Distributed Diagnosis for Petri Nets models with unobservable interactions via common places

George Jiroveanu and René K. Boel

Abstract—In this paper we consider the case of a large plant comprising different local sites. At each site, a local diagnoser must provide the diagnosis of the site based on the local plant model (a Petri Net), the local observation and the information exchanged with its neighbors. The communication between the local diagnosers is not event-driven and the interactions between the local sites (modeled as common places) are considered unobservable (tokens can enter and exit unobservably the local Petri Net models). For this general setting we present in this paper an algorithm that allows the local diagnosers to recover completely the results of a centralized diagnoser after the completion of a communication protocol.

I. INTRODUCTION

Essential for all industrial activities the diagnosis of a plant answers the questions: “Did a fault happen in the plant?” (fault detection) and “Where did it happen?” / “Which kind of fault happened if any?” (fault isolation) [12]. Additionally the diagnosis may be required for answering: “How the fault happened?” (explanations [9]) and “Which are the consequences of the fault occurrence?”.

The approach we follow in this paper for performing diagnosis is model based, with the plant model given as a Petri Net. Reasoning about the past evolution of the plant is based on observing a subset of observable events (whose occurrence is always reported). The faults that must be detected, are modeled as unobservable transitions. This approach assumes that the model and initial state are perfectly known and that observations are always correctly received.

In this paper we consider the case of a large plant consisting several interacting sub-systems (sites). Each sub-system is modeled as a Petri Net (PN). The interactions are represented by token passing via border (common) places from one sub-system to another [6], [13].

Since the centralized plant diagnosis [11] is usually not feasible for large plants, we assume that the knowledge about the model of the plant as well as the observation are distributed among a set of diagnoser agents (d-agents), with one d-agent located at each site. A d-agent knows the local sub-system (the PN model), receives the local site observation and it has the possibility to exchange limited information with its neighbors.

The general setting we consider is as follow. The communication between the d-agents is not event-driven i.e. the time the information exchange is allowed does not necessarily depend on the observations. It is also required that each d-agent performs a preliminary local diagnosis (PLD), based only on the local observations and the local model in absence of any external information.

In this distributed setting the main difficulty in designing an algorithm to compute the plant diagnosis is the lack of knowledge on the marking of places where tokens can enter the local PN model. Basically a d-agent must estimate the behavior of the local site, the “marking” of the border places being uncertain [7].

The case of nondeterministic observation of the interactions was considered in [3] and [6]. Nondeterministic observation means that the input transitions and output transitions of any common place between any two subsystems are observable but there may be different observable transitions emitting the same label when they fire.

The case of unobservable interactions between the local sites (components) of the plant is studied in [2], [12] where the plant-model is given as a network of interacting automata. The proposed solution is to compute preliminary over-estimations for each local component that are checked for consistency by communication between the d-agents.

For PN models this solution is difficult to apply. It would require for each input place of a sub-system the computation of an upper bound on the number of tokens that can enter, implying a global analysis of the plant model. Even though this might be possible (by translating the PN model into a network of communicating automata), the approach based on upper bounds becomes utterly infeasible for PN models whenever the plant structure changes often (i.e. components are plugged in/out), this requiring the recalculation of the (new) upper bounds.

In [4] we proposed for general PN models and unobservable interactions via common places a distributed algorithm that allows the d-agents to detect the state $F$ (“a fault happened for sure” [11]) whenever a centralized d-agent would detect the state $F$.

In this paper we adapt the algorithm presented in [4] s.t. the centralized diagnosis result is completely recovered: right after the communication protocol has been executed the d-agents also report the same faults that could have happened, as would the centralized diagnoser. The motivation is that the d-agents may be required from time to time to correlate perfectly their local estimates of the local states.

Without affecting the generality we consider here the case of only two interacting sites, deterministic labels for the observable events (while the unobservable events are silent),
and a global clock that governs the process (allowing for temporal ordering of the events observed in different sites).

The paper is organized as follows. Section II revises PNs notions and introduces the notation. In Section III we formally present the setting. In Section IV we present an algorithm for computing local preliminary diagnosis and in Section V we show how by communicating the agents accomplish the centralized diagnosis results. Finally in Section VI we conclude the paper with some final remarks.

II. PETRI NETS

A Petri Net is a structure \( N = (P, T, \text{pre}, \text{post}) \) where \( P \) denotes the set of \( \sharp \) places, \( T \) denotes the set of \( \sharp \) transitions, and \( \text{pre} : P \times T \rightarrow N \) and \( \text{post} : T \times P \rightarrow N \) are the pre- and post-incidence function that specify the arcs. We use the standard notations: \( \bullet, \cdot \) for the set of input, respectively output transitions of a place; similarly \( \bullet, \cdot \) and \( i^* \) denote the set of input places to \( i \), and the set of output places of \( t \) respectively. A marking \( M \) of a PN is represented by a \( \sharp P \)-vector, \( M : P \rightarrow N \), that assigns to each place \( N \) a non-negative number of tokens.

Denote by \( \mathcal{L}_N(M_0) \) the set of all possible traces of PN \( \langle N, M_0 \rangle \), where a trace \( \tau \) in \( \langle N, M_0 \rangle \) is defined as: \( \tau = M_0 \cdot t_1 \cdot M_1, \ldots, t_k \cdot M_k \), where for \( i = 1 \ldots k, M_{i-1} \geq \text{pre}(t_i) \). \( M \xrightarrow{\tau} M_0 \) denotes that the enabled sequence \( \tau \) may fire at \( M \) yielding \( M_0 \). Denote by \( R_N(M_0) \) the set of all the reachable markings from \( M_0 \).

The transition set \( T \) is partitioned into the disjoint subsets of observable \( T_o \), and unobservable \( T_u \) transitions. Then \( T_F \) denotes the set of faulty events whose occurrence must be detected (\( T_F \subset T_u \)).

Denote by \( T^\ast \) the Kleene closure of the set \( T \) and by \( \varepsilon \) the empty string. Let \( s \in \mathcal{L}_N(M_0) \subseteq T^\ast \). The projection \( \Pi : \mathcal{L}_N(M_0) \rightarrow T^\ast \) (also denoted \( \Pi_T(\mathcal{L}_N(M_0)) \)) is defined as: i) \( \Pi(\varepsilon) = \varepsilon \); ii) \( \Pi(t) = t \) if \( t \in T_o \); iii) \( \Pi(t) = \varepsilon \) if \( t \in T_u \); iv) \( \Pi(s \cdot t) = \Pi(s) \cdot \Pi(t) \) for \( s \in \mathcal{L}_N(M_0) \) and \( t \in T \).

For a set or a multisets \( X, 2^X \) is the set of all the sub-sets of \( X \). Given \( f : X \rightarrow Y \) and \( A \subset X \) then \( f(A) = \bigcup_{x \in A} f(x) \). Throughout the paper we treat a marking \( M \) as a vector or as a multi set of tokens.

DeDefinition 1: Given a PN \( N \), \( \varnothing = p_0, t_1, \ldots, t_n, p_n \) is a non-trivial unobservable elementary path in \( N \) if: i) \( n > 0 \); ii) \( i_{q+1} \leq p_{q+1} \bullet, t \) for \( q = 1, \ldots, n \); iii) \( t_q \in T_u \) for \( q = 1, \ldots, n \).

DeDefinition 2: An unobservable elementary circuit (uec) denoted \( \zeta \) is an unobservable elementary path \( \varnothing \) that comprises different transitions and different places excepting the initial place \( p_0 \) and the final place \( p_n \) that are the same. If there is a place \( p_j \) \((0 \leq j \leq k)\) of an uec \( \zeta \) that has more than one outgoing transition \(( |p_j^\bullet| \geq 2 \) we say that \( \zeta \) is an uec with choice places and is denoted uecwp.

An observed event is denoted \( t^o \) while a sequence of observed events is \( O = t^o_1 \ldots t^o_\infty \). The time an observable event \( t^o_q \) \((1 \leq q \leq \infty)\) happened is denoted \( \theta^o_q \). We assume that a global clock governs the overall process in the sense that \( \theta^o_q < \theta^o_w \) when \( q < w \).

III. THE SETTING

We consider the distributed plant description as follow:

i) \( N = \{N_1 \cup N_2 \} \) where \( N = (P, T, \text{pre}, \text{post}) \) and for \( i = 1, 2 \)
\[ N_i = (P_i, T_i, \text{pre}_i, \text{post}_i) \]
ii) \( P = P_1 \cup P_2, P_1 \cap P_2 = P_{12}, P_{12} \neq \emptyset \)
iii) \( T = T_1 \cup T_2, T_1 \cap T_2 = \emptyset \)
iv) \( \text{pre}_i = \text{pre} |_{N_i}, \text{post}_i = \text{post} |_{N_i}, i = 1, 2 \)
v) \( P_{12} = \text{IN}_i \cup \text{OUT}_i, \text{IN}_i \cup \text{OUT}_i = \emptyset \)
vi) \( \text{IN}_i = \text{OUT}_j = \{ p \in P_1 | p \subseteq T_i \land \bullet \subseteq T_j \} \)
vii) \( \text{IN}_j = \text{OUT}_i = \{ p \in P_2 | \bullet \subseteq T_i \land \bullet \subseteq T_j \} \)
viii) \( N \) is structurally bounded w.r.t. the observable evolution i.e. \( \forall M \in \mathbb{N}^{P'}, \forall \sigma_{\text{out}} \in T_{\text{out}} : M \rightarrow M' \Rightarrow M' \neq M \)

For simplicity we assume \( \text{IN}_i \) and \( \text{OUT}_i \) disjoint and \( M_{12} = 0 \) \((M_{12} = M_0(P_{12})) \). When fired, an observable transition \( t \in T_o \) emits a deterministic label \( \delta(t) \) (i.e. \( \delta(t_1) = \delta(t_2) \Rightarrow t_1 = t_2 \)), whereas an unobservable event does not emit anything \((\forall t \in T_u \rightarrow \delta(t) = \varepsilon) \).

Given a marking \( M_i \in \mathbb{N}^{P_i} \), denote by \( M_i, M_{IN_i} \), and \( M_{OUT_i} \) the marking of the places \( P_i, \text{pre}_i, \text{OUT}_i \) respectively.

At each site there is one d-agent \( A_i \) \((i = 1, 2) \). The a priori knowledge of the local plant a d-agent \( A_i \) has (denoted \( K_{A_i} \)) comprises the local site model \( N_i \), the set of events \( T_i \) whose occurrence it can observe (and are always observable) and the initial local state \( M_0; K_{A_i} = \langle N_i, T_o, M_0 \rangle \) (see Fig.1).

The information exchange between \( A_{1} \) and \( A_{2} \) is not event-driven. Denote by \( \theta_i \) the first time the agents communicate. Denote by \( O_{\theta_i} = t_1, \ldots, t_k \) (the possible empty) sequence of observed events recorded at the local site \( i \) by the time \( \theta_i \). The global observation \( O_{\theta_i} \), that a centralized agent \( AG \left( K_{AG} = \langle N, T_o, M_0 \rangle \right) \) would receive by the time \( \theta_i \), is \( O_{\theta_i} = O_{\theta_i}^0 \otimes O_{\theta_i}^1 \otimes O_{\theta_i}^2 \) \((\otimes \) states for the interleaving of the local observations \( O_{\theta_i} \) according to a global clock). The assumption made in this paper is that the process "stops" at time \( \theta_i \), when the d-agents are required to achieve their goal by exchanging limited information in several consecutive messages. For \( k = 0, \ldots, K_{\text{max}} \), \( M_{S_{k+1}}^g \) denotes the \( k \)th message sent by \( A_{g_1} \) to \( A_{g_2} \) at the time \( \theta_i \). Notice that there is no message before \( \theta_i \), hence \( M_{S_{-1}}^g = \emptyset \). The local d-agents will not consider observations recorded after the time \( \theta_i \). A communication round with \( k \geq 1 \) implies that \( A_{1} \) and \( A_{2} \) exchange \( M_{S_{k-1}}^g \), \( M_{S_k}^g \) simultaneously. The consideration of asynchronous exchange of information brings nothing new but some more notation.

The set of (global) explanations of the received observation \( O_{\theta_i} \) and the set of estimated states are defined as:

\[ \mathcal{L}_N(O_{\theta_i}) = \{ \tau \in \mathcal{L}_N(M_0) | \Pi_{T_o} \tau = O_{\theta_i} \} \]
\[ \mathcal{M}_N(O_{\theta_i}) = \{ M \mid \exists \tau \in \mathcal{L}_N(O_{\theta_i}) \text{ s.t. } M_0 \xrightarrow{\tau} M \} \]

Eq.1 states that a global explanation \( \tau \) is a possible evolution \( \tau \in \mathcal{L}_N(M_0) \) that obeys the observation \( O_{\theta_i} \).

Consequently the centralized diagnosis at the time \( \theta_i \) (denoted \( D(\theta_i) \)) results by projecting \( \mathcal{L}_N(O_{\theta_i}) \) onto the set of fault events \( T_F \):

\[ D(O_{\theta_i}) = \{ \sigma_f \mid \sigma_f = \Pi_{T_F} \tau \land \tau \in \mathcal{L}_N(O_{\theta_i}) \} \]
Given $D(O_{\theta_i})$ denote by $D_i(O_{\theta_i})$ ($i = 1, 2$) the centralized diagnosis for site $i$:

$$D_i(O_{\theta_i}) = \{ \sigma_f | \sigma_f = \Pi_{\mathcal{T}_f} \sigma_f \in D(O_{\theta_i}) \}$$

(3)

IV. LOCAL PRELIMINARY DIAGNOSIS

Consider the distributed architecture shown in Fig.1. The locally observable transitions are $t_6$ for $N_1$ on the left and $t_{10}$ for $N_2$ on the right. The fault events whose occurrence should be detected are $t_1$ and $t_8$. Let the local observations at the time $\theta_c$ be $O_{\theta_c} = t_6$ at site 1 and $O_{\theta_c} = t_{10}$ at site 2 while the global order is $O_{\theta_c} = t_6t_{10}t_6$.

Before starting to communicate $Ag_2$ does not know the marking of the input place $p_5$ and it must perform a local calculation before receiving external information. A solution would be to consider on the input place $p_5$ the maximum number of tokens that could have come from the beginning of the process up to the time $\theta_c$ but this may lead to local calculations of the same magnitude as the global calculation of the plant [13] that further increase the amount of information exchanged.

In [4] we have proposed for the same setting to calculate the minimum number of tokens required to minimally explain the local observation $O_{\theta_c}$. The computation is based on a backward reachability algorithm that starts from the observed event computing the minimal marking required on the input places $IN_2$ of $N_2$. It results that observing $t_{10}$, the minimal number of tokens required to have come via $p_5$ is $M(p_5) = 0$ if the local minimal explanation is $t_2 \leq t_6t_{10}$, or $M(p_5) = 1$ if $t_2 > t_6t_{10}$.

Here we extend this algorithm in the following way. Assume that $Ag_2$ has minimally explained the local observation as above. Based on the minimal explanations $t_2$ also derived the estimated states: $M_1 = \{ m(p_{10}) = 1 \}$ and $M_2 = \{ m(p_8) = 1, m(p_{10}) = 1, m(p_{11}) = 1 \}$ respectively. What $Ag_2$ knows is that for $t_2$ the token in $p_{10}$ is available after the time $\theta_{t_{10}}$, when $t_{10}$ was observed, and that for $t_2$ a token coming at $p_5$ before $\theta_{t_{10}}$ is required and a tokens in $p_{11}$ is available after $\theta_{t_{10}}$ and a token in $p_{11}$ is available after the time $t_9$ has fired that is after the time the required tokens in $p_5$ has entered.

To take into account the timing information induced by the observation we associate with each token in a marking its rank as follows. Let a linear constraint be of the form $r \sim c$ with $\sim \in \{<, >\}$ where $c$ is a constant ($c \in \mathbb{R}^+$), a variable ($c \in \mathbb{R}^+$) or a conjunction of linear constrains.

Initially all the tokens in $M_0$ are considered as produced by the starting event $t_{\text{start}}$ ($\theta_{\text{start}} = 0$) and they are given the rank $r(p) > 0$. Assume that at time $\theta_t$ a transition $t \in \mathcal{T}$ fires and puts a token in a place $p$. This token is given the rank $\{ r > \theta_t \}$. E.g. in $M_2^t$ $m(p_{10}) = \{ r(p_{10}) > \theta_{t_{10}} \}$ for simplicity we denote a token in a place by its timing constraint. Then any unobservable transition produces tokens having the rank $Max_{p \in \mathcal{T} \in} (c_i) < r(p) < Max_{p \in \mathcal{T} \in} (c_i')$ where $c_i < r(p) < c_i'$ is the timing constraint of the tokens in the input places of $t$ that are consumed by firing $t$.

It means that depending on the tokens that are consumed during a transition, the newly produced tokens result in general with different ranks. Assume that the input places $p_1$ and $p_2$ of a transition $t$ contain each two tokens as follow $m(p_1) = \{ r(p_1) > \theta_{t_1}, r(p_1) > \theta_{t_2} \}$ and $m(p_2) = \{ r(p_2) > \theta_{t_3}, r(p_2) > \theta_{t_4} \}$. Then $t$ can fire in different ways e.g. consuming $r(p_1) > \theta_{t_1}$ and $r(p_2) > \theta_{t_3}$ and producing tokens having the rank $r(p) > \theta_{t_4}$ for $p \in \mathcal{T}$ (if $\theta_{t_2} > \theta_{t_4}$). Notice that we do not distinguish two tokens having the same constraint e.g. $r \sim c_1$ and $r \sim c_2$ where $\sim \sim 1 \sim 2$ (component wise). Moreover we say that a linear constraint is saturated if $\forall c_i$ s.t. $\& (r \sim c_i), c_i = ct \in \mathbb{R}^+$ and not saturated otherwise.

The reason we set a linear constraint depending on variables is as follow. Consider again $Ag_2$ observing $t_{10}$ as before. Thus $t_2 = t_6t_{10}$ requires a token in $p_5$ s.t. $\theta_{t_{10}} > r(p_5)$. Then $M_2 = \{ r(p_5) > 0, r(p_{10}) > \theta_{t_{10}}, r(p_{11}) > r(p_5) \}$ means that the token in $p_{11}$ arrives later than the token in $p_5$; the arrival time of a token in $p_5$ is a variable since there is no local knowledge $Ag_2$ has about its arrival.

Given the ranked marking $M_2^t$. $Ag_2$ estimates by forward search the ranked tokens that could have exited from the local site 2. E.g. $t_2^t$ is extended by firing either $\omega_1 = t_{13}$; $\omega_2 = t_6$; $\omega_3 = t_{11}$; $\omega_4 = t_{12}$; $\omega_5 = t_{13}t_5$; $\omega_6 = t_{13}t_{12}$; $\omega_7 = t_{13}t_1t_2$; ... Thus $t_2^t$ extended by $\omega_7$ will result in a ranked marking $M_\omega_7 = \{ r(p_5) < r(p_5), r(p_5) < \theta_{t_{10}}, r(p_7) > 0 \}$.

A. Local preliminary calculation

In the following we present the backward computation of the set of minimal explanation $Z_{\text{min}}^\omega_7$ of the first observed event in the overall model $N$ afterwards extending the approach to handle a sequence of observed events. Then we show how this method can be applied to a local model (e.g. $N_i$) whose marking is partially unknown (i.e. the marking of the input places $IN_i$ is not known). Finally the set of minimal local explanations are extended for estimating the marking of the output places $OUT_i$. 6307
Deﬁne $a \oplus b = a - b$ if $a \geq b$, and $a \oplus b = 0$ otherwise and extend "$\lor$" to multisets in the natural manner [1].

Deﬁnition 3: Backwards enabling rule: A transition $t$ is backward enabled in a marking $M \in \mathbb{N}^P$ iff $\exists p \in i^* \text{ s.t. } M(p) \geq 1$. Backwards ﬁring rule: A backward enabled transition $t$ in a marking $M \in \mathbb{N}^P$ vaues backwards from $M$ producing $M'$ (denoted $M \xrightarrow{t} M'$) where $M' = M \in \text{Post}(t, \cdot) + \text{Pre}(t, \cdot)$.

A sequence of transitions $\tau = t_1 \ldots t_m$ is backward allowable from $M$ (denoted $M \xrightarrow{\tau} M'$) iff for $q = 1, \ldots, m$, $t_q = t_1 \ldots t_{q-1}$ and $t_q$ is backward enabled in $M''$ where $M \xrightarrow{t_q} M''$.

Deﬁnition 4: Given a PN $N$, consider a marking $M \in \mathbb{N}^P$. Then $M$ is covered by $M'$ iff $\exists \sigma \in \mathcal{L}(M')$, and $M' \xrightarrow{\sigma} M''$ and $M' \xrightarrow{\cdot} M'$. Proposition 1: Given a PN $(N, M_0)$ and a marking $M$, then $M$ is covered by $M_0$ iff $\forall M' < M$ s.t $M \xrightarrow{\cdot} M'$. Denote by $BC_N(M)$ the set of all the markings that cover $M$: $BC_N(M) = \{M' | M \xrightarrow{\cdot} M'\}$. Then we have that $M$ is covered unobservably by $M_0$ iff $\exists M' \in BC_N(M)$ s.t $M' \leq M_0$ and $M \xrightarrow{u_o} M'$ where $\sigma_{uo} \in T_{uo}$. We denote by $BC_{uo}(M)$ the set of markings that unobservably cover the marking $M$.

Let a PN $(N, M_0)$ and the ﬁrst observed transition $t_1$. Denote $M_{t_1} = \text{Pre}(\cdot, t_1)$. Then we have:

\[ \mathcal{L}_{\text{in}}(t_1) = \{\tau = \sigma_{uo} t_1 | M_{t_1} \xrightarrow{u_o} M' \leq M' \in BC_{uo}(M_{t_1}) \} \]

\[ \mathcal{L}_{\text{out}}(t_1) = \{\tau = M_{t_1} t_1 | M' \leq t \in \mathcal{L}_{\text{in}}(t_1) \} \]

We have that $\mathcal{L}_{\text{in}}(t_1) \subseteq \mathcal{L}_{\text{out}}(t_1)$ and:

\[ R_N(M) = \bigcup_{M \in \mathcal{L}_{\text{in}}(t_1)} R_N(M') \]

The following two results allow us to discard backward traces that will not result in minimal traces.

Proposition 2: Given $(N, M_0)$ and a marking $M$ that is not covered by $M_0$ then $\forall M' > M$, $M'$ is not covered by $M_0$.

Proposition 3: Given $(N, M_0)$ and a marking $M$ then:

\[ BC_{uo}(M) \cap M_0 \neq \emptyset \text{ if } \forall M' > M, BC_{uo}(M') \cap M_0 \neq \emptyset \]

Thus, during computation, a set of markings to be processed (say SET) is maintained, where at the current step a marking $M$ is proccessed if there is not any other marking $M'$ in SET s.t. $M' < M$ (Proposition 2). The markings $M'$ that are not minimal elements in SET w.r.t. < are "stopped" until one has checked that $\forall M, M \in \text{SET} \land M' < M' \Rightarrow \exists \sigma_{uo} s.t. M \xrightarrow{uo} M' \land M' < M_0$ (Proposition 3).

Then the method extends to a sequence of observed events $O = t_1 t_2$ in a straightforward manner. E.g. for the second observed event $t_2$ the backward algorithm applies for all $M_{t_1} \in \mathcal{L}_{\text{in}}(t_1)$ (see Eq.4) instead of $M_0$. The minimal explanations for $t_2 = t_1 t_2$ results by concatenating $t_1 t_2$ where $t_1 \in \mathcal{L}_{\text{in}}(t_1), M_{t_1} \xrightarrow{t_1} M_{t_1} \xrightarrow{t_2}$ and $t_2 \in \mathcal{L}_{\text{in}}(t_2), M_{t_1} \xrightarrow{t_1} M_{t_2} \xrightarrow{t_2}$. Notice that the completeness is guaranteed by Eq.5.

Consider in the following the backward calculation for the distributed setting (e.g. $Ag_i$ and $K_{Ag_i}$) where the marking of some places (e.g. $IN_i$) is unknown.

Example 2: Consider again the PN in Fig. 2 where $t_4$ was observed but this time consider that $p_0$ is an input place on the border. In this case the computation does not terminate since running inﬁnitely backward the uecwcp $\zeta := t_4 t_3 t_2$ there will be a minimal local explanation requiring an inﬁnite number of tokens entering at the input place $p_0$ before $t_4$ was observed.

This motivates the following structural assumption we must impose in order to assure that the local backward search terminates without assuming the input places inﬁnite number of (ranked) tokens.

Given an uecwcp $\zeta$, denote by $\mathcal{Y}_{\zeta}$ the set of limiting places of $\zeta$: $\mathcal{Y}_{\zeta} \triangleq \{p | p \not\in \zeta \land \exists t_1 \in \zeta \text{ s.t. } p \in \text{it} \}$. A place $p \in \mathcal{Y}_{\zeta}$ is a limiting places of $\zeta$ since every complete execution of $\zeta$ consumes one token from $p$. For $M_{\zeta_1} \neq \emptyset$ let $M_{\zeta_1} = \{m(p) = 1 | p \in \mathcal{Y}_{\zeta} \}$.

Assumption 1: For any local model $N_i$ ($i = 1, 2$) and for any uecwcp $\zeta_i$, there does not exist an executable sequence
of unobservable transitions \( \sigma_{uo} \) with initial marking the marking \( M \) that has tokens only in the input places \( I_N \), \( (M(p) = 0 \text{ for } p \not\in I_N) \) s.t. by firing from \( M, \sigma_{uo} \) produces a marking \( M' \) greater than the limiting marking of \( \zeta, M_Y \). 

\[
\exists \sigma_{uo} \in T_{uo}^* \text{ s.t. } (M_Y, \sigma_{uo} \otimes M) \wedge (M(p) \neq 0 \Rightarrow p \in I_N).
\]

Then it is easy to see that if the PN model \( \langle N, M_0 \rangle \) is bounded w.r.t. the unobservable evolution (item viii in setting) and Assumption 1 is satisfied the backward calculation terminates after finitely many steps.

Thus for any observed sequence \( O'_b = t'_i^1 \ldots t'_i^n \) a local agent \( A_g \) derives backward the set of local minimal explanations \( Z_{\min}^i(O'_b) \), the set of minimum required tokens \( M_{IN_i} \) and the set of estimated states \( M_{N_i}^{min} \) where:

\[
\forall t_i \in Z_{\min}^i(O'_b) \Rightarrow \Pi_{t_i} t_i = O'_b \wedge \exists M_{IN_i} \wedge \\
\exists M_{\min} \in M_{N_i}^{min} \text{ s.t. } M_0 \cup M_{IN_i}, \delta_i \overrightarrow{\cdot} M_{\min}^{min}.\tag{7}
\]

Notice that \( M_{IN_i} \in M_{N_i}^{min} \) and \( M_{N_i}^{min} \) are multi-sets of ranked tokens where each token has a rank (a timing constraint) associated with it.

B. Information exchange and local updates

Consider below that for the observed sequence \( O'_b \) received locally by the time \( \theta, A_g \) has derived: \( Z_{\min}^i(O'_b) \in M_{N_i}^{min}(O'_b) \) \( \otimes M_{N_i}^{min}(O'_b) \). In order to simplify the notation we drop the indexes that are obvious from the context e.g. \( Z_{\min}^i(O'_b) \) will be denoted in short \( Z_{\min}^{i} \).

Since at \( \theta, A_g \) will be communicating with its neighbor, it should also calculate just prior to \( \theta \) an estimate of the marking of the output places \( OUT \) to be included in the first message that is sent. To do this \( A_g \) computes the "forward unobservable extensions" of the minimal explanations computed as \( Z_{\min}^{i} \) derivating \( Z_{ext}^{i} \) by a forward search starting from every ranked marking \( M_{\min}^{ext} \in M_{N_i}^{min} \):

\[
Z_{ext}^{i}(O_i) \triangleq \{ t_i \tau_i \mid \exists M_{IN_i} \in M_{N_i}^{min} \wedge \\
\wedge M_0 \cup M_{IN_i}, \delta_i \overrightarrow{\cdot} M_{\min}^{ext} \wedge \delta_i \overrightarrow{\cdot} M_{IN_i}^{\min} \wedge \delta_i \overrightarrow{\cdot} T_{uo}^* \}\tag{8}
\]

where \( \tau_i \) represents an unobservable possible continuation from an estimated state \( M_{\min}^{ext} \) reached by considering a minimal explanation \( t_i \in Z_{\min}^{i} \) of the observed event \( O'_b \), providing the minimum number of tokens \( M_{IN_i} \) was received at the input placed \( IN_i \). Hence we obtain:

\[
Z_{ext}^{i}(O_i) \triangleq \{ M_{\min}^{ext} \mid M_0 \cup M_{IN_i}, \delta_i \overrightarrow{\cdot} M_{\min}^{ext} \wedge \\
\wedge \delta_i \overrightarrow{\cdot} Z_{ext}^{i}(O_i) \}\tag{9}
\]

If we project the ranked markings \( M_{\min}^{ext} \in Z_{ext}^{i} \) on to the output places \( OUT \), we obtain the set: \( M_{OUT} \mathbin{\otimes} Z_{ext}^{i} = \{ M_{OUT} \mid M_{\min}^{ext} \in Z_{ext}^{i} \wedge M_{OUT} = M_{\min}^{ext}(OUT) \} \).

It results that having received the set of inputs \( M_{IN_i} \), the local observation is explained by \( Z_{ext}^{i} \) that has as result the set of "output" markings: \( M_{OUT} \mathbin{\otimes} Z_{ext}^{i} \).

The first message sent by \( A_g_i \) to \( A_g_j \) is \( Msg_{i-j} = (\mathcal{M}_{IN_i}, M_{OUT_i}, \Phi_i^1) \) where \( \Phi_i^1 \subseteq \mathcal{M}_{IN_i} \times M_{OUT_i} \) is the input-output correlation relation (non-empty only for compatible combinations of markings at the input-output places). Notice that when \( A_g_i \) sends \( A_g_j \) the message \( Msg_{i-j} \) at the same time \( A_g_j \) sends to \( A_g_i \) the first message \( Msg_{j-i} \) derived in a similarly way.

**Definition 5:** Given two local traces \( t_i \in T_i^* \), \( t_j \in T_j^* \), \( (t_i, t_j) \) is a consistent pair of local traces if \( \exists \tau \in L_N(M_0) \) s.t. \( \Pi_{T_i} \tau = t_i \) and \( \Pi_{T_j} \tau = t_j \).

We "recover" the entire set of pairs of consistent local traces \( \mathcal{L}_0(O_i) \times \mathcal{L}_0(O_j) \) \( (\mathcal{L}_0(O_i) = \Pi_{T_i}(L_N(O_i)), i = 1, 2) \) in the following way.

For each pair \( t_i \in L_i^{ext} \) and \( t_j \in L_j^{ext} \) we check if \( (t_i, t_j) \) is consistent and then if either \( t_i \) or \( t_j \) or both can be extended for generating new pairs. Notice that in general \( \mathcal{L}_0^{ext}(O_i) \not\subseteq \mathcal{L}_0(O_i) \) and \( \mathcal{L}_0^{ext}(O_j) \not\subseteq \mathcal{L}_0^{ext}(O_i) \). Then for a PN \( N \) structurally bounded w.r.t unobservable evolution (see viii in setting), the computation achieves a fix-point (no new pairs can be generated). All the pairs that are not consistent when the fix-point is achieved are dropped.

We illustrate the method by considering an arbitrary pair \( (t_i, t_j) \) where \( M_0 \cup M_{IN_i} \rightarrow M_i \cup M_{OUT_i} \) and \( M_0 \cup M_{IN_j} \rightarrow M_j \cup M_{OUT_j} \).

Let \( M_{OUT_i} \) be partitioned into the set of saturated ranked tokens \( M_{OUT}^s \) and the set of unsaturated ranked tokens \( M_{OUT}^u = M_{OUT} \setminus M_{OUT}^s \). Checking consistency implies to find an assignment between the ranked tokens required and ranked tokens produced such that all the ranked tokens required \( (M_{OUT}^s, M_{OUT}^s) \) are substituted by produced ranked tokens \( (M_{IN_i}, M_{IN_j}) \) and all the timing constraints are satisfied (satisfied).

**Definition 6:** Define the assignment function \( \psi_i : M_{IN_i} \rightarrow M_{OUT_i} \cup \{ \epsilon \} \) where for \( m_i \in M_{IN_i} \) we have:

\[
\psi_i(m_i) = \begin{cases} 
\begin{align*}
m_j \in M_{OUT_i} & \text{ if } m_j := r(p) > c_j \wedge c_j < c_i
\end{align*}
\end{cases} \tag{10}
\]

and for \( m_i \neq m_j \), \( \psi_i(m_i) = \psi_i(m_j) \Rightarrow \psi_i(m_i) = \epsilon \). Similarly define \( \psi_j : M_{IN_j} \rightarrow M_{OUT_j} \cup \{ \epsilon \} \) Then denote by \( \psi = (\psi_i, \psi_j) \) the assignment function of the common place marking and by \( \Psi \) the entire set of assignment functions.

Notice that because of the unobservable interactions there may be circular dependencies between the ranked tokens s.t. substituting e.g. a required ranked token at \( r(p) \in M_{IN_i} \) with a saturated ranked token \( r'(p) \in M_{OUT_i} \) may lead to further saturation of ranked tokens at \( r''(p) \in M_{OUT_i} \). Moreover for assuring the completeness we must also consider the case when there is no substitution for the required tokens but \( \psi(M_{IN_i}) = \epsilon \) although there were enough ranked tokens for substituting the required tokens. All the saturated tokens that are not assigned to required tokens are considered as new entered tokens \( M_{IN_i}^{new}(\psi) \) under the assignment \( \psi_i \). Notice that whenever \( M_{IN_i}^{new}(\psi) \neq \emptyset \) then \( t_i \) can be extended firing new transitions that become possible only after the arrival of the new ranked tokens \( M_{IN_i}^{new}(\psi) \).

Hence \( M_{IN_i} \) under the assignment \( \psi_i \in \Psi \) is:

\[
M_{IN_i}(\Psi) = M_{IN_i}(\psi) \cup M_{IN_i}^{new}(\psi) \cup M_{IN_i}^{new}(\psi) \tag{11}
\]

\[
M_{IN_i}(\psi) = \{ m_i(p) \neq m_j(p) \mid m_i(p) \wedge m_j(p) \in \text{set of assigned tokens (notice that by substituting } m_i(p) \text{ with } m_j(p) \text{ we obtain ranked token } c_j < r(p) < c_i \}.
\]
\{m_i(p) : r(p) < c_i \mid \psi_i(m_i) = \epsilon\} is the set of unassigned tokens and \(M^{\text{new}}_{\text{IN}}(\psi) = \{m_j \in M^{\text{OUT}}_{\text{OUT}} \mid \psi(M_{\text{IN}})\}\) is the set of new entered tokens.

Given two local explanations \(\tau_i, \tau_j\) and an assignment \(\psi\) we have that:

- the pair \((\tau_i, \tau_j)\) is consistent under the assignment \(\psi\)
  if \(M^{\text{IN}}_{\text{IN}}(\psi) = \emptyset\) and \(M^{\text{IN}}_{\text{IN}}(\psi) = \emptyset\)
- if either \(M^{\text{IN}}_{\text{IN}}(\psi) \neq \emptyset\) or \(M^{\text{IN}}_{\text{IN}}(\psi) \neq \emptyset\) then the pair \((\tau_i, \tau_j)\) is inconsistent
- if either \(M^{\text{new}}_{\text{IN}}(\psi) \neq \emptyset\) or \(M^{\text{new}}_{\text{IN}}(\psi) \neq \emptyset\) then the pair \((\tau_i, \tau_j)\) is extendable

For an extendable pair \((\tau_i, \tau_j)\) denote \(\Delta(\tau_i) = \{ \tau_i, \psi_i | \psi_i \in L(M_i \cup M^\text{new}_i) \cap T^\text{new}_i \}\) that is the set of all the traces that extend the extendable trace \(\tau_i\) by firing unobservable strings \(\psi_i\) with the new entered tokens \(M^\text{new}_i\).

Then denote \(\Delta(\tau_i) = \{ \Delta(\tau_i) \mid \forall \tau_i \Psi^\text{OUT}\}\) the local update of \(A_G\) after receiving the first message.

For \(\Delta(\tau_i) \neq \emptyset \) \(A_G\) calculates \(\Delta(\tau_i)\) and then if \(\Delta(\tau_i) \neq \emptyset\) it sends the next message \(\psi_i = (\Delta(\tau_i), \Delta(\tau_i), \psi_i)\) otherwise \(A_G\) sends the termination message (it holds for two agents since with no more new tokens entered a d-agent cannot generate new more tokens). Notice that \(\Delta(\tau_i) = \{ M_{\text{IN}}(\psi) \mid \forall \tau_i \Psi^\text{OUT}\}\).

V. CONCLUSIONS

This research is motivated by our interest in designing distributed algorithms for large plants where (e.g. because of sensors failure) unobservable inputs are sent/received between components placed in different sites. We have shown that by backward/forward search including linear timing constraints the centralized diagnosis result can be recovered. For increasing the efficiency of the local calculations one can use reachability methods based on unfoldings (backward [1] and forward unfolding [3],[10]). Further directions are the extension of this method (for reasonable models where \(K_c \leq 2\)) to time PN models and probabilistic analyze.

REFERENCES

[12] R. Su Distributed diagnosis for Discrete Event Systems PhD These, University of Toronto, 2004