Available online at www.sciencedirect.com

ScienceDirect

IFAC Papers Online CONFERENCE PAPER ARCHIVE

IFAC PapersOnLine 50-1 (2017) 13636–13641

An incremental model repair approach to timed discrete event systems

Basile F. * **Chiacchio P.** * **Coppola J.** *

* *DIEM, Università di Salerno, Italy (e-mail: fbasile@ unisa.it).*

Abstract: New results on the model repair for timed discrete systems, modeled as Time Petri net systems, are presented in this paper. Unexpected and missed behavior in the nominal model, leading to observed but unexpected events and missed event observations, are formulated as logical conditions that can be directly transformed into linear mixed-integer inequalities. The repair model algorithm is incremental, also when multiple deviations from the nominal behavior are observed at a time. A set of logical conditions is preliminarily built from the observed behavior, then a mixed-integer linear programming problem is solved to repair the model.

Keywords: Discrete-event systems, System identification, Model repair, Time Petri nets.

1. INTRODUCTION

In context of logical Discrete Event Systems (DESs), the discrepance between nominal system behavior and observed system behavior, has been formalized in Roth et al. (2011) introducing residuals to take into account two very generic fault symptoms, *unexpected* and *missed* behavior, leading to observed but unexpected events and missed event observations, respectively. In Basile et al. (2016c) and Basile et al. (2016a) these two concepts have been extended to timed DESs context and applied to the identification and model repair of timed net systems, respectively. In Basile et al. (2016a) a model repair approach, based on the formulation of a Mixed Integer Linear Programming Problem (MILPP) whose solution provides the corrections needed to repair the nominal model, is presented.

In this paper, the approach presented in Basile et al. (2016a) is improved. In detail, the repair algorithm is incremental, i.e., it works on the current model and previous corrections to the model are not modified, and it works also when concurrent deviations from the nominal behavior are observed. Moreover, in addition to the extension of the bounds of the firing time of each nominal transition firing, the adding of a single transition for each fault is used to repair the model at current time. Finally, the algorithm complexity does not depend on the length of the observed sequences, since the search for markings enabling a fault is conducted exploring the neighborhood of the current marking.

The problem addressed here is different from net identification, since only the subnet modeling the unexpected and missed behavior of the system is identified while the subnet modeling the timed nominal behavior is assumed to be known. The reader can refer to Fanti and Seatzu (2008) for major details about net identification literature.

In Dotoli et al. (2011) can be found some points of contact with this paper since only a subnet is identified too, and precisely the unobservable behavior of Petri Net (PN) models is considered. Apart from the fact that timed models are not considered, the main difference with respect to our approach is that it is based not only on event observation, but also on marking observation. The problem of modifying the nominal model as a consequence of changes in the system behavior has been investigated also in Cabasino et al. (2014), where the deviations are called *faults* and the model repair is presented as the identification of the *faulty model* of a logical PN system: the occurrence of a faulty firing sequence (i.e., a sequence that cannot be generated by the nominal model of the system) is associated to the unobservable firings of fault transitions, that must be opportunely added and linked to the nominal model of the system, to obtain the faulty model. Hence, also in this case, the structure of the nominal model is changed.

2. NOTATIONS AND PRELIMINARY ASSUMPTIONS

It is assumed that the reader is familiar with the theory of PNs. For a complete review about them, the reader is remanded to Murata (1989).

Definition 1. (TPN system, Seatzu et al. (2013)). Let $\mathcal{I}$ be the set of closed intervals with a lower bound in the set of positive rational numbers $\mathcal{Q}^+$ and an upper bound in $\mathcal{Q}^+ \bigcup \infty$. A *Time* Petri net (TPN) system is the triple $S = \langle N, \boldsymbol{m}_0, I \rangle$, where N is a standard P/T net, $\boldsymbol{m}_0$ is the initial marking, and $I : T \to \mathcal{I}$ is the *statical firing time interval function* which assigns a firing interval $[l_j, u_j]$ to each transition $t_j \in T$.

A transition t_j can be fired at time τ if the time elapsed from the enabling belongs to the interval $I(t_j)$; moreover, an enabled transition must fire if the upper bound of $I(t_j)$ is reached, thus enforcing urgency. ◇

Assumption 1. (Properties of the observed system). The observed system is modeled by a TPN system with the following assumptions: 1) Free labeled nets (it is possible extending the approach to labeled nets with the adding of some technicalities (see Basile et al., 2016b); 2) Single-server firing semantic; 3) Enabling memory policy of timed transitions.

10.1016/j.ifacol.2017.08.2395

Definition 2. (Timed firing sequence). A sequence

$$\mathfrak{S} = (T_1, \tau_1) \dots (T_q, \tau_q) \dots (T_L, \tau_L),$$

where T_q is the set of transitions fired at time τ_q and $\tau_1 < \tau_2 \cdots < \tau_L$ denote firing time instants, is called *timed firing sequence*. The position q the couple (T_q, τ_q) occupies in the sequence is called *time step*, so (T_1, τ_1) is associated with step 1, (T_2, τ_2) is associated with step 2 and so on; the number of couples (T_q, τ_q) in $\mathfrak{S}$ is called length $L = |\mathfrak{S}|$ of the timed firing sequence.

The notation $\boldsymbol{m}[\mathfrak{S}\rangle\boldsymbol{m}'$ is used to denote that $\boldsymbol{m}'$ is reached from $\boldsymbol{m}$ by firing $\mathfrak{S}$. ◇

Definition 3. (Timed Language). Given a TPN system $S = \langle N, \boldsymbol{m}_0, I\rangle$, its timed language, named $\mathcal{L}(S)$, is defined as the set of timed firing sequences generated by S from the initial marking $\boldsymbol{m}_0$. ◇

The marking the system reaches after the firing of all the transitions in T_q is called $\boldsymbol{m}_q$.

Assumption 2. A transition can fire only once in the same time instant.

However, the results presented in this paper are still valid removing this assumption, introducing some technicalities.

The set T_q is made up of $n_q = |T_q|$ transitions whose firing is observed at the same instant τ_q. The firings of these transitions are enabled either by a marking $\boldsymbol{m}_k$ reached at a time $\tau_k < \tau_q$ or by the firing of another transition fired at τ_q with null firing duration.

Definition 4. (Firing Duration). Given a timed transition t_j, fired at the q-th step, enabled at the k-th step, so that $\boldsymbol{m}_k[t_j\rangle$, let $\boldsymbol{m}_k$ be the first marking that enables t_j since its previous firing, the function $\delta(t_j, k, q) : T \times \mathbb{N} \times \mathbb{N} \to \mathcal{Q}^+$ returns the time elapsed from the enabling of t_j at τ_k until its firing at τ_q, i.e., $\delta(t_j, k, q) = \tau_q - \tau_k$. ◇

From now on, it is referred to $\delta(t_j, k, q)$ as the firing duration of transition $t_j \in T_q$ from the marking $\boldsymbol{m}_k$. When $\delta(t_j, k, q) = 0$ the firing of t_j at τ_q is called *immediate*, otherwise, when $\delta(t_j, k, q) > 0$, the firing of t_j is called *timed*.

Let $\boldsymbol{m}_0$ be the initial marking of the system, the set of candidate markings for the enabling of a transition $t_j \in T_q$ can be formally defined as $\mathcal{M}(t_j, q) = \big\{\boldsymbol{m}_k \mid \exists \mathfrak{S}_T^{'}, \mathfrak{S}_T^{''}, \mathfrak{S} = \mathfrak{S}_T^{'}\mathfrak{S}_T^{''}, \ \boldsymbol{m}_0[\mathfrak{S}_T^{'}\rangle\boldsymbol{m}_k[\mathfrak{S}_T^{''}\rangle\boldsymbol{m}_q$, with $t_j \in \mathfrak{S}_T^{''}$, $k < q : \tau_k + l_j \le \tau_q \le \tau_k + u_j\big\}$, having cardinality $|\mathcal{M}(t_j, q)|$.

The set T_q can be partitioned into the couple of sets (T_q^t, T_q^{im}): $T_q^t = \{t_j \in T_q \mid \exists k, \boldsymbol{m}_k \in \mathcal{M}(t_j, q)\}$ is the set of transitions fired at τ_q with timed firing, with cardinality $n_q^t = |T_q^t|$, $T_q^{im} = T_q \setminus T_q^t$, with cardinality n_q^{im}, is the set of transitions fired at τ_q with immediate firing.

Immediate firings always follow the timed ones, even if they are observed at the same time τ_q. Indeed an immediate firing occurs at the same time it has been enabled, while a timed firing occurs in a subsequent time respect the one at which it has been enabled. Consequently, a timed firing enabled by an immediate firing occurred at time τ_q, surely fires in a time greater than τ_q.

The firing of transitions in the set T_q^t is concurrent, however, each firing can have been enabled at a different marking. On the other hand, the firing of transitions in T_q^{im} may be sequential. Given the set of transitions T_q^{im}, these transitions can fire in any order, which, anyway, can include concurrent transition firings.

Denote $\boldsymbol{m}_{q_1}$ the marking reached by firing transitions belonging to T_q^t, Denote $\boldsymbol{m}_{q_s}$, with $s \ge 2$, the marking reached after the immediate firings of transitions.

Given the firing sequence associated to the set T_q^{im}, it can be considered made up of the union of n_q^{im} disjoint subsets of concurrent transition firings. Hence, firing of transitions in T_q^{im} can be considered occurred in n_q^{im} substeps; each substep is denoted by q_s, with $s \in [2, n_q^{im} + 1]$. Finally, it holds that $T_q^{im} = \bigcup_{s=2}^{n_q^{im}+1} T_{q_s}^{im}$.

3. PROBLEM FORMULATION AND REPAIR MODEL ALGORITHM

Two techniques are used to repair the system nominal model to identify a repaired model able to generate the observed faulty behavior: a) the extension of the transition firing intervals; b) the addition of one fault transition for each observed anomaly.

At the generic observation step q two kinds of anomalies can be observed: *unexpected firings* of transitions - a transition fires after a time less than (greater than) its lower (upper) bound - and *missing firings* of transitions - a transition does not fires at τ_q even though it has been enabled for a time equal to its upper bound. Consequently, *the faulty behavior of the system at time* τ_q is characterized by the couple (T_q^{un}, T_q^{miss}), where the set T_q^{un} collects all those transitions for which an unexpected firing occurred at time τ_q and the set T_q^{miss} collects all those transitions for which a missing firing occurred at time τ_q.

Notice that $T_q^{un} \bigcap T_q^{miss} = \emptyset$.

An approach to model repair of TPN models has been presented by the authors in Basile et al. (2016a), as well. Now, authors introduce an incremental algorithm that receives as input the current model of the system and the observed timed firing sequence, and returns as output the repaired model identified by means of the two above mentioned techniques.

In Fig. 1, the repaired model identification algorithm is shown. It works on the basis of a timed firing sequence obtained starting from event observation and enriched by additional information, precisely, time-out occurrences (the term *time-out* is used to denote that nothing else is observed but a transition, enabled for a time equal to the upper bound of its firing interval, does not fire) and firing of fault transitions added to the nominal model.

Let denote S_q as the repaired model at step q and $\mathfrak{S}_k$ the timed firing sequence obtained terminating $\mathfrak{S}$ at the step k. At each step q, the current timed firing sequence $\mathfrak{S}_q$ is build in according to the following algorithm:

Algorithm 1: Building/updating of $\mathfrak{S}_q$.

Input: $\mathfrak{S}_{old}$, t_j (only needed for $\mathfrak{S}_q$ updating) ;
Output: $\mathfrak{S}_q$.