Decentralized diagnosis of Petri nets

Maria Paola Cabasino, Alessandro Giua, Andrea Paoli, Carla Seatzu

Abstract—In this paper we deal with the problem of failure diagnosis of discrete event systems with decentralized information. The decentralized architecture that we use is composed by a set of sites communicating their diagnosis information with a coordinator that is responsible of detecting the occurrence of failures in the system. In particular, we define two protocols that differ for the amount of information exchanged between the local sites and the coordinator, and the rules adopted by the coordinator to compute the global diagnosis states.

I. INTRODUCTION

In this paper we present some preliminary results on the decentralized diagnosis of Petri nets (PNs) based on the results that some of us presented in the centralized case [4], [5]. In particular, we propose an approach for diagnosis of PNs with decentralized information that combines the work of Debouk et al. [8] with our approach in [4], [5]. We start from the same decentralized architecture considered in [4], [5] and from a series of similar assumptions on the considered model. However, here we solve the decentralized diagnosis problem in the context of PNs, while the approach in [8] is in the framework of automata. This enables us to keep the advantages of the centralized approach we proposed in [4], [5].

We assume that the system is monitored by a set of sites. Each site knows the structure of the net and the initial marking but observes the evolution of the system with a different mask, i.e., the set of observable transitions is different for each site. Diagnosis is locally performed using the approach we previously introduced in [4], [5] whose main feature is that of avoiding an exhaustive enumeration of the set of sequences that may have fired given the actual observation. It is also based on the definition of four diagnosis states, each of which can be associated with a number from 0 to 3, depending on the degree of alarm. For instance, 3 is used to capture the fact that the fault has occurred for sure, whereas 0 captures the fact that the fault has not occurred for sure.

Using its own observation, each site performs diagnosis and, according to a given protocol, communicates it, eventually with some other information, to the coordinator who calculates global diagnosis states. In particular, two different protocols are defined that differ for the amount of information exchanged between the coordinator and the local sites, and vice versa. In both cases an important property is proved, namely that the coordinator never produces false alarms. Finally, the diagnosability property under decentralization is investigated.

A. Literature review

The problem of failure detection has received a lot of attention in industrial systems in the past few decades. Solving a problem of diagnosis means that we associate to each observed string of events a diagnosis state, such as “normal” or “faulty” or “uncertain”. In the literature a lot of contributions have been presented for discrete event systems in the centralized framework, e.g., [1], [5], [12], [15], [16]. Due to the intrinsic distributed nature of the real systems, a lot of distributed diagnosis techniques, that take advantage of the natural decompositions of a modular system, have been studied both dealing with automata [3], [7], [8], [13], [14] and PNs [2], [9], [10].

In particular, in [2] Benveniste et al. solved a problem of alarm supervision in telecommunication networks. They use an unfolding approach and they restrict their attention to safe PNs.

In [9] Genc and Lafortune address the problem of detecting and isolating faults or other significant events in the behavior of a modular dynamic system that is modeled as a set of interacting PN modules. Faults are modeled by unobservable events and the common places among the set of PNs modeling a system capture coupling of various system components. The objective is to diagnose the occurrence of fault events based on the sequence of observed events and on the structure of the respective PN modules and their coupling by common places. Obtaining a distributed diagnosis algorithm that takes advantage of the modular structure of the system is sought.

In [10] Jiroveanu and Boel propose an algorithm for the model based design of a distributed protocol for fault detection and diagnosis for very large systems. The overall process is modeled as different time PN models that interact with each other via guarded transitions that become enabled only when certain conditions are satisfied. Different local agents receive local observation as well as messages from neighboring agents. Each agent estimates the state of the part of the overall process for which it has model and from which it observes events by reconciling observations with model based predictions. They design algorithms that use limited information exchange between agents and that can quickly decide questions about whether and where a fault
occurred and whether or not some components of the local processes have operated correctly. The algorithms they derive allow each local agent to generate a preliminary diagnosis prior to any communication and they show that after the communications among agents the diagnosis performances are the same as in the central case.

After a comparison between our approach and the distributed approaches described above, we can conclude that both the problem formulation and the objective in [2] are different from those in this paper. On the other hand, the main difference between our approach and the approaches in [9], [10] is that in these works the authors assume the PN divided into different sub-modules or sites: each site is modeled by a different subset of places and transitions and can interact with the other sites via bordered places [9] or guard transitions [10]. On the contrary, in our approach each site has the perfect knowledge of the entire PN system but it can observe the system with a different observation mask.

II. BACKGROUND ON LABELED PETRI NETS

A Petri net is a structure \( N = (P, T, Pre, Post) \), where \( P \) is the set of \( m \) places, \( T \) is the 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. The function \( C = Post - Pre \) is called incidence matrix.

A marking is a vector \( M : P \rightarrow \mathbb{N} \) that assigns to each place a nonnegative integer number of tokens; the marking of a place \( p \) is denoted with \( M(p) \). A net system \( \langle N, M_0 \rangle \) is a net with initial marking \( M_0 \).

A transition \( t \) is enabled at \( M \) iff \( M \geq Pre(\cdot, t) \) and may fire yielding the marking \( M' = M + C(\cdot, t) \). The notation \( M[\sigma] \) is used to denote that the sequence of transitions \( \sigma = t_1 \ldots t_k \) is enabled at \( M \); moreover we write \( M[\sigma]M' \) to denote the fact that the firing of a \( \sigma \) from \( M \) yields to \( M' \). Given a sequence \( \sigma \in T^* \) we write \( t \in \sigma \) to denote that a transition \( t \) is contained in \( \sigma \).

The set of all sequences that are enabled at the initial marking \( M_0 \) is denoted with \( L(N, M_0) \). Given a sequence \( \sigma \in T^* \), we call \( \pi : T^* \rightarrow \mathbb{N}^n \) the function that associates to \( \sigma \) a vector \( y \in \mathbb{N}^n \), named firing vector, such that \( y(t) = k \) if the transition \( t \) is contained \( k \) times in \( \sigma \).

A marking \( M \) is said to be reachable in \( \langle N, M_0 \rangle \) iff there exists a firing sequence \( \sigma \) such that \( M_0[\sigma]M \). The set of all markings reachable from \( M_0 \) defines the reachability set of \( \langle N, M_0 \rangle \) and is denoted with \( R(N, M_0) \). Finally we define \( PR(N, M_0) \) the potentially reachable set, i.e., the set of all markings \( M \in \mathbb{N}^n \) for which there exists a vector \( y \in \mathbb{N}^n \) that satisfies the state equation \( M = M_0 + C \cdot y \). It holds that \( R(N, M_0) \subseteq PR(N, M_0) \).

A PN having no directed circuits is called acyclic. For such nets if the vector \( y \in \mathbb{N}^n \) satisfies the equation \( M_0 + C \cdot y \geq 0 \), there exists a firing sequence \( \sigma \) fireable from \( M_0 \) and such that the firing vector associated with \( \sigma \) is equal to \( y \). Moreover for acyclic nets \( R(N, M_0) = PR(N, M_0) \).

A labeling function \( L : T \rightarrow L \cup \{ \varepsilon \} \) assigns to each transition a symbol from a given alphabet \( L \) or the empty string \( \varepsilon \). The set of transitions sharing the same label \( \ell \) is denoted as \( T_\ell \). Transitions whose label is \( \varepsilon \) are called silent and are denoted by the set \( T_s \). The set \( T_o = T \setminus T_s \) is the set of observable transitions, i.e., when an observable transition fires we observe its label. We denote as \( C_u \) the restriction of the incidence matrix to \( T_u \) (\( T_s \)). We define the projection over \( T_o \) \( P_o : T^* \rightarrow T_o^* \) as follows: (i) \( P_o(\varepsilon) = \varepsilon \); (ii) for all \( \sigma \in T^* \) and \( t \in T \), \( P_o(\sigma t) = P_o(\sigma) t \) if \( t \in T_o \), and \( P_o(\sigma t) = P_o(\sigma) \) otherwise. Analogously, the projection over \( T_o \) \( P_o : T^* \rightarrow T_o^* \) can be defined.

We denote as \( w = L(\sigma) \) the word of events associated to the sequence \( \sigma \). We define \( S(w) = \{ \sigma \in L(N, M_0) \mid L(\sigma) = w \} \) the set of sequences consistent with \( w \in L^* \). In plain words, given an observation \( w \), \( S(w) \) is the set of sequences that may have fired.

Finally, given a net \( N = (P, T, Pre, Post) \) and a subset \( T' \subseteq T \) of its transitions, we define the \( T' \)-induced subnet of \( N \) as the new net \( N' = (P, T', Pre', Post') \), where \( Pre' \) and \( Post' \) are the restrictions of \( Pre \) and \( Post \) to \( T' \), i.e., \( N' \) is the net obtained from \( N \) removing all transitions in \( T \setminus T' \). We write that \( N' \preceq T' \cdot N \).

III. PROBLEM STATEMENT

We model anomalous or faulty behavior using the set of silent transitions \( T_I \subseteq T_u \). The set \( T_I \) includes all fault transitions and is further decomposed into \( r \) different subsets \( T'_j \), where \( i \in F = \{1, \ldots, r\} \), that model different fault classes. The transition set \( T_{reg} = T_u \setminus T_I \) represents the set of unobservable, but regular, transitions.

The problem of fault diagnosis can be seen as the problem of detecting the firing of any fault transition in \( T_I \), using the knowledge on the firing of observable transitions, or the knowledge on their labels in the case of labeled PNs.

In this work we explore the possibility of performing diagnosis using a decentralized architecture as depicted in Fig. 1. The system is monitored by a set \( J = \{1, \ldots, \nu\} \) of sites. Each site has a complete knowledge of the net structure and of the initial marking, but observes the evolution of the system using its own observation mask. Obviously, different sites have different observation masks. In particular, for any site \( j \in J \), the set of locally observable transitions is the set

![Fig. 1. The decentralized diagnosis architecture.](image-url)
$T_{o,j} \subseteq T_o$. Any centrally observable transition is observed by at least one site, i.e., $\bigcup_{j \in J} T_{o,j} = T_o$. The set of locally unobservable transitions is defined as

$$T_{u,j} = T_{reg} \cup T_f \cup (T_o \setminus T_{o,j}).$$  \hfill (1)

We denote as $L_j \subseteq L (j \in J)$ the alphabet of the $j$-th site, i.e., the set of labels observable by the $j$-th site. Moreover, we denote as $w_j = L_j(\sigma)$ the word of events in $L_j$ associated to the sequence $\sigma$ by the $j$-th site.

As shown in Fig. 1, on the basis of its own observation $w_j = L_j(\sigma)$ ($j \in J$) each site performs a local diagnosis. In particular, for each fault class $i \in \mathcal{F}$ it computes a different diagnosis state $\Delta_{j,i}$ and depending on this, it exchanges information with a coordinator $C$ according to a given protocol\(^1\). The coordinator fuses the information coming from the different sites according to the considered protocol and infers on the occurrence of faults. More precisely, for each fault class $i \in \mathcal{F}$ it computes a diagnosis state $\bar{\Delta}_i$.

In this paper we explore the decentralized architecture under the following assumptions.

A1 The same label $l \in L$ can be associated to more than one transition, but if a site observes a transition labeled $l$, then it observes any transition whose label is $l$, i.e., $\exists t, t' : L(t) = L(t')$ and $t \in T_{o,j}$, while $t' \notin T_{o,j}$.

A2 The $T_{u,j}$-induced subnet $N_{u,j}$ is acyclic for any $j \in J$.

A3 The coordinator $C$ knows which transitions can be observed by each site, i.e., it knows the sets $T_{o,j}$ for any $j \in J$.

A4 There is reliable communication between the local sites and the coordinator, i.e., all messages sent from a local site are received by the coordinator, and vice versa, correctly and in order.

Note that we also investigate an important issue that occurs when performing diagnosis, regardless of the fact that it is centralized or decentralized, namely that of diagnosability.

**Definition 3.1:** Let us consider a PN system $\langle N, M_0 \rangle$ having no deadlock after the occurrence of transition $t_f \in T_f^i$ for all $i \in \mathcal{F}$. Assume that diagnosis is performed according to a given approach (either centralized or decentralized).

We say that $\langle N, M_0 \rangle$ is diagnosable with respect to (wrt) the fault class $T_f^i$ and wrt a given diagnosis approach iff the occurrence of some fault in $T_f^i$ is unambiguously detected using the specified diagnosis approach after a finite number of transition firings.

**Definition 3.2:** A PN system $\langle N, M_0 \rangle$ is diagnosable wrt a given diagnosis approach if it is diagnosable wrt that approach for all fault classes $T_f^i$, $i \in \mathcal{F}$.

Note that in the centralized framework, inspired by the definition of diagnosability for languages introduced in [6], Definition 3.1 can alternatively be formulated as follows.

**Definition 3.3:** A PN system $\langle N, M_0 \rangle$ having no deadlock after the occurrence of transition $t_f \in T_f^i$, for $i \in \mathcal{F}$, is diagnosable wrt the fault class $T_f^i$ if there do not exist two firing sequences $\sigma_1$ and $\sigma_2 \in T^*$ satisfying the following conditions:

- $L(\sigma_1) = L(\sigma_2)$,
- $\sigma_1 \in (T \setminus T_f^i)^*$,
- $\exists$ at least one $t_f \in T_f^i$ such that $t_f \in \sigma_2$,
- $\sigma_2$ is of “arbitrary length" (see [6]) after fault $t_f \in T_f^i$.

A remark should be done concerning the above definition. As discussed in detail in [11] in the case of finite state automata, the assumption that the system has no deadlock after the occurrence of a fault transition, can be relaxed by some technical changes in the definition of diagnosability. The same obviously holds in the case of PNs even if in such a case determining the set of states from which a deadlock may occur is much more burdensome, particularly in the case of unbounded PNs.

IV. BASIC DEFINITIONS AND RESULTS ON CENTRALIZED DIAGNOSIS

In this section we briefly recall the diagnosis procedure we defined in [4], [5] in the centralized framework, that is used by the different sites to perform diagnosis locally. As in the previous section, $T = T_o \cup T_u$ where $T_u = T_{reg} \cup T_f$, and the observations coincide with the labels associated to transitions in $T_o$. In particular, we first provide some preliminary definitions.

- Given a word $w \in L^*$, let $\sigma_o \in T_f^i$ be a sequence of observable transitions such that $L(\sigma_o) = w$. We call justification of $w$ a sequence $\sigma_u$ of unobservable transitions interleaved with $\sigma_o$ whose firing enables $\sigma_o$ and whose firing vector is minimal.
- Since in general $\sigma_o$ is not unique and more than one $\sigma_u$ may be associated to each $\sigma_o$, then the set of justifications of $w$ is not a singleton.
- We denote as $Y_{min}(M_0, w)$ the set of firing vectors relative to justifications of $w$.

The generic element $y \in Y_{min}(M_0, w)$ is called j-vector.

- Finally, we denote as

$$\hat{J}(w) = \{ (\sigma_o, \sigma_u), \sigma_o \in T_f^i, L(\sigma_o) = \sigma_u \in T_u^* \mid$$

$$\exists \sigma \in S(w) : \sigma_o = P_o(\sigma), \sigma_u = P_u(\sigma) \} \wedge$$

$$\exists \sigma' \in S(w) : \sigma_o = P_o(\sigma'), \sigma_u' = P_u(\sigma') \wedge$$

$$\pi(\sigma_u') \leq \pi(\sigma_u) \}$$

the set of couples (sequence $\sigma_o \in T_f^i$ with $L(\sigma_o) = w$ - corresponding justification of $w$).

**Example 4.1:** Let us consider the PN in Fig. 2, where the set of observable transitions is $T_o = \{ t_1, t_2, t_3 \}$ and the set of unobservable transitions is $T_u = \{ e_4, e_5, e_6, e_7, e_8 \}$. The labeling function is $L(t_1) = a$ and $L(t_2) = L(t_3) = b$.

Let $w = ab$ be the observed word. There exist two sequences that are consistent with the actual observation and whose firing vector is minimal, namely $\sigma' = e_4 t_1 e_5 t_2, \sigma'' = e_4 t_1 e_6 t_7 e_8 t_3$. Thus $\sigma'_u = e_1$ and $\sigma''_u = e_4 e_6 e_7 e_8$ are the two justifications of $w$. The set of j-vectors is $Y_{min}(M_0, w) =$
\[\{1 \ 0 \ 0 \ 0\}^T, \{1 \ 0 \ 1 \ 1\}^T\], where \(y' = [1 \ 0 \ 0 \ 0]^T\) is relative to \(\sigma'_u\), while \(y'' = [1 \ 0 \ 1 \ 1]^T\) is relative to \(\sigma''_u\). Finally, \(\hat{J}(w) = \{(t_1t_2, \varepsilon_A), (t_1t_3, \varepsilon_A\varepsilon_6\varepsilon_7\varepsilon_8)\}\).

Let us now recall the notions of diagnoser and diagnosis states.

**Definition 4.2:** A diagnoser is a function \(\Delta : L^* \times \{T_j^1, T_j^2, \ldots, T_j^r\} \rightarrow \{0, 1, 2, 3\}\) that associates to each observation \(w\) and to each fault class \(T_j^i\), \(i = 1, \ldots, r\), a diagnosis state.

- \(\Delta(w, T_j^1) = 0\) if for all \(\sigma \in S(w)\) and for all \(t_f \in T_j^1\) it holds \(t_f \notin \sigma\).

- In such a case the \(i\)-th fault cannot have occurred, because none of the firing sequences consistent with the observation contains fault transitions in \(T_j^1\).

- \(\Delta(w, T_j^1) = 1\) if:
  - (i) there exist \(\sigma \in S(w)\) and \(t_f \in T_j^1\) such that \(t_f \notin \sigma\) and
  - (ii) for all \((\sigma_o, \sigma_u) \in \hat{J}(w)\) and for all \(t_f \in T_j^1\) it holds \(t_f \notin \sigma_u\).

- In such a case a fault transition of the \(i\)-th class may have occurred but is not contained in any justification of \(w\).

- \(\Delta(w, T_j^1) = 2\) if there exist \((\sigma_o, \sigma_u), (\sigma'_o, \sigma'_u) \in \hat{J}(w)\) such that:
  - (i) there exists \(t_f \in T_j^1\) such that \(t_f \in \sigma_u\);
  - (ii) for all \(t_f \in T_j^1\), \(t_f \notin \sigma'_u\).

- In such a case a fault transition in the \(i\)-th class is contained in one (but not in all) justification of \(w\).

- \(\Delta(w, T_j^1) = 3\) if for all \(\sigma \in S(w)\) there exists \(t_f \in T_j^1\) such that \(t_f \notin \sigma\).

- In such a case the \(i\)-th fault must have occurred, because all firing sequences consistent with the observation contain at least one fault transition in the \(i\)-th class.

A systematic procedure has been given in [4], [5] to compute the above diagnosis states that is not recalled here for the sake of brevity.

**Example 4.3:** Let us consider again the PN in Fig. 2, where \(T_j^1 = \{\varepsilon_5, \varepsilon_j\}\). Let \(w = ab\). In such a case it is \(\Delta(w, T_j^1) = 2\). In fact, the \(j\)-vector \(y' = [1 \ 0 \ 0 \ 0]^T\) does not contain fault transitions, while \(y'' = [1 \ 0 \ 1 \ 1]^T\) contains \(\varepsilon_7 \in T_j^1\).

V. DECENTRALIZED DIAGNOSIS

In this section we present the main contributions of the paper. In particular, we introduce two different protocols to solve the decentralized diagnosis problem introduced in Section III.

A. Diagnosis under Protocol 1

Protocol 1 is based on the following very simple rules. Let \(\sigma\) be the sequence that has occurred and \(w_j = L_j(\sigma)\) be the observation of site \(j \in J\). We denote as \(\Delta_{j,i} = \Delta(w_j, T_j^i)\) the diagnosis state of site \(j\) wrt \(T_j^i\).

1. The diagnosis state \(\Delta_i\) of the coordinator relative to each \(T_j^i\) is initially undefined.
2. If there exists a site \(j\) such that \(\Delta_{j,i} = 3\) for some \(i \in F\), then the site \(j\) communicates this information to the coordinator; otherwise it remains silent.
3. When the coordinator receives some information relative to a fault class \(i\), then it sets \(\Delta_i = 3\). This means that a fault in \(T_j^i\) has been detected.

A decentralized diagnoser following Protocol 1 satisfies the following important property. Note that in the following we denote as \(\Delta_i^*\) the diagnosis state relative to the \(i\)-th fault class computed using the centralized approach with set of observable transitions \(T_o\) summarized in the previous section, that is assumed as a target.

**Proposition 5.1:** The coordinator based on Protocol 1 never produces false alarms, namely if \(\Delta_i = 3\), then \(\Delta_i^* = 3\) as well.

**Proof:** If the coordinator diagnosis state is \(\Delta_i = 3\), it means that there exists at least one site \(j \in J\) such that \(\Delta_{j,i} = 3\). Now, by eq. (1) it is \(T_{u,j} \supseteq T_u\). As a consequence, all the justifications that are admissible for the centralized diagnoser are also admissible for the \(j\)-th site. However, there may exist other justifications that are admissible for the \(j\)-th site while they are not admissible for the centralized diagnoser. This applies if \(\Delta_{j,i} = 3\) then all the justifications computed by the \(j\)-th site contain fault transitions in \(T_j^i\), then for sure any subset of such justifications (including the set of justifications computed by the centralized diagnoser) contains fault transitions in \(T_j^i\), thus proving the statement.

It is important to note that it may happen that the centralized diagnosis state is \(\Delta_i^* = 3\), while the coordinator under Protocol 1 is silent because the diagnosis state of all the sites are equal to 2 wrt fault class \(T_j^i\).

**Example 5.2:** Let us consider the PN system in Fig. 3 containing only one fault transition \(t_f\). Assume that the diagnosis is performed according to Protocol 1 by two sites whose sets of observable labels (alphabets) are equal to \(L_1 = \{a, c\}\) and \(L_2 = \{b, c\}\), respectively.

Assume that the sequence \(t_f t_3 t_4 t_5^k\) fires, where \(k\) is an arbitrary integer number.

A centralized diagnoser whose alphabet is \(L = \{a, b, c\}\) observes the word \(w = bac^k\) that has only the justification \(\sigma_u = t_f\). Thus its diagnosis state is set equal to 3.

The word observed by site 1 is \(w_1 = ac^k\) to which correspond two different justifications \(\sigma_{u,1}^o = t_f t_3\) and \(\sigma_{u,1}^o = t_2\), one containing the fault and the other one not. Thus its diagnosis state is set equal to 2.

Similarly, the word observed by site 2 is \(w_2 = bc^k\) to which correspond two different justifications, one containing
the fault and the other one not, namely, $\sigma'_{u,2} = t_1 t_4$ and $\sigma''_{u,2} = t_1$. Thus its diagnosis state is set equal to 2.

According to Protocol 1 the two sites remain silent so the coordinator does not detect the fault.

Let us now discuss diagnosability. The following result obviously holds.

**Corollary 5.3:** If a system is diagnosable in the decentralized framework, then it is also diagnosable in the centralized framework.

Clearly, the other sense of the implication does not hold. However, in the case of diagnosis performed using Protocol 1 the following result can be proved.

**Proposition 5.4:** The system is diagnosable wrt the decentralized approach based on Protocol 1 if and only if for any fault class $i \in F$ there exists at least one site $j \in J$ such that the system is diagnosable wrt the centralized approach with set of observable transitions $T_{o,j}$ and wrt that fault class.

**Proof:** For simplicity, with no loss of generality we assume that there is only one fault class. Let us prove separately the if and only if statements.

**If** If there exists one site $j \in J$ such that the system is diagnosable wrt the centralized approach with set of observable transitions $T_{o,j}$, due to Assumptions A1 and A2, this means that the $j$-th site reconstructs for sure the occurrence of a fault in a finite number of steps. Therefore its diagnosis state becomes equal to 3 after a finite number of transitions firings, as well as the diagnosis state of the coordinator.

**Only if** We prove this by contradiction. Assume that the system is diagnosable wrt the centralized approach with set of observable transitions $T_{o,j}$, but not wrt the decentralized approach. This means that even if a fault is contained in all the justifications computed assuming $T_{o,j}$ as the set of observable transitions, then $\Delta^* = 3$ while $\Delta_j \neq 3$. But this leads to a contradiction because, by Assumption A1, being the set of transitions observable to the centralized diagnoser equal to $T_{o,j}$, the set of justifications is the same in the two cases.

\[ \Box \]

**B. Diagnosis under Protocol 2**

Protocol 2 is a generalization of Protocol 1. It is still based on the idea that a site communicates its diagnosis state if and only if it is equal to 3, otherwise it remains silent. However, in this case it also transmits its set of j-vectors. On the basis of this information, the coordinator polls a certain number of sites and makes a refinement of the set of j-vectors. Such a refinement is then used by the local site to recompute its diagnosis states. This in general leads to an improvement of the performance of the decentralized diagnoser.

To define in a clear and concise way such a protocol, let us introduce some preliminary definitions.

- Let $J_l = \{ k \in J \mid l \in L_k \}$ be the set of sites that are capable of observing label $l$.
- Given a site $j$ and an observed word $w_j$,
  \[ I(j, w_j) = \{ l \in L \mid \exists y \in Y_{\min}(M_0, w_j) \land \exists t \in T \setminus T_{o,j} \mid y(t) > 0 \land \Delta(t) = l \} \]
  is the set of labels relative to transitions that appear in at least a j-vector of the $j$-th module.
- Given a site $j$ and an observed word $w_j$,
  \[ T(j, w_j) = \{ l \in L \mid \exists y \in Y_{\min}(M_0, w_j) \land \exists t \in T \setminus T_{o,j} \mid y(t) > 0 \land \Delta(t) = l \} \]
  is the number of occurrences of label $l$ in the observation $w_j$.
- Given an observation $w_k$ from site $k$, a label $l$, and a j-vector $y$,
  \[ \beta_k(l, y) = |w_k| - \sum_{t : \Delta(t) = l} y(t) \]
  is the difference between the number of times the site $k$ has observed $l$ and the number of times a transition labeled $l$ appears in $y$.

Based on the above definitions, the main steps of the decentralized procedure based on Protocol 2 can be summarized as follows.

1. The diagnosis state $\Delta_i$ of the coordinator relative to each $T^i_j$ is initially undefined.
2. If $\Delta^* = 3$ for some $j \in J$ and some $i \in F$, then the $j$-th site transmits to the coordinator its diagnosis state together with its set of j-vectors.
3. For any label $l \in I(j, w_j)$ the coordinator polls any site $k \in J \setminus \{ j \}$ (if $J \setminus \{ j \}$ is not empty).
4. The $k$-th site transmits to the coordinator the value of $|w_k|_l$.
5. If $\beta_k(l, y) < 0$ for a vector $y \in Y_{\min}(M_0, w_j)$, then the coordinator removes the vector $y$ from the set of j-vectors $Y_{\min}(M_0, w_j)$ relative to the $j$-th site.
6. As a result of this process of refinement, the coordinator computes a new set $Y'_{\min}(M_0, w_j)$ that is communicated to the $j$-th site.
7. The $j$-th site recomputes its diagnosis states according to the new set $Y'_{\min}(M_0, w_j)$ and if some of them are equal to 3, communicates it to the coordinator, otherwise it keeps silent.

The refinement of $Y_{\min}(M_0, w_j)$ is based on the following very simple fact. If $Y_{\min}(M_0, w_j)$ contains a j-vector that assumes a certain number of occurrences of $l$, but this number is not consistent with the observation of a site that is capable of observing $l$, then for sure such a justification is unreachable. Therefore, if $\beta_k(l, y) < 0$ for a certain label $l$ and a certain j-vector $y \in Y_{\min}(M_0, w_j)$, then $y$ should be removed from $Y_{\min}(M_0, w_j)$. In fact, this means that the justification relative to j-vector $y$ assumes a number of occurrences of $l$ that is greater than the real number, that is perfectly known by the $k$-th site. On the contrary, if
\( \beta_k(l, y) \geq 0 \) it means that the \( j \)-vector \( y \) is compatible with
the observation of the \( k \)-th site. In particular, if \( \beta_k(l, y) = 0 \) it means that the justification contains all the occurrences of
label \( l \). The case of \( \beta_k(l, y) > 0 \) is relative to a possible feasible situation. It means that the justification relative to
\( y \) does not contain all the occurrences of \( l \); thus the rest of transitions labeled \( l \), up to the value \( |w_k| \), have fired after
the justification and the observation \( w_j \).

The refinement process has in general positive effects on
diagnosis as shown by the following example.

**Example 5.5:** Let us consider the PN system in Fig. 4. Assume that there are two fault classes: \( T_{1}^f = \{ t_{1}^f, t_{1}^{f2} \} \),
\( T_{2}^f = \{ t_{2}^f \} \).

Assume that the net is locally diagnosed by two sites
whose sets of observable transitions are \( T_{o,1} = \{ t_{3}, t_{6} \} \) and
\( T_{o,2} = \{ t_{1}, t_{2}, t_{4}, t_{5}, t_{6} \} \), respectively. This implies that
\( L_{1} = \{ a, c \} \), \( L_{2} = \{ b, c \} \), \( J_{a} = \{ 1 \} \), \( J_{b} = \{ 2 \} \) and
\( J_{c} = \{ 1, 2 \} \).

Assume that the sequence \( a = t_{1}^f, t_{1}^f, t_{1}^{f2}, t_{2} \) fires, thus \( w = L(\sigma) = bb \). The first site observes the empty string \( \varepsilon \), i.e.,
\( w_1 = \varepsilon \), while the second site observes the word \( w_2 = bb \).

Due to these observations, the diagnosis states of the first
site are \( \Delta_{1,1} = 1 \) and \( \Delta_{1,2} = 1 \), relative to the first and the
second fault class respectively. In fact, transitions from both fault classes may have fired at the initial marking without
the firing of any transition labeled either \( a \) or \( c \).

The diagnosis states of the second site are \( \Delta_{2,1} = 3 \) and
\( \Delta_{2,2} = 2 \), respectively. In fact, the set of justifications of \( w_2 \)
includes the following sequences: \( \sigma''_{u,2} = t_{1}^f, t_{1}^f, t_{2} \), \( \sigma''_{u,2} = \)
t\( t_{1}^f, t_{1}^f, t_{2} \), i.e., both the justifications contain a transition in \( T_{2}^f \),
while only one of them contains a transition in \( T_{1}^f \).

Therefore, the second site communicates \( \Delta_{2,1} = 3 \) to the
coordinator who sets its diagnosis state relative to \( T_{1}^f \) to
\( \Delta_{1} = 3 \). The firing of one transition in \( T_{1}^f \) is thus detected
both using Protocol 1 and Protocol 2.

However, if we use Protocol 1 the firing of \( t_{1}^{f2} \) is not
detected because both sites are silent wrt the second fault
class. On the contrary, if we use Protocol 2 the firing of \( t_{1}^{f2} \)
is detected.

In fact, according to Protocol 2, site 2 also communicates
its set of \( j \)-vectors to the coordinator that is equal to
\( Y_{\min} (M_0, w_2) = \{ y_2', y_2'' \} \), where \( y_2' \) is the firing vector relative to \( \sigma''_{u,2} = t_{1}^f, t_{1}^{f2}, t_{2} \), while \( y_2'' \) is the firing vector relative to \( \sigma''_{u,2} = t_{1}^f, t_{1}^f, t_{1}^f \).

Since \( I(2, w_2) = \{ a \} \) and \( J_{a} = \{ 1 \} \), the coordinator polls
site 1 to know the number of symbols \( a \) it observed. Since
\( |w_1| = 0 \), then \( \beta_1(a, y_2') = 0 \) and \( \beta_2(a, y_2'') < 0 \). It means that \( j \)-vector \( y_2'' \) can be conflated and removed from \( Y_{\min} (M_0, w_2) \). The refined set of \( j \)-vectors is \( Y_{\min}^r (M_0, w_2) = \{ y_2' \} \) thus \( \Delta_{2,2} \)
is updated to 3 and consequently \( \Delta_{2} = 3 \) allowing also the
detection of \( t_{1}^{f2} \).

**Remark 5.6:** Since events occur in an asynchronous way,
i.e., we are not assuming that there is a global clock, it can
obviously happen that the value of \( |w_k| \) transmitted by the
polling sites to the coordinator is affected by some delay. As
a result of this the coordinator receives a value \( |w_{k}|| \) > \( |w_k| \),
because during such a delay other transitions labeled \( l \)
have fired. This implies that the value of \( \beta_k(l, y) \) may be
greater than the correct one. In particular, it may occur that
a negative value of \( \beta_k(l, y) \) becomes null or even positive,
thus certain \( j \)-vectors that should be rejected, are considered
as feasible. However such a delay may never cause a feasible
\( j \)-vector to be rejected.

The following propositions can be stated.

**Proposition 5.7:** The coordinator based on Protocol 2
never produces false alarms, namely if \( \Delta_{i} = 3 \), then \( \Delta_{i}' = 3 \)
as well.

**Proof:** By Proposition 5.1 we know that no false alarm
may occur when using Protocol 1. Now, the effect of
Protocol 2 is that of eventually reduce the cardinality of the
sets of \( j \)-vectors relative to certain sites, with respect to those
computed using Protocol 1. However, by definition such a
reduction consists in only removing those \( j \)-vectors that for
sure are not feasible, because they are not consistent with
the observations of other sites. Thus Protocol 2 guarantees
that no false alarm may occur as well.

**Proposition 5.8:** All sets of \( j \)-vectors obtained as the
result of a refinement carried out according to the rules of
Protocol 2, are not empty, i.e., \( Y_{\min}^r (M_0, w_j) \neq \emptyset \) for all
\( j \in J \) that perform a refinement of \( Y_{\min} (M_0, w_j) \).

**Proof:** Follows from the fact that the set \( Y_{\min} (M_0, w_j) \)
contains certainly the \( j \)-vector \( \hat{y} \) that corresponds to the
word that has actually fired, plus eventually other vectors.

Using the rules of Protocol 2, some of these \( j \)-vectors will
be conflated, but certainly it will not be \( \hat{y} \), therefore \( \hat{y} \in
Y_{\min}^r (M_0, w_j) \), thus proving the statement.

**Proposition 5.9:** The system is diagnosable wrt the
decentralized approach based on Protocol 2 if for any fault
class \( i \in F \) there exists at least one site \( j \in J \) such that the
system is diagnosable wrt the centralized approach with set of
observable transitions \( T_{o,j} \) and wrt that fault class.

**Proof:** This result can be proved using the same arguments
in the proof of the if statement of Proposition 5.4.

The above proposition only provides a sufficient condition
for diagnosability. In fact let us consider for the sake of
simplicity only one fault class. It may happen that the
system is not diagnosable in a centralized framework wrt
all \( T_{o,j} \) (\( j \in J \)), while it is diagnosable in a decentralized
framework using \( \nu \) sites whose sets of observable transitions
are equal to \( T_{o,j} \) (\( j \in J \)).

This is the case of the PN system considered in Example 5.5.
In fact, both the centralized diagnosers observing \( T_{o,1} = \)
\( \{ t_{3}, t_{6} \} \) and \( T_{o,2} = \{ t_{1}, t_{2}, t_{4}, t_{5}, t_{6} \} \) are not able to detect

![Fig. 4. The PN system considered in Example 5.5.](image-url)
the occurrence of $t_{f,2}$ if the sequence $\sigma = t_1^k t_1 t_{f,2} t_2 t_3^k$ fires, where $k$ is an arbitrary integer number. On the contrary, as shown in Example 5.5, the decentralized diagnoser based on Protocol 2 detects the occurrence of $t_{f,2}$ after a sequence that is a prefix of $\sigma$.

We also observe that, as in the case of Protocol 1, it may happen that the centralized diagnosis state is $\Delta_1^c = 3$ while the coordinator under Protocol 2 is silent. The following example clarifies this.

**Example 5.10:** Let us consider the net system in Fig. 5, having a single fault transition $t_f$. The net is locally diagnosed by two sites whose alphabets are equal to $L_1 = \{a, c\}$ and $L_2 = \{b, c\}$, respectively.

Assume that the sequence $\sigma = t_1 t_2$ fires, thus $w_1 = a$ and $w_2 = b$.

The set of j-vectors relative to the first site is $Y_{\text{min}}(M_0, w_1) = \{y_1', y_1''\}$ where $y_1'$ is the firing vector relative to the justification $\sigma_{u,1}' = t_f$, while $y_1''$ is the firing vector relative to $\sigma_{u,1}'' = \varepsilon$. The set of j-vectors relative to the second site is $Y_{\text{min}}(M_0, w_2) = \{y_2', y_2''\}$ where $y_2'$ and $y_2''$ are relative respectively to justifications $\sigma_{u,2}' = t_f t_1$ and $\sigma_{u,2}'' = t_2 t_3$. Hence both sites have a diagnosis state equal to 2.

On the contrary, in a centralized framework, being $L = \{a, b, c\}$ and consequently $w = ab$, the diagnosis state is equal to 3 and the firing of $t_f$ is detected. In fact the only justification of $w$ is $\sigma_u = t_f$.

**Remark 5.11:** Assume, for simplicity of explanation, that there is only one fault class. According to the proposed protocols the coordinator may either be in a fault state or it may be silent. If the coordinator is silent, the fault may either have occurred or not.

If we also want to characterize the situation in which the occurrence of a fault can be excluded for sure, both protocols can be modified as follows. Three different states are defined for the coordinator $C$, e.g., $F$ (fault), $U$ (uncertain) and $N$ (no fault). The sites communicate their diagnosis state to $C$ even if it is equal to 0. If the coordinator receives one 0, then it sets to $N$ its fault state; if it receives one 3 then it sets to $F$ its state; otherwise its state is equal to $U$.

**VI. CONCLUSIONS AND FUTURE WORKS**

In this preliminary paper on decentralized diagnosis we addressed the problem of designing a decentralized diagnoser for PNs. We assume that the system is monitored by a set of local sites: each site knows the structure of the net and the initial marking of the system but observes its evolution with a different mask. Diagnosis is performed locally using a diagnosis approach we previously introduced in the centralized framework. Two different protocols are proposed to determine how a central coordinator elaborates the global diagnosis states. The problem of diagnosability is also addressed and the advantages/disadvantages of the two protocols are discussed.

Our future work will be that of investigating if the performances of the decentralized diagnoser, and its diagnosability properties can be improved, if the sites communicate with the coordinator also in the case of diagnosis state equal to 2, or 1. The problem of determining a technique to test diagnosability in the case of decentralized systems will also be addressed.

Finally, while in this paper we assumed that the sites and their observation masks are given, we will also consider the case in which their definition can be seen as the result of an optimization problem, whose main goal is that of obtaining performances in terms of diagnosis (and diagnosability) that are close as possible to those of the centralized diagnoser.

**REFERENCES**


