] \rightarrow P_2(v) = t_2 \in L(G_2)$.

Since G_1^{ρ} is obtained from G_1 after renaming the unobservable events of Σ_1, there exists a sequence t_1 such that $t_{1\rho} = \rho(t_1)$. Notice that $P_o(t_1) = P_2(t_{1\rho})$ and $P_o(t_2) = P_{1\rho}(t_2)$. Since $t_{1\rho} = P_{1\rho}(v)$ and $t_2 = P_2(v)$, then $P_o(t_1) = P_2(P_{1\rho}(v))$ and $P_o(t_2) = P_{1\rho}(P_2(v))$. Finally, since $P_2(P_{1\rho}(v)) = P_{1\rho}(P_2(v))$, then $P_o(t_1) = P_o(t_2)$.

($\Leftarrow$) Let $t_1 \in L(G_1)$ and $t_2 \in L(G_2)$ be such that $P_o(t_1) = P_o(t_2)$. Define $t_{1\rho} = \rho(t_1) \in L(G_1^{\rho})$ and $\Sigma_{uo,\rho} = \rho(\Sigma_{uo})$. Then, $P_o(t_1) = P_{\rho o}(t_{1\rho})$. Let $P_{\rho o}(t_{1\rho}) = \sigma_1\sigma_2 \ldots \sigma_n$, where $\sigma_i \in \Sigma_o$, $i = 1, \ldots, n$, $n \in \mathbb{N}$. Thus, $t_{1\rho} = v_1\sigma_1 v_2\sigma_2 \ldots v_n\sigma_n v_{n+1}$, where $v_i \in \Sigma_{uo,\rho}^*$, $i = 1, \ldots, n+1$. Since $\Sigma_v = \Sigma_o \dot{\cup} \Sigma_{uo} \dot{\cup} \Sigma_{uo,\rho}$, we may conclude that $P_{1\rho}^{-1}(t_{1\rho}) \supseteq v_1 \Sigma_{uo}^* \sigma_1 v_2 \Sigma_{uo}^* \sigma_2 \ldots v_n\, \Sigma_{uo}^* \sigma_n v_{n+1} \Sigma_{uo}^*$. In addition, $P_o(t_1) = P_o(t_2)$, which implies that $P_o(t_2) = \sigma_1\sigma_2 \ldots \sigma_n$ and $t_2 = w_1\sigma_1 w_2\sigma_2 \ldots w_n\sigma_n w_{n+1}$, where $w_j \in \Sigma_{uo}^*$, $j = 1, \ldots, n+1$, and thus, $P_2^{-1}(t_2) \supseteq \Sigma_{uo,\rho}^* w_1\sigma_1 \Sigma_{uo,\rho}^* w_2\sigma_2 \ldots\ \Sigma_{uo,\rho}^* w_n\ \sigma_n \Sigma_{uo,\rho}^* w_{n+1}$. Since $w_j \in \Sigma_{uo}^*$, $v_i \in \Sigma_{uo,\rho}^*$, we may conclude that $v_1 w_1 \sigma_1 \ldots v_n w_n \sigma_n v_{n+1} w_{n+1} \in P_{1\rho}^{-1}(t_{1\rho}) \cap P_2^{-1}(t_2)$ and $P_{1\rho}^{-1}(t_{1\rho}) \cap P_2^{-1}(t_2) \neq \emptyset$. Therefore, $\emptyset \subset P_{1\rho}^{-1}(t_{1\rho}) \cap P_2^{-1}(t_2) \subseteq P_{1\rho}^{-1}[L(G_1^{\rho})] \cap P_2^{-1}[L(G_2)] = L(V_{12})$, which means that for given t_1, t_2 there exists at least one trace $v \in L(V_{12})$. ■

We now present a necessary and sufficient condition for F- or R- and FR-diagnosabilities in terms of the verifiers constructed in Algorithm 1.

Theorem 2. *Let L_{dil} be the language generated by automaton G_{dil}. Then:*

L_{dil} is not F-diagnosable with respect to projection $P_{dil,o}$ and Σ'_{isf}, if, and only if, at least one of the following conditions holds true:

F1. *there exists in V_{NF} a cyclic path $cl = (x_{NF}^k, \sigma^k, x_{NF}^{k+1}, \sigma^{k+1}, \ldots, x_{NF}^l, \sigma^l, x_{NF}^k)$, where $x_{NF}^p = (x_N^p, x_F^p)$, $p \in \{k, \ldots, l\}$ $(l \geq k > 0)$, such that $x_F^j = (x, F)$, $\forall j \in \{k, k+1, \ldots, l\}$, and $\exists q \in \{k, k+1, \ldots, l\}$ for which $\sigma^q \in \Sigma_{dil}$.*

F2. *there exists in V_{FR} a cyclic path, $cl = (x_{FR}^k, \sigma^k, x_{FR}^{k+1}, \sigma^{k+1}, \ldots, x_{FR}^l, \sigma^l, x_{FR}^k)$, where $x_{FR}^p = (x_F^p, x_R^p)$, $p \in \{k, \ldots, l\}$ $(l \geq k > 0)$ such that $x_F^j = (x, F)$, $\forall j \in \{k, k+1, \ldots, l\}$, and $\exists q \in \{k, k+1, \ldots, l\}$ such that $x_R^q = (x, R)$, and $\exists z \in \{k, k+1, \ldots, l\}$ for which $\sigma^z \in \Sigma_{dil,F}$.*

L_{dil} is not R-diagnosable with respect to projection $P_{dil,o}$ and Σ'_{isf}, if, and only if, at least one of the following conditions holds true:

R1. *there exists in V_{NR} a cyclic path $cl = (x_{NR}^k, \sigma^k, x_{NR}^{k+1}, \sigma^{k+1}, \ldots, x_{NR}^l, \sigma^l, x_{NR}^k)$, where $x_{NR}^p = (x_N^p, x_R^p)$, $p \in \{k, \ldots, l\}$ $(l \geq k > 0)$ such that $x_R^j = (x, R)$, $\forall j \in \{k, k+1, \ldots, l\}$, and $\exists q \in \{k, k+1, \ldots, l\}$ for which $\sigma^q \in \Sigma_{dil}$.*

R2. *there exists in V_{FR} a cyclic path $cl = (x_{FR}^k, \sigma^k, x_{FR}^{k+1}, \sigma^{k+1}, \ldots, x_{FR}^l, \sigma^l, x_{FR}^k)$, where $x_{FR}^p = (x_F^p, x_R^p)$, $p \in \{k, \ldots, l\}$ $(l \geq k > 0)$ such that $x_R^j = (x, R)$, $\forall j \in \{k, k+1, \ldots, l\}$, and $\exists q \in \{k, k+1, \ldots, l\}$ such that $x_F^q = (x, F)$, and $\exists z \in \{k, k+1, \ldots, l\}$ for which $\sigma^z \in \Sigma_{dil}$.*

L_{dil} is not FR-diagnosable with respect to projection $P_{dil,o}$ and Σ'_{isf}, if and only if at least one of the following conditions holds true:

FR1. *there exists in V_{NR} a cyclic path $cl = (x_{NR}^k, \sigma^k, x_{NR}^{k+1}, \sigma^{k+1}, \ldots, x_{NR}^l, \sigma^l, x_{NR}^k)$, where $x_{NR}^p = (x_N^p, x_R^p)$, $p \in \{k, \ldots, l\}$ $(l \geq k > 0)$, in which, $\exists j \in \{k, k+1, \ldots, l\}$ such that $[(x_R^j = (x, R)) \vee (x_R^j = (x, F))] \wedge (\sigma^j \in \Sigma_{dil})$.*

FR2. *there exists in V_{NF} a cyclic path $cl = (x_{NF}^k, \sigma^k, x_{NF}^{k+1}, \sigma^{k+1}, \ldots, x_{NF}^l, \sigma^l, x_{NF}^k)$, where $x_{NF}^p = (x_N^p, x_F^p)$, $p \in \{k, \ldots, l\}$ $(l \geq k > 0)$, in which $\exists j \in \{k, k+1, \ldots, l\}$ such that $[(x_F^j = (x, F)) \vee (x_F^j = (x, R))] \wedge (\sigma^j \in \Sigma_{dil})$.*

Proof. We will only prove the necessary and sufficient condition for F-diagnosability. The proofs of the conditions for R-diagnosability and FR-diagnosability follow the same steps.

($\Rightarrow$) Suppose that there exists in V_{NF} a cyclic path, $cl = (x_{NF}^k, \sigma^k, x_{NF}^{k+1}, \sigma^{k+1}, \ldots, x_{NF}^l, \sigma^l, x_{NF}^k)$, such that $\forall j \in \{k, k+1, \ldots, l\}$,

$x_F^j = (x, F)$, and $\exists q \in \{k, k+1, \ldots, l\}$ such that $\sigma^q \in \Sigma_{dil}$. Thus, there exists a sequence $\upsilon_{NF} = u_{NF}t_{NF} \in L(V_{NF})$, where $t_{NF} = (\sigma^k\sigma^{k+1}\ldots\sigma^l)^p$, $p \in \mathbb{N}$. In accordance with Lemma 1, associated with trace υ_{NF}, there exist a trace $t_{N\rho} \in L(G_N^\rho)$, where $t_{N\rho} = \rho_N(t_N)$, and a trace $t_F \in L(G_F)$, such that $P_{dil,o}(t_N) = P_{dil,o}(t_F)$. Since $x_F^j = (x, F)$ for all $j \in \{k, k+1, \ldots, l\}$, and $\sigma^q \in \Sigma_{dil}$, for at least one $q \in \{k, k+1, \ldots, l\}$, then $t_F = t_F' t_F''$ where $t_F' \in \Psi(\Sigma_{isf}')$ and t_F'' is an arbitrarily long length trace such that $\sigma^q \in t_F''$ and $\Sigma_{isf} \notin t_F''$. Thus, according to Definition 4, L_{dil} is not F-diagnosable.

Suppose now that there exists in V_{FR} a cyclic path, $cl = (x_{FR}^k, \sigma^k, x_{FR}^{k+1}, \sigma^{k+1}, \ldots, x_{FR}^l, \sigma^l, x_{FR}^k)$, such that $\forall j \in \{k, k+1, \ldots, l\}$, $x_F^j = (x, F)$, where $x_{FR}^j = (x_F^j, x_R^j)$, and $\exists q \in \{k, k+1, \ldots, l\}$ such that $x_R^q = (x, R)$, and $\exists z \in \{k, k+1, \ldots, l\}$ such that $\sigma^z \in \Sigma_{dil,F}$. Thus, there exists a sequence $\upsilon_{FR} = u_{FR}t_{FR} \in L(V_{FR})$, where $t_{FR} = (\sigma^k\sigma^{k+1}\ldots\sigma^l)^p$, $p \in \mathbb{N}$. In accordance with Lemma 1, associated with trace υ_{FR}, there exist a trace $t_{F\rho} \in L(G_F^\rho)$, where $t_{F\rho} = \rho_F(t_F)$, and a trace $t_R \in L(G_R)$, such that $P_{dil,o}(t_F) = P_{dil,o}(t_R)$. Since $\forall j \in \{k, k+1, \ldots, l\}$, $x_F^j = (x, F)$, and $\exists z \in \{k, k+1, \ldots, l\}$ such that $\sigma^z \in \Sigma_{dil,F}$, then t_F is an unrecovered faulty sensor trace, *i.e.*, $t_F = t_F' t_F''$, where $t_F' \in \Psi(\Sigma_{isf}')$, and t_F'' is an arbitrarily long length trace such that $\Sigma_{isf} \notin t_F''$. Moreover, since $x_R^q = (x, R)$ for at least one $q \in \{k, k+1, \ldots, l\}$, then t_R is not a recovered sensor trace. Thus, according to Definition 4, L_{dil} is not F-diagnosable.

($\Leftarrow$) Suppose that L_{dil} is not F-diagnosable with respect to projection $P_{dil,o}$ and Σ_{isf}'. Thus, there exist an unrecovered faulty sensor trace $s_F = st \in L(G_F)$, where $s \in \Psi(\Sigma_{isf}')$, and $\Sigma_{isf} \notin t$, $|t| > n$, $\forall n \in \mathbb{N}$, and a trace $\omega \in L_{dil}$, that does not satisfy the conditions to be an unrecovered faulty sensor trace, such that $P_{dil,o}(st) = P_{dil,o}(\omega)$.

Since ω is not an unrecovered faulty sensor trace, ω must belong to the language generated by G_N or/and G_R. In accordance with Lemma 1, all traces of two automata that have the same projection can be associated with a trace in the language generated by the parallel composition of the automata. Thus, associated with traces s_F and ω, there exists a trace υ in the language generated by V_{NF} or/and V_{FR}.

Let us assume that $\upsilon \in L(V_{NF})$ (the case when $\upsilon \in L(V_{FR})$ can be addressed in a similar way). In this case, the only common events are those in Σ_o. Let us define the following projections: (i) $P_{N\rho} : (\Sigma_{dil,N} \cup \Sigma_{dil})^* \rightarrow \Sigma_{dil,N}^*$, and (ii) $P_F : (\Sigma_{dil,N} \cup \Sigma_{dil})^* \rightarrow \Sigma_{dil}^*$. We will split the proof in two parts. *Part* 1: we show that there exists an arbitrarily long length trace $\upsilon \in L(V_{NF})$ such that $P_{N\rho}(\upsilon) = \rho_N(\omega)$ and $P_F(\upsilon) = st$. *Part* 2: we prove that there exists a cyclic path cl, associated with trace υ, satisfying condition **F1**.

In order to prove *Part* 1, let us suppose that there exists a state in V_{NF}, $x_{NF} = (x_N, x_F)$, reachable from the initial state $x_{0,NF}$ after the execution of a trace $u \in L(V_{NF})$, where $u \in \overline{\upsilon}$. Notice that such a state always exists since u can be the empty trace, in which case, $x_{NF} = x_{0,NF}$. Now, let $\sigma \in \Sigma_{dil}$ be a feasible event of x_F, such that $P_F(u)\sigma \in \overline{st}$, and consider the problem of finding a state $\hat{x}_{NF}$ of V_{NF}, reachable from x_{NF}, that has σ as a feasible event. Two cases are possible: (a) $\sigma \in \Sigma_o$; (b) σ is an unobservable event of Σ_{dil}; notice that in this case σ cannot be a renamed event of $\Sigma_{dil,N}$. If case (a) holds true, then σ will be a feasible event of x_{NF} if, and only if, it is feasible for the corresponding state of G_N. Since $P_{dil,o}(st) = P_{dil,o}(\omega)$, there exist a trace $\omega_N \in (\Sigma_{dil,N} \setminus \Sigma_o)^*$ and a state $\hat{x}_{NF} = (\hat{x}_N, x_F)$ such that: (i) $\sigma \in \Gamma(\hat{x}_{NF})$ and (ii) $f_{NF}(x_{NF}, \omega_N) = \hat{x}_{NF}$. When σ satisfies (b) *i.e.*, $\sigma \in \Sigma_{dil} \setminus \Sigma_o$, then, since σ is a private event of G_F, we may conclude that σ is already feasible for $x_{NF} = (x_F, x_N)$. Thus, there exists a trace υ associated with st such that $\upsilon \in P_F^{-1}(st) \cap P_{N_\rho}^{-1}(\omega)$, which implies that $P_F(\upsilon) = st$ and $P_{N_\rho}(\upsilon) = \omega$.

In order to prove *Part* 2, let us assume, without loss of generality, that $s = P_F(s')$ and $t = P_F(t')$. Therefore, t' is also an arbitrarily long length trace of $L(V_{NF})$. Notice that V_{NF} is a finite state automaton,which implies that $\exists n \in \mathbb{N} : |X_{NF}| = n$. Therefore, for $|t'| \geq n+1$, there must exist a cyclic path cl of V_{NF} whose second components are faulty states. Any cyclic path cl in V_{NF} must satisfy one of the following three cases: (i) cl is associated with two cyclic paths, one in G_F and another one in G_N; (ii) cl is associated with a cyclic path in G_F only, *i.e.*, with no cyclic path in G_N; (iii) cl is associated with a cyclic path in G_N only, *i.e.*, with no cyclic path in G_F. If condition (iii) holds true, then all states of cl will have the same first component $x_N \in X_N$. Therefore $\nexists \sigma \in \Sigma_{dil}$ such that σ is an event of the cyclic path cl, which contradicts *Part* 1 of the proof. On the other hand, when either condition (i) or (ii) holds true, then, as shown in the proof of *Part* 1, $\exists \sigma \in \Sigma_{dil}$ in the cyclic path cl, which concludes the proof. ■

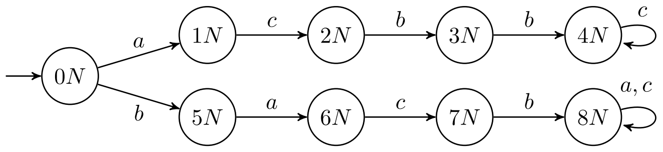


Fig. 7. Automaton G_N.

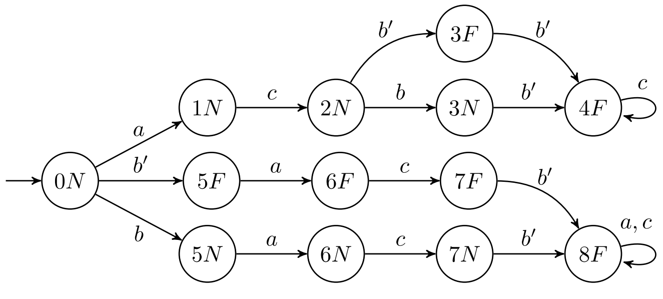


Fig. 8. Automaton G_F.

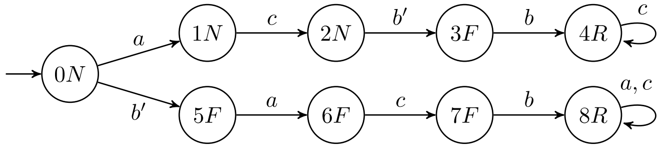


Fig. 9. Automaton G_R.

Remark 3 (*Computational Complexity Analysis*)**.** According to Moreira, Basilio, and Cabral (2016); Moreira et al. (2011), the computational complexity for the construction of verifiers V_{NF}, V_{NR}, and V_{FR} constructed in accordance with Algorithm 1 is $O(|X|^2|\Sigma|)$. Since only three verifiers are built in Algorithm 1, its computational complexity is also $O(|X|^2|\Sigma|)$.

Example 3. We will illustrate the results of this section with automaton G_2 depicted in Fig. 5, already considered in Example 2. We will assume, as in Example 2, that $\Sigma_o = \{b, c\}$, $\Sigma_{uo} = \{a\}$ and $\Sigma_{isf} = \{b\}$. Therefore, $\Sigma_{dil} = \{a, b, c, b'\}$, $\Sigma_{dil,N} = \{a_N, b, c\}$ and $\Sigma_{dil,F} = \{a_F, b, c, b_F'\}$.

In order to verify if L_{dil} is diagnosable with respect to intermittent sensor faults using verifiers, we need, according to Algorithm 1, to build three verifier automata: $V_{NF} = G_N^\rho \parallel G_F$, $V_{NR} = G_N^\rho \parallel G_R$, and $V_{FR} = G_F^\rho \parallel G_R$, where G_N^ρ, G_F^ρ are obtained by renaming the transitions of G_N and G_F, respectively, according to the renaming function defined in Eq. (4) and (5). It is therefore, necessary, to build from G_{dil}^ℓ, automata G_N, G_F and G_R (shown in Figs. 7–9, respectively) in accordance with Steps 2, 3 and 4 of Algorithm 1. After that, applying, according to Step 5 the renaming functions ρ_N and ρ_F to the

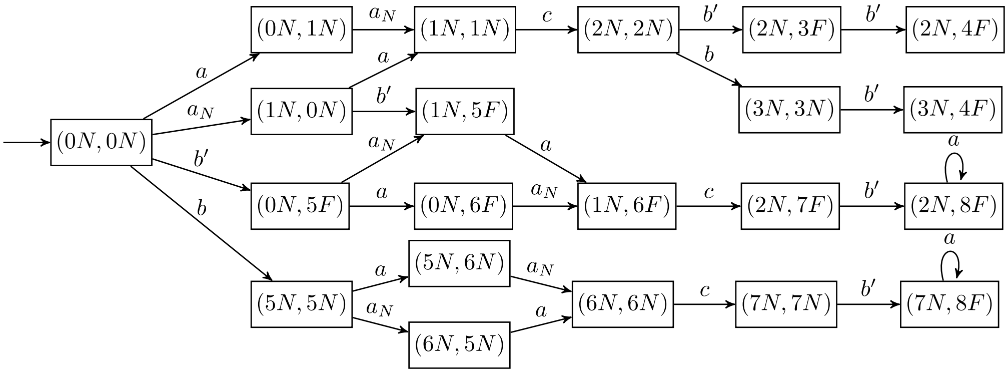


Fig. 10. Verifier V_{NF}.

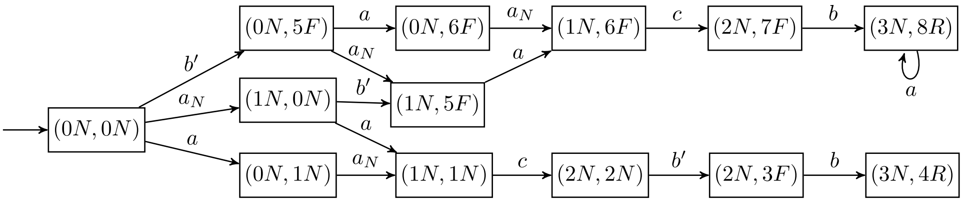


Fig. 11. Verifier V_{NR}.

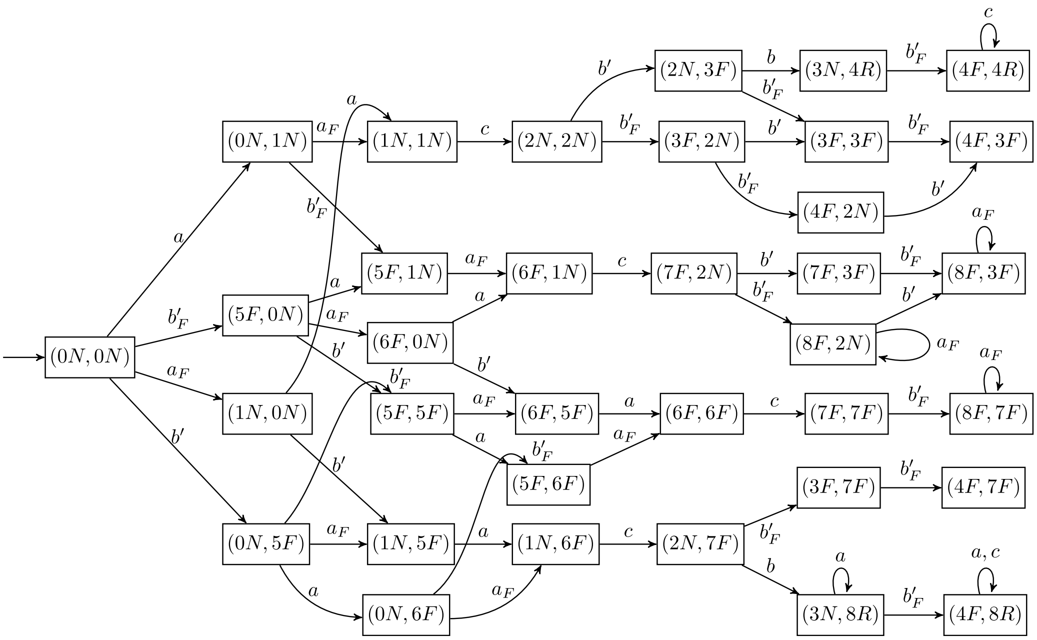


Fig. 12. Verifier V_{FR}.

events of automata G_N and G_F, and performing the parallel compositions given in Step 6, we obtain automata V_{NF}, V_{NR} and V_{FR} depicted in Figs. 10–12, respectively.

Let us now analyze the intermittent sensor fault diagnosability according to Theorem 2.

(1) F-diagnosability. Let us, initially, search for cyclic paths in automata V_{NF} formed with states labeled as $\{(\cdot, N), (\cdot, F)\}$ with at least one transition labeled with an event in Σ_{dil}. Notice that cyclic paths $cl_1 = \{(2N, 8F), a, (2N, 8F)\}$ and $cl_2 = \{(7N, 8F), a, (7N, 8F)\}$ in V_{NF} satisfy condition **F1** of Theorem 2, which implies that L_{dil} is not F-diagnosable. Notice that, although, the decision regarding F-diagnosability has already been made, let us also search for cyclic paths in V_{FR} formed with states whose first components are labeled as $(\cdot, F)$ and with at least one state whose second component is labeled as $(\cdot, R)$ and one event in $\Sigma_{dil,F}$. Notice that two cyclic paths satisfy such requirements: $cl_3 = \{(4F, 8R), c, (4F, 8R)\}$ and $cl_4 = \{(4F, 4R), c, (4F, 4R)\}$. Thus, according to condition **F2** of Theorem 2, we can conclude that L_{dil} is not F-diagnosable.

Regarding the traces that cause the loss of F-diagnosability, notice that, for cyclic path cl_1, it is straightforward to obtain trace $s_1 = b'aa_Ncb'a^n, n \in \mathbb{N}$, from the state diagram of V_{NF}, from which, the normal and faulty traces, $s_{1,N} = ac$ and $s_{1,F} = b'acb'a^n$, respectively, can be formed. It is not difficult to see that $P_{dil,o}(s_{1,N}) = P_{dil,o}(s_{1,F}) = c$. Following the same reasoning, traces $s_{2,N} = bac$ and $s_{2,F} = bacb'a^n$ that satisfy $P_{dil,o}(s_{2,N}) = P_{dil,o}(s_{2,F}) = bc$ are obtained from cyclic path cl_2. For cyclic path cl_3, we can obtain trace $s_3 = b'a_Facba^mb'_Fc^n, m, n \in \mathbb{N}$, which lead to traces $s_{3,F} = acbb'c^n$

and $s_{3,R} = b'acba^m c^n$ that satisfy $P_{dil,o}(s_{3,F}) = P_{dil,o}(s_{3,R}) = cbc^n$. Finally, it can be checked that traces $s_{4,F} = acb'bc^n$ and $s_{4,R} = b'acba^m c^n$, which satisfy $P_{dil,o}(s_{4,F}) = P_{dil,o}(s_{4,R}) = cbc^n$, can be obtained from cyclic path cl_4.

(2) R-diagnosability. In this case we must search for cyclic paths in automaton V_{NR} formed with states whose second components are labeled as $(\cdot, R)$ with, at least, one event in Σ_{dil}, and for cyclic paths in automaton V_{FR} formed with states whose second components are all labeled as $(\cdot, R)$ with, at least, one state whose first component is labeled as $(F, \cdot)$ and at least one event of the cyclic path is in Σ_{dil}. Notice that cyclic paths $\{(3N, 8R), a, (3N, 8R)\}$ of V_{NR} and $\{(4F, 4R), c, (4F, 4R)\}$, $\{(4F, 8R), a, (4F, 8R)\}$ and $\{(4F, 8R), c, (4F, 8R)\}$ of V_{FR} satisfy conditions **R1** and **R2** of Theorem 2, which implies that L_{dil} is not R-diagnosable, as was verified in Example 2. The traces that cause the loss of R-diagnosability can be found in a similar manner as in the F-diagnosability analysis above.

(3) FR-diagnosability. In this case, it is necessary to search for cyclic paths in automata V_{NR} and V_{NF} whose second components of all states are labeled either as $(\cdot, F)$ or $(\cdot, R)$ with at least one transition labeled with one event in Σ_{dil}. It is clear that cyclic paths $\{(3N, 8R), a, (3N, 8R)\}$ of V_{NR} and $\{(2N, 8F), a, (2N, 8F)\}$ and $\{(7N, 8F), a, (7N, 8F)\}$ of V_{NF} satisfy conditions **FR1** and **FR2**, from which, we may conclude that L_{dil} is not FR-diagnosable.

6. Conclusion and future works

We addressed in this paper the problem of diagnosing intermittent sensor faults and presented necessary and sufficient conditions for intermittent sensor fault diagnosability based on both diagnoser and verifier automata. An important aspect of the approach presented here is that cyclic paths formed with unobservable events only are allowed, as opposed to Contant et al. (2004) and other previously proposed approaches, where such cyclic paths are precluded by assumption.

Although we require here that the control and diagnosis systems under consideration be tolerant to sensor faults, one could attempt to extend these results in future work to apply to control and diagnosis systems which are not necessarily tolerant to arbitrary sensor faults. Such extensions could be used to prevent situations (in control or diagnosis systems at least) where sensor faults have been reported as the cause of several accidents that led to either material or life losses.

Acknowledgments

We would like to thank the anonymous reviewers for their comments and suggestions which helped improve the presentation and readability of the paper, and, specially, to one of the reviewers for his/her detailed and insightful review.

References

Alves, M.V.S., Basilio, J.C., da Cunha, A.E.C., Carvalho, L.K., & Moreira, M.V. (2014). Robust supervisory control against intermittent loss of observations. In *Proceedings of 12th IFAC/IEEE workshop on discrete event systems*. Cachan, France (pp. 294–299).

Athanasopoulou, C., & Chatziathanasiou, V. (2009). Intelligent system for identification and replacement of faulty sensor measurements in thermal power plants (IPPAMAS: Part 1). *Expert Systems with Applications*, *36*(5), 8750–8757.

Basilio, J.C., & Lafortune, S. (2009). Robust codiagnosability of discrete event systems. In *Proc. of the American control conference*. St. Louis, Missouri (pp. 2202–2209).

Basilio, J. C., Lima, S. T. S., Lafortune, S., & Moreira, M. V. (2012). Computation of minimal event bases that ensure diagnosability. *Discrete Event Dynamic Systems: Theory and Applications*, *22*(3), 249–292.

Carvalho, L. K., Basilio, J. C., & Moreira, M. V. (2012). Robust diagnosis of discrete-event systems against intermittent loss of observations. *Automatica*, *48*(9), 2068–2078.

Carvalho, L. K., Moreira, M. V., Basilio, J. C., & Lafortune, S. (2013). Robust diagnosis of discrete-event systems against permanent loss of observations. *Automatica*, *49*(1), 223–231.

Cassandras, C. G., & Lafortune, S. (2008). *Introduction to discrete event systems* (2nd ed.). New York: Springer.

Clark, R. N. (1978). Instrument fault detection. *IEEE Transactions on Aerospace and Electronic Systems*, *14*(3), 456–465.

Contant, O., Lafortune, S., & Teneketzis, D. (2004). Diagnosis of intermittent faults. *Discrete Event Dynamic Systems: Theory and Applications*, *14*(2), 171–202.

da Silva, J. C., Saxena, A., Balaban, E., & Goebel, K. (2012). A knowledge-based system approach for sensor fault modeling, detection and mitigation. *Expert Systems with Applications*, *39*(12), 10977–10989.

Ding, E. L., Fennel, H., & Ding, S. X. (2004). Model-based diagnosis of sensor faults esp systems. *Control Engineering Practice*, *12*, 847–856.

Frank, P. M. (1990). Fault-diagnosis in dynamic-systems using analytical and knowledge-based redundancy - a survey and some new results. *Automatica*, *26*(3), 459–474.

Jiang, S., Huang, Z., Chandra, V., & Kumar, R. (2001). A polynomial algorithm for testing diagnosability of discrete-event systems. *IEEE Transactions on Automatic Control*, *46*, 1318–1321.

Lunze, J., & Schröder, J. (2004). Sensor and actuator fault diagnosis of systems with discrete inputs and outputs. *IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics*, *34*(2), 1096–1107.

Moreira, M. V., Basilio, J. C., & Cabral, F. G. (2016). "Polynomial time verification of decentralized diagnosability of discrete event systems" vs. "Decentralized failure diagnosis of discrete event systems": a critical appraisal. *IEEE Transactions on Automatic Control*, *61*(1), 178–181.

Moreira, M. V., Jesus, T. C., & Basilio, J. C. (2011). Polynomial time verification of decentralized diagnosability of discrete event systems. *IEEE Transactions on Automatic Control*, *56*(7), 1679–1684.

Qiu, W., & Kumar, R. (2006). Decentralized failure diagnosis of discrete event systems. *IEEE Transactions on Systems, Man and Cybernetics, Part A*, *36*(2), 384–395.

Ramadge, P. J., & Wonham, W. M. (1989). The control of discrete-event systems. *Proceedings of the IEEE*, *77*, 81–98.

Rohloff, K.R. (2005). Sensor failure tolerant supervisory control. In *Proc. of joint 2005 European control conference and 44th IEEE conference on decision and control*. Seville, Spain (pp. 3493–3498).

Sampath, M., Sengupta, R., Lafortune, S., Sinnamohideen, K., & Teneketzis, D. (1995). Diagnosability of discrete-event systems. *IEEE Transactions on Automatic Control*, *40*, 1555–1575.

Sanchez, A. M., & Montoya, F. J. (2006). Safe supervisory control under observability failure. *Discrete Event Dynamic Systems: Theory and Applications*, *16*(4), 493–525.

Thorsley, D., Yoo, T.-S., & Garcia, H. (2008). Diagnosability of stochastic discrete-event systems under unreliable observations. In *Proc. of the 2008 American control conference*. Seatle, WA (pp. 1158–1365).

Ushio, T., & Takai, S. (2009). Supervisory control of discrete event systems modeled by mealy automata with nondeterministic output functions. In *American control conference*. St. Louis, MO (pp. 4260–4265).

Xu, S., & Kumar, R. (2009). Discrete event control under nondeterministic partial observation. In *IEEE international conference on automation science and engineering*. Bangalore, India, (pp. 127–132).

Yoo, T.-S., & Lafortune, S. (2002). Polynomial-time verification of diagnosability of partially observed discrete-event systems. *IEEE Transactions on Automatic Control*, *47*(9), 1491–1495.

Lilian K. Carvalho was born on March, 11, 1979 in São Paulo, Brazil. She received the Electronic Engineer degree, the M.Sc. degree and the D.Sc. degree in Control from the Federal University of Rio de Janeiro, Rio de Janeiro, Brazil, in 2003, 2005 and 2011, respectively. Since 2011, she has been an Associate Professor at the Department of Electrical Engineering at the Federal University of Rio de Janeiro. From September, 2014, to December, 2015, she spent a sabbatical year at the University of Michigan, Ann Arbor. Her main interests are fault diagnosis of discrete-event systems, cyber-attacks and the development of control laboratory techniques.

Marcos V. Moreira was born on May, 11, 1976 in Rio de Janeiro, Brazil. He received the Electrical Engineer degree, the M.Sc. degree and the D.Sc. degree in Control from the Federal University of Rio de Janeiro, Rio de Janeiro, Brazil, in 2000, 2002 and 2006, respectively. Since 2007, he has been an Associate Professor at the Department of Electrical Engineering at the Federal University of Rio de Janeiro. His main interests are robust failure diagnosis of discrete-event systems, cyber-attacks, smart grids, and the development of control laboratory techniques.

João Carlos Basilio was born on March 15, 1962 in Juiz de Fora, Brazil. He received the Electrical Engineering degree in 1986 from the Federal University of Juiz de Fora, Juiz de Fora, Brazil, the M.Sc. degree in Control from the Military Institute of Engineering, Rio de Janeiro, Brazil, in 1989, and the Ph.D. degree in Control from Oxford University, Oxford, UK, in 1995. He began his career in 1990 as an Assistant Lecturer at the Department of Electrical Engineering of the Federal University of Rio de Janeiro, Rio de Janeiro, Brazil, and, since 2014, has been a Full Professor in Control at the same department. He served as Academic Chair for the Control and Automation Engineering course of Polytechnic School of the Federal University of Rio de Janeiro from January, 2005, to December, 2006, as Chair for the Electrical Engineering Postgraduation Program (COPPE) from January, 2008, to February, 2009, as Head of the Electrical Engineering Department, from May, 2012 to February, 2014, and since 2014 he has been the Dean of Polytechnic School. From September, 2007, to December, 2008, he spent a sabbatical leave at the University of Michigan, Ann Arbor, and was an Invited Professor of École Centrale of Lille, University of Lille, France, during September, 2016. His current interests are fault diagnosis and supervisory control of discrete-event systems. Prof. Basilio is the recipient of the Correia Lima Medal.