Robust Fault Diagnosis of Stochastic Discrete Event Systems

Xiang Yin, *Member, IEEE*, Jun Chen, *Member, IEEE*, Zhaojian Li, *Member, IEEE*, and Shaoyuan Li, *Senior Member, IEEE*

***Abstract*—We investigate the problem of robust fault diagnosis of stochastic discrete-event systems against model uncertainty. In this problem, we assume that the actual behavior of the system is unknown *a priori* and the true model of the system belongs to a set of possible models described by probabilistic automata. The goal of this problem is to almost successfully detect the occurrence of fault in the sense that, first, no false alarm can be made, and second, the misdetection rate is smaller than a given threshold ϵ after some delay K even without knowing the true model *a priori*. A condition termed as robust (ϵ, K)-diagnosability is proposed to capture the existence of such a robust diagnoser that satisfies the above-mentioned requirements. We also propose the notions of robust ϵ-diagnosability and robust A-diagnosability, which require that a given misdetection rate ϵ can be achieved with some delay and any arbitrarily small misdetection rate can be achieved, respectively. For each condition, an effective verification algorithm is also proposed. Our results generalize previous works on fault diagnosis of stochastic discrete-event systems by taking model uncertainty and specific misdetection rate into account.**

***Index Terms*—Discrete-event systems, fault diagnosis, model uncertainty, robustness, stochastic systems.**

I. Introduction

In large-scale complex automated systems, one important task is to detect and isolate faults in the systems. This leads to the fault diagnosis problem, which has drawn considerable attention in the general systems literature. In this technical note, we are concerned with the problem of fault diagnosis of discrete-event systems (DES).

In [29], a language-based approach for fault diagnosis was developed by using DES models. Specifically, the condition of diagnosability was proposed to capture *a priori* whether or not a fault can always be detected within a finite delay. One significant advantage of the DES approach to fault diagnosis is that it is a model-based approach. Therefore, we can formally analyze and infer the system's behavior based on limited observations. Since the seminal work of [29], online fault diagnosis as well as diagnosability analysis have drawn considerable attention in the DES literature; see, e.g., [6], [11], [16], [21], [27], [30], [39], and a recent survey [42] for extensive references.

In many real-world DES, the dynamics of the systems are inherently stochastic, i.e., each event occurrence has its associated probability. Therefore, stochastic DES provides a more realistic way for the analysis of system's behavior. Consequently, state estimation and fault diagnosis of stochastic DES have been widely studied in recent literature (see, e.g., [1]–[4], [12], [13], [18], [23]–[25], [34], [38], [40]). Particularly, in [34], the condition of A-diagnosability was proposed to capture the existence of a stochastic diagnoser that produces no false alarm and arbitrarily small misdetection. This condition is very useful in practice since diagnosability may be too strong in many applications; A-diagnosability does not require a bounded delay but guarantees that the probability of detecting the fault for sure converges to one as the length of observation increases. The condition of A-diagnosability is also termed as SS-diagnosability in [13] and it has been shown in [4] and [12] that verifying A-diagnosability is PSPACE complete. Since the work of [34], several variations of A-diagnosability have also proposed. For example, in [23], the authors generalize it to the case of safe diagnosis and in [24], the condition A-co-diagnosability was proposed to study the decentralized diagnosis problem.

On the other hand, since uncertainties are generally unavoidable in real-world systems, robustness is also an important aspect in the analysis of DES. In the context of fault diagnosis, the problem of robust fault diagnosis has been studied by many works in the literature (see, e.g., [7]–[9], [17], [31], [33], [35]). For example, in [7], [9], [17], [33], and [35], the authors have studied the robust fault diagnosis problem under permanent or intermittent sensor failures. In [8], [19], [20], and [31], the authors investigate the robust fault diagnosis problem with model uncertainties. The effect of model uncertainties has also been considered in fault prognosis problem [32] and supervisory control problem [5], [22], [28], [37].

However, all of the above-mentioned works are still based on the logical DES. In this paper, we study the robust fault diagnosis problem of stochastic discrete-event systems. Specifically, we assume that we do not know the system's model *a priori* and the true model belongs to a set of possible models described by probabilistic automata. The contributions of this paper are as follows. First, we propose the condition of robust (ϵ, K)-diagnosability as a necessary and sufficient condition under which, first, a fault can always be detected with a misdetection rate smaller than ϵ within K steps, and second, no false alarm can be made, even we do not know the true model *a priori*. This condition also generalizes the well known K-diagnosability condition [42] to the stochastic and robust setting by considering the misdetection rate after K steps. Then, we define the condition of robust ϵ-diagnosability by requiring that the system is robust (ϵ, K)-diagnosability for some K. Finally, we say that the system is robustly A-diagnosable if it is robustly ϵ-diagnosable for an arbitrarily small misdetection rate ϵ. Robust A-diagnosability essentially requires that the misdetection rate will converge to zero as more events are executed after the occurrence of

Manuscript received April 14, 2018; revised November 19, 2018; accepted January 11, 2019. Date of publication January 18, 2019; date of current version September 25, 2019. This work was supported by the National Natural Science Foundation of China (61803259, 61833012). Recommended by Associate Editor C. N. Hadjicostis. *(Corresponding author: Xiang Yin.)*

X. Yin and S. Li are with the Department of Automation, Key Laboratory of System Control and Information Processing, Shanghai Jiao Tong University, Shanghai 200240, China (e-mail: yinxiang@sjtu.edu.cn; syli@sjtu.edu.cn).

J. Chen is with the General Motors, Milford, MI 48381 USA (e-mail: jchenee2015@gmail.com).

Z. Li is with the Department of Mechanical Engineering, Michigan State University, East Lansing, MI 48824 USA (e-mail: lizhaoj1@egr.msu.edu).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TAC.2019.2893873

fault. This condition is stronger than A-diagnosability [34] since we consider also model uncertainty, but it is weaker than robust diagnosability [33] as we allow an arbitrarily small misdetection rate. We provide effective approaches for verifying these conditions. In particular, the complexity of the verification algorithm for robust A-diagnosability is exponential in the number of states but polynomial in the number of possible models. To the best of our knowledge, this is the first work that investigates robustness in the context of stochastic DES.

The rest of the paper is organized as follows. In Section II, we present necessary preliminaries. In Section III, the problem of robust fault diagnosis of stochastic DES is formulated and three different conditions for robust diagnosability in the stochastic setting are proposed. For each notion of robust diagnosability, an effective verification algorithm is presented in Section IV. Finally, we conclude the paper in Section V.

II. Preliminary

Let Σ be a finite set of events. A string is a finite sequence of events. We denote by Σ^* the set of strings over Σ with empty string ϵ. For any string $s \in \Sigma^*$, we denote by $|s|$ its length with $|\epsilon| = 0$. A language $L \subseteq \Sigma^*$ is a set of strings; we denote by $\overline{L}$ the prefix closure of L.

A DES is modeled by a finite-state automaton (FSA)

$$G = (X, \Sigma, \delta, x_0) \tag{1}$$

where X is the finite set of states, Σ is the finite set of events, $\delta : X \times \Sigma \to X$ is the partial transition function and x_0 is the initial state. Function δ is also extended to $X \times \Sigma^*$ in the usual manner [10]. Then, $\delta(x, s)$ is the state reached via string s from state x; we write $\delta(x, s)$ by $\delta(s)$ if $x = x_0$. We define $\mathcal{L}(G, x) = \{s \in \Sigma^* : \delta(x, s)!\}$ as the language generated by G from state $x \in X$, where "!" means "is defined". We write $\mathcal{L}(G, x)$ by $\mathcal{L}(G)$ if $x = x_0$. Given an FSA G, a *strongly connected component* (SCC) is a maximal set of states $C \subseteq X$ such that $\forall x_1, x_2 \in C, \exists s \in \Sigma^* : \delta(x_1, s) = x_2$. An SCC $C \subseteq X$ is said to be *terminal* if $\forall x \in C, \forall s \in \mathcal{L}(G, x) : \delta(x, s) \in C$.

We assume that $\Sigma_o \subseteq \Sigma$ is the set of observable events. Then, $P : \Sigma^* \to \Sigma_o^*$ is the natural projection defined by

$$P(\epsilon) = \epsilon \text{ and } P(s\sigma) = \begin{cases} P(s)\sigma & \text{if } \sigma \in \Sigma_o \\ P(s) & \text{if } \sigma \notin \Sigma_o \end{cases}$$

i.e., for any string $s \in \Sigma^*$, $P(s) \in \Sigma_o^*$ only keeps the observable events of s. Projection P is also extended to 2^{Σ^*} by: for any $L \subseteq \Sigma^*$, $P(L) = \{\alpha \in \Sigma_o^* : \exists s \in L \text{ s.t. } P(s) = \alpha\}$. We denote by P^{-1} the inverse projection.

The *observer* automaton for G is a new FSA $\text{Obs}(G) = (Q, \Sigma_o, f, q_0)$, where $Q \subseteq 2^X$ and $f : Q \times \Sigma_o \to Q$ is the transition function such that: for any $q \in Q, \sigma \in \Sigma_o$

$$f(q, \sigma) = \{x \in X : \exists x' \in q, \exists w \in \Sigma_{uo}^* \text{ s.t. } \delta(x', \sigma w) = x\}. \tag{2}$$

The initial state is defined by $q_0 = \{x \in X : \exists w \in \Sigma_{uo}^* \text{ s.t. } \delta(w) = x\}$. Note that, here we also consider $\emptyset$ as a state in the observer. Therefore, f is a total function over $Q \times \Sigma_o$. Then, $f(q, \sigma) = \emptyset$ implies that the observation is not consistent with the system model.

A stochastic discrete event system is then a pair (G, p), where G is an FSA and $p : X \times \Sigma \to [0, 1]$ is the transition probability function. For any $x \in X, \sigma \in \Sigma$, we write $p(\sigma \mid x)$ as the probability that event σ occurs from state x. We assume that p satisfies the following requirements:

1) $\forall x \in X, \sigma \in \Sigma : \delta(x, \sigma)! \Leftrightarrow p(\sigma \mid x) > 0$;
2) $\forall x \in X : \sum_{\sigma \in \Sigma} p(\sigma \mid x) = 1$.

The above-mentioned two conditions also imply that the system is *live*, i.e., $\forall x \in X, \exists \sigma \in \Sigma : \delta(x, \sigma)!$. The transition probability function is also extended to $p : X \times \Sigma^* \to [0, 1]$ recursively by: for any $x \in X, s \in \Sigma^*, \sigma \in \Sigma$, we have

$$p(s\sigma \mid x) = p(\sigma \mid \delta(x, s))p(s \mid x).$$

We write $p(s \mid x)$ as $p(s)$ when $x = x_0$.

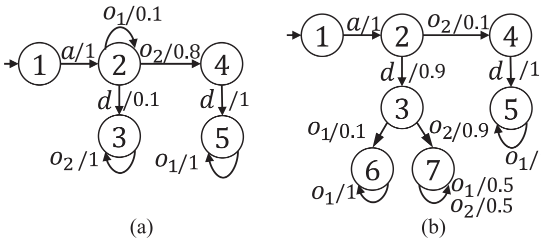


Fig. 1. Two possible models of a simple job processing plant, where $\Sigma_o = \{a, o_1, o_2\}$. The number associated with each transition denotes its transition probability. (a) (G_1, p_1). (b) (G_2, p_2).

Let $x \in X$ be a state and $L \subseteq \mathcal{L}(G, x)$ be a set of strings defined from x. Then, we define $\text{Prob}(L \mid x) = \sum_{s \in L} p(s \mid x)$. Let $\mathcal{L}_n(G, x) := \{s \in \mathcal{L}(G, x) : |s| = n\}$ be the set of all strings in $\mathcal{L}(G, x)$ with length n. It can be shown easily by induction that, for any $x \in X, n \geq 1$, we have $\text{Prob}(\mathcal{L}_n(G, x) \mid x) = 1$.

In the fault diagnosis problem, the system (G, p) is subject to fault. We assume that the normal behavior is modeled by a (nonstochastic) FSA $G^N = (X^N, \Sigma, \delta^N, x_0^N)$ such that $\mathcal{L}(G^N) \subseteq \mathcal{L}(G)$. Without loss of generality, we assume that G^N is a subautomaton of G such that $\forall s \in \mathcal{L}(G) \setminus \mathcal{L}(G^N) : \delta(s) \in X \setminus X^N$, where "$\setminus$" denotes "set difference". Therefore, X^N is the set of nonfaulty states and $X^F := X \setminus X^N$ is the set of faulty state. A string is fault if and only if it goes to a faulty state. We define

$$\Psi(G) := \{s \in \mathcal{L}(G) \setminus \mathcal{L}(G^N) : \forall t \in \overline{\{s\}} \setminus \{s\}, \delta(t) \in X^N\}$$

i.e., the set of strings in which fault occurs for the first time.

III. Robust Diagnosability of Stochastic DES

In the fault diagnosis problem, the goal is to infer the occurrence of a fault based on the observation. However, in many applications, we may not precisely know the model of the system. Instead, we may only know that the actual model belongs to a set of possible models. As a motivating example, let us consider a simple plant processing a job, which is adopted from [41] with some modifications. In this system, event a denotes "arrival of a job", event d denotes "departure of a job", and o_1 and o_2 denote two kinds of plant operations. We assume that the plant has two possible operation modes modeled by (G_1, p_1) and (G_2, p_2) in Fig. 1, respectively. We require that event d should not occur before the occurrence of event o_2; otherwise, we consider it as a fault. Therefore, state 3 is a faulty state in G_1 and states 3, 6, and 7 are faulty states in G_2. Since we do not know the precise operating mode of the system, the question then arises of how to detect the fault with model uncertainty.

To formalize this problem, we assume that the actual system belongs to a set of possible models

$$\{(G_1, p_1), (G_2, p_2), \ldots, (G_n, p_n)\} \tag{3}$$

where $G_i = (X_i, \Sigma, \delta_i, x_{0,i})$. We denote by $\mathcal{I} = \{1, 2, \ldots, n\}$ the index set. Each (G_i, p_i) is associated with a normal model $G_i^N = (X_i^N, \Sigma, \delta_i^N, x_{0,i}^N)$. Let $I \subseteq \mathcal{I}$ be a set of indices. We define

$$\mathcal{U}_I = \{s \in \cup_{i \in I} \mathcal{L}(G_i) : \exists i \in I, \exists t \in \mathcal{L}(G_i^N) \text{ s.t. } P(s) = P(t)\} \tag{4}$$

as the set of strings that can be confused with some nonfaulty strings in a model that belongs to set $I \subseteq \mathcal{I}$. Note that we assume that all possible models have the same event set Σ. This setting is without loss of generality since we can always extend the domain of the event set without changing the transition function.

A (robust) diagnoser is a function

$$D : \cup_{i\in\mathcal{I}} P(\mathcal{L}(G_i)) \to \{0, 1\} \tag{5}$$

that assigns each possible observation a diagnostic decision, where "0" means that "no fault is detected" while "1" means that "a fault is detected". In the stochastic setting, the diagnoser may not detect the occurrence of fault within a finite number of steps. Instead, it may guarantee that the probability of misdetection is smaller than a threshold within a given number of steps. Formally, let $\epsilon > 0$ be a misdetection rate and $K \in \mathbb{N}$ be a detection delay. We require that a robust diagnoser should satisfy the following conditions:

C1) $(\forall i \in \mathcal{I})(\forall s \in \Psi(G_i))$ s.t.
$\text{Prob}\left(\{t \in \mathcal{L}_K(G_i, \delta_i(s)) : D(P(st)) = 0\} \mid \delta_i(s)\right) < \epsilon$

C2) $(\forall i \in \mathcal{I})(\forall s \in \mathcal{L}(G_i^N))[D(P(s)) = 0]$.

Intuitively, the first condition requires that, no matter what the true model is, for any faulty string, the misdetection rate is smaller than ϵ in K steps after the occurrence of fault. The second condition requires that a false alarm should never be generated when the system is operating normally.

Next, we investigate under what condition there exists a robust diagnoser satisfying (C1) and (C2). First, we propose the notion of robust (ϵ, K)-diagnosability.

Definition 3.1: Given a misdetection rate $\epsilon > 0$ and a delay $K \in \mathbb{N}$, the set of possible models $\{(G_i, p_i) : i \in \mathcal{I}\}$ is said to be robustly (ϵ, K)-diagnosable if for any $i \in \mathcal{I}, s \in \Psi(G_i)$, we have $\text{Prob}\left(\{t \in \mathcal{L}_K(G_i, \delta_i(s)) : st \in \mathcal{U}_\mathcal{I}\} \mid \delta_i(s)\right) < \epsilon$.

Intuitively, robust (ϵ, K)-diagnosability says that, no matter what the true model is, we can make sure that, for any faulty string, the probability that the observation can be confused with a nonfaulty string in a possible model is smaller than ϵ in K steps after the occurrence of fault. Recall that, for any $K \in \mathbb{N}$, $\text{Prob}\left(\{t \in \mathcal{L}_K(G_i, \delta_i(s))\} \mid \delta_i(s)\right) = 1$. Therefore, robust (ϵ, K)-diagnosability essentially evaluates the probability of detection in a step-based fashion.

In some cases, one is interested in achieving a given misdetection rate ϵ with *some* delay K. This leads to the definition of robust ϵ-diagnosability, which characterizes whether or not there exists a delay K such that the system is robustly (ϵ, K)-diagnosabale.

Definition 3.2: Given a misdetection rate $\epsilon > 0$, the set of possible models $\{(G_i, p_i) : i \in \mathcal{I}\}$ is said to be robustly ϵ-diagnosable if there exists a delay $K \in \mathbb{N}$ such that $\{(G_i, p_i) : i \in \mathcal{I}\}$ is robustly (ϵ, K)-diagnosable.

Remark 3.1: The proposed notions of robustly (ϵ, K)-diagnosability and robustly ϵ-diagnosability are closely related to the concept of diagnosability degree studied in [2], where the average detection time of faults is investigated. However, our notions focus on how fast the probability of detection converges to a given threshold and we provide matrix-based approaches for verifying these conditions.

Finally, in some applications, we may want the diagnoser to achieve an arbitrarily small misdetection rate ϵ. This leads to the definition of robust A-diagnosability as follows.

Definition 3.3: The set of possible models $\{(G_i, p_i) : i \in \mathcal{I}\}$ is said to be robustly A-diagnosable if for any $\epsilon > 0$, $\{(G_i, p_i) : i \in \mathcal{I}\}$ is robustly ϵ-diagnosable.

The following theorem reveals that robust (ϵ, K)-diagnosability is indeed a necessary and sufficient condition for the existence of a robust diagnoser satisfying conditions (C1) and (C2) simultaneously.

Theorem 3.1: Given $\epsilon > 0$ and $K \in \mathbb{N}$, there exists a diagnoser satisfying conditions (C1) and (C2) if and only if $\{(G_i, p_i) : i \in \mathcal{I}\}$ is robustly ϵ-diagnosable.

Proof: $(\Rightarrow)$ We prove the necessity by contradiction. Suppose that there exists a diagnoser D satisfying conditions (C1) and (C2) and assume that $\{(G_i, p_i) : i \in \mathcal{I}\}$ is not robustly (ϵ, K)-diagnosable. Then, there exist $i \in \mathcal{I}$ and a faulty string $s \in \Psi(G_i)$ such that $\text{Prob}\left(\{t \in \mathcal{L}_K(G_i, \delta_i(s)) : st \in \mathcal{U}_\mathcal{I}\} \mid \delta_i(s)\right) \geq \epsilon$. Since diagnoser D satisfies condition (C2), we know that for any $st \in \mathcal{U}_\mathcal{I}$, $D(P(st)) = 0$; otherwise, if $D(P(st)) = 1$, then we know that $D(P(w)) = D(P(st)) = 1$ for some $w \in \mathcal{L}(G_j^N)$, which violates (C2). Therefore, we know that

$$\{t \in \mathcal{L}_K(G_i, \delta_i(s)) : st \in \mathcal{U}_\mathcal{I}\} \subseteq \{t \in \mathcal{L}_K(G_i, \delta_i(s)) : D(P(st) = 0\}$$

which means $\text{Prob}\left(\{t \in \mathcal{L}_K(G_i, \delta_i(s)) : D(P(st)) = 0\} \mid \delta_i(s)\right) \geq \epsilon$. Therefore, for the above chosen i and s, condition (C1) does not hold for diagnoser D, which is a contradiction.

$(\Leftarrow)$ Suppose that $\{(G_i, p_i) : i \in \mathcal{I}\}$ is robustly (ϵ, K)-diagnosable. We construct a diagnoser D by: for any $w \in \cup_{i\in\mathcal{I}} \mathcal{L}(G_i)$

$$D(P(w)) = \begin{cases} 1, & \text{if } P(w) \notin P(\mathcal{U}_\mathcal{I}) \\ 0, & \text{otherwise} \end{cases}. \tag{6}$$

Next, we claim that the above-mentioned constructed diagnoser satisfies conditions (C1) and (C2). To see that D satisfies (C2), let us consider an arbitrary model $i \in \mathcal{I}$ and arbitrary nonfaulty string $s \in \mathcal{L}(G_i^N)$. Since $s \in \mathcal{U}_\mathcal{I}$, we know that $P(s) \in P(\mathcal{U}_\mathcal{I})$. By (6), we know that $D(P(s)) = 0$, i.e., (C2) holds. To see that (C1) holds, let us consider arbitrary $i \in \mathcal{I}$ and $s \in \Psi(G_i)$. Since $\{(G_i, p_i) : i \in \mathcal{I}\}$ is robustly (ϵ, K)-diagnosable, we know that $\text{Prob}\left(\{t \in \mathcal{L}_K(G_i, \delta_i(s)) : st \in \mathcal{U}_\mathcal{I}\} \mid \delta_i(s)\right) < \epsilon$. Then, for any string $v \in \mathcal{L}_K(G_i, \delta_i(s))$ such that $D(P(sv)) = 0$, by (6), we know that $P(sv) \in P(\mathcal{U}_\mathcal{I})$, which further implies that $sv \in \mathcal{U}_\mathcal{I}$. Therefore, we know that

$$\{t \in \mathcal{L}_K(G_i, \delta_i(s)) : D(P(st)) = 0\} \subseteq \{t \in \mathcal{L}_K(G_i, \delta_i(s)) : st \in \mathcal{U}_\mathcal{I}\}.$$

Since $\text{Prob}\left(\{t \in \mathcal{L}_K(G_i, \delta_i(s)) : st \in \mathcal{U}_\mathcal{I}\} \mid \delta_i(s)\right) < \epsilon$, we know that $\text{Prob}\left(\{t \in \mathcal{L}_K(G_i, \delta_i(s)) : D(P(st)) = 0\} \mid \delta_i(s)\right) < \epsilon$, i.e., condition (C1) also holds. ■

Remark 3.2: It is worth remarking that the "⇐" part of the above-mentioned proof is actually constructive. That is, (6) also tells us how to construct a robust diagnoser satisfying (C1) and (C2) for a robustly ϵ-diagnosable system.

Remark 3.3: In the context of logical DES, the condition of K-diagnosability [42] has been proposed in the literature to capture whether or not any fault can be detected for sure within K steps after the occurrence of fault. Our definition of robust (ϵ, K)-diagnosability generalizes K-diagnosability to the stochastic setting by specifying a misdetection rate after K steps. Also, in [34], the condition of A-diagnosability was proposed in order to capture whether or not any fault can be detected with probability one by knowing the system model precisely; the reader is referred to [34] for its definition. By comparing robust A-diagnosability with A-diagnosability, we see that if the set of possible models is a singleton, i.e., $\mathcal{I} = \{1\}$, then robust A-diagnosability reduces to A-diagnosability. Therefore, our condition generalizes the condition of A-diagnosability in [34] by considering the issue of model uncertainty. This is also why we term our condition as robust A-diagnosability. However, our general case is more complicated to handle, as we do not know the true model *a priori* and a model identification problem is hidden in the robust diagnosis problem.

In the remainder of this paper, we will focus on the verification of robust (ϵ, K)-diagnosability, robust ϵ-diagnosability, and robust

A-diagnosability. Before, we formally present the algorithms, we first illustrate Definitions 3.1–3.3 by the following example.

Example 3.1: Let us still consider the motivating example and suppose we know that (G_1, p_1) and (G_2, p_2) shown in Fig. 1(a) and (b), respectively, are two possible models of the system. We assume that $X_1^N = \{1, 2, 4, 5\}, X_2^N = \{1, 2, 4, 5\}$ and $\Sigma_o = \{a, o_1, o_2\}$, i.e., d is the only unobservable event.

Then, we know that $\{(G_1, p_1), (G_2, p_2)\}$ is not robustly $(\epsilon, 1)$-diagnosable for any $\epsilon < 1$. To see this, first, we have $\mathcal{I} = \{1, 2\}$ and

$$\mathcal{U}_{\mathcal{I}} = \mathcal{L}(G_1^N) \cup \mathcal{L}(G_2^N) \cup \{a\}\{o_1\}^*\{d, do_2\} \cup \{ad\}\{\epsilon, o_2\}\{o_1\}^*.$$

If (G_1, p_1) is the true mode, then for any faulty string $s \in \Psi(G_1)$, we have $\mathcal{L}_1(G_1, \delta_1(s)) = \{o_2\}$ and

$$\mathrm{Prob}\left(\{\mathrm{t} \in \mathcal{L}_1(\mathrm{G}_1, \delta_1(\mathrm{s})) : \mathrm{st} \in \mathcal{U}_{\mathcal{I}}\} \mid \delta_1(\mathrm{s})\right) = 1.$$

Similarly, if (G_2, p_2) is the true mode, then for any faulty string $s \in \Psi(G_2)$, we have $\mathcal{L}_1(G_2, \delta_2(s)) = \{o_1, o_2\}$ and

$$\mathrm{Prob}\left(\{\mathrm{t} \in \mathcal{L}_1(\mathrm{G}_2, \delta_2(\mathrm{s})) : \mathrm{st} \in \mathcal{U}_{\mathcal{I}}\} \mid \delta_2(\mathrm{s})\right) = 1.$$

Therefore, it is not robustly $(\epsilon, 1)$-diagnosable for any $\epsilon < 1$.

However, it is robustly (0.2,5)-diagnosable. To see this, if (G_1, p_1) is the true mode, then for any faulty string $s \in \Psi(G_1)$ and $K \geq 2$, we have

$$\mathrm{Prob}\left(\{\mathrm{t} \in \mathcal{L}_{\mathrm{K}}(\mathrm{G}_1, \delta_1(\mathrm{s})) : \mathrm{st} \in \mathcal{U}_{\mathcal{I}}\} \mid \delta_1(\mathrm{s})\right) = 0.$$

If (G_2, p_2) is the true mode, then for any faulty string $s \in \Psi(G_2)$ and $K \geq 2$, we have

$$\mathrm{Prob}\left(\{\mathrm{t} \in \mathcal{L}_{\mathrm{K}}(\mathrm{G}_1, \delta_1(\mathrm{s})) : \mathrm{st} \in \mathcal{U}_{\mathcal{I}}\} \mid \delta_1(\mathrm{s})\right) = 0.1 + 0.9 \times 0.5^{\mathrm{K}-1}. \tag{7}$$

Moreover, according to (7), we see that any misdetection rate smaller than 0.1 cannot be achieved even when the delay goes to infinity. Therefore, this system is not robustly 0.1-diagnosable and hence, it is not robustly A-diagnosable.

IV. Verification of Robust Diagnosability

In this section, we investigate how to verify different notions of robust diagnosability in stochastic DES.

First, for any $i \in \mathcal{I}$, we define a new automaton

$$V_i = (X_i^V, \Sigma, \delta_{V_i}, q_{0,i}^V) := G_i \| \mathrm{Obs}(G_1) \| \mathrm{Obs}(G_2) \| \ldots \| \mathrm{Obs}(G_n) \tag{8}$$

where "$\|$" denotes the standard parallel composition (see, e.g., [10]) and $\mathrm{Obs}(G_i) = (Q_i, \Sigma_o, f_i, q_{0,i})$ is the observer automaton for model G_i. Recall that the transition function of each observer is total, i.e., $\mathcal{L}(\mathrm{Obs}(G_i)) = \Sigma_o^*$. Therefore, by the property of parallel composition, we know that $\mathcal{L}(V_i) = \mathcal{L}(G_i)$. Moreover, for any $s \in \mathcal{L}(V_i)$, we know that $\delta_{V_i}(s) = (\delta_i(s), f_1(P(s)), \ldots, f_n(P(s)))$. Automaton V_i is also referred to as the *verification automaton* hereafter. Note that we do not assume liveness of the system or the absence of unobservable cycle since V_i tracks the original behavior of the system. Similar construction has also used in the literature for different purposes, e.g., [14], [36].

Definition 4.1: A state $(x, q_1, q_2 \ldots, q_n) \in X_i^V$ in V_i is said to be

1) *robustly certain* if $x \in X_i^F$ and $\forall j \in \mathcal{I} : q_j \subseteq X_j^F$;
2) *robustly uncertain* if $x \in X_i^F$ and $\exists j \in \mathcal{I} : q_j \cap X_j^N \neq \emptyset$.

We denote by X_i^{cer} and X_i^{unc} the set of robustly certain and robustly uncertain states in V_i, respectively.

The following lemma establishes the relationship between robustly uncertain states and set $\mathcal{U}_{\mathcal{I}}$.

Lemma 4.1: For any $i \in \mathcal{I}$ and faulty string $s \in \mathcal{L}(G_i) \setminus \mathcal{L}(G_i^N)$, we have $s \in \mathcal{U}_{\mathcal{I}}$ if and only if $\delta_{V_i}(s) \in X_i^{\mathrm{unc}}$.

Proof: Suppose that $s \in \mathcal{U}_{\mathcal{I}}$ and denote $\delta_{V_i}(s) = (x, q_1, \ldots, q_n)$. Then, we know that $x = \delta(s) \in X_i^F$ and $\exists j \in \mathcal{I}, \exists t \in \mathcal{L}(G_j^N) : P(s) = P(t)$. This implies that $\delta_j(t) \in f_j(P(t)) = q_j$ and $\delta_j(t) \in X_j^N$. Therefore, $\delta_{V_i}(s) \in X_i^{\mathrm{unc}}$. Similarly, suppose that $\delta_{V_i}(s) \in X_i^{\mathrm{unc}}$. Then, we know that $\exists j \in \mathcal{I} : q_j \cap X_j^N \neq \emptyset$, i.e., $\{x \in X_j^N : \exists t \in \mathcal{L}(G_j) \text{ s.t. } x = \delta_j(t) \wedge P(s) = P(t)\} \neq \emptyset$. Therefore, we know that $\exists j \in \mathcal{I}, \exists t \in \mathcal{L}(G_j^N) : P(s) = P(t)$, i.e., $s \in \mathcal{U}_{\mathcal{I}}$. ■

The next result shows that once we enter a robustly certain state in V_i, we will stay in it forever.

Lemma 4.2: For any $i \in \mathcal{I}$ and faulty string $s \in \mathcal{L}(G_i) \setminus \mathcal{L}(G_i^N)$, if $\delta_{V_i}(s) \in X_i^{\mathrm{cer}}$, then for any of its continuation $st \in \mathcal{L}(G_i)$, we have $\delta_{V_i}(st) \in X_i^{\mathrm{cer}}$.

Proof: Since $(x, q_1, \ldots, q_n) = \delta_{V_i}(s) \in X_i^{\mathrm{cer}}$, we know that $\forall j \in \mathcal{I} : f_j(P(s)) \subseteq X_j^F$. Since for any model $j \in \mathcal{I}$, once it enters X_j^F, it will stay in X_j^F for ever. Therefore, we know that $\forall j \in \mathcal{I} : f_j(P(st)) \subseteq X_j^F$, i.e., $\delta_{V_i}(st) = (\delta_i(st), f_1(P(st)), \ldots, f_n(P(st)))$ is also robustly certain. ■

By Lemma 4.2, we know that, first, for any SCC in V_i, if it contains one robustly uncertain state, then all states in it are robustly uncertain, and second, once we reach a robustly certain state, we will stay in robustly certain states forever. Therefore, we simplify the verification automaton V_i as follows.

1) All robustly certain states in V_i are aggregated as a new single state x_{cer} from which no transition is defined.
2) All robustly uncertain states in *terminal* SCCs are aggregated as a new single state x_{unc} from which no transition is defined.

We denote the modified automaton by $\tilde{V}_i = (\tilde{X}_i^V, \Sigma, \tilde{\delta}_{V_i}, q_{0,i}^V)$.

A. Verification of Robust (ϵ, K)-Diagnosability

Now, we discuss how to verify robust (ϵ, K)-diagnosability when ϵ and K are given. According to Definition 3.1, it suffices to compute probability $\mathrm{Prob}\left(\{t \in \mathcal{L}_K(G_i, \delta_i(s)) : st \in \mathcal{U}_{\mathcal{I}}\} \mid \delta_i(s)\right)$ for all possible $s \in \Psi(G_i)$ and test whether or not it is smaller than ϵ. By Lemma 4.1, this probability is in fact the probability of staying at states X_i^{unc} in K steps from string s, which can be computed as follows.

Let $\Psi_X(\tilde{V}_i) := \{x \in \tilde{X}_i^V : \exists s \in \Psi(G_i) \text{ s.t. } x = \tilde{\delta}_{V_i}(s)\}$ be the set of states reached by strings in $\Psi(G_i)$. We denote by $\mathrm{Reach}_i(\Psi_X(\tilde{V}_i)) \subseteq X_i^V$ the set of states reachable from $\Psi_X(\tilde{V}_i)$ in $\tilde{V}_i$ and suppose that states in $\mathrm{Reach}_i(\Psi_X(\tilde{V}_i))$ are ordered as $\mathrm{Reach}_i(\Psi_X(\tilde{V}_i)) = \{x_1^V, \ldots, x_m^V\}$, where each state x_k^V is in the form of $x_k^V = (x_k, q_k^1, \ldots, q_k^n)$.

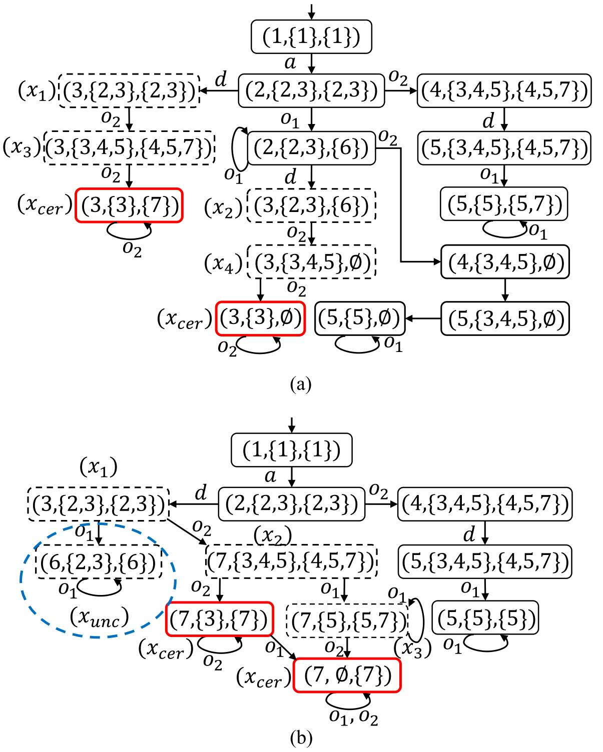
Then, we define a Markov chain (MC) $\mathcal{M}_i$ whose state space is $\mathrm{Reach}_i(\Psi_X(\tilde{V}_i)) = \{x_1^V, \ldots, x_m^V\}$ with a $m \times m$ transition probability matrix $\mathbb{P}_i$, whose k, j entry is

$$p_{k,j} := \begin{cases} \sum_{\sigma \in \Sigma : \tilde{\delta}_{V_i}(x_k^V, \sigma) = x_j^V} p_i(\sigma \mid x_k) & \text{if } x_k^V \notin \{x_{\mathrm{cer}}, x_{\mathrm{unc}}\} \\ 1 & \text{if } \begin{array}{l} [x_k^V = x_j^V = x_{\mathrm{cer}}] \text{ or} \\ [x_k^V = x_j^V = x_{\mathrm{unc}}] \end{array} \\ 0 & \text{otherwise} \end{cases}.$$

Note that $p_i(\sigma \mid x_k)$ corresponds to the probability of transition $\delta_i(x_k, \sigma)$ in the plant model. Therefore, $p_{k,j}$ is the one-step transition probability from state x_k^V to x_j^V if the true model is G_i; and hence, the k, j entry in $(\mathbb{P}_i)^K$ is the K-step transition probability from state x_k^V to x_j^V.

For each state $x \in \Psi_X(\tilde{V}_i)$, we define an m-dimensional vector $\pi_{i,x}^0 : \mathrm{Reach}_i(\Psi_X(\tilde{V}_i)) \to \{0, 1\}$, where only the value of state x is 1.

The following theorem states how to verify robust (ϵ, K)-diagnosability using MCs $\mathcal{M}_i, i \in \mathcal{I}$.



(a)

(b)

Fig. 2. In the figures, states highlighted by bold lines are robustly certain states, states highlighted by dashes lines are robustly uncertain states and the blue dash circle denotes a terminal SCC. (a) $V_1 = G_1 \| \mathrm{Obs}(G_1) \| \mathrm{Obs}(G_2)$. (b) $V_2 = G_2 \| \mathrm{Obs}(G_1) \| \mathrm{Obs}(G_2)$.

Theorem 4.1: Given $\epsilon > 0$ and $K \in \mathbb{N}$, $\{(G_i, p_i) : i \in \mathcal{I}\}$ is robustly (ϵ, K)-diagnosable if and only if

$$\pi_{i,x}^{K} \mathbb{1}_{unc}^{\top} < \epsilon, \text{ for any } i \in \mathcal{I} \text{ and } x \in \Psi_X(\tilde{V}_i)$$

where $\pi_{i,x}^{K} = \pi_{i,x}^{0} (\mathbb{P}_i)^K$ and $\mathbb{1}_{unc}^{\top} : Reach_i(\Psi_X(\tilde{V}_i)) \to \{0, 1\}$ is a m-dimensional vector in which only the value of state x_{cer} is 0, i.e., the values of states in $X_i^{\mathrm{unc}} \cup \{x_{\mathrm{unc}}\}$ are 1.

Proof: For any $i \in \mathcal{I}$, $s \in \Psi(G_i)$, each element in $\pi_{i,\tilde{\delta}_{V_i}(s)}^{K}$ is probability of reaching each state of $\mathrm{Reach}_i(\Psi_X(\tilde{V}_i))$ in K steps given the occurrence of s. Hence, $\pi_{i,\tilde{\delta}_{V_i}(s)}^{K} \mathbb{1}_{\mathrm{unc}}^{\top}$ is the probability that the system is in X_i^{unc} after executing K steps from s. Therefore, by Lemma 4.1, we have

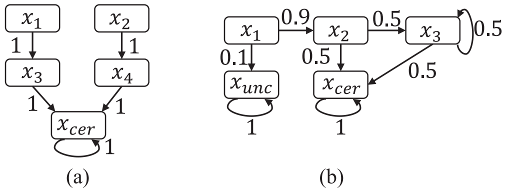
$$\mathrm{Prob}\left(\{t \in \mathcal{L}_K(G_i, \delta_i(s)) : st \in \mathcal{U}_{\mathcal{I}}\} \mid \delta_i(s)\right) = \pi_{i,\tilde{\delta}_{V_i}(s)}^{K} \mathbb{1}_{\mathrm{unc}}^{\top}.$$

Note that, the above-mentioned probability only depends on the state reached by $s \in \Psi(G_i)$. Therefore, the system is robustly (ϵ, K)-diagnosable if and only if $\forall i \in \mathcal{I}, \forall x \in \Psi_X(\tilde{V}_i)$, $\pi_{i,\tilde{\delta}_{V_i}(s)}^{K} \mathbb{1}_{\mathrm{unc}}^{\top} < \epsilon$. ■

We illustrate the above-mentioned theorem by the following example.

Example 4.1: Again, let us consider $\{(G_1, p_1), (G_2, p_2)\}$ shown in Fig. 1 with $X_1^N = \{1, 2, 4, 5\}$, $X_2^N = \{1, 2, 4, 5\}$, and $\Sigma_o = \{a, o_1, o_2\}$. We have discussed in Example 3.1 that the system is robustly (0.2,5)-diagnosable. Here, we verify this result by Theorem 4.1.

First, we construct the verification automata V_1 and V_2 shown in Fig. 2. For V_1, we have $\Psi_1^X(\tilde{V}_1) = \{(3, \{2, 3\}, \{2, 3\}),$ $(3, \{2, 3\}, \{6\})\}$; states $(3, \{3\}, \{7\})$ and $(3, \{3\}, \emptyset)$ are robustly certain states. For the sake of simplicity, states in $Reach_i(\Psi_X(\tilde{V}_i))$ are renamed by $x_1, \ldots, x_4, x_{cer}$ as denoted in the figure. Note that V_1 does not contains a terminal SCC in which all states are uncertain. However, in V_2, state $(6, \{2, 3\}, \{6\})$, which is a robustly uncertain state, forms a terminal SCC by itself. Therefore, state $(6, \{2, 3\}, \{6\})$ is renamed as x_{unc} in V_2.



(a)

(b)

Fig. 3. Associated Markov chains. (a) $\mathcal{M}_1$. (b) $\mathcal{M}_2$.

The associated MCs $\mathcal{M}_1$ and $\mathcal{M}_2$ are shown in Fig. 3 (a) and (b), respectively. Their transition probability matrices (assuming states in $\mathcal{M}_1$ and $\mathcal{M}_2$ are ordered as $x_1, \ldots, x_4, x_{cer}$ and $x_1, \ldots, x_3, x_{cer}, x_{\mathrm{unc}}$, respectively) are as follows:

$$\mathbb{P}_1 = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}, \mathbb{P}_2 = \begin{bmatrix} 0 & 0.9 & 0 & 0 & 0.1 \\ 0 & 0 & 0.5 & 0.5 & 0 \\ 0 & 0 & 0.5 & 0.5 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

Then, for $\mathcal{M}_1$ and $x_1, x_2 \in \Psi_1^X(\tilde{V}_1)$, we have

$$\pi_{1,x_1}^{5} \mathbb{1}_{\mathrm{unc}}^{\top} = [1\ 0\ 0\ 0\ 0](\mathbb{P}_1)^5 [1\ 1\ 1\ 1\ 0]^{\top} = 0 < 0.2$$

$$\pi_{1,x_2}^{5} \mathbb{1}_{\mathrm{unc}}^{\top} = [0\ 1\ 0\ 0\ 0](\mathbb{P}_1)^5 [1\ 1\ 1\ 1\ 0]^{\top} = 0 < 0.2.$$

Similarly, for $\mathcal{M}_2$ and $x_1 \in \Psi_X(\tilde{V}_2)$, we have

$$\pi_{2,x_1}^{5} \mathbb{1}_{\mathrm{unc}}^{\top} = [1\ 0\ 0\ 0\ 0](\mathbb{P}_2)^5 [1\ 1\ 1\ 0\ 1]^{\top} = 0.15625 < 0.2.$$

Therefore, by Theorem 4.1, we know that the system is robustly (0.2,5)-diagnosable.

B. Verification of Robust ϵ-Diagnosability

In this section, we show how to check robust ϵ-diagnosability, i.e., whether or not we can achieve a given misdetection rate $\epsilon > 0$ with some delay. This problem can still be solved using the above defined verification automata and their associated MCs.

We observe that, in each MC $\mathcal{M}_i$, state x_{cer} is absorbing in the sense that once we reach state x_{cer}, we will stay in it forever. Therefore, we know that, for each $x \in \Psi_X(\tilde{V}_i)$, $\pi_{i,x}^{0} (\mathbb{P}_i)^K \mathbb{1}_{\mathrm{unc}}^{\top}$ is nonincreasing as K increases. Moreover, in the construction of $\tilde{V}_i$, we only aggregate uncertain states in a terminal SCC. Therefore, all uncertain states are not absorbing except x_{unc} and the limit of $\pi_{i,x}^{0} (\mathbb{P}_i)^K \mathbb{1}_{\mathrm{unc}}^{\top}$ is the *absorbing probability* of state x_{unc} when the initial distribution vector is $\pi_{i,x}^{0}$. This absorbing probability can be computed by [26]

$$\lim_{K \to \infty} \pi_{i,x}^{0} (\mathbb{P}_i)^K \mathbb{1}_{\mathrm{unc}}^{\top} = \pi_{i,x}^{0} v_i^{\top}$$

where $v_i : \mathrm{Reach}_i(\Psi_X(\tilde{V}_i)) \to \mathbb{R}$ is the minimal m-dimensional nonnegative vector that solves the following equations: for any $x_k \in \{x_1, \ldots, x_m\}$ (recall that we assume $\mathrm{Reach}_i(\Psi_X(\tilde{V}_i)) = \{x_1, \ldots, x_m\}$), we have

$$v_i(x_k) = \begin{cases} 1 & \text{if } x_k = x_{\mathrm{unc}} \\ 0 & \text{if } x_k = x_{\mathrm{cer}} \\ \sum_{x_j \in \mathrm{Reach}_i(\Psi_X(\tilde{V}_i))} v(x_j) \times p_{k,j} & \text{otherwise} \end{cases}. \quad (9)$$

To sum up, we have the following theorem immediately.

Theorem 4.2: Given $\epsilon > 0$, $\{(G_i, p_i) : i \in \mathcal{I}\}$ is robustly ϵ-diagnosable if and only if

$$\pi^0_{i,x} v_i^\top < \epsilon, \text{ for any } i \in \mathcal{I} \text{ and } x \in \Psi_X(\tilde{V}_i).$$

We illustrate Theorem 4.2 by the following example.

Example 4.2: Still, we consider $\{(G_1, p_1), (G_2, p_2)\}$ shown in Fig. 1 with $X_1^N = \{1, 2, 4, 5\}, X_2^N = \{1, 2, 4, 5\}$, and $\Sigma_o = \{a, o_1, o_2\}$. For $\mathcal{M}_1$, the minimal nonnegative solution to the following equations:

$$\begin{cases} v_1(x_1) = v_1(x_3) = v_1(x_{cer}) = v_1(x_2) = v_1(x_4) \\ v_1(x_{cer}) = 0 \end{cases} \tag{10}$$

is $v_1 = [0\ 0\ 0\ 0\ 0]$. For $\mathcal{M}_2$, the minimal nonnegative solution to the following equations:

$$\begin{cases} v_2(x_1) = 0.9 \times v_2(x_2) + 0.1 \times v_2(x_{\text{unc}}) \\ v_2(x_2) = v_2(x_3) = 0.9 \times v_2(x_3) + 0.5 \times v_1(x_{\text{cer}}) \\ v_2(x_{\text{unc}}) = 1 \\ v_1(x_{\text{cer}}) = 0 \end{cases} \tag{11}$$

is $v_2 = [0.1\ 0\ 0\ 0\ 1]$. Then, for $x_1, x_2 \in \Psi_X(\tilde{V}_1)$, we have $\pi^0_{1,x_1} v_1^\top = \pi^0_{1,x_2} v_2^\top = 0$ and, for $x_1 \in \Psi_X(\tilde{V}_2)$, we have $\pi^0_{2,x_1} v_1^\top = 0.1$. Therefore, we know that we can achieve any misdetection rate $\epsilon > 0.1$ with a sufficiently large K.

Remark 4.1: Let us discuss the complexity of verifying robust (ϵ, K)-diagnosability and the complexity of verifying robust ϵ-diagnosability using Theorems 4.1 and 4.2, respectively. For each $i \in \mathcal{I}, x \in \Psi_X(\tilde{V}_i)$, it takes $O(K \cdot (m_i)^3)$ to compute $\pi^K_{0,x}$ and takes $O((m_i)^3)$ to solve (9), where m_i denotes the number of states in $\text{Reach}_i(\Psi_X(\tilde{V}_i))$. Moreover, we need to repeat them for all $i \in \mathcal{I}$ and $x \in \Psi_X(\tilde{V}_i)$. Therefore, the complexity for verifying robust (ϵ, K)-diagnosability is $O(\sum_{i\in\mathcal{I}} K \cdot (m_i)^4)$ and the complexity for verifying robust ϵ-diagnosability is $O(\sum_{i\in\mathcal{I}}(m_i)^4)$. In the worst case, m_i is exponential in the number of possible models and the number of states in each model. Therefore, the overall complexity for verifying robust (ϵ, K)-diagnosability and robust ϵ-diagnosability are both exponential in the number of possible models and the number of states in each model.

C. Verification of Robust A-Diagnosability

Finally, we discuss how to verify robust A-diagnosability, i.e., whether or not the system is robustly ϵ-diagnosable for an arbitrarily small misdetection rate ϵ. This problem is addressed by the following theorem.

Theorem 4.3: $\{(G_i, p_i) : i \in \mathcal{I}\}$ is robustly A-diagnosable if and only if for any $i \in \mathcal{I}$, $x_{\text{unc}} \notin \tilde{X}_i^V$, i.e., V_i does not contain a SCC in which all states are robustly uncertain.

Proof: For any $i \in \mathcal{I}$ and $x \in \Psi_X(\tilde{V}_i)$, since only states $x_{\rm cer}$ and $x_{\rm unc}$ are absorbing states in $\mathcal{M}_i$, we know that $\lim_{K\to\infty} \pi^0_{i,x}(\mathbb{P}_i)^K \mathbb{1}^\top_{\rm unc} = \pi^0_{i,x} v_i^\top = 0$ if and only if $x_{\rm unc}$ is not reachable from x. Therefore, if $x_{\rm unc} \notin \tilde{X}_i^V$, then we know that $\forall x \in \Psi_X(\tilde{V}_i) : \pi^0_{i,x} v_i^\top = 0$. By Theorem 4.2, we know that the system is robustly ϵ-diagnosable for any $\epsilon > 0$, i.e., it is robustly A-diagnosable. If $x_{\rm unc} \in \tilde{X}_i^V$, then let $x \in \Psi_X(\tilde{V}_i)$ be a state such that $x_{\rm unc}$ is reachable from x. Then, we have $\pi^0_{i,x} v_i^\top \neq 0$. Therefore, by Theorem 4.2, the system is not robustly ϵ-diagnosable for any $\epsilon < \pi^0_{i,x} v_i^\top$, i.e., it is not robustly A-diagnosable. ■

Theorem 4.3 provides a direct approach for the verification of robust A-diagnosability. To this end, we just need to construct automaton V_i for each $i \in \mathcal{I}$ and then check whether or not it contains a terminal SCC in which all states are robustly uncertain. For example, in the running example $\{(G_1, p_1), (G_2, p_2)\}$ shown in Fig. 1, since $x_{\rm unc} \in \tilde{X}_2^V$, we know that it is not robustly A-diagnosable. However, the complexity of this approach is exponential in both the size of each automaton and the number of possible models. In particular, the exponential complexity in the number of possible models comes from the fact that Theorem 4.3 requires the parallel composition of *all* observer automata. In fact, we note that, in contrast to verification of robust (ϵ, K)-diagnosability and robust ϵ-diagnosability, whose satisfactions depend on the transition probability matrix, robust A-diagnosability is a purely structural property. This value independency can actually help us to further improve the verification complexity. Specifically, the following theorem shows that, to verify robust A-diagnosability for all possible models, it suffices to verify robust A-diagnosability for *each pair* of models.

Theorem 4.4: The set of all models $\{(G_i, p_i) : i \in \mathcal{I}\}$ is robustly A-diagnosable if and only if any pair of two models $\{(G_i, p_i), (G_j, p_j)\}, i, j \in \mathcal{I}$ is robustly A-diagnosable.

Proof: (⇒) By contraposition. Suppose that there exist $i, j \in \mathcal{I}$ such that $\{(G_i, p_i), (G_j, p_j)\}$ is not robustly A-diagnosable, i.e.

$$\begin{aligned} &(\exists \epsilon > 0)(\forall K > 0)(\exists i' \in \{i, j\})(\exists s \in \Psi(G_{i'})) \\ &\text{s.t. Prob}\left(\{t \in \mathcal{L}_K(G_{i'}, \delta_{i'}(s)) : st \in \mathcal{U}_{\{i,j\}}\} \mid \delta_{i'}(s)\right) \geq \epsilon. \end{aligned} \tag{12}$$

Since $\mathcal{U}_{\{i,j\}} \subseteq \mathcal{U}_{\mathcal{I}}$, we know that

$$\begin{aligned} &\text{Prob}\,(\{t \in \mathcal{L}_K(G_{i'}, \delta_{i'}(s)) : st \in \mathcal{U}_{\mathcal{I}}\} \mid \delta_{i'}(s)) \\ &\quad \geq \text{Prob}\left(\{t \in \mathcal{L}_K(G_{i'}, \delta_{i'}(s)) : st \in \mathcal{U}_{\{i,j\}}\} \mid \delta_{i'}(s)\right) \geq \epsilon. \end{aligned}$$

Therefore, we know that

$$\begin{aligned} &(\exists \epsilon > 0)(\forall K > 0)(\exists i' \in \mathcal{I})(\exists s \in \Psi(G_{i'})) \\ &\text{s.t. Prob}\,(\{t \in \mathcal{L}_K(G_{i'}, \delta_{i'}(s)) : st \in \mathcal{U}_{\mathcal{I}}\} \mid \delta_{i'}(s)) \geq \epsilon \end{aligned} \tag{13}$$

i.e., $\{(G_i, p_i) : i \in \mathcal{I}\}$ is not robustly A-diagnosable.

(⇐) For any two possible models $i, j \in \mathcal{I}$, since $\{(G_i, p_i), (G_j, p_j)\}$ is robustly A-diagnosable, we know that, for any $\epsilon > 0$, there exists an integer $K_{i,j}$, such that for any $i' \in \{i, j\}, s \in \Psi(G_{i'})$, we have

$$\text{Prob}\left(\{t \in \mathcal{L}_{K_{i,j}}(G_{i'}, \delta_{i'}(s)) : st \in \mathcal{U}_{\{i,j\}}\} \mid \delta_{i'}(s)\right) < \frac{\epsilon}{n^2}. \tag{14}$$

Let $K := \max_{i,j\in\mathcal{I}} K_{i,j}$. By the definition of $\mathcal{U}$, we have that

$$\mathcal{U}_{\mathcal{I}} = \bigcup_{i,j\in\mathcal{I}} \mathcal{U}_{\{i,j\}}.$$

Therefore, for the above chosen K, (14) implies that, for any $i' \in \mathcal{I}, s \in \Psi(G_{i'})$, we have

$$\begin{aligned} &\text{Prob}\,(\{t \in \mathcal{L}_K(G_{i'}, \delta_{i'}(s)) : st \in \mathcal{U}_{\mathcal{I}}\} \mid \delta_{i'}(s)) \\ &\quad \leq \sum_{i,j\in\mathcal{I}} \text{Prob}\left(\{t \in \mathcal{L}_K(G_{i'}, \delta_{i'}(s)) : st \in \mathcal{U}_{\{i,j\}}\} \mid \delta_{i'}(s)\right) \\ &\quad \leq \sum_{i,j\in\mathcal{I}} \text{Prob}\left(\{t \in \mathcal{L}_{K_{i,j}}(G_{i'}, \delta_{i'}(s)) : st \in \mathcal{U}_{\{i,j\}}\} \mid \delta_{i'}(s)\right) \\ &\quad < \frac{\epsilon}{n^2} \times |\mathcal{I}|^2 = \epsilon. \end{aligned}$$

Since $\epsilon > 0$ is chosen arbitrarily, we know that $\{(G_i, p_i) : i \in \mathcal{I}\}$ is robustly A-diagnosable. ■

Theorem 4.4 suggests immediately an improved approach for the verification of robust A-diagnosability. Specifically, for each possible model $i \in \mathcal{I}$, instead of constructing $G_i \| \text{Obs}(G_1) \| \ldots \| \text{Obs}(G_n)$, we can simply construct $G_i \| \text{Obs}(G_i) \| \text{Obs}(G_j)$, which contains at most $|X_i| \cdot 2^{|X_i|} \cdot 2^{|X_j|}$ number of states and $|\Sigma| \cdot |X_i| \cdot 2^{|X_i|} \cdot 2^{|X_j|}$ number of transitions, for all $j \in \mathcal{I}$, and then use Theorem 4.3 to test whether or not each pair of models is robustly A-diagnosable, where the complexity of detecting all SCCs is linear in the size of $G_i \| \text{Obs}(G_i) \| \text{Obs}(G_j)$.

Therefore, the overall complexity of testing robust A-diagnosability using Theorem 4.4 is $O(|\Sigma| \cdot \sum_{i,j\in\mathcal{I}} (|X_i| \cdot 2^{|X_i|+|X_j|}))$, which is polynomial in the number of all possible models. Similarly, one can show that both robust ϵ-diagnosability and robust (ϵ, K)-diagnosability can also be verified in such a pairwise manner. However, the verification complexity is still exponential w.r.t. the number of states in each model. It is natural to ask whether or not this complexity can also be improved. In fact, it has been shown in [4] and [12] that verification of A-diagnosability, which is the special case of robust A-diagnosability with a unique model, is already PSPACE hard w.r.t. the number of states in the system model. Therefore, this exponential complexity for robust A-diagnosability also seems to be unavoidable, which essentially comes from the subset construction in the observer automata. One special case, where polynomial-time solution is possible, is that each possible model satisfies a property called *natural observer property* [15]. In this case, the number of states in the observer automaton is smaller than the number of states in the original system. Therefore, for this special case, the complexity for verifying robust A-diagnosability becomes polynomial in both the size of each automaton and the number of possible models.

Finally, recall that robust A-diagnosability guarantees that, for any given misdetection rate ϵ, there exists a delay K such that the misdetection rate ϵ can be achieved in K steps. However, finding the smallest K achieving ϵ requires us to compute the smallest K such that, for each $i \in \mathcal{I}, x \in \Psi_i(\tilde{V}_i), \pi^0_{i,x}(\mathbb{P}_i)^K \mathbb{1}^\top_{\text{unc}} < \epsilon$, which is computationally very challenging. Here, we provide an upper bound for estimating the delay that achieves a given misdetection rate ϵ.

Proposition 4.1: Suppose that $\{(G_i, p_i) : i \in \mathcal{I}\}$ is robustly A-diagnosable and let $\epsilon > 0$ be an arbitrary misdetection rate. Then, for any $i \in \mathcal{I}$ and $s \in \Psi(G_i)$, $Prob(\{t \in \mathcal{L}_K(G_i, \delta_i(s)) : st \in \mathcal{U}_\mathcal{I}\} \mid \delta_i(s)) < \epsilon$ if

$$K > n_{\max} \times \left\lceil \frac{\log \epsilon}{\log(1 - p_{\min}^{n_{\max}})} \right\rceil$$

where $\lceil k \rceil$ denotes the smallest integer greater than or equal to k, $n_{\max} := \max_{i\in\mathcal{I}} |Reach_i(\Psi_X(\tilde{V}_i))|$ is the maximum number of states in each MC $\mathcal{M}_i$ and $p_{\min}$ is the minimum entry in $\mathbb{P}_1, \ldots, \mathbb{P}_n$.

Proof: Let $i \in \mathcal{I}$ be an arbitrary model and $s \in \Psi(G_i)$ be a faulty string. Since the system is robustly A-diagnosable, we know that $x_{\text{unc}} \notin \tilde{X}_i^V$. Therefore, from any state reachable from $\tilde{\delta}_{V_i}(s)$, we can reach x_{cer} in at most $n_{\max}$ steps. Moreover, the probability of reaching x_{cer} in $n_{\max}$ steps is greater than $p_{\min}^{n_{\max}}$. Therefore, for any $k \in \mathbb{N}$, we have

$$\begin{aligned} &\text{Prob}(\{t \in \mathcal{L}_{k\times n_{\max}}(G_i, \delta_i(s)) : st \in \mathcal{U}_\mathcal{I}\} \mid \delta_i(s)) \\ &\quad \leq (1 - p_{\min}^{n_{\max}})^k. \end{aligned}$$

Since $K > n_{\max} \times \lceil \frac{\log \epsilon}{\log(1-p_{\min}^{n_{\max}})} \rceil$, we have

$$\begin{aligned} &\text{Prob}(\{t \in \mathcal{L}_K(G_i, \delta_1(s)) : st \in \mathcal{U}_\mathcal{I}\} \mid \delta_i(s)) \\ &\leq \text{Prob}\left(\{t \in \mathcal{L}_{n_{\max}\times\lceil \frac{\log \epsilon}{\log(1-p_{\min}^{n_{\max}})}\rceil}(G_i, \delta_1(s)) : st \in \mathcal{U}_\mathcal{I}\} \mid \delta_i(s)\right) \\ &\leq (1 - p_{\min}^{n_{\max}})^{\lceil \frac{\log \epsilon}{\log(1-p_{\min}^{n_{\max}})}\rceil} \\ &\leq (1 - p_{\min}^{n_{\max}})^{\frac{\log \epsilon}{\log(1-p_{\min}^{n_{\max}})}} \\ &= \epsilon. \end{aligned}$$

■

Remark 4.2: In this paper, we provide direct approaches for verifying different notions of robust diagnosability against model uncertainty. An alternative approach for addressing the model uncertainty issue is to construct a new automaton such that,[1] first, it starts from a new single initial state from which the initial state of each possible model can be reached unobservably, and second, the dynamic of the new system follows the dynamic of each possible model from its original initial state. One can show that the set of possible models is robust A-diagnosable if and only if the new system is A-diagnosable. Note that the new system contains $1 + \sum_{i\in\mathcal{I}} |X_i|$ states and we can further use Theorem 4.4 to reduce the complexity of verification procedure. The idea of this machinery may also be applied to other robust problems against model uncertainties, e.g., robust prognosis problem [32] and robust control problem [5], [22], [28], [37], to "de-robustify" the problem settings.

V. Conclusion

We studied the robust fault diagnosis problem in the context of stochastic DES. A condition termed as robust (ϵ, K)-diagnosability was proposed to capture whether or not a fault can always be detected with misdetection rate smaller ϵ in K steps even though we do not know the true model *a priori*. We also proposed the conditions of robust ϵ-diagnosability and robust A-diagnosability to capture whether or not a misdetection rate ϵ can be achieved and the misdetection rate converges to zero, respectively. Effective algorithms were also provided to verify these conditions. Our results generalize existing works on fault diagnosis of stochastic DES by handling the robustness issue regarding model uncertainties.

References

[1] E. Athanasopoulou, L. Li, and C. N. Hadjicostis, "Maximum likelihood failure diagnosis in finite state machines under unreliable observations," *IEEE Trans. Autom. Control*, vol. 55, no. 3, pp. 579–593, Mar. 2010.

[2] H. Bazille, E. Fabre, and B. Genes, "Diagnosability degree of stochastic discrete event systems," in *Proc. 56th IEEE Conf. Decis. Control*, 2017, pp. 5726–5731.

[3] N. Bertrand, E. Fabre, S. Haar, S. Haddad, and L. Hélouët, "Active diagnosis for probabilistic systems," in *Proc. Int. Conf. Found. Softw. Sci. Comput. Struct.*, 2014, pp. 29–42.

[4] N. Bertrand, S. Haddad, and E. Lefaucheux, "Foundation of diagnosis and predictability in probabilistic systems," in *Proc. 34th IARCS Conf. Found. Softw. Technol. Theor. Comput. Sci.*, 2014, pp. 417–429.

[5] S. E. Bourdon, M. Lawford, and W. M. Wonham, "Robust nonblocking supervisory control of discrete-event systems," *IEEE Trans. Automat. Control*, vol. 50, no. 12, pp. 2015–2021, Dec. 2005.

[6] M. P. Cabasino, A. Giua, S. Lafortune, and C. Seatzu, "A new approach for diagnosability analysis of petri nets using verifier nets," *IEEE Trans. Autom. Control*, vol. 57, no. 12, pp. 3104–3117, Dec. 2012.

[7] L. K. Carvalho, J. C. Basilio, and M. V. Moreira, "Robust diagnosis of discrete event systems against intermittent loss of observations," *Automatica*, vol. 48, no. 9, pp. 2068–2078, 2012.

[8] L. K. Carvalho, M. V. Moreira, and J. C. Basilio, "Generalized robust diagnosability of discrete event systems," in *Proc. 18th IFAC World Congr.*, 2011, pp. 8737–8742.

[9] L. K. Carvalho, M. V. Moreira, J. C. Basilio, and S. Lafortune, "Robust diagnosis of discrete-event systems against permanent loss of observations," *Automatica*, vol. 49, no. 1, pp. 223–231, 2013.

[10] C. Cassandras and S. Lafortune, *Introduction to Discrete Event Systems*, 2nd ed. New York, NY, USA: Springer, 2008.

[11] F. Cassez, "The complexity of codiagnosability for discrete event and timed systems," *IEEE Trans. Autom. Control*, vol. 57, no. 7, pp. 1752–1764, Jul. 2012.

[12] J. Chen, C. Keroglou, C. N. Hadjicostis, and R. Kumar, "Revised test for stochastic diagnosability of discrete-event systems," *IEEE Trans. Automat. Sci. Eng.*, vol. 15, no. 1, pp. 404–408, Jan. 2018.

[13] J. Chen and R. Kumar, "Failure detection framework for stochastic discrete event systems with guaranteed error bounds," *IEEE Trans. Autom. Control*, vol. 60, no. 6, pp. 1542–1553, Jun. 2015.

[1] This observation belongs to an anonymous reviewer of this paper.

[14] E. Fabre, L. Hélouët, E. Lefaucheux, and H. Marchand, "Diagnosability of repairable faults," in *Proc. 13th Int. Workshop Discrete Event Syst.*, 2016, pp. 230–236.

[15] L. Feng and W. M. Wonham, "Supervisory control architecture for discrete-event systems," *IEEE Trans. Autom. Control*, vol. 53, no. 6, pp. 1449–1461, Jul. 2008.

[16] S. Hashtrudi Zad, R. H. Kwong, and W. M. Wonham, "Fault diagnosis in discrete-event systems: Framework and model reduction," *IEEE Trans. Autom. Control*, vol. 48, no. 7, pp. 1199–1212, Jul. 2003.

[17] N. Kanagawa and S. Takai, "Diagnosability of discrete event systems subject to permanent sensor failures," *Int. J. Control*, vol. 88, no. 12, pp. 2598–2610, 2015.

[18] C. Keroglou and C. N. Hadjicostis, "Detectability in stochastic discrete event systems," *Syst. Control Lett.*, vol. 84, pp. 21–26, 2015.

[19] R. H. Kwong and D. L. Yonge-Mallo, "Fault diagnosis in discrete-event systems: Incomplete models and learning," *IEEE Trans. Syst. Man Cybern., B*, vol. 41, no. 1, pp. 118–130, Feb. 2011.

[20] R. H. Kwong and D. L. Yonge-Mallo, "Fault diagnosis in discrete-event systems with incomplete models: Learnability and diagnosability," *IEEE Trans. Cybern.*, vol. 45, no. 7, pp. 1236–1249, Jul. 2015.

[21] D. Lefebvre and C. Delherm, "Diagnosis of des with petri net models," *IEEE Trans. Automat. Sci. Eng.*, vol. 4, no. 1, pp. 114–118, Jan. 2007.

[22] F. Lin, "Robust and adaptive supervisory control of discrete event systems," *IEEE Trans. Autom. Control*, vol. 38, no. 12, pp. 1848–1852, Dec. 1993.

[23] F. Liu and D. Qiu, "Safe diagnosability of stochastic discrete event systems," *IEEE Trans. Autom. Control*, vol. 53, no. 5, pp. 1291–1296, Jun. 2008.

[24] F. Liu, D. Qiu, H. Xing, and Z. Fan, "Decentralized diagnosis of stochastic discrete event systems," *IEEE Trans. Autom. Control*, vol. 53, no. 2, pp. 535–546, Mar. 2008.

[25] J. Lunze and J. Schröder, "State observation and diagnosis of discrete-event systems described by stochastic automata," *Discrete Event Dyn. Syst., Theory Appl.*, vol. 11, no. 4, pp. 319–369, 2001.

[26] J. R. Norris, *Markov Chains*. vol. 2. Cambridge, U.K.: Cambridge Univ. Press, 1998.

[27] N. Ran, H. Su, A. Giua, and C. Seatzu, "Codiagnosability analysis of bounded petri nets," *IEEE Trans. Autom. Control*, vol. 63, no. 4, pp. 1192–1199, Apr. 2018.

[28] A. Saboori and S. Hashtrudi Zad, "Robust nonblocking supervisory control of discrete-event systems under partial observation," *Syst. Control Lett.*, vol. 55, no. 10, pp. 839–848, 2006.

[29] M. Sampath, R. Sengupta, S. Lafortune, K. Sinnamohideen, and D. Teneketzis, "Diagnosability of discrete-event systems," *IEEE Trans. Autom. Control*, vol. 40, no. 9, pp. 1555–1575, Sep. 1995.

[30] R. Su and W. M. Wonham, "Global and local consistencies in distributed fault diagnosis for discrete-event systems," *IEEE Trans. Autom. Control*, vol. 50, no. 12, pp. 1923–1935, Dec. 2005.

[31] S. Takai, "Verification of robust diagnosability for partially observed discrete event systems," *Automatica*, vol. 48, no. 8, pp. 1913–1919, 2012.

[32] S. Takai, "Robust prognosability for a set of partially observed discrete event systems," *Automatica*, vol. 51, pp. 123–130, 2015.

[33] S. Takai and T. Ushio, "Verification of codiagnosability for discrete event systems modeled by mealy automata with nondeterministic output functions," *IEEE Trans. Autom. Control*, vol. 57, no. 3, pp. 798–804, Mar. 2012.

[34] D. Thorsley and D. Teneketzis, "Diagnosability of stochastic discrete-event systems," *IEEE Trans. Autom. Control*, vol. 50, no. 4, pp. 476–492, Apr. 2005.

[35] J. H. A. Tomola, F. G. Cabral, L. K. Carvalho, and M. V. Moreira, "Robust disjunctive-codiagnosability of discrete-event systems against permanent loss of observations," *IEEE Trans. Autom. Control*, vol. 62, no. 11, pp. 5808–5815, Nov. 2017.

[36] G. S. Viana, J. C. Basilio, and M. V. Moreira, "Computation of the maximum time for failure diagnosis of discrete-event systems," in *Proc. Amer. Control Conf.*, 2015, pp. 396–401.

[37] F. Wang, S. Shu, and F. Lin, "Robust networked control of discrete event systems," *IEEE Trans. Automat. Sci. Eng.*, vol. 13, no. 4, pp. 1528–1540, Oct. 2016.

[38] X. Yin, "Initial-state detectability of stochastic discrete-event systems with probabilistic sensor failures," *Automatica*, vol. 80, pp. 127–134, 2017.

[39] X. Yin and S. Lafortune, "Codiagnosability and coobservability under dynamic observations: Transformation and verification," *Automatica*, vol. 61, pp. 241–252, 2015.

[40] X. Yin and S. Lafortune, "On the decidability and complexity of diagnosability for labeled petri nets," *IEEE Trans. Autom. Control*, vol. 62, no. 11, pp. 5931–5938, Nov. 2017.

[41] S. Yokota, T. Yamamoto, and S. Takai, "Computation of the delay bounds and synthesis of diagnosers for decentralized diagnosis with conditional decisions," *Discrete Event Dyn. Syst.*, vol. 27, no. 1, pp. 45–84, 2017.

[42] J. Zaytoon and S. Lafortune, "Overview of fault diagnosis methods for discrete event systems," *Annu. Rev. Control*, vol. 37, no. 2, pp. 308–320, 2013.