Decentralized Diagnosis by Petri Nets and Integer Linear Programming

Publisher version DOI: 10.1109/TSMC.2017.2726108

Decentralized Diagnosis by Petri Nets and Integer Linear Programming

Xuya Cong[ab], Maria Pia Fanti[c*], *Fellow, IEEE*, Agostino Marcello Mangini[c], and Zhiwu Li[da], *Fellow, IEEE*

[a] School of Electro-Mechanical Engineering, Xidian University
No. 2 South Taibai Road, Xi'an 710071, China
e-mail: congxuya@163.com

[b] Key Laboratory of Electronic Equipment Structure Design, Ministry of Education, Xi'an 710071, China.

[c] Department of Electrical and Information Engineering,
Polytechnic of Bari, 70125 Bari, Italy
e-mail: mariapia.fanti@poliba.it; agostinomarcello.mangini@poliba.it

[d] Institute of Systems Engineering, Macau University of Science and Technology, Taipa, Macau
e-mail: zhwli@must.edu.mo

[*]Corresponding author, e-mail: mariapia.fanti@poliba.it

Abstract

This paper proposes a novel decentralized on-line fault diagnosis approach based on the solution of some integer linear programming problems for discrete event systems in a Petri net framework. The decentralized architecture consists of a set of local sites communicating with a coordinator that decides whether the system behaviour is normal or subject to some possible faults. To this aim, some results allow defining the rules applied by the coordinator and the local sites to provide the global diagnosis results. Moreover, two protocols for the detection and diagnosis of faults are proposed: they differ for the information exchanged between local sites and coordinator and the diagnostic capability. In addition, a sufficient and necessary condition under which the diagnosability is achieved in the decentralized architecture is introduced. Finally, some examples are presented to show the efficiency of the proposed approach.

Keywords: Fault diagnosis, Discrete Event Systems, Petri nets, Integer linear programming.

I. 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. Generally, the aim of fault diagnosis is to achieve three complementary tasks: fault detection, fault isolation, and fault identification [1]. Fault detection is a function that determines whether a system is normal or whether a fault has occurred. On the other hand, fault isolation and identification respectively aim at localizing and identifying the system component(s) and the nature of the fault. In this paper we use the terminology of *fault diagnosis* to describe the objective of the detection and localization of a particular fault.

In the related literature, a lot of works are presented to solve the problem of fault detection and diagnosis in the centralized setting [2–9]. On the other hand, many large real systems are physically distributed: for instance manufacturing, transportation and power systems have intrinsically distributed architecture. Hence, such systems take advantage of the natural decomposition in sub systems that can be controlled by decentralized approaches [10]. Consequently, also in the case of fault detection and diagnosis some contributions are presented to deal with such complex problems by exploiting the distributed system setting in the framework of automata [11–16] and Petri Nets (PNs) [17–23].

This paper solves the decentralized fault diagnosis problem in a PN framework on the basis of an extension of the centralized on-line fault detection method presented in [5]. By employing the decentralized diagnosis architecture presented in [12] and [18], we assume that the system is observed by a number of sites. Each site has the information about the system structure (the structure of the PN) and the initial marking but can locally observe the system, i.e., each site can observe a different set of observable transitions. At each observable event occurrence, local diagnosis is performed by the sites that exploit the approach based on some Integer Linear Programming (ILP) problem solutions [5]. By applying a protocol, each site transmits its fault detection information to the coordinator that determines the global diagnosis state. The coordinator does not have any information about the structure and the dynamics of the system and has few computational capabilities. In particular, two diagnosis protocols specify the actions performed by the local sites and the coordinator.

The first protocol (Protocol 1) detects the faulty or normal behaviour of the DES and it can be useful for systems where the occurrence of a fault implies the process stop. More precisely, the coordinator receives the diagnosis results from the local sites and makes a decision (global diagnosis result) just by collecting the information obtained by the sites that observe the last event.

The second protocol (Protocol 2) performs the global diagnosis by detecting the faults occurred

after the observation of an event sequence. Then, the coordinator collects the local diagnosis information, infers the global diagnosis result and sends it to the local sites that use such information for the subsequent fault diagnosis. Also in this case the designed coordinator works with limited memory and computational capability, but it gathers the information received by the local sites in order to make a global decision.

Hence, the key features of the coordinator are the following: i) it performs the fault detection as the centralized diagnoser under a set of assumptions when the distributed setting of the system requires a decentralized approach; ii) it allows the sites to avoid the message exchange among themselves by reducing errors and delays.

Finally, introducing the definition of fault ambiguous sequences, we prove a sufficient and necessary condition under which the diagnosability is achieved in a decentralized architecture by applying Protocol 2.

The rest of the paper is structured as follows. Section II presents a literature review and comments the previous approaches. Section III exposes some basic definitions and notations that are necessary in the paper. Section IV describes the decentralized fault diagnosis problem and recalls the basics of the centralized diagnoser proposed in [5]. Section V introduces the specification of fault diagnosis for the local sites. Moreover, in Section VI some results are proved in order to describe the actions of the local sites and the coordinator under Protocol 1. A second protocol is proposed in Section VII as an extension of the protocol in Section VI and a sufficient and necessary condition under which the diagnosability is achieved in the decentralized architecture is given. Finally, Section VIII analyzes the computational complexity of the proposed diagnosis technique and Section IX presents conclusions and future research.

II. Literature Review

The problem of decentralized fault detection and diagnosis is usually solved by considering two different distributed system settings.

In the first setting each site, dedicated to perform the fault detection and diagnosis, knows and observes only a part of the system. Such sites can communicate with a set of near sites to improve the diagnosis performance. In particular, Jiroveau and Boel [19] present a distributed fault diagnosis method for large systems. The whole process is depicted as different time PN models (each one modeling a local process) that interact with each other by guarded transitions that become enabled only when some conditions are satisfied. The work in [19] considers that

different local agents receive local observation and information from neighboring agents to improve the performance of fault diagnosis. In [21], Genc and Lafortune tackle the on-line fault diagnosis problem. The modular dynamic system consists of a group of place-bordered PNs. Each module is supervised by a diagnoser that has local information only on a part of the system. The paper [21] can detect the occurrence of the faults by the observed word, the structure of the respective PN modules and their connections by common places. Moreover, Fanti *et al.* [20] propose an approach that combines the modular setting presented by Genc and Lafortune [21] and the approach based on the ILP problems proposed in [5]. Compared with the study in [21], the method in [20] computes and communicates the markings of the common places only and it does not need the full generation of reachable states at each event occurrence, thereby avoiding the well known state explosion problem.

Moreover, the codiagnosability is proposed in [28–31], where local diagnosers perform the diagnosis without communicating with the other local sites and the coordinator. In particular, Qiu and Kumar [28] solve the diagnosis problem by building offline non deterministic multiple automata diagnosers. Moreover, Takai and Ushio [29] extend the results of [28] to Mealy automata with nondeterministic output functions: the system has a finite state set and the language is generated by a finite automaton. In addition, Cassez [30] analyzes the fault codiagnosis problem by finite automata and timed automata and the coordinator is a simple agent listening to local diagnosers. Recently, in [31] the authors investigate the relationship between decentralized fault diagnosis and decentralized control of DES under dynamic observations. In particular, they present a new approach for the verification of transition-based codiagnosability on the basis of the property of language-based coobservability.

In the second distributed system setting, each site has perfect knowledge of the PN structure and initial marking but can locally observe a subset of the system events. Each site locally performs the fault detection (diagnosis) and communicates its results with a coordinator that is used to produce the global diagnosis state. In particular, Benveniste *et. al* [17] handle the problem of alarm supervision in the field of telecommunication networks. Their study is based on a net unfolding approach and restricted to safe PNs. Moreover, Debouk *et al.* [12] propose a general strategy for decentralized diagnosis in the framework of automata. They propose three protocols that are based on different levels of information to be transmitted between the coordinator and the local sites. Motivated by the work in [12], Cabasino *et al.* [18] develop a method for the decentralized diagnosis of PNs that extends the centralized approach in [3] and [4] to the

distributed system setting considered in [12]. By using an approach based on the notions of basis markings and justifications [3, 4], the paper [18] does not need to enumerate the state space as in [12].

Now, comparing the proposed approach with the decentralized fault diagnosis presented in the related literature, we consider the three protocols using automata proposed in [12], named here P1, P2 and P3. Protocol P3 of [12] is similar to Protocol 1 of this paper since both require that a local site communicates with the coordinator only when a fault is detected. However, P3 requires enumerating the automata states with the consequent state space explosion. On the other hand, in P1 and P2 of [12] each site communicates to the coordinator all the possible reachable states after each observed event. On the contrary, in Protocol 2 the local sites communicate to the coordinator only the faults that have occurred.

Furthermore, Cabasino *et al.* [18] propose three protocols for decentralized diagnosis in the framework of labeled PNs. However, they need to enumerate the basis markings after each observable transition firing and the structure of the diagnoser is strictly related to the structure of the DES. Similarly, the approaches of [28–31] require the off-line construction of the diagnoser automata for DES with a limited number of states.

On the contrary, the protocols proposed in this paper exploit the advantages from the diagnosis approach proposed in [5]: they do not require off-line calculations based on the structure of the considered PN system. Hence, the proposed protocols turn out to be easily applicable to situations in which the system structure may change.

III. Basic Definitions and Notations

In this section, we review some basics of PNs [24].

A PN is a net structure described by the quadruple $PN = (P, T, \boldsymbol{Pre}, \boldsymbol{Post})$, where: P is a set of m places, T is a set of n transitions, $\boldsymbol{Pre}$: $P \times T \rightarrow \mathbb{N}$ and $\boldsymbol{Post} : P \times T \rightarrow \mathbb{N}$ are the pre- and post-incidence matrices that specify the arcs ($\mathbb{N}$ is the set of non-negative integers). The incidence matrix $\boldsymbol{C}$ of the net is $C = \boldsymbol{Post} - \boldsymbol{Pre}$.

A marking is a vector $\boldsymbol{M} : P \rightarrow \mathbb{N}^m$ that assigns to each place an integer number of tokens. A PN system $\langle PN, \boldsymbol{M}_0 \rangle$ is a net PN with an initial marking $\boldsymbol{M}_0$.

If it holds $\boldsymbol{M} \geq \boldsymbol{Pre}(\cdot, t_j)$ then transition $t_j \in T$ is enabled at $\boldsymbol{M}$: this is denoted by $\boldsymbol{M}[t_j\rangle$. When t_j fires, the new marking $\boldsymbol{M}'$ is reached, i.e., $\boldsymbol{M}[t_j\rangle\boldsymbol{M}'$. Marking $\mathbf{M}'$ is obtained by the PN

state equation $\boldsymbol{M'} = \boldsymbol{M} + \boldsymbol{C} \cdot \boldsymbol{t}_j$, where $\boldsymbol{t}_j$ is an n-dimensional firing vector corresponding to the jth canonical basis vector.

Let $\sigma = t_1 t_2 \dots t_k$ be a sequence of transitions of length k with $\sigma \in T^*$. The fact that a transition $t \in T$ appears in the sequence σ is denoted by $t \in \sigma$. Moreover, the notation $\boldsymbol{M}[\sigma\rangle\boldsymbol{M'}$ denotes that σ is enabled at m and its firing yields $\boldsymbol{M'}$. In addition, $\boldsymbol{\sigma}$: $T \to \mathbb{N}^n$ is the firing vector associated with the sequence σ.

A marking $\boldsymbol{M}$ is said to be reachable from $\langle PN, \boldsymbol{M}_0\rangle$ if there exists a firing sequence σ such that $\boldsymbol{M}_0[\sigma\rangle\boldsymbol{M}$.

A PN having no directed cycles is said to be *acyclic*. Now, if the PN system $\langle PN, \boldsymbol{M}_0\rangle$ is acyclic, then it is proved that a marking $\mathbf{M}$ is reachable from $\mathbf{M}_0$ if and only if there exists a non-negative integer solution $\boldsymbol{y}$ satisfying the state equation $\boldsymbol{M} = \boldsymbol{M}_0 + \boldsymbol{C} \cdot \boldsymbol{y}$ [25], [26].

A language is employed to represent a DES behaviour. 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, which is called the DES language. If a DES is modeled by a PN system, events are associated with transitions.

Now, we define the transition labeling function λ: $T \to E \cup \{\varepsilon\}$ that assigns to each transition $t \in T$ either a symbol $e_i \in E$ or the empty string ε.

Therefore, the set of transitions can be partitioned into two disjoint subsets $T = T_o \cup T_u$, where T_o collects the set of observable transitions and T_u is the set of unobservable or silent transitions. More precisely, 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 $E = T_o$. We extend the form of the transition labeling function to $\lambda : T^* \to E^*$, then it holds $w = \lambda(\sigma)$.

Given a net $PN = (P, T, \boldsymbol{Pre}, \boldsymbol{Post})$ and the subnet $T_A \subset T$ of its transitions, we define the T_A-induced subnet of PN as the new net $PN_A = (P, T_A, \boldsymbol{Pre}_A, \boldsymbol{Post}_A)$, denoted by $PN_A \angle_{T_A} PN$, that results from PN removing all transitions in $T \backslash T_A$, where $\boldsymbol{Pre}_A$ and $\boldsymbol{Post}_A$ are the restrictions of $\boldsymbol{Pre}$ and $\boldsymbol{Post}$ to T_A, respectively.

IV. Problem Statement

A. Decentralized Diagnosis Architecture and Assumptions

Let $\Delta = \{f_1, f_2, \ldots, f_F\}$ be the set of 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.

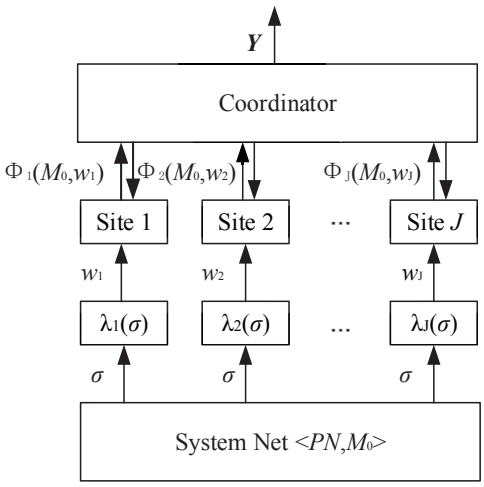

Fig. 1: Decentralized fault diagnosis architecture.

This paper focuses on the problem of fault diagnosis in a decentralized setting, as shown in Fig. 1. The system is supervised by a set $\mathcal{J} = \{1, 2, \ldots, J\}$ of sites that performs 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 $T_{o,j} \subset T_o$ 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:

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

and H_j denotes the cardinality of the transition set $T_{u,j}$.

Moreover, for all sites $j \in \mathcal{J}$, we define the labeling function as follows:

$$\lambda_j(t) = \begin{cases} \lambda(t), & if\ t \in T_{o,j} \\ \varepsilon, & otherwise \end{cases} \tag{2}$$

Now, $w_j = \lambda_j(\sigma)$ is the word associated with the sequence σ in the j-th site.

As depicted in Fig. 1, each site locally executes fault diagnosis once it observes word $w_j = \lambda_j(\sigma)$, i.e., each site waits for an observable event and computes a local diagnosis state. Then, based on such a result, the local site communicates with a coordinator according to a suitable protocol. By some given rules in the related protocol, the coordinator elaborates the information from the local sites and infers whether the system is normal or undergoes some possible faults. In summary, the coordinator determines a global fault diagnosis vector state $\boldsymbol{Y}$.

In this paper, the following assumptions hold for the decentralized fault diagnosis problem.

A1) Two transitions can not share the same label in the net systems.

A2) No unobservable transition fires after the last observable transition of any sequence σ.

A3) The net structure and its initial marking are known by any site $j \in \mathcal{J}$.

A4) The $T_{u,j}$-induced subnet $PN_{u,j} \angle_{T_{u,j}} PN$ is acyclic for any site $j \in \mathcal{J}$.

A5) Any observable transition $t \in T_o$ must be observed by at least one site $j \in \mathcal{J}$.

Assumption A1 guarantees that the system is deterministic since no source of non determinism originating from the fact that different observable transitions share the same label are present. Assumption A2 reports a condition about the silent closure, which is a common assumption in the field of fault diagnosis both in the centralized and decentralized architecture in an *optimistic* approach [5, 20]. Assumption A3 shows the knowledge-level of each site j. Assumption A4 is a standard hypothesis that is stated in decentralized fault diagnosis both in the framework of automata [12] and PNs [18]: cycles of unobservable events in each local site are not permitted, in order to allow local fault detection. Assumption A5 guarantees that each observable transition must be observed by at least one local site.

B. Basics of Centralized Fault Diagnosis

This section briefly reviews basics of the centralized fault diagnosis method in [5] that are also necessary for each local site.

The input of the diagnoser is a PN system $\langle PN, \boldsymbol{M}_0 \rangle$ and an observed word $w \in L$ such that $w = \lambda(\sigma)$, where $\sigma = \sigma_{u_1} t_1 \sigma_{u_2} t_2 \dots \sigma_{u_h} t_h$ $(h \geq 1)$ is the sequence of observable and unobservable transitions corresponding to the word w. In particular, we denote by $\sigma_o \in \sigma$ the

subsequence of σ composed by the observable transitions, i.e., $\sigma_o = t_1 t_2 \dots t_h$ with $t_i \in T_o$, $i = 1, 2, \dots, h$. Moreover, $\sigma_u = \sigma_{u_1} \sigma_{u_2} \dots \sigma_{u_h} \in \sigma$ is the subsequence of the unobservable transitions where each $\sigma_{u_i} \in T_u^*$. By Assumption A1 $E = T_o$, then it holds $\sigma_o = w$. Then, the diagnoser determines whether the system is normal or undergoes some possible faults.

In order to specify the diagnoser, we define the following function, where symbol N denotes the normal behaviour of the system.

Definition 1: [5] Given an initial marking $\boldsymbol{M}_0 \in \mathbb{N}^m$ and a sequence σ_o of observable transitions, we define $\Sigma(\boldsymbol{M}_0, \sigma_o) = \{\sigma \in T^* | \boldsymbol{M}_0[\sigma\rangle, \sigma_o \in \sigma\}$ as the set of interpretations of σ_o at $\boldsymbol{M}_0$.

That is to say, $\Sigma(\boldsymbol{M}_0, \sigma_o)$ is defined as the set of sequences consistent with σ_o.

Definition 2: [5] Given an initial marking $\boldsymbol{M}_0 \in \mathbb{N}^m$ and an observable sequence σ_o, we define the set of interpretations of σ_o at $\boldsymbol{M}_0$ containing fault f_k as: $\Sigma(\boldsymbol{M}_0, \sigma_o, f_k) = \{\sigma \in \Sigma(\boldsymbol{M}_0, \sigma_o) | \tau_k \in \sigma\}$.

Definition 3: [5] Let $\langle PN, \boldsymbol{M}_0 \rangle$ be a PN system and $w \in L$ be an observed word. The (set-valued) function Φ: $\mathbb{N}^m \times T_o^* \to \Delta \cup \{N\}$ assigns to each initial marking $\boldsymbol{M}_0 \in \mathbb{N}^m$ and to each $w \in T_o^*$ the following sets:

1) $\Phi(\boldsymbol{M}_0, w) = \{N\}$ if $\forall f_k \in \Delta$, $\Sigma(\boldsymbol{M}_0, \sigma_o, f_k) = \emptyset$ holds, i.e., there exists no interpretation of σ_o containing a fault transition $\tau_k \in T_f$, then the behaviour of the system is *normal*.
2) $\Phi(\boldsymbol{M}_0, w) = \{f_k \in \Delta | \Sigma(\boldsymbol{M}_0, \sigma_o, f_k) \neq \emptyset, \sigma_o = w\}$, i.e., each interpretation of σ_o includes at least a fault that is collected in $\Phi(\boldsymbol{M}_0, w)$. Then the behaviour of the system is *faulty*.
3) $\Phi(\boldsymbol{M}_0, w) = \{f_k \in \Delta | \Sigma(\boldsymbol{M}_0, \sigma_o, f_k) \neq \emptyset, \sigma_o = w\} \cup \{N\}$, i.e., two possible cases can appear: i) one or more faults are contained in at least one interpretation of σ_o; and ii) there exists at least one interpretation of σ_o without any fault transition. Then, the behaviour of the system is *ambiguous*.

Example 1: Let us consider the PN system of Fig. 2 with $\boldsymbol{M}_0 = [1, 1, 0, 0, 0, 0, 0]^T$. The set of observable transitions is $T_o = \{t_1, t_2, t_3, t_4\}$, and the set of unobservable transitions is $T_u = \{\tau_1, \tau_2, \tau_3\}$, where τ_1 and τ_2 model the faults f_1 and f_2, respectively. Suppose that the observed word $w = \sigma_o = t_1$ occurs at $\boldsymbol{M}_0$. Since it holds $\Sigma(\boldsymbol{M}_0, t_1)$=$\{\tau_1 t_1, t_1\}$, then, by Definition 3, $\Phi(\boldsymbol{M}_0, t_1) = \{f_1, N\}$, i.e., fault f_1 may be occurred but the system may also be normal: the system is ambiguous. Then, assume that the observed word $w = \sigma_o = t_1 t_2$ occurs at $\boldsymbol{M}_0$. We have $\Sigma(\boldsymbol{M}_0, t_1 t_2) = \{\tau_1 t_1 t_2, t_1 \tau_1 t_2\}$: in this case all the interpretations of σ_o contain fault f_1, then $\Phi(\boldsymbol{M}_0, t_1 t_2) = \{f_1\}$, i.e., the system is faulty.

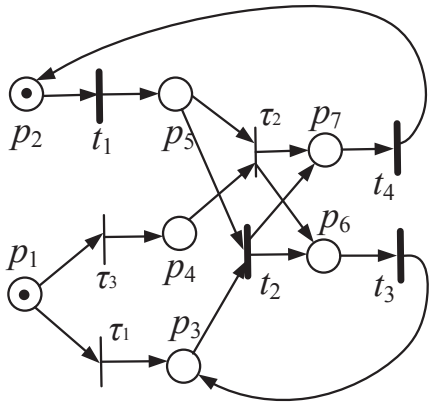

Fig. 2: The PN of Examples 1, 2, 3, 4 and 6.

V. Fault Diagnosis for Local Sites

In this section, the Fault Diagnosis Algorithm (FDA) is designed for each site $j \in \mathcal{J}$ of the PN system derived from the centralized method in [5].

Then, given the transition sequence σ and the word $w_j = \lambda_j(\sigma)$ in the jth site, we denote by $\sigma_u^j \in \sigma$ ($\sigma_o^j \in \sigma$) the subsequence of σ composed of the unobservable (observable) transitions and by $\boldsymbol{\sigma}_u^j \in \mathbb{N}^{K+F+H_j}$ ($\boldsymbol{\sigma}_o^j \in \mathbb{N}^{O_j}$) the corresponding firing vector. Similarly, let $\sigma_f \in \sigma_u^j$ denote the subsequence of σ_u^j composed of the fault transitions and by $\boldsymbol{\sigma}_f$ its corresponding firing vector.

Thus, we review Proposition 12 in [5] in order to provide a local linear algebraic representation of a sequence $\sigma \in T^*$ that is consistent with $w_j = \lambda_j(\sigma) = \sigma_o^j$.

Proposition 1: Consider a site j satisfying Assumptions A1-A5. Given a locally observed word $w_j = \lambda_j(\sigma)$ denoted by $w_j = \sigma_o^j = t_1^j t_2^j \dots t_r^j$, a sequence $\sigma = \sigma_{u_1}^j t_1^j \sigma_{u_2}^j t_2^j \dots \sigma_{u_r}^j t_r^j$ with $|\sigma_{u_i}^j| \geq 0$ for $i = 1, 2, \dots, r$ satisfies $\sigma \in \Sigma(\boldsymbol{M}_0, \sigma_o^j)$ if and only if there exist r firing vectors $\boldsymbol{\sigma}_{u_1}^j, \boldsymbol{\sigma}_{u_2}^j, \dots, \boldsymbol{\sigma}_{u_r}^j$ that satisfy the following set of constraints:
$\xi_j(w_j, \boldsymbol{M}_0, \boldsymbol{Post}, \boldsymbol{Pre}) =$

$$\begin{cases} \boldsymbol{\sigma}_{u_i}^j \in \mathbb{N}^{F+K+H_j}, & for\ i = 1, \dots, r \\ \boldsymbol{C}_u^j \sum_{i=1}^{k} \boldsymbol{\sigma}_{u_i}^j \geq \boldsymbol{Pre} \cdot \boldsymbol{t}_k^j - \boldsymbol{M}_0 - \boldsymbol{C} \sum_{i=1}^{k-1} \boldsymbol{t}_i^j, & for\ k = 1, \dots r \end{cases} \tag{3}$$

where $\boldsymbol{C}_u^j$ is the restriction of the incidence matrix $\boldsymbol{C} = \boldsymbol{Post} - \boldsymbol{Pre}$ to $T_{u,j}$.

Proof: *(Only if)* Assume that $\sigma \in \Sigma(M_0, \sigma_o^j)$ such that $w_j = \lambda_j(\sigma)$, $\sigma = \sigma_{u_1}^j t_1^j \dots \sigma_{u_r}^j t_r^j$ and $\boldsymbol{M}_0[\sigma_{u_1}^j t_1^j\rangle \boldsymbol{M}_1 \dots \boldsymbol{M}_{r-1}[\sigma_{u_r}^j t_r^j\rangle \boldsymbol{M}_r$, in which $\boldsymbol{M}_i$ is the marking reached after the firing of transition t_i^j for $i = 1, \dots, r$. The corresponding firing vectors $\boldsymbol{\sigma}_{u_i}^j$ for $i = 1, \dots, r$ satisfy the enabling condition and the state equation as follows:

$$\boldsymbol{M}_{i-1} + \boldsymbol{C}_u^j \cdot \boldsymbol{\sigma}_{u_i}^j \geq \boldsymbol{Pre} \cdot \boldsymbol{t}_i^j \quad for \quad i = 1, \dots, r \tag{4}$$

$$\boldsymbol{M}_{i-1} + \boldsymbol{C}_u^j \cdot \boldsymbol{\sigma}_{u_i}^j + \boldsymbol{C} \cdot \boldsymbol{t}_i^j = \boldsymbol{M}_i \quad for \quad i = 1, \dots, r \tag{5}$$

By re-writing Eqs. (4) and (5) for each $i = 1, \dots, r$ and recursively deleting all the intermediate markings $\boldsymbol{M}_i$ for $i = 1, \dots, r$ from the derived equations, it holds that $\boldsymbol{C}_u^j \sum_{i=1}^{k} \boldsymbol{\sigma}_{u_i}^j \geq \boldsymbol{Pre} \cdot \boldsymbol{t}_k^j - \boldsymbol{M}_0 - \boldsymbol{C} \sum_{i=1}^{k-1} \boldsymbol{t}_i^j$ for $k = 1, \dots r$ where $\boldsymbol{Pre}$, $\boldsymbol{M}_0$, and $\boldsymbol{C}$ are known terms.

(If) If there exist some firing vectors $\boldsymbol{\sigma}_{u_i}^j$ for $i = 1, \dots, r$ that satisfy the set of constraints $\xi_j(w_j, \boldsymbol{M}_0, \boldsymbol{Post}, \boldsymbol{Pre})$, then we can find a sequence of markings $\boldsymbol{M}_1, \dots, \boldsymbol{M}_{r-1}, \boldsymbol{M}_r$ that satisfies Eqs. (4) and (5). Since the $T_{u,j}$-induced subnet $PN_{u,j} \angle_{T_{u,j}} PN$ is acyclic, there exists a sequence $\sigma = \sigma_{u_1}^j t_1^j \sigma_{u_2}^j t_2^j \dots \sigma_{u_r}^j t_r^j$ that is enabled at $\boldsymbol{M}_0$ and may fire leading to the evolution $\boldsymbol{M}_0[\sigma_{u_1}^j t_1^j\rangle \boldsymbol{M}_1 \dots \boldsymbol{M}_{r-1}[\sigma_{u_r}^j t_r^j\rangle \boldsymbol{M}_r$. Thus, $\sigma \in \Sigma(\boldsymbol{M}_0, \sigma_o^j)$. □

Algorithm 1 provides the FDA that is performed by each site $j \in \mathcal{J}$. Before introducing the FDA, we introduce the following definitions and recall two propositions proved in [5].

The (set-valued) function Φ_j: $\mathbb{N}^m \times T_{o,j}^* \to \Delta \cup \{N\}$ assigns to each initial marking $\boldsymbol{M}_0 \in \mathbb{N}^m$ and to each $w_j \in T_{o,j}^*$ the following sets:

1) $\Phi_j(\boldsymbol{M}_0, w_j) = \{N\}$ if $\forall f_k \in \Delta$, $\Sigma(\boldsymbol{M}_0, \sigma_o^j, f_k) = \emptyset$ holds, the behaviour is *normal* for site j;
2) $\Phi_j(\boldsymbol{M}_0, w_j) = \{f_k \in \Delta | \Sigma(\boldsymbol{M}_0, \sigma_o^j, f_k) \neq \emptyset, \sigma_o^j = w_j\}$, the behaviour is *faulty* for site j;
3) $\Phi_j(\boldsymbol{M}_0, w_j) = \{f_k \in \Delta | \Sigma(\boldsymbol{M}_0, \sigma_o^j, f_k) \neq \emptyset, \sigma_o^j = w_j\} \cup \{N\}$, the behaviour is *ambiguous* for site j.

Proposition 2: Consider a site j satisfying Assumptions A1-A5. Given a locally observed word $w_j = \lambda_j(\sigma)$ denoted by $w_j = \sigma_o^j = t_1^j t_2^j \dots t_r^j$, the ILP problem, named ILPP 1, is defined as:

$$\begin{cases} max\ \varphi_{1,j}(\boldsymbol{\sigma}_{u_1}^j, \boldsymbol{\sigma}_{u_2}^j, \dots, \boldsymbol{\sigma}_{u_r}^j) = \sum_{i=1}^{r} \boldsymbol{\sigma}_{u_i}^j(\tau_\theta) \\ s.t.\ \ \xi_j(w_j, \boldsymbol{M}_0, \boldsymbol{Post}, \boldsymbol{Pre}) \end{cases}$$

Algorithm 1: FDA to determine $\Phi_j(\boldsymbol{M}_0, w_j)$.

Input: $\langle PN, \boldsymbol{M}_0 \rangle$, w_j

Output: $\Phi_j(\boldsymbol{M}_0, w_j)$

1. *Initialization*

   $r := |w_j|$, $\Phi_j(\boldsymbol{M}_0, w_j) := \emptyset$, $\boldsymbol{\varphi}_{1,j}^{max} \in \mathbb{N}^F$, $\boldsymbol{\varphi}_{1,j}^{max} := \mathbf{0}_F$

2. *Deciding the faults that may have occurred*

   for each $f_\theta \in \Delta$ **do**

   Solve ILPP 1

   $z_{1,j} = max\ \varphi_{1,j}(\boldsymbol{\sigma}_{u_1}^j, \boldsymbol{\sigma}_{u_2}^j, \ldots, \boldsymbol{\sigma}_{u_r}^j)$ s.t. $\xi_j(w_j, \boldsymbol{M}_0, \boldsymbol{Post}, \boldsymbol{Pre})$

   $\varphi_{1,j}^{max}(\theta) := z_{1,j}$

   if $\varphi_{1,j}^{max}(\theta) > 0$ **then**

   $\Phi_j(\boldsymbol{M}_0, w_j) := \Phi_j(\boldsymbol{M}_0, w_j) \cup \{f_\theta\}$

   end for

3. *Check if the behaviour is normal*

   if $\boldsymbol{\varphi}_{1,j}^{max} = \mathbf{0}_F$ **then**

   $\Phi_j(\boldsymbol{M}_0, w_j) := \{N\}$ and go to Step 5

4. *Check if the behaviour can be normal*

   Solve ILPP 2

   $z_{2,j} = min\ \varphi_{2,j}(\boldsymbol{\sigma}_{u_1}^j, \boldsymbol{\sigma}_{u_2}^j, \ldots, \boldsymbol{\sigma}_{u_r}^j)$ s.t. $\xi_j(w_j, \boldsymbol{M}_0, \boldsymbol{Post}, \boldsymbol{Pre})$

   if $z_{2,j} = 0$ **then** $\Phi_j(\boldsymbol{M}_0, w_j) := \Phi_j(\boldsymbol{M}_0, w_j) \cup \{N\}$

5. Returning to the condition of recording the events

6. End

If for $\tau_\theta \in T_f$ ILPP 1 admits a solution $\boldsymbol{\sigma}_{u_1}^j, \boldsymbol{\sigma}_{u_2}^j, \ldots, \boldsymbol{\sigma}_{u_r}^j$ and $\varphi_{1,j}(\boldsymbol{\sigma}_{u_1}^j, \boldsymbol{\sigma}_{u_2}^j, \ldots, \boldsymbol{\sigma}_{u_r}^j) = \varphi_{1,j}^{max}(\theta) > 0$ with $\boldsymbol{\varphi}_{1,j}^{max} \in \mathbb{N}^F$, then $\sigma = \sigma_{u_1}^j t_1^j \sigma_{u_2}^j t_2^j \ldots \sigma_{u_r}^j t_r^j \in \Sigma(\boldsymbol{M}_0, \sigma_o^j, f_\theta)$ holds.

Proposition 3: Consider a site j satisfying Assumptions A1-A5. Given a locally observed word $w_j = \lambda_j(\sigma)$ denoted by $w_j = \sigma_o^j = t_1^j t_2^j \ldots t_r^j$, the ILP problem, named ILPP 2, is defined as:

$$\begin{cases} min\ \varphi_{2,j}(\boldsymbol{\sigma}_{u_1}^j, \boldsymbol{\sigma}_{u_2}^j, \ldots, \boldsymbol{\sigma}_{u_r}^j) = \mathbf{1}_F^T \sum_{i=1}^{r} \boldsymbol{\sigma}_{f_i} \\ s.t.\ \ \xi_j(w_j, \boldsymbol{M}_0, \boldsymbol{Post}, \boldsymbol{Pre}) \end{cases}$$

where $\mathbf{1}_F^T$ is the F dimensional column vector with each element being 1.

If ILPP 2 does not find a solution $\boldsymbol{\sigma}_{u_1}^j, \boldsymbol{\sigma}_{u_2}^j, \ldots, \boldsymbol{\sigma}_{u_r}^j$ such that its objective function $\varphi_{2,j}^{min} = 0$, then the system is faulty for this site.

Now, we briefly describe the details of Algorithm 1. The inputs of Algorithm 1 are the net system and the observable event sequence of the jth site. In Step 1, we initialize the variables of the algorithm and define vector $\boldsymbol{\varphi}_{1,j}^{max} \in \mathbb{N}^F$ that saves the objective values $z_{1,j}$ of ILPP 1 for each $f_\theta \in \Delta$. In Step 2, we define and solve ILPP 1 for each $f_\theta \in \Delta$ and save its corresponding objective value in $\varphi_{1,j}^{max}(\theta)$. If ILPP 1 finds a solution $\boldsymbol{\sigma}_{u_1}^j, \boldsymbol{\sigma}_{u_2}^j, \ldots, \boldsymbol{\sigma}_{u_r}^j$ for f_θ and its objective value $z_{1,j} > 0$, then by [5], we have that $\sigma = \sigma_{u_1}^j t_1^j \sigma_{u_2}^j t_2^j \ldots \sigma_{u_r}^j t_r^j \in \Sigma(\boldsymbol{M}_0, \sigma_o^j, f_\theta)$ and $\Phi_j(\boldsymbol{M}_0, w_j) = \Phi_j(\boldsymbol{M}_0, w_j) \cup \{f_\theta\}$. Furthermore, Step 3 determines whether the system is normal for the site j: if $\boldsymbol{\varphi}_{1,j}^{max} = \mathbf{0}_F$ (we denote by $\mathbf{0}_F$ the vector of F elements equal to 0), then the site j provides $\Phi_j(\boldsymbol{M}_0, w_j) = \{N\}$, i.e., the system is normal for the site j. In addition, Step 4 checks if there exists at least one interpretation of σ_o^j that does not contain any fault transition. Thus, ILPP 2 is defined. If its objective value $z_{2,j} = 0$, then $N \in \Phi_j(\boldsymbol{M}_0, w_j)$, i.e., the system is ambiguous for site j.

VI. Decentralized Fault Diagnosis

In this section, first we prove some results in order to provide rules for the coordinator to detect the global faulty behaviour of the system. Second, based on these propositions, we define Algorithm 2, namely Protocol 1 that is devoted to decide if the behaviour of the paper is faulty or normal.

A. Results for Decentralized Fault Diagnosis

Definition 4: Assume that $w = t_1 t_2 \ldots t_h$ $(h \geq 1)$ is the observed word and $w_j = t_1^j t_2^j \ldots t_r^j$ $(r \leq h)$ is the locally observed word of the site j. $\mathcal{J}^* = \{j \in \mathcal{J} | t_r^j = t_h\}$ is defined as the set of sites that can observe the last event in the word w.

Remark 1 ensures that $\mathcal{J}^* \subseteq \mathcal{J}$ cannot be empty.

Remark 1: Under Assumption A5, for each $t \in T_o$, there exists at least a site j such that $t \in T_{o,j}$. Thus, the set of sites that can observe the last event in the word w $(w \neq \varepsilon)$ is not empty, i.e., $\mathcal{J}^* \neq \emptyset$.

Based on Remark 1, Proposition 4 shows the relationships between interpretations of σ_o at $\boldsymbol{M}_0$ and the interpretations of σ_o^j at $\boldsymbol{M}_0$ for each site $j \in \mathcal{J}^*$.

Proposition 4: Consider the observed word $w \in L$ at $\boldsymbol{M}_0$ and $w = \sigma_o$. Under Assumption A4, for each site $j \in \mathcal{J}^*$, $\Sigma(\boldsymbol{M}_0, \sigma_o) \subseteq \Sigma(\boldsymbol{M}_0, \sigma_o^j)$ holds.

Proof: By Remark 1 (where Assumption A4 necessarily holds), we have $\mathcal{J}^* \neq \emptyset$. Since $T_{u,j} \supset T_u$ and $T_{o,j} \subset T_o$ for each $j \in \mathcal{J}^*$, then $w_j \in w$ and $\sigma_o^j \in \sigma_o$ hold. If there exists $\sigma \in \Sigma(\boldsymbol{M}_0, \sigma_o)$ with $w = \lambda(\sigma)$, then we can find a sequence $\sigma_o^j \in \sigma_o$ such that $\sigma_o^j = w_j = \lambda_j(\sigma)$. We conclude that $\Sigma(\boldsymbol{M}_0, \sigma_o) \subseteq \Sigma(\boldsymbol{M}_0, \sigma_o^j)$ is true. □

Example 2: Consider the net in Fig. 2. Assume that the net system consists of two sites with the sets of observable transitions $T_{o,1} = \{t_1, t_3\}$ and $T_{o,2} = \{t_2, t_4\}$, respectively.

Assume that the observable word $w = \sigma_o = t_1 t_2 t_3$ occurs at $\boldsymbol{M}_0$. Thus, only site 1 is in $\mathcal{J}^*$ and $w_1 = \sigma_o^1 = t_1 t_3$. Since it holds $\Sigma(\boldsymbol{M}_0, \sigma_o) = \{\tau_1 t_1 t_2 t_3, t_1 \tau_1 t_2 t_3\}$ and $\Sigma(\boldsymbol{M}_0, \sigma_o^1) = \{\tau_1 t_1 t_2 t_3, t_1 \tau_1 t_2 t_3, \tau_3 t_1 \tau_2 t_3, t_1 \tau_3 \tau_2 t_3\}$, then $\Sigma(\boldsymbol{M}_0, \sigma_o) \subseteq \Sigma(\boldsymbol{M}_0, \sigma_o^1)$ is true.

The following property ensures that ILPP 1 in Algorithm 1 for any site $j \in \mathcal{J}^*$ always admits a solution, i.e., we can obtain a non-empty fault diagnosis result for each site $j \in \mathcal{J}^*$.

Property 1: Under Assumptions A1-A5, for any site $j \in \mathcal{J}^*$, the output of Algorithm 1 is not empty, i.e., $\Phi_j(\boldsymbol{M}_0, w_j) \neq \emptyset$.

Proof: By Remark 1 (where Assumption A5 necessarily holds), we have $\mathcal{J}^* \neq \emptyset$. Since $w = \lambda(\sigma)$ where $\sigma = \sigma_{u_1} t_1 \ldots \sigma_{u_h} t_h$ with $h \geq 1$, we have $\sigma \in \Sigma(\boldsymbol{M}_0, \sigma_o)$, i.e., $\Sigma(\boldsymbol{M}_0, \sigma_o) \neq \emptyset$. By Proposition 4, $\Sigma(\boldsymbol{M}_0, \sigma_o^j) \neq \emptyset$ is true. According to Proposition 1 (where Assumptions A1-A5 necessarily hold), ILPP 1 of Algorithm 1 admits a solution for any site $j \in \mathcal{J}^*$, leading to $\Phi_j(\boldsymbol{M}_0, w_j) \neq \emptyset$. □

The following Proposition is a rule for a coordinator to decide whether the system is normal according to the information of a local site.

Proposition 5: Consider the observed word $w \in L$ at $\boldsymbol{M}_0$ and $w = \sigma_o$. Under Assumptions A1-A5, if there exists a site $j \in \mathcal{J}^*$ that computes $\Phi_j(\boldsymbol{M}_0, w_j) = \{N\}$, then $\Phi(\boldsymbol{M}_0, w) = \{N\}$ holds.

Proof: By Remark 1 (where Assumption A5 necessarily holds), we have $\mathcal{J}^* \neq \emptyset$. Under Assumptions A1-A5, we obtain $\Phi_j(\boldsymbol{M}_0, w_j)$ from Algorithm 1. Since there exists a site $j \in \mathcal{J}^*$ in which $\Phi_j(\boldsymbol{M}_0, w_j) = \{N\}$, by Definition 3, we have $\Sigma(\boldsymbol{M}_0, \sigma_o^j, f_k) = \emptyset$ for each $f_k \in \Delta$, i.e., there exists no sequence in $\Sigma(\boldsymbol{M}_0, \sigma_o^j)$ that contains a fault transition. According to Proposition 4, there exists no sequence in $\Sigma(\boldsymbol{M}_0, \sigma_o)$ that contains a fault transition either. Thus, it holds $\Sigma(\boldsymbol{M}_0, \sigma_o, f_k) = \emptyset$ for each $f_k \in \Delta$, i.e., $\Phi(\boldsymbol{M}_0, w) = \{N\}$ and the proposition is proved. □

Moreover, the following proposition provides a rule for the coordinator to determine whether a system is faulty according to the information of a local site.

Proposition 6: Consider the observed word $w \in L$ at $\boldsymbol{M}_0$ and $w = \sigma_o$. Under Assumptions A1-A5, if there exists a site $j \in \mathcal{J}^*$ that computes $N \notin \Phi_j(\boldsymbol{M}_0, w_j)$, then $N \notin \Phi(\boldsymbol{M}_0, w)$ holds, i.e., the system is faulty.

Proof: By Remark 1 (where Assumption A5 necessarily holds), we have $\mathcal{J}^* \neq \emptyset$. Under Assumptions A1-A5, we obtain $\Phi_j(\boldsymbol{M}_0, w_j)$ from Algorithm 1. By assumption, $N \notin \Phi_j(\boldsymbol{M}_0, w_j)$, then all the sequences in $\Sigma(\boldsymbol{M}_0, \sigma_o^j)$ contain at least one fault transition. According to Proposition 4, $\Sigma(\boldsymbol{M}_0, \sigma_o) \subseteq \Sigma(\boldsymbol{M}_0, \sigma_o^j)$, then $N \notin \Phi(\boldsymbol{M}_0, w)$, i.e., the system is faulty during the observed word w. Thus, the conclusion holds. □

Now the following proposition allows the coordinator to determine the fault that has occurred in the system.

Proposition 7: Consider the observed word $w \in L$ at $\boldsymbol{M}_0$ and $w = \sigma_o$. Under Assumptions A1-A5, if there exists a site $j \in \mathcal{J}^*$ that computes $\Phi_j(\boldsymbol{M}_0, w_j) = \{f_\theta\}$ with $f_\theta \in \Delta$, then $\Phi(\boldsymbol{M}_0, w) = \{f_\theta\}$ holds.

Proof: Since $\Phi_j(\boldsymbol{M}_0, w_j) = \{f_\theta\}$ with $f_\theta \in \Delta$, i.e., $N \notin \Phi_j(\boldsymbol{M}_0, w_j)$ for a site $j \in \mathcal{J}^*$, then by Proposition 6 (where Assumptions A1-A5 necessarily hold), the system is faulty, i.e., $N \notin \Phi(\boldsymbol{M}_0, w)$. Moreover, since $f_k \notin \Sigma(\boldsymbol{M}_0, \sigma_o^j)\ \forall k \in \{1, 2, \ldots, F\}$ and $k \neq \theta$ for the site j, by Definition 3, $\Sigma(\boldsymbol{M}_0, \sigma_o^j, f_k) = \emptyset\ \forall k \in \{1, 2, \ldots, F\}$ and $k \neq v$. According to Proposition 4, $\Phi(\boldsymbol{M}_0, w) = \{f_\theta\}$ and the thesis holds. □

Proposition 7 implies that if only one fault is detected in a local site and the system cannot be normal for this site, then it is possible to decide that such a fault has occurred in the system and the system is faulty.

Example 3: Consider the PN system in Fig. 2. Assume that the observable word $w = t_1 t_2 = \sigma_o$ occurs at $\boldsymbol{M}_0$. Thus, only site 2 is in $\mathcal{J}^*$ and $w_2 = \sigma_o^2 = t_2$. By Algorithm 1 and Proposition 7, we have $\Phi_2(\boldsymbol{M}_0, w_2) = \{f_1\}$ and $\Phi(\boldsymbol{M}_0, w) = \{f_1\}$.

B. Fault Diagnosis under Protocol 1

This subsection presents a protocol applied by the coordinator in order to determine whether the system behaviour is faulty or normal. The following definition specifies the system output diagnosis states performed by the coordinator.

Definition 5: The output of the coordinator is a vector $\boldsymbol{Y} \in \{0,1\}^{F+2}$ that at each observed event can provide the following *diagnosis states* under Protocol 1:

1) $Y(1) = 1$, if the system behaviour is *faulty*, $Y(1) = 0$ otherwise.
2) $Y(2) = 1$, if the system behaviour is *normal*, $Y(2) = 0$ otherwise .
3) $Y(k+2) = 1$ for $k = 1, ..., F$, if the system is *faulty* and $f_k \in \Delta$ occurred, $Y(k+2) = 0$ otherwise.

Based on the aforementioned results, Algorithm 2 is proposed to solve the problem of decentralized fault diagnosis.

Now, we discuss the detailed steps of Algorithm 2. Step 1 initializes vector $\boldsymbol{Y}$ and Step 2 waits for a new transition $t \in T_o$ firing. In Step 3.1, each site $j \in \mathcal{J}^*$ receives an observable event associated with transition $t \in T_o$. In Step 3.2, site j performs Algorithm 1 and obtain $\Phi_j(\boldsymbol{M}_0, w_j)$. In Step 3.3, if $N \notin \Phi_j(\boldsymbol{M}_0, w_j)$, i.e., the system cannot be normal for this site, then it sends $\Phi_j(\boldsymbol{M}_0, w_j)$ to the coordinator. In this case, in Step 3.3.1, if $\Phi_j(\boldsymbol{M}_0, w_j) = \{f_k\}$ then it sends f_k to the coordinator. Moreover, if $\Phi_j(\boldsymbol{M}_0, w_j) = \{N\}$, i.e., the system is normal for this site, then it sends N to the coordinator in Step 3.4.

In addition, Steps 4.1-4.4 are performed by the coordinator. More precisely, in Step 4.1 according to Proposition 7, if there exists a site $j \in \mathcal{J}^*$ such that the system is faulty and only one fault $f_k \in \Delta$ is detected, then the system is faulty and f_v has occurred in the system. Hence, the coordinator updates the diagnosis states $Y(1) = 1$, $Y(2) = 0$ and $Y(k+2) = 1$. In Step 4.2, according to Proposition 6, if there exists a site $j \in \mathcal{J}^*$ that detects a faulty behaviour, then the system is faulty, the coordinator updates the diagnosis states $Y(1) = 1$ and $Y(2) = 0$. In Step 4.3, according to Proposition 5, if there exists a site $j \in \mathcal{J}^*$ such that the system is normal, then the system behaviour is normal and the coordinator updates the diagnosis state $Y(2) = 1$. In this case, the algorithm goes to Step 2 to wait a new event. Finally, if $\boldsymbol{Y} = \boldsymbol{0}_{F+2}$, then the coordinator cannot determine whether the system is faulty or normal, then the algorithm returns to Step 2 to wait a new event.

Example 4: Consider the net in Fig. 2. Assume that the observable sequence $\sigma_o = t_1 t_2$ occurs at $\boldsymbol{M}_0$. The centralized diagnoser in [5] provides the following results: $\Phi(\boldsymbol{M}_0, t_1) = \{f_1, N\}$, $\Phi(\boldsymbol{M}_0, t_1 t_2) = \{f_1\}$.

Now, Protocol 1 is applied. First, let consider $\sigma_o = t_1$. Then, site 1 provides $\Phi_1(\boldsymbol{M}_0, t_1) = \{f_1, N\}$ and according to Protocol 1, site 1 does not send any information to the coordinator that does not provide any result.

Algorithm 2: Protocol 1

Input: $\langle PN, M_0 \rangle$

Output: $\boldsymbol{Y}$

1. $\boldsymbol{Y} := \mathbf{0}_{F+2}$

2. Wait until a new observable transition $t \in T_o$ fires.

3. **Steps performed by each site** $j \in \mathcal{J}^*$

3.1. $w'_j := w_j$ and $w_j := w'_j \lambda_j(t)$.

3.2. Site j computes $\Phi_j(\boldsymbol{M}_0, w_j)$ by Algorithm 1

3.3. **if** $N \notin \Phi_j(\boldsymbol{M}_0, w_j)$

then send $\Phi_j(\boldsymbol{M}_0, w_j)$ to the coordinator.

end if

3.3.1. **if** $\Phi_j(\boldsymbol{M}_0, w_j) = \{f_\theta\}$

then send $\Phi_j(\boldsymbol{M}_0, w_j)$ to the coordinator

end if

3.4. **if** $\Phi_j(\boldsymbol{M}_0, w_j) = \{N\}$ **then**

transmit $\Phi_j(\boldsymbol{M}_0, w_j)$ to the coordinator.

end if

4. **Steps performed by the coordinator**

4.1. **If** the coordinator receives $\Phi_j(\boldsymbol{M}_0, w_j) = \{f_k\}$,

then it sets $Y(1) = 1$, $Y(2) = 0$ and $Y(k+2) = 1$.

Output $\boldsymbol{Y}$ and go to step 5.

4.2. **If** the coordinator receives $\Phi_j(\boldsymbol{M}_0, w_j)$ and $N \notin \Phi_j(\boldsymbol{M}_0, w_j)$,

then it sets $Y(1) = 1$ and $Y(2) = 0$.

Output $\boldsymbol{Y}$ and go to Step 5

4.3. **If** the coordinator receives $\Phi_j(\boldsymbol{M}_0, w_j) = \{N\}$

then it sets $Y(2) = 1$.

Output $\boldsymbol{Y}$ and go to Step 2.

4.4. **if** $\boldsymbol{Y} = \mathbf{0}_{F+2}$ **then** go to Step 2.

5. End

Now, let $\sigma_o = t_1 t_2$: only site 2 performs its local fault diagnosis and provides $\Phi_2(\boldsymbol{M}_0, t_2) = \{f_1\}$. According to Protocol 1, it transmits $\Phi_2(\boldsymbol{M}_0, t_2) = \{f_1\}$ to the coordinator. The coordinator sets $Y(1) = 1$, $Y(2) = 0$ and $Y(3) = 1$. Finally, the output of Protocol 1 is $\boldsymbol{Y} = [1, 0, 1, 0]^T$, then the occurrence of fault f_1 is detected as in the centralized case [5].

VII. Decentralized Fault Diagnosis and Diagnosability Analysis

This section proposes a protocol that can be applied by the local sites and the coordinator in order to determine not only the faulty behaviour of the system but also the occurred faults. In order to improve the quality of the fault diagnosis, it is necessary to introduce new results and an additional ILP problem that the local sites have to solve. Moreover, the diagnosability achieved in the decentralized setting by applying the presented second protocol is proved.

A. New Results for Decentralized Diagnosis

The following proposition proves that it is possible to decide if all the sequences in the set $\Sigma(\boldsymbol{M}_0, \sigma_o^j)$ contain the same fault transition $\tau_\theta \in T_f$ by solving a new ILP problem.

Proposition 8: Consider a site j satisfying Assumptions A1-A5. Given a locally observed word $w_j = \lambda_j(\sigma)$ denoted by $w_j = \sigma_o^j = t_1^j t_2^j \dots t_r^j$, an ILP problem named ILPP 3 is defined as:

$$\begin{cases} min\ \varphi_{3,j}(\boldsymbol{\sigma}_{u_1}^j, \boldsymbol{\sigma}_{u_2}^j, \dots, \boldsymbol{\sigma}_{u_r}^j) = \sum_{i=1}^{r} \boldsymbol{\sigma}_{u_i}^j(\tau_\theta) \\ s.t.\ \ \xi_j(w_j, \boldsymbol{M}_0, \boldsymbol{Post}, \boldsymbol{Pre}) \end{cases}$$

If for $\tau_\theta \in T_f$ ILPP 3 admits a solution $\boldsymbol{\sigma}_{u_1}^j, \boldsymbol{\sigma}_{u_2}^j, \dots, \boldsymbol{\sigma}_{u_r}^j$ with $\varphi_{3,j}^{min}(\theta) > 0$ and $\boldsymbol{\varphi}_{3,j}^{min} \in \mathbb{N}^F$, then all the interpretations of σ_o contain the fault transition τ_θ, i.e., $\Sigma(\boldsymbol{M}_0, \sigma_o^j, f_\theta) = \Sigma(\boldsymbol{M}_0, \sigma_o^j)$.

Proof: According to Definition 2, it holds $\Sigma(\boldsymbol{M}_0, \sigma_o^j, f_\theta) \subseteq \Sigma(\boldsymbol{M}_0, \sigma_o^j)$. We prove $\Sigma(\boldsymbol{M}_0, \sigma_o^j, f_\theta) = \Sigma(\boldsymbol{M}_0, \sigma_o^j)$ by contradiction, assuming that $\Sigma(\boldsymbol{M}_0, \sigma_o^j, f_\theta) \neq \Sigma(\boldsymbol{M}_0, \sigma_o^j)$. Since $\Sigma(\boldsymbol{M}_0, \sigma_o^j, f_\theta) \subseteq \Sigma(\boldsymbol{M}_0, \sigma_o^j)$, there exists a sequence $\sigma = \sigma_{u_1}^j t_1^j \dots \sigma_{u_r}^j t_r^j$ such that $\sigma \in \Sigma(\boldsymbol{M}_0, \sigma_o^j)$ and $\sigma \notin \Sigma(\boldsymbol{M}_0, \sigma_o^j, f_\theta)$, i.e., $\tau_\theta \notin \sigma$. Hence, we infer that $\sigma_{u_i}^j(\tau_\theta) = 0$ for all $i \in \{1, \dots, r\}$, i.e., $\varphi_{3,j}^{min}(\theta) = 0$ which contradicts $\varphi_{3,j}^{min}(\theta) > 0$. The conclusion holds. □

Based on Proposition 8, Proposition 9 provides a rule for the coordinator to determine whether a particular fault has occurred.

Proposition 9: Under Assumptions A1-A5, if there exists a site $j \in \mathcal{J}^*$ in which the solution of the ILPP3 gives $\varphi_{3,j}^{min}(\theta) > 0$ for w_j with $\theta \in \{1, 2, \dots, F\}$, then $f_\theta \in \Phi(\boldsymbol{M}_0, w)$ and $N \notin \Phi(\boldsymbol{M}_0, w)$ holds.

Proof: If there exists a site j where the solution of the ILPP 3 provides $\varphi_{3,j}^{min}(\theta) > 0$ for w_j, by Proposition 8 it holds $\Sigma(\boldsymbol{M}_0, \sigma_o^j, f_\theta) = \Sigma(\boldsymbol{M}_0, \sigma_o^j)$. According to Property 4, all the sequences in $\Sigma(\boldsymbol{M}_0, \sigma_o)$ also contain the fault f_θ, i.e., $N \notin \Phi(\boldsymbol{M}_0, w)$ and $f_\theta \in \Phi(\boldsymbol{M}_0, w)$. □

Moreover, we propose Propositions 10 and 11 to show the relations between the fault diagnosis results of two observed words, which can be used to reduce the computational cost of Protocol 2.

Proposition 10: Given two observed words $w' = \sigma_o' = t_1 t_2 \dots t_q$ and $w = w'u = \sigma_o' \dots t_h = t_1 t_2 \dots t_q \dots t_h$ $(q < h)$, if $N \notin \Phi(\boldsymbol{M}_0, w')$, then $N \notin \Phi(\boldsymbol{M}_0, w)$ holds.

Proof: Let us assume that the h firing vectors $\boldsymbol{\sigma}_{u_1}, \boldsymbol{\sigma}_{u_2}, \dots, \boldsymbol{\sigma}_{u_h}$ are solutions of the set of constraints $\xi(w, \boldsymbol{M}_0, \boldsymbol{Post}, \boldsymbol{Pre})$ in [5]. By Proposition 12 in [5], the q firing vectors $\boldsymbol{\sigma}_{u_1}, \boldsymbol{\sigma}_{u_2}, \dots, \boldsymbol{\sigma}_{u_q}$ can also be a solution for the set of constraints $\xi(w', \boldsymbol{M}_0, \boldsymbol{Post}, \boldsymbol{Pre})$. That is to say, for each sequence $\sigma = \sigma_{u_1} t_1 \sigma_{u_2} t_2 \dots \sigma_{u_h} t_h \in \Sigma(\boldsymbol{M}_0, \sigma_o)$, there exists a sequence σ' such that $\sigma' = \sigma_{u_1} t_1 \sigma_{u_2} t_2 \dots \sigma_{u_q} t_q \in \Sigma(\boldsymbol{M}_0, \sigma_o')$ with $q < h$.

Now, we prove $N \notin \Phi(\boldsymbol{M}_0, w)$ by contradiction. Suppose that $N \in \Phi(\boldsymbol{M}_0, w)$. By Definition 3, there is at least one sequence $\sigma = \sigma_{u_1} t_1 \sigma_{u_2} t_2 \dots \sigma_{u_h} t_h \in \Sigma(\boldsymbol{M}_0, \sigma_o)$ that does not contain any fault transition. Thus, we have $\sigma' = \sigma_{u_1} t_1 \sigma_{u_2} t_2 \dots \sigma_{u_q} t_q \in \Sigma(\boldsymbol{M}_0, \sigma_o')$ that neither contains any fault transition. That is to say, $N \in \Phi(\boldsymbol{M}_0, w')$ which contradicts $N \notin \Phi(\boldsymbol{M}_0, w')$. The conclusion holds. □

Proposition 11: Given two observed words $w' = \sigma_o' = t_1 t_2 \dots t_q$ and $w = w'u = \sigma_o' \dots t_h = t_1 t_2 \dots t_q \dots t_h$ $(q < h)$, if $\forall \sigma' \in \Sigma(\boldsymbol{M}_0, \sigma_o')$, there exists a fault $f_\theta \in \Delta$ such that $\tau_\theta \in \sigma'$ then $f_\theta \in \Phi(\boldsymbol{M}_0, w)$ and $N \notin \Phi(\boldsymbol{M}_0, w)$ hold.

Proof: By Proposition 12 in [5], there exists at least one sequence $\sigma' = \sigma_{u_1} t_1 \sigma_{u_2} t_2 \dots \sigma_{u_q}\ t_q \in \Sigma(\boldsymbol{M}_0, \sigma_o')$ such that $\sigma = \sigma_{u_1} t_1 \sigma_{u_2} t_2 \dots \sigma_{u_h} t_h \in \Sigma(\boldsymbol{M}_0, \sigma_o)$ with $h > q$. Since all the sequences in $\Sigma(\boldsymbol{M}_0, \sigma_o')$ contain the fault transition τ_θ, there exists at least one sequence $\sigma \in \Sigma(\boldsymbol{M}_0, \sigma_o)$ that contains the fault transition τ_θ, i.e., $f_\theta \in \Phi(\boldsymbol{M}_0, w)$.

Since all the sequences in $\Sigma(\boldsymbol{M}_0, \sigma_o')$ contain τ_θ, then $N \notin \Phi(\boldsymbol{M}_0, w')$. By Proposition 10, we have $N \notin \Phi(\boldsymbol{M}_0, w)$ and the conclusion holds. □

Proposition 12: Given two observed words $w' = \sigma_o' = t_1 t_2 \dots t_q$ and $w = w'u = \sigma_o' \dots t_h = t_1 t_2 \dots t_q \dots t_h$ $(q < h)$, under Assumptions A1-A5, if there exists a site $j \in \mathcal{J}^*$ in which $\Phi_j(M_0, w_j') = \{f_\theta\}$ with $f_\theta \in \Delta$, then $f_\theta \in \Phi(\boldsymbol{M}_0, w)$ and $N \notin \Phi(\boldsymbol{M}_0, w)$ hold.

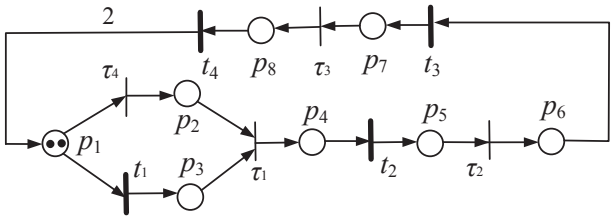

Fig. 3: The PN of Examples 5 and 7.

Proof: Since there exists a site $j \in \mathcal{J}^*$ in which $\Phi_j(\boldsymbol{M}_0, w'_j) = \{f_\theta\}$, according to Proposition 7, we have $\Phi(\boldsymbol{M}_0, w') = \{f_\theta\}$, i.e., the system is faulty. Hence, all the sequences in $\Sigma(\boldsymbol{M}_0, \sigma'_o)$ contain the fault transition τ_θ. By Proposition 11, we have $f_\theta \in \Phi(\boldsymbol{M}_0, w)$ and $N \notin \Phi(\boldsymbol{M}_0, w)$. The conclusion holds. □

Proposition 13: Given two observed words $w' = \sigma'_o = t_1 t_2 \dots t_q$ and $w = w'u = \sigma'_o \dots t_h = t_1 t_2 \dots t_q \dots t_h$ $(q < h)$, under Assumptions A1-A5, if there exists a site $j \in \mathcal{J}^*$ in which $\varphi^{min}_{3,j}(\theta) > 0$ for w'_j, then $f_\theta \in \Phi(\boldsymbol{M}_0, w)$ and $N \notin \Phi(\boldsymbol{M}_0, w)$ hold.

Proof: Since there exists a site $j \in \mathcal{J}^*$ in which $\varphi^{min}_{3,j}(\theta) > 0$ for w'_j, according to the proof of Proposition 9, all the sequences in $\Sigma(\boldsymbol{M}_0, \sigma'_o)$ contain the fault f_θ. By Proposition 11, we have $f_\theta \in \Phi(\boldsymbol{M}_0, w)$ and $N \notin \Phi(\boldsymbol{M}_0, w)$. The conclusion holds. □

Example 5: Consider the net in Fig. 3. Let us assume $T_o = \{t_1, t_2, t_3, t_4\}$ and $T_u = \{\tau_1, \tau_2, \tau_3, \tau_4\}$, where transitions τ_1, τ_2, and τ_3 represent faults f_1, f_2, and f_3, respectively. Assume that the system is locally observed by two sites with the sets of observable transitions $T_{o,1} = \{t_1, t_3\}$ and $T_{o,2} = \{t_2, t_4\}$, respectively.

Let $w' = t_1 t_2$ and $w = t_1 t_2 t_3$ be two observed words. For the word w', site 2 observes $w'_2 = t_2$ and it obtains $\Phi_2(\boldsymbol{M}_0, t_2) = \{f_1\}$ by Algorithm 1. According to Proposition 12, we have $f_1 \in \Phi(\boldsymbol{M}_0, t_1 t_2 t_3)$ and $N \notin \Phi(\boldsymbol{M}_0, t_1 t_2 t_3)$.

Now consider that t_4 occurs, i.e., $w' = t_1 t_2 t_3$ and $w = t_1 t_2 t_3 t_4$. For the word w', site 1 observes $w'_1 = t_1 t_3$ and it obtains $\Phi_1(\boldsymbol{M}_0, t_1 t_3) = \{f_1, f_2\}$ by Algorithm 1. In addition, we have $\varphi^{min}_{3,1}(1) = 1$ and $\varphi^{min}_{3,1}(2) = 1$ for w'_1. According to Proposition 13, it holds $f_1 \in \Phi(\boldsymbol{M}_0, t_1 t_2 t_3 t_4)$, $f_2 \in \Phi(\boldsymbol{M}_0, t_1 t_2 t_3 t_4)$, and $N \notin \Phi(\boldsymbol{M}_0, t_1 t_2 t_3 t_4)$.

B. Fault Diagnosis under Protocol 2

On the basis of the previous results, Protocol 2 is presented in Algorithm 3 and the steps of the protocol are discussed. We remark that in Protocol 2 the coordinator receives the diagnosis decisions from the local sites and, when the diagnosis state is updated, the coordinator sends it to the local sites.

In Step 1, the coordinator and the sites define vector $\boldsymbol{Y} = \mathbf{0}_{F+2}$.

All the sites wait for a new observable transition. The sites that observe a new event (the corresponding transition fires) compute $\Phi_j(\boldsymbol{M}_0, w_j)$ by Algorithm 1 (see Step 3.2).

In Step 3.3, if $N \notin \Phi_j(\boldsymbol{M}_0, w_j)$ then by Proposition 6, the behaviour of the system is faulty and the site transmits $\Phi_j(\boldsymbol{M}_0, w_j)$ to the coordinator. In this case the site tries to determine the faults that have occurred.

If $\Phi_j(\boldsymbol{M}_0, w_j) = \{f_\theta\}$ then by Proposition 7 the system is faulty and the fault f_θ occurred (Step 3.3.1). Hence, the site transmits the fault to coordinator that updates in Step 4 $Y(1) = 1$, $Y(2) = 0$ and $Y(\theta + 2) = 1$.

On the contrary, the site has to check if the fault $f_\theta \in \Phi_j(\boldsymbol{M}_0, w_j)$ has occurred (step 3.3.2). To this aim the site checks whether the fault occurred during a previous observation (if $Y(\theta+2) = 0$), in such a case, by Proposition 11, the fault occurred after the last observation. Hence, the site solves the ILPP 3: if the result is $\varphi_{3,j}^{min}(\theta) > 0$, then the site sends f_θ to the coordinator.

In Step 3.4, if $\Phi_j(\boldsymbol{M}_0, w_j) = \{N\}$ then the site transmits $\Phi_j(\boldsymbol{M}_0, w_j)$ to the coordinator.

Step 4 is performed by the coordinator that does not update the diagnosis state if it did not receive any message from the local sites. On the contrary, it updates the values of $\boldsymbol{Y}$: if $\Phi_j(\boldsymbol{M}_0, w_j) = \{N\}$ then $Y(2) = 1$ else $Y(1) = 1$, $Y(2) = 0$ and $Y(\theta + 2) = 1$ for each f_θ that the coordinator received.

Finally, the coordinator sends the updated diagnosis state $\boldsymbol{Y}$ to each site $j \in \mathcal{J}$.

Example 6: Consider the net in Fig. 2. Assume that the observable word $w = \sigma_o = t_1t_2t_3t_4$ occurs at $\boldsymbol{M}_0$. A centralized diagnoser in [5] produces the following results: $\Phi(\boldsymbol{M}_0, t_1) = \{f_1, N\}$, $\Phi(\boldsymbol{M}_0, t_1t_2) = \{f_1\}$, $\Phi(\boldsymbol{M}_0, t_1t_2t_3) = \{f_1\}$, and $\Phi(\boldsymbol{M}_0, t_1t_2t_3t_4) = \{f_1\}$.

Now, assume that the sites and the coordinator apply Protocol 2. First, let $w = \sigma_o = t_1$: it holds $w_1 = t_1$ and $w_2 = \varepsilon$ for sites 1 and 2, respectively. Then, only site 1 provides $\Phi_1(\boldsymbol{M}_0, t_1) = \{f_1, N\}$ and does not send any information to the coordinator that cannot determine whether the system is faulty or normal and does not provide any result.

Algorithm 3: Protocol 2

Input: $\langle PN, \boldsymbol{M}_0 \rangle$

Output: $\boldsymbol{Y}$

1. $w_j := \varepsilon$, the coordinator and each site $j \in \mathcal{J}$ set $\boldsymbol{Y} := \boldsymbol{0}_{F+2}$.

2. Wait until a new observable transition $t \in T_o$ fires.

3. **Steps performed by each site** $j \in \mathcal{J}^*$

   3.1. $w'_j := w_j$ and $w_j := w'_j \lambda_j(t)$.

   3.2. Site j computes $\Phi_j(\boldsymbol{M}_0, w_j)$ by Algorithm 1.

   3.3. **if** $N \notin \Phi_j(\boldsymbol{M}_0, w_j)$ **then**

   site j transmits $\Phi_j(\boldsymbol{M}_0, w_j)$ to the coordinator.

   3.3.1. **if** $\Phi_j(\boldsymbol{M}_0, w_j) = \{f_\theta\}$ **then**

   site j transmits f_θ to the coordinator and **go to** Step 4

   3.3.2. **for** $\theta = 1$ to F

   if $f_\theta \in \Phi_j(\boldsymbol{M}_0, w_j)$ and $Y(\theta + 2) = 0$ **then** site j solves ILPP 3 for f_θ

   if $\varphi_{3,j}^{min}(\theta) > 0$ **then**

   site j transmits f_θ to the coordinator.

   end for

   3.4. **if** $\Phi_j(\boldsymbol{M}_0, w_j) = \{N\}$ **then**

   site j transmits $\Phi_j(\boldsymbol{M}_0, w_j)$ to the coordinator.

4. **Steps performed by the coordinator**

   4.1. **if** the coordinator does not receive any message from the local sites

   then go to Step 2.

   4.2. **if** the coordinator receives $\Phi_j(\boldsymbol{M}_0, w_j) = \{N\}$,

   then it sets $Y(2) = 1$ and **go to** Step 5

   else it sets $Y(1) = 1$ and $Y(2) = 0$

   4.3. **if** the coordinator receives f_θ, **then** it sets $Y(\theta + 2) = 1$.

5. The coordinator transmits to each $j \in \mathcal{J}$ vector $\boldsymbol{Y}$, outputs $\boldsymbol{Y}$ and **go to** Step 2.

Let $w = \sigma_o = t_1t_2$ and it holds $w_1 = t_1$ and $w_2 = t_2$: only site 2 performs the local fault diagnosis and provides $\Phi_2(\boldsymbol{M}_0, t_2) = \{f_1\}$. Site 2 transmits f_1 to the coordinator that sets $Y(1) = 1$, $Y(2) = 0$ and $Y(3) = 1$. Then, the output of Protocol 2 is vector $\boldsymbol{Y} = [1, 0, 1, 0]^T$ that is received by each site.

Let $w = \sigma_o = t_1t_2t_3$: it holds $w_1 = t_1t_3$ and $w_2 = t_2$ for sites 1 and 2, respectively. Only site 1 performs the local fault diagnosis and computes $\Phi_1(\boldsymbol{M}_0, t_1t_3) = \{f_1, f_2\}$. Since $Y(4) = 0$, site 1 solves ILPP 3 for f_2 and obtains $\varphi_{3,1}^{min}(2) = 0$. Thus, fault f_2 did not occur and it is not transmitted to the coordinator. The coordinator does not update the diagnosis state $\boldsymbol{Y}$.

Finally, t_4 occurs: $w = \sigma_o = t_1t_2t_3t_4$, $w_1 = t_1t_3$ and $w_2 = t_2t_4$. Then, site 2 provides $\Phi_2(\boldsymbol{M}_0, t_2t_4) = \{f_1\}$ and, since $Y(3) = 1$ then site 2 does not solve ILPP 3. Hence, the output of Protocol 2 remains $\boldsymbol{Y} = [1, 0, 1, 0]^T$ which detects the occurrence of fault f_1.

Example 7: Now, consider the net in Fig. 3 and assume that the observable word $w = t_1t_2t_3t_4$ occurs at $\boldsymbol{M}_0$. The centralized diagnoser of [5] gives $\Phi(\boldsymbol{M}_0, t_1) = \{N\}$, $\Phi(\boldsymbol{M}_0, t_1t_2) = \{f_1\}$, $\Phi(\boldsymbol{M}_0, t_1t_2t_3) = \{f_1, f_2\}$, and $\Phi(\boldsymbol{M}_0, t_1t_2t_3t_4) = \{f_1, f_2, f_3\}$.

The decentralized diagnosis performed by Protocol 2 provides the following results:

- $w = \sigma_o = t_1$, $w_1 = t_1$ and $w_2 = \varepsilon$, site 1 provides $\Phi_1(\boldsymbol{M}_0, t_1) = \{N\}$ and the coordinator sets and transmits $\boldsymbol{Y} = [0, 1, 0, 0, 0]^T$, i.e., the behaviour is normal;
- $w = \sigma_o = t_1t_2$, $w_1 = t_1$ and $w_2 = t_2$, site 2 provides $\Phi_2(\boldsymbol{M}_0, t_2) = \{f_1\}$ and the coordinator sets $\boldsymbol{Y} = [1, 0, 1, 0, 0]^T$, i.e., fault f_1 occurred;
- $w = \sigma_o = t_1t_2t_3$, $w_1 = t_1t_3$ and $w_2 = t_2$, site 1 provides $\Phi_1(\boldsymbol{M}_0, t_1t_3) = \{f_1, f_2\}$, solves ILPP 3 for f_2 and obtains $\varphi_{3,1}^{min}(2) = 1$. The coordinator transmits $\boldsymbol{Y} = [1, 0, 1, 1, 0]^T$, i.e., f_1 and f_2 occurred;
- $w = t_1t_2t_3t_4$, $w_1 = t_1t_3$ and $w_2 = t_2t_4$, site 2 provides $\Phi_2(\boldsymbol{M}_0, t_2t_4) = \{f_1, f_2, f_3\}$, solves the ILPP 3 for f_3 and obtains $\varphi_{3,2}^{min}(3) = 1$. Hence, the coordinator sets $\boldsymbol{Y} = [1, 0, 1, 1, 1]^T$, i.e., the diagnosis is that f_1, f_2 and f_3 occurred.

C. Diagnosability in the Decentralized Setting

In this section, we prove a sufficient and necessary condition under which the diagnosability is achieved in the decentralized architecture by applying Protocol 2. In order to analyse this issue, a fault ambiguous sequence is defined.

Definition 6: Consider a PN system $\langle PN, \boldsymbol{M}_0 \rangle$, the set of observable transitions T_o and a word $w \in L$. Given a fault transition $\tau_k \in T_f$, a sequence $\sigma \in \Sigma(\boldsymbol{M}_0, \sigma_o)$, such that $\sigma_0 = w$ and $\tau_k \in \sigma$, is said to be *fault ambiguous* wrt τ_k if $\exists \sigma' \neq \sigma$ such that $\sigma' \in \Sigma(\boldsymbol{M}_0, \sigma_o)$ and $\sigma' \notin \Sigma(\boldsymbol{M}_0, \sigma_o, f_k)$.

In other words, a sequence $\sigma \in \Sigma(\boldsymbol{M}_0, \sigma_o)$ is fault ambiguous wrt the fault transition τ_k if there exists an interpretation $\sigma' \neq \sigma$ of σ_o that does not contain τ_k.

Definition 7: Consider a PN system $\langle PN, \boldsymbol{M}_0 \rangle$ and the set of observable transitions T_o. The system is said to be τ_k-diagnosable, if all the sequences σ such that $w = \lambda(\sigma)$ with $w \in L$ are not fault ambiguous wrt τ_k.

Definition 8: Consider a PN system $\langle PN, \boldsymbol{M}_0 \rangle$, a site set $\mathcal{J} = \{1, 2, \ldots, J\}$ and the set of locally observable transitions $T_{o,j} \subset T_o$ for each $j \in \mathcal{J}$. Given a fault transition $\tau_k \in T_f$, a word $w \in L$, a sequence $\sigma \in \Sigma(\boldsymbol{M}_0, \sigma_o)$, such that $\sigma_o = w$ and $\tau_k \in \sigma$, σ is said to be *fault ambiguous* wrt τ_k and $\mathcal{J}$, if the following two conditions are satisfied:

1) $\forall j \in \mathcal{J}$, given $\sigma_o^j = w_j = \lambda_j(\sigma)$, $\exists \sigma' \neq \sigma$ and $\sigma' \in \Sigma(\boldsymbol{M}_0, \sigma_o^j)$, such that $\sigma' \notin \Sigma(\boldsymbol{M}_0, \sigma_o^j, f_k)$,
2) $\forall \sigma' \in \Sigma(\boldsymbol{M}_0, \sigma_o)$, it holds $\sigma' \in \Sigma(\boldsymbol{M}_0, \sigma_o, f_k)$.

That is to say, a sequence σ containing a fault transition $\tau_k \in T_f$ is fault ambiguous wrt a set of sites if, 1) the sequence σ is ambiguous for each local site wrt τ_k, i.e., in each local site its observation has at least one local interpretation that does not contain τ_k; and 2) the sequence σ is not ambiguous wrt τ_k in the PN system.

Now the following proposition about the diagnosability performed by Protocol 2 is proved:

Proposition 14: Let $\langle PN, \boldsymbol{M}_0 \rangle$ be a PN system supervised by a set $\mathcal{J} = \{1, 2, \ldots, J\}$ of sites and $\tau_k \in T_f$ be the fault transition associated with $f_k \in \Delta$. Assume that the system is τ_k-diagnosable. $\langle PN, \boldsymbol{M}_0 \rangle$ is also τ_k-diagnosable in the decentralized architecture under Protocol 2 if and only if there is no fault ambiguous sequence wrt τ_k and $\mathcal{J}$.

Proof: (*If*) Given a fault transition $\tau_k \in T_f$, if there is no fault ambiguous sequence $\sigma \in T^*$ wrt τ_k and $\mathcal{J}$, then $\exists j \in \mathcal{J}$ such that $\forall \sigma \in \Sigma(\boldsymbol{M}_0, \sigma_o^j)$ it holds $\sigma \in \Sigma(\boldsymbol{M}_0, \sigma_o^j, f_k)$. Then each sequence in $\Sigma(\boldsymbol{M}_0, \sigma_o^j)$ contains τ_k: according to Protocol 2, site j and the coordinator detect the fault. Thus, the fault is also diagnosable in the decentralized architecture by Protocol 2.

(*Only if*) We prove the proposition by contradiction. Assume that there exists a fault ambiguous sequence σ wrt τ_k and $\mathcal{J}$ and the system is τ_k-diagnosable. Hence, by Definition 11 it holds $\forall j \in \mathcal{J}$, given $\sigma_o^j = w_j = \lambda_j(\sigma)$, $\exists \sigma' \neq \sigma$ and $\sigma' \in \Sigma(\boldsymbol{M}_0, \sigma_o^j)$, such that $\sigma' \notin \Sigma(\boldsymbol{M}_0, \sigma_o^j, f_k)$.

In this case, Protocol 2 can not detect the fault f_k: this contradicts the assumption that the system is τ_k-diagnosable in the decentralized architecture under Protocol 2. □

On the basis of Proposition 14, given a τ_k-diagnosable PN system supervised by a set $\mathcal{J}$ of sites with $\bigcup_{j\in\mathcal{J}} T_{o,j} = T_o$, the possibility of detecting a fault ambiguous sequence wrt τ_k and $\mathcal{J}$ decreases if the number of observable transition increases in each site (see the proof of Proposition 4). As a consequence the diagnosis capability of Protocol 2 improves.

VIII. Computational Complexity

This section discusses the computational complexity of Protocols 1 and 2.

First, we consider the computational complexity of Protocol 1. In Protocol 1, each site $j \in \mathcal{J}^*$ solves at most $F+1$ ILP problems that are NP hard. As known, the computational cost of solving an ILP problem mainly depends on the number of constraints and variables. From Eq. (3), we have $r \cdot (F + K + H_j)$ variables and $r \cdot m$ constraints for each of ILP problem in the worst case, where r is the length of the word w_j, F is the cardinality of the set of T_f, K is the cardinality of the set of T_{nf}, H_j is the cardinality of the set of $T_{u,j}$, and m is the number of places in the whole net.

As for the computational complexity of Protocol 2, we note that each site $j \in \mathcal{J}^*$ needs to solve $2F + 1$ ILP problems in the worst case.

As a result, the on-line computational cost of Protocols 1 and 2 increases with the number of observed events. To overcome this drawback, it is shown and proved in [5] that if the subnet $PN_{u,j}\angle_{T_{u,j}}PN$ is an acyclic state machine and $\langle PN, \boldsymbol{M}_0\rangle$ is bounded, then each basic solution of the LP relaxations of ILPPs 1, 2, and 3 is an integer-valued solution. In such a case the solution of each ILPP can be obtained in real time.

IX. Conclusion

This paper extends the centralized on-line fault detection method presented in [5] to a distributed system architecture by proposing a new decentralized diagnosis strategy. To this aim some results are proved in order to propose two protocols performed by a set of local sites and a coordinator. At each observable event occurrence, local diagnosis is performed by the sites that exploit the approach based on some Integer Linear Programming (ILP) problem solutions. The two protocols are defined by the diagnostic information and operation managed by the local

sites, the communication exchanged between the sites and the coordinator and the coordinator decision rules.

Using the first protocol the coordinator provides the faulty or normal system state by collecting the local site diagnosis. However, in this case the coordinator simply listens the local diagnosis states.

By the second protocol the coordinator collects the local diagnosis information, communicates and gathers the information received by the local sites and makes a global decision. In this case, the coordinator can be able to single out the occurred fault by exploiting a larger computational effort of the local sites with respect to the first protocol.

We remark the following issues of the decentralized diagnosis in comparison with the centralized approach:

- it is necessary to define the communication protocol between the local sites and the coordinator;
- each site has to consider a larger number of unobservable transitions with a consequent reduction of the diagnosis capability;
- the computational complexity of each local site diagnosis does not change.

On the other hand, when a centralized diagnosis is not possible due to the physically distributed nature of the underlying system, it is necessary to use decentralized diagnosers possessing the own set of sensors and computational capability.

Finally, some results about the diagnosability achieved by the proposed decentralized architecture is proved.

Future work will focus on the decentralized fault diagnosis problem in more complex system settings, for instance in the case of an event that is associated with more transitions.

REFERENCES

[1] J. Zaytoon and S. Lafortune, "Overview of fault diagnosis methods for discrete event systems," *Annu. Rev. Control*, vol. 37, no. 2, pp. 308–320, Dec. 2013.

[2] F. Basile, P. Chiacchio, and G. De Tommasi, "An efficient approach for online diagnosis of discrete event systems," *IEEE Trans. Autom. Control*, vol. 54, no. 4, pp. 748–759, Apr. 2009.

[3] M. P. Cabasino, A. Giua, and C. Seatzu, "Fault detection for discrete event systems using Petri nets with unobservable transitions," *Automatica*, vol. 46, no. 9, pp. 1531–1539, Sep. 2010.

[4] M. P. Cabasino, A. Giua, M. Pocci, and C. Seatzu, "Discrete event diagnosis using labeled Petri nets. An application to manufacturing systems," *Control Eng. Pract.*, vol. 19, no. 9, pp. 989–1001, Sep. 2011.

[5] M. Dotoli, M. P. Fanti, A. M. Mangini, and W. Ukovich, "On-line fault detection in discrete event systems by Petri nets and integer linear programming," *Automatica*, vol. 45, no. 11, pp. 2665–2672, Nov. 2009.

[6] M. P. Cabasino, A. Giua, and C. Seatzu, "Diagnosis using labeled Petri nets with silent or undistinguishable fault events," *IEEE Trans. Syst. Man Cybern. Syst.*, vol. 43, no. 2, pp. 345–355, Mar. 2013.

[7] M. P. Cabasino, A. Giua, and C. Seatzu, "Diagnosability of discrete-event systems using labeled Petri nets," *IEEE Trans. Autom. Sci. Eng.*, vol. 11. no. 1, pp. 144-153, Jan. 2014.

[8] A. Ramirez-Trevino, E. Ruiz-Beltran, I. Rivera-Rangel, and E. Lopez- Mellado, "Online fault diagnosis of discrete event systems. A Petri net-based approach," *IEEE Trans. Autom. Sci. Eng.*, vol. 4, no. 1, pp. 31–39, Jan. 2007.

[9] C. Mahulea, C. Seatzu, M. P. Cabasino, and M. Silva, "Fault diagnosis of discrete-event systems using continuous Petri nets," *IEEE Trans. Syst. Man Cybern.-Part A: Syst. Humans*, vol. 42, no. 4, pp. 970–984, Jul. 2012.

[10] J. H. Ye, Z. W. Li, and A. Giua, "Decentralized supervision of Petri nets with a coordinator," *IEEE Trans. Syst. Man Cybern. Syst.*, vol. 45, no. 6, pp. 955–966, Jun. 2015.

[11] R. K. Boel, and J. H. van. Schuppen, "Decentralized failure diagnosis for discrete-event systems with costly communication between diagnosers," in *Proc. 6th Workshop Discrete Event Syst.*, Zaragoza, Spain, Oct. 2002, pp. 175–181.

[12] R. Debouk, S. Lafortune, and D. Teneketzis, "Coordinated decentralized protocols for failure diagnosis of discrete-event systems," *Discrete Event Dyn. Syst.*, vol. 10, no. 1, pp. 33–86, Jan. 2000.

[13] R. Su, W. M. Wonham, J. Kurien, and X. Koutsoukos, "Distributed diagnosis for qualitative systems," in *Proc. 6th Workshop Discrete Event Syst.*, Zaragoza, Spain, Oct. 2002, pp. 169–174.

[14] Y. Wang, T.-S. Yoo, and S. Lafortune, "Diagnosis of discrete event systems using

decentralized architectures," *Discrete Event Dyn. Syst.*, vol. 17, no. 2, pp. 233–263, Jun. 2007.

[15] S. Yokota, T. Yamamoto, and S. Takai, "Computation of the delay bounds and synthesis of diagnosers for decentralized diagnosis with conditional decisions," *Discrete Event Dyn. Syst.*, vol. 21, no. 1, pp. 45–84, Mar. 2017.

[16] W. Qiu and R. Kumar, "Distributed diagnosis under bounded-delay communication of immediately forwarded local observations," *IEEE Trans. Syst. Man Cybern. Part A: Syst Humans*, vol, 38 no. 3, pp. 628–643, Apr. 2008.

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

[18] M. P. Cabasino, A. Giua, A. Poali, and C. Seatzu, "Decentralized diagnosis of discrete-event systems using labeled Petri nets," *IEEE Trans. Syst. Man Cybern. Syst.*, vol. 43, no. 6, pp. 1477–1485, Nov. 2013.

[19] G. Jiroveanu and R. K. Boel, "A distributed approach for fault detection and diagnosis based on time Petri nets," *Math. Comput. Simul.*, vol. 70, no. 1, pp. 287–313, Feb. 2006.

[20] M. P. Fanti, A. M. Mangini, and W. Ukovich, "Fault detection by labeled Petri nets in centralized and distributed approaches," *IEEE Trans. Autom. Sci. Eng.*, vol. 10, no. 2, pp. 392–404, Apr. 2013.

[21] S. Genc and S. Lafortune, "Distributed diagnosis of place-bordered Petri nets," *IEEE Trans. Autom. Sci. Eng.*, vol. 4, no. 2, pp. 206–219, Apr. 2007.

[22] J. Arámburo-Lizárraga, A.Ramírez-Treviño, and E. López-Mellado, "Optimal communication distributed Petri net based diagnosers of discrete event systems," in *8th Int. Conf. Electr. Eng., Comput. Sci. Autom. Control.*, Merida City, Mexico, Oct, 2011, pp. 1–7.

[23] F. Basile, P. Chiacchio, and G. De Tommasi, "Decentralized K-diagnosability of Petri nets," in *Proc. 11th Workshop Discrete Event Syst.*, vol. 45, no. 9, 2012, pp. 214-220.

[24] J. L. Peterson, *Petri net theory and the modeling of systems*, Englewood Cliffs, NJ, USA: Prentice Hall, 1981.

[25] A. Ichikawa and K. Hiraishi. "Analysis and control of discrete event systems represented by Petri nets," *Discrete Event Systems: models and applications*, Springer Berlin Heidelberg, pp. 115–134, 1988.

[26] Y. Li and W. M. Wonham, "Control of vector discrete-event systems. II. Controller

synthesis," *IEEE Trans. Autom. Control*, vol. 39, no. 3, pp. 512–531, Mar. 1994.

[27] M. Sampath, R. Sengupta, S. Lafortune, K. Sinnamohideen, and D. Teneketzis, "Diagnosability of discrete event systems," *IEEE Trans. Autom. Control*, vol. 40, no. 9, pp. 1555–1575, Sep. 1995.

[28] W. Qiu and R. Kumar, "Decentralized failure diagnosis of discrete event systems," *IEEE Trans. Syst. Man Cybern.-Part A: Syst. Humans*, vol. 36, no. 2, pp. 384–395, Feb. 2006.

[29] S. Takai and T. Ushio, "Verification of codiagnosability for discrete event systems modeled by Mealy automata with nondeterministic output functions," *IEEE Trans. Autom. Control*, vol. 57, no. 3, pp.798–804, Jan. 2012.

[30] F. Cassez, "The complexity of codiagnosability for discrete event and timed systems," *IEEE Trans. Autom. Control*, vol. 57, no. 7, pp. 1752–1764, Jan. 2012.

[31] X. Yin and S. Lafortune, "Codiagnosability and coobservability under dynamic observations: Transformation and verification," *Automatica*, vol. 61, pp. 241–252, Sep. 2015.

[32] M. P. Cabasino, A. Giua, A. Paoli, and C. Seatzu, "Decentralized diagnosability analysis of discrete event systems using Petri nets," in *Proc. IFAC World Congr.*, Milan, Italy, Aug. 2011, pp. 6060–6066.