12th IFAC/IEEE Workshop on Discrete Event Systems
Cachan, France. May 14-16, 2014

Model Checking on Fault Diagnosis Graph ⋆

Xu Wang * **Cristian Mahulea** * **Manuel Silva** *

* *Instituto de Investigación en Ingenierá de Aragón (I3A), Universidad de Zaragoza, María de Luna 1, E-50018 Zaragoza, Spain (email:{xuwang, cmahulea, silva}@unizar.es)*

Abstract: This paper investigates the use of model checking techniques for fault diagnosis on timed systems. The timed systems are modeled with time Petri nets (TPN). Our approach is based on the fault diagnosis graph (FDG), which is obtained from the state class graph of TPN, by removing nodes and edges that are not used in fault diagnosis. In order to apply the reduction rules, we assume that the FDG is bounded and completely constructed. We first propose some reduction rules on the FDG to obtain a more compact representation and then we use model checking techniques on the reduced FDG to compute the diagnosis states. We compare the complexity of model checking on FDG with the one on the reduced FDG.

1. INTRODUCTION

Fault diagnosis problem of Discrete Event Systems (DESs) is an important research topic in last decades. Many works have been proposed both in automata [1] and Petri nets [2]. Grabiec et al. [3] study on-line diagnosis of distributed systems. The systems are represented using TPN extended with time parameters and the proposed approach is based on unfolding. The extension of time parameter is that time bounds associated to transitions can be symbolic expressions instead of rational constants. Cabasino et al. [2] address the problem of fault diagnosis on untimed PN where faults can be modeled by observable transitions. In their work, observable fault transitions may share the same label with other observable fault transitions, which can belong to different fault classes. The approach is based on the *basis reachability graph* and they assume that the unobservable subnets are acyclic. Lefebvre et al. [4] investigate the problem of diagnosability of untimed Petri nets that can be either bounded or unbounded. They use the coverability graph to construct the diagnoser such that for unbounded PNs diagnosers with finite numbers of states are available.

In [5] we propose *Fault Diagnosis Graph* (FDG) for the fault diagnosis on TPN, which have been adapted to decentralized fault diagnosis in [6]. The diagnosis algorithms constructs the FDG incrementally with the observed events. If a part of the FDG will be used for diagnosis, it would be constructed. Using the incremental approach, the computation of the whole FDG could be avoided.

In this paper, we address the problem of fault diagnosis on TPN by applying model checking techniques on FDG that is assumed to be bounded. First, we propose some reduction rules on FDG and, second, investigate model checking algorithms on the reduced FDG. Last, time complexities of model checking algorithms on both reduced and not reduced FDG are compared in detail. Comparing with our previous works, the contributions are as follows: 1) The reduction rules eliminate nodes and edges from a fully constructed FDG in order to reduce the complexity of model checking algorithms on FDG. By means of the reduction rules, the complexity of model checking algorithms could be reduced. 2) Model checking algorithms are applied on the FDG for fault diagnosis. The diagnosis algorithms in [5] updates the diagnosis states after the observation of an event while the model checking algorithms deal with an observation word. We compare the complexity of model checking algorithms on both non-reduced and reduced FDGs.

⋆ This work has been partially supported by CICYT - FEDER project DPI2010-20413. The Group of Discrete Event Systems Engineering (GISED) is partially co-financed by the Aragonese Government (Ref. T27) and the European Social Fund.

2. TIME PETRI NET

In this section, we recall the basic definition of TPN system (for a general introduction, see [7, 8]).

Definition 1. A *TPN system* is a pair $\langle \mathcal{N}, \boldsymbol{m}_0 \rangle$, where $\mathcal{N} = \langle P, T, \boldsymbol{Pre}, \boldsymbol{Post}, I \rangle$ is a net structure with a set of places P; a set of transitions T; the pre and post incidence matrices $\boldsymbol{Pre}, \boldsymbol{Post} \in \mathbb{N}_{\geq 0}^{|P| \times |T|}$; $I : T \to \mathbb{Q}_{\geq 0} \times \mathbb{Q}_{\geq 0} \cup \{\infty\}$ is the time function associating a *time interval* to each transition; and $\boldsymbol{m}_0 \in \mathbb{N}_{\geq 0}^{|P|}$ is the initial marking, where $|P|$ is the number of places and $|T|$ is the number of transitions.

A transition $t \in T$ is enabled at a marking $\boldsymbol{m}$ if $\boldsymbol{m} \geq \boldsymbol{Pre}[\cdot, t]$, where $\boldsymbol{Pre}[\cdot, t]$ is the column of $\boldsymbol{Pre}$ corresponding to transition t. Considering $I(t) = [l, u]$, then when t is enabled, it cannot be fired earlier than l time units and it has to be fired no later than u time units. If a marking $\boldsymbol{m}'$ is reachable from $\boldsymbol{m}$ by firing a sequence $\sigma = t_{i1} t_{i2} \cdots t_{in} \in T^*$, where $t_{ij} \in T, j = 1, 2, \ldots, n$ and T^* is the Kleene closure of T. The fundamental state equation can be written as $\boldsymbol{m}' = \boldsymbol{m} - \boldsymbol{Pre} \cdot \boldsymbol{\sigma} + \boldsymbol{Post} \cdot \boldsymbol{\sigma}$, where $\boldsymbol{\sigma} \in \mathbb{N}^{|T|}$ is the *firing count vector* of σ that counts how many times each transition is fired in σ, and $\boldsymbol{m}[\sigma\rangle$ denotes that σ is fireable from $\boldsymbol{m}$, while $\boldsymbol{m}[\sigma\rangle\boldsymbol{m}'$ means the firing of σ drives $\boldsymbol{m}$ to $\boldsymbol{m}'$. The single server semantic is used in this paper, which means that a transition cannot be enabled simultaneously more than once.

The set of transitions T is partitioned into two subsets: $T = T_o \cup T_u, T_o \cap T_u = \emptyset$, where T_o is the set of *observable* transitions, whose firing can be detected by an external observer, and T_u is the set of *unobservable* transitions. The firing sequence σ_o is an observable firing sequence, if $t \in \sigma_o$, then $t \in T_o$; σ_u is an unobservable firing sequence, if $t \in \sigma_u$, then $t \in T_u$. An observation function is $\mathcal{O} : \sigma \to T_o^*$, and it extracts the sequence of observable transitions $\mathcal{O}(\sigma)$ from σ. Let $\sigma = \sigma_{u1}\sigma_{o1}\sigma_{u2}\sigma_{o2}\cdots\sigma_{un}$, then $\mathcal{O}(\sigma) = \sigma_{o1}\sigma_{o2}\cdots\sigma_{on-1}$. In figures, observable transitions are represented by white rectangles, e.g., t_3 in Fig. 1, while unobservable ones are black rectangles, e.g., ε_1 in Fig. 1. We use $|\sigma|$ to denote the number of transitions in σ. For every node $v \in P \cup T$, the set of its input and output nodes are denoted as ${}^\bullet v$ and $v^\bullet$, respectively.

Definition 2. The *unobservable subnet* of a TPN $\mathcal{N} = \langle P, T, \boldsymbol{Pre}, \boldsymbol{Post}, I\rangle$ is $\mathcal{N}_u = \langle P, T_u, \boldsymbol{Pre}_u, \boldsymbol{Post}_u, I_u\rangle$, where: 1) T_u is the set of unobservable transitions of $\mathcal{N}$, 2) P is the set of places, 3) $\boldsymbol{Pre}_u$ and $\boldsymbol{Post}_u$ are pre and post incidence matrices restricted to T_u, 4) $I_u : T_u \to \mathbb{Q}_0 \times \mathbb{Q}_0 \cup \{\infty\}$.

A *directed circuit* of PN is a sequence $p_1t_1p_2t_2\cdots p_nt_np_1$, where $p_j \in P$, $t_j \in T$, $p_j \in {}^\bullet t_j$, $t_j \in {}^\bullet p_{j+1}$, and $\forall j \neq k, p_j \neq p_k, j, k = 1, 2, \ldots, n$. A net having no directed circuits is called *acyclic*.

Definition 3. An *observed word* is a sequence of ordered pairs $w = \langle t_1, \tau_1\rangle \ldots \langle t_k, \tau_k\rangle \in (T_o \times \mathbb{Q}_0)^*$, in which t_1 is the first observed transition and it is observed at τ_1, while t_k is the latest observed transition at τ_k. Let $\langle \mathcal{N}, \boldsymbol{m}_0\rangle$ be a TPN system and $w = \langle t_1, \tau_1\rangle \ldots \langle t_k, \tau_k\rangle$ be an observed word. We define the *set of firing sequences consistent with* w by $\mathcal{L}(w) = \{\sigma | \boldsymbol{m}_0[\sigma\rangle, w = \mathcal{O}(\sigma) = t_1 \ldots t_k,$ such that t_i is fireable at $\tau_i, i = 1, \ldots, k\}$.

A *fault* is modeled by an unobservable transition, but there may be unobservable transitions whose firing corresponds to regular behaviors. To model faulty and regular behaviors in Petri net, the set of unobservable transitions is partitioned into two subsets $T_u = T_f \cup T_{reg}$, where T_f includes all fault transitions and T_{reg} includes all transitions relative to unobservable but regular events. The set T_f is further partitioned into r subsets as $T_f = T_f^1 \cup T_f^2 \cup \cdots \cup T_f^r$, where all transitions in the same subset correspond to the same *fault class*. We say that the i-th fault has occurred when a transition in T_f^i has been fired. We now provide the definition of the diagnoser of a TPN system.

Definition 4. A *diagnoser* is a function $\Delta : (T_o \times \mathbb{Q}_0)^* \times \{T_f^1, T_f^2, \ldots, T_f^r\} \to \{\text{N, F, U}\}$, where $(T_o \times \mathbb{Q}_o)^*$ is the set of observation $w = \langle t_1, \tau_1\rangle \ldots \langle t_j, \tau_j\rangle$ and N, F and U represent Normal, Faulty and Uncertain states, respectively. The diagnoser associates to each observed word w and to each fault class $T_f^i, i = 1, \ldots, r$, a diagnosis state.

- $\Delta(w, T_f^i) = \text{N}$ if for all $\sigma \in \mathcal{L}(w)$ and for all $t_f \in T_f^i$ it holds $t_f \notin \sigma$.
  In this case, *none* of the firing sequences consistent with the observation contains any fault transition of class i, the i-th fault cannot have occurred.
- $\Delta(w, T_f^i) = \text{U}$ if: 1) there exists $\sigma \in \mathcal{L}(w)$ and $t_f \in T_f^i$ such that $t_f \in \sigma$, but 2) there exists $\sigma' \in \mathcal{L}(w)$ such that $t_f \notin \sigma', \forall t_f \in T_f^i$
  In this case, a fault transition of class i may have occurred or not, i.e., it is uncertain.
- $\Delta(w, T_f^i) = \text{F}$ if for all $\sigma \in \mathcal{L}(w)$ and $\exists t_f \in T_f^i$ it holds $t_f \in \sigma$.
  In such a case, the i-th fault have occurred, because all fireable sequences consistent with the observation contain at least one fault transition of class i.

We make the following assumptions: (A1) the initial marking and the net structure are known; (A2) the unobservable induced subnet is acyclic; (A3) the bounds of time intervals of transitions are rational numbers; (A4) the TPN is bounded.

3. FAULT DIAGNOSIS GRAPH

In this section, we briefly introduce *Fault Diagnosis Graph* (FDG), which has been proposed in [5], for diagnosis on TPN systems.

The FDG is obtained from the *State Class Graph* (SCG) [8, 9]. A *state class* is a pair $\alpha = \langle \boldsymbol{m}, F\rangle$, where $\boldsymbol{m}$ is a reachable marking and F is the conjunction of inequalities representing the *firing domains*, i.e., the possible firing intervals of transitions. If t_j is an enabled transition at $\boldsymbol{m}$ and has associated a firing interval $[l, u]$, then there exists an inequality $l \leq x_j \leq u$ in F, where x_j is the time delay when t_j can be fired at $\boldsymbol{m}$.

In the construction of the FDG from an SCG, paths containing unobservable transitions are obtained from the SCG and represented by edges in the FDG. States (nodes) from the SCG are not added into the FDG if they are not used in the diagnosis, i.e., not reached by firing of an observable transition. Therefore, an edge in the FDG is associated with a firing sequence, while in the SCG it is associated with transitions.

Definition 5. A *Fault Diagnosis Graph* (FDG) is a 4-tuple $\mathcal{G} = \langle \Omega, \twoheadrightarrow, \alpha_0, \Gamma\rangle$, where 1) $\alpha_0 = \langle \boldsymbol{m}_0, F_0\rangle$ is the initial state class, 2) $\twoheadrightarrow$ is the set of edges, where $\alpha \twoheadrightarrow \alpha'$ means that $\exists \sigma_u \in T_u^*$ and $t_o \in T_o$ such that α' is reachable from α by firing $\sigma_u t_o$, 3) $\Omega = \{\alpha | \alpha_0 \twoheadrightarrow^* \alpha\}$, where $\twoheadrightarrow^*$ is the reflexive and transitive closure of $\twoheadrightarrow$, is the set of reachable state classes, 4) $\Gamma : \twoheadrightarrow \to T_o^* \times \{\mathbb{Q}_0 \times \mathbb{Q}_0 \cup \{\infty\}\} \times \{\text{N, F, U}\}^r$ is the labeling function of edges.

The label of an edge corresponding to a firing sequence σ is $\langle w, I, D\rangle$, where $w = \mathcal{O}(\sigma)$, I is the firing domain of σ and D encodes the firing of fault transitions in σ. Considering a fault class T_f^i: 1) if $\forall t \in T_f^i$, $t \notin \sigma$, then $D(i) = \text{N}$ and 2) if $\exists t \in T_f^i$, $t \in \sigma$, then $D(i) = \text{F}$. The notation $D(i) = \text{U}$ will be used in Sec. 4. We denote the edge from α to α' whose label is $\langle w, I, D\rangle$ as $e : \langle \alpha, \langle w, I, D\rangle, \alpha'\rangle$.

4. REDUCTION RULES ON FDG

The FDG is a reduced SCG from which some nodes are removed. In this section, we propose some reduction rules on the FDG, in order to further reduce its size.

4.1 Reduction Rules on TPN

In the analysis of systems based on untimed PN, structural reduction rules are powerful tools [10]. For time models,