Multi-agent distributed contextual diagnosis for large Petri Net models

George Jiroveanu and René K. Boel

University of Ghent, SYSTeMS Research Group
Technologypark 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 diagnosis 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 observability 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 unobservedly 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. Besides 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 \( \mathcal{N} = (\mathcal{P}, \mathcal{T}, F) \) 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. \( F = \text{Pre} \cup \text{Post} \) where \( \text{Pre}(p, t) : \mathcal{P} \times \mathcal{T} \rightarrow \mathbb{N} \) and \( \text{Post}(t, p) : \mathcal{T} \times \mathcal{P} \rightarrow \mathbb{N} \) 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 \( x^* = \{ y \in \mathcal{X} \mid x \mathrel{F} y \} \) and \( x^c = \{ y \in \mathcal{X} \mid y \mathrel{F} x \} \).

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

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 \( M \geq \text{Pre}(\cdot, t) \). Firing, an enabled transition \( t \) consumes \( \text{Pre}(\cdot, t) \) tokens in the input places of \( t \) (\( p \in t^* \)) and produces \( \text{Post}(t, \cdot) \) tokens in the output places of \( t \) (\( p \in t^c \)). The next marking is \( M' = M + \text{Post}(t, \cdot) - \text{Pre}(\cdot, t) \). A trace \( \tau \) 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 \( i = 1, \ldots, k, M_{i-1} \geq \text{Pre}(\cdot, t_i) \); \( M_0 \xrightarrow{\tau} M_k \) denotes that the enabling conditions are all satisfied so that \( \tau \) 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 \( \mathcal{R}_\mathcal{N}(M_0) = \{ M \mid \exists \tau \in \mathcal{L}_\mathcal{N}(M_0) \land M_0 \xrightarrow{\tau} M \} \).

The set of transitions \( \mathcal{T} \) is partitioned into disjoint sets of observable transitions \( \mathcal{T}_o \) and unobservable (silent) transitions \( \mathcal{T}_u \).

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: \( \forall t \in \mathcal{T}_u \Rightarrow \delta(t) = \epsilon \) where \( \epsilon \) is the empty string. .
Denote by $T^*$ the Kleene closure of the set $T$. Let $\sigma \in \mathcal{L}_N(M_0) \subseteq T^*$ and $T' \subset T$. The projection $\Pi_{T'} : \mathcal{L}_N(M_0) \rightarrow T'^*$ is defined as:

i) $\Pi_{T'}(\varepsilon) = \varepsilon$;

ii) $\Pi_{T'}(t) = t$ if $t \in T'$;

iii) $\Pi_{T'}(t) = \varepsilon$ if $t \notin T \setminus T'$;

iv) $\Pi_{T'}(\sigma t) = \Pi_{T'}(\sigma)\Pi_{T'}(t)$ for $\sigma \in \mathcal{L}_N(M_0)$ and $t \in T$.

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

A1) self-loop free $\forall t \in T^* t \cap t^* = \emptyset$

A2) bounded w.r.t. to the unobservable evolution: $\forall M \in \mathcal{R}_N(M_0); M \xrightarrow{\tau} M' \wedge \tau \in T^+_\text{u} \Rightarrow M' \not\sim M$

A3) and all the arcs have capacity one $\forall (p, t), \text{Pre}(p, t) \leq 1 \wedge \text{Post}(t, p) \leq 1$

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

**Definition 2** A multi set $S_N$ over a non empty set $S$ is a function $S_N : S \rightarrow S \times \mathbb{N}$ 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 $\alpha$ in $S_N(\alpha) (S_N(\alpha) = (\alpha, \mu(\alpha)))$. An element of a multi-set $S_N$ is denoted $(\alpha, \nu(\alpha))$ where $0 < \nu(\alpha) \leq \mu(\alpha)$, $\nu(\alpha) \in \mathbb{N}$.

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

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

The letters $\sigma, \tau$ are used for denoting strings of letters or traces. Whenever necessary we treat a marking $M$ in a PN $N$ as a multi-set defined by the marked places and the number of tokens contained in each marked place. Thus for $M \subseteq M'$ 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 $N$, $\varphi = p_0 t_1 \ldots t_n p_n$ is a non-trivial unobservable elementary path in $N$ if: i) $n > 0$; ii) $t_{q+1} \subseteq p_q^* \cap p_{q+1}^*$ for $q = 1, \ldots, n$; iii) $t_q \in T_{uo}$ for $q = 1, \ldots, n$. An unobservable elementary circuit (vec) denoted $\zeta$ is an unobservable elementary path $\varphi$ 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 $f : X \rightarrow Y$ 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 ($\forall a, b, c \in V, (a \preceq b) \land (b \preceq c) \Rightarrow (a \preceq c)$)

iii) $\preceq$ is antisymmetric ($a, b \in V, (a \preceq b) \land (b \preceq a) \Rightarrow (a = b)$)

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

Definition 5 Given a $PN \mathcal{N} = (P, T, F)$ the immediate dependence relation $\preceq_1 \subset (P \times T) \cup (T \times P)$ is defined as:

$$\forall (a, b) \in (P \times T) \cup (T \times P) : a \preceq_1 b \iff F(a, b) \neq 0$$

Then define $\preceq$ as the transitive closure of $\preceq_1$ ($\preceq = \preceq_1^*$).

Definition 6 Given a $PN \mathcal{N} = (P, T, F)$ the immediate conflict relation $\preceq_2 \subset T \times T$ is defined as:

$$\forall (t_1, t_2) \in T \times T : t_1 \preceq_2 t_2 \iff t_1 \cap \cdot t_2 \neq 0$$

Then define $\preceq \subset (P \cup T) \times (P \cup T)$ as:

$$\forall (a, b) \in (P \cup T) \times (P \cup T) : a \preceq b \iff \exists t_1, t_2 \text{ s.t } t_1 \preceq_2 t_2 \text{ and } t_1 \preceq_1 a \text{ and } t_2 \preceq_1 b$$

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

$$\forall (a, b) \in (P \cup T) \times (P \cup T) : a \parallel b \Rightarrow a \not\preceq b \land a \not\preceq b \land b \not\preceq a$$

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

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

Definition 9 An occurrence net is a net $\mathcal{O} = (B, E, \preceq_1)$ such that:

i) $\forall a \in B \cup E : \neg (a \preceq_1 a)$ (acyclic)

ii) $\forall a \in B \cup E : |\{b : a \preceq_1 b\}| < \infty$ (well-formed)

iii) $\forall a \in B : |\cdot b| \leq 1$ (no backward conflict)

In the following $B$ is referred as the set of conditions while $E$ is the set of events. Denote by $X^E_{\infty}$ a set of pairwise concurrent nodes, by $X^E_{\infty}$ a concurrent set of events, and by $X^B_\infty$ 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 $a \preceq b$ can be interpreted as a happens before $b$.

Definition 10 A configuration $C = (B, E, \preceq_1)$ in the occurrence net $\mathcal{O}$ is defined as follows:

i) $C$ is a sub-net of $\mathcal{O}$ ($C \subseteq \mathcal{O}$)

ii) $C$ is conflict free i.e. $\forall a, b \in (B \cup E) \times (B \cup E) \Rightarrow a \not\preceq b$

iii) $C$ is causally upward-closed i.e. $\forall b \in B \cup E : a \preceq_1 b \Rightarrow a \in B \cup E$

iv) $\text{Min}(C) = \text{Min}(\mathcal{O})$
Denote by C the set of all the configurations of the occurrence net \( \Omega \).

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

1. the restriction of \( \phi \) to Min(\( \Omega \)) is a bijection between Min(\( \Omega \)) and \( M_0 \) (the set of initially marked places).  
2. \( \phi(B) \subseteq P \) and \( \phi(E) \subseteq T \).  
3. \( \forall a, b \in E : (a^* = b^*) \land (a^* = b^*) \Rightarrow a = b \)

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

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

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

There exists (up to an isomorphism) a unique maximum branching process (w.r.t. \( \subseteq \)) that is the unfolding of \( N \) and is denoted \( \mathcal{U}_N \) [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 \( \mathcal{N} \) (obtained by reversing the direction of all the arcs in \( \mathcal{N} \) [17]).

4.1 **Coverability and Reverse Occurrence Nets**

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

**Definition 13** Backwards enabling rule: A transition \( t \) is backward enabled in a marking \( M \in \mathbb{N}^P \) iff \( \exists p \in t^* \) s.t. \( M(p) > 1 \). Backwards firing rule: A backward enabled transition \( t \) in a marking \( M \in \mathbb{N}^P \) fires backwards from \( M \) producing \( M' \) (denoted \( M \xrightarrow{t} M' \)) where \( M' = M \circ \text{Post}(t) + \text{Pre}(t) \).

A sequence of transitions \( \tau = t_1 \ldots t_m \) is backward allowable from \( M \) (denoted \( M \xrightarrow{\tau} M' \)) iff for \( q = 1, \ldots, m \), \( \tau_q = t_1 \ldots t_{q-1} \) and \( t_q \) is backward enabled in \( M' \) where \( M \xrightarrow{t_q} M'' \).
Definition 14 Given a PN $\mathcal{N}$, consider a marking $M \in \mathbb{N}^P$. Then $M$ is covered by $M'$ if $\exists \sigma \in \mathcal{L}_p(M')$ s.t. $M' \models M' \land M'' \geq M$.

Proposition 1 Given a PN $(\mathcal{N}, M_0)$ and a marking $M$, then $M$ is covered by $M_0$ iff $\exists M' \leq M_0$ s.t. $M \models M'$.

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

i) $\forall a \in \hat{B} \cup \hat{E} : \neg (a \leq a)$ (acyclic)

ii) $\forall a \in \hat{B} \cup \hat{E} : |\{a : a \leq b\}| < \infty$ (well-formed)

iii) $\forall a \in \hat{B} : |a^\bullet| \leq 1$ (no-forward conflict)

iv) $\max(\hat{\Sigma}) \subseteq \hat{B}$

Definition 16 Given a PN $\mathcal{N}$ and a final marking $M_{\text{fin}}$, the reverse branching process of $(\mathcal{N}, M_{\text{fin}})$ is $\hat{\mathbb{B}} = (\hat{\Sigma}, \hat{\phi})$ s.t.:

i) $\phi(\hat{B}) \subseteq \mathcal{P}$ and $\phi(\hat{E}) \subseteq \mathcal{T}$

ii) $M_{\text{fin}} \subseteq \phi(\max(\hat{\Sigma}))$

iii) $\forall a, b \in \hat{E} : (a^\bullet = b^\bullet) \land (a^\bullet = b^\bullet) \Rightarrow a = b$

Remark 2 Notice that above condition ii) requires that $M_{\text{fin}} \subseteq \phi(\max(\hat{\Sigma}))$ and not $M_{\text{fin}} = \phi(\max(\hat{\Sigma}))$ since our aim is to compute markings that cover $M_{\text{fin}}$ and not markings that reach $M_{\text{fin}}$.

Definition 17 Given a PNN the immediate backward conflict relation $\preceq_1 \subseteq \mathcal{T} \times \mathcal{T}$ is defined as follows:

$$\forall (t_1, t_2) \in \mathcal{T} \times \mathcal{T} : t_1 \preceq_1 t_2 \iff t_1^\bullet \cap t_2^\bullet$$

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

$$\forall (a, b) \in (P \cup \mathcal{T}) \times (P \cup \mathcal{T}) : a \preceq b \Rightarrow \exists (t_1, t_2) \in \preceq_1 \text{ s.t. } a \preceq t_1 \text{ and } b \preceq t_2.$$ 

Definition 18 Given a PN $\mathcal{N}$, a final marking $M_{\text{fin}}$, and a reverse branching process $\hat{\mathbb{B}} = (\hat{\Sigma}, \hat{\phi})$, the immediate causally confusion relation $\preceq_{\text{ca}} \subseteq \hat{E} \times \hat{E}$ is defined as follows:

$$\forall (e_1, e_2) \in \hat{E} \times \hat{E} : \phi(e_1) = \phi(e_2) \land e_1^\bullet \cap e_2^\bullet \neq \emptyset \land e_1^\bullet \neq e_2^\bullet$$

Then define $\preceq_c \subseteq (B \cup \hat{E}) \times (B \cup \hat{E})$ as:

$$\forall (a, b) \in (B \cup \hat{E}) \times (B \cup \hat{E}) : a \preceq_c b \Rightarrow \exists (e_1, e_2) \in \preceq_{\text{ca}} \text{ s.t. } a \preceq e_1 \text{ and } b \preceq e_2.$$ 

Definition 19 A configuration $\hat{C} = (\hat{B}, \hat{E}, \preceq_1)$ in a reverse occurrence net $\hat{\Sigma}$ is defined as follows:

i) $\hat{C}$ is a sub-net of $\hat{\Sigma}$

ii) $\hat{C}$ is causally downward-closed - $\forall b \in \hat{B} : b \preceq a \Rightarrow a \in \hat{B}$

iii) $\hat{C}$ is backward conflict free - $\forall (a, b) \in (B \cup \hat{E}) \times (B \cup \hat{E}) : a \preceq_c b$

iv) $\hat{C}$ is causally confusion free - $\forall (a, b) \in (B \cup \hat{E}) \times (B \cup \hat{E}) : a \preceq_c b$
v) \( \text{Max}(\hat{C}) \subseteq \text{Max}(\hat{\omega}) \) and \( M_{f_{\text{in}}} \subseteq \phi(\text{Max}(\hat{C})) \)

Denote by \( \hat{C} \) the set of all the configurations of a reverse occurrence net \( \hat{\omega} \).

By item ii) and iii) we require that in a configuration \( \hat{C} \) every condition-node \( b \in B_C \) has at most one input event-node in \( \hat{U}_N(M_{f_{\text{in}}}) \). The reason we put this condition is that we need \( C \) to result as a configuration in a forward unfolding \( U_N \). 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 PNN and a final marking \( M_{f_{\text{in}}} \) and two reverse branching processes \( \hat{\mathcal{B}}, \hat{\mathcal{B}}' \) then \( \hat{\mathcal{B}}' \subseteq \hat{\mathcal{B}} \) if there exists an injective homomorphism \( \psi : \hat{\mathcal{B}}' \rightarrow \hat{\mathcal{B}} \) s.t. \( \psi(\text{Min}(\hat{\mathcal{B}}')) = \text{Min}(\hat{\mathcal{B}}) \) and \( \hat{\phi} \circ \psi = \hat{\phi}' \).

**Definition 21** Given a PNN with an initial marking \( M_0 \) and a final marking \( M_{f_{\text{in}}} \) denote by \( \hat{U}_N(M_{f_{\text{in}}}) \) the maximal branching process w.r.t. set inclusion s.t. \( \forall C \in \hat{C}, \exists C' \in \hat{C} \) s.t. \( C \subseteq C' \) and \( \phi(\text{Min}(C')) = M_0 \).

**Proposition 2** \( \hat{U}_N(M_{f_{\text{in}}}) \) is unique up to isomorphism.

**Proof.** First denote \( \hat{C}' = \left\{ C' \in \hat{C} \mid \phi(\text{Min}(C')) = M_0 \right\} \). Then we have by definition that every maximal configuration \( \hat{C}' \in \hat{C}' \) in the backward unfolding \( \hat{U}_N(M_{f_{\text{in}}}) \) is also a configuration in the forward unfolding \( U_N \). Since \( U_N \) is unique up to isomorphism it results that also \( \hat{U}_N(M_{f_{\text{in}}}) \) is unique. \( \square \)

### 4.2 Algorithm to construct \( \hat{U}_N(M_{f_{\text{in}}}) \)

Given a configuration \( \hat{C} = (\hat{B}, \hat{E}, \hat{X}_1) \) in the backward unfolding \( \hat{U}_N(M_{f_{\text{in}}}) \) denote by \( \text{Cut}^\rightarrow(\hat{C}) \) the maximal set (clique) of concurrent conditions and then denote by \( \hat{\phi}(\hat{C}) \) the marking that corresponds to \( \text{Cut}(\hat{C}) \).

\[
\text{Cut}^\rightarrow(\hat{C}) = \left\{ e^* \mid e \in \hat{E} \right\} \cup \text{Max}(\hat{C}) \setminus \left\{ e^* \mid e \in \hat{E} \right\}
\]

Denote in the following by \( \hat{X}_{co}^B \) a co-set of conditions in \( \hat{C} \). A transition \( t \) is backward enabled in \( \hat{U}_N \) by a configuration \( \hat{C} \) if \( \hat{X}_{co}^B \subseteq \text{Cut}^\rightarrow(\hat{C}) \) and \( 0 < \hat{\phi}(\hat{X}_{co}^B) \leq t^* \).

Denote by \( \text{Enable}(\hat{C}) \) the set of all backwards enabled transitions.

\[
\text{Enable}(\hat{C}) = \left\{ (\hat{X}_{co}^B, t) \mid (\hat{X}_{co}^B, t) \text{ backwards enabled} \right\}
\]

A configuration \( \hat{C} \) is extended by a backwards enabled transition \( t \) in the following way:

i) add an event \( e \) with \( \hat{\phi}(e) = t \)

ii) add arcs from each \( b \in \hat{X}_{co}^B \) to \( e \)

iv) add conditions \( b \) s.t. \( \hat{\phi}(b) = p \land p \in t^* \setminus \hat{\phi}(\hat{X}_{co}^B) \) and add arcs from each \( b \) to \( e \)

iii) add conditions \( b \) s.t. \( \hat{\phi}(b) = p \land p \in t^* \)
\(\tilde{U}_N\) is generated extending each configuration by enabled transitions the only requirement being that \(\phi(e_1) = \phi(e_2) \land e_1^* = e_2^* \Rightarrow e_1 = e_2\) (no redundancy).

Throughout the remaining paper we use the notation \(C \circ e\) and \(e \circ \tilde{C}\) to indicate that a configuration \(C\) resp. \(\tilde{C}\) is extended forward resp. backwards by appending an event \(e\).

**Example 1** To illustrate the computation of \(\tilde{U}_N(M_{\text{fim}})\) consider for simple PN \(N\) displayed in Fig. 1.a where \(M_{\text{fim}} = \{m(p_2) = 1, m(p_3) = 1, m(p_4) = 1\}\) and \(M_0 = \{m(p_0) = 2\}\). Then Fig. 1.b displays \(U_N\) while in Fig. 1.c \(\tilde{U}_N(M_{\text{fim}})\) is displayed. We have that \(\tilde{C} = \{C_1, C_2\}\) where the event node-sets for \(C_1\) and \(C_2\) are \(E_1 = \{e_0, e_0, e_1, e_2, e_3\}\) and \(E_2 = \{e_0, e_0, e_1, e_2, e_3\}\) respectively.

![Fig. 1.](image)

### 5 PN analysis under partial observation

Consider an agent \(Ag\) that supervises a plant. The agent has the plant model given as a PN \(N\) 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 $O_{\theta_e}$ the sequence of observed events received up to time $\theta_e$ by $Ag$ where $O_{\theta_e} = \langle t_1^e, \theta_1^e \rangle, \langle t_2^e, \theta_2^e \rangle, \ldots, \langle t_n^e, \theta_n^e \rangle$ with $\theta_k^e$ the time the observed event $t_k^e$ happened in the plant.

Consider the plant observation $O_{\theta_e} = t_1^e, \ldots, t_n^e$. Since $O_{\theta_e}$ 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 $N$ that start from the known initial marking $M_0$ and obey the observation:

$$\mathcal{L}_N(O_{\theta_e}) = \{ \tau \in \mathcal{L}_N(M_0) \mid \Pi_{T_{\tau}} \tau = O_{\theta_e} \}$$ (1)

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

$$\mathcal{M}_N(O_{\theta_e}) = \{ M \mid \exists \tau \in \mathcal{L}_N(O_{\theta_e}) \land M_0 \xrightarrow{\tau} M \}$$ (2)

Consequently the plant diagnosis at the time $\theta_e$ after observing $O_{\theta_e}$ is obtained by projecting the set of possible evolutions on to the set of fault events $T_F$:

$$\mathcal{D}_N(O_{\theta_e}) = \{ \sigma_f \mid \sigma_f = \Pi_{T_{\sigma_f}} \tau \land \tau \in \mathcal{L}_N(O_{\theta_e}) \}$$ (3)

Then the centralized diagnosis result is:

$$\mathcal{DR}_N(O_{\theta_e}) = \begin{cases} N & \text{iff } \mathcal{D}_N(O_{\theta_e}) = \{ \epsilon \} \\ F & \text{iff } \epsilon \notin \mathcal{D}_N(O_{\theta_e}) \\ UF & \text{iff } \epsilon \subset \mathcal{D}_N(O_{\theta_e}) \end{cases}$$ (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 $\mathcal{L}_N(O_{\theta_e}), \mathcal{D}_N(O_{\theta_e}), \mathcal{DR}_N(O_{\theta_e})$ and $\mathcal{M}_N(O_{\theta_e})$ 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. $t_1^e$) $Ag$ starts unfolding $\langle N, M_0 \rangle$ computing the maximal configurations such that each maximal configuration contains only one event node $e \in E$ that corresponds to an observable transition $\phi(e) \in T_\epsilon$ that is the observable transition that was observed ($\phi(e) = t_1^e$).

Denote $\mathcal{U}_N(t_1^e)$ the net unfolding obtained in this way (notice that we drop the lower index $N$ whenever clear from the context that we refer to $N$). Then at the
receiving of the second observed event (e.g. \( t_2^a \)) \( Ag \) extends \( \mathcal{U}(\ell) \) in a similar manner for finding configurations that will also include one node that corresponds to \( t_2^a \).

Denote by \( \mathcal{U}(\Omega_b) \) the net unfolding that is obtained considering the sequence of observed events \( \Omega_b \). Then denote by \( \mathcal{C}(\Omega_b) \) the set of configurations in \( \mathcal{U}(\Omega_b) \) s.t. \( \forall C \in \mathcal{C}(\Omega_b), C = (b \subseteq C, E_C, \leq) \) we have:

i) \( \phi \) is a bijection between \( E_C \) and \( \Sigma_{\Omega_b} \), where \( E_C = \{ e \in E_C \ | \ \phi(e) \in \tau_a \} \)

ii) if \( \theta_{t_1} < \theta_{t_2} \) then either \( \phi^{-1}(t_1^a) < \phi^{-1}(t_2^a) \) or \( \phi^{-1}(t_1^a) = \phi^{-1}(t_2^a) \).

In \( \mathcal{U}_a \) denote by \([a^a] \) the upward closure of a node \( a [a^a] = \{ b : b \preceq a \} \). Then denote by \([a^a] \)' the set of condition nodes that are first successors of nodes that are predecessors of \( a \) and are not contained in \([a^a]\): \([a^a] \)' = \{ \( c \in B \setminus [a^a] \ | \ \exists b \in [a^a] \setminus [b^a], c \} \).

Abusing notation \([a^a] \cup [a^a] \)' denotes also the corresponding (proper) subnet of \( \mathcal{U}_a \).

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

\[
\text{MinC}(t) = [e^a] \cup [e^a]' \cup \left\{ \text{Min}(\mathcal{U}_a) \setminus [e^a] \right\}
\]

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

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

\[
\langle \text{MinE} \rangle = \{ \sigma = e_1 \ldots e_m \ | \ \forall i,j : e_i < e_j \Rightarrow 1 \leq i < j \leq m \}
\]

Then \( \text{MinE}(t_1^a) \) denotes the set of all minimal explanations:

\[
\text{MinE}(t_1^a) = \{ \sigma \ | \ \sigma \in \langle \text{MinE} \rangle \land \text{MinC} \in \text{MinC}(t_1^a) \}
\]

The set of minimal traces in \( N \) that explain \( t_1^a \) is:

\[
\mathcal{L}^{\text{min}}(t_1^a) = \{ \tau \ | \ \tau = \phi(\sigma) \land \sigma \in \text{MinE}(t_1^a) \}
\]  \hspace{1cm} (5)

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

For an arbitrary observation \( \Omega_b \), denote by \( \text{MinC}(\Omega_b) \) the set of all the minimal configurations and by \( \text{MinE}(\mathcal{C}(\Omega_b)) \) the set of minimal explanations of \( \mathcal{C}(\Omega_b) \). Consequently the set of minimal traces that explain \( \mathcal{C}(\Omega_b) \) is:

\[
\mathcal{L}^{\text{min}}(\Omega_b) = \{ \tau \ | \ \tau = \phi(\sigma) \land \sigma \in \langle \text{MinE}(\mathcal{C}(\Omega_b)) \rangle \}
\]

and the set of estimated states considering the minimal explanations of \( \Omega_b \) is:

\[
\mathcal{M}^{\text{min}}(\Omega_b) = \{ M \ | \ M_0 \xrightarrow{\mathcal{L}} M \land \tau \in \mathcal{L}^{\text{min}}(\Omega_b) \}
\]

Thus we have that \( \mathcal{L}^{\text{min}}(\Omega_b) \subseteq \mathcal{L}(\Omega_b) \) and

\[
\forall \Omega_b \ igcup_{M' \in \mathcal{M}^{\text{min}}(\Omega_b)} \mathcal{R}(M') = \bigcup_{M'' \in \mathcal{L}(\Omega_b)} \mathcal{R}(M'')
\]  \hspace{1cm} (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:

$$\forall M \in R_N(M_0) : \exists t \in T \setminus T_F \text{ s.t. } \text{Pre}(\cdot,t) \leq M$$

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

$$\forall O_{t_{\theta}} \quad DR(O_{t_{\theta}}) = F \iff DR^{\text{min}}(O_{t_{\theta}}) = F$$


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 $L^{\text{min}}(O_{t_{\theta}})$ that is usually very small comparing with $L(O_{t_{\theta}})$.

The computation of $L^{\text{min}}(O_{t_{\theta}})$ is made backwards starting from the observed events in the following way.

First the reverse occurrence net $\tilde{U}(t^n)$ that corresponds to the first observed event $t^n$ is calculated by Algorithm 1.

### Algorithm 1 $B_{\text{Unfold}}(t^n)$

**Input:** $t^n, M_0$

**Output:** $\tilde{U}(t^n)$

1. $\tilde{U} = \emptyset \cup \mathcal{e} \cup \mathcal{e}^*$ where $\mathcal{e}(e) = t^n$
2. $\tilde{C}_0 = \tilde{U}, \tilde{C} = \{ \tilde{C}_0 \}$
3. Enable $= \bigcup_{C \in \tilde{C}} \text{Enable}(C) \cap T_\alpha$
4. while Enable $\neq 0$
5. pick and delete $e = (X_{\text{cor}}, t) \in \text{Enable}$
6. $\tilde{C}_{\text{new}} = e \otimes \tilde{C} \{ \text{extend } \tilde{U} \}$
7. $\tilde{C} = \tilde{C} \cup \tilde{C}_{\text{new}}$
8. Enable $:= \text{Enable} \cup \text{Enable}(\tilde{C}_{\text{new}})$
9. end while

### Remark 3 Notice that in $B_{\text{Unfold}}(t^n)$ 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 unobservably by $M_0$. Notice that $\langle N', M_0 \rangle$ is assumed bounded w.r.t. the unobservable evolution.

Consider now the observed sequence $O_{t_{\theta}} = t^1 \ldots t^n$ the computation of $\tilde{U}(O_{t_{\theta}})$ and $\tilde{C}(O_{t_{\theta}})$ is done recursively as is presented in Algorithm 2.

### Proposition 4 Given $\text{Min}_U(O_{t_{\theta}}) \subseteq \tilde{U}(O_{t_{\theta}})$ and $\tilde{C}(O_{t_{\theta}})$ we have that:
Algorithm 2 $\mathcal{B}_\text{Unfold}(\mathcal{O}_{\theta_e})$

Input: $\mathcal{O}_{\theta_e}$
Output: $\mathcal{U}(\mathcal{O}_{\theta_e})$

1: $k := 1$
2: B\_Unfold($t_i^0, M_0$) \{compute $\mathcal{U}(t_i^0)$\}
3: while $k \leq n$ do
4: \hspace{1em} while $\mathcal{C}(\mathcal{O}_{\theta_e}^k) \neq \emptyset$ do
5: \hspace{2em} pick and delete $\mathcal{C} \in \mathcal{C}(\mathcal{O}_{\theta_e}^k)$
6: \hspace{2em} B\_Unfold($t_i^k, M_0$) \{compute $\mathcal{U}(t_i^k, \phi(\mathcal{C}))$\}
7: \hspace{2em} $\mathcal{C}(\mathcal{O}_{\theta_e}^{k+1}) = \mathcal{C}(\mathcal{O}_{\theta_e}^k) \cup \mathcal{C}(t_i^{k+1})$ \{compute $\mathcal{U}(t_i^1, \ldots, t_i^k)$\}
8: \hspace{1em} $\mathcal{U}(\mathcal{O}_{\theta_e}^{k+1}) = \mathcal{U}(\mathcal{O}_{\theta_e}^k) \cup \mathcal{C}(\mathcal{O}_{\theta_e}^{k+1})$
9: \hspace{1em} end while
10: $k := k + 1$
11: end while

i) $\forall \mathcal{C} \in \mathcal{C}(\mathcal{O}_{\theta_e}) \implies \exists \text{MinC} \in \mathcal{U}(\mathcal{O}_{\theta_e})$ s.t. $\mathcal{C} \equiv \text{MinC}$ (read as $\mathcal{C}$ is isomorphic with MinC)

ii) $\forall \text{MinC} \in \mathcal{U}(\mathcal{O}_{\theta_e}) \implies \exists \mathcal{C} \in \mathcal{C}(\mathcal{O}_{\theta_e})$ $\mathcal{C} \equiv \text{MinC}$

Thus it results that $\bigcup_{\mathcal{C} \in \mathcal{C}(\mathcal{O}_{\theta_e})} \phi(\{E\}) = \mathcal{L}^{\text{min}}(\mathcal{O}_{\theta_e})$.

![Fig. 2.](image-url)
6 The distributed setting

We consider the distributed plant description as follows:

i) $N = \bigcup_{i \in I} N_i$ where $N = \langle P, T, F \rangle$, $N_i = \langle P_i, \mathcal{T}_i, F_i \rangle$, and $i \in I$

ii) $P = \bigcup_{i \in I} P_i, \forall i \in I, \exists j \in I, i \neq j \text{ s.t. } P_i \cap P_j \supseteq \neq P_{ij} \neq \emptyset$

iii) $T = \bigcup_{i \in I} \mathcal{T}_i, \forall i, j \in I, i \neq j \Rightarrow \mathcal{T}_i \cap \mathcal{T}_j = \emptyset$

iv) $F = F \upharpoonright N$

v) $P_{ij} = P_{IN_{ij}} \cup P_{OUT_{ij}}, P_{IN_{ij}} \cap P_{OUT_{ij}} = \emptyset$

vi) $P_{IN_{ij}} = P_{OUT_{ij}} = \{ p \in P_{ij} | \mathcal{P} \subseteq \mathcal{T}_i \land \mathcal{P} \subseteq \mathcal{T}_j \}$

vii) $P_{IN_{ij}} = P_{OUT_{ij}} = \{ p \in P_{ij} | \mathcal{P} \subseteq \mathcal{T}_i \land \mathcal{P} \subseteq \mathcal{T}_j \}$

viii) $N$ is structurally bounded w.r.t. the unobservable evolution i.e. $\forall M \in \mathbb{N}^P \land \forall \sigma_{ao} \in \mathcal{T}_{ao} : M \xrightarrow{\sigma_{ao}} M' \Rightarrow M' \neq M$

For simplicity we assume at item v above that $P_{IN_{ij}}$ and $P_{OUT_{ij}}$ are disjunct and moreover we consider $M_{0_{ij}} = 0$ ($M_{0_{ij}} = M_0(P_{ij}), \forall i, j \in I$). Denote $P_{IN} = \{ P_{IN_{ij}} | j \in I, j \neq i \land P_{IN_{ij}} \neq \emptyset \}$ and $P_{OUT} = \{ P_{OUT_{ij}} | j \in I, j \neq i \land P_{OUT_{ij}} \neq \emptyset \}$. 

Fig. 3.

The unfolding $\mathcal{U}(t_0)$ of $\langle N, M_0 \rangle$ given the observation $Q_{t_0} = t_0$ 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 $\mathcal{U}_N$ indicate the corresponding node in $N$ (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 $\mathcal{U}_N$ that correspond to the same node in $N$. $\text{MinC}_1$ (in grey) represents a minimal configuration: $\text{MinC}_1 = [ee_1^{e_i} \cup [ee_2^{e_i}]]$ where $\phi(e_i) = t_0$.

In dark grey there is represented the configuration $C_1$, $\text{MinC}_1 \subseteq C_1$. Notice that $C_1 \setminus \text{MinC}_1$ includes unobservable nodes that are concurrent with $ee_1^{e_i}$ (e.g. $ee_2^{e_i}$) and nodes that are successors of $ee_1^{e_i}$ (e.g. $ee_2^{e_i}$). $C_1$ compactly represents a set of traces that can be obtained by linearizing the partial order relation between the nodes $E_1 = \{ e_2, e_2, ee_5, ee_6, ee_7, ee_8 \}$ (e.g. $t_3 \leq t_4 \leq t_5, t_3 \leq t_4 \leq t_5, t_3 \leq t_4 \leq t_5, etc.$).

The backward unfolding $\mathcal{U}(t_0)$ is presented in Fig. 4. $C_1$ compactly represents $t_{12}t_{10}t_{9}t_0$ and $t_0 \neq t_3t_4t_5$. 

$L_{\text{min}}(t_0) = \{ t_0t_4t_6; t_1t_4t_6; t_2t_4t_6; t_0t_2t_3t_6; t_{12}t_{10}t_{9}t_0; t_0t_2t_3t_6; \ldots \}$
Given the set of agents $\mathcal{A} = \{A_g_i | i \in I\}$, where the knowledge an agent $A_g_i$ has is: $\mathcal{K}_i = (\mathcal{N}_i, T_{ai}, T_{ai}, M_{ai}, \mathcal{P}_{IN}, \mathcal{P}_{OUT})$ consider that:

i) the plant observation is distributed $O_{\theta_i} = \otimes_{k \in I} O_{\theta_k}$. $O_{\theta_k} = t_{\theta_k}^0 \ldots t_{\theta_k}^m$ is the local observation recorded at site $i \in I$, where the observed events $(t_{\theta_k}^0, \theta_k)$ have the time tag $\theta_k$, indicating the time event $t_{\theta_k}^0$, 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, $A_g_i (i \in I)$ derives a local preliminary diagnosis of the local site $i$

R2) when the communication is allowed (e.g. at the global time $\theta_c$) 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 iterate 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 $\theta_c$ 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 $\theta_c$). The consideration of asynchronous communication protocol 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

Consider the distributed architecture shown in Fig. 5. Let the local observation at site 1 and site 2 be: $\mathcal{O}^1 = t_0$ 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 $M_0$, and resp. $M_0$ 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 $N_2$ and then leave via $p_9$. The question we must answer is: "what $Ag_2$ should do before
communicating with the neighboring agent \( A_{g_i} \). One solution would be to consider upper bounds for the marking of the input places of each component (e.g., \( P_b \) for \( N_2 \) 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 cannot 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 \( A_{g_i} \) 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 \( A_{g_i} \) \((i \in I)\) before it initiates the communication with its neighbors.

Consider in the following the case of the agent \( A_{g_i} \) having received the local site observation \( O_{i,b}^t = e_{i_{1}, ... , e_{i_{m}}}. \) Since there is not a priori knowledge of the marking of the input places \( P_{IN_i} \), \( A_{g_i} \) can make any assumption on the number of tokens that could have entered \( N_i. \)

Thus if \( A_{g_i} \) considers for each \( p_i \in P_{IN_i} \) a marking \( \omega \) it can then perform a backward search for finding the minimal configurations (minimal explanations) of \( O_{i,b} \), considering as initial marking \( M_{0_i}^\omega \) where:

\[
M_{0_i}^\omega = \begin{cases} 
M_{0_i}^\omega (p_i) = M_{0_i} & \text{for } p_i \in P_{IN_i} \setminus P_{IN_i}, \\
M_{0_i}^\omega (p_i) = \omega & \text{for } p_i \in P_{IN_i}, 
\end{cases}
\]  

As presented in Section 4 \( A_{g_i} \) can construct \( \overset{\sim}{U}_i(O_{i}) \) by running the algorithm \( B_{Unfold}(O_{i,b}) \) with the inputs: \( \langle N_i, M_{0_i}^\omega, O_{i,b}, T_{o_i}, T_{ao_i} \rangle \).

By computing \( \overset{\sim}{U}_i(O_{i,b}) \) \( A_{g_i} \) derives the set of configurations \( \overset{\sim}{C}_i(O_{i,b}) \). Given a configuration \( \overset{\sim}{C}_i \in \overset{\sim}{C}_i(O_{i,b}) \) denote \( \overset{\sim}{\text{Min}}(B_{IN_i}) \) the set of conditions that correspond to the input places \( p_i \in P_{IN_i} \):

\[
\overset{\sim}{\text{Min}}(B_{IN_i}) = \left\{ b_i \mid b_i \in \overset{\sim}{\text{Min}}(B_i) \wedge \phi(b_i) = p_i \wedge p_i \in P_{IN_i} \right\}
\]

and let \( \overset{\sim}{M}_i(P_{IN_i}) = \phi(\overset{\sim}{\text{Min}}(B_{IN_i})) \) be the minimal marking of the input places \( P_{IN_i} \) s.t. \( \overset{\sim}{C}_i \) is allowable. In the following we use the simplified notations: \( \overset{\sim}{M}_i \) for \( \overset{\sim}{M}_i(P_{IN_i}) \) and. \( \overset{\sim}{M}_{0_i} = M_{0_i} \overset{\sim}{M}_i \). Then denote \( \overset{\sim}{M}_i \) the set of minimal assumptions on the marking of the input places \( P_{IN_i} \):
\[ \mathcal{M}_{J_{N_i}} = \left\{ \tilde{M}_{J_{N_i}} \mid \tilde{C}_i \in \tilde{C}_i(O^i_{\theta_c}) \land \mathcal{M}_{J_{N_i}} = \phi(\text{Min}(\tilde{B}_{J_{N_i}})) \right\} \]

Denote \( \mathcal{E}_i \) the set of minimal preliminary explanations of the local observation \( O^i_{\theta_c} \) based on the minimal assumptions \( \mathcal{M}_{J_{N_i}} \):

\[ \mathcal{E}_i = \left\{ \sigma_i \mid \exists \tilde{C}_i \in \tilde{C}_i(O^i_{\theta_c}) \land \sigma_i \in \tilde{(E_i)} \right\} \]

Denote by \( \mathcal{M}_n \) the set of estimated markings based on the set of minimal explanations \( \mathcal{E}_i \) and the minimal assumptions \( \mathcal{M}_{J_{N_i}} \):

\[ \mathcal{M}_n = \left\{ M_n \mid \exists M_n \in \mathcal{M}(P_{J_{N_i}}), \exists \tau_n \in \phi(\mathcal{E}_i) : M_n \xrightarrow{\tau_n} M_n \right\} \]

Given an unobservable elementary cycle \( \zeta \), denote by \( T_\zeta \) the set of limiting places of \( \zeta \): \( T_\zeta \triangleq \{ p \mid p \not\in \zeta \land \exists t \in \zeta \land p \in \ast t \} \). A place \( p \in T_\zeta \) is a limiting place of \( \zeta \) since every complete execution of \( \zeta \) consumes tokens from \( p \). Denote \( M_{T_\zeta} \), the minimal marking of \( T_\zeta \) that allows for a complete execution of \( \zeta \).

**Assumption 5** For any local model \( N_i \) and for any vec \( \zeta_i \), there does not exist an executable sequence of unobservable transitions \( \sigma_{uo} \), with initial marking the marking \( M \) that has tokens only in the input places \( I N_i(p) = 0 \) for \( p \not\in P_{J_{N_i}} \) s.t. by firing from \( M \), \( \sigma_{uo} \) produces a marking \( M' \) greater than the limiting marking of \( \zeta_i \), \( M_{T_\zeta} \). \( \exists t \in T_{uo} \) s.t. \( (M_{T_\zeta}, \sigma_{uo}, M) \land (M(p(i)) \neq 0 \Rightarrow p \in P_{J_{N_i}} \).

**Proposition 5** Given a PN model \( N \) s.t. \( \forall i \in I \) Assumption 5 holds true for \( N_i \), then \( \forall \theta_{\zeta} \) by running \texttt{B.Unfold}(\( O^i_{\theta_c} \)) (Algorithm 2) for \( (N_i, M^i_0) \) and \( O^i_{\theta_c} \) we obtain the set of minimal assumptions of the marking \( \mathcal{M}_{J_{N_i}} \) s.t. \( \forall \mathcal{M}_{J_{N_i}} \in \mathcal{M}_{J_{N_i}}, \forall \mathcal{M}_n \in \mathcal{M}_{J_{N_i}} \Rightarrow \mathcal{M}_{J_{N_i}}, (p_i) < +\infty. \)

**Proof.** By Assumption 5 we have that for any marking \( M_{J_{N_i}} \) of the input places \( I N_i \), any cycle in \( N_i \) cannot be executed finitely many times. Thus any node in a configuration will have a finite number of predecessor-nodes. \( \square \)

Consider that at the time \( \theta_{\zeta} \) when the communication with the neighboring agents is the first time allowed \( Ag_i \) has computed \( \tilde{U}(O^i_{\theta_c}) \) having derived \( \tilde{C}(O^i_{\theta_c}) \) that comprises the set of preliminary minimal explanations \( \mathcal{E}_i \) and the set of minimal assumptions \( \mathcal{M}_{J_{N_i}} \). Then \( Ag_i \) must calculate, based on the set of minimal assumptions regarding the tokens that have entered \( \mathcal{M}_{J_{N_i}} \), the estimate of the number of tokens that could have exited \( N_i \) via \( P_{\text{OUT}} \).

For doing this \( Ag_i \) extends every minimal configuration \( \tilde{C}_i \in \tilde{C}_i(O^i_{\theta_c}) \) by considering all the unobservable extensions (sequences of unobservable transitions) that can be appended. Thus \( \hat{C}_i \) is forward extended by starting from the set of maximal conditions \( \text{Max}(\tilde{C}_i) \) (\( \phi(\text{Max}(\tilde{C}_i)) = \mathcal{M}_i \) where \( \mathcal{M}_i \xrightarrow{\tau_n} M_i \) and \( \tau_n \in \phi(\tilde{(E_i)}) \)).

The unobservable transitions that are enabled in \( \mathcal{M}_i / \text{Max}(\tilde{C}_i) \) 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 \( \mathcal{M}_{0_i} \in \mathcal{M}_n \), denote by \( \text{Min}\mathcal{U}(O^i_{\theta_c}, \mathcal{M}_{0_i}) \) the subnet of \( \tilde{U}(O^i_{\theta_c}) \) that corresponds to \( \mathcal{M}_{0_i} \). Then let \( \text{Min}\mathcal{U}(O^i_{\theta_c}, \mathcal{M}_{0_i}) \) be the set of minimal unfoldings \( \text{Min}\mathcal{U}(O^i_{\theta_c}, \mathcal{M}_{0_i}) \) and denote by \( \text{Min}\mathcal{C}(O^i_{\theta_c}, \mathcal{M}_{0_i}) \) the set of all minimal configurations.

Then denote by \( \mathcal{U}(O^i_{\theta_c}, \mathcal{M}_{0_i}) \) the maximal unobservable extension (w.r.t. set inclusion) of a minimal configuration \( \text{Min}\mathcal{C}(O^i_{\theta_c}, \mathcal{M}_{0_i}) \) and denote \( \text{C}(O^i_{\theta_c}, \mathcal{M}_{0_i}) \) the set of configurations in \( \mathcal{U}(O^i_{\theta_c}, \mathcal{M}_{0_i}) \) where:
\[
\mathcal{C}(O^i_{\theta}, \mathcal{M}_{0}) = \{ C \mid C = \text{Min}C(O^i_{\theta}, \mathcal{M}_{0}) \circ e_{i_1} \ldots \circ e_{i_k}, \land \phi(e_{i_q}) \in T_{\text{loc}}, q_i = 1, \ldots, k_i \}
\]

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

\[
\mathcal{E}(O^i_{\theta}, \mathcal{M}_{0}) = \{ \sigma \mid \sigma \in \langle \mathcal{E}(O^i_{\theta}, \mathcal{M}_{0}) \rangle \}
\]

Finally let \( \mathcal{C}(O^i_{\theta}, \mathcal{M}_{0}), \mathcal{L}(O^i_{\theta}, \mathcal{M}_{0}) \) and \( \mathcal{M}(O^i_{\theta}, \mathcal{M}_{0}) \) 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 \( O^i_{\theta} \) and the set of (minimal) assumptions \( \mathcal{M}_{0} \) on the marking of the input places \( P_{I N} \):

\[
\mathcal{C}(O^i_{\theta}, \mathcal{M}_{0}) = \{ \mathcal{C}(O^i_{\theta}, \mathcal{M}_{0}) \mid \mathcal{M}_{0} \in \mathcal{M}_{0} \} \tag{8}
\]

\[
\mathcal{E}(O^i_{\theta}, \mathcal{M}_{0}) = \{ \phi(\mathcal{E}(O^i_{\theta}, \mathcal{M}_{0})) \mid \mathcal{C}(O^i_{\theta}, \mathcal{M}_{0}) \in \mathcal{C}(O^i_{\theta}, \mathcal{M}_{0}) \} \tag{9}
\]

\[
\mathcal{M}(O^i_{\theta}, \mathcal{M}_{0}) = \{ \phi(\text{Max}(C(O^i_{\theta}, \mathcal{M}_{0})) \mid C(O^i_{\theta}, \mathcal{M}_{0}) \in C(O^i_{\theta}, \mathcal{M}_{0}) \} \tag{10}
\]

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

\[
\mathcal{PLD}_i(O^i_{\theta}) = \{ \tau_{i} \mid \tau_{i} = \Pi_{T_i} \tau_{i} \lor \tau_{i} \in \mathcal{L}(O^i_{\theta}, \mathcal{M}_{0}) \} \tag{11}
\]

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 \( O^2_{\theta} = t_{10} \). The reverse unfolding of \( O^2_{\theta} \) is displayed in Fig. 6 where \( \mathcal{U}_2(O^2_{\theta}) \) comprises two configurations: \( \mathcal{C}_2(O^2_{\theta}) = \{ C_{12}, C_{22} \} \). Notice that \( C_{12} \) contains the assumption on the border condition \( b_5 \) while \( C_{22} \) has not any assumption on the border conditions. Then for \( \text{Min}C_{12} \equiv \mathcal{C}_{12} \) we present in Fig. 7 the forward extensions of \( \text{Min}C_{12} \), where \( \text{Min}C_{12} \subseteq C_{12} \subseteq C_{22} \).

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 \( O^1_{\theta} = t_6 \). \( \mathcal{U}_1(O^1_{\theta}) \) is displayed in Fig. 8. Then for \( \text{Min}C_{11} \equiv \mathcal{C}_{11} \) we present in Fig. 8 the forward extensions of \( \text{Min}C_{11} \), where \( \text{Min}C_{11} \subseteq C_{11} \).
7.3 Procedure for information exchange

In what follows we restrict the presentation considering a minimal configuration $\text{Min}C_i \in \text{Min}\mathcal{C}(\mathcal{O}_{b_i}, \mathcal{M}_0)$. Thus $\text{Min}C_i = (\text{Min}B_i, \text{Min}E_i, \preceq)$ requires the border conditions represented by $\text{Min}B_{1N}$, $(\phi(\text{Min}B_{1N}) = \mathcal{M}_{1N})$ must be satisfied. Notice that we have $\forall b_{1N} \in \text{Min}B_{1N}, \exists \emptyset \in \text{Min}E_i$ s.t. $\phi(\emptyset) \in \phi^{-1}(\mathcal{O}_{b_i}) \land b_{1N} \preceq \emptyset_i$.

Denote $E_i = \{e_i \mid e_i \in \text{Min}E_i \cap \phi(\mathcal{O}_{b_i})\}$ the set of nodes of $C_i$ that correspond to the observed events in $\mathcal{O}_{b_i}$. Given a configuration $C_i \in \mathcal{C}(\mathcal{O}_{b_i}, \mathcal{M}_0)$ (Min$C_i \subseteq C_i$) denote $Y_i(C_i) = \text{Min}C_i \cup B_{1N} \cup E_i \cup B_{OUT}$ the set of nodes of $C_i$ that corresponds to either the places marked by $M_0$ (Min($C_i$)) or to the input places $p_i \in \mathcal{P}_{IN}$ ($B_{IN}$) or to the output places $p_i \in \mathcal{P}_{OUT}$ ($B_{OUT}$) or to the observed transitions ($E_i$).

Denote $\Pi_Y C_i$ the isotope map of $C_i$ onto the set of nodes $Y(C_i)$, $\Pi_Y C_i : B_i \cup E_i \rightarrow Y_i$ that is the projection of one graph onto a subset of nodes by preserving the order relation between the nodes:

$$\forall x_i, y_i \in Y_i \text{ if } x_i \sim_i y_i \text{ then } \Pi_Y x_i \sim \Pi_Y y_i \text{ where } \sim = \{\preceq_i, ||\}$$

Denote for simplicity $\Pi_Y C_i$ by $C_Y$. Then $C_Y$ represent the causality between the input nodes ($B_{IN}$), the output nodes ($B_{OUT}$), the observations ($E_i$), and the local initial marking (Min($C_i$)).

Then for $b_{1N} \in B_{IN}$, denote $E_i(b_{1N}) = \{e_i \in E_i \mid b_{1N} \in [(e_i)]\}$ that is the set of nodes in $C_i$ that correspond to observed events that have $b_{1N}$ as a "cause" (predecessor). Then the time $b_{1N}$ "must have been satisfied" (a token must have entered $N_i$ via $p_i = \phi(b_{1N})$) is:

$$\theta_{b_{1N}} \leq \min_{e_i \in \theta_{b_{1N}}} c_i \in E_i(b_{1N}) \quad (12)$$

Thus to each border condition $b_{1N}$, we can associate a temporal constraint of the form given by Eq. 12. For simplifying the notation denote $b_{1N}^b$ for $b_{1N} \in B_{1N}$:
Algorithm 3 Preliminary Local Calculation (Agk considered)

**Input:** C'i(Oi', M0k)

**Output:** C'i(Oi', M0k); PLD(Oi')

1. C'i(Oi', M0k) = \emptyset, L'(Oi', M0k) = \emptyset
2. B_Unfold(Oi') {calculate U(i)(Oi')}
3. calculate MinC(Oi')
4. for all MinCi \in MinC(Oi') do
5. calculate C'i(Oi', M0k) {the unobservable extensions of MinCi}
6. C'i(Oi', M0k) = C'i(Oi', M0k) \cup C'i(Oi', M0k)
7. end for
8. for all Ci \in C'i(Oi', M0k) do
9. L'(Oi', M0k) = L'(Oi', M0k) \cup \phi(Ei)
10. end for
11. PLD(Oi') = H_{TF} L'(Oi', M0k)

\[ \theta_{b_{IN_i}} \leq \min_{\theta_{b_{IN_i}}} \theta_{b_{IN_i}} \] 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 \subseteq C_i) is allowable can be expressed as a conjunction of temporal conditions on the border places:

\[ \text{MinB}_{IN_i}^\theta = \bigwedge_{b_{IN_i} \in B_{IN_i}} b_{IN_i}^\theta \] (13)

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

First consider the local initial marking M_{0i} 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}, 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:

\[ \theta_{b_{OUT_i}} \geq \max_{\theta_{x_i}, \theta_{x_i}} x_i \in [b_{OUT_i}^\theta] \cap Y_i \] (14)
Similarly denote the timing constraint given by Eq. 14 by $b^\theta_{OUT}$. Notice that
$b^\theta_{OUT}$ is the earliest global time a token could have exited $N_i$ given $B^\theta_i$, satisfied
while $b_{IN}$ is the latest global time a token must have entered $N_i$.

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:

$$B^\theta_{OUT} = \bigwedge_{b^\theta_{OUT} \in B^\theta_{OUT}} b^\theta_{OUT} \quad (15)$$

Hence for each minimal configuration $MinC_i \in MinC(O_i, \mu_0)$ and for each
unobservable extension $C_i$ of $MinC_i$, $A_{Gi}$ derives $B^\theta_i$, and $B^\theta_{OUT}$ (see Eq. 13 and
Eq. 15 respectively). Notice that for a configuration $C_i$ s.t. $MinC_i \subseteq C_i$ we have
that $MinB^\theta_{IN} = B^\theta_{IN}$.

Denote by $B^\theta_{OUT}$ the set of output border constraints derived for all the unob-
servable continuations (extensions) of $MinC_i$:

$$B^\theta_{OUT} = \{ b^\theta_{OUT} \mid MinC_i \subseteq C_i \}$$

Denote $(B^\theta_{OUT}, \preceq)$ the partial order relation defined as follows:

$$\forall B^\theta_{OUT}, B'^\theta_{OUT} \in B^\theta_{OUT} : B'^\theta_{OUT} \preceq B^\theta_{OUT} \iff \forall b^\theta_{OUT}, \in B^\theta_{OUT} : b^\theta_{OUT} \in B'^\theta_{OUT}$$

Denote $\max_{\preceq}(B^\theta_{OUT})$ the maximal elements of $B^\theta_{OUT}$ w.r.t. $\preceq$. Then the minimal
information that $A_{Gi}$ should send to its neighboring agents is:

$$\mathcal{M}G_i = \{(MinB^\theta_{IN}, B^\theta_{OUT}) \mid MinC_i \in \mathcal{M}(O_i, \mu_0) \land B^\theta_{OUT} \in \max_{\preceq}(B^\theta_{OUT})\} \quad (16)$$
Since a local agent does not know the models of the neighboring agents but only the set of input and output places \((\mathcal{P}_{IN}, \mathcal{P}_{OUT})\) the message that is sent by \(Ag_i\) to its neighbor \(Ag_j\) comprises only information about their common border-places \(\mathcal{P}_{ij} = \mathcal{P}_{IN,j} \cup \mathcal{P}_{OUT,j}\):

\[
\mathcal{MSG}_{i \rightarrow j} = \left\{ (\text{Min}B^\theta_{IN,i}, B^\theta_{OUT,i}) \mid \text{Min}C_i \in \mathcal{M}(O^i_{\theta_i}; M^i_{\theta_i}) \land B^\theta_{OUT,i} \in \text{Max}_\mathcal{M}(B^\theta_{OUT,i}) \right\}
\]

where

\[
\text{Min}B^\theta_{IN,i} = \bigwedge_{\theta_{IN,i} \in B^\theta_{IN,i}} \theta_{IN,i} \quad \text{and} \quad B^\theta_{OUT,j} = \bigwedge_{\theta_{OUT,j} \in B^\theta_{OUT,j}} \theta_{OUT,j}
\]

(17)

(18)

**Remark 4** The reason \(Ag_i\) selects only the maximal elements of \(B^\theta_{OUT,i}\) to send them to its neighbors is as follows. The minimal requirement \(\text{Min}B^\theta_{IN,i}\) is common to all the unobservable continuations of \(\text{Min}C_i\) thus if \(\text{Min}B^\theta_{IN,i}\) will not be satisfied then all the configuration that are extensions of \(\text{Min}C_i\) can be discarded. Otherwise if \(\text{Min}B^\theta_{IN,i}\) can be satisfied there is enough to send to neighbors only the maximal (w.r.t. \(\leq\)) border conditions. This is because if what can be maximally provided \(B^\theta_{OUT,i} \in \text{Max}_\mathcal{M}(B^\theta_{OUT,i})\) is enough for satisfying the minimal requirement \(\text{Min}B^\theta_{IN,i}\) derived by \(Ag_i\) for \(\text{Min}C_j\) 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 \(\text{Max}_\mathcal{M}(B^\theta_{OUT,i})\) then it is obvious that would have been useless to send information about the rest of the non-maximal elements of \(B^\theta_{OUT,i}\).

**Algorithm 4** Communication exchange (\(Ag_i\) considered)

**Input:** \(\mathcal{C}(O^i_{\theta_i}; M^i_{\theta_i})\)

**Output:** \(\mathcal{MSG}_i; \mathcal{MSG}_{i \rightarrow j}\)

1. **for all** \(C_i \in C_i\) **do**
2. calculate \(C^\theta_i\)
3. calculate \(B^\theta_{IN,i}\) \(\{\text{see Eq. 13}\}\)
4. calculate \(B^\theta_{OUT,i}\) \(\{\text{see Eq. 14}\}\)
5. calculate \(\text{Max}_\mathcal{M}(B^\theta_{OUT,i})\)
6. **end for**
7. calculate \(\mathcal{MSG}_i\) \(\{\text{see Eq. 16}\}\)
8. **for all** neighboring agents \(Ag_j\) **do**
9. calculate \(\mathcal{MSG}_{i \rightarrow j}\) \(\{\text{see Eq. 17}\}\)
10. **end for**

**Example 4** Consider again the case of \(Ag_2\) observing \(C^\theta_{\theta_2} = t_{10}\). In Fig. 7 we have that \(\text{Min}C_{t_1} \subseteq C_{t_1} \subseteq C_{t_2}\). Then for \(C_{t_2}\) we have that \(B_{IN_2} = \{\theta_{0}^2\} \) with \(\theta_{0}^2 \leq \theta_{t_{10}}\) and \(B_{OUT_2} = \{\theta_{0}^2, \theta_{0}^3, \theta_{0}^4\} \) with \(\theta_{0}^3 \geq \theta_{0}, \theta_{0}^4 \geq \theta_{t_{10}}\) and \(\theta_{0}^4 \geq \theta_{t_{10}}\). Thus \((B_{IN_2}, B_{OUT_2})\) is part of the message that will be sent to \(Ag_i\).

**7.4 Procedure for updating a local calculation**

Consider in this section that having received the local observation \(O^i_{\theta_i}\), the agent \(Ag_i\) has derived the preliminary local calculation of local site model \(\mathcal{N}_i\) \((\mathcal{M}_{\theta_i}, \text{Min}C(O^i_{\theta_i}; M^i_{\theta_i}), \mathcal{C}(O^i_{\theta_i}; M^i_{\theta_i}))\) and then has received the message \(\mathcal{MSG}_{j \rightarrow i}\) sent by \(Ag_j\) based on a similar preliminary computation of site \(j\).
In this section we present how $A_{ii}$ updates its preliminary local calculation by taking into account the received information $\mathcal{MSG}_{j \rightarrow i}$. To simplify the presentation consider:

1. an arbitrary minimal configuration $\text{MinC}_i \in \text{MinC}(O^i_\theta, \bar{A}^i_\theta)$,
2. the set of unobservable continuations (extensions) $\bar{C}_i$ of $\text{MinC}_i$,
3. an arbitrary minimal configuration $\text{MinC}_j \in \text{MinC}(O^j_\theta, \bar{A}^j_\theta)$,
4. the set of unobservable continuations (extensions) $\bar{C}_j$ of $\text{MinC}_j$,
5. and the information $\mathcal{MSG}'_{j \rightarrow i} \subseteq \mathcal{MSG}_{j \rightarrow i}$ that is received by $A_{ii}$ regarding $\text{MinC}_j$ and $\bar{C}_j$ ($\mathcal{MSG}'_{j \rightarrow i} = \{(B_{IN_{ij}}, B_{OUT_{ij}}) \mid B_{OUT_{ij}} \in \text{Max}_{\varepsilon}(B_{OUT_{ij}})\}$)

Thus in what follows we present how $A_{ii}$ processes $\mathcal{MSG}'_{j \rightarrow i}$ for updating $\text{MinC}_i$ and $\bar{C}_i$. Since the elements of $\mathcal{MSG}'_{j \rightarrow i}$ are distinct we present in following the update $A_{ii}$ makes, considering only $(B^\theta_{IN_{ij}}, B^\theta_{OUT_{ij}}) \in \mathcal{MSG}'_{j \rightarrow i}$.

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

Since $\text{MinC}_i$ and its unobservable extensions $\bar{C}_i$ depend on the set of hypothesis $B^\theta_{IN_{ij}}$ that should be satisfied it means that $A_{ii}$ interprets the local results by considering the information sent by $A_{ij}$.

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

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

$$\psi_i(b^\theta_{IN_{ij}}) = \begin{cases} b^\theta_{OUT_{ij}} & \text{if } \theta_{b^\theta_{OUT_{ij}}} \leq \theta_{b^\theta_{IN_{ij}}} \\
\varepsilon & \text{or } \varepsilon \end{cases}$$

and for $b^\theta_{IN_{ij}} \neq b^\theta_{IN_{ij}}$, $\psi_i(b^\theta_{IN_{ij}}) = \psi_i(b^\theta_{IN_{ij}}) \Rightarrow \psi_i(b^\theta_{IN_{ij}}) = \varepsilon$. Similarly define $\psi_j : B^\theta_{IN_{ij}} \rightarrow B^\theta_{OUT_{ij}} \cup \{\varepsilon\}$. Then denote by $\psi_{ij} = (\psi_i, \psi_j)$ the interpretation function of the common place marking and by $\Psi_{ij}$ the entire set of interpretation functions.

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

$$B^\theta_{IN_{ij}} = \{b^\theta_{IN_{ij}} \in B^\theta_{IN_{ij}} \land \psi_i(b^\theta_{IN_{ij}}) = b^\theta_{OUT_{ij}}\}$$

Then denote by $B^\theta_{IN_{ij}}$ the set of input border conditions that were not-assigned to determined conditions:

$$B^\theta_{IN_{ij}} = \{b^\theta_{IN_{ij}} \in B^\theta_{IN_{ij}} \land \psi_i(b^\theta_{IN_{ij}}) = \varepsilon\}$$

and denote by $B^\theta_{IN_{ij}}$ the set of new input border conditions that can be provided by site $j$ under the interpretation $\psi_i$:

$$B^\theta_{IN_{ij}} = \{b^\theta_{IN_{ij}} \in B^\theta_{IN_{ij}} \land b^\theta_{OUT_{ij}} \in B^\theta_{OUT_{ij}} \setminus \psi_i^{-1}(B^\theta_{IN_{ij}})\}$$

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

$$B^\theta_{IN_{ij}} = B^\theta_{IN_{ij}} \cup B^\theta_{IN_{ij}} \cup B^\theta_{IN_{ij}}$$
Definition 25 Consider an input-border condition \( b_{ij}^{\psi_i} \in B_{IN_{ij}}^{\psi_i} \) under the assignment \( \psi_{ij} = (\psi_1, \psi_2), \psi_{ij} \in \Psi_{ij} \). Then we say that:

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

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

![Diagram](image-url)

Fig. 10.

Example 5 Consider two configurations \( C_1 \) and \( C_2 \). As presented in Example 4 the message sent by \( A_{g2} \) to \( A_1 \) regarding \( C_2 \) is \((B_{IN_2}, B_{OUT_2})\). Now having observed \( O_{b_2} = t_6 \), \( A_1 \) has preliminary derived for \( C_1 \), \( B_{IN_1} = \{b_6^{\theta_1}\} \) with \( \theta_{b_6} \leq \theta_{c_6} \) and \( B_{OUT_1} = \{b_6^{\theta_1}, b_{b_6}^{\theta_2}\} \) with \( \theta_{b_6} \geq \theta_{c_6} \) and \( \theta_{b_{b_6}} \geq \theta_{\text{start}} \). Recall that for \( C_2 \) we have \( B_{IN_2} = \{b_6^{\theta_2}\} \) with \( \theta_{b_6} \leq \theta_{c_6} \) and \( B_{OUT_2} = \{b_6^{\theta_2}, b_{b_6}^{\theta_3}, b_{b_{b_6}}^{\theta_4}\} \) with \( \theta_{b_6} \geq \theta_{b_{b_6}}, \theta_{b_{b_6}} \geq \theta_{c_6} \) and \( \theta_{b_{b_{b_6}}} \geq \theta_{\text{start}} \).

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

\[
\psi_{12} = \begin{cases} 
\theta_{b_6}^{\theta_1} \rightarrow \theta_{b_6}^{\theta_2} & \theta_{\text{start}} \leq \theta_{b_{b_6}} \leq \theta_{c_6} \\
\theta_{b_6}^{\theta_2} \rightarrow \theta_{b_{b_6}}^{\theta_3} & \theta_{c_6} \leq \theta_{b_{b_6}}^{\theta_3} \\
\theta_{b_6}^{\theta_3} \rightarrow \theta_{b_{b_{b_6}}}^{\theta_4} & \theta_{b_{b_6}}^{\theta_3} \leq \theta_{c_6} \\
\theta_{b_6}^{\theta_4} \rightarrow \theta_{b_{b_{b_{b_6}}}}^{\theta_5} & \theta_{b_{b_{b_6}}}^{\theta_4} \leq \theta_{\text{start}} \\
\theta_{b_6}^{\theta_5} \rightarrow \theta_{b_{b_{b_{b_{b_6}}}}}^{\theta_6} & \theta_{b_{b_{b_{b_6}}}}^{\theta_5} \leq \theta_{\text{start}} 
\end{cases}
\]  

(21)
\[
\psi_{12}^2 = \begin{cases}
\frac{b_0}{b_{0_2}} \xrightarrow{\psi_1} \frac{b_{0_2}}{b_{0_2}} \quad \theta_{b_{0_2}} \leq \theta_{e_1} \\
\frac{b_{0_1}}{b_{0_2}} \xrightarrow{\psi_2} \frac{b_{0_2}}{b_{0_1}} \quad \theta_{\text{start}} \leq \theta_{b_{0_1}} \leq \theta_{e_1} \\
\frac{b_{0}}{b_{0_1}} \xrightarrow{\psi_2} \frac{b_{0_1}}{b_{0_1}} \quad \theta_{e_0} \leq \theta_{b_{0_1}} \\
\frac{b_{0_1}}{b_{0_1}} \xrightarrow{\psi_2} \frac{b_{0_1}}{b_{0_1}} \quad \theta_{b_{0_1}} \leq \theta_{b_{0_1}} \\
\frac{b_{0_1}}{b_{0_1}} \xrightarrow{\psi_2} \frac{b_{0_1}}{b_{0_1}} \quad \theta_{\text{start}} \leq \theta_{b_{0_1}} \leq \theta_{e_1}
\end{cases}
\] (22)

and so on. Notice that \((C_1, C_2, \psi_1^1)\), is consistent while \((C_1, C_2, \psi_2^1)\) it is not. This is because the border condition \(b_{0_2}^0\) is not used for satisfying \(b_{0_2}^0\) (\(b_{0_2}^0\) 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 \(\psi_{1,2}'\) by assigning \(b_{0_1}^0 \xrightarrow{\psi_1} b_{0_2}^0\) and \(b_{0_2}^0 \xrightarrow{\psi_2} b_{0_1}^0\) 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 \(\mathbb{B}_{IN_{ij}} = \emptyset\) and \(\mathbb{B}_{IN_{ij}} = \emptyset\).

**Definition 27** Given a tuple \(C_1, \ldots, C_{|\mathcal{I}|}\) of local configurations then \((C_1, \ldots, C_{|\mathcal{I}|})\) is globally consistent if \(\forall i, j \in \mathcal{I}, i \neq j\) there is an interpretation function \(\psi_{ij}\), 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 \(\psi_{ij}\), if either \(\mathbb{B}_{IN_{ij}} \neq \emptyset\) or \(\mathbb{B}_{IN_{ij}} \neq \emptyset\) then \((C_i(\psi_{ij}), C_j(\psi_{ij}))\) is extendable.

The interpretation of \(C_i\) under the assignment \(\psi_{ij}\) \((C_i(\psi_{ij}))\) 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 \(\mathbb{B}_{IN_{ij}}\) represents the new tokens that could have entered \(N_i\). 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 \(C_i(\psi_{ij})\) the set of configurations that can be obtained from \(C_i\) considering the interpretation function \(\psi_{ij}\) and all its maximal unobservable extensions. The let \(\Delta(C_i(\psi_{ij})) = C_i(\psi_{ij}) \setminus C_i\) the local update of \(C_i\).

Similarly with what has been presented above \(A_{gi}\) derives first the local update \(\Delta(C_i(O_{bi}, M_{bi}, MSG_{j-i})\) of the local calculation \(C_i(O_{bi}, M_{bi})\) given the received message \(MSG_{j-i}\) (Update Local Calculation below). Then based on the local update \(\Delta(C_i(O_{bi}, M_{bi}, MSG_{j-i})\) \(A_{gi}\) derives the update of the information to be exchanged \(\Delta(MSG_{j})\).

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 $\text{Local Calculation (Ag)}$ considered

Input: $\mathcal{O}(i, j, \mathcal{M}_0)$, $\mathcal{M}_j, \mathcal{M}_{j+1}$
Output: $\Delta(\mathcal{O}(i, j, \mathcal{M}_0), \mathcal{M}_j, \mathcal{M}_{j+1})$

1. $\Delta(\mathcal{O}(i, j, \mathcal{M}_0), \mathcal{M}_j, \mathcal{M}_{j+1}) = \emptyset$
2. $\mathcal{L}^{\text{gcon}}(\mathcal{O}(i, j, \mathcal{M}_0)) = \emptyset$
3. for all $\mathcal{C}_i \in \mathcal{C}(\mathcal{O}(i, j, \mathcal{M}_0))$
   4. for all $(B_{IN_{ji}}, B_{OUT_{ji}}) \in \mathcal{M}_j$
   5. for all $\psi_{ji} \in \Psi_{ji}$
   6. if $(C_i, C_j, \psi_{ji})$ - globally consistent then
   7. $\mathcal{C}^{gcon}_i(C_i, \mathcal{M}_0) = \mathcal{C}^{gcon}_i(\mathcal{O}(i, j, \mathcal{M}_0)) \cup (\ldots, C_i(\psi_{ji}), \ldots, C_j(\psi_{ji}), \ldots)$
   8. else if $(C_i, \psi_{ji})$ - extendable then
   9. calculate $\Delta(C_i(\psi_{ji}))$ (extend $C^{gcon}_{ij} \in \Delta(C_i(\psi_{ji}))$ by using $B_{IN_{ji}}^{new, \psi_{ji}} \not= \emptyset$
10. $\Delta(\mathcal{C}(\mathcal{O}(i, j, \mathcal{M}_0), \mathcal{M}_j, \mathcal{M}_{j+1}) = \Delta(\mathcal{C}(\mathcal{O}(i, j, \mathcal{M}_0), \mathcal{M}_j, \mathcal{M}_{j+1}) \cup \Delta(C_i(\psi_{ji}))$
11. end if
12. end for
13. end for
14. end for
15. for all $\mathcal{C}_i \in \Delta(\mathcal{C}(\mathcal{O}(i, j, \mathcal{M}_0)))$
16. $\Delta L_i(\mathcal{O}(i, j, \mathcal{M}_0)) = \mathcal{L}(\mathcal{O}(i, j, \mathcal{M}_0)) \cup \phi(E_i)$
17. if $\mathcal{C}_i$ globally consistent then
18. $\Delta L^{gcon}(\mathcal{O}(i, j, \mathcal{M}_0)) = \Delta L^{gcon}(\mathcal{O}(i, j, \mathcal{M}_0)) \cup \Delta \mathcal{L}(\mathcal{O}(i, j, \mathcal{M}_0))$
19. end if
20. end for
21. $\mathcal{PCLD}(\mathcal{O}(i, j, \mathcal{M}_0)) = \mathcal{PCLD}(\mathcal{O}(i, j, \mathcal{M}_0)) \cup \mathcal{H}_{TP}(\Delta \mathcal{L}(\mathcal{O}(i, j, \mathcal{M}_0)))$
22. $\mathcal{PCLD}^{\text{gcon}}(\mathcal{O}(i, j, \mathcal{M}_0)) = \mathcal{PCLD}^{\text{gcon}}(\mathcal{O}(i, j, \mathcal{M}_0)) \cup \mathcal{H}_{TP}(\Delta \mathcal{L}^{gcon}(\mathcal{O}(i, j, \mathcal{M}_0)))$

Now for $p_{ij}$ denote by $c^p_{ij}$ and $c^q_{ij}$ how many times an unobservable oriented path $\phi$ that starts in $p_i$ crosses $\mathcal{P}_i \setminus \mathcal{P}_{ij}$ and $\mathcal{P}_j \setminus \mathcal{P}_{ij}$ respectively. Let $c_{ij} = \max(c^p_{ij}, c^q_{ij})$ and denote $K_c = \max_{\phi \in N_i}(c_{ij})$ $(N_i = N_i \cup N_j)$. If $\exists \phi \in N_{ij}$ s.t. $\phi$ is an unc 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 $\mathcal{O}_{\theta_c} = \mathcal{O}_{\theta_c} \otimes^g_c \mathcal{O}_{\theta_c}$. Then the global consistent local diagnosis $\mathcal{PCLD}^{gcon}$ derived by the $d$-agent $Ag_d$ at the time $\theta_c$ after the $k^{th}$ communication round by running the algorithm $DD\text{Algo}_2$ is such that:

i) if $K_c$ is finite then after $k \geq K_c$ communication rounds, the consistent local diagnosis result $\mathcal{PCLD}^{gcon}(\mathcal{O}_{\theta_c})$ recovers the centralized diagnosis result of site $i$: $\mathcal{PCLD}^{gcon}(\mathcal{O}_{\theta_c}) = \mathcal{D}_i(\mathcal{O}_{\theta_c})$

ii) if $K_c$ is infinite then $\exists_{k_{max} \in \mathbb{N}^+}$ finite s.t. after $k \geq k_{max}$ communication rounds $\mathcal{PCLD}^{gcon}(\mathcal{O}_{\theta_c}) = D_i(\mathcal{O}_{\theta_c})$ 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 proof that the computation of $\mathcal{PCLD}^{gcon}(\mathcal{O}_{\theta_c})$ 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 $DD\text{Algo}$ terminates after finitely many communication rounds relies on the assumption that the PN
models are structurally bounded (see viii) in setting). It means that $\mathcal{L}_N(M_0 \cup \epsilon_I \bigcup_{M_{Ic}})$ is finite and is recovered by $Ag_i$ and $Ag_j$ by distributed calculations. Then since $\mathcal{L}_N(M_0) \subseteq \mathcal{L}_N(M_0 \cup \epsilon_I \bigcup_{M_{Ic}})$ it results that for any observation $O_{b_i}$ there is a $\mathcal{L}_N(M_0 \cup \epsilon_I \bigcup_{M_{Ic}}, O_{b_i})$. Then we have that $H_T, \mathcal{L}_N(O_{b_i}) \subseteq H_T, \mathcal{L}_N(O_{b_i})$. While $\mathcal{L}_N(O_{b_i})$ is trivial. The result is proved straightforward by projecting equal set onto the local set of faulty transitions $T_{f_i}$.

Then for i) the proof that $DD_{Algo}$ terminates in $k < K_c$ 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 a loop (unc) that comprises places and only unobservable transitions in both $N_i$ and $N_j$. 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 ($|I| > 2$). 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 $DD_{Algo}$ below 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. $Ag_{j1}$) and the less accessed agent ($Ag_{j2}$) 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 $O_{b_i} = \otimes_{i \in I} O_{b_i}^i$ the algorithm $DD_{Algo}$ terminates in finite time and the local diagnosis $PD_{i}^{com}(O_{b_i})$ 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 $O_{b_i}$ and the knowledge of the overall plant.

$$\forall i \in I, \quad D_i(O_{b_i}) = PD_{i}^{com}(O_{b_i})$$

**Proof.** The proof is similar with the proof of Theorem 1 and it relies on structurally boundness assumption see viii) that implies that $\mathcal{L}_N(M_0 \cup \epsilon_I \bigcup_{M_{Ic}})$ is finite. Thus the algorithm terminates after a finite number of communication rounds.
### Algorithm 7 $DD_{\text{Alg}} (A_g)$ considered

**Input:** $N; M_f; O_{x_e}$  
**Output:** $D_i(O_{x_e})$

1. **for all** neighbor $A_{gj}$ **do**
2. $n_{\text{com}}(i, j) = 0$ [initialize communication counter]
3. **end for**
4. **while** global\_stop=true **do**
5. **if** $M_{S_g} = \emptyset$ **then**
6. local\_stop=true
7. **else** if $M_{S_g} \neq \emptyset$ **then**
8. choose a neighbor $A_{gj}$ s.t. $\forall j_1, j_2 : |n_{\text{com}}(i, j_1) - n_{\text{com}}(i, j_2)| \leq N_{\text{com}}$
9. $n_{\text{com}}(i, j) = n_{\text{com}}(i, j) + 1$
10. $DD_{\text{Alg}}(A_{gj})$
11. **end if**
12. **end while**
13. $D_i(O_{x_e}) = PLD^{f_{\text{com}}}(O_{x_e})$

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 $M_f$ in 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 $\omega$-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 $K_e \leq 2$) 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

4. R. K. Boel and G. Jiroueku Distributed Contextual Diagnosis for very large systems - WODES, Reims, France, 2004
6. A. Campolini, P. Mello and S. Storani Distributed Medical Diagnosis with abductive logic agents - ECAI, Lyon, France, 2002
14. S. Gené and S. Lafortune A distributed algorithm for on-line diagnosis of place-bounded Petri Nets - IFAC Congress, Prague, 2005
16. A. Gui and X. Xie Control of safe ordinary Petri nets with marking specifications using unfoldings WODES’04, Reims, France, 2004
18. S. McIlraith Explanatory diagnosis: Conjecturing actions to explain observation - 6th Int. Conf. on Principles of Knowledge Representation and Reasoning, 1998
27. R. Su and W.M. Wonham A model of component consistency in distributed diagnosis WODES, Reims, France, 2004
29. A. Valinari Compositional analysis with place-bounded subsets LNCS 815, 1994