Distributed Prognosis of Discrete Event Systems under Bounded-Delay Communications

Shigemasa Takai and Ratnesh Kumar

Abstract

The task of failure prognosis requires the prediction of impending failures. This paper formulates and studies the problem of distributed prognosis of discrete event systems, where the local prognosers exchange their observations for the sake of arriving at a prognostic decision. The observations are exchanged over communication channels that introduce bounded delays. A property of joint-prognosability is introduced to capture the condition under which any failure can be predicted by some local prognoser prior to its occurrence. We provide an algorithm to check the joint-prognosability property.

I. Introduction

Any system is subject to faults as a result of which it can violate its specification. The execution of a behavior that violates a specification is called a failure, and to emphasize this fact a specification is called a nonfailure specification. For undertaking possible corrective actions in response to failures, it is important to be able to perform failure detection, and if possible also failure prediction (or prognosis). Failures can occur due to the occurrence of system faults or due to the presence of modeling/design errors, and their detection or prediction is a monitoring task that needs to be performed to determine any violations of the specification (after or before they occur) so that the higher level controllers/operators can be informed to initiate any remedial actions.

This paper concerns with the problem of failure prognosis of discrete event systems (DESs). There already exist some prior works on this topic. The prediction of a failure based on a statistical analysis was considered in [2]. Due to the statistical nature of the analysis, the issuance of a prediction alert only signifies a high confidence in a future occurrence of a failure (but not full confidence). To capture the...
inevitability of a future failure, the notion of indicator traces (which indicate that a failure is guaranteed to occur) was introduced in [4], where their bounded delay detection was also studied. In [3], a notion of uniformly-bounded predictability of failures was formulated as follows: Each failure trace must possess a nonfailure prefix such that any indistinguishable trace has the property that a failure is inevitable within a uniformly bounded number of steps. Note while the existence of a uniform bound for the delay of failure detection is essential for defining diagnosability (otherwise a diagnoser may end up waiting for an arbitrarily long period before diagnosing a failure), the existence of a uniform bound within which a failure is guaranteed to occur is not essential for defining prognosability. This observation led us to weaken the definition of prognosability in [6]: Each failure trace must possess a nonfailure prefix such that each indistinguishable trace is an indicator trace. (Recall an indicator trace is one for which a failure is inevitable.) Our work in [6] also provided a test for prognosability that is polynomial in the size of a plant and a nonfailure specification.

The problem of failure prognosis was studied in a decentralized setting in [6], where a local prognoser issues a prognostic decision based on its own observations. This paper formulates its extension, namely, distributed prognosis, where the local prognosers exchange their observations of the events executed by the plant for the sake of arriving at a prognostic decision. The observations are exchanged over communication channels that introduce bounded delays, in contrast to [1], [8], where it is assumed that there is no communication delay. (Such communication channels have also been used in the setting of distributed diagnosis [7] and distributed control [10].) A property of joint-prognosability is introduced to capture the condition under which any failure can be predicted by some local prognoser prior to its occurrence. We provide an algorithm to check the joint-prognosability property that uses the plant model extended to include the communication channel models.

While the paper follows the setting of distributed diagnosis [7] for the communication channel models and also the extended plant model that encapsulates such channel models, in contrast to [7], where the joint-diagnosability property is shown to be equivalent to codiagnosability of the extended system, the joint-prognosability property studied here is not equivalent to the coprognosability of the extended system. A stronger property is required (see Remark 3). This is a key difference between the problems of distributed diagnosis studied in [7] and distributed prognosis studied here, and establishes the contribution of the current paper in contrast to [7].

The results presented in this paper were first reported at a conference [9] but without proofs. This paper contains their proofs.

II. Notation and Preliminaries

An (nondeterministic) automaton, denoted by $G$, is a four-tuple $G = (X, \Sigma, \alpha, X_0)$, where $X$ is the set of states, $\Sigma$ is the finite set of events, a function $\alpha : X \times (\Sigma \cup \{\varepsilon\}) \rightarrow 2^X$ is the transition function,
and \( X_0 \subseteq X \) is the set of initial states. \( G \) is said to be deterministic if the transition function can be written as a partial function \( \alpha : X \times \Sigma \to X \) and \( |X_0| = 1 \). Let \( \Sigma^* \) be the set of all finite sequences (also called traces) of elements of \( \Sigma \), including the empty trace \( \varepsilon \). The function \( \alpha \) can be generalized to \( \alpha : 2^X \times \Sigma^* \to 2^X \) in a natural way. The generated language of \( G \), denoted by \( L(G) \), is defined as \( L(G) = \{ s \in \Sigma^* | \alpha(X_0, s) \neq \emptyset \} \).

For each trace \( s \in \Sigma^* \), \( |s| \) denotes its length. For any nonnegative integer \( m \in \mathbb{Z}^+ \), \( \Sigma^m := \{ s \in \Sigma^* | |s| \geq m \} \) denotes the set of all traces with \( m \) or more events. For a trace \( s \in \Sigma^* \), the set of all prefixes of \( s \) is denoted by \( pr(s) \). The notation \( t \leq s \) denotes that \( t \) is a prefix of \( s \). For a language \( K \), the set of all prefixes of traces in \( K \) is defined as \( pr(K) = \bigcup_{s \in K} pr(s) \). \( K \) is said to be (prefix)-closed if \( K = pr(K) \). A closed language \( K \) is said to be deadlock-free if, for any \( s \in K \), there exists a trace \( t \neq \varepsilon \) such that \( st \in K \); otherwise \( s \in K \) is called a deadlocking trace of \( K \). The language \( K \) after \( s \in \Sigma^* \), denoted by \( K \setminus s \), is defined as \( K \setminus s := \{ t \in \Sigma^* | st \in K \} \). For traces \( s, t, u \in \Sigma^* \), if \( s = tu \), then \( u \) is written as \( u = s \setminus t \).

Given two automata \( G_1 = (X_1, \Sigma_1, \alpha_1, X_{1,0}) \) and \( G_2 = (X_2, \Sigma_2, \alpha_2, X_{2,0}) \), the synchronous composition of \( G_1 \) and \( G_2 \) is defined as \( G_1 \parallel G_2 = (X_1 \times X_2, \Sigma_1 \cup \Sigma_2, \alpha, X_{1,0} \times X_{2,0}) \), where the transition function \( \alpha : (X_1 \times X_2) \times (\Sigma_1 \cup \Sigma_2 \cup \{ \varepsilon \}) \to 2^{X_1 \times X_2} \) is defined as follows:

\[
\alpha((x_1, x_2), \sigma) = \begin{cases} 
\alpha_1(x_1, \sigma) \times \alpha_2(x_2, \sigma), & \text{if } \sigma \in \Sigma_1 \cap \Sigma_2 \\
\alpha_1(x_1, \sigma) \times \{x_2\}, & \text{if } \sigma \in \Sigma_1 - \Sigma_2 \\
\{x_1\} \times \alpha_2(x_2, \sigma), & \text{if } \sigma \in \Sigma_2 - \Sigma_1 \\
(\alpha_1(x_1, \varepsilon) \times \{x_2\}) \cup (\{x_1\} \times \alpha_2(x_2, \varepsilon)), & \text{if } \sigma = \varepsilon.
\end{cases}
\]

Let \( G = (X, \Sigma, \alpha, \{x_0\}) \) and \( R = (Y, \Sigma, \beta, \{y_0\}) \) be the deterministic finite plant and nonfailure specification models, respectively, such that \( L(R) \subseteq L(G) \). The task of prognosis is to predict the execution of any failure trace in \( L(G) - L(R) \). In order to represent failure traces in \( L(G) - L(R) \) as failure states, we refine the plant model with respect to the nonfailure specification model as follows. We augment the automaton \( R \) by adding a dump state \( \text{“}F\text{”} \) and certain transitions. Formally, the augmented automaton is denoted by \( \overline{R} = (Y, \Sigma, \overline{\beta}, \{y_0\}) \), where \( Y := Y \cup \{F\} \) and \( \overline{\beta} : Y \times \Sigma \to Y \) is defined as

\[
\overline{\beta}(\overline{y}, \sigma) = \begin{cases}
\beta(\overline{y}, \sigma), & \text{if } \overline{y} \in Y \text{ and } \beta(\overline{y}, \sigma) \text{ is defined} \\
F, & \text{otherwise}.
\end{cases}
\]

Then, for the synchronous composition \( G \parallel \overline{R} \) of \( G \) and \( \overline{R} \), it can be verified that \( L(G \parallel \overline{R}) = L(G) \cap L(\overline{R}) = L(G) \cap \Sigma^* = L(G) \). Also, traces in \( G \parallel \overline{R} \) that end at a state with the second coordinate \( F \) belong to \( L(G) - L(R) \). Without loss of generality, the plant language \( L(G) \) can be taken to be deadlock-free. Otherwise, we can extend each deadlocking trace by an unbounded sequence of a newly added event that is unobservable to all prognosters. This will make the language deadlock-free without altering any
of the prognosability properties since the newly added event does not produce any observation to any of the prognosers.

In this paper, we study the problem of failure prognosis in a distributed setting where the local prognosers exchange their observations to arrive at a prognostic decision. Let $I = \{1, 2, \ldots, n\}$ denote the index set of local prognosers that perform the task of prognosis. We assume that the limited sensing capabilities of the $i$th local prognoser ($i \in I$) can be represented as the local observation mask, $M_i : \Sigma \cup \{\varepsilon\} \rightarrow \Delta_i \cup \{\varepsilon\}$, where $\Delta_i$ is the set of locally observed symbols, and $M_i(\varepsilon) = \varepsilon$. Without loss of generality, we assume that $\Sigma \cap \Delta_i = \emptyset$ and $\Delta_i \cap \Delta_j = \emptyset$ ($i \neq j$) (otherwise, we can simply rename some of the symbols). The map $M_i$ is generalized to $M_i : \Sigma^* \rightarrow \Delta_i^*$ and $M_i : 2^{\Sigma^*} \rightarrow 2^{\Delta_i^*}$ in a natural way. The inverse of the map $M_i$, $M_i^{-1} : \Delta_i^* \rightarrow 2^{\Sigma^*}$, is defined as $M_i^{-1}(o_i) := \{s \in \Sigma^* | M_i(s) = o_i\}$.

### III. Review of Decentralized Prognosis

We review the decentralized prognosis framework introduced in [6]. The following definition introduces the key notions of boundary traces (for which a failure can occur in a next step), indicator traces (for which a failure in future is guaranteed), and nonindicator traces (that are not indicator traces).

**Definition 1**: Given a pair $(L, K)$ of closed languages over $\Sigma$ with $K \subseteq L$ (here $K$ represents a nonfailure specification and $L$ represents a plant language), we define the set of

- **boundary traces** of $K$ with respect to $L$ as, $\partial_L(K) := \{s \in K | \{s\} \Sigma \cap (L - K) \neq \emptyset\}$;
- **indicator traces** of $K$ with respect to $L$ as, $\Im_L(K) := \{s \in K | \exists m \in \mathbb{Z}^+: L \setminus s \cap \Sigma^m \subseteq [L - K] \setminus s\}$;
- **nonindicator traces** of $K$ with respect to $L$ as, $\Ye_L(K) := K - \Im_L(K)$.

The $i$th ($i \in I$) prognoser is a map $P_i : M_i(L(R)) \rightarrow \{1, \phi\}$ that, for each observation of a nonfailure trace in $L(R)$, issues a prognostic decision either “1” or “$\phi$”, where “1” means a failure is inevitable and “$\phi$” means a failure is not inevitable or its inevitability is not known.

A set of local prognosers $\{P_i\}_{i \in I}$ should possess the following properties:

- There are no missed detections, i.e., each failure is prognosed prior to its occurrence: 
  \[(\forall s \in L(G) - L(R))(\exists t \in pr(s) \cap L(R))(\exists i \in I)(\forall u \in [pr(s) \cap L(R)] \setminus t)P_i(M_i(tu)) = 1. \quad (1)\]

- There are no false alarms, i.e., an incorrect prognostic decision is never issued: 
  \[(\forall s \in \Ye_{L(G)}(L(R)))(\forall i \in I)P_i(M_i(s)) \neq 1. \quad (2)\]

In order to characterize the condition for the existence of local prognosers such that there are no missed detections or false alarms, the following definition of coprognosability was introduced in [6]:

**Definition 2**: [6] The language pair $(L(G), L(R))$ is said to be $\{M_i\}$-coprognosable if 

\[(\forall s \in L(G) - L(R))(\exists t \in pr(s) \cap L(R))(\exists i \in I)(\forall u \in L(R))M_i(t) = M_i(u) \Rightarrow u \in \Im_{L(G)}(L(R)).\]
The above definition states that, for each failure trace \( s \in L(G) - L(R) \), there exists a nonfailure prefix \( t \in pr(s) \cap L(R) \) such that, for some local prognoser \( P_i \), any locally indistinguishable nonfailure trace is an indicator trace. Then, the prognoser \( P_i \) can predict the inevitability of a failure following the execution of the nonfailure prefix \( t \) of a failure trace \( s \).

The following theorem was proved in [6] showing that \( \{ M_i \} \)-coprognostability is a necessary and sufficient condition for the existence of a decentralized prognoser satisfying (1) and (2).

**Theorem 1:** [6] For the language pair \( (L(G), L(R)) \), there exists a set of local prognosers \( \{ P_i : M_i(L(R)) \rightarrow \{1, \phi\} \} \) satisfying (1) and (2) if and only if \( (L(G), L(R)) \) is \( \{ M_i \} \)-coprognosable.

## IV. Distributed Prognosis and Joint\(^k\)-Prognostability

In the setting of distributed prognosis, the \( i \)th prognoser performs failure prognosis based on the local observations and the communicated information received from other prognosers. Information is communicated among the various prognosers over communication channels that are loss-free and order-preserving but introduce bounded delays. In this paper, we consider the immediate observation passing protocol [7], where each local prognoser transmits its observation to other prognosers immediately. In the following, we assume that there are two local prognosers, i.e., \( I = \{1, 2\} \), for simplicity. (The results continue to hold for arbitrary number of prognosers.)

An event \( \sigma \in \Sigma \) executed by a plant \( G \) is observed as \( M_i(\sigma) \in \Delta_i \cup \{\varepsilon\} \) by the \( i \)th prognoser (\( i \in I \)), and then forwarded to the \( j \)th prognoser (\( j \in I; j \neq i \)) along the channel connecting \( i \) to \( j \), and with delay bound \( k \in \mathbb{Z}^+ \). (This means that, at any given moment, at most \( k \) forwarded observations can remain pending their delivery. This simply means that the worst communication delay is better than the least execution time of \( k + 1 \) events in the plant.) We use \( C_{ij}^k \), called the masked-communication model between the \( i \)th and \( j \)th prognosers, for capturing the communication of the masked observations from the \( i \)th prognoser to the \( j \)th prognoser along a \( k \)-bounded delay channel. Formally, \( C_{ij}^k \) is defined as a finite automaton \( C_{ij}^k = (Z^k, \Sigma \cup \Delta_i, \gamma_{ij}^k, \{z_0\}) \) [7]. Here the set \( Z^k := \{z \in \Sigma^* | |z| \leq k + 1\} \) is the set of states, which represent the event traces executed in \( G \) whose observed values by the \( i \)th prognoser are pending to be received by the \( j \)th prognoser. Since the message arrivals and departures in a communication channel occur asynchronously, and since the delay of communication is bounded by \( k \), the length of such a trace is less than or equal to \( k + 1 \). \( \Sigma \cup \Delta_i \) is the event set, where \( \Sigma \) is the set of input events and \( \Delta_i \) is the set of output events. The initial state is \( z_0 = \varepsilon \). The transition function \( \gamma_{ij}^k : Z^k \times (\Sigma \cup \Delta_i \cup \{\varepsilon\}) \rightarrow Z^k \) is defined as follows:

- “Arrival” due to an event execution in \( G \): \( \forall z \in Z^k, \forall \sigma \in \Sigma: |z| \leq k \Rightarrow \gamma_{ij}^k(z, \sigma) = z\sigma \),
- “Departure” due to a reception at the destination prognoser: \( \forall z \in Z^k, \forall \delta_i \in \Delta_i \cup \{\varepsilon\}: z \neq \varepsilon \land M_i(head(z)) = \delta_i \Rightarrow \gamma_{ij}^k(z, \delta_i) = z\setminus head(z) \).
Fig. 1. Masked-communication models $C_{12}^1$, $C_{21}^1$.

- Undefined: otherwise,

where $\text{head}(z) \in \Sigma$ is the first event in a nonempty trace $z$, i.e., $z \in \{\text{head}(z)\} \Sigma^*$. It follows from the above definition that $C_{ij}^k$ is a subautomaton of $C_{ij}^{k+1}$.

**Example 1:** We consider a plant with the event set $\Sigma = \{a, b, c, d\}$. Let $\Delta_1 = \{a'\}$, $\Delta_2 = \{b'\}$, and, for $\sigma \in \Sigma$, let

$$M_1(\sigma) = \begin{cases} a', & \text{if } \sigma = a \\ \varepsilon, & \text{otherwise}, \end{cases} \quad M_2(\sigma) = \begin{cases} b', & \text{if } \sigma = b \\ \varepsilon, & \text{otherwise}. \end{cases}$$

For $k = 1$, Fig. 1(a) and (b) show the masked-communication models $C_{12}^1$ and $C_{21}^1$, respectively.

The masked-communication models $C_{12}^k$ and $C_{21}^k$ can be encapsulated with the plant model $G$ to obtain an extended plant model $G^k := G \parallel C_{12}^k \parallel C_{21}^k$ for capturing the system that generates events and forwards their observations as seen by the $i$th prognoser ($i \in I$) to the $j$th prognoser ($j \in I; j \neq i$). The extended plant $G^k$ generates events in $\Sigma \cup \Delta_1 \cup \Delta_2$, which are observed immediately by each prognoser (since the communication delay is already encapsulated in the extended plant model) as shown in Fig. 2. The observations of the $i$th prognoser ($i = 1, 2$) of the events generated by the extended plant can be captured...
using an extended mask function $\mathcal{M}_i : \Sigma \cup \Delta_1 \cup \Delta_2 \cup \{\varepsilon\} \to \Delta_1 \cup \Delta_2 \cup \{\varepsilon\}$ defined as follows:

$$\mathcal{M}_i(\sigma) := \begin{cases} 
M_i(\sigma), & \text{if } \sigma \in \Sigma \\
\sigma, & \text{if } \sigma \in \Delta_j \ (j \neq i) \\
\varepsilon, & \text{if } \sigma \in \Delta_i \cup \{\varepsilon\}.
\end{cases}$$

The extended observation mask $\mathcal{M}_i$ is generalized to $\mathcal{M}_i : (\Sigma \cup \Delta_1 \cup \Delta_2)^* \to (\Delta_1 \cup \Delta_2)^*$ and $\mathcal{M}_i : 2^{(\Sigma \cup \Delta_1 \cup \Delta_2)^*} \to 2^{(\Delta_1 \cup \Delta_2)^*}$ in a natural way.

We define a projection map $\Pi_\Sigma : \Sigma \cup \Delta_1 \cup \Delta_2 \cup \{\varepsilon\} \to \Sigma$ as follows:

$$\Pi_\Sigma(\sigma) := \begin{cases} 
\sigma, & \text{if } \sigma \in \Sigma \\
\varepsilon, & \text{otherwise}.
\end{cases}$$

The map $\Pi_\Sigma$ is generalized to $\Pi_\Sigma : (\Sigma \cup \Delta_1 \cup \Delta_2)^* \to \Sigma^*$ in a natural way. The inverse projection map $\Pi_\Sigma^{-1} : \Sigma^* \to 2^{(\Sigma \cup \Delta_1 \cup \Delta_2)^*}$ is defined as $\Pi_\Sigma^{-1}(s) := \{v \in (\Sigma \cup \Delta_1 \cup \Delta_2)^* \mid \Pi_\Sigma(v) = s\}$. Let $\Pi_{\Delta_i} : (\Sigma \cup \Delta_1 \cup \Delta_2)^* \to \Delta_i^*$ and $\Pi_{\Sigma \cup \Delta_i} : (\Sigma \cup \Delta_1 \cup \Delta_2)^* \to (\Sigma \cup \Delta_i)^*$ ($i \in I$) be the projection maps defined in the same way as $\Pi_\Sigma$. Then, the generated language of the extended plant model $G^k$ can be written as $L(G^k) = \{s \in (\Sigma \cup \Delta_1 \cup \Delta_2)^* \mid \Pi_\Sigma(s) \in L(G), \Pi_{\Sigma \cup \Delta_1}(s) \in L(C^k_{12}), \Pi_{\Sigma \cup \Delta_2}(s) \in L(C^k_{21})\}$.

To characterize the set of aggregate observation sequences received by the $i$th prognoser, we define an aggregate observation map $O^k_i : \Sigma^* \to 2^{(\Delta_i \cup \Delta_2)^*}$ as follows [7]:

$$O^k_i(s) := \mathcal{M}_i(\Pi_\Sigma^{-1}(s) \cap L(G^k)).$$

For a trace $s \in L(G)$, $O^k_i(s) \in 2^{(\Delta_i \cup \Delta_2)^*}$ is the set of possible aggregate observations received by the $i$th prognoser. It consists of the observations in $\Delta_i$ received directly from the plant, and observations in $\Delta_j \ (j \neq i)$ forwarded by the $j$th prognoser. Note that $O^k_i(s)$ is set-valued (in contrast $M_i(s)$ is point-valued) owing to the variability of communication delay, and further it is trace-based (in contrast $M_i$ is event-based), i.e., the set of aggregate observations of a trace is not the same as the concatenation of those
of the constituent events. The map $O^k_i$ is generalized to $O^k_i : 2^{Σ^∗} \rightarrow 2^{(Δ_1∪Δ_2)^∗}$ as $O^k_i(H) := \bigcup_{s \in H} O^k_i(s)$.

In the setting of distributed prognosis under the immediate observation passing protocol, the $i$th prognoser is defined as a map $P_i : O^k_i (L(R)) \rightarrow \{1, \phi\}$ that maps each possible aggregate observation to either a positive prognostic decision 1 or a non-positive (negative or unsure) prognostic decision $\phi$.

A set of local prognosers $\{P_i\}_{i \in I}$ should possess the following properties:

- There are no missed detections, i.e., each failure is prognosed prior to its occurrence:
  \[(\forall s \in L(G) - L(R)) (\exists t \in pr(s) \cap L(R)) (\exists i \in I)\]
  \[(\forall u \in [pr(s) \cap L(R)] \setminus t) (\forall o_i \in O^k_i(tu)) P_i(o_i) = 1. \quad (3)\]

- There are no false alarms, i.e., an incorrect prognostic decision is never issued:
  \[(\forall s \in Υ_{L(G)}(L(R))) (\forall i \in I) (\forall o_i \in O^k_i(s)) P_i(o_i) \neq 1. \quad (4)\]

In order to characterize the condition for the existence of local prognosers so there are no missed detections or false alarms, we introduce the definition of $\{M_i\}$-joint $k$-prognosability of the pair $(L(G), L(R))$ of the plant and nonfailure specification languages.

**Definition 3:** The language pair $(L(G), L(R))$ is said to be $\{M_i\}$-joint $k$-prognosable if
\[(\forall s \in L(G) - L(R)) (\exists t \in pr(s) \cap L(R)) (\exists i \in I)\]
\[(\forall u \in L(R)) O^k_i(t) \cap O^k_i(u) \neq \emptyset \Rightarrow u \in Υ_{L(G)}(L(R)).\]

The following theorem, which can be proved in the same way as [6, Theorem1], shows that $\{M_i\}$-joint $k$-prognosability is a necessary and sufficient condition for the existence of a set of local prognosers satisfying (3) and (4).

**Theorem 2:** For the language pair $(L(G), L(R))$, there exists a set of local prognosers $\{P_i : O^k_i (L(R)) \rightarrow \{1, \phi\}\}_{i \in I}$ satisfying (3) and (4) if and only if $(L(G), L(R))$ is $\{M_i\}$-joint $k$-prognosable.

**Remark 1:** If $(L(G), L(R))$ is not $\{M_i\}$-joint $k$-prognosable, then we need to modify local observation masks $\{M_i\}_{i \in I}$ so that $\{M_i\}$-joint $k$-prognosability is satisfied. This may be performed by a top-down or a bottom-up approach as presented in [5].

**Example 2:** We consider a plant modeled by the automaton $G$ shown in Fig. 3(a). Note that the event set is $Σ = \{a, b, c, d\}$. Let $Δ_1 = \{a', \}$, $Δ_2 = \{b', \}$, and, for $σ \in Σ$, let

\[M_1(σ) = \begin{cases} a', & \text{if } σ = a \\ ε, & \text{otherwise} \end{cases}\]

\[M_2(σ) = \begin{cases} b', & \text{if } σ = b \\ ε, & \text{otherwise} \end{cases}\]

Also, let $R$ be a nonfailure specification model shown in Fig. 3(b). We have $L(G) - L(R) = (acb + bca)d^{≥1}$ and $Υ_{L(G)}(L(R)) = \{a, ac, acb, b, bc, bca\}$. 

June 29, 2011  DRAFT
We first show that the language pair \((L(G), L(R))\) is not \(\{M_i\}\)-copronosable. Consider \(acbd \in L(G) - L(R)\). For any \(t \in pr(acbd) \cap L(R)\) and \(i \in I\), there exists \(u \in L(R) - \mathbb{I}_L(G)(L(R))\) such that \(M_i(t) = M_i(u)\). For example, for \(ac \in pr(acbd) \cap L(R)\), we have \(ca, cb \in L(R) - \mathbb{I}_L(G)(L(R))\), \(M_1(acb) = M_1(ca) = a'\), and \(M_2(acb) = M_2(cb) = b'\). Thus, \((L(G), L(R))\) is not \(\{M_i\}\)-copronosable.

We next show that \((L(G), L(R))\) is \(\{M_i\}\)-joint-prognosable. We consider any \(s \in acbd^{\geq 1} \subseteq L(G) - L(R)\). For \(acb \in pr(s) \cap L(R)\) with \(O_{L_1}^1(acb) = \{a'b'\}\), we have \(O_{L_2}^1(acb) \cap O_{L_2}^1(u) = \emptyset\) for any \(u \in L(R)\) such that \(u \neq acb\). The execution of a failure trace \(s \in acbd^{\geq 1}\) can be predicted by the second prognoser after the execution of \(acb\). We also consider \(s' \in bcad^{\geq 1} \subseteq L(G) - L(R)\). For \(bca \in pr(s') \cap L(R)\) with \(O_{L_1}^1(bca) = \{b'a'\}\), we have \(O_{L_2}^1(bca) \cap O_{L_2}^1(u') = \emptyset\) for any \(u' \in L(R)\) such that \(u' \neq bca\). The execution of a failure trace \(s' \in bcad^{\geq 1}\) can be predicted by the first prognoser after the execution of \(bca\). We can conclude that \((L(G), L(R))\) is \(\{M_i\}\)-joint-prognosable.

**Remark 2**: By the definition, \(L(G^k) \subseteq L(G^{k+1})\) holds for any \(k \in \mathbb{Z}^+\). Thus, if \((L(G), L(R))\) is \(\{M_i\}\)-joint\(^k\)-prognosable, then it is \(\{M_i\}\)-joint\(^k\)\(^{-}\)prognosable. The converse need not hold as shown in [9, Example 3].

**V. Verification of \(\{M_i\}\)-Joint\(^k\)-Prognosability**

According to Theorem 2, the existence of desired prognosers can be checked by verifying the \(\{M_i\}\)-joint\(^k\)-prognosability condition. The definition of this property involves the aggregate observation masks \(\{O_i^k\}\), which differ from conventional observation masks in two ways: They are set-valued, and further they are trace-dependent. Thus, the existing test for \(\{M_i\}\)-copronosability [6] that involves conventional observation masks cannot be directly applied, and a new test is required, which we present in this section.

Similar to the extended plant model, we introduce the extended nonfailure specification model \(R^k := R^k \| C_{12}^k \| C_{21}^k\). We begin by establishing certain relationships between the traces of the extended models and those of the original models. The first proposition is taken from [7].

**Proposition 1**: [7] For the original plant and nonfailure specification models \(G\) and \(R\), and the extended plant and nonfailure specification models \(G^k\) and \(R^k\), the following relationship holds.

- \(\forall s \in L(R^k), \forall t \in (\Delta_1 \cup \Delta_2)^* : st \in L(G^k) \Rightarrow st \in L(R^k)\);
\[ \forall s \in L(G^k) : \Pi_{\Sigma}(s) \in L(G); \]
\[ \forall s \in L(R^k) : \Pi_{\Sigma}(s) \in L(R); \]
\[ \forall s \in L(R) : \Pi_{\Sigma}^{-1}(s) \cap L(G^k) \subseteq L(R^k); \]
\[ \forall s \in L(G^k) - L(R^k) : \Pi_{\Sigma}(s) \in L(G) - L(R); \]
\[ \forall s \in L(G) - L(R) : \Pi_{\Sigma}^{-1}(s) \cap L(G^k) \subseteq L(G^k) - L(R^k). \]

The following proposition relates the indicator traces of the extended models with those of the original models.

**Proposition 2:** For the indicator trace set \( \Im_{L(G)}(L(R)) \) of \( L(R) \) with respect to \( L(G) \) and the indicator trace set \( \Im_{L(G^k)}(L(R^k)) \) of \( L(R^k) \) with respect to \( L(G^k) \),
\[ \forall s \in \Im_{L(G)}(L(R)) : \Pi_{\Sigma}^{-1}(s) \cap L(R^k) \subseteq \Im_{L(G^k)}(L(R^k)). \]

**Proof:** For any \( s \in \Im_{L(G)}(L(R)) \), there exists \( m \in \mathbb{Z}^+ \) such that \( L(G) \setminus s \cap \Sigma \geq m \subseteq [L(G) - L(R)] \setminus s \). Consider any \( s' \in \Pi_{\Sigma}^{-1}(s) \cap L(R^k) \subseteq \Pi_{\Sigma}^{-1}(s) \cap L(G^k) \). For any \( t' \in L(G^k) \setminus s' \cap (\Sigma \cup \Delta_1 \cup \Delta_2) \geq 2(k+1)+3m \), we have by the second part of Proposition 1 that \( \Pi_{\Sigma}(s') = s' \Pi_{\Sigma}(t') \in L(G) \). Also, since \( |t'| \geq 2(k+1)+3m \), we have \( |\Pi_{\Sigma}(t')| \geq m \). It follows that \( \Pi_{\Sigma}(t') \in L(G) \setminus s \cap \Sigma \geq m \subseteq [L(G) - L(R)] \setminus s \), i.e., \( s' \Pi_{\Sigma}(t') \in L(G) - L(R) \). By the sixth part of Proposition 1, we have \( s't' \in \Pi_{\Sigma}^{-1}(s) \Pi_{\Sigma}(t') \cap L(G^k) \subseteq L(G^k) - L(R^k) \), i.e., \( t' \in [L(G^k) - L(R^k)] \setminus s' \). Thus, we have \( s' \in \Im_{L(G^k)}(L(R^k)) \).

The next proposition relates the boundary traces of the extended models with those of the original models.

**Proposition 3:** For the boundary trace set \( \partial_{L(G)}(L(R)) \) of \( L(R) \) with respect to \( L(G) \) and the boundary trace set \( \partial_{L(G^k)}(L(R^k)) \) of \( L(R^k) \) with respect to \( L(G^k) \),
\[ \forall s \in \partial_{L(G^k)}(L(R^k)) : \Pi_{\Sigma}(s) \in \partial_{L(G)}(L(R)). \]

**Proof:** Consider any \( s \in \partial_{L(G^k)}(L(R^k)) \). By the first part of Proposition 1, there exists \( \sigma \in \Sigma \) such that \( s \sigma \in L(G^k) - L(R^k) \). Then, it follows from the third and fifth parts of Proposition 1 that \( \Pi_{\Sigma}(s) \in L(R) \) and \( \Pi_{\Sigma}(s \sigma) = \Pi_{\Sigma}(s \sigma) \in L(G) - L(R) \). Thus, we have \( \Pi_{\Sigma}(s) \in \partial_{L(G)}(L(R)) \).

It was shown in [6, Lemma 3] that the property of \( \{M_i\}\)-coprognoisability is equivalent to the fact that each boundary trace is unambiguously known as an indicator trace to at least one of the local prognoisers. A similar result for \( \{M_i\}\)-joint-prognosability can be proved in the same way.

**Lemma 1:** The language pair \( (L(G), L(R)) \) is \( \{M_i\}\)-joint-prognosable if and only if
\[ (\forall t \in \partial_{L(G)}(L(R))) (\exists i \in I) (\forall u \in L(R)) O^k_i(t) \cap O^k_i(u) \neq \emptyset \Rightarrow u \in \Im_{L(G)}(L(R)). \]

In what follows next, we will use this characterization of the \( \{M_i\}\)-joint-prognosability to develop an algorithm for verifying it.
Remark 3: In [7], where the problem of distributed diagnosis under bounded delay communication of immediately forwarded observations was studied, it was shown that \( \{M_i\} \)-joint-diagnosability of \((L(G), L(R))\) is equivalent to \( \{M_i\} \)-codiagnosability of \((L(\mathcal{G}^k), L(\mathcal{R}^k))\) [7, Theorem 1]. Based on this fact, an initial intuition would be to think that \( \{M_i\} \)-joint-\(k\)-prognosability of \((L(G), L(R))\) should be same as \( \{M_i\} \)-coprognosability of \((L(\mathcal{G}^k), L(\mathcal{R}^k))\). But contrary to such an initial intuition, this is not true. The following proposition shows that \( \{M_i\} \)-joint-\(k\)-prognosability of \((L(G), L(R))\) is strictly stronger than \( \{M_i\} \)-coprognosability of \((L(\mathcal{G}^k), L(\mathcal{R}^k))\).

Proposition 4: If the language pair \((L(G), L(R))\) is \( \{M_i\} \)-joint-\(k\)-prognosable, then \((L(\mathcal{G}^k), L(\mathcal{R}^k))\) is \( \{M_i\} \)-coprognosable. The converse need not hold.

Proof: By [6, Lemma 3], \((L(\mathcal{G}^k), L(\mathcal{R}^k))\) is \( \{M_i\} \)-coprognosable if and only if

\[
(\forall t \in \partial_{L(\mathcal{G}^k)}(L(\mathcal{R}^k)))(\exists i \in I)(\forall u \in L(\mathcal{R}^k)), M_i(t) = M_i(u) \Rightarrow u \in \Im_{L(\mathcal{G}^k)}(L(\mathcal{R}^k)).
\]

Consider any \( t \in \partial_{L(\mathcal{G}^k)}(L(\mathcal{R}^k)) \). Then, by Proposition 3, we have \( t' := \Pi_{\Sigma}(t) \in \partial_{L(G)}(L(R)) \). Since \((L(G), L(R))\) is \( \{M_i\} \)-joint-\(k\)-prognosable, it follows from Lemma 1 that there exists \( i \in I \) such that

\[
(\forall u' \in L(R))O^k_i(t') \cap O^k_i(u') \neq \emptyset \Rightarrow u' \in \Im_{L(G)}(L(R)).
\]

Consider any \( u \in L(\mathcal{R}^k) \) such that \( M_i(t) = M_i(u) \). By the third part of Proposition 1, we have \( u' := \Pi_{\Sigma}(u) \in L(R) \). Since \( M_i(t) \in O^k_i(t') \), \( M_i(u) \in O^k_i(u') \), and \( M_i(t) = M_i(u) \), we have \( O^k_i(t') \cap O^k_i(u') \neq \emptyset \). It follows from (6) that \( u' \in \Im_{L(G)}(L(R)) \). By Proposition 2, we have \( u \in \Pi_{\Sigma}^{-1}(u') \cap L(\mathcal{R}^k) \subseteq \Im_{L(\mathcal{G}^k)}(L(\mathcal{R}^k)) \). Thus, \((L(\mathcal{G}^k), L(\mathcal{R}^k))\) is \( \{M_i\} \)-coprognosable.

To see that the converse need not hold, we show an example in which \( \{M_i\} \)-coprognosability of \((L(\mathcal{G}^k), L(\mathcal{R}^k))\) holds, but \( \{M_i\} \)-joint-\(k\)-prognosability of \((L(G), L(R))\) does not hold. Consider a plant model \( G \) and a nonfailure specification model \( R \) shown in Fig. 4 (a) and (b), respectively. Note that the event set \( \Sigma \) is \( \{a, b, c, d\} \). Let \( \Delta_1 = \{a'\} \), \( \Delta_2 = \{b'\} \), and, for \( \sigma \in \Sigma \), let

\[
M_1(\sigma) = \begin{cases} a', & \text{if } \sigma = a \\ \varepsilon, & \text{otherwise} \end{cases} \quad M_2(\sigma) = \begin{cases} b', & \text{if } \sigma = b \\ \varepsilon, & \text{otherwise} \end{cases}
\]

For \( k = 1 \), we have \( L(\mathcal{G}^1) - L(\mathcal{R}^1) = (aa'bb' + abab' + abb'a')d^{21} + (aa'b + aba')d + (aa'bb' + abab')d^3 + \Im_{L(\mathcal{G}^1)}(L(\mathcal{R}^1)) = \Im_{L(\mathcal{G}^1)}(L(\mathcal{R}^1)) = pr(aa'bb' + abab' + abb'a') - \varepsilon \). Consider any \( s \in aa'bb'd^{21} + aa'bd + \)
\[ aabdble \subseteq L(G^1) - L(\mathcal{R}^1) \]. For \( aabd \in \text{pr}(s) \cap L(\mathcal{R}^1) \), we have \( M_2(aabd) = a'b' \). Since there does not exist \( u \in L(\mathcal{R}^1) - 3L_{G^1}(L(\mathcal{R}^1)) \) such that \( M_2(u) = M_2(aabd) = a'b' \). Also, consider any \( s' \in aabd \cdot d^2 = aabd + aabd \cdot d^2 \subseteq L(G^1) - L(\mathcal{R}^1) \). For \( aabd \in \text{pr}(s') \cap L(\mathcal{R}^1) \), we have \( M_2(aabd) = b'a' \). There does not exist \( u' \in L(\mathcal{R}^1) - 3L_{G^1}(L(\mathcal{R}^1)) \) such that \( M_2(u') = M_2(aabd) = b'a' \). Moreover, consider any \( s'' \in abbab' \cdot d^2 = aabd + abbab' \cdot d^2 \subseteq L(G^1) - L(\mathcal{R}^1) \). For \( abbab' \in \text{pr}(s'') \cap L(\mathcal{R}^1) \), we have \( M_2(abbab') = b'a' \). There does not exist \( u'' \in L(\mathcal{R}^1) - 3L_{G^1}(L(\mathcal{R}^1)) \) such that \( M_2(u'') = M_2(abbab') = b'a' \). Thus, we can conclude that \( (L(G^1), L(\mathcal{R}^1)) \) is \( \{ M_1 \}-\)coprogносable.

We next show that \( (L(G), L(R)) \) is not \( \{ M_1 \}-\)joint-prognosable. Consider \( ab \in \partial_{L(G)}(L(R)) \). We have \( ca, cb \in L(R) - 3L_{G^1}(L(R)) \), \( O_1(ab) \cap O_1(ca) = \{ a'b', a' \} \cap \{ a' \} \neq \emptyset \), and \( O_1(ab) \cap O_2(cb) = \{ a'b', b'a', b' \} \cap \{ b' \} \neq \emptyset \). By Lemma 1, \( (L(G), L(R)) \) is not \( \{ M_1 \}-\)joint-prognosable.

In order to construct a testing automaton for verification, we introduce certain extended models which are obtained by performing the synchronous composition among an original model and certain masked-communication models [7].

- **Refined extended plant model:**
  \[
  \overline{G}^k := G^k \cdot |R^k| \cdot C_{12}^k \cdot C_{21}^k = (X \times Y \times Z^k \times Z^k, \Sigma \cup \Delta_1 \cup \Delta_2, \overline{\alpha}^k, (x_0, y_0, z_0, 0))
  \]
  which generates the same language as \( G^k \), but the execution of faulty traces reaches a state with the second coordinate “F”.

- **Extended local specification models:**
  \[
  R_1^k := R \cdot C_{12}^k = (Y \times Z^k, \Sigma \cup \Delta_2, \xi_1^k, (y_0, z_0)), \quad R_2^k := R \cdot C_{12}^k = (Y \times Z^k, \Sigma \cup \Delta_1, \xi_2^k, (y_0, z_0)).
  \]

Using these extended models, we construct the testing automaton \( T^k := (Z^k_T, \Sigma_T, \xi^k_T, Z^k_T, 0) \) as follows:

- \( Z^k_{T,0} = (X \times Y \times Z^k \times Z^k) \times (Y \times Z^k) \times (Y \times Z^k) \).
- \( Z_{T,0} = \{(x_0, y_0, z_0, y_0, z_0, 0)\} \).
- \( \Sigma_T = (\Sigma \cup \Delta_1 \cup \Delta_2 \cup \{ \varepsilon \}) \times (\Sigma \cup \Delta_2 \cup \{ \varepsilon \}) \times (\Sigma \cup \Delta_1 \cup \{ \varepsilon \}) \).
- \( \xi^k_T : Z^k_T \times \Sigma_T \rightarrow Z^k_T \) is defined as follows: For each \( z_T = (x, y, z_1, z_2, y_1, z_1, z_2) \in Z^k_T \) and \( \sigma_T = (\sigma, \sigma_1, \sigma_2) \in \Sigma_T \),
  \[
  \xi^k_T(z_T, \sigma_T) = \begin{cases} 
    \xi^k((x, y, z_1, z_2), \sigma) \times \xi^k((y_1, z_1, \sigma_1) \times \xi^k((y_2, z_2), \sigma_2), \\
    \emptyset, \quad \text{otherwise}.
  \end{cases}
  \]

The following definition identifies the boundary states (from which a failure can happen in a next step) and the nonindicator states (from which a failure is not inevitable) for the original plant and nonfailure specification models.

**Definition 4:** [6] Given the plant model \( G \) and the specification model \( R \), the set of
• **boundary** states $\partial(X \times Y) \subseteq X \times Y$ are states $(x, y)$ of $G\|R$ such that there exists $\sigma \in \Sigma$ with $(\alpha(x, \sigma), \beta(y, \sigma)) \in X \times \{F\}$;

• **nonindicator** states $\mathcal{Y}(Y) \subseteq Y$ are states of $R$ from which a cycle in $R$ can be reached.

The following lemma is immediate from Definitions 1 and 4.

**Lemma 2:** Given the pair $(L(G), L(R))$ of regular languages, for any $s \in L(R)$,

1) $s \in \partial_{L(G)}(L(R)) \iff (\alpha(x_0, s), \beta(y_0, s)) \in \partial(X \times Y)$;

2) $s \in \mathcal{Y}_{L(G)}(L(R)) \iff \beta(y_0, s) \in \mathcal{Y}(Y)$.

We have the following test for $\{M_i\}$-joint$^k$-prognosable of $(L(G), L(R))$.

**Theorem 3:** The pair $(L(G), L(R))$ of regular languages is not $\{M_i\}$-joint$^k$-prognosable if and only if there exists a reachable state $z_T = (x, y_1, z_1, z_2, y_1, z_1, y_2, z_2) \in Z_T^k$ of the testing automaton $T^k$ such that $(x, y)$ is a boundary state of $G\|R$ and $y_1$ and $y_2$ are nonindicator states of $R$.

**Proof:** ($\Leftarrow$) Let $z_T = (x, y_1, z_1, z_2, y_1, z_1, y_2, z_2) \in Z_T^k$ be a reachable state of $T_k^k$ such that $(x, y)$ is a boundary state of $G\|R$ and $y_1$ and $y_2$ are nonindicator states of $R$. There exist traces $t \in L(G^k) = L(G^k)$, $u_i \in L(R_i^k)$, and $u_2 \in L(R_2^k)$ such that $(x, y_1, z_1, z_2) \in \zeta^k((x_0, y_0, z_0, z_0), t), (y_1, z_2) \in \zeta^k((y_0, z_0, u_1), u_1)$, and $M_i(t) = M_i(u_i) (i = 1, 2)$.

Since $\Pi_{\Sigma}(t) \in L(G\|R) = L(R)$ and $(\alpha(x_0, \Pi_{\Sigma}(t)), \beta(y_0, \Pi_{\Sigma}(t))) = (x, y) \in \partial(X \times Y)$, we have by Lemma 2 that $\Pi_{\Sigma}(t) \in \partial_{L(G)}(L(R))$. Also, for each $u_i \in L(R_i^k) (i \in I)$, we define $u'_i \in (\Sigma \cup \Delta_1 \cup \Delta_2)^*$ as follows:

- If $u_i = \varepsilon$, then $u'_i = \varepsilon$.
- If $u_i \neq \varepsilon$, then we can write $u_i := a_1 a_2 \cdots a_l$, where $a_k \in \Sigma \cup \Delta_j \cup \{\varepsilon\} (k = 1, 2, \ldots, l)$ and $l = 2|\Pi_{\Sigma}(u_i)| - |\gamma_{j_i}(z_0, u_i)|$. Let $\Pi_{\Sigma}(u_i) = \sigma_1 \sigma_2 \cdots \sigma_{|\Pi_{\Sigma}(u_i)|}$. For each $k = 1, 2, \ldots, l$, we have $a_k = \sigma_{k'} (k' \in \{1, 2, \ldots, |\Pi_{\Sigma}(u_i)|\})$ or $a_k = M_j(\sigma_{k''}) (k'' \in \{1, 2, \ldots, |\Pi_{\Sigma}(u_i)| - |\gamma_{j_i}(z_0, u_i)|\})$.

Then, we define $u'_i := a'_1 a'_2 \cdots a'_l$ with

$$a'_{k'} = \begin{cases} 
\sigma_{k'}, & \text{if } a_k = \sigma_{k'} \\
M_j(\sigma_{k''})M_i(\sigma_{k''}), & \text{if } a_k = M_j(\sigma_{k''}) 
\end{cases}$$

By the construction of $u'_i$, we have $u'_i \in L(R_i^k) = M_i(u'_i) = M_i(u_i)$, and $\Pi_{\Sigma}(u'_i) = \Pi_{\Sigma}(u_i)$. Since $\Pi_{\Sigma}(u'_i) = \Pi_{\Sigma}(u_i) \in L(R)$ and $\beta(y_0, \Pi_{\Sigma}(u'_i)) = y_i \in \mathcal{Y}(Y)$, we have by Lemma 2 that $\Pi_{\Sigma}(u'_i) \in \mathcal{Y}_{L(G)}(L(R)) = L(R) - \mathcal{Y}_{L(G)}(L(R))$. Further, we have $M_i(t) = M_i(\Pi_{\Sigma}(u'_i) \cap L(G^k)) = O_i^k(\Pi_{\Sigma}(t))$ and $M_i(t) = M_i(u'_i) \in M_i(\Pi_{\Sigma}(u'_i) \cap L(G^k)) = O_i^k(\Pi_{\Sigma}(u'_i))$. Since $M_i(t) = M_i(u_i)$, we have $O_i^k(\Pi_{\Sigma}(t)) \cap O_i^k(\Pi_{\Sigma}(u'_i)) \neq \emptyset$.

Thus, we have $\Pi_{\Sigma}(t) \in \partial_{L(G)}(L(R))$, $\Pi_{\Sigma}(u'_i) \in L(R)$, $O_i^k(\Pi_{\Sigma}(t)) \cap O_i^k(\Pi_{\Sigma}(u'_i)) \neq \emptyset$, and $\Pi_{\Sigma}(u'_i) \notin \mathcal{Y}_{L(G)}(L(R)) (i = 1, 2)$. By Lemma 1, $(L(G), L(R))$ is not $\{M_i\}$-joint$^k$-prognosable.
(⇒) Suppose that \((L(G), L(R))\) is not \(\{M_i\}\)-joint\(^k\)-prognosable. By Lemma 1, there exists \(t \in \partial_{L(G)}(L(R))\) such that
\[
(\forall i \in I)(\exists u_i \in L(R))O^k_i(t) \cap O^k_i(u_i) \neq \emptyset \land u_i \notin \Xi_{L(G)}(L(R)).
\]
Consider any \(o_i \in O^k_i(t) \cap O^k_i(u_i)\). There exist \(t' \in \Pi_{k-1}^1(t) \cap L(G^k)\) and \(u'_i \in \Pi_{k-1}^1(u_i) \cap L(G^k)\) such that \(o_i = M_i(t') = M_i(u'_i)\). Since \(u_i \in L(R)\), we have by the fourth part of Proposition 1 that \(u'_i \in \Pi_{k-1}^1(u_i) \cap L(G^k) \subseteq L(R^k)\). It follows that \(v'_1 = \Pi_{k} \cup \Delta(v'_1) \in L(R^k_1)\) and \(v'_2 = \Pi_{k} \cup \Delta(v'_2) \in L(R^k_2)\). Also, we have \(M_i(t') = M_i(u'_i) = M_i(v'_i)\). Thus, there exists a reachable state \(z_T = (x, \overline{y}, z_1, z_2, y_1, z_{11}, y_2, z_{22}) \in Z_T^k\) of \(T^k\) such that \((x, \overline{y}, z_1, z_2) \in \xi^k((x_0, y_0, z_0, z_0), t')\) and \((y_1, z_{11}, y_2, z_{22}) \in \xi^k((y_0, z_0), v'_i) (i = 1, 2)\).

Since \(t \in \partial_{L(G)}(L(R))\), it follows from Lemma 2 that \((x, \overline{y}) = (\alpha(x_0, \Pi_{k}^1(t')), \beta(y_0, \Pi_{k}^1(t'))) = (\alpha(x_0, t), \beta(y_0, t)) \in \partial(X \times Y)\). Also, since \(u_i \in L(R) \cap \Xi_{L(G)}(L(R)) = \gamma_{L(G)}(L(R))\) and \(\Pi_{k}^1(v'_i) = \Pi_{k}^1(u'_i) = u_i\), we have by from Lemma 2 that \(y_i = \beta(y_0, u_i) \in \gamma(Y)\). This completes the proof.

Remark 4: We discuss the complexity of checking \(\{M_i\}\)-joint\(^k\)-prognosability. Note that the number of states of the masked-communication model \(C^k_{ij}\) is \(1 + |\Sigma| + |\Sigma|^2 + \cdots |\Sigma|^{k+1} = O(|\Sigma|^{k+2})\). Since the numbers of the states and the transitions of the testing automaton \(T^k\) are \(O(|X| \cdot |Y|^3 \cdot |\Sigma|^{4(k+2)})\) and \(O(|X| \cdot |Y|^3 \cdot |\Sigma|^{4(k+2)+3})\), respectively, it follows from Theorem 3 that the complexity of checking \(\{M_i\}\)-joint\(^k\)-prognosability is \(O(\|X| \cdot |Y|^3 \cdot |\Sigma|^{4(k+2)+3})\) which is polynomial in the number of the states of the plant and speciation and the numbers of the events, but exponential in the delay bound.

The following example illustrates the test of \(\{M_i\}\)-joint\(^k\)-prognosability.

Example 3: We revisit the example considered in the proof of Proposition 4 with \(k = 1\). Since \((\alpha(x_2, d), \overline{y}(y_2, d)) = (x_2, F) \in G||\overline{R}, (x_2, y_2)\) is a unique boundary state of \(G||R\), i.e., \(\partial(X \times Y) = \{(x_2, y_2)\}\). Also, since there is a self-loop at the state \(y_4\) in \(R\), which can be reached from \(y_0, y_3,\) and \(y_4\), the states \(y_0, y_3,\) and \(y_4\) are nonindicator states of \(R\), i.e., \(\gamma(Y) = \{y_0, y_3, y_4\}\).

A part of the testing automaton \(T^1\) is shown in Fig. 5. The state \((x_2, y_2, ab, ab, y_4, ca, y_4, cb)\) is a reachable state of \(T^1\). Since \(\partial(X \times Y) = \{(x_2, y_2)\}\) and \(\gamma(Y) = \{y_0, y_3, y_4\}\), the path shown in Fig. 5 indicates that the first (resp., second) prognoser cannot distinguish between a boundary trace \(ab \in \partial_{L(G)}(L(R))\) and a nonindicator trace \(ca\) (resp., \(cb\)). Thus, \((L(G), L(R))\) is not \(\{M_i\}\)-joint\(^1\)-prognosable.
VI. Conclusion

The paper studied the problem of distributed failure prognosis of DESs. The local prognosers exchange their observations of the plant events among each other over communication channels that introduce bounded delays, and use such aggregated observations to arrive at a prognostic decision. The property of joint-prognosability was introduced to capture the condition under which any failure can be predicted by some local prognoser prior to its occurrence. An algorithm to check the joint-prognosability property was also presented. To cope with the complexity of the verification problem in a practical setting, a future direction would be to cast the problem as a model-checking problem so as to take advantage of the existing tools.

References