Available online at www.sciencedirect.com

ScienceDirect

IFAC PapersOnLine 50-1 (2017) 13624–13629

Decentralized Fault Diagnosis by Petri Nets and Integer Linear Programming

Xuya Cong *, **Maria Pia Fanti** **,
Agostino Marcello Mangini ***, **Zhiwu Li** ****

* *School of Electro-Mechanical Engineering, Xidian University No. 2 South Taibai Road, Xi'an 710071, China (e-mail: congxuya@163.com).*
** *Department of Electrical and Information Engineering, Polytechnic of Bari, 70125 Bari, Italy (e-mail: mariapia.fanti@poliba.it)*
*** *Department of Electrical and Information Engineering, Polytechnic of Bari, 70125 Bari, Italy (e-mail: agostinomarcello.mangini@poliba.it)*
**** *Institute of Systems Engineering, Macau University of Science and Technology, Taipa, Macau (e-mail: zhwli@must.edu.mo)*

Abstract: This paper addresses the problem of decentralized on-line fault diagnosis in the Petri net framework by using integer linear programming. The decentralized architecture consists of a set of local sites communicating with a coordinator that determines whether the behaviour of a system is normal or faulty. In particular, a protocol is presented for the communication between the local sites and the coordinator, and the rules for the coordinator to decide the global diagnosis results are proposed.

Keywords: Fault diagnosis; Petri nets; integer linear programming.

1. INTRODUCTION

Fault diagnosis of Discrete Event Systems (DESs) has received extensive attention in recent years. A fault causes a non-desired deviation of a system or of one of its components from its normal behaviour. In the literature, a lot of works have been presented to solve the problem of fault diagnosis in the centralized setting such as Basile et al. (2009, 2016); Cabasino et al. (2010); Dotoli et al. (2009); Cabasino et al. (2013a). By taking advantage of the essentially distributed characteristic of real systems, some contributions of decentralized fault diagnosis have been made both in the framework of automata (Debouk et al. (2000)) and in Petri Nets (PNs) (Cabasino et al. (2013b); Fanti et al. (2013); Genc and Lafortune (2007); Jiroveanu and Boel (2006)).

The problem of decentralized fault detection and diagnosis is usually solved by considering two different distributed system settings. Indeed, some works assume that each site, dedicated to perform the fault detection and diagnosis, knows and observes only a part of the system. Such sites can communicate with several nearby sites to improve the diagnosis performance (Jiroveanu and Boel (2006); Genc and Lafortune (2007); Fanti et al. (2013)).

Concerned with the second distributed system setting, each site has the information of the whole net such as its structure and initial marking but can locally observe a subset of the events in a system. Each site locally performs the fault diagnosis and communicates its results with a coordinator that produces the global diagnosis state.

In particular, Debouk et al. (2000) propose a general strategy for decentralized diagnosis in the framework of automata. The main idea of their work is to use three protocols that transmit a different amount of information between the coordinator and the local sites.

Cabasino et al. (2013b) propose a method for the decentralized diagnosis of PNs that extends the centralized approach in Cabasino et al. (2010) to the distributed system setting considered in Debouk et al. (2000). Unlike Debouk et al. (2000), the work in Cabasino et al. (2013b) does not need to enumerate the state space by using an approach based on the notions of basis markings and justifications.

In this paper, we model the system in a PN framework and we suppose that the system is observed by a number of local sites. Each site has the information of the whole system (the structure of the PN) and initial marking but can locally observe the system, i.e., each site can observe a subset of observable transitions. At each observable event occurrence, local sites perform a local fault diagnosis by Integer Linear Programming (ILP) problems.Then, each site transmits its diagnosis state to the coordinator that determines the global diagnosis state by a protocol.

In particular, the protocol proposed in this paper can perform the fault diagnosis by providing the faulty or normal state of the system. Such a protocol can be useful for systems where the occurrence of a fault implies the process stop (permanent faults). The contribution of this work is an extension of a centralized on-line fault diagnosis method presented in Dotoli et al. (2009) to a decentralized architecture. Our proposed communication protocol is very similar to protocol D3 in Debouk et al. (2000) and to Protocol 1 in Cabasino et al. (2013b). However, with respect to the above cited contributions, the proposed work exhibits the following advantages:

10.1016/j.ifacol.2017.08.2390

- unlike Debouk et al. (2000), our approach does not need to enumerate the set of space state that may require a large memory;
- the proposed fault diagnosis technique does not have to be redefined and redesigned whenever the system varies, as in Debouk et al. (2000) and Cabasino et al. (2013b).

The drawback is the use of ILP problems that are NP-hard. However, in some cases depending by the PN structure the authors demonstrate in Dotoli et al. (2009) that the ILP problems can be relaxed to linear programming problems with consequently polynomial complexity.

The paper is structured as follows. Section 2 exposes some basic PN definitions and notations. Section 3 describes the decentralized fault diagnosis problem, while Section 4 introduces the specification of fault diagnosis for the local sites. In Section 5, a protocol is proposed for the communication among local sites and coordinator. Finally, Section 6 summarizes the conclusions and future works.

2. BASIC DEFINITIONS AND NOTATIONS

In this section, we review some basics of PNs (Peterson (1981)).

Definition 1. A PN is a bipartite graph described by the four-tuple $PN = (P, T, Pre, \ Post)$, 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 matrices, respectively, which specify the arcs connecting places and transitions. More precisely, for each $p \in P$ and $t \in T$ element $Pre(p, t)$ $(Post(p, t))$ is equal to a natural number indicating the arc multiplicity if an arc going from p to t (from t to p) exists, and it is equal 0 otherwise. Note that $\mathbb{N}$ is the set of non-negative integers. Matrix $C = Post - Pre$ is the $m \times n$ incidence matrix of the net PN.

The state of a PN is given by its current marking that is a mapping $M : P \to \mathbb{N}^m$, assigning to each place an integer number of tokens. A PN system $\langle PN, M_0\rangle$ is a net PN with an initial marking M_0.

A transition $t_j \in T$ is enabled at M if $M \geq Pre(\cdot, t_j)$ holds and $M[t_j\rangle$ is used to denote that $t_j \in T$ is enabled at marking M. When fired, t_j produces a new marking M', denoted by $M[t_j\rangle M'$ that is computed by the PN state equation $M' = M + C \cdot \overrightarrow{t_j}$, where $\overrightarrow{t_j}$ is an n-dimensional firing vector corresponding to the jth canonical basis vector.

Let $\sigma = t_1 t_2 \ldots t_k$ be a sequence of transitions (firing sequence) and let k be its length. The fact that a transition $t \in T$ appears in the sequence σ is denoted by $t \in \sigma$. The notation $M[\sigma\rangle$ denotes that σ is enabled at M and $M[\sigma\rangle M'$ denotes that the firing of σ yields M'. In addition, $\boldsymbol{\sigma} : T \to \mathbb{N}^n$ is the firing vector associated with a sequence σ. A marking M is said to be reachable from $\langle PN, M_0\rangle$ if there exists a sequence σ such that $M_0[\sigma\rangle M$. A PN having no directed cycles is said to be *acyclic*. The following theorem in Corona et al. (2004) shows an important property of this subclass of PNs.

Theorem 1. Let $\langle PN, M_0\rangle$ be an acyclic PN.

(1) If vector y satisfies equation $M_0 + C \cdot y \geq 0$, there exists a firing sequence σ fireable from M_0 such that $\boldsymbol{\sigma} = y$.
(2) A marking M is reachable from M_0 iff there exists a non-negative integer solution y satisfying the state equation $M = M_0 + C \cdot y$.

A language has been employed to represent the behaviour of a DES. The event set E is regarded as a given alphabet and $L \subseteq E^*$ denotes the set of all words (sequence of events) generated by a DES. If a DES is modeled by a PN system, system events are associated with transitions. Given a PN, the function λ: $T \to E \cup \{\varepsilon\}$ is the transition labeling function that assigns to each transition $t \in T$ either a symbol $e_i \in E$ or the empty string ε.

We assume that the set of transitions is divided into two disjoint subsets, i.e., $T = T_o \cup T_u$, where T_o represents the set of observable transitions and T_u represents the set of unobservable or silent transitions. Consequently, the labeling function is defined as follows: if $t \in T_u$, then $\lambda(t) = \varepsilon$, otherwise $\lambda(t) \neq \varepsilon$.

In this paper, we assume that a label $e_i \in E$ can be associated with only one transition. Thus, the labeling function restricted to T_o is an isomorphism and with no loss of generality we assume $E = T_o$.

Finally, given a net $PN = (P, T, Pre, Post)$ and a subnet $T_A \subseteq T$ of its transitions, we define the T_A-induced subnet of PN as the new net $PN_A = (P, T_A, Pre_A, Post_A)$ where Pre_A and $Post_A$ are the restrictions of Pre and $Post$ to T_A, i.e., PN_A is the net obtained from PN removing all transitions in $T \backslash T_A$, which is denoted by $PN_A \angle_{T_A} PN$.

3. PROBLEM STATEMENT

3.1 Decentralized Diagnosis Architecture and Assumptions

Let $\Delta = \{f_1, f_2, \ldots, f_F\}$ be the set of permanent faults that may occur in a system and F the corresponding cardinality. We model each fault $f_i \in \Delta$ by an unobservable fault transition $\tau_i \in T_f$ with $T_f = \{\tau_1, \tau_2, \ldots, \tau_F\} \subseteq T_u$. The transition set $T_{nf} = \{\tau_{F+1}, \tau_{F+2}, \ldots, \tau_{F+K}\}$ represents the set of K unobservable transitions that are not faulty such that $T_{nf} = T_u \setminus T_f$. It is obvious that we have $O = n - K - F$ observable transitions in total. We extend the form of the transition labeling function to $\lambda : T^* \to E^*$. Then, an observed word w can be associated with the sequence $\sigma \in T^*$, i.e., $w = \lambda(\sigma)$.

This paper focuses on the problem of fault diagnosis in a decentralized setting, as shown in Fig. 1. The system is monitored by a set $\mathcal{J} = \{1, 2, \ldots, J\}$ of sites that perform local fault diagnosis. Each site knows the PN structure and the initial marking but it observes a subset of transitions in the net and different sites can observe different subsets of transitions. Then, the set $T_{o,j} \subseteq T_o$ with cardinality $|T_{o,j}| = O_j$ denotes the set of locally observable transitions for each site $j \in \mathcal{J}$. Any observable transition can be observed by at least one site, i.e., $\bigcup_{j\in\mathcal{J}} T_{o,j} = T_o$. The set of unobservable transitions for each site $j \in \mathcal{J}$ can be defined as:

$$T_{u,j} = T \backslash T_{o,j} = T_{nf} \cup T_f \cup (T_o \backslash T_{o,j}), \qquad (1)$$