Preprints of the 7th IFAC Symposium on
Fault Detection, Supervision and Safety of Technical Processes
Barcelona, Spain, June 30 - July 3, 2009

On fault diagnosis of random free-choice Petri nets

Jana Flochova * **Rene K. Boel** **

* *FIIT STU, Ilkovicova 13, Bratislava, Slovakia, (e-mail: jana.flochova@stuba.sk)*
** *SYSTeMS, EESA Department, Ghent University, Technologiepark 913, B-9052 Zwijnaarde, Belgium, (e-mail: rene.boel@ugent.be)*

Abstract: This paper presents an on-line diagnosis algorithm for Petri nets where a priori probabilistic knowledge about the plant operation is available. We follow the method developed by Benveniste, Fabre, and Haar to assign probabilities to configurations in a net unfolding thus avoiding the need for randomizing all concurrent interleavings of transitions. We consider different settings of the diagnosis problem, including estimating the likelihood that a fault may have happened prior to the most recent observed event, the likelihood that a fault will have happened prior to the next observed event. A novel problem formulation treated in this paper considers deterministic diagnosis of faults that occurred prior to the most recent observed event, and simultaneous calculation of the likelihood that a fault will occur prior to the next observed event.

1. INTRODUCTION

In this paper we derive an on-line diagnosis algorithm for Petri nets (PNs) where a priori probabilistic knowledge about the plant operation is available. We consider the plant model described by a free-choice PN. The plant observation is given by a subset of events - transitions whose occurrence is reported without delay. Other transitions are silent and unobservable. Some unobservable transitions represent faults. The model-based diagnosis for PNs requires to detect the occurrence of a fault transition based on the model and the on-line observation generated by the plant. First the set of traces that are legal from the initial marking and that are compatible with the received observation is derived and then the diagnosis result of the plant is obtained by checking whether some or all of the legal traces include fault transitions. Having probabilistic information about the execution of the transitions in the model we extend the diagnosis algorithm to distinguish between faults whose occurrence is likely or unlikely.

A variety of diagnosis approaches analyzing the plant model under partial observations have been proposed based on the type and level of details chosen for the system models and on the kind of faults to be diagnosed. The notion of diagnosability has been defined e.g. in M. Sampath et al. [1995]. Deterministic and stochastic finite-automata models are used in Thorsley and Theneketzis [2005], Wang et al. [2004], deterministic Petri nets e.g. in Benveniste et al. [2003], Haar [2003], Boel and Jiroveanu [2004], Giua and Seatzu [2005], Jiroveanu [2006], Genc and Lafortune [2007], Jiroveanu et al. [2008], partially stochastic Petri nets in Aghasaryan et al. [1998], and timed Petri nets in Jiroveanu et al. [2006].

Adding probabilities to this deterministic setting has two main advantages. First it allows incorporating some statistical knowledge on the loss or masking of alarms or on the occurrence of faults based on past experience in monitoring the plant. Secondly, it incorporates some smoothness in the fault net, and allows accounting for incomplete knowledge on the consequences of faults, or on the alarms they generate.

We follow the probabilistic method developed by Benveniste and coauthors (Benveniste et al. [2003], Aghasaryan et al. [1998], Benveniste et al. [2004], Abbes and Benveniste [2008]) to assign probabilities to configurations in a net unfolding thus avoiding the need for randomizing all concurrent interleavings of transitions. We consider different settings of the diagnosis problem, including estimating the likelihood that a fault may have happened prior to the most recent observed event, the likelihood that a fault will have happened prior to the next observed event; we also consider the following novel problem formulation of deterministically diagnosing faults that occurred prior to the most recent observed event, and simultaneously obtaining the likelihood that a fault will happen between the time of the most recent observed event and of the next observed event. This approach combines the deterministic diagnosis of faults that may have occurred in the past of Jiroveanu et al. [2008] with a probabilistic unfolding of future traces.

The paper is organized as follows. Section 2 introduces some basic notions of PNs. Section 3 defines the probabilistic Petri net under study, the diagnosis problems to be solved, and we show implementable algorithms for achieving this diagnosis. In section 4 we briefly discuss including of unreliable observations in our model, and we conclude in Section 5.

⋆ This paper presents research results of the Belgian Network DYSCO, funded by the IAP Programme, initiated by the Belgian State, Science Policy Office. The work of the first author was supported by the VEGA grants 1/0649/09, VG 1/0822/08 of the Slovak Grant Agency. The scientific responsibility rests with the authors

2. DEFINITIONS

We use the standard notation of Petri nets $\mathcal{N} = (\mathcal{P}, \mathcal{T}, F)$ where $\mathcal{P}$ denotes the set of places, $\mathcal{T}$ denotes the set of transitions, $F = Pre \cup Post$ is the incidence function, $Pre(p,t) : \mathcal{P} \times \mathcal{T} \to \{0,1\}$, and $Post(t,p) : \mathcal{T} \times \mathcal{P} \to \{0,1\}$ specify the arcs. M_0 denotes the initial marking. Denote by $\mathcal{L}_{\mathcal{N}}(M_0)$ the set of all legal traces of a PN $\langle \mathcal{N}, M_0 \rangle$, by $\mathcal{T}^*$ the Kleene closure of the set $\mathcal{T}$, by ϵ the empty string, by ${}^\bullet p$, $p^\bullet$ the set of input, output transitions of a place; ${}^\bullet t$ and $t^\bullet$ for the set of input, output places of a transition, and by $\preceq$, $\sharp$ and $\|$ the dependence, conflict, and concurrency relation of PN nodes. A trace τ of events belongs to the language $\mathcal{L}_{\mathcal{N}}(M_0)$ if $\tau = M_0 \xrightarrow{t_1} M_1 \xrightarrow{t_2} \ldots \xrightarrow{t_k} M_k$, $i = 1 \ldots k$, $M_{i-1} \geq Pre(t_i)$. The projection $\Pi_{\mathcal{T}'} : \mathcal{L}_{\mathcal{N}}(M_0) \to \mathcal{T}'^*$ is defined as: *i)* $\Pi_{\mathcal{T}'}(\epsilon) = \epsilon$; *ii)* $\Pi_{\mathcal{T}'}(t) = t$ if $t \in \mathcal{T}'$; *iii)* $\Pi_{\mathcal{T}'}(t) = \epsilon$ if $t \in \mathcal{T} \setminus \mathcal{T}'$; *iv)* $\Pi_{\mathcal{T}'}(\sigma t) = \Pi_{\mathcal{T}'}(\sigma)\Pi_{\mathcal{T}'}(t)$ for $\sigma \in \mathcal{L}_{\mathcal{N}}(M_0)$ and $t \in \mathcal{T}$.

A free choice Petri net is an ordinary Petri net such that every arc from a place is a unique incoming or a unique outgoing arc to a transition.

Definition 1. An occurrence net (Nielsen et al. [1981], Benveniste et al. [2003], J. Esparza et al. [1996]) is a net $O = (B, E, \preceq_1)$ such that:

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

B is referred to as the set of conditions, E the set of events, $\preceq_1$ the immediate dependence relation, and $\bullet b$ the set of input events of b.

Definition 2. A configuration $C = (B_C, E_C, \preceq)$ in the occurrence net O is a proper sub-set of O that is conflict free, i.e. $\forall a, b \in (B_C \cup E_C) \times (B_C \cup E_C) \Rightarrow \neg(a \sharp b)$ such that C is causally upward-closed, i.e. $\forall b \in B_C \cup E_C : a \in B \cup E$ and $a \preceq_1 b \Rightarrow a \in B_C \cup E_C$ and such that $\mathtt{min}_{\preceq}(C) = \mathtt{min}_{\preceq}(O)$

Definition 3. Consider a PN $\langle \mathcal{N}, M_0 \rangle$ s.t. $\forall p \in \mathcal{P} : M_0(p) \in \{0,1\}$. A branching process B of a PN $\langle \mathcal{N}, M_0 \rangle$ is a pair $B = (O, \phi)$ where O is an occurrence net and ϕ is a homomorphism $\phi : O \to \mathcal{N}$ s.t.:

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

For a configuration C in O denote by $CUT(C)$ the maximal (w.r.t. set inclusion) set of conditions in C that have no successors in C:

$$CUT(C) = \{e^\bullet \mid e \in E_C\} \cup \mathtt{min}_{\preceq}(O) \setminus \{{}^\bullet e \mid e \in E_C\}$$

There exists a unique maximum branching process that is the unfolding of $\langle \mathcal{N}, M_0 \rangle$ and is denoted $\mathcal{U}_{\mathcal{N}}(M_0)$.

Definition 4. (stopping prefix). A branching process $\mathcal{B} = (B, E, \preceq, \phi)$ is called a stopping prefix if it satisfies the following condition: $\forall b \in B$ s.t. $\phi(b) \in \mathcal{P}$, either $b^\bullet_{\mathcal{B}} = \emptyset$ or $b^\bullet_{\mathcal{B}} = b^\bullet$, where $b^\bullet_{\mathcal{B}}$ denotes the post set of condition b.

Given the set $\mathcal{C}$ of all configurations in $\mathcal{U}_{\mathcal{N}}(M_0)$. The set of string linearizations $\langle E_C \rangle_{\preceq} = \{\sigma = e_1 e_2 \ldots e_v \mid \forall e_\iota, e_\lambda \in E_C : e_\iota = e_\lambda$ then $\iota = \lambda$ and for $\iota \neq \lambda, e_\iota \preceq e_\lambda$ then $\iota < \lambda\}$.

3. PROBABILISTIC DIAGNOSIS BASED ON BACKWARD UNFOLDING

We consider dynamics of the PN that allows to model causal dependencies, concurrency and interleaving. Faults are considered to be a subset of the set of unobservable events. The following plant description is considered in Jiroveanu et al. [2008]:

(1) the PN model $\langle \mathcal{N}, M_0 \rangle$ is free-choice with the set of choice places $\mathcal{P}_c = \{p \in \mathcal{P} : p^\bullet > 1\}$
(2) $\mathcal{T} = \mathcal{T}_o \cup \mathcal{T}_{uo}$ where $\mathcal{T}_o$ is the set of observable events and $\mathcal{T}_{uo}$ is the set of unobservable (silent) events; the PN does not contain any unobservable cycle
(3) l_o is the observation labeling function $l_o : \mathcal{T} \to \Omega_o \cup \{\epsilon\}$ where Ω_o is a set of labels and ϵ is the empty label. $l_o(t) = \epsilon$ if $t \in \mathcal{T}_{uo}$ and $l_o(t) \in \Omega_o$ if $t \in \mathcal{T}_o$
(4) when an observable transition $t^o \in \mathcal{T}_o$ is executed in the plant the label $l_o(t^o)$ is emitted without delay; the execution of an unobservable event is silent
(5) the faults are unpredictable
(6) $\forall p \in \mathcal{P}_c$, $\forall p^\bullet \subseteq \mathcal{T}_o$ or $\forall p^\bullet \subseteq \mathcal{T}_{uo}$.

A minimal explanation of a given observed event $t_o \in \mathcal{T}_o$ minimal explanation is a linearization of a set of events, since there must exist a trace of firable events that executes these events and whose occurrence enables t_o to fire prior to any other observable event. But we are not interested (in fact we wants to avoid) in enumerating all possible interleaving of these events. One recursively searches backward explaining all observations computing the explanations and minimal markings that allow the execution of the observed sequences. The set of minimal explanations can be obtained running a backward unfolding algorithm (Jiroveanu et al. [2008]). The diagnosis of the occurrence of the fault in the past can be derived based on the set of minimal explanations, while the diagnosis of the faults in the past or in the future uses the set of all explanations of the received observation including unobservable reachable transitions after the observed event. In our approach we distinguish two cases:

(1) A stochastic analysis of faults that either occurred in the past or that may occur in the future prior to the next observed event occurrence so that the explanation only includes unobservable future events not belonging to the minimal explanations. (Flochova et al. [2007]);
(2) A deterministic analysis of faults that must have occurred in the past (Jiroveanu et al. [2008]) and a probabilistic analysis of faults that may occur in the future prior to the next observed event occurrence.

Let $\pi : \mathcal{T} \to (0,1]$ assign the probability for each set of choice transitions, where π satisfies:

$$\sum_{t \in p^\bullet} \pi(t) = 1 \tag{1}$$

The probability π can be extended to strings of transitions $\pi : \mathcal{T}^* \to (0,1]$:

$$\pi(\tau) = Prod_{t \in \Sigma_\tau} \pi(t) \tag{2}$$

In the global model the collection of probabilities of strings must be normalized. The diagnosis is usually performed in the following steps. First, the set of all possible traces that match the system description and observations are derived, and then it is checked whether these traces contain faulty transitions. We consider a diagnoser that knows the plant model. Using knowledge about the plant model the diagnoser constructs, as in Jiroveanu et al. [2008], the set of allowable sequences of events - further on called explanations - that contain the first observed event as only observable event, and then generates the set of possible states the plant can be in after observing the first observation. Recursively for each new observed event, the diagnoser derives the set of explanations of the last observed event by considering as initial state any one of the estimated states derived at the last step (after the previous observation). The diagnoser checks after each observation whether these explanations contain faulty transitions.

Given a PN $\mathcal{N} = (\mathcal{P}, \mathcal{T}, F)$ with initial marking M_0, let $t^o \in \mathcal{T}^o$ be the first observed event. Then minimal context of t^o $MinC(t^o)$=$\langle MinM,\ MinE\rangle$ where:

(1) $MinM \in \wp(M_o)$ ($MinM$ is the minimal marking)
(2) $MinE \in \mathcal{L}_{\mathcal{N}}(MinM)(MinE)$ is the minimal explanation with $MinE = \sigma_{uo} t^o\ \sigma_{uo} \in \mathcal{T}^*_{uo}$
(3) $\forall M' \subset MinM$ then $MinE \notin \mathcal{L}_{\mathcal{N}}(M')$
(4) $\forall \sigma'_{uo} t^0$ obtained from σ_{uo} by deleting a transition $t \in \sigma_{uo} \Rightarrow \sigma'_{uo} t^0 \notin \mathcal{L}_{\mathcal{N}}(MinM)$

Denote by $\mathcal{C}_{\mathcal{B}}$ the set of maximal configurations of the branching process $\mathcal{B}$ and by $All\mathcal{B}$ the set of all branching processes that are stopping prefixes. Denote by $\pi : \mathcal{C} \to (0, 1]$ the unnormalized probability function on the set of configurations $\mathcal{C}$ in the net unfolding $\mathcal{U}_{\mathcal{N}}(M_0)$ that is defined as follows:

$$\forall C \in \mathcal{C} \quad \pi(C) = Prod_{e \in E_C}(\pi(e)) \tag{3}$$

Normalization will by carried out later on when the probability of faults having occurred is defined.

Consider two branching processes $\mathcal{B}, \mathcal{B}' \in All\mathcal{B}$; $\mathcal{B} \subseteq \mathcal{B}'$. Given a configuration $C_{\mathcal{B}}$ denote by $Ext(C_{\mathcal{B}}, \mathcal{B}')$ the set of the maximal configurations in $\mathcal{B}'$ that are extensions of $C_{\mathcal{B}}$:

$$Ext(C_{\mathcal{B}}, \mathcal{B}') = \{C'_{\mathcal{B}'} \in \mathcal{C}_{\mathcal{B}'} \mid C_{\mathcal{B}} \subseteq C'_{\mathcal{B}'}\} \tag{4}$$

$$\pi(C_{\mathcal{B}}) = \sum_{C'_{\mathcal{B}'} \in Ext(C_{\mathcal{B}}, \mathcal{B}')} \pi(C'_{\mathcal{B}'}) \tag{5}$$

The observations available at the time of the n_{th} observed event is denoted as $\mathcal{O}_n = \langle obs_1, \ldots, obs_n\rangle$, where $obs_k \in \Omega_o$ is the label of the k_{th} observation. Since the observations obs_k are received without errors and without delays, the set $\mathcal{L}_{\mathcal{N}}(\mathcal{O}_n)$ of all possible plant evolutions that agree with the model with the initial conditions, and such that the observed sequence of event labels is given by :

$$\mathcal{L}_{\mathcal{N}}(\mathcal{O}_n) = \{\tau \in \mathcal{L}_{\mathcal{N}}(M_0) \mid \Pi_{\mathcal{T}_o}(\tau) = \mathcal{O}_n\} \tag{6}$$

The plant diagnoser $\mathcal{D}_{\mathcal{N}}(\mathcal{O}_n)$ (Jiroveanu et al. [2008]) after observing $\mathcal{O}_n$ is based on the set of all explanations and the diagnosis result $\mathcal{DR}_{\mathcal{N}}(\mathcal{O}_n)$ is obtained by projecting the set of all possible evolutions onto the set of fault events:

$$\mathcal{D}_{\mathcal{N}}(\mathcal{O}_n) = \left\{\sigma_f \mid \sigma_f = \Pi_{\mathcal{T}_f}(\tau) \wedge \tau \in \mathcal{L}_{\mathcal{N}}(\mathcal{O}_n)\right\} \tag{7}$$

$$\mathcal{DR}_{\mathcal{N}}(\mathcal{O}_n) = \begin{cases} \mathtt{N} & \text{if } \mathcal{D}_{\mathcal{N}}(\mathcal{O}_n) = \{\epsilon\} \\ \mathtt{F} & \text{if } \epsilon \notin \mathcal{D}_{\mathcal{N}}(\mathcal{O}_n) \\ \mathtt{UF} & \text{otherwise} \end{cases} \tag{8}$$

N, F, UF are the diagnoser state *normal*, *fault*, *uncertain* (M. Sampath et al. [1995]).

The set of configurations $\mathcal{C}(O_n) \in \mathcal{U}_{\mathcal{N}}(M_0)$ contains all sequences C of observations s.t. their string linearization E_C contains exactly n observable events satisfying: $l_o(t^o_i) = obs_i, i = 1, \ldots, n$ and $\forall\ e^o_i, e^o_j \in E^o_C$, if $i < j$ then $e^o_i \preceq e^o_j$ or $e^o_i \parallel e^o_j$. The set of explanations of the received observation $\mathcal{L}_{\mathcal{N}}(\mathcal{O}_n)$ can be derived as follows:

$$\mathcal{L}_{\mathcal{N}}(\mathcal{O}_n) = \{\tau \mid \sigma \in \langle E_C\rangle_{\preceq} \wedge C \in \mathcal{C}(\mathcal{O}_n)\} \tag{9}$$

The set of minimal configurations $\underline{\mathcal{C}}(\mathcal{O}_n)$, respectively the set of minimal explanations of the received observation $\underline{\mathcal{L}}_{\mathcal{N}}(\mathcal{O}_n)$ are defined as follows. $\underline{C} \in \underline{\mathcal{C}}(\mathcal{O}_n)$ if $\forall e \in E_{\underline{C}}$ if :

$$\phi(e) \in \mathcal{T}_{uo}\ then\ \exists e^o \in E_{\underline{C}} s.t. e \preceq e^o and\ \phi(e^o) \in \mathcal{T}_o \tag{10}$$

$$\underline{\mathcal{L}}_{\mathcal{N}}(\mathcal{O}_n) = \left\{\tau \mid \sigma \in \langle E_{\underline{C}}\rangle_{\preceq} \wedge \underline{C} \in \underline{\mathcal{C}}(\mathcal{O}_n)\right\} \tag{11}$$

The plant diagnosis $\underline{\mathcal{D}}_{\mathcal{N}}(\mathcal{O}_n)$ and the diagnosis result $\underline{\mathcal{DR}}_{\mathcal{N}}(\mathcal{O}_n)$ are obtained by projecting the sets of minimal explanations and the set of all explanations onto the set of fault events of the type i $\mathcal{T}_{f_i}$:

$$\underline{\mathcal{D}}_{\mathcal{N}}(\mathcal{O}_n) = \left\{\sigma_{f_i} \mid \sigma_{f_i} = \Pi_{\mathcal{T}_{f_i}}(\tau) \wedge \tau \in \underline{\mathcal{L}}_{\mathcal{N}}(\mathcal{O}_n)\right\} \tag{12}$$

$$\underline{\mathcal{DR}}_{\mathcal{N}}(\mathcal{O}_n) = \begin{cases} \underline{\mathtt{N}} & \text{if } \underline{\mathcal{D}_{\mathcal{N}}}(\mathcal{O}_n) = \{\epsilon\} \\ \underline{\mathtt{F}} & \text{if } \epsilon \notin \underline{\mathcal{D}_{\mathcal{N}}}(\mathcal{O}_n) \\ \underline{\mathtt{UF}} & \text{otherwise} \end{cases} \tag{13}$$

We partition the set of fault events into disjoint fault sets belonging to different fault types $\sum_f = \sum_{f1} \bigcup \cdots \bigcup \sum_{fm}$.

Denote by $\underline{\mathcal{C}}^{fault_i}(\mathcal{O}_n)$ respectively $\underline{\mathcal{C}}^{without fault_i}(\mathcal{O}_n)$ the set of minimal configurations that contains at least a fault event of the type i $\mathcal{T}_{f_i}$ respectively the set of minimal configurations that does not contain faults of the type i $\mathcal{T}_{f_i}$.

$$\underline{\mathcal{C}}^{fault_i}(\mathcal{O}_n) = \left\{\underline{C} \in \underline{\mathcal{C}}(\mathcal{O}_n) \mid \exists e \in E_{\underline{C}} \text{ s.t. } \phi(e) \in \mathcal{T}_{f_i}\right\}$$
$$\underline{\mathcal{C}}^{without f_i}(\mathcal{O}_n) = \left\{\underline{C} \in \underline{\mathcal{C}}(\mathcal{O}_n) \mid \forall e \in E_{\underline{C}}, \phi(e) \in \mathcal{T} \setminus \mathcal{T}_{f_i}\right\}$$

Than:

$$\pi_i(\underline{\mathcal{DR}}(\mathcal{O}_n) = \underline{\mathtt{F}_i}) = \frac{\sum_{\underline{C} \in \underline{\mathcal{C}}^{fault_i}(\mathcal{O}_n)} \pi(\underline{C})}{\sum_{\underline{C} \in \underline{\mathcal{C}}(\mathcal{O}_n)} \pi(\underline{C})}$$
$$\pi_i(\underline{\mathcal{DR}}(\mathcal{O}_n) = \underline{\mathtt{NF}_i}) = \frac{\sum_{\underline{C} \in \underline{\mathcal{C}}^{without f_i}(\mathcal{O}_n)} \pi(\underline{C})}{\sum_{\underline{C} \in \underline{\mathcal{C}}(\mathcal{O}_n)} \pi(\underline{C})} \tag{14}$$

where $\pi_i(\underline{\mathcal{DR}}(\mathcal{O}_n) = \underline{\mathtt{F}_i})$ denotes the probability of a fault of the type i have happened before the last observed event while $\pi_i(\underline{\mathcal{DR}}(\mathcal{O}_n) = \underline{\mathtt{NF}_i})$ denotes the probability that no fault of the type i has happened before the last observed event.

Similarly denote by $\mathcal{C}^{fault_i}(\mathcal{O}_n)$ respectively $\mathcal{C}^{without f_i}(\mathcal{O}_n)$ the set of all configurations that contains at least a fault event of the type faults: Denote by $\mathcal{D}(\mathcal{O}_n)$ the probabilistic diagnosis result based on all explanations.

$$\mathcal{D}_{\mathcal{N}}(\mathcal{O}_n) = \left\{\sigma_{f_i} \mid \sigma_{f_i} = \Pi_{\mathcal{T}_{f_i}}(\tau) \wedge \tau \in \mathcal{L}_{\mathcal{N}}(\mathcal{O}_n)\right\} \tag{15}$$

$$\mathcal{C}^{fault_i}(\mathcal{O}_n) = \{C \in \mathcal{C}(\mathcal{O}_n) \mid \exists e \in E_C \text{ s.t. } \phi(e) \in \mathcal{T}_{f_i}\}$$
$$\mathcal{C}^{withoutf_i}(\mathcal{O}_n) = \{C \in \mathcal{C}(\mathcal{O}_n) \mid \forall e \in E_C, \phi(e) \in \mathcal{T} \setminus \mathcal{T}_{f_i}\}$$

Using the same methodology we can also derive the likelihood of a fault based on all explanations and we receive the same formulae as in (14) removing all underscores.

$$\pi_i(\mathcal{DR}(\mathcal{O}_n) = \mathtt{F}_i) = \frac{\sum_{C \in \mathcal{C}^{fault_i}(\mathcal{O}_n)} \pi(C)}{\sum_{C \in \mathcal{C}(\mathcal{O}_n)} \pi(C)}$$
$$\pi_i(\mathcal{DR}(\mathcal{O}_n) = \mathtt{NF}_i) = \frac{\sum_{C \in \mathcal{C}^{withoutf_i}(\mathcal{O}_n)} \pi(C)}{\sum_{C \in \mathcal{C}(\mathcal{O}_n)} \pi(C)} \quad (16)$$

A novel approach to the diagnosis problem is proposed in the next paragraphs. We suggest that an interesting and computationally often feasible solution can be obtained by combining the deterministic analysis of what must have happened for sure prior to the last observed event (Jiroveanu [2006], Jiroveanu et al. [2008]), with a probabilistic analysis of what may happen prior to the next event observation. Deterministic minimal contexts are derived while the set of "possible continuations of these minimal contexts" are equipped with probabilities (Flochova et al. [2007]).

The sets of explanations, equipped with their probabilities, can be calculated as follows :

(1) Compute the set of minimal explanations of the most recent observed event i.e. carry out a backward search in the reverse net $\mathcal{RN}$. Derive minimal explanations of the last observed event t_0 and minimal explanations of a sequence of observed events.
(2) Compute the unnormalized probability of all minimal explanations
$$\forall \underline{C} \in \mathcal{C} \quad \pi(\underline{C}) = Prod_{e \in \underline{C}}(\pi(e)) \quad (17)$$
(3) Sort explanations in descending order starting from the most probable ones. Shellsort can be used, branch and bound like improvements can be useful in order to avoid enumerating very unlikely explanations.
(4) Accept top x % (0-100 %) of explanations according to the input requirements.
(5) Compute the set of maximal explanations of the most recent observed event, if required.
(6) Compute the unobservable continuations, which follow after the next observable transitions and partition the continuations into the following sets: the set of configurations, which contain at least a faulty event; a set of configurations, which contain at least a faulty event of the fault of the type i, and the set of configurations, which don't contain any faulty event. A modification of classical AI depth search, which evaluates at first the node that has the most nodes between itself and the last observed transition, can be used for computing the set of continuations equipped with probabilities.
(7) Compute the unnormalized probabilities of the faults (faults of the type i) of all continuations (of unobservable reaches after the last observation).
(8) Compute the unnormalized probabilities of the faults (faults of the type i) based on the sets of all explanations.
(9) Normalize the probabilities and and evaluate (16), (17) to derive the normalized probability of a fault of type i occurring.

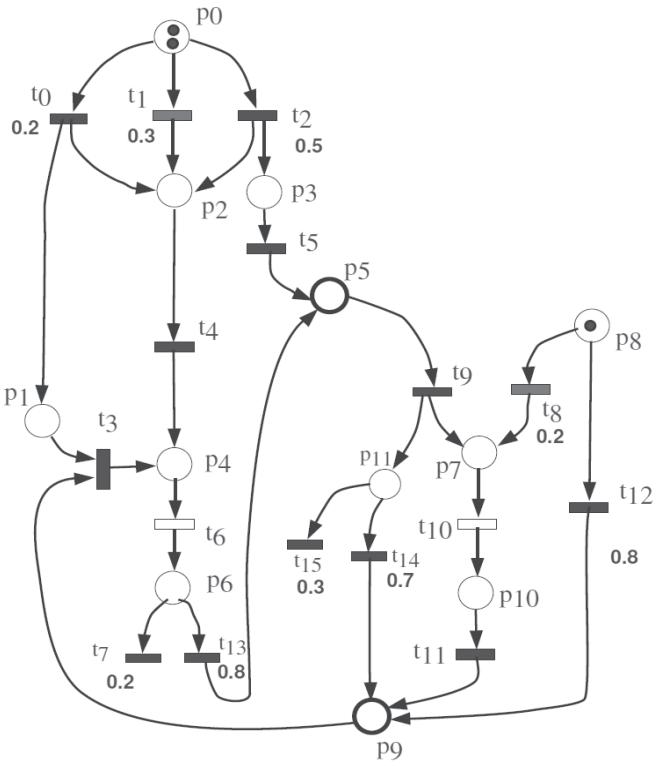

Fig. 1. Probabilistic free-choice Petri net

Consider as an example the free-choice Petri net PN in fig. 1 where t_6 and t_{1o} are observable events and t_1, t_8 are faulty events. After having received as the first and so far only observation t_6 the above algorithm leads to the following calculations. The unfolding of PN is shown in figure 2.

The possible configurations are:

C_1: E_1=e_{12},e_0,e_3,e'_6, C_2: E_2=e_{12},e_0,e_3,e'_6,e'_7

C_3: E_3=e_{12},e_0,e_3,e'_6,e'_{13}, C_4: E_4=e_{12},e_0,e_3,e'_6,e'_{13},e_9

C_5: E_5=e_{12},e_0,e_3,e'_6,e'_{13},e_9,e_{15}

C_6: E_6=e_{12},e_0,e_3,e'_6,e'_{13},e_9,e_{14}

C_7: E_7=e_{12},e_0,e_3,e'_6,e'_{13},e_9,e_{14},e'_0,e^*_3

C_8: E_8=e_{12},e_0,e_3,e'_6,e'_{13},e_9,e_{14},ee_1

C_9: E_9=e_{12},e_0,e_3,e'_6,e'_{13},e_9,e_{14},ee_1,e_4

C_{10}: E_{10}=e_0,e_4,e_6, C_{11}: E_{11}=e_1,e'_4,e''_6

C_{12}: E_{12}=e_2,e''_4,e'''_6. C_{13}: E_{13}=ee_0,ee'''_4,ee'''_6

C_{14}: E_{14}=ee_1,ee''_4,ee''_6, C_{15}: E_{15}=ee_2,ee'_4,ee'_6

C_{16}: E_{16}=e_{12},ee_0,ee_3,ee_6

Configurations C_2 - C_9 are continuation of C_1. The set of minimal configurations consists of C_1 and C_{10} - C_{16}. Probability of configuration C_1 ($\tau = t_{12}t_0t_3t_6$) equals $\pi(\tau) = \pi(t_{12})\pi(t_0)\pi(t_3)\pi(t_6) = 0.8*0.2*1*1 = 0.16$. Probability of configuration C_{10} ($\tau = t_0t_4t_6$) equals $\pi(\tau) = \pi(t_0)\pi(t_4)\pi(t_6) = 0.2*1*1 = 0.2$ etc.

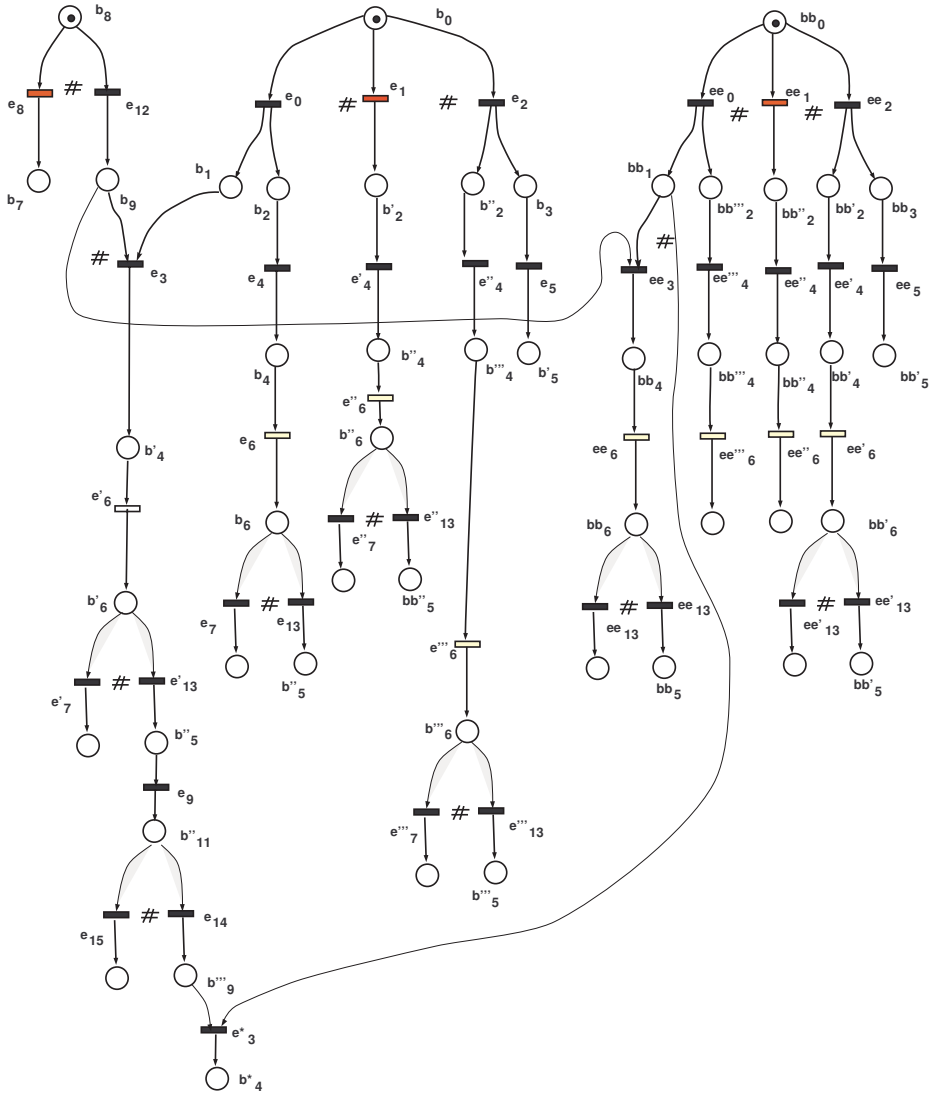

Fig. 2. Unfolding of Petri net in figure 1

Failure probabilities assigned to minimal explanations are shown in table 1 (the probability of the failure configurations containing t_1 and t_8 is 0.258), to all explanations in table 2 (the probability of a failure is 0.233).

The analysis of the possible future unobservable events is shown in table 3. The probability of a failure that happened after the last observed event equals 0.11.

minimal explanations						
	t12	*t0*	*t1*	*t2*		
C1	0.8	0.2			0.16	0.07
C10		0.2			0.20	0.09
C11			0.3		0.30	0.13
C12				0.5	0.50	0.22
C13		0.2			0.20	0.09
C14			0.3		0.30	0.13
C15				0.5	0.50	0.22
C16	0.8	0.2			0.16	0.07
					2.32	1.00

Table 1. Failure probabilities assigned to minimal explanations

The results of the proposed algorithms have been compared with the results of the stochastic diagnoser of Thorsley and Theneketzis [2005] after redrawing automata models into corresponding Petri net models. The same results

all explanations											
	t12	*t0*	*t1*	*t2*	*t7*	*t8*	*t13*	*t14*	*t15*		
C1	0.8	0.2								0.16	0.06
C2	0.8	0.2			0.2					0.03	0.01
C3	0.8	0.2					0.8				0.05
C4	0.8	0.2					0.8				0.05
C5	0.8	0.2					0.8		0.3	0.04	0.01
C6	0.8	0.2					0.8	0.7			0.03
C7	0.8	0.0					0.8	0.7		0.02	0.01
C8	0.8	0.2	0.3				0.8	0.7		0.03	0.01
C9	0.8	0.2	0.3				0.8	0.7		0.03	0.01
C10		0.2								0.20	0.07
C11			0.3							0.30	0.11
C12				0.5						0.50	0.18
C13		0.2								0.20	0.07
C14			0.3							0.30	0.11
C15				0.5						0.50	0.18
C16	0.8	0.2								0.16	0.06
										2.81	1.00

Table 2. Failure probabilities assigned to all explanations

are obtained. The proposed algorithms have been included in the tool PNDesigner (Flochova et al. [2006]).

4. UNRELIABLE OBSERVATIONS

In this section we discuss the diagnosis problem for unreliable systems, where faulty sensors may lead to misclassi-

all explanations, deterministic past, probabilistic future										
	t0	*t1*	*t2*	*t7*	*t8*	*t13*	*t14*	*t15*		
C2				0.2					0.200	0.066
C3						0.8			0.800	0.262
C4						0.8			0.800	0.262
C5						0.8		0.3	0.240	0.079
C6						0.8	0.7		0.560	0.184
C7	0.2					0.8	0.7		0.112	0.037
C8		0.3				0.8	0.7		0.168	0.055
C9		0.3				0.8	0.7		0.168	0.055
									3.048	1.000

Table 3. Deterministic calculations in the past and probabilistic in the future

fication or misdetection of observable events. These errors include, in their most basic form, event insertions and deletions and could arise under a variety of conditions (e.g. due to sensor failures or in the communication links connecting the sensors to the diagnoser). The diagnosis problem for these systems can be reduced to that of section III by modifying the model as follows. The misleading observability (not detecting a signal generated by an observable event) can be solved by including a new choice in the model structure (fig. 3a) or by adding a new arc to an existing conflict (fig. 3b). If the unreliable observations don't insert an unobservable cycle in the model the algorithms can be applied without changes. The misdetecting of an event can be modelled with a probabilistic self loop (fig. 3cd). The algorithms can be applied without changes in this case, one has to take care to implement *Pre* and *Post* incidence matrices respecting selfloops.

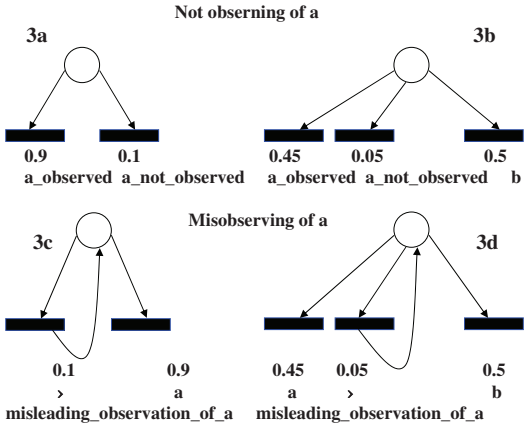

Fig. 3. Unreliable observations

5. CONCLUSIONS AND FUTURE WORKS

By using the techniques in Abbes and Benveniste [2008], Aghasaryan et al. [1998], Benveniste et al. [2004], Jiroveanu et al. [2008], Jiroveanu [2006] the proposed probabilistic analysis can be can be extended to decentralized and distributed settings (Su and Wonham [2002]). Another direction to explore is to relax the assumption that the PN models are free-choice, following the construction proposed in Haar [2003]. The proposed algorithms have been included in the tool PNDesigner (Flochova et al. [2006]).

REFERENCES

S. Abbes and A. Benveniste. True-concurrency probabilistic models: Markov Nets and the law of large numbers. *Theoretical Computer Science*, ISSN 0304-3975, 390:-3 129–170, 2008.

A. Aghasaryan, E. Fabre, A. Benveniste, R. Boubour, C. Jard. Fault Detection and Diagnosis in Distributed Systems: An Approach by Partially Stochastic Petri Nets. *Journal Discrete Event Dynamic Systems*, ISSN 0924-6703, 8:203–231, 1998.

A. Benveniste, E. Fabre, S. Haar, C. Jard. Diagnosis of asynchronous discrete event systems, a net unfolding approach. *IEEE Trans. on Aut. Control*, 48:714–727, 2003.

A. Benveniste, S. Haar, E. Fabre, C. Jard. Distributed Monitoring of concurrent and asynchronous systems-extended version. INRIA, No. 4842, 2004.

R. Boel and G. Jiroveanu. Distributed Contextual Diagnosis for very Large Systems. *Proceeding of WODES04*, Reims, France, 343–348, 2004.

J. Esparza. S. Romer and W. Vogler. An improvement of McMillan's unfolding algorithm. *Lect. Notes in Computer Science 1055*, 87–106, Springer-Verlag, 1996.

J. Flochova, R. K. Boel, and G. Jiroveanu. On Probabilistic Diagnosis for Free-Choice Petri Nets. *Proceeding of ACC*, NYC, US, 5655–5656, 2007.

J. Flochova, F. Auxt, M. Radakovic, O. Jombik. PNDesigner a Tool designed for model based diagnosis and supervisory control of DES. *Proceeding of WODES'08*, ISBN 1-4244-0053-8, 471–472, 2006.

S. Genc and S. Lafortune. Distributed diagnosis of place-bordered petri nets. *IEEE Trans. on Automation Science and Engineering*, 4:206–219, 2007.

A. Giua and C. Seatzu. Fault detection for DES using Petri nets with unobservable transitions. *Proc. of IEEE Conference on Decision and Control*, Sevilla, Spain, 6323–6328.

S. Haar. Probabilistic cluster unfoldings for Petri Nets, Technical report 1517, IRISA, Rennes, France, 2003.

G. Jiroveanu. Fault Diagnosis for Large Petri Nets , *PhD thesis*, Ghent University, Belgium. 210 pp, 2006.

G. Jiroveanu, R. Boel, and B. De Schutter. Fault Diagnosis for Timed Petri Nets. *Proc. of WODES*, Ann Arbor, US, ISBN 1-4244-0053-8, 2006.

G. Jiroveanu, R.K. Boel, and B. Bordbar. On-Line Monitoring of Large Petri Net Models Under Partial Observation. *Journal Discrete Event Dynamic Systems*, 18:323–354, 2008.

M. Nielsen, G. Plotkin, and G. Winskel. Petri nets, event structures and domains, part I. *Theoret. Computer Science*, 13:85–108, 1981.

M. Sampath, R. Sengupta, K. Sinnamohideen, S. Lafortune, and D. Teneketzis. Diagnosability of discrete event models. *IEEE Trans. Control Systems Technology*, 40: 1555–1575, 1995.

R. Su and W.M. Wonham. Probabilistic Reasoning in Distributed Diagnosis for Qualitative Systems *Proc. of IEEE Conference on Decision and Control*, Las Vegas, USA, 429–434, 2002.

D. Thorsley and D. Theneketzis. Diagnosability of Stochastic Discrete-Event Systems. *Proc. of Trans. on Automatic Control*, 50:476–492, 2005.

X. Wang, I. Chattopadhyay, and A. Ray. Probabilistic Fault Diagnosis in DES. *IEEE Conference on Decision and Control*, Nassau, Bahamas, 4794–4799, 2004.