Automatica 51 (2015) 123–130

Contents lists available at ScienceDirect

Automatica

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

Brief paper

Robust prognosability for a set of partially observed discrete event systems☆

Shigemasa Takai [1]

Division of Electrical, Electronic and Information Engineering, Osaka University, Suita, Osaka 565-0871, Japan

ARTICLE INFO

Article history:
Received 14 May 2013
Received in revised form
13 September 2014
Accepted 29 September 2014

Keywords:
Discrete event system
Failure prognosis
Robust prognosability
Robust prognoser

ABSTRACT

In this paper, we consider a robust failure prognosis problem for partially observed discrete event systems. Given a set of possible models, each of which has its own nonfailure specification, we consider a single prognoser such that, for all possible models, it predicts any failure prior to its occurrence. We call such a prognoser a robust prognoser. We introduce a notion of robust prognosability and show that it serves as a necessary and sufficient condition for the existence of a robust prognoser. We then present a method for verifying the robust prognosability condition. Moreover, we discuss online synthesis of a robust prognoser.

1. Introduction

Recently, failure prognosis of discrete event systems (DESs) has received considerable attention. Prognosis of a failure is important to perform corrective actions for the occurrence of an impending failure. In Genc and Lafortune (2009), a problem of predicting the occurrence of a significant event such as a failure event was formulated for partially observed DESs. A notion of predictability introduced in Genc and Lafortune (2009) means that, for any impending significant event, it is unambiguously known that it occurs within a uniformly bounded number of steps. A polynomial algorithm was developed to verify predictability in Genc and Lafortune (2009). The notion of predictability was extended to predict the occurrence of a certain sequence pattern in Jéron, Marchand, Genc, and Lafortune (2007).

A notion of indicator strings was introduced to capture inevitability of a future failure in the setting of temporal logic (Jiang & Kumar, 2004). A nonfailure string is said to be an indicator string if a failure is guaranteed to occur in future. Using the notion of indicator strings, a decentralized failure prognosis problem was studied in Kumar and Takai (2010), where a nonfailure specification language is specified, and a failure is modeled by violation of the specification language. A notion of prognosability was introduced to characterize the class of systems such that inevitability of any failure is detected (Kumar & Takai, 2010). A polynomial algorithm was presented to verify prognosability in Kumar and Takai (2010). The results of Kumar and Takai (2010) were extended to inference-based prognosis (Takai & Kumar, 2011), prognosis in a general decentralized architecture (Khoumsi & Chakib, 2012), and distributed prognosis under bounded delay communications (Takai & Kumar, 2012). Failure prognosis was also studied in the stochastic setting in Chen and Kumar (2014).

Model uncertainty is one of the important issues in model-based approaches to DESs (Kwong & Yonge-Mallo, 2011; Lin, 1993; Young & Garg, 1995). Young and Garg (1995) considered a case where a set of possible models, which includes the exact model of a system, is given, and developed an algorithm to determine the exact model from the set of possible models. If the exact model cannot be determined, then we need a scheme that does not require the resolution of the model uncertainty. In the context of supervisory control of DESs (Ramadge & Wonham, 1987), a robust supervisory control problem was formulated in Lin (1993). This problem requires us to synthesize a single supervisor that achieves the legal behavior for all possible models. The result of Lin (1993) was extended in several ways in Bourdon, Lawford, and Wonham (2005), Saboori and Hashtrudi Zad (2006) and Takai (2000). In addition, a robust failure diagnosis problem was considered in Carvalho, Moreira, and Basilio (2011) and Takai (2012a). The objective of the robust failure diagnosis problem is to synthesize a single diagnoser such that, for all possible models, it detects the

☆ This work was supported in part by Grant-in-Aid for Scientific Research (No. 24560547). The material in this paper was partially presented at the 2012 American Control Conference (ACC2012), June 27–29, 2012, Montreal, Canada. This paper was recommended for publication in revised form by Associate Editor Jan Komenda under the direction of Editor Ian R. Petersen.

E-mail address: takai@eei.eng.osaka-u.ac.jp.

[1] Tel.: +81 6 6879 7693; fax: +81 6 6879 7263.

http://dx.doi.org/10.1016/j.automatica.2014.10.104

occurrence of any failure within a uniformly bounded number of steps.

Prior works on failure prognosis mentioned above assume that a single model of a system to be prognosed is given. In this paper, we assume as in Bourdon et al. (2005), Saboori and Hashtrudi Zad (2006) and Takai (2012a) that a set of possible models, each of which has its own nonfailure specification, is given and consider a robust failure prognosis problem. We first introduce a notion of prognosability, called *robust prognosability*, for a set of possible models with respect to a set of nonfailure specification languages and compare it with the existing notion of prognosability. Then, we show that robust prognosability is a necessary and sufficient condition for the existence of a single prognoser such that, for all possible models, it detects inevitability of any failure. Such a prognoser is called a *robust prognoser*. Furthermore, we present methods for verifying the robust prognosability condition and synthesizing a robust prognoser as an online prognoser.

The robust prognosis problem is different from the decentralized/distributed prognosis problems considered in Khoumsi and Chakib (2012), Kumar and Takai (2010) and Takai and Kumar (2011, 2012). In the setting of robust prognosis, a single prognoser prognoses multiple models, whereas multiple prognosers prognose a single model in the setting of decentralized/distributed prognosis.

Kwong and Yonge-Mallo (2011) studied failure diagnosis using incomplete DES models. They assumed that the given nominal model is missing some transitions that exist in the system to be diagnosed and proposed learning diagnosers to deal with the existence of such missed transitions. In this paper, we consider a different type of model uncertainty and take the different approach.

This paper is an extended version of Takai (2012b). It generalizes the results of Takai (2012b) by allowing the existence of deadlocking states and contains technical proofs omitted in Takai (2012b) and some additional results. It is shown that the computational complexity for verifying robust prognosability can be reduced under the assumption that there is no deadlocking state.

2. Preliminaries

We consider a DES modeled as an automaton $G = (Q, \Sigma, f, q_0)$, where Q is the set of states, Σ is the finite set of events, $f : Q \times \Sigma \to Q$ is the partial state transition function, and $q_0 \in Q$ is the initial state. Let Σ^* be the set of all finite strings of elements of Σ, including the empty string ε. The state transition function $f : Q \times \Sigma \to Q$ can be generalized to $f : Q \times \Sigma^* \to Q$ in the usual manner. The notation $f(q, s)!$ means that $f(q, s)$ is defined for $q \in Q$ and $s \in \Sigma^*$. In addition, $\neg f(q, s)!$ denotes the negation of $f(q, s)!$. The generated language of G, denoted by $L(G)$, is defined as $L(G) = \{s \in \Sigma^* \mid f(q_0, s)!\}$. Furthermore, the set of deadlocking strings is defined as $L_d(G) = \{s \in L(G) \mid \{s\}\Sigma \cap L(G) = \emptyset\}$.

For each $s \in \Sigma^*$, $|s|$ denotes its length. (Note that, for a finite set A, $|A|$ denotes the number of its elements.) The set of all prefixes of s is denoted by $pr(s)$. Let $K \subseteq \Sigma^*$ be a language. The set of all prefixes of strings in K is defined as $pr(K) = \bigcup_{s \in K} pr(s) = \{t \in \Sigma^* \mid \exists u \in \Sigma^* : tu \in K\}$. If $K = pr(K)$, K is said to be (prefix-)closed. The postlanguage of K after s is defined as $K/s = \{t \in \Sigma^* \mid st \in K\}$.

3. Failure prognosis

A prognoser for G observes the occurrence of an event through the observation mask $M : \Sigma \to \Delta \cup \{\varepsilon\}$, where Δ is the set of symbols observed by a prognoser. An event $\sigma \in \Sigma$ with $M(\sigma) = \varepsilon$ is unobservable to a prognoser. The observation mask $M : \Sigma \to \Delta \cup \{\varepsilon\}$ is extended to $M : \Sigma^* \to \Delta^*$ in the usual manner. Strings $s, s' \in \Sigma^*$ are said to be indistinguishable (under M) if $M(s) = M(s')$. For any language $K \subseteq \Sigma^*$, $M(K) \subseteq \Delta^*$ is defined as $M(K) = \{M(s) \in \Delta^* | s \in K\}$. In addition, for any $\tau \in \Delta^*$ and any $K' \subseteq \Delta^*$, $M^{-1}(\tau) \subseteq \Sigma^*$ and $M^{-1}(K') \subseteq \Sigma^*$ are defined as $M^{-1}(\tau) = \{s \in \Sigma^* | M(s) = \tau\}$ and $M^{-1}(K') = \{s \in \Sigma^* | M(s) \in K'\}$, respectively.

A prognoser is formally defined as a function $\mathcal{P} : \Delta^* \to \{0, 1\}$. If $\mathcal{P}$ is certain that a failure is guaranteed to occur in future, then it issues the decision "1". Otherwise, the decision "0" is issued by $\mathcal{P}$. Let $K \subseteq L(G)$ be a nonempty closed sublanguage that describes the nonfailure behavior of the system G. The fault behavior of G is represented by $L(G) - K$. The notions of *boundary* strings (for which a failure can occur in a next step), *indicator* strings (for which a failure in future is guaranteed), and *nonindicator* strings (that are not indicator strings) are defined as follows.

Definition 1 (*Kumar & Takai, 2010*)**.** For any closed language $K \subseteq L(G)$,

- the set $\partial_{L(G)}(K)$ of *boundary* strings of K with respect to $L(G)$ is defined as

$$\partial_{L(G)}(K) = \{s \in K \mid \{s\}\Sigma \cap (L(G) - K) \neq \emptyset\};$$

- the set $\Im_{L(G)}(K)$ of *indicator* strings of K with respect to $L(G)$ is defined as

$$\Im_{L(G)}(K) = \{s \in K \mid \exists m \in \mathcal{N},\ \forall t \in L(G)/s : [|t| \geq m \vee st \in L_d(G)] \Rightarrow st \in L(G) - K\};$$

- the set $\Upsilon_{L(G)}(K)$ of *nonindicator* strings of K with respect to $L(G)$ is defined as

$$\Upsilon_{L(G)}(K) = K - \Im_{L(G)}(K).$$

Remark 2. In Definition 1, the definition of $\Im_{L(G)}(K)$ of Kumar and Takai (2010) is extended in the presence of deadlocking strings.

It follows from the definition of indicator strings that any nonfailure extension of an indicator string is also an indicator string. That is, the following lemma, which will be used later, holds.

Lemma 3. *Let $K \subseteq L(G)$ be a nonempty closed language. For any $s \in K$, if $s \in \Im_{L(G)}(K)$, then $\{s\}\Sigma^* \cap K \subseteq \Im_{L(G)}(K)$.*

A prognoser $\mathcal{P} : \Delta^* \to \{0, 1\}$ is required to satisfy the following condition:

(C1) $\forall s \in L(G) - K,\ \exists t \in pr(s) \cap K : \mathcal{P}(M(t)) = 1.$

The condition (C1) means that the occurrence of any failure is predicted prior to its occurrence. In addition, $\mathcal{P}$ is required to issue the decision "1" only if a failure is guaranteed to occur in future. That is, $\mathcal{P}$ should also satisfy the following condition:

(C2) $\forall s \in \Upsilon_{L(G)}(K) : \mathcal{P}(M(s)) \neq 1.$

The following definition of prognosability of G was introduced in Kumar and Takai (2010).

Definition 4 (*Kumar & Takai, 2010*)**.** The system G is said to be *prognosable* with respect to a nonempty closed language $K \subseteq L(G)$ if

$$\forall s \in L(G) - K, \quad \exists t \in pr(s) \cap K : M^{-1}M(t) \cap K \subseteq \Im_{L(G)}(K).$$

As shown in the following proposition, G is prognosable if and only if each boundary string in $\partial_{L(G)}(K)$ can be distinguished from any nonindicator string in $\Upsilon_{L(G)}(K)$.

Proposition 5 (*Kumar & Takai, 2010*)**.** *The system G is prognosable with respect to a nonempty closed language $K \subseteq L(G)$ if and only if $\partial_{L(G)}(K) \cap M^{-1}M(\Upsilon_{L(G)}(K)) = \emptyset$.*

Given a nonempty closed language $K \subseteq L(G)$, there exists a prognoser $\mathcal{P} : \Delta^* \to \{0, 1\}$ that satisfies (C1) and (C2) if and only if G is prognosable with respect to K (Kumar & Takai, 2010).