Diagnosis of discrete event systems using labeled Petri nets

Maria Paola Cabasino, Alessandro Giua, Carla Seatzu

Abstract

In this paper we provide an approach to on-line diagnosis of discrete event systems based on labeled Petri nets. The proposed procedure is based on our previous results on unlabeled Petri nets and allows us to also consider events that are undistinguishable, namely events that produce an output signal that is observable, but that is common to other events.

Our approach is based on the notion of basis markings and j-vectors and it is shown that, in the case of bounded Petri nets, the most burdensome part of the procedure may be moved off-line, computing a particular graph that we call *Basis Reachability Graph*.

Published as:

M.P. Cabasino, A. Giua, C. Seatzu, "Diagnosis of discrete event systems using labeled Petri nets," DCDS09: 2nd IFAC Work. on Dependable Control of Discrete Systems (Bari, Italy), Jun 2009.

This work has been partially supported by the European Community's Seventh Framework Programme under project DISC (Grant Agreement n. INFSO-ICT-224498) and by the US National Science Foundation (Grant ECCS-0624281).

M.P. Cabasino and A. Giua and C. Seatzu are with the Department of Electrical and Electronic Engineering, University of Cagliari, Piazza D'Armi, 09123 Cagliari, Italy {cabasino,giua,seatzu}@diee.unica.it

I. INTRODUCTION

Faults are physical conditions that cause a device or a component to fail to perform in a required manner. Automatic fault detection and diagnosis is a research area that received a lot of attention in the last years not only within the framework of time-driven systems, but also in the case of discrete event systems (DES). In this framework several original theoretical approaches have been proposed ([1]; [2]; [3]; [4]; [5]; [6]).

Petri net (PN) models have often been used in this context: the intrinsically distributed nature of PNs where the notion of state (i.e., marking) and action (i.e., transition) is local has often been an asset to reduce the computational complexity involved in solving a diagnosis problem. Among the different contributions in this area we recall the work of [7], [8], [9], [10], [11], [12], [13]. Finally, [14] solve the same problem considered in this paper using the Diagnoser Approach for DES. However, most of these approaches require an exhaustive enumeration of the state space.

The main difference between our diagnosis approach ([15], [16]) and the approaches cited above is the concept of *basis marking*. This concept allows us to represent the reachability space in a compact manner, i.e., our approach requires to enumerate only a subset of the reachability space. In our previous papers we presented an approach for on-line diagnosis for PNs that are unlabeled and where some transitions are unobservable (silent). In this paper we extend this approach considering PNs that are labeled —i.e., PNs where two or more transitions can share the same label — and where some transitions are unobservable. This extended setting requires to reformulate the concepts of basis markings, minimal explanations, minimal e-vectors and j-vectors on which our procedure is based on. Moreover we redefine four diagnosis states, each one corresponding to a different degree of alarm. We give a procedure to compute the actual diagnosis state given the current observation. Finally we show that, as for the unlabeled PNs, in the case of bounded net systems, the most burdensome part of the procedure can be moved off-line defining a particular graph, that we call *Basis Reachability Graph*.

II. BASIC DEFINITIONS

In this section we recall the formalism used in the paper. For more details on PNs we refer to [17].

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; $Pre: P \times T \rightarrow \mathbb{N}$ and $Post: P \times T \rightarrow \mathbb{N}$ are the pre– and $post$– incidence functions that specify the arcs; $C = Post - Pre$ is the incidence matrix.

A *marking* is a vector $M: P \rightarrow \mathbb{N}$ that assigns to each place of a P/T net a non–negative 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 $\pi: T^* \rightarrow \mathbb{N}^n$ 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 net is said *structurally bounded* if it is bounded for any initial marking.

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

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*. 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. Note that in this paper 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., $\mathcal{L}(t_1) = \mathcal{L}(t_2) = l \in L$. The set of transitions sharing the same label l are denoted as T_l.

In the following we denote as C_u (C_o) the restriction of the incidence matrix to T_u (T_o) and

denote as n_u and n_o, respectively, the cardinality of the above sets. Moreover, given a sequence $\sigma \in T^*$, $P_u(\sigma)$ ($P_o(\sigma)$) denotes the projection of σ over T_u (T_o).

We denote as w the word of events associated to the sequence σ, i.e., $w = \mathcal{L}(\sigma)$. Note that the length of a sequence σ (denoted $|\sigma|$) is always greater than or equal to the length of the corresponding word w (denoted $|w|$). In fact, if σ contains k' transitions in T_u then $|\sigma| = k' + |w|$.

***Definition** 2.1:* Let $\langle N, M_0 \rangle$ be a labeled net system with labeling function $\mathcal{L} : T \to L \cup \{\varepsilon\}$, where $N = (P, T, Pre, Post)$ and $T = T_o \cup T_u$. Let $w \in L^*$ be an observed word. We define

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

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

$$\mathcal{C}(w) = \{M \in R(N, M_0) \mid \exists \sigma \in T^* : \mathcal{L}(\sigma) = w \wedge M_0[\sigma\rangle M\}$$

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

In plain words, given an observation w, $\mathcal{S}(w)$ is the set of sequences that may have fired, while $\mathcal{C}(w)$ is the set of markings in which the system may actually be.

***Example** 2.2:* Let us consider the PN in Fig. 1. Let us assume $T_o = \{t_1, t_2, t_3, t_4, t_5, t_6, t_7\}$ and $T_u = \{\varepsilon_8, \varepsilon_9, \varepsilon_{10}, \varepsilon_{11}, \varepsilon_{12}, \varepsilon_{13}\}$, where for a better understanding unobservable transitions have been denoted ε_i rather than t_i. The labeling function is defined as follows: $\mathcal{L}(t_1) = a$, $\mathcal{L}(t_2) = \mathcal{L}(t_3) = b$, $\mathcal{L}(t_4) = \mathcal{L}(t_5) = c$, $\mathcal{L}(t_6) = \mathcal{L}(t_7) = d$.

First let us consider $w = acd$. The set of firing sequences that are consistent with w is $\mathcal{S}(w) = \{t_1t_5t_6, t_1t_5\varepsilon_{12}\varepsilon_{13}t_7\}$, and the set of markings consistent with w is $\mathcal{C}(w) = \{[0\ 1\ 0\ 0\ 0\ 0\ 0\ 1\ 0\ 0\ 0]^T\}$. Thus two different firing sequences may have fired (the second one also involving silent transitions), but they both lead to the same marking.

Different markings can be reached if we consider $w = ab$. In particular, $\mathcal{S}(w) = \{t_1t_2, t_1t_2\varepsilon_8, t_1t_2\varepsilon_8\varepsilon_9, t_1t_2\varepsilon_8\varepsilon_9\varepsilon_{10}, t_1t_2\varepsilon_8\varepsilon_{11}\}$, and $\mathcal{C}(w) = \{[0\ 0\ 1\ 0\ 0\ 0\ 0\ 1\ 0\ 0\ 0]^T, [0\ 0\ 0\ 1\ 0\ 0\ 0\ 1\ 0\ 0\ 0]^T, [0\ 0\ 0\ 0\ 1\ 0\ 0\ 1\ 0\ 0\ 0]^T, [0\ 1\ 0\ 0\ 0\ 0\ 0\ 1\ 0\ 0\ 0]^T, [0\ 0\ 0\ 0\ 0\ 1\ 0\ 1\ 0\ 0\ 0]^T\}$. ■

III. Minimal explanations and minimal e-vectors

In [16] we gave the following two definitions.

***Definition** 3.1:* Given a marking M and an observable transition $t \in T_o$, we define

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

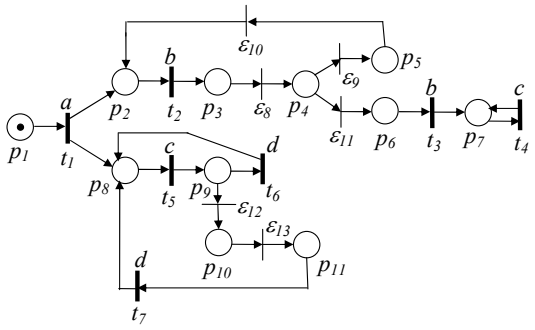

Fig. 1. A PN system modeling.

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.

***Definition** 3.2:* 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 this section we generalize the above definitions.

***Definition** 3.3:* 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). ■

Obviously, $\hat{\Sigma}_{\min}(M,l)$ and $\hat{Y}_{\min}(M,l)$ are a generalization of the sets of minimal explanations and minimal e-vectors introduced for unlabeled PNs with unobservable transitions. Moreover, in the above sets $\hat{\Sigma}_{\min}(M,l)$ and $\hat{Y}_{\min}(M,l)$ different sequences σ and different e-vectors e, respectively, are associated in general to the same $t \in T_l$.

IV. Basis markings and j-vectors

In [16] the notions of *basis markings* and *j-vectors* have been defined for unlabeled PNs. In particular, given a sequence of observed transitions $w \in T_o^*$, 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 necessary to enable w. A j-vector $y \in Y_{min}(M_0, w)$ is a firing vector of unobservable transitions whose firing is necessary to reach M_b.

Here we basically use the same definitions, even if with a slight but crucial difference. In fact, in the case of labeled PNs the observation w is a sequence of labels, namely $w \in L^*$. In general several sequences $\sigma_o \in T_o^*$ may correspond to the same w, i.e., there are several sequences of observable transitions such that $\mathcal{L}(\sigma_o) = w$ that may have actually fired. Moreover, in general, to any of such sequences σ_o a different sequence of unobservable transitions interleaved with it is necessary to make it firable at the initial marking. Thus we need to introduce the following definition of pairs (sequence of transitions in T_o labeled w – corresponding *justification*).

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

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

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

$$\begin{aligned}\hat{Y}_{\min}(M_0, w) = \{(\sigma_o, y),\ \ &\sigma_o \in T_o^*,\ \mathcal{L}(\sigma_o) = w,\ y \in \mathbb{N}^{n_u}\ \mid \\ &\exists (\sigma_o, \sigma_u) \in \hat{\mathcal{J}}(w) : \pi(\sigma_u) = y\}\end{aligned}$$

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

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. The firing vectors of these sequences are called *j-vectors*.

***Definition** 4.2:* Let $\langle N, M_0\rangle$ be a net system with labeling function $\mathcal{L} : T \to L \cup \{\varepsilon\}$, 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 minimal 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 minimal 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** 4.3:* Let $\langle N, M_0\rangle$ be a net system with labeling function $\mathcal{L} : T \to L \cup \{\varepsilon\}$, where $N = (P, T, Pre, Post)$ and $T = T_o \cup T_u$. Let $w \in L^*$ be an observed word. We define

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

the set of pairs (basis marking – relative j-vector) that are *consistent* with $w \in L^*$. ■

Note that the set $\mathcal{M}(w)$ does not keep into account the sequences of observable transitions that may have actually fired. It only keeps track of the basis markings that can be reached and of the firing vectors relative to sequences of unobservable transitions that have fired to reach them. Indeed, this is the information really significant when performing diagnosis. The notion of $\mathcal{M}(w)$ is fundamental to provide a recursive way to compute the set of minimal explanation.

***Proposition** 4.4:* Given a net system $\langle N, M_0\rangle$ with labeling function $\mathcal{L} : T \to L \cup \{\varepsilon\}$, where $N = (P, T, Pre, Post)$ and $T = T_o \cup T_u$. Assume that the T_u-induced subnet is acyclic. Let $w = w'l$ be a given observation.

The set $\hat{Y}_{\min}(M_0, wl)$ is defined as:

$$\begin{aligned}\hat{Y}_{\min}(M_0, wl) = \ & \{(\sigma_o, y)\ \mid\ \sigma_o = \sigma_0' t \wedge y = y' + e\ : \\ & (\sigma_o', y') \in \hat{Y}_{\min}(M_0, w), \\ & (t, e) \in \hat{Y}_{\min}(M_b', l) \text{ and } \mathcal{L}(t) = l\},\end{aligned}$$

where $M_b' = M_0 + C_u \cdot y' + C_o \cdot \sigma_o'$.

Proof: Trivially follows from Definitions 3.3, 4.1, 4.2 and from the fact that in PNs where the unobservable subnet is acyclic basis markings completely characterize the set of consistent markings (see [16]). □

***Example** 4.5:* Let us consider the PN in Fig. 1 previously introduced in Example 2.2. Let us assume $w = acd$. The set of justifications is $\hat{\mathcal{J}}(w) = \{(t_1t_5t_6, \varepsilon), (t_1t_5t_7, \varepsilon_{12}\varepsilon_{13})\}$ and the set of j-vectors is
$\hat{Y}_{min}(M_0, w) = \{(t_1t_5t_6, \vec{0}), (t_1t_5t_7, [0\ 0\ 0\ 0\ 1\ 1]^T)\}$. The above j-vectors lead to the same basis marking $M_b = [0\ 1\ 0\ 0\ 0\ 0\ 0\ 1\ 0\ 0\ 0]^T$ thus $\mathcal{M}(w) = \{(M_b, \vec{0}), (M_b, [0\ 0\ 0\ 0\ 1\ 1]^T)\}$.

Now, let us consider $w = ab$. In this case $\hat{\mathcal{J}}(w) = \{(t_1t_2, \varepsilon)\}$, $\hat{Y}_{min}(M_0, w) = \{(t_1t_2, \vec{0})\}$ and the basis marking is the same as in the previous case, namely $M_b = [0\ 1\ 0\ 0\ 0\ 0\ 0\ 1\ 0\ 0\ 0]^T$, thus $\mathcal{M}(w) = \{(M_b, \vec{0})\}$. ■

Under the assumption of acyclicity of the T_u-induced subnet, the set $\mathcal{M}(w)$ can be easily constructed as follows.

***Algorithm** 4.6:* **[Computation of the basis markings and j-vectors]**

1. Let $w = \varepsilon$.

2. Let $\mathcal{M}(w) = \{(M_0, \vec{0})\}$.

3. Wait until a new label l is observed.

4. Let $w' = w$ and $w = w'l$.

5. Let $\mathcal{M}(w) = \emptyset$.

6. For all M' such that $(M', y') \in \mathcal{M}(w')$, do

6.1. for all $t \in T_l$, do

6.1.1. for all $e \in Y_{\min}(M', t)$, do

6.1.1.1. let $M = M' + C_u \cdot e + C(\cdot, t)$,

6.1.1.2. for all y' such that $(M', y') \in \mathcal{M}(w')$, do

6.1.2.1. let $y = y' + e$,

6.1.2.2. let $\mathcal{M}(w) = \mathcal{M}(w) \cup \{(M, y)\}$.

7. Goto step 3. ■

In simple words, the above algorithm can be explained as follows. We assume that a certain word w (that is equal to the empty string at the initial step) has been observed. Then, a new observable t fires and we observe its label $\mathcal{L}(t)$ (e.g., l). We consider all basis markings at the observation w' before the firing of t, and we select among them those that may have allowed

the firing of at least one transition $t \in T_l$, also taking into account that this may have required the firing of appropriate sequences of unobservable transitions. In particular, we focus on the minimal explanations, and thus on the corresponding minimal e-vectors (step 6.1.1). Finally, we update the set $\mathcal{M}(w)$ including all pairs of new basis markings and j-vectors, taking into account that for each basis marking at w' it may correspond more than one j-vector.

Let us now recall the following result.

***Definition** 4.7:* ([16]) 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 T_u-induced subnet is acyclic. Let $w \in T_o^*$ be an observed word. We denote

$$\mathcal{M}_{basis}(w) = \{M \in \mathbb{N}^m \ \mid \ \exists y \in \mathbb{N}^{n_u} \ \text{ and } \ (M, y) \in \mathcal{M}(w)\}$$

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.

***Theorem** 4.8 ([16]):* Let us consider a net system $\langle N, M_0 \rangle$ whose unobservable subnet is acyclic. For any $w \in L^*$ it holds that

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

V. Diagnosis using Petri nets

Assume that the set of unobservable transitions is partitioned in two subsets, namely $T_u = T_f \cup T_{reg}$ where T_f includes all fault transitions (modeling anomalous or fault behavior), while T_{reg} includes all transitions relative to unobservable but regular events. The set T_f is further partitioned into r different subsets T_f^i, where $i = 1, \ldots, r$, that model the different fault classes.

The following definition introduces the notion of *diagnoser*. It is based on that introduced in [16] in the case of unlabeled PNs.

***Definition** 5.1:* A *diagnoser* is a function $\Delta : L^* \times \{T_f^1, T_f^2, \ldots, T_f^r\} \rightarrow \{0, 1, 2, 3\}$ 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 ith 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 $t_f \notin \sigma_u$.
  In such a case a fault transition of class i may have occurred but is not contained in any justification of 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 $t_f \in \sigma_u$;
  (ii) for all $t_f \in T_f^i$, $t_f \notin \sigma'_u$.
  In such a case a fault transition of class i is contained in one (but not in all) justification of w.
- $\Delta(w, T_f^i) = 3$ 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 ith 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 2.2. Let $T_f = \{\varepsilon_{11}, \varepsilon_{12}\}$. Assume that the two fault transitions belong to different fault classes, i.e., $T_f^1 = \{\varepsilon_{11}\}$ and $T_f^2 = \{\varepsilon_{12}\}$.

Let us observe $w = acd$. Then $\Delta(w, T_f^1) = 0$ and $\Delta(w, T_f^2) = 2$, being $\hat{\mathcal{J}}(w) = \{(t_1 t_5 t_6, \varepsilon), (t_1 t_5 t_7, \varepsilon_{12}\varepsilon_{13})\}$ and $\mathcal{S}(w) = \{t_1 t_5 t_6, t_1 t_5 \varepsilon_{12} \varepsilon_{13} t_7\}$.

Now, let us consider $w = ab$. In this case $\Delta(w, T_f^1) = 1$ and $\Delta(w, T_f^2) = 0$, being $\hat{\mathcal{J}}(w) = \{(t_1 t_2, \varepsilon)\}$ and $\mathcal{S}(w) = \{t_1 t_2, t_1 t_2 \varepsilon_8, t_1 t_2 \varepsilon_8 \varepsilon_9, t_1 t_2 \varepsilon_8 \varepsilon_9 \varepsilon_{10}, t_1 t_2 \varepsilon_8 \varepsilon_{11}\}$. ■

The following two results proved in [16] for unlabeled PNs still hold in the case of labeled PNs.

***Proposition** 5.3:* ([16]) Consider an observed word $w \in L^*$.

- $\Delta(w, T_f^i) \in \{0, 1\}$ iff for all $(M, y) \in \mathcal{M}(w)$ and for all $t_f \in T_f^i$ it holds $y(t_f) = 0$.
- $\Delta(w, T_f^i) = 2$ iff there exist $(M, y) \in \mathcal{M}(w)$ and $(M', y') \in \mathcal{M}(w)$ such that:
  (i) there exists $t_f \in T_f^i$ such that $y(t_f) > 0$,
  (ii) for all $t_f \in T_f^i$, $y'(t_f) = 0$.
- $\Delta(w, T_f^i) = 3$ iff for all $(M, y) \in \mathcal{M}(w)$ there exists $t_f \in T_f^i$ such that $y(t_f) > 0$.

Let us show how to distinguish between states 0 and 1.

***Proposition** 5.4:* ([16]) For a PN whose unobservable subnet is acyclic, let $w \in L^*$ be an observed word such that for all $(M, y) \in \mathcal{M}(w)$ it holds $y(t_f) = 0 \ \forall \ t_f \in T_f^i$. Let us consider the constraint set

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

- $\Delta(w, T_f^i) = 0$ if $\forall \ (M, y) \in \mathcal{M}(w)$ the constraint set (1) is not feasible.
- $\Delta(w, T_f^i) = 1$ if $\exists \ (M, y) \in \mathcal{M}(w)$ such that the constraint set (1) 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 $\mathcal{M}(w)$ 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 the PN in Fig. 1 where $T_f^1 = \{\varepsilon_{11}\}$ and $T_f^2 = \{\varepsilon_{12}\}$.

Let $w = acd$. It is $\mathcal{M}(w) = \{(M_b, \vec{0}), (M_b, [0\ 0\ 0\ 0\ 1\ 1]^T)\}$, where $M_b = [0\ 1\ 0\ 0\ 0\ 0\ 0\ 1\ 0\ 0\ 0]^T$ has been computed in Example 4.5. It is $\Delta(w, T_f^1) = 0$ being $\mathcal{T}(M_b)$ not feasible.

Let $w = ab$. In this case $\mathcal{M}(w) = \{(M_b, \vec{0})\}$, where $M_b = [0\ 1\ 0\ 0\ 0\ 0\ 0\ 1\ 0\ 0\ 0]^T$ as in the previous case. Being $\mathcal{T}(M_b)$ feasible only for the fault class T_f^1 it holds $\Delta(w, T_f^1) = 1$ and $\Delta(w, T_f^2) = 0$. ■

VI. Basis Reachability Graph

In [16] we have shown that in the case of bounded PNs a useful tool to perform diagnosis on-line is the *Basis Reachability Graph* (BRG). In this section we show how the BRG can still be defined in the case of arbitrary labeled PNs.

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 entries of this vector may only take binary values: 1 if $\mathcal{T}(M)$ is feasible, 0 otherwise.

Arcs are labeled with observable events in L and e-vectors. 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 $(\mathcal{L}(t), e)$, where $e \in Y_{\min}(M, t)$ and $M' = M + C_u \cdot e + C(\cdot, t)$.

Note that the number of nodes of the BRG is always finite being the set of basis markings a subset of the set of reachable markings, that is finite being the net bounded. Moreover, the row vector of binary values associated to the nodes of the BRG allows us to distinguish between the diagnosis state 1 or 0.

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

***Algorithm** 6.1:* **[Computation of the BRG]**

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

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

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 $l \in L$

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 $\forall i = 1, \ldots, r$,

    $$x'(T_f^i) = \begin{cases} 1 & \text{if } \mathcal{T}(M') \text{ is feasible,} \\ 0 & \text{otherwise.} \end{cases}$$

    and arc (l, e) from (M, x) to (M', x')
  - else
    - add arc (l, e) from (M, x) to (M', x')

    if it does not exist yet

2.3. tag the node "old".

M_0	$[\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ ]^T$
M_1	$[\ 0\ 1\ 0\ 0\ 0\ 0\ 0\ 1\ 0\ 0\ 0\ ]^T$
M_2	$[\ 0\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 1\ 0\ 0\ ]^T$
M_3	$[\ 0\ 0\ 1\ 0\ 0\ 0\ 0\ 1\ 0\ 0\ 0\ ]^T$
M_4	$[\ 0\ 0\ 1\ 0\ 0\ 0\ 0\ 0\ 1\ 0\ 0\ ]^T$
M_5	$[\ 0\ 0\ 0\ 0\ 0\ 0\ 1\ 1\ 0\ 0\ 0\ ]^T$
M_6	$[\ 0\ 0\ 0\ 0\ 0\ 0\ 1\ 0\ 1\ 0\ 0\ ]^T$

TABLE I

THE MARKINGS OF THE BRG IN FIG. 2.

	ε_8	ε_9	ε_{10}	ε_{11}	ε_{12}	ε_{13}
e_1	0	0	0	0	1	1
e_2	1	1	1	0	0	0
e_3	1	0	0	1	0	0

TABLE II

THE E-VECTORS OF THE BRG IN FIG. 2.

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 faults may occur at M_0. Now, we consider all the labels $l \in L$ 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). 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 strict subset of the reachability space. However, as in general for diagnosis approaches, the combinatory explosion cannot be avoided.

***Example** 6.2:* Let us consider the PN in Fig. 1, where $T_o = \{t_1, t_2, t_3, t_4, t_5, t_6, t_7\}$, $T_u = \{\varepsilon_8, \varepsilon_9, \varepsilon_{10}, \varepsilon_{11},\ \varepsilon_{12}, \varepsilon_{13}\}$, $T_f^1 = \{\varepsilon_{11}\}$ and $T_f^2 = \{\varepsilon_{12}\}$. The labeling function is defined as follows: $\mathcal{L}(t_1) = a$, $\mathcal{L}(t_2) = \mathcal{L}(t_3) = b$, $\mathcal{L}(t_4) = \mathcal{L}(t_5) = c$, $\mathcal{L}(t_6) = \mathcal{L}(t_7) = d$.

The BRG is shown in Fig. 2. The notation used in in this figure is detailed in Tables I and II. Each node contains a different basis marking and a binary row vector of dimension two, being

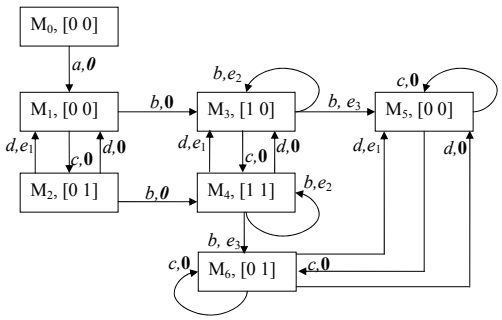

Fig. 2. The BRG of the PN in Fig. 1.

two the number of fault classes. As an example, the binary vector $[0\ 0]$ is associated to M_0 because $\mathcal{T}(M_0)$ is not feasible for both fault classes. From node M_0 to node M_1 there is one arc labeled a and with the null vector as minimal explanation. The node containing the basis marking M_2 has binary vector $[0\ 1]$, because $\mathcal{T}(M_2)$ is feasible only for T_f^2. Node $(M_2, [0\ 1])$ has two output arcs both labeled with d and both directed to node $(M_1, [0\ 0])$ with two different minimal explanations $\vec{0}$ and e_1, respectively, plus another output arc $(b, \vec{0})$ directed to node $(M_4, [1\ 1])$. ■

The BRG can be used to perform diagnosis on-line as shown in the following example. The diagnostic algorithm is not reported here for the sake of brevity, but can be found in the online version of [16].

***Example** 6.3:* 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 $\Delta(\varepsilon, T_f^1) = \Delta(\varepsilon, T_f^2) = 0$ being both entries of the row vector associated to M_0 equal to 0.

Now, let us consider $w = ab$. In such a case $\mathcal{M}(w) = \{(M_3, \vec{0})\}$. It holds $\Delta(ab, T_f^1) = 1$ and $\Delta(ab, T_f^2) = 0$ being the row vector in the node equal to $[1\ 0]$.

Finally, for $w = abbc$ it holds $\Delta(abbc, T_f^1) = 2$ and $\Delta(abbc, T_f^2) = 1$. In fact $\mathcal{M}(w) = \{(M_4, y_1), (M_5, y_2),$
$(M_6, y_3)\}$, where $y_1 = e_2$ and $y_2 = y_3 = e_3$, and the row vectors associated to M_4, M_5 and M_6 are respectively $[1\ 1], [0\ 0]$ and $[0\ 1]$. ■

VII. Conclusions and future work

The main contribution of this paper consists in the generalization of our previous results on the diagnosis of unlabeled PNs to arbitrary labeled PNs. Basically we proved that our previous definitions of basis markings, j-vectors, diagnosis states, etc. can be easily generalized to this more general setting. Analogously, a diagnoser can be computed using the same approach proposed in the unlabeled case. Finally, we showed how in the case of bounded net systems, the most burdensome part of the procedure may be moved off-line computing the Basis Reachability Graph.

Our future work will be that of providing, within this framework, necessary and sufficient conditions for the diagnosability of labeled PNs, namely to establish a priori whether the occurrence of a fault event may be detected after a finite number of observations. Moreover, we will investigate the possibility to extend our diagnosis approach to the case of distributed systems.

References

[1] M. Sampath and S. Lafortune, "Active diagnosis of discrete-event systems," *IEEE Trans. Automatic Control*, vol. 43, pp. 908–929, 1998.

[2] R. Debouk, S. Lafortune, and D. Teneketzis, "Coordinated decentralized protocols for failure diagnosis of discrete-event systems," *Discrete Events Dynamical Sys.*, vol. 20, pp. 33–79, 2000.

[3] R. Boel and J. van Schuppen, "Decentralized failure diagnosis for discrete-event systems with costly communication between diagnosers," in *Proc. IFAC WODES'02: 6th Work. on Discrete Event Systems (Zaragoza, Spain)*, Oct. 2002, pp. 175–181.

[4] S. H. Zad, R. Kwong, and W. Wonham, "Fault diagnosis in discrete-event systems: framework and model reduction," *IEEE Trans. Automatic Control*, vol. 48, no. 7, pp. 1199–1212, Jul. 2003.

[5] S. Jiang and R. Kumar, "Failure diagnosis of discrete-event systems with linear-time temporal logic specifications," *IEEE Trans. Automatic Control*, vol. 49, no. 6, pp. 934–945, Jun. 2004.

[6] J. Lunze and J. Schroder, "Sensor and actuator fault diagnosis of systems with discrete inputs and outputs," *IEEE Trans. Systems, Man and Cybernetics, Part B*, vol. 34, no. 3, pp. 1096–1107, Apr. 2004.

[7] T. Ushio, L. Onishi, and K. Okuda, "Fault detection based on Petri net models with faulty behaviors," in *Proc. SMC'98: IEEE Int. Conf. on Systems, Man, and Cybernetics (San Diego, CA, USA)*, Oct. 1998, pp. 113–118.

[8] 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 Sys.*, vol. 8, pp. 203–231, Jun. 1998.

[9] A. Benveniste, E. Fabre, S. Haar, and C. Jard, "Diagnosis of asynchronous discrete event systems, a net unfolding approach," *IEEE Trans. Automatic Control*, vol. 48, no. 5, pp. 714–727, May 2003.

[10] R. Boel and G. Jiroveanu, "Distributed contextual diagnosis for very large systems," in *Proc. IFAC WODES'04: 7th Work. on Discrete Event Systems (Reims, France)*, Sep. 2004.

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

[12] F. Basile, P. Chiacchio, and G. D. Tommasi, "An efficient approach for online diagnosis of discrete event systems," *IEEE Trans. Automatic Control*, 2008.

[13] M. Dotoli, M. Fanti, and A. Mangini, "Fault detection of discrete event systems using Petri nets and integer linear programming," in *Proc. of 17th IFAC World Congress*, 2008.

[14] S. Genc and S. Lafortune, "Distributed diagnosis of discrete event systems using Petri nets," in *Proc. of the 24th ATPN*, Jun. 2003, pp. 316–336.

[15] 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*, Dec. 2005, pp. 6323–6328.

[16] M. Cabasino, A. Giua, and C. Seatzu, "Fault detection for discrete event systems using Petri nets with unobservable transitions," *Automatica*, 2009, preliminary accepted. A longer version is available as Technical Report at: http://www.diee.unica.it/automatica/TR/DIEE-2009-AUT-01.pdf.

[17] T. Murata, "Petri nets: properties, analysis and applications," *Proceedings of the IEEE*, vol. 77, no. 4, 1989.