Automatica 96 (2018) 201–212

Contents lists available at ScienceDirect

Automatica

journal homepage: www.elsevier.com/locate/automatica

Model-based fault identification of discrete event systems using partially observed Petri nets[☆]

Guanghui Zhu [a,c], Zhiwu Li [b,a,*], Naiqi Wu [b]

[a] School of Electro-Mechanical Engineering, Xidian University, Xi'an, China
[b] Institute of Systems Engineering, Macau University of Science and Technology, Taipa, Macau
[c] Aix Marseille University, Universite de Toulon, CNRS, LIS, Marseille, France

ARTICLE INFO

Article history:
Received 9 August 2016
Received in revised form 19 March 2018
Accepted 10 June 2018

Keywords:
Fault identification
Petri net
Integer linear programming
Discrete event system

ABSTRACT

This paper deals with the problem of fault identification in a system. The system is originally modeled by a Petri net, called a nominal (fault-free) net, and faults are considered as unobservable transitions not contained in the nominal net. It is assumed that partial places of the nominal net are observable and the output of the system is defined as an *observed evolution*, i.e., a sequence involving transitions and markings of the observable places. When faults occur, the observed evolution cannot be generated by the nominal net. We provide an approach that identifies unobservable transitions by constructing and solving an Integer Linear Programming problem according to the observed evolution and the nominal net. A faulty net is obtained by adding the identified unobservable transitions to the nominal one such that it coincides with the observed evolution. In addition, two methods to ensure acyclicity of the identified subnet, i.e., a net that includes unobservable transitions only, are reported.

1. Introduction

The dynamic behavior of a system can be described by its outputs, i.e., the measured data during the system operation. Model identification consists in inferring a mathematical model from the knowledge of the measured data such that the behavior of a system can be characterized by the model. As a kind of discrete event system models, Petri nets provide graphical description and exact mathematical definition for the causal relationship among processes such as sequence, concurrency, and conflict, and rich results exist for supervisory control (Chen, Li, Barkaoui, & Giua, 2015; Chen, Li, Barkaoui, & Uzam, 2014; Chen, Li, Barkaoui, Wu, & Zhou, 2017), fault diagnosis (Basile, Chiacchio, & De Tommasi, 2009; Cabasino, Giua, & Seatzu, 2010; Dotoli, Fanti, Mangini, & W, 2009; Ru & Hadjicostis, 2009), and knowledge discovery (Liu, You, Li, & Tian, 2017; van der Aalst, 2011) based on Petri nets. Thus, Petri nets are usually considered as models for the problem of model identification in computer science and automatic control domain.

In the context of automatic control, there is a deluge of studies focusing on the identification of discrete event systems (DES) using Petri nets. In these studies, a Petri net model is derived by executing an algorithm or solving an Integer Linear Programming (ILP) problem. A related problem to model identification is fault identification, called model repair (Basile, Chiacchio, & Coppola, 2016a) or identification of unobservable behavior (Dotoli, Fanti, Mangini, & Ukovich, 2011), which estimates the faults in a system according to the nominal model (also called *fault-free* model) and outputs of the system. In other words, if faults exist in a system, anomalous outputs may be observed, which cannot be generated by the nominal model. Fault identification consists in determining a faulty model by refining the nominal one such that it coincides with the anomalous outputs.

The key issue of fault identification is how to define and represent a fault in a model. Wu and Hadjicostis in Wu and Hadjicostis (2005) define two types of faults in a Petri net model: transition and place faults. A transition fault occurs if tokens in the input places of a transition are not removed or no token is deposited into its output places even though the transition has fired. A place fault denotes that the place contains incorrect number of tokens after firing a transition. The faults can be detected by introducing redundancy into the given net model.

[☆] This work was supported in part by the National Natural Science Foundation of China under Grant Nos. 61374068 and 61703321, in part by the Science and Technology Development Fund, MSAR, under Grant Nos. 078/2015/A3, 112/2017/A3, and 106/2016/A3, and in part by the State Scholarship Fund of China under Grant No. 201700260156. The material in this paper was not presented at any conference. This paper was recommended for publication in revised form by Associate Editor Christoforos Hadjicostis under the direction of Editor Christos G. Cassandras.

[*] Corresponding address: Institute of Systems Engineering, Macau University of Science and Technology, Taipa, Macau, SAR China.

E-mail addresses: zhuguanghui86@gmail.com (G. Zhu), zhwli@xidian.edu.cn (Z. Li), nqwu@must.edu.mo (N. Wu).

https://doi.org/10.1016/j.automatica.2018.06.039
0005-1098/

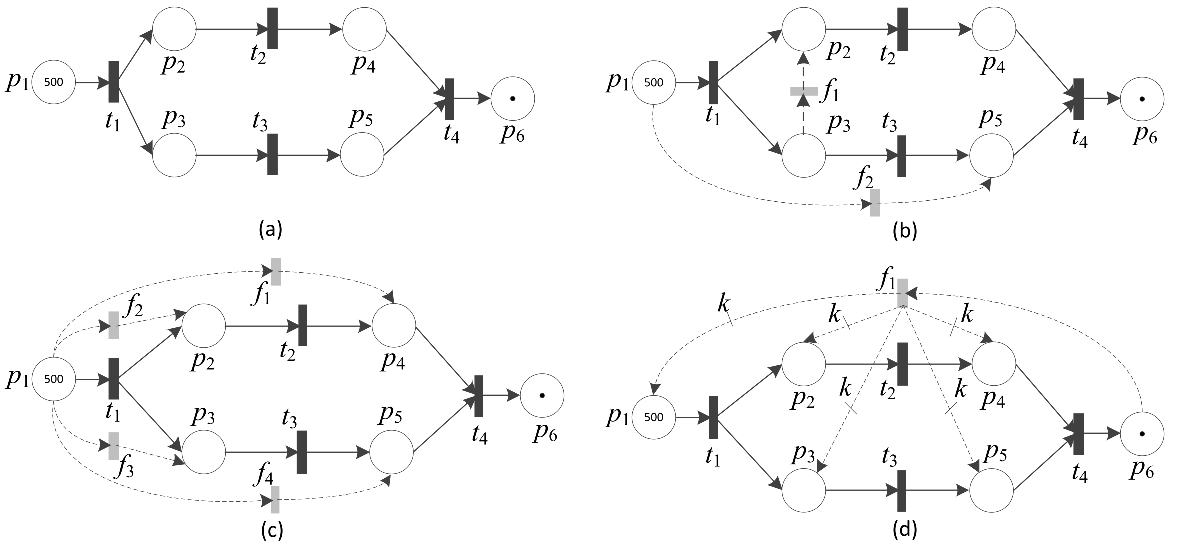

Fig. 1. (a) A fault-free net N_1, (b) a faulty net N_2 with two fault transitions, (c) a possible faulty net N_3 with four fault transitions, and (d) a possible faulty net N_4 with one fault transition.

On the other hand, the faults are considered as unobservable transitions that are not contained in the nominal net model in Basile et al. (2016a), Basile, Chiacchio, and Coppola (2016b), Cabasino, Giua, Hadjicostis, and Seatzu (2015) and Dotoli et al. (2011). Based on the fault-free net model and the anomalous observation of a system, these faults can be identified by solving ILP problems. This paper preserves such a definition of a fault and presents an approach that can provide estimations for the number and locations of faults on the basis of more information that the system exhibits during its operation.

1.1. Motivation

In Basile et al. (2016a, b), given a fault-free net, the authors assume that the observed outputs are multiple transition sequences with time instances. An ILP problem is built based on these transition sequences and fault transitions are identified by solving ILP problems. Cabasino et al. (2015) consider a language of a net with the length of its longest word less than or equal to a given positive integer as the output of a system. They also build and solve an ILP problem for the identification of faults from the knowledge of anomalous observations.

The aforementioned studies assume that all places of the fault-free net are unobservable, i.e., the observation contains transition sequences only, without information on the markings of the net. In some cases (for example there are many tokens in several places), the proposed approaches do not work well because of a large number of possible solutions. We next provide an intuitive example to demonstrate this.

Example 1. Consider a net model N_1 of a system shown in Fig. 1(a). Assume that transitions t_1, t_2, t_3, t_4 are observable and the observation contains observable transitions only. If transition sequence $t_1t_2t_2t_4$ is observed, we infer that one or more faults have occurred since sequence $t_1t_2t_2t_4$ cannot be generated in N_1. The real faults are shown in Fig. 1(b), which are modeled by unobservable transitions f_1 and f_2 graphically depicted by gray bars with dashed lines. Our goal is to identify possible faults by modifying the fault-free net N_1 such that the transition sequence $t_1t_2t_2t_4$ can be observed in the modified one. Two special solutions are given in Fig. 1(c) and (d).

Net N_3 shown in Fig. 1(c) is a possible solution since the sequence $t_1t_2t_2t_4$ can be observed. For example, if the firing sequence is $t_1t_2f_2t_2f_4t_4$, then the corresponding observed sequence is $t_1t_2t_2t_4$ (fault transitions f_2 and f_4 are unobservable). We observe that N_3 has four fault transitions and place p_1 has many tokens. Each other place can "borrow" a token from p_1 by firing a fault transition. Net N_4 shown in Fig. 1(d) is another possible solution, where k represents a large positive integer. It has only one fault transition, but this transition can deposit a large number of tokens into its output places. We have an intuition from these two solutions that there may exist a large number of solutions for the identification of faults in this example, i.e., it is difficult to find the solution that coincides with the real physical faults in a system because of too many possibilities if only transition sequences can be observed.

However, if more information on the evolution of a system is provided, a more accurate estimation of faults can be obtained. For example, if all places of N_1 are observable, i.e., there is a sensor associated with each place, and the observed output is

$$\begin{bmatrix}500\\0\\0\\0\\0\\1\end{bmatrix} t_1 \begin{bmatrix}499\\1\\1\\0\\0\\1\end{bmatrix} t_2 \begin{bmatrix}499\\0\\1\\1\\0\\1\end{bmatrix} \begin{bmatrix}499\\1\\0\\1\\0\\1\end{bmatrix} t_2 \begin{bmatrix}499\\0\\0\\2\\0\\1\end{bmatrix} \begin{bmatrix}498\\0\\0\\2\\1\\1\end{bmatrix} t_4 \begin{bmatrix}498\\0\\0\\1\\0\\2\end{bmatrix}$$

where each column vector (except the first one) gives the observed marking after firing an observable transition or the number of tokens in one of the observable places changes. In such a case, the faulty net shown in Fig. 1(b) can be readily obtained. Moreover, studies have been conducted on the identification of Petri nets under the condition that all places of a net are observable (Dotoli, Fanti, & Mangini, 2008; Dotoli et al., 2011; Estrada-Vargas, López-Mellado, & Lesage, 2014; Wu & Hadjicostis, 2005; Zhu, Li, Wu, & Al-Ahmari, 2017).

Different from the condition in Basile et al. (2016a, b) and Cabasino et al. (2015) that the observation contains transitions only (though the time instances of transitions are also observed in Basile et al., 2016a, b), the work in Dotoli et al. (2011) explores the identification of faults under the assumption that all places of the fault-free net are observable and thus the observed output is a transition-marking sequence, i.e., a transition is followed by a marking. However, in some cases, it is difficult to associate each place with a sensor because of the technical or financial consideration.