Diagnosis using labeled Petri nets: faults may either be silent or undistinguishable events

Maria Paola Cabasino, Alessandro Giua, Carla Seatzu
Department of Electrical and Electronic Engineering, University of Cagliari
Piazza D'Armi, 09123 Cagliari, Italy. E-mail:{cabasino,giua,seatzu}@diee.unica.it.

October 26, 2010

Abstract

In this paper we generalize our previous results on the diagnosis of discrete event systems using Petri nets based on the notions of minimal explanations and basis markings. In particular, in our previous submissions we assumed that fault events only correspond to silent transitions, and there also exist silent transitions modeling regular behavior. Moreover, labeled transitions model regular behavior but they introduce a further form of nondeterminism because in general the same label can be shared by two or more transitions.

Now, we assume that fault events can also be modeled by labeled transitions that share the same label with other fault transitions (e.g., belonging to different fault classes) and with other transitions modeling regular behavior. This requires redefining the main concepts on which our approach is based on and adapting the algorithms for diagnosis.

Published as: M.P. Cabasino, A. Giua, C. Seatzu, "Diagnosis using labeled Petri nets: faults may either be silent or undistinguishable events," *CASE10: 6th IEEE Conference on Automation Science and Engineering* (Toronto, ON, Canada), Aug 2010.

This work has been partially supported by the European Communitys Seventh Framework Programme under project DISC (Grant Agreement n. INFSO-ICT-224498).

1 Introduction

In this paper we focus on the problem of deriving an efficient approach for the fault diagnosis of discrete event systems (DES). This problem has been extensively investigated in the last decades and several original theoretical approaches have been proposed both using automata [3, 6, 10, 12, 13] and Petri nets (PNs) [1, 2, 4, 5, 7–9].

The main feature of our procedure [4, 5, 8] is the concept of *basis marking* that allows one to represent the reachability space in a more compact manner, only enumerating a subset of its markings.

In our previous papers [5, 8] we presented an approach for on-line diagnosis for PNs where fault transitions are only modeled by silent transitions, but there are also other silent transitions that model regular behavior. In [4] we also dealt with labeled PNs and this enabled us to also take into account a new source of nondeterminism originating from the fact that different transitions modeling regular behavior may share the same label. Both approaches apply to all net systems whose unobservable subnet is acyclic.

In this paper we consider a more general setting and assume that fault transitions are not necessarily silent, but they can also be labeled observable transitions that share the same label with transitions belonging to different fault classes and/or with transitions modeling a regular behavior. As for the previous approaches we require that the unobservable subnet of the considered net system is acyclic.

This requires to redefine the four diagnosis states previously defined in [4], each one corresponding to a different degree of alarm, and the procedure to compute the actual diagnosis state given the current observation.

Finally we show that, as in the previous less general case [4, 5, 8], if the net system is bounded, the most burdensome part of the procedure can be moved off-line defining a particular graph, that we call *Basis Reachability Graph*.

2 Notation

In this section we recall the formalism used in the paper. For more details on PNs we refer to [11].

A *Place/Transition net* (P/T net) is a structure $N = (P, T, Pre, Post)$, where P is a set of m places; T is a set of n transitions; $Pre : P \times T \to \mathbb{N}$ and $Post : P \times T \to \mathbb{N}$ are the *pre*– and *post*– incidence functions that specify the arcs; $C = Post - Pre$ is the incidence matrix.

A *marking* is a vector $M : P \to \mathbb{N}$ that assigns to each place of a P/T net a nonnegative integer number of tokens, represented by black dots. We denote $M(p)$ the marking of place p. A P/T *system* or *net system* $\langle N, M_0 \rangle$ is a net N with an initial marking M_0. A transition t is enabled at M iff $M \geq Pre(\cdot\,, t)$ and may fire yielding the marking $M' = M + C(\cdot\,, t)$. We write $M\ [\sigma\rangle$ to

denote that the sequence of transitions $\sigma = t_{j_1} \cdots t_{j_k}$ is enabled at M, and we write $M\ [\sigma\rangle\ M'$ to denote that the firing of σ yields M'. We also write $t \in \sigma$ to denote that a transition t is contained in σ. The set of all sequences that are enabled at the initial marking M_0 is denoted $L(N, M_0)$, i.e., $L(N, M_0) = \{\sigma \in T^* \mid M_0[\sigma\rangle\}$.

Given a sequence $\sigma \in T^*$, we call $\pi : T^* \to \mathbb{N}^n$ the function that associates to σ a vector $y \in \mathbb{N}^n$, named the *firing vector* of σ. In particular, $y = \pi(\sigma)$ is such that $y(t) = k$ if the transition t is contained k times in σ.

A marking M is *reachable* in $\langle N, M_0\rangle$ iff there exists a firing sequence σ such that $M_0\ [\sigma\rangle\ M$. The set of all markings reachable from M_0 defines the *reachability set* of $\langle N, M_0\rangle$ and is denoted $R(N, M_0)$.

A PN having no directed circuits is called *acyclic*. A net system $\langle N, M_0\rangle$ is *bounded* if there exists a positive constant k such that, for $M \in R(N, M_0)$, $M(p) \leq k$.

A *labeling function* $\mathcal{L} : T \to E \cup \{\varepsilon\}$ assigns to each transition $t \in T$ either a symbol from a given alphabet L or the empty string ε.

3 Problem Setting

In this paper we solve the diagnosis problem for labeled Petri nets where faults can be modeled either by unobservable transitions or by undistinguishable events, i.e., the same label may be assigned to fault transitions and to transitions modeling regular behavior.

We denote as T_o the set of transitions labeled with a symbol in L. Transitions in T_o are called *observable* because when they fire their label can be observed. We assume that the same label $l \in L$ can be associated to more than one transition. In particular, two transitions $t_1, t_2 \in T_o$ are called *undistinguishable* if they share the same label, i.e., $\mathcal{L}(t_1) = \mathcal{L}(t_2)$. The set of transitions sharing the same label l are denoted as T_l. The set of observable transitions is partitioned into two subsets, namely $T_o = T_{o,f} \cup T_{o,reg}$ where $T_{o,f}$ includes fault transitions that are observable, while $T_{o,reg}$ includes all transitions relative to observable and regular events.

We denote as T_u the set of transitions whose label is ε, i.e., $T_u = \{t \in T \mid \mathcal{L}(t) = \varepsilon\}$. Transitions in T_u are called *unobservable* or *silent*. The set of unobservable transitions is partitioned into two subsets, namely $T_u = T_{u,f} \cup T_{u,reg}$ where $T_{u,f}$ includes fault transitions, while $T_{u,reg}$ includes all transitions relative to unobservable but regular events.

The set of fault transitions $T_f = T_{u,f} \cup T_{o,f}$ is further partitioned into r different subsets T_f^i, where $i = 1, \ldots, r$, that model the different fault classes.

In the following we denote as C_u (C_o, $C_{o,f}$) the restriction of the incidence matrix to T_u (T_o, $T_{o,f}$) and denote as n_u, n_o and $n_{o,f}$, respectively, the cardinality of the sets T_u, T_o and $T_{o,f}$. Moreover, given a sequence $\sigma \in T^*$, $P_u(\sigma)$, resp., $P_o(\sigma)$, $P_{o,f}(\sigma)$, denotes the projection of σ over T_u, resp., T_o, $T_{o,f}$.

4 Characterization of the set of consistent markings

Let $w = P_o(\sigma)$ be the observed word of events associated to a sequence σ.

Definition 4.1 [4] Let $\langle N, M_0\rangle$ be a labeled net system with labeling function $\mathcal{L} : T \to E \cup \{\varepsilon\}$, where $N = (P, T, Pre, Post)$ and $T = T_o \cup T_u$. Let $w \in L^*$ be an observed word. We define

$$\mathcal{S}(w) = \{\sigma \in L(N, M_0) \mid P_o(\sigma) = w\}$$

the set of firing sequences *consistent* with $w \in L^*$, and

$$\mathcal{C}(w) = \{M \in \mathbb{N}^m \mid \exists\, \sigma \in \mathcal{S}(w) \ \wedge M_0[\sigma\rangle M\}$$

the set of markings *consistent* with $w \in L^*$. ■

To solve a diagnosis problem, it is essential to be able to compute the set of sequences and markings consistent with a given observation w. In this section we provide a formalism that allows one to characterize these sets without resorting to explicit enumeration. Our approach is based on the notions of minimal explanations and basis markings that are introduced in the following two subsections. In the rest of this section we recall some definitions and results already presented in [4, 5] adapting them to the new problem setting.

4.1 Minimal explanations and minimal e-vectors

Definition 4.2 *[5]* Given a marking M and an observable transition $t \in T_o$, we define

$$\Sigma(M, t) = \{\sigma \in T_u^* \mid M[\sigma\rangle M',\ M' \geq Pre(\cdot, t)\}$$

the set of *explanations* of t at M, and $Y(M, t) = \pi(\Sigma(M, t))$ the *e-vectors* (or *explanation vectors*), i.e., firing vectors associated to the explanations. ■

Thus $\Sigma(M, t)$ is the set of unobservable sequences whose firing at M enables t. Among the above sequences we want to select those whose firing vector is minimal. The firing vector of these sequences are called *minimal e-vectors*.

Definition 4.3 *[5]* Given a marking M and a transition $t \in T_o$, we define

$$\Sigma_{\min}(M, t) = \{\sigma \in \Sigma(M, t) \mid \nexists\, \sigma' \in \Sigma(M, t) : \pi(\sigma') \lneqq \pi(\sigma)\}$$

the set of *minimal explanations* of t at M, and we define

$$Y_{\min}(M, t) = \pi(\Sigma_{\min}(M, t))$$

the corresponding set of *minimal e-vectors*. ■

In the case of labeled PNs what we observe are symbols in L. Thus, it is useful to compute the following sets.

Definition 4.4 *[4]* Given a marking M and an observation $l \in L$, we define the set of *minimal explanations of l at M* as

$$\hat{\Sigma}_{\min}(M,l) = \cup_{t \in T_l} \cup_{\sigma \in \Sigma_{\min}(M,t)} (t,\sigma),$$

i.e., the set of pairs (transition labeled l, corresponding minimal explanation), and we define the set of *minimal e-vectors of l at M* as

$$\hat{Y}_{\min}(M,l) = \cup_{t \in T_l} \cup_{e \in Y_{\min}(M,t)} (t,e),$$

i.e., the set of pairs (transition labeled l, corresponding minimal e-vector). ■

4.2 Basis markings and j-vectors

Given a sequence of observed events $w \in L^*$, a basis marking M_b is a marking reached from M_0 with the firing of the observed word w and of all unobservable transitions whose firing is strictly necessary to enable w. Such a sequence of unobservable transitions is called *justification.*

Definition 4.5 Let $\langle N, M_0 \rangle$ be a net system with labeling function $\mathcal{L} : T \to E \cup \{\varepsilon\}$, where $N = (P, T, Pre, Post)$ and $T = T_o \cup T_u$. Let $w \in L^*$ be a given observation. We define

$$\begin{aligned} \hat{\mathcal{J}}(w) \quad &= \{\ (\sigma_o, \sigma_u),\ \sigma_o \in T_o^*,\ \mathcal{L}(\sigma_o) = w,\ \sigma_u \in T_u^* \ \mid \\ &\quad [\exists \sigma \in \mathcal{S}(w)\ :\ \sigma_o = P_o(\sigma),\ \sigma_u = P_u(\sigma)] \wedge \\ &\quad [\nexists \sigma' \in \mathcal{S}(w) :\ \sigma_o = P_o(\sigma'),\ \sigma'_u = P_u(\sigma') \wedge \\ &\qquad\qquad \pi(\sigma'_u) \lneq \pi(\sigma_u)]\} \end{aligned}$$

the set of pairs (sequence $\sigma_o \in T_o^*$ with $\mathcal{L}(\sigma_o) = w$, corresponding *justification* of w). ■

In simple words, $\hat{\mathcal{J}}(w)$ is the set of pairs whose first element is the sequence $\sigma_o \in T_o^*$ labeled w and whose second element is the corresponding sequence of unobservable transitions interleaved with σ_o whose firing enables σ_o and whose firing vector is minimal.

Definition 4.6 *[4]* Let $\langle N, M_0 \rangle$ be a net system with labeling function $\mathcal{L} : T \to E \cup \{\varepsilon\}$, where $N = (P, T, Pre, Post)$ and $T = T_o \cup T_u$. Let w be a given observation and $(\sigma_o, \sigma_u) \in \hat{\mathcal{J}}(w)$ be a generic pair (sequence of observable transitions labeled w; corresponding justification). The marking

$$M_b = M_0 + C_u \cdot y + C_o \cdot y', \qquad y = \pi(\sigma_u),\ \ y' = \pi(\sigma_o),$$

i.e., the marking reached firing σ_o interleaved with the justification σ_u, is called *basis marking* and y is called its *j-vector* (or *justification-vector*). ■

Obviously, because in general more than one justification exists for a word w (the set $\hat{\mathcal{J}}(w)$ is generally not a singleton), the basis marking may be not unique as well.

Definition 4.7 Let $\langle N, M_0 \rangle$ be a net system with labeling function $\mathcal{L} : T \to E \cup \{\varepsilon\}$, where

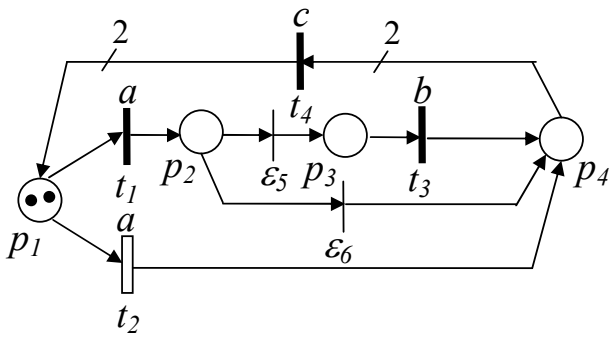

Figure 1: The PN system considered in Sections 4 to 6.

$N = (P, T, Pre, Post)$ and $T = T_o \cup T_u$. Let $w \in L^*$ be an observed word. We define

$$\begin{aligned}\bar{\mathcal{M}}(w) = \{(M, y, \gamma) \mid\ & (\exists \sigma \in \mathcal{S}(w)\ :\ M_0[\sigma\rangle M) \wedge \\ & (\exists (\sigma_o, \sigma_u) \in \hat{\mathcal{J}}(w)\ :\ \sigma_o = P_o(\sigma), \\ & \quad \sigma_u = P_u(\sigma),\ y = \pi(\sigma_u)) \wedge \\ & \sigma_{o,f} = P_{o,f}(\sigma),\ \gamma = \pi(\sigma_{o,f})\}\end{aligned}$$

where $\gamma = \pi(\sigma_{o,f})$ is called γ-*vector* of sequence $\sigma_{o,f}$. ■

In simple words the set $\bar{\mathcal{M}}(w)$ is the set of triples (basis marking, relative j-vector, relative γ-vector) that are *consistent* with $w \in L^*$. It keeps track of the basis markings that can be reached, of the firing vectors relative to sequences of unobservable transitions that have fired to reach them, and of the sequences of fault observable transitions that may have actually fired,

Example 4.8 Let us consider the PN in Fig. 1 representing the final stage of a production line that produces shoes. In this stage the nominal behavior of the net system expects that each shoe is moved by a robot in the input buffer of the polishing machine (event a, transition t_1), each shoe is polished (events ε_5, b) and each pair of shoes is put in a box (event c). A fault occurs when a shoe is not polished. It can occur either that the robot moves the shoe directly in the output buffer of the polishing machine (event a, transition t_2) or that the machine runs out of shoe polish (event ε_6).

Here $T_o = \{t_1, t_2, t_3, t_4\}$, $T_{o,reg} = \{t_1, t_3, t_4\}$, $T_{o,f} = \{t_2\}$, and $T_u = \{\varepsilon_5, \varepsilon_6\}$, $T_{u,reg} = \{\varepsilon_5\}$, $T_{u,f} = \{\varepsilon_6\}$, where for a better understanding unobservable transitions have been denoted ε_i rather than t_i. The labeling function is defined as follows: $\mathcal{L}(t_1) = \mathcal{L}(t_2) = a$, $\mathcal{L}(t_3) = b$ and $\mathcal{L}(t_4) = c$.

Let us assume $w = a$. In this case $\hat{\mathcal{J}}(w) = \{(t_1, \varepsilon), (t_2, \varepsilon)\}$, $\hat{Y}_{min}(M_0, w) = \{(t_1, \vec{0}), (t_2, \vec{0})\}$, $\sigma_{o,f,1} = P_{o,f}(t_1) = \varepsilon$, $\sigma_{o,f,2} = P_{o,f}(t_2) = t_2$, $\gamma_1 = \pi(\sigma_{o,f,1}) = [0]$ and $\gamma_2 = \pi(\sigma_{o,f,2}) = [1]$. The basis markings are respectively $M_b^1 = [1\ 1\ 0\ 0]^T$ and $M_b^2 = [1\ 0\ 0\ 1]^T$, thus $\bar{\mathcal{M}}(w) = \{(M_b^1, \vec{0}, 0), (M_b^2, \vec{0}, 1)\}$. ■

In the rest of the paper we assume that the following assumption holds:

(A) The unobservable subnet is acyclic.

Under assumption (A) the set $\bar{\mathcal{M}}(w)$ can be recursively constructed using a procedure similar to the one presented in [4].

Definition 4.9 Let $\langle N, M_0\rangle$ be a net system where $N = (P, T, Pre, Post)$ and $T = T_o \cup T_u$. Assume that the unobservable subnet is acyclic. Let $w \in T_o^*$ be an observed word. We denote

$$\mathcal{M}_{basis}(w) = \{M \in \mathbb{N}^m \mid \exists y \in \mathbb{N}^{n_u},\ \exists \gamma \in \mathbb{N}^{n_{o,f}},\ (M, y, \gamma) \in \bar{\mathcal{M}}(w)\}$$

the set of basis markings at w. Moreover, we denote as

$$\mathcal{M}_{basis} = \bigcup_{w \in T_o^*} \mathcal{M}_{basis}(w)$$

the set of all basis markings for any observation w. ■

Note that if the net system is bounded then the set $\mathcal{M}_{basis}$ is *finite* being the set of basis markings a subset of the reachability set.

Finally, the set of consistent markings in terms of basis markings can be characterized as follows.

Theorem 4.10 *[4]* Let us consider a net system $\langle N, M_0\rangle$ whose unobservable subnet is acyclic. For any $w \in L^*$ it holds that

$$\mathcal{C}(w) = \{M \in \mathbb{N}^m \mid M = M_b + C_u \cdot y\ : y \geq \vec{0},\ M_b \in \mathcal{M}_{basis}(w)\}.$$

5 Diagnosis using Petri nets

In this section we solve the diagnosis problem, i.e., the problem of identifying the occurrence of a fault given an observation, in the setting introduced in Section 3. The following definition introduces the notion of *diagnoser*.

Definition 5.1 A *diagnoser* is a function $\Delta : L^* \times \{T_f^1, T_f^2, \ldots, T_f^r\} \to \{0, 1, 2, 3\}$ that associates to each observation $w \in L^*$ and to each fault class T_f^i, $i = 1, \ldots, r$, a *diagnosis state*.

• $\Delta(w, T_f^i) = 0$ if for all $\sigma \in \mathcal{S}(w)$ and for all $t_f \in T_f^i$ it holds $t_f \notin \sigma$.

In such a case the i-th fault cannot have occurred, because none of the firing sequences consistent with the observation contains fault transitions of class i.

• $\Delta(w, T_f^i) = 1$ if:

(i) there exist $\sigma \in \mathcal{S}(w)$ and $t_f \in T_f^i$ such that $t_f \in \sigma$ but

(ii) for all $(\sigma_o, \sigma_u) \in \hat{\mathcal{J}}(w)$ and for all $t_f \in T_f^i$ it holds that $t_f \notin \sigma_u$ and $t_f \notin \sigma_o$.

In such a case a fault transition of class i may have occurred but it is neither contained in any justification of w, nor it is contained in a sequence of observed transitions labeled w.

• $\Delta(w, T_f^i) = 2$ if there exist $(\sigma_o, \sigma_u), (\sigma'_o, \sigma'_u) \in \hat{\mathcal{J}}(w)$ such that

(i) there exists $t_f \in T_f^i$ such that: either $t_f \in \sigma_u$ or $t_f \in \sigma_o$;

(ii) for all $t_f \in T_f^i$, $t_f \notin \sigma'_u$ and $t_f \notin \sigma'_o$.

In such a case a fault transition of class i is either contained in one justification of w or in a sequence of observable transitions labeled w, but there also exist at least one other sequence of transitions that is consistent with the observation w that do not contain fault transitions and whose justifications do not contain fault transitions as well.

• $\Delta(w, T_f^i) = 3$ if for all $\sigma \in \mathcal{S}(w)$ there exists $t_f \in T_f^i$ such that $t_f \in \sigma$.

In such a case the i-th fault must have occurred, because all firable sequences consistent with the observation contain at least one fault in T_f^i. ■

Example 5.2 Let us consider the PN in Fig. 1 previously introduced in Example 4.8. Let us consider only one fault class T_f, where $T_{o,f} = \{t_2\}$ and $T_{u,f} = \{\varepsilon_6\}$.

Let us first assume that no event is observed, i.e., $w = \varepsilon$. Then $\Delta(w, T_f) = 0$, being obviously $\hat{\mathcal{J}}(w) = \{(\varepsilon, \varepsilon)\}$ and $\mathcal{S}(w) = \{\varepsilon\}$. This means that no fault may have occurred.

Let us now observe $w = a$. Then $\Delta(w, T_f) = 2$, being $\hat{\mathcal{J}}(w) = \{(t_1, \varepsilon), (t_2, \varepsilon)\}$. This means that a fault may have occurred.

Finally, let us observe $w = ab$. Then $\Delta(w, T_f) = 0$, being $\hat{\mathcal{J}}(w) = \{(t_1 t_3, \varepsilon_5)\}$ and $\mathcal{S}(w) = \{t_1 \varepsilon_5 t_3\}$. This means that no fault may have occurred. ■

Proposition 5.3 Consider an observed word $w \in L^*$.

• $\Delta(w, T_f^i) \in \{0, 1\}$ iff for all $(M, y, \gamma) \in \bar{\mathcal{M}}(w)$ it holds that: for all $t_f \in T_f^i \cap T_{u,f}$, $y(t_f) = 0$, and for all $t_f \in T_f^i \cap T_{o,f}$, $\gamma(t_f) = 0$.

• $\Delta(w, T_f^i) = 2$ iff there exist $(M, y, \gamma) \in \bar{\mathcal{M}}(w)$ and $(M', y', \gamma') \in \bar{\mathcal{M}}(w)$ such that:
(i) either there exists $t_f \in T_f^i \cap T_{u,f}$ such that $y(t_f) > 0$ or there exists $t_f \in T_f^i \cap T_{o,f}$ such that $\gamma(t_f) > 0$ (or both),
(ii) for all $t_f \in T_f^i \cap T_{u,f}$ it is $y'(t_f) = 0$, and for all $t_f \in T_f^i \cap T_{o,f}$ it is $\gamma'(t_f) = 0$.

• $\Delta(w, T_f^i) = 3$ iff for all $(M, y, \gamma) \in \bar{\mathcal{M}}(w)$ either there exists $t_f \in T_f^i \cap T_{u,f}$ such that $y(t_f) > 0$ or there exists $t_f \in T_f^i \cap T_{o,f}$ such that $\gamma(t_f) > 0$ (or both).

Proof. By Definition 5.1, $\Delta(w, T_f^i) = 0$ iff no fault transition $t_f \in T_f^i$ is contained in any firing sequence that is consistent with w, while $\Delta(w, T_f^i) = 1$ iff no fault $t_f \in T_f^i$ is contained in any justification of w and no observed label in w may correspond to a transition in $T_f^i \cap T_{o,f}$, but there exists at least one sequence that is consistent with w that contains a transition $t_f \in T_f^i$. Therefore, a necessary and sufficient condition to have $\Delta(w, T_f^i) \in \{0, 1\}$ is that for all j-vectors y at w and all $t_f \in T_f^i$ it is $y(t_f) = 0$ and $\gamma(t_f) = 0$, thus proving the first item.

Analogously, $\Delta(w, T_f^i) = 2$ either if a transition $t_f \in T_f^i$ is contained in at least one (but not in all) justification of w, or at least one (but not all) sequence of observable transitions that

may have actually fired contains a transition in $T_f^i \cap T_{o,f}$, or both cases occur. Thus, to have $\Delta(w, T_f^i) = 2$ it is necessary and sufficient that either there exists at least one j-vector y or at least one γ-vector γ that contains at least one transition $t_f \in T_f^i$, and one j-vector y' and the corresponding γ-vector γ' that do not contain transitions $t_f \in T_f^i$, thus proving the second item.

Finally, given an observed word w and a fault class T_f^i we have $\Delta(w, T_f^i) = 3$ if all firable sequences consistent with w contain at least one fault transition $t_f \in T_f^i$. Thus, to have $\Delta(w, T_f^i) = 3$ it is necessary and sufficient that either all the justifications contain at least one transition $t_f \in T_f^i$, or all the γ-vectors relative to justifications containing no transition in T_f^i, contain themselves a transition in T_f^i (or both conditions hold). This proves the third item. □

The following proposition shows how to distinguish between diagnosis states 0 and 1.

Proposition 5.4 For a PN whose unobservable subnet is acyclic, let $w \in L^*$ be an observed word such that for all $(M, y, \gamma) \in \bar{\mathcal{M}}(w)$ it holds $y(t_f) = 0 \ \forall \ t_f \in T_f^i \cap T_{u,f}$ and $\gamma(t_f) = 0 \ \forall \ t_f \in T_f^i \cap T_{o,f}$. Let us consider the constraint set

$$\mathcal{T}_i(M) \quad = \quad \begin{cases} M + C_u \cdot z \geq \vec{0}, \\ \sum\limits_{t_f \in T_f^i} z(t_f) > 0, \\ z \in \mathbb{N}^{n_u}. \end{cases} \tag{1}$$

- $\Delta(w, T_f^i) = 0$ if $\forall \ (M, y, \gamma) \in \bar{\mathcal{M}}(w)$ the constraint set (1) is not feasible.
- $\Delta(w, T_f^i) = 1$ if $\exists \ (M, y, \gamma) \in \bar{\mathcal{M}}(w)$ such that the constraint set (1) is feasible.

Proof. Let $w \in L^*$ be an observed word such that $\forall (M, y) \in \mathcal{M}(w)$ it is $y(t_f) = 0 \ \forall \ t_f \in T_f^i \cap T_{u,f}$ and $\gamma(t_f) = 0 \ \forall \ t_f \in T_f^i \cap T_{u,f}$. By Definition 5.1 it immediately follows that:

- $\Delta(w, T_f^i) = 0$ if $\forall (M, y, \gamma) \in \bar{\mathcal{M}}(w)$ and $\forall t_f \in T_f^i$ there does not exist a sequence $\sigma \in T_u^*$ such that $M[\sigma\rangle$ and $t_f \in \sigma$;
- $\Delta(w, T_f^i) = 1$ if $\exists$ at least one $(M, y, \gamma) \in \bar{\mathcal{M}}(w)$ and a sequence $\sigma \in T_u^*$ such that for at least one $t_f \in T_f^i$, $M[\sigma\rangle$ and $t_f \in \sigma$.

Now, if a Petri net is *acyclic* the state equation gives necessary and sufficient conditions for marking reachability [11]. Therefore, being the unobservable subnet acyclic, the set $\mathcal{T}_i(M)$ characterizes the reachability set of the unobservable net at marking M. Thus, due to this fact and the above two items, we can conclude that there exists a sequence containing a transition $t_f \in T_f^i$ firable at M on the unobservable subnet if and only if $\mathcal{T}_i(M)$ is feasible. □

On the basis of the above two results, if the unobservable subnet is acyclic, diagnosis may be carried out by simply looking at the set $\bar{\mathcal{M}}(w)$ for any observed word w and, should the diagnosis state be either 0 or 1, by additionally evaluating whether the corresponding integer constraint set (1) admits a solution.

Example 5.5 Let us consider again the PN in Fig. 1 where $T_f = T_{o,f} \cup T_{u,f} = \{t_2\} \cup \{\varepsilon_6\}$.

Let $w = a$. In this case $\bar{\mathcal{M}}(w) = \{(M_b^1, \vec{0}, 0), (M_b^2, \vec{0}, 1)\}$, where M_b^1 and M_b^2 are reported in Example 4.8. It is $\Delta(w, T_f) = 2$.

Let $w = ab$. It is $\Delta(w, T_f) = 0$ being $\bar{\mathcal{M}}(w) = \{(M_b^2, [1\ 0]^T, 0)\}$ and $\mathcal{T}_1(M_b^2)$ not feasible.

Let $w = abac$. In this case $\bar{\mathcal{M}}(w) = \{(M_0, [1\ 1]^T, 0),\ (M_0, [1\ 0]^T, 1)\}$. It is $\Delta(w, T_f) = 3$. ■

6 Basis Reachability Graph

The diagnosis approach described in the previous section can be applied both to bounded and unbounded PNs: it is an on-line approach that for each new observed event updates the diagnosis state for each fault class computing the set of basis markings and j-vectors. Moreover if for a given fault class is necessary to distinguish between diagnosis states 0 and 1, it is also necessary to solve for each basis marking M_b and for each fault class T_f^i the constraint set $\mathcal{T}_i(M_b)$.

In this section we show that, as in the case where fault events may only correspond to silent events [4,5], if the considered net system is bounded, the most burdensome part of the procedure can be moved off-line defining a graph called *Basis Reachability Graph* (BRG).

Definition 6.1 The BRG is a deterministic graph that has as many nodes as the number of possible basis markings.

To each node is associated a different basis marking M and a row vector with as many entries as the number of fault classes. The i-th entry of this vector may only take binary values: 1 if $\mathcal{T}_i(M)$ is feasible, 0 otherwise.

Arcs are labeled with observable events in L, e-vectors and vectors $z \in \{0,1\}^{n_{o,f}}$ where z are binary vectors with as many entries as the number $n_{o,f}$ of transitions in $T_{o,f}$: if the current label l is relative to a transition $t \in T_{o,f}$, then the only non zero entry of z is $z(t)$, if $t \in T_{o,reg}$ otherwise z is a zeros' vector. More precisely, an arc exists from a node containing the basis marking M to a node containing the basis marking M' if and only if there exists a transition t for which an explanation exists at M and the firing of t and one of its minimal explanations leads to M'. The arc going from M to M' is labeled $(\mathcal{L}(t), e, z)$, where $e \in Y_{\min}(M, t)$, $M' = M + C_u \cdot e + C(\cdot, t)$. ■

The main steps for the computation of the BRG in the case of labeled PNs are summarized in the following algorithm.

Algorithm 6.2 [Computation of the BRG]

1. Label the initial node (M_0, x_0) where $\forall i = 1, \ldots, r$,

$$x_0(T_f^i) = \begin{cases} 1 & \text{if } \mathcal{T}_i(M_0) \text{ is feasible,} \\ 0 & \text{otherwise.} \end{cases}$$

Assign no tag to it.

2. While nodes with no tag exist
select a node with no tag and do
2.1. let M be the marking in the node (M, x),
2.2. for all $l \in E$
2.2.1. for all $t : \mathcal{L}(t) = l \wedge Y_{\min}(M, t) \neq \emptyset$, do
- for all $e \in Y_{\min}(M, t)$, do
  - let $M' = M + C_u \cdot e + C(\cdot, t)$,
  - if $\nexists$ a node (M, x) with $M = M'$, do
    - add a new node to the graph containing (M', x') where $\forall i = 1, \ldots, r$,
      $x'(T_f^i) = \begin{cases} 1 & \text{if } \mathcal{T}_i(M') \text{ is feasible,} \\ 0 & \text{otherwise.} \end{cases}$
      and arc (l, e, z) from (M, x) to (M', x')
      where $\forall i = 1, \ldots, r$, $z_i = \begin{cases} 1 & \text{if } t \in T_{o,f} \\ 0 & \text{otherwise} \end{cases}$
  - else
    - add arc (l, e, z) from (M, x) to (M', x') if it does not exist yet
      where $\forall i = 1, \ldots, r$, $z_i = \begin{cases} 1 & \text{if } t \in T_{o,f} \\ 0 & \text{otherwise} \end{cases}$

2.3. tag the node "old".
3. Remove all tags. ■

The algorithm constructs the BRG starting from the initial node to which it corresponds the initial marking and a binary vector defining which classes of fault may occur at M_0. Now, we consider all the labels $l \in E$ such that there exists a transition t with $\mathcal{L}(t) = l$ for which a minimal explanation at M_0 exists. For any of these transitions we compute the marking resulting from firing t at $M_0 + C_u \cdot e$, for any $e \in Y_{\min}(M_0, t)$. If a pair (marking, binary vector) not contained in the previous nodes is obtained, a new node is added to the graph. The arc going from the initial node to the new node is labeled (l, e, z) where z keeps track of the label l may be associated to a fault transition. The procedure is iterated until all basis markings have been considered. Note that, our approach always requires to enumerate a state space that is a subset (usually a strict subset) of the reachability space. However, as in general for diagnosis approaches, the combinatory explosion cannot be avoided.

Example 6.3 Let us consider again the PN in Fig. 1, where $T_o = \{t_1, t_2, t_3, t_4\}$, $T_{o,reg} = \{t_1, t_3, t_4\}$, $T_{o,f} = \{t_2\}$, $T_u = \{\varepsilon_5, \varepsilon_6\}, T_{u,reg} = \{\varepsilon_5\}$, $T_{u,f} = \{\varepsilon_6\}$. The labeling function is defined as follows: $\mathcal{L}(t_1) = \mathcal{L}(t_2) = a$, $\mathcal{L}(t_3) = b$ and $\mathcal{L}(t_4) = c$.

The BRG is shown in Fig. 2. Each node contains a different basis marking and a scalar, because there is only one fault class. As an example, 0 is associated with M_0 because $\mathcal{T}_1(M_0)$ is not feasible, while 1 is associated with M_b^1 because $\mathcal{T}_1(M_b^1)$ is feasible. From node M_0 two different arcs labeled a exit. The arc $(a, [0\ 0]^T, 0)$ goes from M_0 to M_b^1 and the arc $(a, [0\ 0]^T, 1)$ goes from M_0 to M_b^2. This means that both basis markings M_b^1 and M_b^2 are reached firing a transition

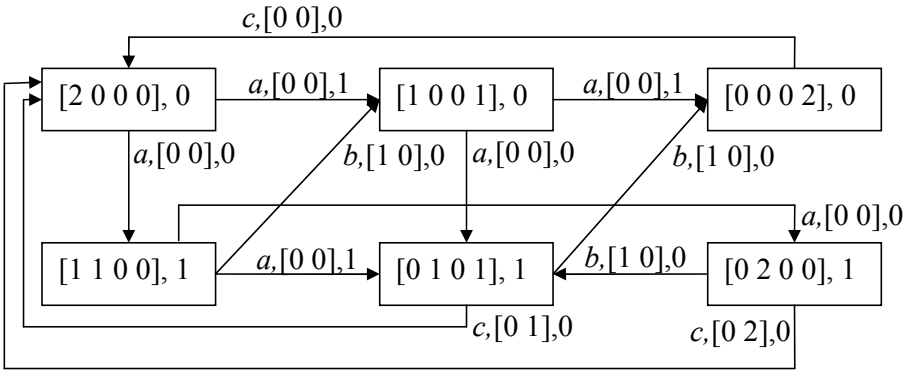

Figure 2: The BRG of the PN in Fig. 1.

labeled a: M_b^1 is reached firing $t_1 \in T_{o,reg}$ while M_b^2 is reached firing $t_2 \in T_{o,f}$, thus $z_1 = 0$ and $z_2 = 1$. ■

The following algorithm summarizes the main steps of the on-line diagnosis carried out by looking at the BRG.

Algorithm 6.4 [Diagnosis using the BRG]

1. Let $w = \varepsilon$.
2. Let $\bar{\mathcal{M}}(w) = \{(M_0, \vec{0}, \vec{0})\}$.
3. Wait until a new observable transition fires.
Let l be the observed event.
4. Let $w' = w$ and $w = w'l$.
5. Let $\bar{\mathcal{M}}(w) = \emptyset$, **[Computation of $\mathcal{M}(w)$]**
6. For all nodes containing M' : $(M', y', \gamma') \in \bar{\mathcal{M}}(w')$, do
6.1. for all arcs exiting from the node with M', do
6.1.1. let M be the marking of the output node,
e be the minimal e-vector on the edge, and
z be the third vector on the edge (see Def. 6.1)
from M' to M,
6.1.2. for all y' such that $(M', y', \gamma') \in \bar{\mathcal{M}}(w')$, do
6.1.2.1. let $y = y' + e$,
6.1.2.2. let $\gamma = \gamma' + z$,
6.1.2.3. **let** $\bar{\mathcal{M}}(w) = \bar{\mathcal{M}}(w) \cup \{(M, y, \gamma)\}$**,**
7. for all $i = 1, \ldots, r$, do
[Computation of the diagnosis state]
7.1. if $\forall\ (M, y, \gamma) \in \bar{\mathcal{M}}(w)$ and
$\forall t_f \in T_f^i$ it is $y(t_f) = 0$ and $\gamma(t_f) = 0$, do
7.1.1. if $\forall\ (M, y, \gamma) \in \bar{\mathcal{M}}(w)$ it holds $x(i) = 0$,
where x is the binary vector in node M, do
7.1.1.1. let $\Delta(w, T_f^i) = 0$,
7.1.2. else

7.1.2.1. let $\Delta(w, T_f^i) = 1$,

7.2. if $\exists\ (M, y, \gamma) \in \bar{\mathcal{M}}(w)$ and $(M', y', \gamma') \in \bar{\mathcal{M}}(w)$ s.t.:
(i) $\exists t_f \in T_f^i$ such that $y(t_f) > 0$ or $\gamma(t_f) > 0$,
(ii) $\forall t_f \in T_f^i$, $y'(t_f) = 0$ and $\gamma'(t_f) = 0$,
or both, do

7.2.1. let $\Delta(w, T_f^i) = 2$,

7.3. if $\forall\ (M, y, \gamma) \in \bar{\mathcal{M}}(w)\ \exists t_f \in T_f^i : y(t_f) > 0$ or $\gamma(t_f) > 0$, do

7.3.1. let $\Delta(w, T_f^i) = 3$.

8. Goto Step 3. ■

Steps 1 to 6 of Algorithm 6.4 enable us to compute the set $\bar{\mathcal{M}}(w)$.

Step 7 of Algorithm 6.4 computes the diagnosis state. Let us consider the generic ith fault class. If $\forall (M, y, \gamma) \in \bar{\mathcal{M}}(w)$ and $\forall t_f \in T_f^i$ it holds $y(t_f) = 0$ and $\gamma(t_f) = 0$, we have to check the ith entry of all the binary row vectors associated to the basis markings M, such that $(M, y, \gamma) \in \bar{\mathcal{M}}(w)$. If the ith entry is equal to 0, we set $\Delta(w, T_f^i) = 0$, otherwise we set $\Delta(w, T_f^i) = 1$. On the other hand, if there exists at least one triple $(M, y, \gamma) \in \bar{\mathcal{M}}(w)$ with either $y(t_f) > 0$ or $\gamma(t_f) > 0$ (or both) for any $t_f \in T_f^i$, and there exists at least one triple $(M', y', \gamma') \in \bar{\mathcal{M}}(w)$ with $y(t_f) = 0$ and $\gamma(t_f) = 0$ for all $t_f \in T_f^i$, then $\Delta(w, T_f^i) = 2$. Finally, if for all triples $(M, y, \gamma) \in \bar{\mathcal{M}}(w)$, either $y(t_f) > 0$ or $\gamma(t_f) > 0$ (for both) for any $t_f \in T_f^i$, then $\Delta(w, T_f^i) = 3$.

The following example shows how to perform diagnosis on-line simply looking at the BRG.

Example 6.5 Let us consider the PN in Fig. 1 and its BRG in Fig. 2. Let $w = \varepsilon$. By looking at the BRG we establish that $\Delta(\varepsilon, T_f) = 0$ being the scalar associated with M_0 equal to 0.

Now, let us consider $w = aa$. In such a case

$$\bar{\mathcal{M}}(w) = \{([0\ 1\ 0\ 1]^T, [0\ 0]^T, 1), ([0\ 2\ 0\ 0]^T, [0\ 0]^T, 0), ([0\ 0\ 0\ 2]^T, [0\ 0]^T, 2)\}.$$

Thus $\Delta(aa, T_f) = 2$.

Finally, for $w = aabc$ it holds $\Delta(aa, T_f) = 3$. In fact $\bar{\mathcal{M}}(w) = \{(M_0, [1\ 1]^T, 0), (M_0, [1\ 0]^T, 1)\}$.
■

7 Conclusions and future work

This paper presents a diagnosis approach for labeled PNs using basis markings, that enable us to avoid an exhaustive enumeration of the reachability set.

The main difference with respect to our previous works in this framework is that now fault transitions do not necessarily correspond to silent events, but may also be observable undis-

tinguishable events, i.e., they share the same label with transitions belonging to different fault classes and/or with transitions modeling regular behavior.

Our future work will be that of studying the diagnosis problem for distributed systems investigating the possibility of extending the approach here presented to this case.

References

[1] A. Aghasaryan, E. Fabre, A. Benveniste, R. Boubour, and C. Jard. Fault detection and diagnosis in distributed systems: an approach by partially stochastic Petri nets. *Discrete Events Dynamical Systems*, 8:203–231, June 1998.

[2] A. Benveniste, E. Fabre, S. Haar, and C. Jard. Diagnosis of asynchronous discrete event systems, a net unfolding approach. *IEEE Trans. on Automatic Control*, 48(5):714–727, May 2003.

[3] R.K. Boel and J.H. van Schuppen. Decentralized failure diagnosis for discrete-event systems with costly communication between diagnosers. In *Proc. WODES'02: 6th Work. on Discrete Event Systems*, pages 175–181, October 2002.

[4] M.P. Cabasino, A. Giua, and C. Seatzu. Diagnosis of discrete event systems using labeled Petri nets. In *Proc. 2nd IFAC Workshop on Dependable Control of Discrete Systems (Bari, Italy)*, June 2009.

[5] M.P. Cabasino, A. Giua, and C. Seatzu. Fault detection for discrete event systems using Petri nets with unobservable transitions. *Automatica*, 2010. In press.

[6] R. Debouk, S. Lafortune, and D. Teneketzis. Coordinated decentralized protocols for failure diagnosis of discrete-event systems. *Discrete Events Dynamical Systems*, 10(1):33–86, January 2000.

[7] S. Genc and S. Lafortune. Distributed diagnosis of discrete event systems using Petri nets. In *Proc. of the 24th ATPN*, pages 316–336, June 2003.

[8] A. Giua and C. Seatzu. Fault detection for discrete event systems using Petri nets with unobservable transitions. In *Proc. 44th IEEE Conf. on Decision and Control*, pages 6323–6328, December 2005.

[9] G. Jiroveanu and R.K. Boel. Contextual analysis of Petri nets for distributed applications. In *16th Int. Symp. on Mathematical Theory of Networks and Systems (Leuven, Belgium)*, July 2004.

[10] J. Lunze and J. Schroder. Sensor and actuator fault diagnosis of systems with discrete inputs and outputs. 34(3):1096–1107, April 2004.

[11] T. Murata. Petri nets: properties, analysis and applications. *Proceedings of the IEEE*, 77(4):541–580, 1989.

[12] M. Sampath, S. Lafortune, and D. Teneketzis. Active diagnosis of discrete-event systems. *IEEE Trans. on Automatic Control*, 43(7):908–929, July 1998.

[13] S. H. Zad, R.H. Kwong, and W.M. Wonham. Fault diagnosis in discrete-event systems: framework and model reduction. *IEEE Trans. on Automatic Control*, 48(7):1199–1212, July 2003.