Multi-agent distributed contextual diagnosis for large Petri Net models

George Jiroveanu and René K. Boel

University of Ghent, SYSTeMS Research Group
Technologiepark 914, Zwijnaarde B-9052, Gent, Belgium
{George.Jiroveanu,Rene.Boel}@UGent.be

Abstract. In this paper we consider the case of a large plant comprising different local sites each site being modeled as a Petri Net. The interactions between the local sites (modeled as common places) are considered unobservable (tokens can enter and exit unobservably the local Petri Net models). At each site a local diagnoser must provide a diagnosis of the site based on the local plant model, the local observations, and the information exchanged with its neighbors. The communication between the local diagnosers does not take place each time an observation is (locally) received but at some times according with some prescribed rules. For this general setting we present an algorithm that allows the local diagnosers to recover completely the results of a centralized diagnoser after the completion of a communication protocol and we show that under reasonable assumptions the preliminary calculation that a local diagnoser performs before communicating is useful for taking control actions even when the information exchange does not take place.

1 Introduction

This paper presents an algorithm for distributed diagnosis of large plants in a very general setting. The algorithm design is model-based with the plant model given as a (large) Petri Net (PN). Since it is commonly accepted that large and complex systems cannot be analyzed monolithically (because of the computational complexity of exploration huge state spaces), modular/distributed algorithms are designed where the plant analysis reduces to the analysis of consistent local state spaces [2–4, 7, 13, 14, 21, 27].

We consider in this paper the case of a large plant that comprises different local sites, each site being modeled as a PN. The interactions between local sites are modeled as tokens passing from one PN model to another via common (border) places [3, 4, 13, 14, 29]. At each site there is an agent supervising the activity of the local site. Each local site has its own set of sensors that can be read only by the local agent. The sensor readings are represented in a PN model by a subset of transitions (events) that are observable: whenever an observable event happens in the plant the agent is notified about its occurrence.

The plant model includes the normal plant behavior as well as the abnormal behavior that can occur after a fault modified the plant dynamics. The abnormal behavior is initiated by a subset of unobservable (silent) transitions that represent the fault events that may happen in the plant. The diagnoser must use the plant model and the plant observation in order to ask the following questions: *"Did a fault happen or not ?"*(fault detection), *"Which kind of fault happened if any ?"* (fault isolation) [26] and *"How it happened ?"*(explanations) [18].

The distributed diagnosis problem can be formulated as follows. First the local agents perform a preliminary local diagnosis, then they exchange information updating their preliminary calculations until the consistency is achieved. We require that at the time the agents achieve consistency of their local results, the agents

recover the result that would have been derived by a centralized agent that knows the overall plant model and receives the whole plant observation.

Moreover very important it is that a preliminary local diagnosis (calculated locally in absence of information exchange) to be useful for control/isolation actions that are necessary after a fault occurrence whenever a communication channel breaks down and the (global) consistency of a local site result was not achieved yet. This problem is of practical importance for spatially distributed large systems with unreliable communication between sites and is related to the question how the diagnosis result relates with some control/isolation actions that may be required to be taken in response to fault occurrences. To model the unreliable communication channels we impose as requirement that the communication between agents is not initiated by the local observations but it takes place at different times according to some prescribed rules. Thus before being able to communicate, a local agent may receive a sequence of observed events and is required to have a local preliminary calculation that *explains* what was locally observed.

A difficult problem arises when no assumption is made on the observabiltiy of the border places (i.e. the observability of the input/output transitions of the border places). When the input/output transitions of the border places are unobservable the number of tokens in the input places is unknown and the problem we face is to analyze a PN model with an uncertain initial marking [15].

When *a priori* knowledge of the token traffic between two sites is assumed known the problem can be solved by considering for the preliminary calculations upper bounds (maximum number of tokens that could have entered a local site) that result in the preliminary calculation of an over-estimate of the local plant behavior. Based on this overestimate each local agent computes an over-diagnosis of the local site. This may be useful for very conservative applications [27]. This method is a translation of the methods proposed in [2] and [26] for the plant model given as a network of communicative automata . This translation is not straightforward. Structural assumptions must be satisfied otherwise the calculation of the upper-bounds is not possible unless first generating the overall plant state space (that is usually not feasible for a large plant whose structure changes often).

In this paper we assume that the unobservable transitions are silent: tokens can move unobseravbly from one PN model to another. Thus we extend the distributed diagnosis methodology to the situation when a sensor failure is reported to the supervisor, the plant operation cannot be stopped, and the sensor is not repaired immediately. To avoid that local calculations would have the same magnitude as the global plant calculation [29] we have proposed in [4] a backward search method that starts from the locally observed events and derives the minimum number of tokens required to have entered from the neighboring sites. In this way we derive the set of minimal explanations of all the local observation together. Here we extend this method in several ways. First we drop the structural assumption considered in [4] namely *"any oriented path that leads from an input place of one site to one of its output places must contain at least one observable transition"*. The distributed algorithm proposed in this paper *recovers completely* the results of a centralized agents (by exchanging limited information the local agents) and not only the centralized diagnoser state F (a fault happened for sure [24]).

After locally computing the set of minimal explanations of the local observation based on the minimal number of tokens required to have entered, a local agent extends (forward) the minimal explanations for estimating the tokens that could have exited the local site PN model. Notice that the local preliminary calculation performed in this way does not include, nor is included in the *projection* of the global centralized calculation onto the local site. Then the algorithm checks whether local preliminary traces can be matched to consistent traces, or not (preliminary traces that can not be matched are discarded) while some new traces may be generated

because by communication "new things may be found that were possible". This is because initially a minimum number of tokens was assumed to have entered while later it may be found that more tokens than this minimal number may have entered the local site. Since at each communication round new traces are generated, we need to show that the algorithm terminates by achieving a fix point when no new traces are generated by any agent. Then the set of local traces that were found consistent recover the result of a centralized agent.

To increase the computational efficiency we use the unfolding technique for both forward [3, 19] and backward [1] calculations. Beside the advantage that a configuration in an unfolding compactly represents a family of traces (obtained by linearizing the partial order relation between the event nodes of the configuration) there is also the advantage that the partial order between the nodes induces the time information on the border-conditions (tokens that must have entered and tokens that could have exited). The information exchanged allows each local agent to check the consistency of its local results with the results of the neighboring agents.

The paper is organized as follow. Section 2 revises PN notions that are used in the paper and introduces the notation. In Section 3 we formally present the occurrence nets and the net unfolding technique. Then the reverse occurrence nets (backward unfolding) is introduced in Section 4. In Section 5 we present the centralized diagnosis of a PN model of a large plant under partial observation. Then in Section 6 we formally describe the setting of distributed plant analysis while Section 7 presents the distributed algorithm. Then in Section 8 we prove that in finitely many communication rounds the proposed distributed algorithm recovers the centralized diagnosis result by local calculations and limited information exchange. Finally Section 9 concludes the paper with some remarks and future work.

2 Definitions and notation

2.1 Petri nets

A Petri Net is a structure $\mathcal{N} = \langle \mathcal{P}, \mathcal{T}, F \rangle$ where $\mathcal{P}$ denotes the set of $\sharp\mathcal{P}$ places, $\mathcal{T}$ denotes the set of $\sharp\mathcal{T}$ transitions, and $F \subseteq (\mathcal{P} \times \mathcal{T}) \cup (\mathcal{T} \times \mathcal{P})$ is the flow relation. $F = Pre \cup Post$ where $Pre(p,t) : \mathcal{P} \times \mathcal{T} \to \mathbb{N}$ and $Post(t,p) : \mathcal{T} \times \mathcal{P} \to \mathbb{N}$ are the *pre-* and the *post-incidence relations* that specify the arcs. Denote $\mathcal{X} = \mathcal{P} \cup \mathcal{T}$. Then for $x \in \mathcal{X}$ we use the standard notations $x^\bullet = \{y \in \mathcal{X} \mid xFy\}$ and ${}^\bullet x = \{y \in \mathcal{X} \mid yFx\}$.

A *marking* M of a PN $\mathcal{N}$ is represented by a $\sharp\mathcal{P}$-vector that assigns to each place p of $\mathcal{P}$ a non-negative number of tokens $M : \mathcal{P} \to \mathbb{N}$.

The set of all possible traces of a PN $\mathcal{N}$, with an initial marking M_0 (denoted $\langle \mathcal{N}, M_0 \rangle$) is defined as follows. A transition t is *enabled* at the marking M if $M \geq Pre(\cdot, t)$. Firing, an enabled transition t consumes $Pre(\cdot, t)$ tokens in the input places of t ($p \in^\bullet t$) and produces $Post(t, \cdot)$ tokens in the output places of t ($p \in t^\bullet$). The next marking is $M' = M + Post(t, \cdot) - Pre(\cdot, t)$. A trace τ in $\langle \mathcal{N}, M_0 \rangle$ is defined as: $\tau = M_0 \xrightarrow{t_1} M_1 \xrightarrow{t_2} \ldots \xrightarrow{t_k} M_k$, where for $i = 1, \ldots, k$, $M_{i-1} \geq Pre(\cdot, t_i)$; $M_0 \xrightarrow{\tau} M_k$ denotes that the enabling conditions are all satisfied so that τ may fire at M_0 yielding M_k.

The set of all allowable traces in $\langle \mathcal{N}, M_0 \rangle$ is denoted by $\mathcal{L}_\mathcal{N}(M_0)$ while the set of reachable markings is $\mathcal{R}_\mathcal{N}(M_0) = \left\{ M \mid \exists \tau \in \mathcal{L}_\mathcal{N}(M_0) \wedge M_0 \xrightarrow{\tau} M \right\}$.

The set of transitions $\mathcal{T}$ is partitioned into disjunct sets of observable transitions $\mathcal{T}_o$ and unobservable (silent) transitions $\mathcal{T}_{uo}$.

Assumption 1 *When fired, an observable transition $t \in \mathcal{T}_o$ 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: $\forall t \in \mathcal{T}_{uo} \Rightarrow \delta(t) = \epsilon$ where ϵ is the empty string. .*

Denote by $\mathcal{T}^*$ the Kleene closure of the set $\mathcal{T}$. Let $\sigma \in \mathcal{L}_{\mathcal{N}}(M_0) \subseteq \mathcal{T}^*$ and $\mathcal{T}' \subset \mathcal{T}$. The projection $\Pi_{\mathcal{T}'} : \mathcal{L}_{\mathcal{N}}(M_0) \to \mathcal{T}'^*$ is defined as:

i) $\Pi_{\mathcal{T}'}(\epsilon) = \epsilon$;
ii) $\Pi_{\mathcal{T}'}(t) = t \ if \ t \in \mathcal{T}'$;
iii) $\Pi_{\mathcal{T}'}(t) = \epsilon \ if \ t \in \mathcal{T} \setminus \mathcal{T}'$;
iv) $\Pi_{\mathcal{T}'}(\sigma t) = \Pi_{\mathcal{T}'}(\sigma)\Pi_{\mathcal{T}'}(t)$ for $\sigma \in \mathcal{L}_{\mathcal{N}}(M_0)$ and $t \in \mathcal{T}$.

Assumption 2 *We make the assumption that the PN under investigation is:*

A1) self-loop free $\forall t \in \mathcal{T} \ {}^\bullet t \cap t^\bullet = \emptyset$
A2) bounded w.r.t to the unobservable evolution: $\forall M \in \mathcal{R}_{\mathcal{N}}(M_0)$: $M \xrightarrow{\tau} M' \wedge \tau \in \mathcal{T}_{uo}^* \Rightarrow M' \not> M$
A3) and all the arcs have capacity one $\forall (p,t),\ Pre(p,t) \leq 1 \wedge Post(t,p) \leq 1$

Definition 1 *A PN $\mathcal{N}' = \langle \mathcal{P}', \mathcal{T}', F' \rangle$ is a sub-net of the PN $\mathcal{N} = \langle \mathcal{P}, \mathcal{T}, F \rangle$ iff: $\mathcal{P}' \subseteq \mathcal{P}$, $\mathcal{T}' \subseteq \mathcal{T}$ and F' is the restriction of F to $\mathcal{P}'$ and $\mathcal{T}'$ (e.g. $F'(p,t) = F(p,t)$ if $p \in \mathcal{P}' \wedge t \in \mathcal{T}'$ otherwise it is not-defined and similarly for $F'(t,p)$). A sub-net $\mathcal{N}'$ of the PN $\mathcal{N}$ is a proper sub-net iff for any transition $\forall t \in \mathcal{T}'$ all its input and output places in $\mathcal{N}$ are preserved in $\mathcal{N}'$.*

Definition 2 *A multi set $S_{\mathbb{N}}$ over a non empty set S is a function $S_{\mathbb{N}} : S \to S \times \mathbb{N}$ that associates with each element $\alpha \in S$ the pair $(\alpha, \mu(\alpha))$ where the non-negative integer $\mu(\alpha) \in \mathbb{N}$ is the number of appearances of the element α in $S_{\mathbb{N}}(\alpha)$ ($S_{\mathbb{N}}(\alpha) = (\alpha, \mu(\alpha))$). An element of a multi-set $S_{\mathbb{N}}$ is denoted $(\alpha, \nu(\alpha))$ where $0 < \nu(\alpha) \leq \mu(\alpha)$, $\nu(\alpha) \in \mathbb{N}$.*

Given an allowable trace $\tau \in \mathcal{L}_{\mathcal{N}}(M_0)$ we denote by $alph(\tau)$ the alphabet of τ that is the set of transitions that fired in τ; $\mu(t) \mid_\tau$ counts for the number of executions of a transition $t \in alph(\tau)$ in τ. Denote by $\Sigma_{\mathbb{N}}(\tau)$ (or simply Σ_τ) the multi set corresponding with the events that are considered in τ:

$$\Sigma_\tau = \{(\alpha, \mu(\alpha) \mid_\tau) \mid \alpha \in alph(\tau)\}$$

The letters σ, τ are used for denoting strings of letters or traces. Whenever necessary we treat a marking M in a PN $\mathcal{N}$ as a multi-set defined by the marked places and the number of tokens contained in each marked place. Thus for $M \leq M'$ we use also $M \subseteq M'$. When the markings are interpreted as multisets we use $\uplus$ to denote the addition with summation of two markings.

Definition 3 *Given a PN $\mathcal{N}$, $\wp = p_0 t_1 \ldots t_n p_n$ is a non-trivial unobservable elementary path in $\mathcal{N}$ if: i) $n > 0$; ii) $t_{q+1} \subseteq p_q^\bullet \cap {}^\bullet p_{q+1}$ for $q = 1, \ldots, n$; iii) $t_q \in \mathcal{T}_{uo}$ for $q = 1, \ldots, n$. An unobservable elementary circuit (*uec*) denoted ζ is an unobservable elementary path $\wp$ that comprises different transitions and different places except for the initial place p_0 that is the same as the final place p_n.*

For a set or a multiset X, 2^X is the set of all the sub-sets of X. Given $f : X \to Y$ and $A \subseteq X$ then $f(A) = \bigcup_{x \in A} f(x)$.

3 Occurrence Nets and net unfoldings

To make the paper self-content we present in this section the unfolding technique. For more details the reader is referred to [3, 9, 10, 19].

Definition 4 *Let V be a multi set and $\preceq$ a binary relation in V ($\preceq \subseteq V \times V$). $\preceq$ is an ordering relation in V denoted $(V, \preceq)$, or V is ordered by $\preceq$ if:*

i) $\preceq$ *is reflexive* $(a \in V \Rightarrow a \preceq a)$
ii) $\preceq$ *is transitive* $(\forall a, b, c \in V, (a \preceq b) \wedge (b \preceq c) \Rightarrow (a \preceq c))$
iii) $\preceq$ *is antisymmetric* $(a, b \in V, (a \preceq b) \wedge (b \preceq a) \Rightarrow (a = b))$

For $(V, \preceq)$ *if* $\forall a, b \in V$, *either* $a \preceq b$ *or* $b \preceq a$ *then* $\preceq$ *is a total ordering relation on* V *otherwise* $\preceq$ *is a partial order in* V.

Denote by $\texttt{Min}(V)$ and $\texttt{Max}(V)$ the set of minimal respectively the set of maximal nodes of V, where $\texttt{Min}(V) = \{a \mid b \preceq a \Rightarrow a = b\}$ and $\texttt{Max}(V) = \{a \mid a \preceq b \Rightarrow a = b\}$.

Definition 5 *Given a PN* $\mathcal{N} = \langle \mathcal{P}, \mathcal{T}, F \rangle$ *the immediate dependence relation* $\prec_1 \subset (\mathcal{P} \times \mathcal{T}) \cup (\mathcal{T} \times \mathcal{P})$ *is defined as:*

$$\forall (a, b) \in (\mathcal{P} \times \mathcal{T}) \cup (\mathcal{T} \times \mathcal{P}) : a \prec_1 b \text{ iff } F(a, b) \neq 0$$

Then define $\prec$ *as the transitive closure of* $\prec_1$ $(\prec = \prec_1^*)$.

Definition 6 *Given a PN* $\mathcal{N} = \langle \mathcal{P}, \mathcal{T}, F \rangle$ *the immediate conflict relation* $\sharp_1 \subset \mathcal{T} \times \mathcal{T}$ *is defined as:*

$$\forall (t_1, t_2) \in \mathcal{T} \times \mathcal{T} : t_1 \sharp_1 t_2 \text{ iff } {}^\bullet t_1 \cap {}^\bullet t_2 \neq 0$$

Then define $\sharp \subset (\mathcal{P} \cup \mathcal{T}) \times (\mathcal{P} \cup \mathcal{T})$ *as:*

$$\forall (a, b) \in (\mathcal{P} \cup \mathcal{T}) \times (\mathcal{P} \cup \mathcal{T}) : a \sharp b \text{ iff } \exists t_1, t_2 \text{ s.t } t_1 \sharp_1 t_2 \text{ and } t_1 \preceq a \text{ and } t_2 \preceq b$$

Definition 7 *Given a PN* $\mathcal{N} = \langle \mathcal{P}, \mathcal{T}, F \rangle$ *the independence relation* $\| \subset (\mathcal{P} \cup \mathcal{T}) \times (\mathcal{P} \cup \mathcal{T})$ *is defined as:*

$$\forall (a, b) \in (\mathcal{P} \cup \mathcal{T}) \times (\mathcal{P} \cup \mathcal{T}) : a \| b \Rightarrow a \neg\sharp b \wedge a \not\preceq b \wedge b \not\preceq a$$

Definition 8 *Given two PNs* $\mathcal{N} = \langle \mathcal{P}, \mathcal{T}, F \rangle$ *and* $\mathcal{N}' = \langle \mathcal{P}', \mathcal{T}', F' \rangle$, ϕ *is a homomorphism from* $\mathcal{N}$ *to* $\mathcal{N}'$, *denoted* $\phi : \mathcal{N} \to \mathcal{N}'$ *where:*

1. $\phi(\mathcal{P}) \subseteq \mathcal{P}'$ *and* $\phi(\mathcal{T}) \subseteq \mathcal{T}'$
2. $\forall t \in \mathcal{T}$, *the restriction of* ϕ *to* ${}^\bullet t$ *is a bijection between* ${}^\bullet t$ *and* ${}^\bullet \phi(t)$
3. $\forall t \in \mathcal{T}$, *the restriction of* ϕ *to* $t^\bullet$ *is a bijection between* $t^\bullet$ *and* $\phi(t)^\bullet$

Definition 9 *An occurrence net is a net* $\mathfrak{O} = (B, E, \prec_1)$ *such that:*

i) $\forall a \in B \cup E : \neg(a \prec a)$ *(acyclic)*
ii) $\forall a \in B \cup E : \mid \{b : a \preceq b\} \mid < \infty$ *(well-formed)*
iii) $\forall a \in B : \mid {}^\bullet b \mid \leq 1$ *(no backward conflict)*

In the following B is referred as the set of conditions while E is the set of events. Denote by X_{co} a set of pairwise concurrent nodes, by X_{co}^E a concurrent set of events, and by X_{co}^B a concurrent set of conditions. A maximal (w.r.t. set inclusion) set of concurrent conditions is called a cut.

Remark 1 *The partial order relation* $\preceq$ *introduces the roughest notion of time. For instance* $a, b \in E$, $a \neq b$ *and* $a \prec b$ *can be interpreted as a happens before b.*

Definition 10 *A configuration* $C = (B, E, \prec_1)$ *in the occurrence net* $\mathfrak{O}$ *is defined as follows:*

i) C *is a sub-net of* $\mathfrak{O}$ $(C \subseteq \mathfrak{O})$
ii) C *is conflict free i.e.* $\forall a, b \in (B \cup E) \times (B \cup E) \Rightarrow a \neg\sharp b$
iii) C *is causally upward-closed i.e.* $\forall b \in B \cup E : a \prec_1 b \Rightarrow a \in B \cup E$
iv) $\texttt{Min}(C) = \texttt{Min}(\mathfrak{O})$

Denote by $\mathcal{C}$ the set of all the configurations of the occurrence net $\mathfrak{O}$.

Definition 11 *Consider a PN $\langle \mathcal{N}, M_0 \rangle$ s.t. $\forall p \in \mathcal{P} : M_0(p) \in \{0,1\}$. A branching process $\mathfrak{B}$ of a PN $\mathcal{N}$ is a pair $\mathfrak{B} = (\mathfrak{O}, \phi)$ where $\mathfrak{O}$ is an occurrence net and ϕ is a homomorphism $\phi : \mathfrak{O} \to \mathcal{N}$ s.t.:*

1. *the restriction of ϕ to $\texttt{Min}(\mathfrak{O})$ is a bijection between $\texttt{Min}(\mathfrak{O})$ and M_0 (the set of initially marked places).*
2. *$\phi(B) \subseteq \mathcal{P}$ and $\phi(E) \subseteq \mathcal{T}$*
3. *$\forall a, b \in E : ({}^\bullet a = {}^\bullet b) \wedge (a^\bullet = b^\bullet) \Rightarrow a = b$*

For a PN $\mathcal{N} = \langle \mathcal{P}, \mathcal{T}, F \rangle$ with a general initial marking $M_0 \in \mathbb{N}^{\sharp \mathcal{P}}$ the branching process $\mathfrak{O}$ of $\langle \mathcal{N}, M_0 \rangle$ is constructed in the following way (see [9]):

1. let $\mathcal{N}' = \langle \mathcal{P}', \mathcal{T}', F' \rangle$ where:
   1.1 $\mathcal{P}' = \mathcal{P} \cup \{\mathcal{P}_{start}\}$
   1.2 $\mathcal{T}' = \mathcal{T} \cup \{\mathcal{T}_{start}\}$
   1.3 $\forall (a,b) \in (\mathcal{P} \times \mathcal{T}) \cup (\mathcal{T} \times \mathcal{P}) : F'(a,b) = F(a,b)$
   1.4 for each marked place p and for each token in $M_0(p)$ we have p_{start}, t_{start} s.t. ${p_{start}}^\bullet = t_{start} \wedge t_{start}^\bullet = p$
   1.5 $\forall p_{start} \in \mathcal{P}_{start}, \ {}^\bullet p_{start} = \emptyset$
   1.6 Let $M_0'(p) = 1$ for $p \in \mathcal{P}_{start}$ and $M_0'(p) = 0$ otherwise
2. construct $\mathfrak{O}'$
3. remove $\mathcal{P}_{start}, \mathcal{T}_{start}$ and their corresponding arcs

Definition 12 *Given a PN $\langle \mathcal{N}, M_0 \rangle$ and two branching processes $\mathfrak{B}, \mathfrak{B}'$ then $\mathfrak{B}' \sqsubseteq \mathfrak{B}$ if there exists an injective homomorphism $\psi : \mathfrak{B}' \to \mathfrak{B}$ s.t. $\psi(\texttt{Min}(\mathfrak{B}')) = \texttt{Min}(\mathfrak{B})$ and $\phi \circ \psi = \phi'$.*

There exists (up to an isomorphism) a unique maximum branching process (w.r.t. $\sqsubseteq$) that is the unfolding of $\mathcal{N}$ and is denoted $\mathcal{U}_{\mathcal{N}}$ [10, 19].

4 Reverse Petri Nets (RPNs)

Backwards search methods were found applicable in different fields as model-checking [1, 12, 8], fault detection and diagnosis [22, 25, 28] modeling and analysis [20, 23], and plant estimation [15]. We present in the following the reverse occurrence nets that may be simply understood as the unfolding technique applied to the reverse net $\overleftarrow{\mathcal{N}}$ (obtained by reversing the direction of all the arcs in $\mathcal{N}$ [17]).

4.1 Coverability and Reverse Occurrence Nets

Define $a \ominus b = a - b$ if $a \geq b$, and $a \ominus b = 0$ otherwise and extend "$\ominus$" to multisets in the natural manner [1].

Definition 13 Backwards enabling rule: *A transition t is backward enabled in a marking $M \in \mathbb{N}^{\sharp \mathcal{P}}$ iff $\exists p \in t^\bullet$ s.t. $M(p) \geq 1$.* Backwards firing rule: *A backward enabled transition t in a marking $M \in \mathbb{N}^{\sharp \mathcal{P}}$ fires backwards from M producing M' (denoted $M \overset{t}{\rightsquigarrow} M'$) where $M' = M \ominus Post(t, \cdot) + Pre(\cdot, t)$.*

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

Definition 14 Given a PN $\mathcal{N}$, consider a marking $M \in \mathbb{N}^{\sharp\mathcal{P}}$. Then M is covered by M' iff $\exists \sigma \in \mathcal{L}_{\mathcal{N}}(M')$, s.t. $M' \xrightarrow{\sigma} M'' \wedge M'' \geq M$.

Proposition 1 Given a PN $\langle \mathcal{N}, M_0 \rangle$ and a marking M, then M is covered by M_0 iff $\exists M' \leq M_0$ s.t $M \overset{\sigma}{\rightsquigarrow} M'$.

Definition 15 *A reverse occurrence net (RON)* $\overleftarrow{\mathfrak{O}}$ *is a net* $\overleftarrow{\mathfrak{O}} = (\overleftarrow{B}, \overleftarrow{E}, \preceq_1)$ *s.t.:*

i) $\forall a \in \overleftarrow{B} \cup \overleftarrow{E} : \neg(a \preceq a)$ *(acyclic)*
ii) $\forall a \in \overleftarrow{B} \cup \overleftarrow{E} : \mid \{a : a \preceq b\} \mid < \infty$ *(well-formed)*
iii) $\forall a \in \overleftarrow{B} : \mid a^\bullet \mid \leq 1$ *(no-forward conflict)*
iv) $\texttt{Max}(\overleftarrow{\mathfrak{O}}) \subseteq \overleftarrow{B}$

Definition 16 *Given a PN* $\mathcal{N}$ *and a final marking* M_{fin}*, the reverse branching process of* $\langle \mathcal{N}, M_{fin} \rangle$ *is* $\overleftarrow{\mathfrak{B}} = (\overleftarrow{\mathfrak{O}}, \phi)$ *s.t.:*

i) $\phi(\overleftarrow{B}) \subseteq \mathcal{P}$ *and* $\phi(\overleftarrow{E}) \subseteq \mathcal{T}$
ii) $M_{fin} \subseteq \phi(\texttt{Max}(\overleftarrow{\mathfrak{O}}))$
iii) $\forall a, b \in \overleftarrow{E} : ({}^\bullet a = {}^\bullet b) \wedge (a^\bullet = b^\bullet) \Rightarrow a = b$

Remark 2 *Notice that above condition ii) requires that* $M_{fin} \subseteq \phi(\texttt{Max}(\overleftarrow{\mathfrak{O}}))$ *and not* $M_{fin} = \phi(\texttt{Max}(\overleftarrow{\mathfrak{O}}))$ *since our aim is to compute markings that cover* M_{fin} *and not markings that reach* M_{fin}*.*

Definition 17 *Given a PN* $\mathcal{N}$ *the immediate backward conflict relation* $\overleftarrow{\sharp}_1 \subseteq \mathcal{T} \times \mathcal{T}$ *is defined as follows:*

$$\forall (t_1, t_2) \in \mathcal{T} \times \mathcal{T} : t_1 \overleftarrow{\sharp}_1 t_2 \text{ iff } t_1^\bullet \cap t_2^\bullet$$

Then define $\overleftarrow{\sharp} \subseteq (\mathcal{P} \cup \mathcal{T}) \times (\mathcal{P} \cup \mathcal{T})$ *as:*

$$\forall (a, b) \in (\mathcal{P} \cup \mathcal{T}) \times (\mathcal{P} \cup \mathcal{T}) : a \overleftarrow{\sharp} b \Rightarrow \exists (t_1, t_2) \in \overleftarrow{\sharp}_1 \text{ s.t. } a \preceq t_1 \text{ and } b \preceq t_2.$$

Definition 18 *Given a PN* $\mathcal{N}$*, a final marking* M_{fin}*, and a reverse branching process* $\overleftarrow{\mathfrak{B}} = (\overleftarrow{\mathfrak{O}}, \phi)$*, the immediate causally confusion relation* $\overleftarrow{\sharp}_{c_1} \subseteq \overleftarrow{E} \times \overleftarrow{E}$ *is defined as follows:*

$$\forall (e_1, e_2) \in \overleftarrow{E} \times \overleftarrow{E},\ \phi(e_1) = \phi(e_2) \text{: } e_1 \overleftarrow{\sharp}_{c_1} e_2 \text{ iff } \exists b \in \overleftarrow{B} \text{ s.t. } e_1^\bullet \cap e_2^\bullet \neq \emptyset \wedge e_1^\bullet \neq e_2^\bullet$$

Then define $\overleftarrow{\sharp}_c \subseteq (\overleftarrow{B} \cup \overleftarrow{E}) \times (\overleftarrow{B} \cup \overleftarrow{E})$ *as:*

$$\forall (a, b) \in (\overleftarrow{B} \cup \overleftarrow{E}) \times (\overleftarrow{B} \cup \overleftarrow{E}) : a \overleftarrow{\sharp}_c b \Rightarrow \exists (e_1, e_2) \in \overleftarrow{\sharp}_{c_1} \text{ s.t. } a \preceq e_1 \text{ and } b \preceq e_2.$$

Definition 19 *A configuration* $\overleftarrow{C} = (\overleftarrow{B}_C, \overleftarrow{E}_C, \preceq_1)$ *in a reverse occurrence net* $\overleftarrow{\mathfrak{O}}$ *is defined as follows:*

i) $\overleftarrow{C}$ *is a sub-net of* $\overleftarrow{\mathfrak{O}}$
ii) $\overleftarrow{C}$ *is causally downward-closed -* $\forall b \in \overleftarrow{B}_C \cup \overleftarrow{E}_C : b \preceq a \Rightarrow a \in \overleftarrow{B}_C \cup \overleftarrow{E}_C$
iii) $\overleftarrow{C}$ *is backward conflict free -* $\forall (a, b) \in (B_C \cup E_C) \times (B_C \cup E_C) \Rightarrow a \neg \overleftarrow{\sharp} b$
iv) $\overleftarrow{C}$ *is causally confusion free -* $\forall (a, b) \in (B \cup E) \times (B \cup E) \Rightarrow a \neg \overleftarrow{\sharp}_c b$

v) $\texttt{Max}(\overleftarrow{C}) \subseteq \texttt{Max}(\overleftarrow{\mathfrak{O}})$ *and* $M_{fin} \subseteq \phi(\texttt{Max}(\overleftarrow{C}))$

Denote by $\overleftarrow{\mathcal{C}}$ *the set of all the configurations of a reverse occurrence net* $\overleftarrow{\mathfrak{O}}$.

By item *ii)* and *iii)* we require that in a configuration $\overleftarrow{C}$ every condition-node $b \in B_C$ has at most one input event-node in $\overleftarrow{\mathcal{U}}_{\mathcal{N}}(M_{fin})$. The reason we put this condition is that we need $\overleftarrow{C}$ to result as a configuration in a forward unfolding $\mathcal{U}_{\mathcal{N}}$. In the remaining of the paper we drop the lower index of E_C, B_C whenever this is clear from the context.

Definition 20 *Given a PN* $\mathcal{N}$ *and a final marking* M_{fin} *and two reverse branching processes* $\overleftarrow{\mathfrak{B}}, \overleftarrow{\mathfrak{B}'}$ *then* $\overleftarrow{\mathfrak{B}'} \sqsubseteq \overleftarrow{\mathfrak{B}}$ *if there exists an injective homomorphism* $\overleftarrow{\psi} : \overleftarrow{\mathfrak{B}'} \to \overleftarrow{\mathfrak{B}}$ *s.t.* $\overleftarrow{\psi}(\texttt{Min}(\overleftarrow{\mathfrak{B}'})) = \texttt{Min}(\overleftarrow{\mathfrak{B}})$ *and* $\overleftarrow{\phi} \circ \overleftarrow{\psi} = \overleftarrow{\phi'}$.

Definition 21 *Given a PN* $\mathcal{N}$ *with an initial marking* M_0 *and a final marking* M_{fin} *denote by* $\overleftarrow{\mathcal{U}}_{\mathcal{N}}(M_{fin})$ *the maximal branching process w.r.t. set inclusion s.t.* $\forall \overleftarrow{C} \in \overleftarrow{\mathcal{C}}, \exists \overleftarrow{C'} \in \overleftarrow{\mathcal{C}}$ *s.t.* $\overleftarrow{C} \sqsubseteq \overleftarrow{C'}$ *and* $\phi(\texttt{Min}(\overleftarrow{C'})) = M_0$.

Proposition 2 $\overleftarrow{\mathcal{U}}_{\mathcal{N}}(M_{fin})$ *is unique up to isomorphism.*

Proof. First denote $\overleftarrow{\mathcal{C}'} = \left\{ \overleftarrow{C'} \in \overleftarrow{\mathcal{C}} \mid \phi(\texttt{Min}(\overleftarrow{C'})) = M_0 \right\}$. Then we have by definition that every maximal configuration $\overleftarrow{C'} \in \overleftarrow{\mathcal{C}'}$ in the backward unfolding $\overleftarrow{\mathcal{U}}_{\mathcal{N}}(M_{fin})$ is also a configuration in the forward unfolding $\mathcal{U}_{\mathcal{N}}$. Since $\mathcal{U}_{\mathcal{N}}$ is unique up to isomorphism it results that also $\overleftarrow{\mathcal{U}}_{\mathcal{N}}(M_{fin})$ is unique. □

4.2 Algorithm to construct $\overleftarrow{\mathcal{U}}_{\mathcal{N}}(M_{fin})$

Given a configuration $\overleftarrow{C} = (\overleftarrow{B}, \overleftarrow{E}, \preceq_1)$ in the backward unfolding $\overleftarrow{\mathcal{U}}_{\mathcal{N}}(M_{fin})$ denote by $\texttt{Cut}(\overleftarrow{C})$ the maximal set (clique) of concurrent conditions and then denote by $\phi(\overleftarrow{C})$ the marking that corresponds to $\texttt{Cut}(\overleftarrow{C})$.

$$\texttt{Cut}(\overleftarrow{C}) = \left\{ {}^\bullet e \mid e \in \overleftarrow{E} \right\} \cup \texttt{Max}(\overleftarrow{C}) \setminus \left\{ e^\bullet \mid e \in \overleftarrow{E} \right\}$$

Denote in the following by $\overleftarrow{X^B_{co}}$ a co-set of conditions in $\overleftarrow{C}$. A transition t is backward enabled in $\overleftarrow{\mathcal{U}}_{\mathcal{N}}$ by a configuration $\overleftarrow{C}$ if $\overleftarrow{X^B_{co}} \subseteq \texttt{Cut}(\overleftarrow{C})$ and $0 < \phi(\overleftarrow{X^B_{co}}) \leq t^\bullet$.

Denote by $\texttt{Enable}(\overleftarrow{C})$ the set of all backwards enabled transitions.

$$\texttt{Enable}(\overleftarrow{C}) = \left\{ (\overleftarrow{X^B_{co}}, t) \mid (\overleftarrow{X^B_{co}}, t) \ \text{ – backwards enabled } \right\}$$

A configuration $\overleftarrow{C}$ is extended by a backwards enabled transition t in the following way:

i) add an event e with $\phi(e) = t$

ii) add arcs from each $b \in \overleftarrow{X^B_{co}}$ to e

iv) add conditions b s.t. $\phi(b) = p \wedge p \in t^\bullet \setminus \phi(\overleftarrow{X^B_{co}})$ and add arcs from each b to e

iii) add conditions b s.t. $\phi(b) = p \wedge p \in {}^\bullet t$

$\overleftarrow{\mathcal{U}}_{\mathcal{N}}$ is generated extending each configuration by enabled transitions the only requirement being that $\phi(e_1) = \phi(e_2) \wedge e_1^\bullet = e_2^\bullet \Rightarrow e_1 = e_2$ (no redundancy).

Throughout of the remaining paper we use the notation $C \odot e$ and $e \odot \overleftarrow{C}$ to indicate that a configuration C resp. $\overleftarrow{C}$ is extended forward resp. backwards by appending an event e.

Example 1 *To illustrate the computation of* $\overleftarrow{\mathcal{U}}_{\mathcal{N}}(M_{fin})$ *consider for simple PN* $\mathcal{N}$ *displayed in Fig. 1.a where* $M_{fin} = \{m(p_2) = 1, m(p_3) = 1, m(p_4) = 1\}$ *and* $M_0 = \{m(p_0) = 2\}$. *Then Fig. 1.b displays* $\mathcal{U}_{\mathcal{N}}$ *while in Fig. 1.c* $\overleftarrow{\mathcal{U}}_{\mathcal{N}}(M_{fin})$ *is displayed. We have that* $\overleftarrow{\mathcal{C}} = \left\{\overleftarrow{C}_1, \overleftarrow{C}_2\right\}$ *where the event node-sets for* $\overleftarrow{C}_1$ *and* $\overleftarrow{C}_2$ *are* $\overleftarrow{E}_1 = \{e_0', ee_0, e_1, e_2, e_3\}$ *and* $\overleftarrow{E}_2 = \{e_0, ee_0', e_1, e_2, e_3\}$ *respectively.*

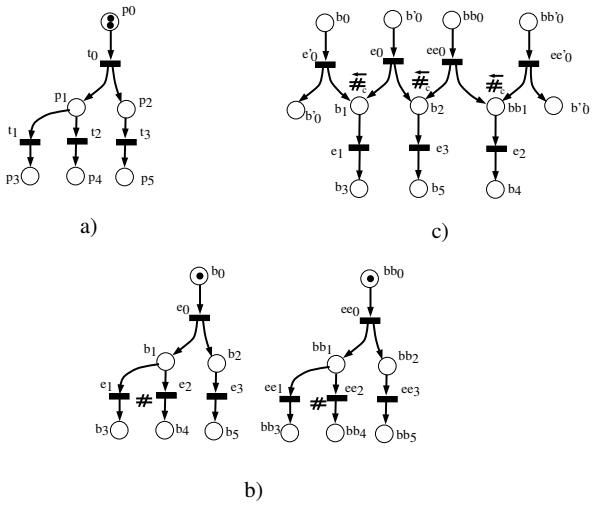

Fig. 1.

5 PN analysis under partial observation

Consider an agent Ag that supervises a plant. The agent has the plant model given as a PN $\mathcal{N}$ and receives the plant observation via the readings of a set of sensors. The plant observation is abstracted into the observation of a subset of events (i.e. the observable transitions) in the PN model. The agent Ag derives the plant estimation by deriving the set of possible evolutions from the initial state and the set of possible states the plant can be in. Further based on the plant estimation agent Ag can take some control actions in response to unpredictable (and unobservable) events (e.g. fault events) whose occurrences may lead the plant out of the desired behavior.

Assumption 3 *We consider in this paper that the observation is correct and is always received (no loss of observation or sensor failure). Moreover we consider that the observation of an event includes also the time tag when the event happened in the plant and that this time is measured with accuracy according to a global clock(GPS).*

This assumption is not too restrictive since the GPS technology is a common use nowadays. Besides in our field application (the electrical transmission power network [5]) almost all the electrical utilities have synchronized clocks at each substation.

Denote in the following by $\mathcal{O}_{\theta_c}$ the sequence of observed events received up to time θ_c by Ag where $\mathcal{O}_{\theta_c} = \langle t_1^o, \theta_{t_1^o} \rangle, \langle t_2^o, \theta_{t_2^o} \rangle, \ldots, \langle t_n^o, \theta_{t_n^o} \rangle$ with $\theta_{t_k^o}$ the time the observed event t_k^o happened in the plant.

Consider the plant observation $\mathcal{O}_{\theta_c} = t_1^o \ldots t_n^o$. Since $\mathcal{O}_{\theta_c}$ is correct and there are no delays in receiving the observation the possible ways the plant evolved is given by the set of all the possible traces in the PN model $\mathcal{N}$ that start from the known initial marking M_0 and obey the observation:

$$\mathcal{L}_{\mathcal{N}}(\mathcal{O}_{\theta_c}) = \{\tau \in \mathcal{L}_{\mathcal{N}}(M_0) \mid \Pi_{\mathcal{T}_o} \tau = \mathcal{O}_{\theta_c}\} \tag{1}$$

The set of the possible states the plant can be in is:

$$\mathcal{M}_{\mathcal{N}}(\mathcal{O}_{\theta_c}) = \left\{ M \mid \exists \tau \in \mathcal{L}_{\mathcal{N}}(\mathcal{O}_{\theta_c}) \wedge M_0 \xrightarrow{\tau} M \right\} \tag{2}$$

Consequently the plant diagnosis at the time θ_c after observing $\mathcal{O}_{\theta_c}$ is obtained by projecting the set of possible evolutions on to the set of fault events $\mathcal{T}_F$:

$$\mathcal{D}_{\mathcal{N}}(\mathcal{O}_{\theta_c}) = \{\sigma_f \mid \sigma_f = \Pi_{\mathcal{T}_F} \tau \wedge \tau \in \mathcal{L}_{\mathcal{N}}(O_{\theta_c})\} \tag{3}$$

Then the centralized diagnosis result is:

$$\mathcal{DR}_{\mathcal{N}}(\mathcal{O}_{\theta_c}) = \begin{cases} N & \text{iff } \mathcal{D}_{\mathcal{N}}(\mathcal{O}_{\theta_c}) = \{\epsilon\} \\ F & \text{iff } \epsilon \notin \mathcal{D}_{\mathcal{N}}(\mathcal{O}_{\theta_c}) \\ UF & \text{iff } \epsilon \subsetneq \mathcal{D}_{\mathcal{N}}(\mathcal{O}_{\theta_c}) \end{cases} \tag{4}$$

where N, F and UF are the diagnoser state *normal* (no fault has happened), *fault* (a fault of kind F has happened *for sure*) and respectively *uncertain* (a fault may have happened) [24].

The standard method that allows Ag for deriving $\mathcal{L}_{\mathcal{N}}(\mathcal{O}_{\theta_c})$, $\mathcal{D}_{\mathcal{N}}(\mathcal{O}_{\theta_c})$, $\mathcal{DR}_{\mathcal{N}}(\mathcal{O}_{\theta_c})$ and $\mathcal{M}_{\mathcal{N}}(\mathcal{O}_{\theta_c})$ is the forward (reachability) search starting from the known initial marking M_0. The simplest method for (forward) state space exploration for PN models is based on the generation of the reachability tree rooted in M_0. Even though it has the advantage that has a simple implementation this method is rarely used in practice because it is enumerative and the consideration of all the possible interleavings of the concurrent events leads in general to state space explosion.

The unfolding technique that is considered in the following for computing the plant evolution however popular in model-checking community for decades has been only recently introduced in the control community firstly by [3] for diagnosis and alarms interpretation and then by [16] for supervisory control. Beside a more efficient computation, the unfolding technique encodes in a configuration (that represents a possible evolution of the plant) the dependency relation between the events that are assumed that happened.

Consider again the case of the centralized agent Ag and moreover consider that the plant size is such that the off-line plant calculation (e.g. an off-line derived diagnoser automaton [24]) and its usage require more time than the on-line plant analysis.

At the receiving of the first observed event in the plant (e.g. t_1^o) Ag starts unfolding $\langle \mathcal{N}, M_0 \rangle$ computing the maximal configurations such that each maximal configuration contains only one event node $e \in E$ that corresponds to an observable transition $\phi(e) \in \mathcal{T}_o$ that is the observable transition that was observed ($\phi(e) = t_1^o$).

Denote $\mathcal{U}_{\mathcal{N}}(t_1^o)$ the net unfolding obtained in this way (notice that we drop the lower index $\mathcal{N}$ whenever clear from the context that we refer to $\mathcal{N}$). Then at the

receiving of the second observed event (e.g. t_2^o) Ag extends $\mathcal{U}(t_1^o)$ in a similar manner for finding configurations that will also include one node that corresponds to t_2^o.

Denote by $\mathcal{U}(\mathcal{O}_{\theta_c})$ the net unfolding that is obtained considering the sequence of observed events $\mathcal{O}_{\theta_c}$. Then denote by $\mathcal{C}(\mathcal{O}_{\theta_c})$ the set of configurations in $\mathcal{U}(\mathcal{O}_{\theta_c})$ s.t. $\forall C \in \mathcal{C}(\mathcal{O}_{\theta_c})$, $C = (B_C, E_C, \preceq)$ we have:

i) ϕ is a bijection between E_C^o and $\Sigma_{\mathcal{O}_{\theta_c}}$ where $E_C^o = \{e \in E_C \mid \phi(e) \in \mathcal{T}_o\}$
ii) if $\theta_{t_i^o} < \theta_{t_j^o}$ then either $\phi^{-1}(t_i^o) \prec \phi^{-1}(t_j^o)$ or $\phi^{-1}(t_i^o) \| \phi^{-1}(t_j^o)$.

In $\mathcal{U}_\mathcal{N}$ denote by $[a^\uparrow]$ the upward closure of a node a $[a^\uparrow] = \{b : b \preceq a\}$. Then denote by $[a^\uparrow]'$ the set of condition nodes that are first successors of nodes that are predecessors of a and are not contained in $[a^\uparrow]$: $[a^\uparrow]' = \{c \in B \setminus [a^\uparrow] \mid \exists b \in [a^\uparrow] \wedge b \preceq_1 c\}$. Abusing notation $[a^\uparrow] \cup [a^\uparrow]'$ denotes also the corresponding (proper) subnet of $\mathcal{U}_\mathcal{N}$.

Definition 22 *Given the unfolding $\mathcal{U}_\mathcal{N}$ of a PN $\langle \mathcal{N}, M_0 \rangle$ and an event-node e that corresponds to an arbitrary transition t ($\phi(e) = t$) then $MinC(t)$ is a minimal configuration that allows for the execution of e (resp. t):*

$$MinC(t) = [e^\uparrow] \cup [e^\uparrow]' \cup \{\texttt{Min}(\mathcal{U}_\mathcal{N}) \setminus [e^\uparrow]\}$$

If e corresponds with the first observed event t_1^o then excepting $e = \phi^{-1}(t_1^o)$, $MinC(t_1^o)$ contains only unobservable event-nodes. Denote by $Min\mathcal{C}(t_1^o)$ the set of minimal configurations of the first observed event.

Given a minimal configuration $MinC \in Min\mathcal{C}(t_1^o)$ we say that $MinE$ (the set of event-nodes of $MinC$) is the minimal explanation of t_1^o. We denote by $\langle MinE \rangle$ the set of linearizations of the partial order between the nodes of $MinE$ that is:

$$\langle MinE \rangle = \{\ \sigma = e_1 \ldots e_m \mid \forall i, j \ :\ e_i \prec e_j \Rightarrow 1 \leq i < j \leq m\}$$

Then $Min\mathcal{E}(t_1^o)$ denotes the set of all minimal explanations:

$$Min\mathcal{E}(t_1^o) = \{\sigma \mid \sigma \in \langle MinE \rangle \wedge MinC \in Min\mathcal{C}(t_1^o)\}$$

The set of minimal traces in $\mathcal{N}$ that explain t_1^o is:

$$\mathcal{L}^{min}(t_1^o) = \{\tau \mid \tau = \phi(\sigma) \wedge \sigma \in Min\mathcal{E}(t_1^o)\} \tag{5}$$

Definition 23 *$MinC \in \mathcal{C}(\mathcal{O}_{\theta_c})$ is a minimal configuration for a sequence of observed events $\mathcal{O}_{\theta_c} = t_1 \ldots t_k$ if $\forall a \in MinE \Rightarrow \exists b \in MinE$ s.t. $\phi(b) \in alph(\mathcal{O}_{\theta_c}) \wedge a \preceq b$.*

For an arbitrary observation $\mathcal{O}_{\theta_c}$, denote by $Min\mathcal{C}(\mathcal{O}_{\theta_c})$ the set of all the minimal configurations and by $Min\mathcal{E}(\mathcal{O}_{\theta_c})$ the set of minimal explanations of $\mathcal{O}_{\theta_c}$. Consequently the set of minimal traces that explain $\mathcal{O}_{\theta_c}$ is:

$$\mathcal{L}^{min}(\mathcal{O}_{\theta_c}) = \{\tau \mid \tau = \phi(\sigma) \wedge \sigma \in \langle MinE(\mathcal{O}_{\theta_c}) \rangle\}$$

and the set of estimated states considering the minimal explanations of $\mathcal{O}_{\theta_c}$ is:

$$\mathcal{M}^{min}(\mathcal{O}_{\theta_c}) = \left\{M \mid M_0 \xrightarrow{\tau} M \wedge \tau \in \mathcal{L}^{min}(\mathcal{O}_{\theta_c})\right\}$$

Thus we have that $\mathcal{L}^{min}(\mathcal{O}_{\theta_c}) \subseteq \mathcal{L}(\mathcal{O}_{\theta_c})$ and

$$\forall \mathcal{O}_{\theta_c} \quad \bigcup_{M' \in \mathcal{M}^{min}(\mathcal{O}_{\theta_c})} \mathcal{R}_\mathcal{N}(M') \ = \bigcup_{M'' \in \mathcal{M}(\mathcal{O}_{\theta_c})} \mathcal{R}_\mathcal{N}(M'') \tag{6}$$

Assumption 4 *We make the natural assumption that the fault events are (unobservable) choices that the plant may take as not obeying the (normal) designed behavior. Thus in any reachable marking M, there exists at least one normal (not-faulty) transition that is enabled:*

$$\forall M \in \mathcal{R}_{\mathcal{N}}(M_0) \quad : \quad \exists t \in \mathcal{T} \setminus \mathcal{T}_F \ s.t. \ Pre(\cdot, t) \leq M$$

Proposition 3 *Given a PN $\langle \mathcal{N}, M_0 \rangle$ and an arbitrary observation $\mathcal{O}_{\theta_c}$ then whenever $\mathcal{DR}(\mathcal{O}_{\theta_c}) = F$ (the diagnosis result based on $\mathcal{L}(\mathcal{O}_{\theta_c})$ indicates that a fault happened for sure see Eq. 4) then the diagnosis result based on $\mathcal{L}^{min}(\mathcal{O}_{\theta_c})$ also indicates that the a fault happened for sure ($\mathcal{DR}^{min}(\mathcal{O}_{\theta_c}) = F$).*

$$\forall \mathcal{O}_{\theta_c} \quad \mathcal{DR}(\mathcal{O}_{\theta_c}) = F \Leftrightarrow \mathcal{DR}^{min}(\mathcal{O}_{\theta_c}) = F$$

Proof. Straightforward based on Assumption 4. □

Based on Proposition 3 we have that if the agent Ag is allowed to take control actions only when the diagnosis result indicates that a fault happened for sure in the plant then there is sufficient to calculate $\mathcal{L}^{min}(\mathcal{O}_{\theta_c})$ that is usually very small comparing with $\mathcal{L}(\mathcal{O}_{\theta_c})$.

The computation of $\mathcal{L}^{min}(\mathcal{O}_{\theta_c})$ is made backwards starting from the observed events in the following way.

First the reverse occurrence net $\overleftarrow{\mathcal{U}}(t_1^o)$ that corresponds to the first observed event t_1^o is calculated by Algorithm 1.

Algorithm 1 B_Unfold(t^o)

Input: t^o, M_0

Output: $\overleftarrow{\mathcal{U}}(t^o)$

1: $\overleftarrow{\mathcal{U}} = {}^\bullet e \cup e \cup e^\bullet$ where $\phi(e) = t^o$

2: $\overleftarrow{C}_0 = \overleftarrow{\mathcal{U}}; \overleftarrow{\mathcal{C}} = \left\{ \overleftarrow{C}_0 \right\}$

3: $\texttt{Enable} = \bigcup_{\overleftarrow{C} \in \overleftarrow{\mathcal{C}}} \texttt{Enable}(\overleftarrow{C}) \cap \mathcal{T}_{uo}$

4: **while** $\texttt{Enable} \neq 0$ **do**

5: pick and delete $e = (\overleftarrow{X}^B_{co}, t) \in \texttt{Enable}$

6: $\overleftarrow{C}_{new} = e \odot \overleftarrow{C}$ {*extend* $\overleftarrow{\mathcal{U}}$}

7: $\overleftarrow{\mathcal{C}} = \overleftarrow{\mathcal{C}} \cup \overleftarrow{C}_{new}$

8: $\texttt{Enable} := \texttt{Enable} \cup \texttt{Enable}(\overleftarrow{C}_{new})$

9: **end while**

Remark 3 *Notice that in B_Unfold(t^o) the termination conditions that guarantee that the computation terminates are not presented. This can be easily implemented by counting the executions of the unobservable cycles and using the fact that if M is not unobservably covered by M_0 then $\forall M' > M$, M' is also not covered unbseravably by M_0. Notice that $\langle \mathcal{N}, M_0 \rangle$ is assumed bounded w.r.t. the unobservable evolution.*

Consider now the observed sequence $\mathcal{O}_{\theta_c} = t_1^o \ldots t_n^o$ the computation of $\overleftarrow{\mathcal{U}}(\mathcal{O}_{\theta_c})$ and $\overleftarrow{\mathcal{C}}(\mathcal{O}_{\theta_c})$ is done recursively as is presented in Algorithm 2.

Proposition 4 *Given $Min\mathcal{U}(\mathcal{O}_{\theta_c}) \subseteq \mathcal{U}(\mathcal{O}_{\theta_c})$ and $\overleftarrow{\mathcal{U}}(\mathcal{O}_{\theta_c})$ we have that:*

Algorithm 2 B_Unfold($\mathcal{O}_{\theta_c}$)

Input: $\mathcal{O}_{\theta_c}$

Output: $\overleftarrow{\mathcal{U}}(\mathcal{O}_{\theta_c})$

1: $k := 1$;
2: B_Unfold(t_1^o, M_0) {compute $\overleftarrow{\mathcal{U}}(t_1^o)$}
3: **while** $k \leq n$ **do**
4: **while** $\overleftarrow{\mathcal{C}}(\mathcal{O}_{\theta_c}^k) \neq \emptyset$ **do**
5: pick and delete $\overleftarrow{C} \in \overleftarrow{\mathcal{C}}(\mathcal{O}_{\theta_c}^k)$
6: B_Unfold(t_{k+1}^o) {compute $\overleftarrow{\mathcal{U}}(t_{k+1}^o, \phi(\texttt{Max}(\overleftarrow{C}))$}
7: $\overleftarrow{C}(\mathcal{O}_{\theta_c}^{k+1}) = \overleftarrow{C}(\mathcal{O}_{\theta_c}^k) \odot \overleftarrow{C}(t_{k+1}^o)$ {compute $\overleftarrow{\mathcal{U}}(t_1^o, \ldots, t_k^o)$}
8: $\overleftarrow{\mathcal{U}}(\mathcal{O}_{\theta_c}^{k+1}) = \overleftarrow{\mathcal{U}}(\mathcal{O}_{\theta_c}^{k+1}) \cup \overleftarrow{C}(\mathcal{O}_{\theta_c}^{k+1})$
9: **end while**
10: $k := k + 1$
11: **end while**

i) $\forall \overleftarrow{C} \in \overleftarrow{\mathcal{C}}(\mathcal{O}_{\theta_c}) \Rightarrow \exists\ MinC \in \mathcal{U}(\mathcal{O}_{\theta_c})$ *s.t.* $\overleftarrow{C} \equiv MinC$ *(read as* $\overleftarrow{C}$ *is isomorphic with* $MinC$*)*

ii) $\forall MinC \in \mathcal{U}(\mathcal{O}_{\theta_c}) \Rightarrow \exists\ \forall \overleftarrow{C} \in \overleftarrow{\mathcal{C}}(\mathcal{O}_{\theta_c})\ MinC \equiv \overleftarrow{C}$

Thus it results that $\bigcup_{\overleftarrow{C} \in \overleftarrow{\mathcal{C}}(\mathcal{O}_{\theta_c})} \phi(\langle \overleftarrow{E} \rangle) = \mathcal{L}^{min}(\mathcal{O}_{\theta_c})$.

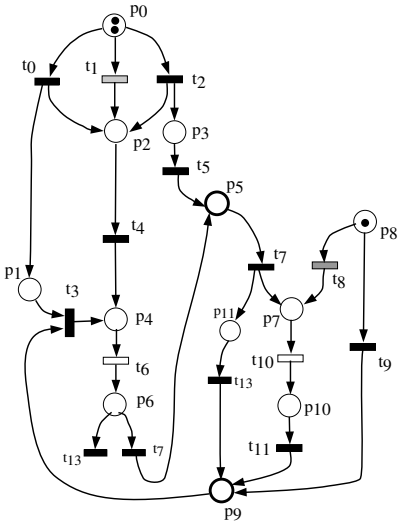

Fig. 2.

Example 2 *Consider the PN* $\langle \mathcal{N}, M_0 \rangle$ *displayed in Fig. 2 where the observable transitions are* t_6 *and* t_{10} *and the fault transitions are* t_1, t_8*. The initial marking is* $M_0 = \{m(p_0) = 2; m(p_8) = 1\}$*. Let the first observed event be* t_6*. By a simple (forward) reachability analysis one can obtain:*

$$\mathcal{L}_{\mathcal{N}}(t_6) = \{t_0 t_4 t_6; t_0 t_0 t_4 t_6; t_0 t_4 t_6 t_7; t_1 t_4 t_6 t_0;\ \ etc\}$$

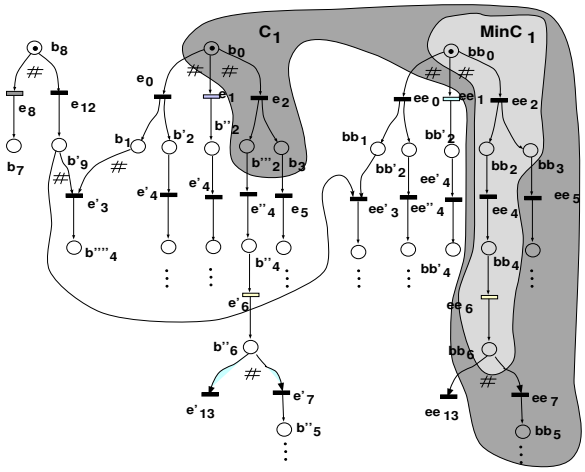

Fig. 3.

The unfolding $\mathcal{U}(t_6)$ of $\langle \mathcal{N}, M_0 \rangle$ given the observation $\mathcal{O}_{\theta_c} = t_6$ is displayed in Fig.3. The two tokens in $M_0(p_0)$ are represented by the conditions b_0 and bb_0 (the start places and the start transitions were removed). The lower index of the labels of the nodes in $\mathcal{U}_\mathcal{N}$ indicate the corresponding node in $\mathcal{N}$ (e.g. $\phi(e_i) = t_i$ and $\phi(b_i) = p_i$) while the double notation ee and bb with prime and multi-prime are used for distinct nodes in $\mathcal{U}_\mathcal{N}$ that correspond to the same node in $\mathcal{N}$. $MinC_1$ (in grey) represents a minimal configuration: $MinC_1 = [ee_6'' \uparrow] \cup [ee_6'' \uparrow]'$ where $\phi(ee_6'') = t_6$. In darken grey there is represented the configuration C_1, $MinC_1 \sqsubseteq C_1$. Notice that $C_1 \setminus MinC_1$ includes unobservable nodes that are concurrent with ee_6'' (e.g. ee_5, e_2) and nodes that are successors of ee_6'' (e.g. ee_7''). C_1 compactly represents a set of traces that can be obtained by linearizing the partial order relation between the nodes $E_1 = \{e_2, ee_2, ee_5, ee_4'', ee_6'', ee_7''\}$ (e.g. $t_2t_2t_4t_6t_7t_5; t_2t_4t_2t_6t_7t_5; t_2t_4t_6t_2t_7t_5$; etc.).

The backward unfolding $\overleftarrow{\mathcal{U}}(t_6)$ is presented in Fig. 4. $\overleftarrow{C_1}$ compactly represents $t_{12}t_0t_3t_6$ and $t_0t_{12}t_3t_6$.

$$\mathcal{L}^{min}(t_6) = \{t_0t_4t_6; t_1t_4t_6; t_2t_4t_6; t_0t_{12}t_3t_6; t_{12}t_0t_3t_6; t_0t_2t_5t_9t_{13}t_3t_6; \ \ldots\}$$

6 The distributed setting

We consider the distributed plant description as follow:

i) $\mathcal{N} = \bigcup_{i \in I} \mathcal{N}_i$ where $\mathcal{N} = \langle \mathcal{P}, \mathcal{T}, F \rangle$, $\mathcal{N}_i = \langle \mathcal{P}_i, \mathcal{T}_i, F_i \rangle$, and $i \in I$
ii) $\mathcal{P} = \bigcup_{i \in I} \mathcal{P}_i$, $\forall i \in I$, $\exists j \in I$, $i \neq j$ s.t. $\mathcal{P}_i \cap \mathcal{P}_j \triangleq \mathcal{P}_{ij} \neq \emptyset$
iii) $\mathcal{T} = \bigcup_{i \in I} \mathcal{T}_i$, $\forall i, j \in I$, $i \neq j \Rightarrow \mathcal{T}_i \cap \mathcal{T}_j = \emptyset$
iv) $F_i = F \mid_{\mathcal{N}_i}$
v) $\mathcal{P}_{ij} = \mathcal{P}_{IN_{ij}} \cup \mathcal{P}_{OUT_{ij}}$, $\mathcal{P}_{IN_{ij}} \cap \mathcal{P}_{OUT_{ij}} = \emptyset$
vi) $\mathcal{P}_{IN_{ij}} = \mathcal{P}_{OUT_{ji}} = \{p \in \mathcal{P}_{ij} \mid p^\bullet \subseteq \mathcal{T}_i \wedge {}^\bullet p \subseteq \mathcal{T}_j\}$
vii) $\mathcal{P}_{IN_{ji}} = \mathcal{P}_{OUT_{ij}} = \{p \in \mathcal{P}_{ji} \mid {}^\bullet p \subseteq \mathcal{T}_i \wedge p^\bullet \subseteq \mathcal{T}_j\}$
viii) $\mathcal{N}$ is structurally bounded w.r.t. the unobservable evolution i.e. $\forall M \in \mathbb{N}^{\sharp\mathcal{P}} \ \wedge$ $\forall \sigma_{uo} \in \mathcal{T}_{uo}^* : M \xrightarrow{\sigma_{uo}} M' \Rightarrow M' \not> M$

For simplicity we assume at item v above that $\mathcal{P}_{IN_{ij}}$ and $\mathcal{P}_{OUT_{ij}}$ are disjunct and moreover we consider $M_{0_{ij}} = 0$ ($M_{0_{ij}} = M_0(\mathcal{P}_{12})$, $\forall i, j \in I$). Denote $\mathcal{P}_{IN_i} = \{\mathcal{P}_{IN_{ij}} \mid j \in I, j \neq i \wedge \mathcal{P}_{IN_{ij}} \neq \emptyset\}$ and $\mathcal{P}_{OUT_i} = \{\mathcal{P}_{OUT_{ij}} \mid j \in I, j \neq i \wedge \mathcal{P}_{OUT_{ij}} \neq \emptyset\}$.

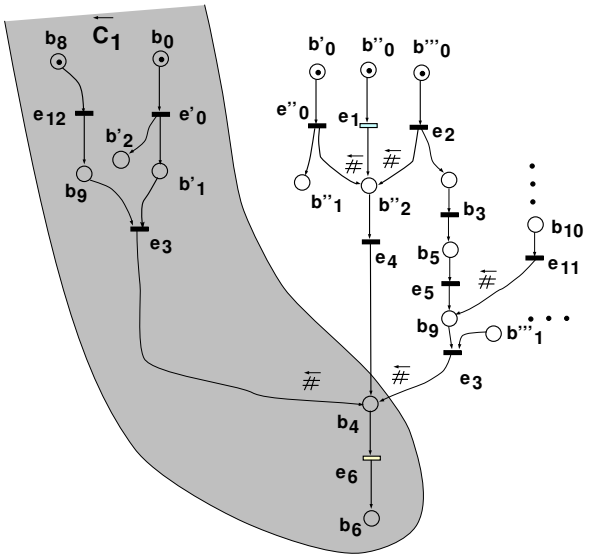

Fig. 4.

Given the set of agents $\mathcal{AG} = \{Ag_i \mid i \in I\}$, where the knowledge an agent Ag_i has is: $\mathcal{K}_i = \langle \mathcal{N}_i, \mathcal{T}_{o_i}, \mathcal{T}_{F_i}, M_{0_i}, \mathcal{P}_{IN_i}, \mathcal{P}_{OUT_i} \rangle$ consider that:

i) the plant observation is distributed $\mathcal{O}_{\theta_c} = \otimes_{i \in I}^{gc} \mathcal{O}^i_{\theta_c}$. $\mathcal{O}^i_{\theta_c} = t^o_{1_i} \ldots t^o_{n_i}$ is the local observation recorded at site $i \in I$, where the observed events $\langle t^o_{k_i}, \theta_{k_i} \rangle$ have the time tag θ_{k_i} indicating the time event $t^o_{k_i}$ happened in the plant is measured according with a global clock (denoted gc in short).
ii) the communication between agents is not event-driven i.e. the agents are allowed to communicate at $\theta_c, \theta'_c \ldots$.

Problem formulation: Given the above setting design a distributed algorithm such that:

R1) before communicating with the other agents, Ag_i ($i \in I$) derives a local preliminary diagnosis of the local site i
R2) when the communication is allowed (e.g. at the global time θ_c) then
  2.1) each local agent derives the (limited) information that should be sent to the neighboring agents for achieving the consistency of the local calculations
  2.2) the local calculation of site i is updated when new information is received
R3) then each local agent iterates the step 2.1) and 2.2) until a stopping criterion is achieved (the communication protocol terminates)
R4) the completion of the communication protocol at the communication time θ_c guarantees that the agents recover the diagnosis result a centralized agent by consistent pairs of local diagnostics

The assumption made above is that the communication exchange between two neighboring agent is simultaneous (synchronous) and takes place in different communication rounds and that the local calculations at each site do not include new observations (events observed happening after θ_c). The consideration of asynchronous communication exchange brings nothing new but some more notation.

In the following section we present a distributed algorithm that comprises:

i) a procedure for performing the local preliminary calculations in absence of of any external information (Section 7.2)

ii) a procedure for information exchange (Section 7.3)
iii) a procedure for updating a local calculation to incorporate the received information (Section 7.4)

Then in Section 8 we prove the main result of our paper that is the distributed algorithm we propose terminates after finitely many communication rounds and by the completion of the information exchange (communication protocol) the centralized diagnosis result is recovered.

7 The distributed algorithm

We start this section by emphasizing first the difficulties in designing a distributed algorithm under the setting that we consider and then the three procedures afore mentioned are presented in detail.

7.1 Discussion

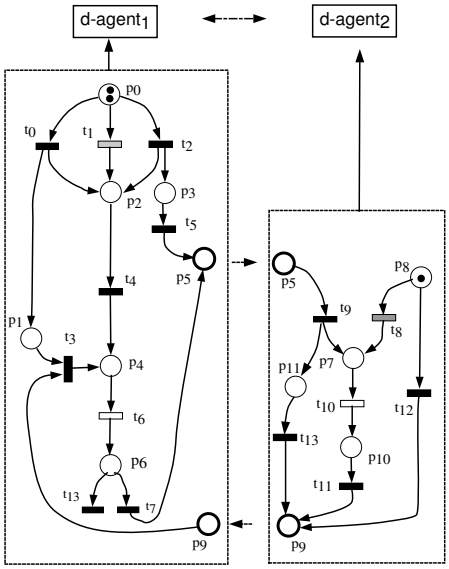

Fig. 5.

Consider the distributed architecture shown in Fig.5. Let the local observation at site 1 and site 2 be: $\mathcal{O}^1 = t_6$ and $\mathcal{O}^2 = t_{10}$ respectively. The input and output transitions of the border places p_5 and p_9 are unobservable thus Ag_1 and Ag_2 should analyze PN models whose initial markings are uncertain that is even though the agents know the initial local marking M_{0_1} and resp. M_{0_2} tokens from the neighboring site could have entered the local PN models.

Since there is required a preliminary local calculation before communicating with the other agents (see $R1$ above) we are in trouble because the local agents should handle PN models with uncertain markings (due to the unobservable interactions with the neighboring site).

Consider the case of Ag_2. Via the border place p_5 tokens can enter $\mathcal{N}_2$ and then leave via p_9. The question we must answer is: *"what Ag_2 should do before*

communicating with the neighboring agent Ag_1 ?". One solution would be to consider upper bounds for the marking of the input places of each component (e.g. p_5 for $\mathcal{N}_2$ in Fig. 5), computing in this way an over-estimate of the local site behavior that is checked for consistency by communication.

This solution was proposed in [2] for modular analysis and in [26] for distributed computation of a plant model given as a network of communicating automata but it can not be translated straightforward for Petri Nets models unless the PN model is converted into a communicative automata model but by this the advantage of compact state representation of PN models would vanish.

The approach we follow for designing the distributed algorithm that can be outlined as follow:

i) the local preliminary computation comprises two phases: $i.1$) first a backward calculation is performed for deriving the set of minimal configurations that provide the minimal explanations of the local observation based on the assumption that the minimal number of tokens have entered the local site; $i.2$) then the minimal configurations are extended for finding the tokens that could have exited the local site if the minimum number of tokens would have been provided.
ii) then by communicating limited information with its neighbors Ag_i checks the consistency of its local results and also generates new local traces that are checked consistent in a new communication round.
iii) when a fix point is achieved the consistent set of local results recover the centralized diagnosis result.

7.2 Procedure for performing local preliminary calculations

In this subsection we present formally the preliminary calculations performed by a local agent Ag_i ($i \in I$) before it initiates the communication with its neighbors.

Consider in the following the case of the agent Ag_i having received the local site observation $\mathcal{O}^i_{\theta_c} = t^o_{1_i} \dots t^o_{n_i}$. Since there is not a priori knowledge of the marking of the input places $\mathcal{P}_{IN_i}$, Ag_i can make any assumption on the number of tokens that could have entered $\mathcal{N}_i$.

Thus if Ag_i considers for each $p_i \in \mathcal{P}_{IN_i}$ a marking ω it can then perform a backward search for finding the minimal configurations (minimal explanations) of $\mathcal{O}^i_{\theta_c}$ considering as initial marking $M^\omega_{0_i}$ where:

$$M^\omega_{0_i} = \begin{cases} M^\omega_{0_i}(p_i) = M_{0_i} \ \ for \ \ p_i \in \mathcal{P}_i \setminus \mathcal{P}_{IN_i} \\ M^\omega_{0_i}(p_i) = \omega \ \ for \ \ p_i \in \mathcal{P}_{IN_i} \end{cases} \tag{7}$$

As presented in Section 4 Ag_i can construct $\overleftarrow{\mathcal{U}}_i(\mathcal{O}^i)$ by running the algorithm **B_Unfold**($\mathcal{O}_{\theta_c}$) with the *inputs*: $\langle \mathcal{N}_i, M^\omega_{0_i} \rangle$, $\mathcal{O}^i_{\theta_c}$, $\mathcal{T}_{o_i}$, $\mathcal{T}_{uo_i}$.

By computing $\overleftarrow{\mathcal{U}}_i(\mathcal{O}^i_{\theta_c})$ Ag_i derives the set of configurations $\overleftarrow{\mathcal{C}}_i(\mathcal{O}^i_{\theta_c})$. Given a configuration $\overleftarrow{C}_i \in \overleftarrow{\mathcal{C}}_i(\mathcal{O}^i_{\theta_c})$ denote $\mathtt{Min}(\overleftarrow{B}_{IN_i})$ the set of conditions that correspond to the input places $p_i \in \mathcal{P}_{IN_i}$:

$$\mathtt{Min}(\overleftarrow{B}_{IN_i}) = \left\{ b_i \mid b_i \in \mathtt{Min}(\overleftarrow{B}_i) \wedge \phi(b_i) = p_i \wedge p_i \in \mathcal{P}_{IN_i} \right\}$$

and let $\underline{M}_i(\mathcal{P}_{IN_i}) = \phi(\mathtt{Min}(\overleftarrow{B}_{IN_i}))$ be the minimal marking of the input places $\mathcal{P}_{IN_i}$ s.t. $\overleftarrow{C}_i$ is allowable. In the following we use the simplified notations: $\underline{M}_{IN_i}$ for $\underline{M}_i(\mathcal{P}_{IN_i})$ and. $\underline{M}_{0_i} = M_{0_i} \uplus \underline{M}_{IN_i}$. Then denote $\underline{\mathcal{M}}_{IN_i}$ the set of minimal assumptions on the marking of the input places $\mathcal{P}_{IN_i}$:

$$\underline{\mathcal{M}}_{IN_i} = \left\{ \underline{M}_{IN_i} \mid \overleftarrow{C}_i \in \overleftarrow{\mathcal{C}}_i(\mathcal{O}^i_{\theta_c}) \wedge \underline{M}_{IN_i} = \phi(\mathtt{Min}(\overleftarrow{B}_{IN_i})) \right\}$$

Denote $\underline{\mathcal{E}}_i$ the set of minimal preliminary explanations of the local observation $\mathcal{O}^i_{\theta_c}$ based on the minimal assumptions $\underline{\mathcal{M}}_{IN_i}$

$$\overleftarrow{\underline{\mathcal{E}}}_i = \left\{ \sigma_i \mid \exists \overleftarrow{C}_i \in \overleftarrow{\mathcal{C}}_i(\mathcal{O}^i_{\theta_c}) \wedge \sigma_i \in \langle \overleftarrow{E}_i \rangle \right\}$$

Denote by $\underline{\mathcal{M}}_i$ the set of estimated markings based on the set of minimal explanations $\underline{\mathcal{E}}_i$ and the minimal assumptions $\underline{\mathcal{M}}_{IN_i}$:

$$\underline{\mathcal{M}}_i = \left\{ \underline{M}_i \mid \exists \underline{M}_i \in \underline{\mathcal{M}}_i(\mathcal{P}_{IN_i}), \exists \tau_i \in \phi(\underline{\mathcal{E}}_i) : \underline{M}_{0_i} \xrightarrow{\tau_i} \underline{M}_i \right\}$$

Given an unobservable elementary cycle ζ, denote by Υ_ζ the set of limiting places of ζ: $\Upsilon_\zeta \triangleq \{p \mid p \notin \zeta \wedge \exists t \in \zeta \ s.t. \ p \in {}^\bullet t\}$. A place $p \in \Upsilon_\zeta$ is a limiting places of ζ since every complete execution of ζ consumes tokens from p. Denote M_{Υ_ζ} the minimal marking of Υ_ζ that allows for a complete execution of ζ.

Assumption 5 *For any local model $\mathcal{N}_i$ and for any* uec *ζ_i, there does not exist an executable sequence of unobservable transitions σ_{uo_i} with initial marking the marking M that has tokens only in the input places IN_i ($M(p) = 0$ for $p \notin \mathcal{P}_{IN_i}$) s.t. by firing from M, σ_{uo_i} produces a marking M' greater than the limiting marking of ζ_i, $M_{\Upsilon_{\zeta_i}}$. $\nexists \sigma_{uo} \in T^*_{uo_i}$ s.t. $(M_{\Upsilon_{\zeta_i}} \overset{\sigma_{uo_i}}{\rightsquigarrow} M) \wedge (M(p) \neq 0 \Rightarrow p \in \mathcal{P}_{IN_i})$.*

Proposition 5 *Given a PN model $\mathcal{N}$ s.t. $\forall i \in I$ Assumption 5 holds true for $\mathcal{N}_i$, then $\forall \mathcal{O}^i_{\theta_c}$ by running **B_Unfold**($\mathcal{O}_{\theta_c}$) (Algorithm 2) for $\langle \mathcal{N}_i, M^\omega_{0_i} \rangle$ and $\mathcal{O}^i_{\theta_c}$ we obtain the set of minimal assumptions of the marking of input places $\mathcal{P}_{IN_i}$ s.t. $\forall \underline{M}_{IN_i} \in \underline{\mathcal{M}}_{IN_i}$ and $\forall p_i \in \mathcal{P}_{IN_i} \Rightarrow \underline{M}_{IN_i}(p_i) < +\infty$.*

Proof. By Assumption 5 we have that for any marking M_{IN_i} of the input places IN_i any cycle in $\mathcal{N}_i$ cannot be executed finitely many times. Thus any node in a configuration will have a finite number of predecessor-nodes. □

Consider that at the time θ_c when the communication with the neighboring agents is the first time allowed Ag_i has computed $\overleftarrow{\mathcal{U}}(\mathcal{O}^i_{\theta_c})$ having derived $\overleftarrow{\mathcal{C}}(\mathcal{O}^i_{\theta_c})$ that comprises the set of preliminary minimal explanations $\overleftarrow{\mathcal{E}}_i$ and the set of minimal assumptions $\underline{\mathcal{M}}_{IN_i}$. Then Ag_i must calculate, based on the set of minimal assumptions regarding the tokens that have entered $\underline{\mathcal{M}}_{IN_i}$, the estimate of the number of tokens that could have exited $\mathcal{N}_i$ via $\mathcal{P}_{OUT_i}$.

For doing this Ag_i extends every minimal configuration $\overleftarrow{C}_i \in \overleftarrow{\mathcal{C}}_i(\mathcal{O}^i_{\theta_c})$ by considering all the unobservable extensions (sequences of unobservable transitions) that can be appended. Thus $\overleftarrow{C}_i$ is forward extended by starting from the set of maximal conditions $\mathtt{Max}(\overleftarrow{C}_i)$ ($\phi(\mathtt{Max}(\overleftarrow{C}_i)) = \underline{M}_i$ where $\underline{M}_{0_i} \xrightarrow{\tau_i} \underline{M}_i$ and $\tau_i \in \phi(\langle \overleftarrow{E}_i \rangle)$).

The unobservable transitions that are enabled in $M_i/\mathtt{Max}(\overleftarrow{C}_i)$ are appended generating new configurations that are further extended until the set of enabled events contains only observable events (that were not observed yet) when the calculation stops.

Given $\underline{M}_{0_i} \in \underline{\mathcal{M}}_{0_i}$ denote by $Min\mathcal{U}(\mathcal{O}^i_{\theta_c}, \underline{M}_{0_i})$ the subnet of $\overleftarrow{\mathcal{U}}(\mathcal{O}^i_{\theta_c})$ that corresponds to $\underline{M}_{0_i}$. Then let $Min\mathcal{U}(\mathcal{O}^i_{\theta_c}, \underline{\mathcal{M}}_{0_i})$ be the set the minimal unfoldings $Min\mathcal{U}(\mathcal{O}^i_{\theta_c}, \underline{M}_{0_i})$ and denote by $Min\mathcal{C}(\mathcal{O}^i_{\theta_c}, \underline{\mathcal{M}}_{0_i})$ the set of all minimal configurations.

Then denote by $\mathcal{U}(\mathcal{O}^i_{\theta_c}, \underline{M}_{0_i})$ the maximal unobservable extension (w.r.t. set inclusion) of a minimal configuration $MinC(\mathcal{O}^i_{\theta_c}, \underline{M}_{0_i})$ and denote $\mathcal{C}(\mathcal{O}^i_{\theta_c}, \underline{M}_{0_i})$ the set of configurations in $\mathcal{U}(\mathcal{O}^i_{\theta_c}, \underline{M}_{0_i})$ where:

$$\mathcal{C}(\mathcal{O}^i_{\theta_c}, \underline{M}_{0_i}) = \{C \mid C = MinC(\mathcal{O}^i_{\theta_c}, \underline{M}_{0_i}) \odot e_{1_i} \ldots \odot e_{k_i} \ \wedge \\ \wedge \ \phi(e_{q_i}) \in \mathcal{T}_{uo_i}, q_i = 1_i, \ldots, k_i\}$$

Abusing notation denote $\mathcal{E}(\mathcal{O}^i_{\theta_c}, \underline{M}_{0_i})$ the set of local traces in $\mathcal{N}_i$ that are obtained by linearizing $\langle \mathcal{E}(\mathcal{O}^i_{\theta_c}, \underline{M}_{0_i}) \rangle$:

$$\mathcal{E}(\mathcal{O}^i_{\theta_c}, \underline{M}_{0_i}) = \{\sigma \mid \sigma \in \langle \mathcal{E}(\mathcal{O}^i_{\theta_c}, \underline{M}_{0_i}) \rangle\}$$

Finally let $\mathcal{C}(\mathcal{O}^i_{\theta_c}, \underline{\mathcal{M}}_{0_i})$, $\mathcal{L}(\mathcal{O}^i_{\theta_c}, \underline{\mathcal{M}}_{0_i})$ and $\mathcal{M}(\mathcal{O}^i_{\theta_c}, \underline{\mathcal{M}}_{0_i})$ be respectively the set of all extended configurations, the set of all extended explanations and the set of all estimated present states of the local site i based on the locally received observation $\mathcal{O}_{\theta_c}$ and the set of (minimal) assumptions $\underline{\mathcal{M}}_{0_i}$ on the marking of the input places $\mathcal{P}_{IN_i}$:

$$\mathcal{C}(\mathcal{O}^i_{\theta_c}, \underline{\mathcal{M}}_{0_i}) = \{\mathcal{C}(\mathcal{O}^i_{\theta_c}, \underline{M}_{0_i}) \mid \underline{M}_{0_i} \in \underline{\mathcal{M}}_{0_i}\} \tag{8}$$

$$\mathcal{E}(\mathcal{O}^i_{\theta_c}, \underline{\mathcal{M}}_{0_i}) = \{\phi(\langle \mathcal{E}(\mathcal{O}^i_{\theta_c}, \underline{M}_{0_i}) \rangle) \mid C(\mathcal{O}^i_{\theta_c}, \underline{M}_{0_i}) \in \mathcal{C}(\mathcal{O}^i_{\theta_c}, \underline{\mathcal{M}}_{0_i})\} \tag{9}$$

$$\mathcal{M}(\mathcal{O}^i_{\theta_c}, \underline{\mathcal{M}}_{0_i}) = \{\phi(\mathtt{Max}(C(\mathcal{O}^i_{\theta_c}, \underline{M}_{0_i})) \mid C(\mathcal{O}^i_{\theta_c}, \underline{M}_{0_i}) \in \mathcal{C}(\mathcal{O}^i_{\theta_c}, \underline{\mathcal{M}}_{0_i})\} \tag{10}$$

Then the local preliminary diagnosis $\mathcal{PLD}_i(\mathcal{O}^i_{\theta_c})$ is:

$$\mathcal{PLD}_i(\mathcal{O}^i_{\theta_c}) = \{\tau_{f_i} \mid \tau_{f_i} = \Pi_{\mathcal{T}_{F_i}} \tau_i \wedge \tau_i \in \mathcal{L}(\mathcal{O}^i_{\theta_c}, \underline{\mathcal{M}}_{0_i})\} \tag{11}$$

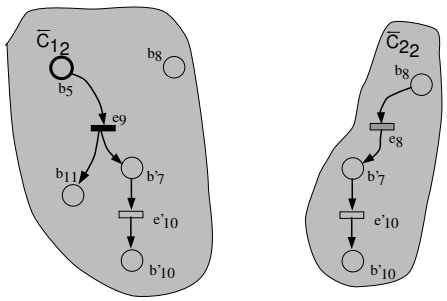

Fig. 6.

Example 3 *Consider the case of Ag_2 having the PN $\mathcal{N}_2$ displayed on right hand side of Fig. 5 and the local observation $\mathcal{O}^2_{\theta_c} = t_{10}$. The reverse unfolding of $\mathcal{O}^2_{\theta_c}$ is displayed in Fig. 6 where $\overleftarrow{U}_2(\mathcal{O}^2_{\theta_c})$ comprises two configurations: $\overleftarrow{\mathcal{C}}_2(\mathcal{O}^2_{\theta_c}) = \left\{\overleftarrow{C}_{1_2}, \overleftarrow{C}_{2_2}\right\}$. Notice that $\overleftarrow{C}_{1_2}$ contains the assumption on the border condition b_5 while $\overleftarrow{C}_{2_2}$ has not any assumption on the border conditions. Then for $MinC_{1_2} \equiv \overleftarrow{C}_{1_2}$ we present in Fig. 7 the forward extensions of $MinC_{1_2}$ where $MinC_{1_2} \sqsubset C_{1_2} \sqsubset C_{2_2}$.*

In the similar way, consider Ag_1 having the PN $\mathcal{N}_1$ showed in left hand side of Fig. 5 and the local observation $\mathcal{O}^1_{\theta_c} = t_6$. $\overleftarrow{U}_1(\mathcal{O}^1_{\theta_c})$ is displayed in Fig. 8. Then for $MinC_{1_1} \equiv \overleftarrow{C}_{1_1}$ we present in Fig. 8 the forward extensions of $MinC_{1_1}$ where $MinC_{1_1} \sqsubset C_{1_1}$.

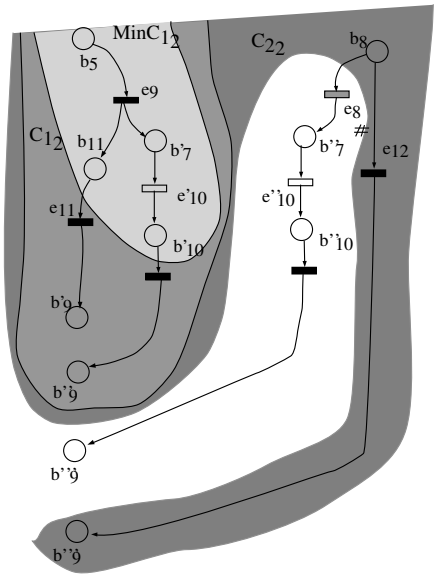

Fig. 7.

7.3 Procedure for information exchange

In what follows we restrict the presentation considering a minimal configuration $MinC_i \in Min\mathcal{C}(\mathcal{O}^i_{\theta_c}, \underline{\mathcal{M}}_{0_i})$.

Thus $MinC_i = (MinB_i, MinE_i, \preceq_i)$ requires the border conditions represented by $MinB_{IN_i}$ ($\phi(MinB_{IN_i}) = \underline{M}_{IN_i}$) must be satisfied. Notice that we have $\forall b_{IN_i} \in MinB_{IN_i} : \exists e^o_i \in MinE_i$ s.t. $\phi(e^o_i) \in \phi^{-1}(\mathcal{O}^i_{\theta_c}) \wedge b_{IN_i} \preceq e^o_i$.

Denote $E^o_i = \{e^o_i \mid e^o_i \in MinE_i \cap \phi(\mathcal{O}_{\theta_c})\}$ the set of nodes of C_i that correspond to the observed events in $\mathcal{O}^i_{\theta_c}$. Given a configuration $C_i \in \mathcal{C}_i(\mathcal{O}^i_{\theta_c}, \underline{M}_{0_i})$ ($MinC_i \sqsubseteq C_i$) denote $Y_i(C_i) = \texttt{Min}(C_i) \cup B_{IN_i} \cup E^o_i \cup B_{OUT_i}$ the set of nodes of C_i that corresponds to either the places marked by M_{0_i} ($\texttt{Min}(C_i)$) or to the input places $p_i \in \mathcal{P}_{IN_i}$ (B_{IN_i}) or to the output places $p_i \in \mathcal{P}_{OUT_i}$ (B_{OUT_i}) or to the observed transitions (E^o_i).

Denote $\Pi_{Y_i} C_i$ the isotone map of C_i onto the set of nodes $Y(C_i)$, $\Pi_{Y_i} C_i : B_i \cup E_i \to Y_i$, that is the projection of one graph onto a subset of nodes by preserving the order relation between the nodes:

$$\forall x_i, y_i \in Y_i, \text{ if } x_i \sim y_i \text{ then } \Pi_{Y_i} x_i \sim \Pi_{Y_i} y_i \text{ where } \sim = \{\preceq, \|\}$$

Denote for simplicity $\Pi_{Y_i} C_i$ by C_{Y_i}. Then C_{Y_i} represent the causality between the input nodes (B_{IN_i}), the output nodes (B_{OUT_i}), the observations (E^o_i), and the local initial marking ($\texttt{Min}(C_i)$).

Then for $b_{IN_i} \in B_{IN_i}$ denote $E^o_i(b_{IN_i}) = \left\{e^o_i \in E^o_i \mid b_{IN_i} \in [(e^o_i)^\uparrow]\right\}$ that is the set of nodes in C_i that correspond to observed events that have b_{IN_i} as a "cause" (predecessor). Then the time b_{IN_i} *"must have been satisfied"* (a token must have entered $\mathcal{N}_i$ via $p_i = \phi(b_{IN_i})$) is:

$$\theta_{b_{IN_i}} \leq \texttt{min}_{e^o_{q_i}} \theta_{t^o_{q_i}} \quad e_{q_i} \in E^o_i(b_{IN_i}) \tag{12}$$

Thus to each border condition b_{IN_i} we can associate a temporal constraint of the form given by Eq. 12. For simplifying the notation denote $b^\theta_{IN_i}$ for $b_{IN_i} \in B_{IN_i}$:

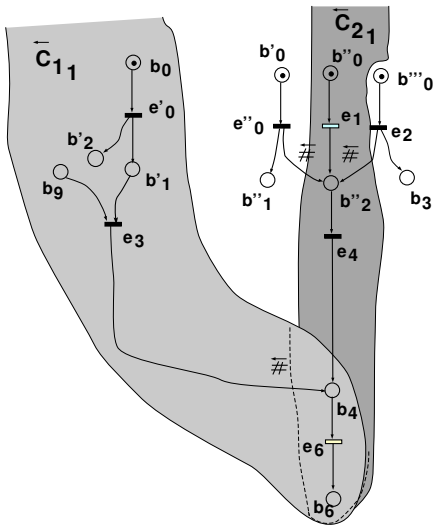

Fig. 8.

Algorithm 3 Preliminary_Local_Calculation (Ag_i considered)

Input: $\mathcal{O}^i_{\theta_c}$
Output: $\mathcal{C}_i(\mathcal{O}^i_{\theta_c}, \underline{\mathcal{M}}_{0_i})$; $\mathcal{PLD}(\mathcal{O}^i_{\theta_c})$
1: $\mathcal{C}_i(\mathcal{O}^i_{\theta_c}, \underline{\mathcal{M}}_{0_i}) = \emptyset$; $\mathcal{L}_i(\mathcal{O}^i_{\theta_c}, \underline{\mathcal{M}}_{0_i}) = \emptyset$
2: B_Unfold($\mathcal{O}^i_{\theta_c}$) {calculate $\overleftarrow{\mathcal{U}}_i(\mathcal{O}^i_{\theta_c})$}
3: calculate $Min\mathcal{C}_i(\mathcal{O}^i_{\theta_c})$
4: **for all** $MinC_i \in Min\mathcal{C}_i(\mathcal{O}^i_{\theta_c})$ **do**
5: calculate $\mathcal{C}_i(\mathcal{O}^i_{\theta_c}, \underline{M}_{0_i})$ {the unobseravble extensions of $MinC_i$}
6: $\mathcal{C}_i(\mathcal{O}^i_{\theta_c}, \underline{\mathcal{M}}_{0_i}) = \mathcal{C}_i(\mathcal{O}^i_{\theta_c}, \underline{\mathcal{M}}_{0_i}) \cup \mathcal{C}_i(\mathcal{O}^i_{\theta_c}, \underline{M}_{0_i})$
7: **end for**
8: **for all** $C_i \in \mathcal{C}_i(\mathcal{O}^i_{\theta_c}, \underline{\mathcal{M}}_{0_i})$ **do**
9: $\mathcal{L}_i(\mathcal{O}^i_{\theta_c}, \underline{\mathcal{M}}_{0_i}) = \mathcal{L}_i(\mathcal{O}^i_{\theta_c}, \underline{\mathcal{M}}_{0_i}) \cup \phi(\langle E_i \rangle)$
10: **end for**
11: $\mathcal{PLD}(\mathcal{O}^i_{\theta_c}) = \Pi_{\mathcal{T}_F} \mathcal{L}_i(\mathcal{O}^i_{\theta_c}, \underline{\mathcal{M}}_{0_i})$

$\theta_{b_{IN_i}} \leq \mathtt{min}_{e^o_{q_i}} \theta_{t^o_{q_i}}$. When omitted, the left resp. the right timing constraints are $0 < \theta$ and $\theta < \infty$ respectively.

Hence the minimal requirement s.t. $MinC_i$ (and any of its unobservable extensions $MinC_i \sqsubseteq C_i$) is allowable can be expressed as a conjunction of temporal conditions on the border places:

$$MinB^{\theta}_{IN_i} = \bigwedge_{b_{IN_i} \in B_{IN_i}} b^{\theta}_{IN_i} \tag{13}$$

Consider now a configuration C_i that unobservably extends $MinC_i$ ($MinC_i \sqsubseteq C_i$). The timing constraints for the output conditions B_{OUT_i} are derived as follows.

First consider the local initial marking M_{0_i} as produced by a transition t_{start} supposed fired at the global time $\theta_{t_{start}} = 0$ when the process starts. Then for each output condition $b_{OUT_i} \in B_{OUT_i}$ let $\theta_{b_{OUT_i}}$ be the time the condition b_{OUT_i} could be satisfied by a token that would leave $\mathcal{N}_i$ via $p_{OUT_i} = \phi(b_{OUT_i})$ where:

$$\theta_{b_{OUT_i}} \geq \mathtt{max}_{x_i} \theta_{x_i} \quad x_i \in [b^{\uparrow}_{OUT_i}] \cap Y_i \tag{14}$$

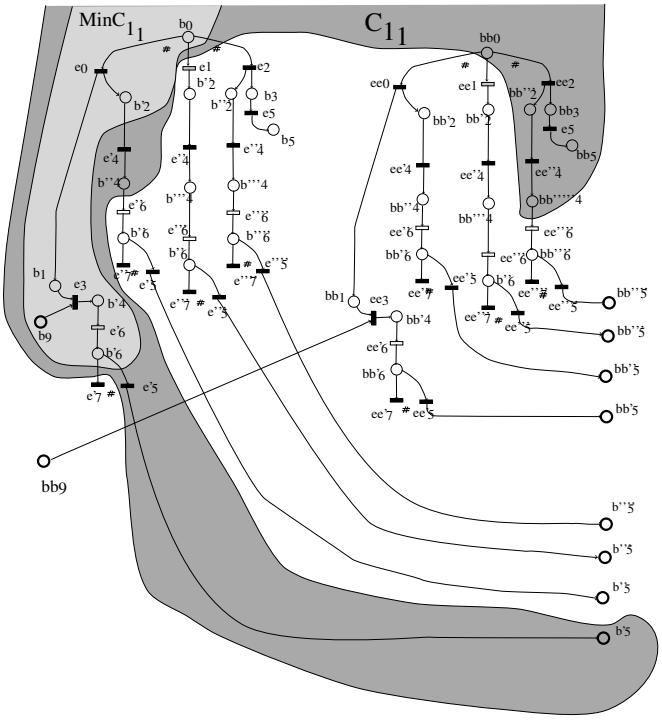

Fig. 9.

Similarly denote the timing constraint given by Eq. 14 by $b^{\theta}_{OUT_i}$. Notice that $\theta^{\theta}_{b_{OUT_i}}$ is the earliest global time a token *could have exited* $\mathcal{N}_i$ given $B^{\theta}_{IN_i}$ satisfied while b_{IN_i} is the latest global time a token *must have entered* $\mathcal{N}_i$.

Then for an unobservable extension C_i of $MinC_i$, the output border-conditions that could have been satisfied is given by the conjunction of constraints having the form:

$$B^{\theta}_{OUT_i} = \bigwedge_{b_{OUT_i} \in B_{OUT_i}} b^{\theta}_{OUT_i} \tag{15}$$

Hence for each minimal configuration $MinC_i \in Min\mathcal{C}(\mathcal{O}^i_{\theta_c}, \underline{\mathcal{M}}_{0_i})$ and for each unobservable extension C_i of $MinC_i$, Ag_i derives $B^{\theta}_{IN_i}$ and $B^{\theta}_{OUT_i}$ (see Eq. 13 and Eq. 15 respectively). Notice that for a configuration C_i s.t. $MinC_i \sqsubseteq C_i$ we have that $MinB^{\theta}_{IN_i} = B^{\theta}_{IN_i}$.

Denote by $\mathcal{B}^{\theta}_{OUT_i}$ the set of output border constraints derived for all the unobservable continuations (extensions) of $MinC_i$:

$$\mathcal{B}^{\theta}_{OUT_i} = \left\{ B^{\theta}_{OUT_i} \mid MinC_i \sqsubseteq C_i \right\}$$

Denote $(\mathcal{B}^{\theta}_{OUT_i}, \trianglelefteq)$ the partial order relation defined as follows:

$$\forall B'^{\theta}_{OUT_i}, B''^{\theta}_{OUT_i} \in \mathcal{B}^{\theta}_{OUT_i} : B'^{\theta}_{OUT_i} \trianglelefteq B''^{\theta}_{OUT_i} \text{ iff } \forall b'^{\theta}_{OUT_i} \in B'^{\theta}_{OUT_i},\ b'^{\theta}_{OUT_i} \in B''^{\theta}_{OUT_i}$$

Denote $\texttt{Max}_{\trianglelefteq}(\mathcal{B}^{\theta}_{OUT_i})$ the maximal elements of $\mathcal{B}^{\theta}_{OUT_i}$ w.r.t. $\trianglelefteq$. Then the minimal information that Ag_i should send to its neighboring agents is:

$$\mathcal{MSG}_i = \left\{ (MinB^{\theta}_{IN_i}, B^{\theta}_{OUT_i}) \mid MinC_i \in \mathcal{M}(\mathcal{O}^i_{\theta_c}, \underline{\mathcal{M}}_{0_i}) \wedge B^{\theta}_{OUT_i} \in \texttt{Max}_{\trianglelefteq}(\mathcal{B}^{\theta}_{OUT_i}) \right\} \tag{16}$$

Since a local agent does not know the models of the neighboring agents but only the set of input and output places $(\mathcal{P}_{IN_i}, \mathcal{P}_{OUT_i})$ the message that is sent by Ag_i to its neighbor Ag_j comprises only information about their common border-places $\mathcal{P}_{ij} = \mathcal{P}_{IN_{ij}} \cup \mathcal{P}_{OUT_{ij}}$:

$$\mathcal{MSG}_{i\to j} = \left\{ (MinB^{\theta}_{IN_{ij}}, B^{\theta}_{OUT_{ij}}) \mid MinC_i \in \mathcal{M}(\mathcal{O}^i_{\theta_c}, \underline{\mathcal{M}}_{0_i}) \wedge B^{\theta}_{OUT_i} \in \mathtt{Max}_{\trianglelefteq}(\mathcal{B}^{\theta}_{OUT_i}) \right\} \tag{17}$$

where

$$MinB^{\theta}_{IN_{ij}} = \bigwedge_{b_{IN_{ij}} \in B_{IN_{ij}}} b^{\theta}_{IN_{ij}} \quad \text{and} \quad B^{\theta}_{OUT_{ij}} = \bigwedge_{b_{OUT_{ij}} \in B^{\theta}_{OUT_{ij}}} b^{\theta}_{OUT_{ij}} \tag{18}$$

Remark 4 *The reason Ag_i selects only the maximal elements of $\mathcal{B}^{\theta}_{OUT_i}$ to send them to its neighbors is as follows. The minimal requirement $MinB^{\theta}_{IN_i}$ is common to all the unobservable continuations of $MinC_i$ thus if $MinB^{\theta}_{IN_i}$ will not be satisfied then all the configuration that are extensions of $MinC_i$ can be discarded. Otherwise if $MinB^{\theta}_{IN_i}$ can be satisfied there is enough to send to neighbors only the maximal (w.r.t. $\trianglelefteq$) border conditions. This is because if what can be maximally provided $B^{\theta}_{OUT_i} \in \mathtt{Max}_{\trianglelefteq}(\mathcal{B}^{\theta}_{OUT_i})$ is enough for satisfying the minimal requirement $MinB^{\theta}_{IN_{ji}}$ derived by Ag_i for $MinC_j$ then Ag_i and Ag_j will know that providing less but more than the minimal requirement leads to consistent pairs whereas if the minimal requirement is not less that a maximal element of $\mathtt{Max}_{\trianglelefteq}(\mathcal{B}^{\theta}_{OUT_i})$ than it is obvious that would have been useless to send information about the rest of the non-maximal elements of $\mathcal{B}^{\theta}_{OUT_i}$.*

Algorithm 4 Communication_exchange (Ag_i considered)

Input: $\mathcal{C}_i(\mathcal{O}^i_{\theta_c}, \underline{\mathcal{M}}_{0_i})$
Output: $\mathcal{MSG}_i$; $\mathcal{MSG}_{i\to j}$
1: **for all** $C_i \in \mathcal{C}_i$ **do**
2: calculate C^{θ}_i
3: calculate $B^{\theta}_{IN_i}$ {see Eq. 13}
4: calculate $\mathcal{B}^{\theta}_{OUT_i}$ {see Eq. 14}
5: calculate $\mathtt{Max}_{\trianglelefteq}(B^{\theta}_{OUT_i})$
6: **end for**
7: calculate $\mathcal{MSG}_i$ {see Eq. 16}
8: **for all** neighboring agents Ag_j **do**
9: calculate $\mathcal{MSG}_{i\to j}$ {see Eq. 17}
10: **end for**

Example 4 *Consider again the case of Ag_2 observing $\mathcal{O}^2_{\theta_c} = t_{10}$. In Fig.7 we have that $MinC_{1_2} \sqsubseteq C_{1_2} \sqsubseteq C_{2_2}$. Then for C_{2_2} we have that $B_{IN_2} = \{b^{\theta}_5\}$ with $\theta_{b_5} \leq \theta_{e_{10}}$ and $B_{OUT_2} = \{b'^{\theta}_9, b''^{\theta}_9, b'''^{\theta}_9\}$ with $\theta_{b'_9} \geq \theta_{b_5}$, $\theta_{b''_9} \geq \theta_{e_{10}}$ and $\theta_{b'''_9} \geq \theta_{start}$. Thus (B_{IN_2}, B_{OUT_2}) is part of the message that will be sent to Ag_1.*

7.4 Procedure for updating a local calculation

Consider in this section that having received the local observation $\mathcal{O}^i_{\theta_c}$ the agent Ag_i has derived the preliminary local calculation of local site model $\mathcal{N}_i$ $(\underline{\mathcal{M}}_{IN_i}, Min\mathcal{C}(\mathcal{O}^i_{\theta_c}, \underline{\mathcal{M}}_{0_i}), \mathcal{C}(\mathcal{O}^i_{\theta_c}, \underline{\mathcal{M}}_{0_i}))$ and then has received the message $\mathcal{MSG}_{j\to i}$ sent by Ag_j based on a similar preliminary computation of site j.

In this section we present how Ag_i updates its preliminary local calculation by taking into account the received information $\mathcal{MSG}_{j\to i}$. To simplify the presentation consider:

1. an arbitrary minimal configuration $MinC_i \in Min\mathcal{C}(\mathcal{O}^i_{\theta_c}, \underline{\mathcal{M}}_{0_i})$,
2. the set of unobservable continuations (extensions) $\mathcal{C}_i$ of $MinC_i$
3. an arbitrary minimal configuration $MinC_j \in Min\mathcal{C}(\mathcal{O}^j_{\theta_c}, \underline{\mathcal{M}}_{0_j})$,
4. the set of unobservable continuations (extensions) $\mathcal{C}_j$ of $MinC_j$
5. and the information $\mathcal{MSG}'_{j\to i} \subseteq \mathcal{MSG}_{j\to i}$ that is received by Ag_i regarding $MinC_j$ and $\mathcal{C}_j$ ($\mathcal{MSG}'_{j\to i} = \left\{(B_{IN_{ji}}, B_{OUT_{ji}}) \mid B_{OUT_{ji}} \in \mathtt{Max}_{\trianglelefteq}(\mathcal{B}_{OUT_{ji}})\right\}$)

Thus in what follows we present how Ag_i processes $\mathcal{MSG}'_{j\to i}$ for updating $MinC_i$ and $\mathcal{C}_i$. Since the elements of $\mathcal{MSG}'_{j\to i}$ are distinct we present in following the update Ag_i makes, considering only $(B^\theta_{IN_{ji}}, B^\theta_{OUT_{ji}}) \in \mathcal{MSG}'_{j\to i}$.

Notice that $MinC_i$ and $\mathcal{C}_i$ require $B^\theta_{IN_{ij}}$ to be satisfied providing then $\mathcal{B}^\theta_{OUT_{ij}}$ while $\mathcal{B}^\theta_{OUT_{ji}}$ is the set of border-conditions that may be satisfied whenever $B^\theta_{IN_{ji}}$ is satisfied.

Since $MinC_i$ and its unobservable extensions $\mathcal{C}_i$ depend on the set of hypothesis $B^\theta_{IN_{ij}}$ that should be satisfied it means that Ag_i *interprets* the local results by considering the information sent by Ag_j.

Let $(B^\theta_{IN_{ji}}, B^\theta_{OUT_{ji}}) \in \mathcal{MSG}'_{j\to i}$. Then we have for the border places $\mathcal{P}_{IN_{ij}} = \mathcal{P}_{OUT_{ji}}$ the set of border-conditions $B^\theta_{OUT_{ji}}$ that provides the set of possible conditions that could have been satisfied and $B^\theta_{IN_{ij}}$ expressing conditions that must be satisfied. Similarly for the border places $\mathcal{P}_{OUT_{ij}} = \mathcal{P}_{IN_{ji}}$ we have that $B^\theta_{IN_{ji}}$ expresses the set of conditions that must be satisfied and $B^\theta_{OUT_{ij}}$ the set conditions that could have been satisfied.

Definition 24 *Define the interpretation function $\psi_i : B^\theta_{IN_{ij}} \to B^\theta_{OUT_{ji}} \cup \{\varepsilon\}$ where:*

$$\psi_i(b^\theta_{IN_{ji}}) = \begin{cases} b^\theta_{OUT_{ij}} \in B^\theta_{OUT_{ji}} & \text{if } \theta_{b_{OUT_{ji}}} \leq \theta_{b_{IN_{ij}}} \\ \text{or } \varepsilon \end{cases} \tag{19}$$

and for $b_{IN_{ji}} \neq b'_{IN_{ji}}$, $\psi_i(b_{IN_{ji}}) = \psi_i(b'_{IN_{ji}}) \Rightarrow \psi(b_{IN_{ji}}) = \varepsilon$. Similarly define $\psi_j : B_{IN_{ji}} \to B_{OUT_{ij}} \cup \{\varepsilon\}$. Then denote by $\psi_{ij} = (\psi_i, \psi_j)$ the interpretation function of the common place marking and by Ψ_{ij} the entire set of interpretation functions.

Denote $B^{a,\psi_i}_{IN_{ij}}$ the set of input border conditions that were assigned to conditions $b^\theta_{OUT_{ji}} \in B^\theta_{OUT_{ji}}$:

$$B^{a,\psi_i}_{IN_{ij}} = \left\{ b^{a,\psi_i}_{IN_{ij}} = b^\theta_{IN_{ij}} \wedge b^\theta_{OUT_{ji}} \mid \psi_i(b^\theta_{IN_{ij}}) = b^\theta_{OUT_{ji}} \right\}$$

Then denote by $B^{ua,\psi_i}_{IN_{ji}}$ the set of input border conditions that were not-assigned to determined conditions:

$$B^{ua,\psi_i}_{IN_{ij}} = \left\{ b^{ua,\psi_i}_{IN_{ij}} = b^\theta_{IN_{ij}} \mid \psi_i(b^\theta_{IN_{ij}}) = \varepsilon \right\}$$

and denote by $B^{new,\psi_i}_{IN_{ji}}$ the set of new input border conditions that can be provided by site j under the interpretation ψ_i

$$B^{new,\psi_i}_{IN_{ij}} = \left\{ b^{new,\psi_i}_{OUT_{ji}} = b^\theta_{OUT_{ji}} \mid b^\theta_{OUT_{ji}} \in B^\theta_{OUT_{ji}} \setminus \psi_i^{-1}(B^a_{IN_{ji}}) \right\}$$

Then denote $B^{\psi_i}_{IN_{ij}}$ the set of input conditions under the interpretation ψ_i where:

$$B^{\psi_i}_{IN_{ij}} = B^{a,\psi_i}_{IN_{ij}} \cup B^{ua,\psi_i}_{IN_{ij}} \cup B^{new,\psi_i}_{IN_{ij}} \tag{20}$$

Definition 25 *Consider an input-border condition* $b_{IN_i}^{\theta,\psi_i} \in B_{IN_{ij}}^{\psi_i}$ *under the assignment* $\psi_{ij} = (\psi_i, \psi_j)$,$\psi_{ij} \in \Psi_{ij}$. *Then we say that:*

- $b_{IN_{ij}}^{\psi_i}$ *is matched iff all the limits of ist timing constraints are determined (i.e. are positive constants* $ct \in \mathbb{R}^+$, 0 *or* $+\infty$*)*
- *otherwise* $b_{IN_{ij}}^{\psi_i}$ *is not matched*

Then let $B_{IN_{ij}}^{\psi_i}$ be partitioned as $B_{IN_{ij}}^{\psi_i} = B_{IN_{ij}}^{m,\psi_i} \cup B_{IN_{ij}}^{nm,\psi_i}$ where $B_{IN_{ij}}^{m,\psi_i}$ is the set of matched input border conditions and $B_{IN_{ij}}^{nm,\psi_i}$ is the set of not-matched input-border conditions.

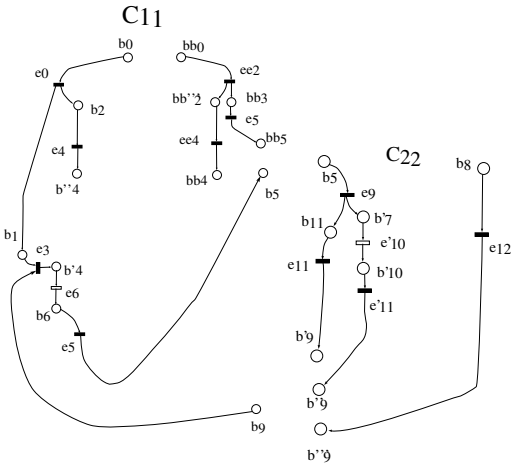

Fig. 10.

Example 5 *Consider two configurations* C_{1_1} *and* C_{2_2}. *As presented in Example 4 the message sent by* Ag_2 *to* Ag_1 *regarding* C_{2_2} *is* (B_{IN_2}, B_{OUT_2}). *Now having observed* $\mathcal{O}_{\theta_c}^1 = t_6$, Ag_1 *has preliminary derived for* C_{1_1}, $B_{IN_1} = \left\{b_{9_1}^{\theta}\right\}$ *with* $\theta_{b_{9_1}} \leq \theta_{e_6}$ *and* $B_{OUT_1} = \left\{b_{5_1}^{\theta}, bb_{5_1}^{\theta}\right\}$ *with* $\theta_{b_{5_1}} \geq \theta_{e_6}$ *and* $\theta_{bb_{5_1}} \geq \theta_{start}$. *Recall that for* C_{2_2} *we have* $B_{IN_2} = \left\{b_{5_2}^{\theta}\right\}$ *with* $\theta_{b_{5_2}} \leq \theta_{e_{10}}$ *and* $B_{OUT_2} = \left\{b_{9_2}^{\prime\theta}, b_{9_2}^{\prime\prime\theta}, b_{9_2}^{\prime\prime\prime\theta}\right\}$ *with* $\theta_{b'_{9_2}} \geq \theta_{b_{5_2}}$, $\theta_{b''_{9_2}} \geq \theta_{e_{10}}$ *and* $\theta_{b'''_{9_2}} \geq \theta_{start}$.

The we have the following interpretation functions $\psi_1^k : B_{IN_1} \rightarrow B_{OUT_2}$ *and* $\psi_2^k : B_{IN_2} \rightarrow B_{OUT_1}$ $(k = 1, 2, \ldots)$.

$$\psi_{12}^1 = \begin{cases} bb_{5_1}^{\theta} \xrightarrow{\psi_2^1} b_{5_2}^{a} & \theta_{start} \leq \theta_{b_{5_2}^a} \leq \theta_{e_{10}} \\ b_{5_1}^{\theta} \xrightarrow{\psi_2^1} b_{5_2}^{new} & \theta_{e_6} \leq \theta_{b_{5_2}^{new}} \\ b_{9_2}^{\prime\theta} \xrightarrow{\psi_1^1} b_{9_1}^{a} & \theta_{b_{5_2}^a} \leq \theta_{b_{9_1}^a} \leq \theta_{e_6} \\ b_{9_2}^{\prime\prime\theta} \xrightarrow{\psi_1^1} b_{9_1}^{\prime new} & \theta_{e_{10}} \leq \theta_{b_{9_1}^{\prime new}} \\ b_{9_2}^{\prime\prime\prime\theta} \xrightarrow{\psi_1^1} b_{9_2}^{\prime\prime new} & \theta_{start} \leq \theta_{b_{9_1}^{\prime new}} \end{cases} \tag{21}$$

$$\psi_{12}^2 = \begin{cases} b_{5_2} \xrightarrow{\psi_2^1} b_{5_2}^{ua} & \theta_{b_{5_2}^a} \leq \theta_{e_{10}} \\ bb_{5_1}^{\theta} \xrightarrow{\psi_2^2} bb_{5_2}^{new} & \theta_{start} \leq \theta_{b_{5_2}^{new}} \leq \theta_{e_{10}} \\ b_{5_1}^{\theta} \xrightarrow{\psi_2^2} b_{5_2}^{new} & \theta_{e_6} \leq \theta_{b_{5_2}^{new}} \\ b_{9_2}'^{\theta} c \xrightarrow{\psi_1^2} b_{9_1}'^{new} & \theta_{b_{5_2}^{ua}} \leq \theta_{b_{9_1}'^{new}} \\ b_{9_2}''^{\theta} \xrightarrow{\psi_1^2} b_{9_1}''^{new} & \theta_{e_{10}} \leq \theta_{b_{9_1}''^{new}} \\ b_{9_2}'''^{\theta} \xrightarrow{\psi_1^2} b_{9_2}^{a} & \theta_{start} \leq \theta_{b_{9_1}^a} \leq \theta_{e_6} \end{cases} \tag{22}$$

and so on. Notice that $(C_{1_1}, C_{2_2}, \psi_1^1)$*, is consistent while* $(C_{1_1}, C_{2_2}, \psi_1^2)$ *it is not. This is because the border condition* $bb_{5_1}^{\theta}$ *is not used for satisfying* $b_{5_2}^{\theta}$ *(*$b_{5_2}^{\theta}$ *remains unassigned) but is assumed that has entered as a new condition (token). We need to consider this since in general because of the unobservable loops the new entered conditions may produce new output-border conditions and so on. Notice that in* ψ_{12}^1 *by assigning* $bb_{5_1}^{\theta} \xrightarrow{\psi_2^1} b_{5_2}^{\theta}$ *and* $b_{9_2}'^{\theta} \xrightarrow{\psi_1^1} b_{9_1}^{\theta}$ *cyclic unobservable interactions are determined.*

Definition 26 *Given* C_i*,* C_j *and an interpretation function* $\psi_{ij} = (\psi_i, \psi_j)$,$\psi_{ij} \in \Psi_{ij}$ *then* $(C_i(\psi_{ij}), C_j(\psi_{ij}))$ *are locally consistent if* $B_{IN_{ij}}^{nm,\psi_i} = \emptyset$ *and* $B_{IN_{ji}}^{nm,\psi_j} = \emptyset$*.*

Definition 27 *Given a tuple* $C_1, \ldots, C_{|I|}$ *of local configurations then* $(C_1, \ldots, C_{|I|})$ *is globally consistent if* $\forall i, j \in I$*,* $i \neq j$ *there is an interpretation function* ψ_{ij}*, s.t. any pair* $(C_i(\psi_{ij}), C_j(\psi_{ij}))$ *is locally consistent.*

Definition 28 *Given* C_i*,* C_j *and an interpretation function* ψ_{ij}*, if either* $B_{IN_{ij}}^{new,\psi_i} \neq \emptyset$ *or* $B_{IN_{ji}}^{new,\psi_j} \neq \emptyset$ *then* $(C_i(\psi_{ij}), C_j(\psi_{ij}))$ *is extendable.*

The interpretation of C_i under the assignment ψ_{ij} $(C_i(\psi_{ij}))$ contains new temporal information (because of the input border that were assigned) that updates the temporal information for the output border-conditions. Moreover the set of new input-border conditions $B_{IN_{ij}}^{new}$ represents the new tokens that could have entered $\mathcal{N}_i$. Obviously $C_i(\psi_{ij})$ can be updated by considering all the new extensions (unobservable continuations) that become possible with these new tokens.

Denote by $\mathcal{C}_i(\psi_{ij})$ the set of configurations that can be obtained from C_i considering the interpretation function ψ_{ij} and all its maximal unobservable extensions. The let $\Delta(C_i(\psi_{ij})) = \mathcal{C}_i(\psi_{ij}) \setminus C_i$ the local update of C_i.

Similarly with what has been presented above Ag_i derives first the local update $\Delta(\mathcal{C}_i(\mathcal{O}_{\theta_c}^i, \underline{\mathcal{M}}_{0_i}, \mathcal{MSG}_{j \to i})$ of the local calculation $\mathcal{C}_i(\mathcal{O}_{\theta_c}^i, \underline{\mathcal{M}}_{0_i})$ given the received message $\mathcal{MSG}_{j \to i}$ (*Update_Local_Calculation* bellow). Then based on the local update $\Delta(\mathcal{C}_i(\mathcal{O}_{\theta_c}^i), \underline{\mathcal{M}}_{0_i}, \mathcal{MSG}_{j \to i})$ Ag_i derives the update of the information to be exchanged $\Delta(\mathcal{MSG}_i)$.

8 The main result

In this section we start first considering the case of two agents and then we generalize our results to an arbitrary number of agents.

Consider the following distributed diagnosis algorithm presented for the case of only two agents: Ag_i and Ag_j (see Algorithm 8).

Algorithm 5 Update_Local_Calculation (Ag_i considered)

Input: $\mathcal{C}_i(\mathcal{O}^i_{\theta_c}, \underline{\mathcal{M}}_{0_i})$; $\mathcal{MSG}_{j\to i}$
Output: $\Delta(\mathcal{C}_i(\mathcal{O}^i_{\theta_c}, \underline{\mathcal{M}}_{0_i}), \mathcal{MSG}_{j\to i})$
1: $\Delta(\mathcal{C}_i(\mathcal{O}^i_{\theta_c}, \underline{\mathcal{M}}_{0_i}), \mathcal{MSG}_{j\to i}) = \emptyset$
2: $\mathcal{C}_i^{gcon}(\mathcal{O}^i_{\theta_c}, \underline{\mathcal{M}}_{0_i}) = \emptyset$
3: **for all** $C_i \in \mathcal{C}_i(\mathcal{O}^i_{\theta_c}, \underline{\mathcal{M}}_{0_i})$ **do**
4: **for all** $(B_{IN_{ji}}, B_{OUT_{ji}}) \in \mathcal{MSG}_{j\to i}$ **do**
5: **for all** $\psi_{ij} \in \Psi_{ij}$ **do**
6: **if** (C_i, C_j, ψ_{ij}) - globally consistent **then**
7: $\mathcal{C}_i^{gcon}(\mathcal{O}^i_{\theta_c}, \underline{\mathcal{M}}_{0_i}) = \mathcal{C}_i^{gcon}(\mathcal{O}^i_{\theta_c}, \underline{\mathcal{M}}_{0_i}) \cup ((\ldots, C_i(\psi_{ij}), \ldots, C_j(\psi_{ij}), \ldots)$
8: **else if** $(C_i\psi_{ij}, C_j\psi_{ij})$ - extendable **then**
9: calculate $\Delta(C_i(\psi_{ij}))$ {extend $C_i^{\psi_{ij}} \in \Delta(C_i(\psi_{ij}))$ by using $B^{new,\psi_i}_{IN_{ij}} \neq \emptyset$}
10: $\Delta(\mathcal{C}_i(\mathcal{O}^i_{\theta_c}, \underline{\mathcal{M}}_{0_i}), \mathcal{MSG}_{j\to i}) = \Delta(\mathcal{C}_i(\mathcal{O}^i_{\theta_c}, \underline{\mathcal{M}}_{0_i}), \mathcal{MSG}_{j\to i}) \cup \Delta(C_i(\psi_{ij}))$
11: **end if**
12: **end for**
13: **end for**
14: **end for**
15: **for all** $C_i \in \Delta(\mathcal{C}_i(\mathcal{O}^i_{\theta_c}, \underline{\mathcal{M}}_{0_i}))$ **do**
16: $\Delta\mathcal{L}_i(\mathcal{O}^i_{\theta_c}, \underline{\mathcal{M}}_{0_i}) = \mathcal{L}_i(\mathcal{O}^i_{\theta_c}, \underline{\mathcal{M}}_{0_i}) \cup \phi(\langle E_i \rangle)$
17: **if** C_i globally consisted **then**
18: $\Delta\mathcal{L}_i^{gcon}(\mathcal{O}^i_{\theta_c}) = \Delta\mathcal{L}_i^{gcon}(\mathcal{O}^i_{\theta_c}) \cup \Delta\mathcal{L}_i(\mathcal{O}^i_{\theta_c}, \underline{\mathcal{M}}_{0_i})$
19: **end if**
20: **end for**
21: $\mathcal{PLD}_i(\mathcal{O}^i_{\theta_c}) = \mathcal{PLD}_i(\mathcal{O}^i_{\theta_c}) \cup \Pi_{\mathcal{T}_F}(\Delta\mathcal{L}_i(\mathcal{O}^i_{\theta_c}, \underline{\mathcal{M}}_{0_i}))$
22: $\mathcal{PLD}_i^{gcon}(\mathcal{O}^i_{\theta_c}) = \mathcal{PLD}_i^{gcon}(\mathcal{O}^i_{\theta_c}) \cup \Pi_{\mathcal{T}_F}(\Delta\mathcal{L}_i^{gcon}(\mathcal{O}^i_{\theta_c}, \underline{\mathcal{M}}_{0_i}))$

Now for $p_0 \in \mathcal{P}_{ij}$ denote by $c^i_\wp$ and $c^j_\wp$ how many times an unobservable oriented path $\wp$ that starts in p_0 crosses $\mathcal{P}_i \setminus \mathcal{P}_{ij}$ and $\mathcal{P}_j \setminus \mathcal{P}_{ij}$ respectively. Let $c_\wp = max(c^i_\wp, c^j_\wp)$ and denote $K_c = Max_{\wp\in\mathcal{N}}(c_\wp)$ ($\mathcal{N} = \mathcal{N}_i \cup \mathcal{N}_j$). If $\exists \wp \in \mathcal{N}_{ij}$ s.t. $\wp$ is an *uec* then $K_c = \infty$ otherwise K_c is finite.

Theorem 1 *Consider a distributed description of the plant comprising two local sites and two local agents and an arbitrary distributed observation $\mathcal{O}_{\theta_c} = \mathcal{O}^i_{\theta_c} \otimes^{gc} \mathcal{O}^j_{\theta_c}$. Then the global consistent local diagnosis $\mathcal{PLD}_i^{gcon}$ derived by the d-agent Ag_i at the time θ_c after the k^{th} communication round by running the algorithm* DD_Algo_2 *is such that:*

i) if K_c is finite then after $k \geq K_c$ communication rounds, the consistent local diagnosis result $\mathcal{PLD}_i^{gcon}(\mathcal{O}^i_{\theta_c})$ recovers the centralized diagnosis result of site i: $\mathcal{PLD}_i^{gcon}(\mathcal{O}^i_{\theta_c}) = \mathcal{D}_i(\mathcal{O}_{\theta_c})$
ii) if K_c is infinite then $\exists\ k_{max} \in \mathbb{N}^+$ finite s.t. after $k \geq k_{\max}$ communication rounds $\mathcal{PLD}_i^{gcon}(\mathcal{O}^i_{\theta_c}) = \mathcal{D}_i(\mathcal{O}_{\theta_c})$ where k_{max} depends on both the PN topology and the initial marking M_0.

Proof. The proof of *i*) and *ii*) is similar and comprises the following steps. First we proof that the computation of $\mathcal{PLD}_i^{gcon}(\mathcal{O}^i_{\theta_c})$ is sound. Then we show that the computation achieves a fix point (terminates) after finitely many communication rounds. Finally we prove that at the time the fixed point is achieved the diagnosis based on the set of global consistent traces is the diagnosis that a centralized agent would have computed for the local site i resp. j.

First the computation of the global consistent configurations is sound by Def. 27 and by algorithm construction. Then the proof that *DD_Algo* terminates after finitely many communication rounds relies on the assumption that the PN

Algorithm 6 DD_Algo_2 for two agents: Ag_i,Ag_j (Ag_i considered)

Input: Ag_j
Output: $(\mathcal{C}_i^{gcon}(\mathcal{O}^i_{\theta_c}, \underline{\mathcal{M}}_{0_i})$

```
1: Preliminary_Local_Calculation(N_i; O^i_{θ_c})
2: Communication_exchange(C_i(O^i_{θ_c}, M_{0_i})
3: repeat
4:    send MSG_{i→j}
5:    receive MSG_{j→i}
6:    Update_Local_Calculation(C_i(O^i_{θ_c}, M_{0_i}); MSG_{j→i})
7:    Communication_exchange(Δ(C_i(O^i_{θ_c}, M_{0_i}, MSG_{j→i}))){Update_Message}
8:    if Δ(MSG_{i→j}) = ∅ then
9:       MSG_{j→i} = stop
10:   else
11:      MSG_{j→i} = Δ(MSG_{i→j})
12:   end if
13: until MSG_{j→i} = stop
```

models are structurally bounded (see *viii*) in setting). It means that $\mathcal{L}_{\mathcal{N}}(M_0 \uplus_{i\in I} \underline{M}_{IN_i})$ is finite and is recovered by Ag_i and Ag_j by distributed calculations. Then since $\mathcal{L}_{\mathcal{N}}(M_0) \subseteq \mathcal{L}_{\mathcal{N}}(M_0 \uplus_{i\in I} \underline{M}_{IN_i})$ it results that for any observation $\mathcal{O}_{\theta_c}$ we have $\mathcal{L}_{\mathcal{N}}(M_0, \mathcal{O}_{\theta_c}) \subseteq \mathcal{L}_{\mathcal{N}}(M_0 \uplus_{i\in I} \underline{M}_{IN_i}, \mathcal{O}_{\theta_c})$. Then we have that $\Pi_{\mathcal{T}_i}\mathcal{L}_{\mathcal{N}}(\mathcal{O}_{\theta_c}) \subseteq \mathcal{L}_i^{gcon}(\mathcal{O}^i_{\theta_c})$ while $\mathcal{L}_i^{gcon}(\mathcal{O}^i_{\theta_c}) \subseteq \Pi_{\mathcal{T}_i}\mathcal{L}_{\mathcal{N}}(\mathcal{O}_{\theta_c})$ is trivial. The result is proved straightforward by projecting equal set onto the local set of faulty transitions $\mathcal{T}_{F_i}$.

Then for *i*) the proof that *DD_Algo* terminates in $k \leq K_c$ is simple since K_c denotes how many times a token can cross unobservable the border. For *ii*) we have that $K_c = \infty$ that implies that there is an loop (*uec*) that comprises places and only unobservable transitions in both $\mathcal{N}_i$ and $\mathcal{N}_j$. In this case the maximum number of communication rounds however finite does not depend only on the net structure but on both the net structure and the initial marking. □

Now consider the of more than two agents ($\mid I \mid > 2$). By Theorem 1 we have that two neighboring agents Ag_i, Ag_j achieve local consistency after finitely communication rounds. Without affecting the generality we assume in the following a communication protocol s.t. when two neighboring agents communicate they do not initiate communication with another agent until they have become locally consistent. Moreover we require that the information exchange is *fair* [3] i.e. any local agent is disallowed to communicate infinitely often with some neighbors ignoring to communicate with some other neighboring agents. This is implemented in *DD_Algo* bellow by counting the number of communication rounds between each two agents $n_{com}(i,j)$. Then Ag_i must maintain for its neighboring agents the difference between the most accessed agent (e.g. Ag_{j_1}) and the less accessed agent (Ag_{j_2}) lower than a certain threshold (e.g. N_{com}): $n_{com}(i,j_1) - n_{com}(i,j_2) \leq N_{com}$.

Theorem 2 *Consider a distributed description of the plant and an arbitrary distributed observation* $\mathcal{O}_{\theta_c} = \otimes_{i\in I}^{gc}\mathcal{O}^i_{\theta_c}$ *the algorithm* DD_Algo *terminates in finite time and the local diagnosis* $\mathcal{PLD}_i^{gcon}$ *(*$i \in I$*) derived by each local d-agent* Ag_i *(*$i \in I$*) is the diagnosis a centralized agent would have obtained for the local site i having the entire plant observation* $\mathcal{O}_{\theta_c}$ *and the knowledge of the overall plant.*

$$\forall i \in I, \quad \mathcal{D}_i(\mathcal{O}^i_{\theta_c}) = \mathcal{PLD}_i^{gcon}(\mathcal{O}^i_{\theta_c})$$

Proof. The proof is similar with the proof of Theorem 1 and it relies on structurally boundness assumption see *viii*) that implies that $\mathcal{L}_{\mathcal{N}}(M_0 \uplus_{i\in I} \underline{M}_{IN_i})$ is finite. Thus the algorithm terminates after a finite number of communication rounds.

Algorithm 7 DD_Algo (Ag_i considered)

Input: $\mathcal{N}_i; M_{0_i}; \mathcal{O}^i_{\theta_c}$
Output: $\mathcal{D}_i(\mathcal{O}^i_{\theta_c})$

for all neighbor Ag_j **do**
  $n_{com}(i,j) = 0$ {initialize communication counter}
end for
while global_stop=true **do**
  if $\mathcal{MSG}_i = \emptyset$ **then**
    local_stop=true
  else if $\mathcal{MSG}_i \neq \emptyset$ **then**
    choose a neighbor Ag_j s.t. $\forall j_1, j_2 : \mid n_{com}(i,j_1) - n_{com}(i,j_2) \mid \leq N_{com}$
    $n_{com}(i,j) = n_{com}(i,j) + 1$
    $DD\_Algo(Ag_j)$
  end if
end while
$\mathcal{D}_i(\mathcal{O}^i_{\theta_c}) = \mathcal{PLD}_i^{gcon}(\mathcal{O}^i_{\theta_c})$

Before concluding the paper we discuss the assumptions made along the paper. Assumption 1 that states that the observation is deterministic is not strong and can be dropped. The amount of computation increases and this is because the backward search will start from different final markings M_{fin} that corresponds to the marking of the input places of the transitions whose shared label was received. This increase in the amount of calculations can be intuitively interpreted as the increase that would be obtained for a forward search when the initial state is given by a set of initial markings. Then Assumption 3 can also be dropped. For the case of communication delays and unordered local observations the reader is referred to [3],[7]. The only *strict* assumptions made are that the PN model is structurally-bounded w.r.t. the unobservable behavior (item *viii*) in setting) and Assumption 5. These assumptions are made in order to avoid to work with ω-markings.

9 Conclusions

This research is motivated by our interest in designing distributed algorithms for large and complex systems where (e.g. because of sensors failure) unobservable inputs are sent/received between components placed in different sites. We have shown that by backward and forward search an by timing constraints propagation the centralized diagnosis result can be recovered after finitely many communication rounds. For increasing the efficiency of the local calculations we have used reachability methods based on unfoldings (backward and forward unfolding). Further directions are the extension of this method (for reasonable models where $K_c \leq 2$) to time PN models and probabilistic analysis.

Acknowledgment: This research was partially supported by the IAP Program, initiated by the Belgian Federal Science Policy Office. G. Jiroveanu is partially supported by a BOF project of Ghent University on Optimal Supervisory Control of Hybrid Systems. The scientific responsibility rests with its authors.

References

1. P.A. Abdulla, S.P. Iyer and A. Nylen On Unfolding unbounded Petri Nets *Proceedings of Computer Aid Verification*, LNCS, vol.1855, 2000
2. P.Baroni, G.Lamperti and et.al. Diagnosis of large active systems. *Artificial Intelligence*, 110(1):135–183, 1999.

3. A. Benvensite, E. Fabre et al. Diagnosis of asynchronous Discrete Event Systems, a net unfolding approach - *IEEE Transactions on Automatic Control*,48(5), 2003
4. R. K. Boel and G. Jiroveanu Distributed Contextual Diagnosis for very large systems - *WODES*, Reims, France, 2004
5. R. K. Boel and G. Jiroveanu Petri Nets Model-Based Fault Section Detection and Diagnosis System in Electrical Power Networks 6^{th} *IPEC Conference*, Singapore, 2003
6. A. Ciampolini, P. Mello and S. Storari Distributed Medical Diagnosis with abductive logic agents - *ECAI*, Lyon, France, 2002
7. R. Debouk, S. Lafortune and D. Teneketzis Coordinated Decentralized Protocols for Failure Diagnosis of Discrete Event Systems *Journal of Discrete Event Dynamic Systems*, January,2000
8. G. Delzanno, J-F. Raskin, L. van Begin Covering Sharing Trees: A compact data structure for parameterized verification *Software Tools for Technology Transfer*, 2001
9. J. Engelfriet Branching Processes of Petri Nets *Acta Informatica* 1991
10. J. Esparza Model checking using net unfoldings *Science of Computer Programming* 23(2), 151-194 1994
11. E. Fabre, A. Benvensite et al. Distributed Monitoring of Concurrent and Asynchronous Systems - *Journal of Discrete Event Dynamic Systems*, March, 2005
12. A. Finkel, J-F. Raskin, et al. Monotonic extensions of Petri Nets: forward and backward search revisited *Technology Transfer*, 2001
13. S. Genc and S. Lafortune Distributed diagnosis for DES using Petri Nets - *ATPN*, Eindhoven, The Nederlands, 2003
14. S. Genc and S. Lafortune A distributed algorithm for on-line diagnosis of place-bordered Petri Nets - *IFAC Congress*, Prague, 2005
15. A. Giua, D. Corona and C. Seatzu State estimation of Λ-free labeled Petri Nets with contact-free nondeterministic transitions *Journal of Discrete Event Dynamic Systems*, March, 2005
16. A. Giua and X. Xie Control of safe ordinary Petri Nets with marking specifications using unfoldings *WODES'04*, Reims, France, 2004
17. G. Jiroveanu, R.K. Boel and B. Bordbar Contextual analysis of partially observable large Petri Net models *submitted to JDEDS*, 2004
18. S. McIlraith Explanatory diagnosis: Conjecturing actions to explain observation - 6^{th} *Int. Conf. on Principles of Knowledge Representation and Reasoning*, 1998
19. K. L. McMillan Using unfoldings to avoid the state space explosion problem in verification of asynchronous circiuts *Proceedings of the* 4^{th} *International Workshop on Computer Aid Verification* LNCS, vol. 663, Springer-Verlaag, 1992
20. C. Mancel, Pierre Lopez and et al. Relationships between Petri Nets and constraint graphs: application to manufacturing *15th IFAC Triennial World Congress*, Spain, 2002
21. Y. Pencolé, M.-O. Cordier et al. Incremental decentralized diagnosis approach for the supervision of a telecommunication network *DX'01*, Italy, 2001
22. L.Portinale and C. Anglano B-W Analysis: a Backward Reachability Analysis for Diagnostic Problem Solving suitable to parallel implementation *15th Int. Conference on Application and Theory of Petri Nets*, Zaragoza, Spain, LNCS 815, pp. 39-58, 1994
23. N. Riviere Modélisation et anallyse temporelle par réaseaux de Petri et logique linéaire *Thése Doctoral*, INSA Toulouse, 2003
24. M. Sampath, R. Sengupa et.al Diagnosability of Discrete Event Systems - *IEEE Transactions On Automatic Control*, Vol. 40(9), 1995
25. V.S. Srinivasan and M.A. Jafari Fault Detection/Monitoring using Timed Petri Nets *IEEE Trans. On Sys. Man and Cyb*, 1993, vol.23, No.4, pp. 1155-1162
26. R. Su Distributed diagnosis for Discrete Event Systems *PhD Thesis*, University of Toronto, 2004
27. R. Su and W.M. Wonham A model of component consistency in distributed diagnosis *WODES*, Reims, France, 2004
28. R.Valette and et. al. Petri Net based reasoning for the diagnosis of Dynamic Discrete Event Systems *6th Int. Fuzzy Syst. Assoc. World Congress*, pp. 333-336, July, 1995
29. A. Valmari Compositional analysis with place-bordered subnets *LNCS 815*, 1994