Automatica 46 (2010) 1510–1516

Contents lists available at ScienceDirect

Automatica

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

Brief paper

Reliable supervisory control for general architecture of decentralized discrete event systems[☆]

Fuchun Liu[a,b,*], Hai Lin[b]

[a] Faculty of Computer, Guangdong University of Technology, Guangzhou, 510006, China

[b] Department of Electrical and Computer Engineering, National University of Singapore, Singapore, 117576, Singapore

ARTICLE INFO

Article history:
Received 17 June 2009
Received in revised form
8 May 2010
Accepted 18 May 2010
Available online 3 July 2010

Keywords:
Discrete event systems
Decentralized supervisors
Reliable control
General architecture

ABSTRACT

In this paper, we investigate the reliable decentralized supervisory control of discrete event systems (DESs) under the general architecture, where the decision for controllable events is a combination of the conjunctive and disjunctive fusion rules. By reliable control, we mean that the performance of closed-loop systems will not be degraded even in the face of possible failures of some local supervisors. The main contributions are twofold. First, a necessary and sufficient condition for the existence of a k-reliable decentralized supervisor under the general architecture is presented after introducing notions of $\widetilde{\Sigma}_{uc}$-controllability and k-reliable $\widetilde{\Sigma}_c$-coobservability. Second, a polynomial-time algorithm to verify the reliable $\widetilde{\Sigma}_c$-coobservability of a specification is proposed.

1. Introduction

Motivated by the fact that more and more man-made systems built nowadays are becoming distributed and networked, the decentralized framework of discrete event systems (DESs) has attracted many researchers' attention (Kumar & Takai, 2007; Liu, Qiu, Xing, & Fan, 2008; Park & Cho, 2007; Rohloff & Lafortune, 2003). In particular, Yoo and Lafortune (2002) presented a framework named the general architecture for decentralized supervisory control of DESs based on a combination of the conjunctive and disjunctive fusion rules for local decisions. Up to now, this kind of general architecture has been extensively adopted. For example, Rohloff and Lafortune (2003) presented a new approach for safe controllers synthesis of DESs under the general architecture. Kumar and Takai (2007) investigated inference-based ambiguity management in decentralized decision-making for the general decentralized framework. In Yoo and Lafortune (2004), the decentralized supervisory control for conditional decisions under the general architecture was studied. Park and Cho (2007) dealt with the decentralized control of DESs with conjunctive and permissive decision structures under communication delays.

In this paper, the problem of reliable control under the general decentralized architecture is investigated, and the results in Liu and Lin (2009) are extended. By reliable supervisory control, we mean that the performance of a closed-loop system will not be degraded even in the face of possible failures of some local supervisors. In fact, the reliable control issue has been considered for the control of continuous variable systems, stochastic systems, and switched systems (e.g. Zhang, Guan, & Feng, 2008, and the references therein). Recently, the reliable control of DESs was also addressed (Liu & Lin, 2009; Takai & Ushio, 2000, 2003a). In the view of Takai and Ushio (2000), a decentralized supervisor of a DES equipped with n local supervisors is called k-reliable ($1 \leq k \leq n$) if it achieves the given specification under possible failure of no more than $n-k$ local supervisors. A necessary and sufficient condition for the existence of a k-reliable decentralized supervisor was deduced in Takai and Ushio (2000), which was then extended to the case of non-closed marked language specifications in Takai and Ushio (2003a). We also dealt with reliable decentralized supervisory control of DESs with communication delays in Liu and Lin (2009).

This paper aims to investigate the following issues for reliable decentralized supervisory control of DESs under the general architecture:

> **Existence problem:** Given a specification and a plant equipped with a number of local supervisors, does there exist a reliable decentralized supervisor such that it can achieve exactly the specification under possible failures of some local supervisors?

☆ This work was supported in part by the National Natural Science Foundation under Grant 60974019, the Guangdong Province Natural Science Foundation under Grant 9451009001002686 of China, the Guangdong University of Technology's Foundation, and Singapore Ministry of Education's AcRF Tier 1 funding, TDSI, TL. This work was not presented at any IFAC meeting. This paper was recommended for publication in revised form by Associate Editor Bart De Schutter under the direction of Editor Ian R. Petersen.

* Corresponding author at: Faculty of Computer, Guangdong University of Technology, Guangzhou, 510006, China.

E-mail addresses: liufch8@gmail.com (F. Liu), elelh@nus.edu.sg (H. Lin).

0005-1098/$ – see front matter © 2010 Elsevier Ltd. All rights reserved.
doi:10.1016/j.automatica.2010.06.011

Verification problem: If positive, then how to formalize the verification of the reliable decentralized supervisor with an efficient algorithm?

To answer these questions, we first introduce the concepts of $\widetilde{\Sigma}_{uc}$-controllability and k-reliable $\widetilde{\Sigma}_c$-coobservability under the general architecture, and then a necessary and sufficient condition for the existence of a k-reliable decentralized supervisor is proposed. We notice that the general architecture for reliable control is also considered in Takai and Ushio (2003b), but there exist several distinctive features between our current work and Takai and Ushio (2003b). First, the definition of a reliable decentralized supervisor employed here is different from that defined in Takai and Ushio (2003b). Second, in order to characterize the existence of a reliable decentralized supervisor, we introduce a new concept, namely k-reliable $\widetilde{\Sigma}_c$-coobservability, to describe the requirement for the controllable events. By contrast, the authors of Takai and Ushio (2003b) partitioned the controllable event set into four subsets and defined the corresponding notion of reliable coobservability over the four subsets. The third difference is the verification of the reliable decentralized supervisor. In this paper, a constructive methodology for verifying such a k-reliable decentralized supervisor is presented, which is based on the construction of two nondeterministic automata to track the violation of k-reliable $\widetilde{\Sigma}_c$-coobservability.

2. Problem formulation

A DES is modeled by an automaton $G = (Q, \Sigma, \delta, q_0, Q_m)$, where Q is the set of states with the initial state q_0, Σ is the finite set of events, δ is the transition function, and $Q_m \subseteq Q$ is the marked state set. Let Σ^* denote the set of all finite strings over Σ, including the empty string ϵ. δ can be extended to domain $Q \times \Sigma^*$ in a usual manner. A subset of Σ^* is usually called a *language*. The languages generated and marked by G are $L(G) = \{s \in \Sigma^* : \delta(q_0, s) \text{ is defined}\}$ and $L_m(G) = \{s \in L(G) : \delta(q_0, s) \in Q_m\}$, respectively. A language $K \subseteq \Sigma^*$ is *prefix-closed* if $K = \overline{K}$, where $\overline{K}$ is the set of all prefixes of strings in K; and K is $L_m(G)$-*closed* if $K = \overline{K} \cap L_m(G)$.

In the decentralized architecture, a plant is jointly controlled by n local supervisors, each of which observes the locally observable events and controls the locally controllable events. Let $I = \{1, \ldots, n\}$. For $i \in I$, denote $\Sigma_{i,c}$ and $\Sigma_{i,uc}$ as the sets of locally controllable and uncontrollable events, respectively, and denote $\Sigma_{i,o}$ and $\Sigma_{i,uo}$ as the sets of locally observable and unobservable events, respectively. Denote $\Sigma_{uc} = \Sigma - \Sigma_c$ and $\Sigma_{uo} = \Sigma - \Sigma_o$ where $\Sigma_c = \cup_{i\in I} \Sigma_{i,c}$ and $\Sigma_o = \cup_{i\in I} \Sigma_{i,o}$. In particular, for the general decentralized architecture proposed in Yoo and Lafortune (2002), the decision fusion for global enable and disable events is a fixed combination of the conjunctive and disjunctive fusions. Formally, the set of controllable events Σ_c is further partitioned into $\Sigma_{c,e}$ and $\Sigma_{c,d}$, i.e., $\Sigma_c = \Sigma_{c,e} \dot\cup \Sigma_{c,d}$, where the local decisions over $\Sigma_{c,e}$ are processed by the conjunctive fusion rule, while the local decisions over $\Sigma_{c,d}$ are made by the disjunctive fusion rule. The local supervisor is defined as a function $S_{P_i} : P_i(\Sigma^*) \to \Gamma = \{\gamma \in 2^\Sigma : \Sigma_{uc} \cup (\Sigma_{c,e} - \Sigma_{i,c}) \subseteq \gamma, (\Sigma_{c,d} - \Sigma_{i,c}) \cap \gamma = \emptyset\}$, where P_i is projection mapping.

In order to formalize the notion of reliable decentralized supervisor in the general architecture, we extend the decentralized supervisor defined in Yoo and Lafortune (2002) to an A-decentralized supervisor synthesized by a part of the local supervisors, where $A \subseteq I$. Denote $\Sigma_{A,c} = \cup_{i\in A} \Sigma_{i,c}$ and $\Sigma_{A,uc} = \Sigma - \Sigma_{A,c}$.

Definition 1. Let $S_{P_1}, \ldots, S_{P_n}$ be the local supervisors and $A \subseteq I$. The *A-decentralized supervisor*, denoted by $\{S_{P_i} : i \in A\}$ or simply S_A, is defined as: for $s \in \Sigma^*$,

$$S_A(s) = P_{\Sigma_{c,e}}\left(\bigcap_{i\in A} S_{P_i}(P_i(s))\right) \cup P_{\Sigma_{c,d}}\left(\bigcup_{i\in A} S_{P_i}(P_i(s))\right) \cup \Sigma_{A,uc}, \quad (1)$$

where $P_{\Sigma_{c,e}} : \Sigma \to \Sigma^*_{c,e}$ and $P_{\Sigma_{c,d}} : \Sigma \to \Sigma^*_{c,d}$ are projection mappings.

Definition 2. *The language generated by* S_A, denoted by $L(G, S_A)$, is defined recursively in the usual manner: $\epsilon \in L(G, S_A)$, and $s\sigma \in L(G, S_A)$ if and only if $s \in L(G, S_A)$, $s\sigma \in L(G)$ and $\sigma \in S_A(s)$. *The marked language* is defined as $L_m(G, S_A) = L(G, S_A) \cap L_m(G)$.

Definition 3. Let $A \in 2^I$. A language $K \subseteq L(G)$ is said to be $\Sigma_{A,uc}$-*controllable* (*with respect to* $L(G)$ *and* $\Sigma_{A,uc}$) if $\overline{K}\Sigma_{A,uc} \cap L(G) \subseteq \overline{K}$.

Definition 4. Let $A \in 2^I$. A language $K \subseteq L(G)$ is said to be $\Sigma_{A,c}$-*coobservable* (*with respect to* $L(G)$ *and* $\Sigma_{A,c}$), if for any $s \in \overline{K}$ and $\sigma \in \Sigma_{A,c}$, the following conditions hold:

(1) $[\sigma \in \Sigma_{c,e}] \wedge [s\sigma \in L(G) - \overline{K}] \Rightarrow$

$$(\exists i \in A \cap In(\sigma))P_i^{-1}P_i(s)\sigma \cap \overline{K} = \emptyset; \quad (2)$$

(2) $[\sigma \in \Sigma_{c,d}] \wedge [s\sigma \in \overline{K}] \Rightarrow$

$$(\exists i \in A \cap In(\sigma))(P_i^{-1}P_i(s) \cap \overline{K})\sigma \cap L(G) \subseteq \overline{K}, \quad (3)$$

where $In(\sigma) = \{i \in I : \sigma \in \Sigma_{i,c}\}$.

Remark 1. If $A = I$, then Definition 4 degenerates into the coobservability under the conjunctive architecture and the coobservability under the disjunctive architecture when $\Sigma_c = \Sigma_{c,e}$ and when $\Sigma_c = \Sigma_{c,d}$, respectively.

Proposition 1. *Let* $A \in 2^I$. *For a nonempty language* $K \subseteq L(G)$, *there is an A-decentralized supervisor* S_A *such that* $L(G, S_A) = \overline{K}$ *if and only if* K *is* $\Sigma_{A,uc}$-*controllable and* $\Sigma_{A,c}$-*coobservable.*

Proof. The proof is similar to that of Theorem 1 in Liu and Lin (2009), so we omit it here for lack of space. □

Definition 5. Let $S_{P_1}, S_{P_2}, \ldots, S_{P_n}$ be the local supervisors and $K \subseteq L(G)$. A decentralized supervisor $\{S_{P_i} : i \in I\}$ is said to be *k-reliable*, if for any $A \in 2^I$ with $|A| \geq k$,

$$L(G, S_A) = \overline{K}, \quad (4)$$

where $1 \leq k \leq n$, and $|A|$ is the number of elements of A.

Intuitively, a k-reliable decentralized supervisor means that the plant may achieve exactly the specification under the control of at least k arbitrary local supervisors.

Example 1. We consider a DES G with $L(G) = \overline{\sigma_1 + \sigma_2 + \sigma_4\sigma_5\sigma_1 + \sigma_3\sigma_5\sigma_2}$ and a specification $K = \sigma_1 + \sigma_2 + \sigma_4\sigma_5 + \sigma_3\sigma_5$. Assume $n = 3$, and $\Sigma_{1,o} = \{\sigma_1, \sigma_2, \sigma_5\}$, $\Sigma_{2,o} = \{\sigma_1, \sigma_4\}$, $\Sigma_{3,o} = \{\sigma_2, \sigma_3\}$; $\Sigma_{1,c} = \{\sigma_1, \sigma_2\}$, $\Sigma_{2,c} = \{\sigma_1, \sigma_4\}$, $\Sigma_{3,c} = \{\sigma_2, \sigma_3\}$, where $\Sigma_{c,e} = \{\sigma_1, \sigma_3\}$, $\Sigma_{c,d} = \{\sigma_2, \sigma_4\}$.

We can design the local supervisors as follows:

$$S_{P_1}(P_1(s)) = \begin{cases} \{\sigma_1, \sigma_2, \sigma_3, \sigma_5\}, & \text{if } P_1(s) = \epsilon, \\ \{\sigma_3, \sigma_5\}, & \text{if } P_1(s) = \sigma_5, \\ \{\sigma_2, \sigma_3, \sigma_5\}, & \text{otherwise.} \end{cases}$$

$$S_{P_2}(P_2(s)) = \begin{cases} \{\sigma_1, \sigma_3, \sigma_4, \sigma_5\}, & \text{if } P_2(s) = \epsilon, \\ \{\sigma_3, \sigma_4, \sigma_5\}, & \text{otherwise.} \end{cases}$$

$$S_{P_3}(P_3(s)) = \begin{cases} \{\sigma_1, \sigma_2, \sigma_3, \sigma_5\}, & \text{if } P_3(s) = \epsilon, \\ \{\sigma_1, \sigma_5\}, & \text{if } P_3(s) = \sigma_3, \\ \{\sigma_1, \sigma_2, \sigma_5\}, & \text{otherwise.} \end{cases}$$

Then the languages generated by at least two arbitrary local supervisors can be calculated as $L(G, S_{\{1,2\}}) = L(G, S_{\{1,3\}}) = L(G, S_{\{2,3\}}) = L(G, S_{\{1,2,3\}}) = \overline{\sigma_1 + \sigma_2 + \sigma_4\sigma_5 + \sigma_3\sigma_5} = \overline{K}$, which indicates that the decentralized supervisor is 2-reliable. □

3. Existence of reliable decentralized supervisor

First we introduce some notations and notions. For $i \in I$, denote $\widetilde{\Sigma}_{i,uc} = \Sigma - \widetilde{\Sigma}_{i,c}$, where

$$\widetilde{\Sigma}_{i,c} = \{\sigma \in \Sigma_{i,c} : |In(\sigma)| \geq n - k + 1\}. \quad (5)$$

For $A \in 2^I$, let $\widetilde{\Sigma}_{A,c} = \cup_{i\in A} \widetilde{\Sigma}_{i,c}$ and $\widetilde{\Sigma}_{A,uc} = \Sigma - \widetilde{\Sigma}_{A,c}$. For the sake of simplicity, denote $\widetilde{\Sigma}_c = \widetilde{\Sigma}_{I,c}$ and $\widetilde{\Sigma}_{uc} = \widetilde{\Sigma}_{I,uc}$ when $A = I$.

Definition 6. A language $K \subseteq L(G)$ is said to be $\widetilde{\Sigma}_{uc}$*-controllable* if $\overline{K}\widetilde{\Sigma}_{uc} \cap L(G) \subseteq \overline{K}$.

Definition 7. Let $1 \leq k \leq n$. A language $K \subseteq L(G)$ is said to be *k-reliably* $\widetilde{\Sigma}_c$*-coobservable*, if for any $s \in \overline{K}$ and $\sigma \in \widetilde{\Sigma}_c$, we have $|A_{s,\sigma}| \geq n - k + 1$, where

$$A_{s,\sigma} = \begin{cases} \{i \in In(\sigma) : s\sigma \in L(G) - \overline{K} \Rightarrow \\ \quad P_i^{-1}P_i(s)\sigma \cap \overline{K} = \emptyset\}, \quad \text{if } \sigma \in \Sigma_{c,e}; \\ \{i \in In(\sigma) : s\sigma \in \overline{K} \Rightarrow \\ \quad (P_i^{-1}P_i(s) \cap \overline{K})\sigma \cap L(G) \subseteq \overline{K}\}, \quad \text{if } \sigma \in \Sigma_{c,d}. \end{cases} \quad (6)$$

Remark 2. The above notion extends the corresponding notion of reliable $(\widetilde{\Sigma}_c,\ k)$-coobservability presented in Takai and Ushio (2000) to the general architecture. When $\Sigma_c = \Sigma_{c,e}$, these two notions are consistent.

Theorem 1. *Let $1 \leq k \leq n$ and $K \subseteq L(G)$ be nonempty. There is a k-reliable decentralized supervisor under the general architecture, if and only if, K is $\widetilde{\Sigma}_{uc}$-controllable and k-reliably $\widetilde{\Sigma}_c$-coobservable.*

Proof. $(\Rightarrow)$ (1) We first prove the $\widetilde{\Sigma}_{uc}$-controllability of K. For any $s \in \overline{K}$ and $\sigma \in \widetilde{\Sigma}_{uc}$ with $s\sigma \in L(G)$, there is $A \in 2^I$ with $|A| \geq k$ such that $\sigma \in \Sigma_{A,uc}$ due to $|In(\sigma)| \leq n - k$. From the k-reliability of the decentralized supervisor, $L(G, S_A) = \overline{K}$. By Proposition 1, K is $\Sigma_{A,uc}$-controllable, i.e., $\overline{K}\Sigma_{A,uc} \cap L(G) \subseteq \overline{K}$. Therefore, $s\sigma \in \overline{K}$, and then $\overline{K}\widetilde{\Sigma}_{uc} \cap L(G) \subseteq \overline{K}$.

(2) Next, we verify the k-reliable $\widetilde{\Sigma}_c$-coobservability of K by contradiction. Suppose that there is $s \in \overline{K}$ and $\sigma \in \widetilde{\Sigma}_c$ satisfying $|A_{s,\sigma}| \leq n - k$, then $|In(\sigma) - A_{s,\sigma}| \geq 1$ due to $|In(\sigma)| \geq n - k + 1$. Therefore, there is $j \in In(\sigma)$ and $B \in 2^I$ with $|B| \geq k$ such that $A_{s,\sigma} \cap B = \emptyset$ and $j \in B$, which implies $\sigma \in \Sigma_{B,c}$. Due to the k-reliability of the decentralized supervisor, we have $L(G, S_B) = \overline{K}$. According to Proposition 1, K is $\Sigma_{B,c}$-coobservable. By Definition 4, for the above s and σ, if $\sigma \in \Sigma_{c,e}$ and $s\sigma \in L(G) - \overline{K}$, then there exists $\ell \in B \cap \mathrm{In}(\sigma)$ satisfying $P_\ell^{-1}P_\ell(s)\sigma \cap \overline{K} = \emptyset$, i.e., $\ell \in A_{s,\sigma}$. Hence $\ell \in A_{s,\sigma} \cap B$, which is in contradiction with $A_{s,\sigma} \cap B = \emptyset$. On the other side, if $\sigma \in \Sigma_{c,d}$ and $s\sigma \in \overline{K}$, then by Definition 4, there exists $h \in B \cap In(\sigma)$ with $(P_h^{-1}P_h(s) \cap \overline{K})\sigma \cap L(G) \subseteq \overline{K}$, i.e., $h \in A_{s,\sigma}$. So $h \in A_{s,\sigma} \cap B$, which is also in contradiction with $A_{s,\sigma} \cap B = \emptyset$.

$(\Leftarrow)$ Define the local supervisor S_{P_i} $(i \in I)$ as follows:

$$\begin{aligned} S_{P_i}(P_i(s)) = &\{\sigma \in \Sigma_{i,c,e} : P_i^{-1}P_i(s)\sigma \cap \overline{K} \neq \emptyset\} \\ &\cup \{\sigma \in \Sigma_{i,c,d} : (P_i^{-1}P_i(s) \cap \overline{K})\sigma \cap L(G) \subseteq \overline{K}\} \\ &\cup (\Sigma_{c,e} - \Sigma_{i,c}) \cup \Sigma_{uc}. \end{aligned} \quad (7)$$

To prove $\{S_{P_i} : i \in I\}$ being k-reliable, by Proposition 1, we only need to show that K is both $\Sigma_{A,uc}$-controllable and $\Sigma_{A,c}$-coobservable for any $A \in 2^I$ with $|A| \geq k$.

(1) Notice that for any $A \in 2^I$ with $|A| \geq k$, $\Sigma_{A,uc} = \Sigma_{uc} \cup (\Sigma_c - \Sigma_{A,c}) \subseteq \Sigma_{uc} \cup \{\sigma \in \Sigma_c : |In(\sigma)| \leq n - k\} = \widetilde{\Sigma}_{uc}$. Therefore, $\overline{K}\Sigma_{A,uc} \cap L(G) \subseteq \overline{K}\widetilde{\Sigma}_{uc} \cap L(G) \subseteq \overline{K}$ from the $\widetilde{\Sigma}_{uc}$-controllability of K. That is, K is $\Sigma_{A,uc}$-controllable.

(2) For any $A \in 2^I$ with $|A| \geq k$, $s \in \overline{K}$ and $\sigma \in \Sigma_{A,c}$, we prove that K is $\Sigma_{A,c}$-coobservable from the following two cases.

Case 1: If $\sigma \in \Sigma_{A,c} \cap \widetilde{\Sigma}_c$, then $|A_{s,\sigma}| \geq n - k + 1$ since K is k-reliably $\widetilde{\Sigma}_c$-coobservable. Consequently, $A \cap A_{s,\sigma} \neq \emptyset$, i.e., there is $i_0 \in A$ such that $i_0 \in A_{s,\sigma}$. When $\sigma \in \Sigma_{c,e}$ and $s\sigma \in L(G) - \overline{K}$, by Eq. (6), $i_0 \in In(\sigma)$ and $P_{i_0}^{-1}P_{i_0}(s)\sigma \cap \overline{K} = \emptyset$, i.e., Eq. (2) holds. On the other hand, when $\sigma \in \Sigma_{c,d}$ and $s\sigma \in \overline{K}$, by Eq. (6), we have $i_0 \in \mathrm{In}(\sigma)$ and $(P_{i_0}^{-1}P_{i_0}(s) \cap \overline{K})\sigma \cap L(G) \subseteq \overline{K}$, i.e., Eq. (3) holds. So K is $\Sigma_{A,c}$-coobservable.

Case 2: If $\sigma \in \Sigma_{A,c} - (\Sigma_{A,c} \cap \widetilde{\Sigma}_c)$, then $s\sigma \notin L(G) - \overline{K}$ according to the $\widetilde{\Sigma}_{uc}$-controllability of K. So we only need to prove Eq. (3) of Definition 4. Due to $\sigma \in \Sigma_{A,c}$, $A \cap In(\sigma) \neq \emptyset$. Moreover, for each $i \in A \cap In(\sigma)$, we have $(P_i^{-1}P_i(s) \cap \overline{K})\sigma \cap L(G) \subseteq \overline{K}\widetilde{\Sigma}_{uc} \cap L(G) \subseteq \overline{K}$, i.e., Eq. (3) holds. Therefore, we also obtain that K is $\Sigma_{A,c}$-coobservable in this case. □

Remark 3. Theorem 1 generalizes the results of Takai and Ushio (2000) to the general architecture. The existence condition of a k-reliable decentralized supervisor in Takai and Ushio (2000) is a special case of the above Theorem 1 with $\Sigma_c = \Sigma_{c,e}$.

4. Verification of reliable decentralized supervisors

Theorem 1 illustrates that the existence of k-reliable decentralized supervisors depends on the $\widetilde{\Sigma}_{uc}$-controllability and the k-reliable $\widetilde{\Sigma}_c$-coobservability of specification.

For the conventional controllability of K (i.e., $\overline{K}\Sigma_{uc} \cap L(G) \subseteq \overline{K}$), a test algorithm is described in Cassandras and Lafortune (1999). So, the $\widetilde{\Sigma}_{uc}$-controllability of K (i.e., $\overline{K}\widetilde{\Sigma}_{uc} \cap L(G) \subseteq \overline{K}$) can be similarly checked by this test algorithm with a slight change that $\widetilde{\Sigma}_{uc}$ replaces Σ_{uc}, which requires the computational complexity of $O(|Q^G| \cdot |Q^H|)$, where $|Q^G|$ and $|Q^H|$ are the sizes of state sets of G and H, respectively.

For the test of the standard coobservability, a polynomial-time algorithm was originally presented in Rudie and Willems (1995). This was then developed in Yoo and Lafortune (2002, 2004) and others. Next, based on the methodology of Rudie and Willems (1995), we present an approach to construct two nondeterministic automata, namely the $\Sigma_{c,e}$-discriminator (denoted by M_e) and the $\Sigma_{c,d}$-discriminator (denoted by M_d), to check the k-reliable $\widetilde{\Sigma}_c$-coobservability $|A_{s,\sigma}| \geq n - k + 1$ for $\sigma \in \widetilde{\Sigma}_c \cap \Sigma_{c,e}$ and $\sigma \in \widetilde{\Sigma}_c \cap \Sigma_{c,d}$, respectively.

Let specification K be generated by automaton H, i.e., $K = L_m(H)$ and $\overline{K} = L(H)$. For checking the k-reliable $\widetilde{\Sigma}_c$-coobservability of K, we introduce a symbol f (for "failure") to label the local supervisors out of operation, where $f \notin Q^H \cup Q^G$.

Definition 8. Given a specification automaton $H = (Q^H, \Sigma, \delta^H, q_0^H, Q_m^H)$ and a plant $G = (Q^G, \Sigma, \delta^G, q_0^G, Q_m^G)$ with n local supervisors. *The $\Sigma_{c,e}$-discriminator of k-reliable $\widetilde{\Sigma}_c$-coobservability* is defined as a nondeterministic automaton

$$M_e = (Q^{M_e}, \Sigma, \delta^{M_e}, q_0^{M_e}, Q_m^{M_e}), \quad (8)$$

where

(1) the state space is

$$Q^{M_e} = \underbrace{(Q^H \cup \{f\}) \times \cdots \times (Q^H \cup \{f\})}_{n} \times Q^H \times Q^G.$$

(2) $q_0^{M_e} = (q_0^H, \ldots, q_0^H, q_0^H, q_0^G) \in Q^{M_e}$ is the initial state.

(3) The transition function $\delta^{M_e} : Q^{M_e} \times \Sigma \to 2^{Q^{M_e}}$ will be given in Definition 9.

(4) The marked state set $Q_m^{M_e}$ will be defined in Definition 11.

Before defining the transition function δ^{M_e}, we first give the following conditions: for $(p_1, \ldots, p_n, p_{n+1}, p_{n+2}) \in Q^{M_e}$ and $\sigma \in \widetilde{\Sigma}_c$, conditions (C1), ..., (Cn) and (C0) are defined as

Condition (Ci): either $\sigma \notin \Sigma_{i,c}$ or $\delta^H(p_i, \sigma)$ and $\delta^G(p_{n+2}, \sigma)$ are defined but $\delta^H(p_{n+1}, \sigma)$ is undefined, where $i \in I$.

Condition (C0): $\sigma \in \widetilde{\Sigma}_c \cap \Sigma_{c,e}$ and at least one of the conditions (C1), ..., (Cn) holds.

Definition 9. The transition function of M_e is defined as a partial function $\delta^{M_e} : Q^{M_e} \times \Sigma \to 2^{Q^{M_e}}$, for $q^{M_e} = (p_1, \ldots, p_n, p_{n+1}, p_{n+2}) \in Q^{M_e}$ and $\sigma \in \Sigma$, $\delta^{M_e}(q^{M_e}, \sigma)$ is informally defined as all possible states. In particular, if Condition (C0) holds, $\delta^{M_e}(q^{M_e}, \sigma) = (\Delta_1, \ldots, \Delta_n, p_{n+1}, p_{n+2})$, where for each $i \in I$, $\Delta_i = f$ if Condition (Ci) holds; otherwise, $\Delta_i = p_i$. For simplicity, we formally define δ^{M_e} for the case of three local supervisors (i.e., $n = 3$), which can be extended directly to the case of any finite number of local supervisors:

(i) For $\sigma \notin (\Sigma_{1,o} \cup \Sigma_{2,o} \cup \Sigma_{3,o})$,

$$\delta^{M_e}((p_1, p_2, p_3, p_4, p_5), \sigma) = \begin{cases} (\delta^H(p_1, \sigma), p_2, p_3, p_4, p_5), \\ (p_1, \delta^H(p_2, \sigma), p_3, p_4, p_5), \\ (p_1, p_2, \delta^H(p_3, \sigma), p_4, p_5), \\ (p_1, p_2, p_3, \delta^H(p_4, \sigma), \delta^G(p_5, \sigma)), \\ (\delta^H(p_1, \sigma), \delta^H(p_2, \sigma), \delta^H(p_3, \sigma), \delta^H(p_4, \sigma), \delta^G(p_5, \sigma)), \\ (\Delta_1, \Delta_2, \Delta_3, p_4, p_5), \quad \text{if Condition (C0) holds.} \end{cases}$$

(ii) For $\sigma \in \Sigma_{1,o} \setminus (\Sigma_{2,o} \cup \Sigma_{3,o})$,

$$\delta^{M_e}((p_1, p_2, p_3, p_4, p_5), \sigma) = \begin{cases} (p_1, \delta^H(p_2, \sigma), p_3, p_4, p_5), \\ (p_1, p_2, \delta^H(p_3, \sigma), p_4, p_5), \\ (\delta^H(p_1, \sigma), p_2, p_3, \delta^H(p_4, \sigma), \delta^G(p_5, \sigma)), \\ (\delta^H(p_1, \sigma), \delta^H(p_2, \sigma), \delta^H(p_3, \sigma), \delta^H(p_4, \sigma), \delta^G(p_5, \sigma)), \\ (\Delta_1, \Delta_2, \Delta_3, p_4, p_5), \quad \text{if Condition (C0) holds.} \end{cases}$$

(iii) For $\sigma \in \Sigma_{2,o} \setminus (\Sigma_{1,o} \cup \Sigma_{3,o})$,

$$\delta^{M_e}((p_1, p_2, p_3, p_4, p_5), \sigma) = \begin{cases} (\delta^H(p_1, \sigma), p_2, p_3, p_4, p_5), \\ (p_1, p_2, \delta^H(p_3, \sigma), p_4, p_5), \\ (p_1, \delta^H(p_2, \sigma), p_3, \delta^H(p_4, \sigma), \delta^G(p_5, \sigma)), \\ (\delta^H(p_1, \sigma), \delta^H(p_2, \sigma), \delta^H(p_3, \sigma), \delta^H(p_4, \sigma), \delta^G(p_5, \sigma)), \\ (\Delta_1, \Delta_2, \Delta_3, p_4, p_5), \quad \text{if Condition (C0) holds.} \end{cases}$$

(iv) For $\sigma \in \Sigma_{3,o} \setminus (\Sigma_{1,o} \cup \Sigma_{2,o})$,

$$\delta^{M_e}((p_1, p_2, p_3, p_4, p_5), \sigma) = \begin{cases} (\delta^H(p_1, \sigma), p_2, p_3, p_4, p_5), \\ (p_1, \delta^H(p_2, \sigma), p_3, p_4, p_5), \\ (p_1, p_2, \delta^H(p_3, \sigma), \delta^H(p_4, \sigma), \delta^G(p_5, \sigma)), \\ (\delta^H(p_1, \sigma), \delta^H(p_2, \sigma), \delta^H(p_3, \sigma), \delta^H(p_4, \sigma), \delta^G(p_5, \sigma)), \\ (\Delta_1, \Delta_2, \Delta_3, p_4, p_5), \quad \text{if Condition (C0) holds.} \end{cases}$$

(v) For $\sigma \in (\Sigma_{1,o} \cap \Sigma_{2,o}) \setminus \Sigma_{3,o}$,

$$\delta^{M_e}((p_1, p_2, p_3, p_4, p_5), \sigma) = \begin{cases} (p_1, p_2, \delta^H(p_3, \sigma), p_4, p_5), \\ (\delta^H(p_1, \sigma), \delta^H(p_2, \sigma), p_3, \delta^H(p_4, \sigma), \delta^G(p_5, \sigma)), \\ (\delta^H(p_1, \sigma), \delta^H(p_2, \sigma), \delta^H(p_3, \sigma), \delta^H(p_4, \sigma), \delta^G(p_5, \sigma)), \\ (\Delta_1, \Delta_2, \Delta_3, p_4, p_5), \quad \text{if Condition (C0) holds.} \end{cases}$$

(vi) For $\sigma \in (\Sigma_{1,o} \cap \Sigma_{3,o}) \setminus \Sigma_{2,o}$,

$$\delta^{M_e}((p_1, p_2, p_3, p_4, p_5), \sigma) = \begin{cases} (p_1, \delta^H(p_2, \sigma), p_3, p_4, p_5), \\ (\delta^H(p_1, \sigma), p_2, \delta^H(p_3, \sigma), \delta^H(p_4, \sigma), \delta^G(p_5, \sigma)), \\ (\delta^H(p_1, \sigma), \delta^H(p_2, \sigma), \delta^H(p_3, \sigma), \delta^H(p_4, \sigma), \delta^G(p_5, \sigma)), \\ (\Delta_1, \Delta_2, \Delta_3, p_4, p_5), \quad \text{if Condition (C0) holds.} \end{cases}$$

(vii) For $\sigma \in (\Sigma_{2,o} \cap \Sigma_{3,o}) \setminus \Sigma_{1,o}$,

$$\delta^{M_e}((p_1, p_2, p_3, p_4, p_5), \sigma) = \begin{cases} (\delta^H(p_1, \sigma), p_2, p_3, p_4, p_5), \\ (p_1, \delta^H(p_2, \sigma), \delta^H(p_3, \sigma), \delta^H(p_4, \sigma), \delta^G(p_5, \sigma)), \\ (\delta^H(p_1, \sigma), \delta^H(p_2, \sigma), \delta^H(p_3, \sigma), \delta^H(p_4, \sigma), \delta^G(p_5, \sigma)), \\ (\Delta_1, \Delta_2, \Delta_3, p_4, p_5), \quad \text{if Condition (C0) holds.} \end{cases}$$

(viii) For $\sigma \in (\Sigma_{1,o} \cap \Sigma_{2,o} \cap \Sigma_{3,o})$,

$$\delta^{M_e}((p_1, p_2, p_3, p_4, p_5), \sigma) = \begin{cases} (\delta^H(p_1, \sigma), \delta^H(p_2, \sigma), \delta^H(p_3, \sigma), \delta^H(p_4, \sigma), \delta^G(p_5, \sigma)), \\ (\Delta_1, \Delta_2, \Delta_3, p_4, p_5), \quad \text{if Condition (C0) holds.} \end{cases}$$

(ix) $\delta^{M_e}((p_1, p_2, p_3, p_4, p_5), \sigma)$ is undefined for any σ if $p_1 = f$ or $p_2 = f$ or $p_3 = f$.

The aim of constructing M_e is to trace all possible strings that could happen and have the same projection in the local supervisors, and check $i \in A_{s,\sigma}$. If $\delta^{M_e}(q_0^{M_e}, t) = q^{M_e}$ where $q^{M_e} = (p_1, \ldots, p_n, p_{n+1}, p_{n+2})$, then there are $s_1, \ldots, s_n, s \in \Sigma^*$ with $P_i(s) = P_i(s_i)$, where each s_i leads to p_i, s leads to p_{n+1} and p_{n+2} and $i \in I$. If both conditions (C0) and (Ci) are satisfied, then $\sigma \in \widetilde{\Sigma}_c \cap \Sigma_{c,e}$, and either $i \notin In(\sigma)$ or $s\sigma \in L(G) - L(H)$ and $s_i\sigma \in L(H)$, i.e., $i \notin A_{s,\sigma}$. So $i \notin A_{s,\sigma}$ is captured by conditions (C0) and (Ci), where $i \in I$.

Definition 10. For state $q^{M_e} = (p_1, \ldots, p_n, p_{n+1}, p_{n+2}) \in Q^{M_e}$, each p_i is a *component* of q^{M_e}. In particular, p_i is called an *f-component* of q^{M_e} if $p_i = f$, where $i \in I$. q^{M_e} is said to be *a j-f state of* M_e if there are j f-components in q^{M_e}, where $1 \le j \le n$.

Definition 11. *The marked state set of the* $\Sigma_{c,e}$*-discriminator* M_e is defined as

$$Q_m^{M_e} = \bigcup_{j=k}^{n} \left\{ q^{M_e} \in Q^{M_e} : q^{M_e} \text{ is a } j\text{-}f \text{ state} \right\}. \tag{9}$$

Definition 12. Given a specification automaton $H = (Q^H, \Sigma, \delta^H, q_0^H, Q_m^H)$ and a plant $G = (Q^G, \Sigma, \delta^G, q_0^G, Q_m^G)$ with n local supervisors. *The* $\Sigma_{c,d}$*-discriminator of k-reliable* $\widetilde{\Sigma}_c$*-coobservability* is defined as a nondeterministic automaton

$$M_d = (Q^{M_d}, \Sigma, \delta^{M_d}, q_0^{M_d}, Q_m^{M_d}), \tag{10}$$

where

(1) the state space

$$Q^{M_d} = \underbrace{Q^G \times (Q^H \cup \{f\}) \times \cdots \times Q^G \times (Q^H \cup \{f\})}_{2n} \times Q^H.$$

(2) The initial state is $q_0^{M_d} = (q_0^G, q_0^H, \ldots, q_0^G, q_0^H, q_0^H) \in Q^{M_d}$.

(3) The transition function $\delta^{M_d} : Q^{M_d} \times \Sigma \to 2^{Q^{M_d}}$ will be defined in Definition 13.

(4) The marked state set $Q_m^{M_d}$ will be defined in Definition 15.

Before defining δ^{M_d}, we give the following conditions: for $q^{M_d} = (p_1^G, p_1^H, \ldots, p_n^G, p_n^H, p_{n+1}^H) \in Q^{M_d}$ and $\sigma \in \widetilde{\Sigma}_c$, conditions (D1), ..., (Dn) and (D0) are defined as

Condition (Di): either $\sigma \notin \Sigma_{i,c}$ or $\delta^G(p_i^G, \sigma)$ and $\delta^H(p_{n+1}^H, \sigma)$ are defined but $\delta^H(p_i^H, \sigma)$ is undefined, where $i \in I$.

Condition (D0): $\sigma \in \widetilde{\Sigma}_c \cap \Sigma_{c,d}$ and at least one of the conditions (D1), ..., (Dn) holds.

Definition 13. The transition function of M_d is defined as a partial function $\delta^{M_d} : Q^{M_d} \times \Sigma \to 2^{Q^{M_d}}$, for $q^{M_d} = (p_1^G, p_1^H, \ldots, p_n^G, p_n^H, p_{n+1}^H) \in Q^{M_d}$ and $\sigma \in \Sigma$, $\delta^{M_d}(q^{M_d}, \sigma)$ is informally defined as all possible states. In particular, if Condition (D0) holds, then $\delta^{M_d}(q^{M_d}, \sigma) = (p_1^G, \Lambda_1, \ldots, p_n^G, \Lambda_n, p_{n+1}^H)$, where for each $i \in I$, $\Lambda_i = f$ if Condition (Di) holds; otherwise, $\Lambda_i = p_i^H$. For simplicity, we formally define δ^{M_d} for the case of three local supervisors (i.e., $n = 3$), which can be extended directly to the case of any finite number of local supervisors:

(i) For $\sigma \notin (\Sigma_{1,o} \cup \Sigma_{2,o} \cup \Sigma_{3,o})$,

$$\delta^{M_d}((p_1^G, p_1^H, p_2^G, p_2^H, p_3^G, p_3^H, p_4^H), \sigma) = \begin{cases} (\delta^G(p_1^G, \sigma), \delta^H(p_1^H, \sigma), p_2^G, p_2^H, p_3^G, p_3^H, p_4^H), \\ (p_1^G, p_1^H, \delta^G(p_2^G, \sigma), \delta^H(p_2^H, \sigma), p_3^G, p_3^H, p_4^H), \\ (p_1^G, p_1^H, p_2^G, p_2^H, \delta^G(p_3^G, \sigma), \delta^H(p_3^H, \sigma), p_4^H), \\ (p_1^G, p_1^H, p_2^G, p_2^H, p_3^G, p_3^H, \delta^H(p_4^H, \sigma)), \\ (\delta^G(p_1^G, \sigma), \delta^H(p_1^H, \sigma), \delta^G(p_2^G, \sigma), \delta^H(p_2^H, \sigma), \\ \quad \delta^G(p_3^G, \sigma), \delta^H(p_3^H, \sigma), \delta^H(p_4^H, \sigma)), \\ (p_1^G, \Lambda_1, p_2^G, \Lambda_2, p_3^G, \Lambda_3, p_4^H), \quad \text{if Condition (D0) holds.} \end{cases}$$

(ii) For $\sigma \in \Sigma_{1,o} \setminus (\Sigma_{2,o} \cup \Sigma_{3,o})$,

$$\delta^{M_d}((p_1^G, p_1^H, p_2^G, p_2^H, p_3^G, p_3^H, p_4^H), \sigma) = \begin{cases} (\delta^G(p_1^G, \sigma), \delta^H(p_1^H, \sigma), p_2^G, p_2^H, p_3^G, p_3^H, \delta^H(p_4^H, \sigma)), \\ (p_1^G, p_1^H, \delta^G(p_2^G, \sigma), \delta^H(p_2^H, \sigma), p_3^G, p_3^H, p_4^H), \\ (p_1^G, p_1^H, p_2^G, p_2^H, \delta^G(p_3^G, \sigma), \delta^H(p_3^H, \sigma), p_4^H), \\ (\delta^G(p_1^G, \sigma), \delta^H(p_1^H, \sigma), \delta^G(p_2^G, \sigma), \delta^H(p_2^H, \sigma), \\ \quad \delta^G(p_3^G, \sigma), \delta^H(p_3^H, \sigma), \delta^H(p_4^H, \sigma)), \\ (p_1^G, \Lambda_1, p_2^G, \Lambda_2, p_3^G, \Lambda_3, p_4^H), \quad \text{if Condition (D0) holds.} \end{cases}$$

(iii) For $\sigma \in \Sigma_{2,o} \setminus (\Sigma_{1,o} \cup \Sigma_{3,o})$,

$$\delta^{M_d}((p_1^G, p_1^H, p_2^G, p_2^H, p_3^G, p_3^H, p_4^H), \sigma) = \begin{cases} (\delta^G(p_1^G, \sigma), \delta^H(p_1^H, \sigma), p_2^G, p_2^H, p_3^G, p_3^H, p_4^H), \\ (p_1^G, p_1^H, \delta^G(p_2^G, \sigma), \delta^H(p_2^H, \sigma), p_3^G, p_3^H, \delta^H(p_4^H, \sigma)), \\ (p_1^G, p_1^H, p_2^G, p_2^H, \delta^G(p_3^G, \sigma), \delta^H(p_3^H, \sigma), p_4^H), \\ (\delta^G(p_1^G, \sigma), \delta^H(p_1^H, \sigma), \delta^G(p_2^G, \sigma), \delta^H(p_2^H, \sigma), \\ \quad \delta^G(p_3^G, \sigma), \delta^H(p_3^H, \sigma), \delta^H(p_4^H, \sigma)), \\ (p_1^G, \Lambda_1, p_2^G, \Lambda_2, p_3^G, \Lambda_3, p_4^H), \quad \text{if Condition (D0) holds.} \end{cases}$$

(iv) For $\sigma \in \Sigma_{3,o} \setminus (\Sigma_{1,o} \cup \Sigma_{2,o})$,

$$\delta^{M_d}((p_1^G, p_1^H, p_2^G, p_2^H, p_3^G, p_3^H, p_4^H), \sigma) = \begin{cases} (\delta^G(p_1^G, \sigma), \delta^H(p_1^H, \sigma), p_2^G, p_2^H, p_3^G, p_3^H, p_4^H), \\ (p_1^G, p_1^H, \delta^G(p_2^G, \sigma), \delta^H(p_2^H, \sigma), p_3^G, p_3^H, p_4^H), \\ (p_1^G, p_1^H, p_2^G, p_2^H, \delta^G(p_3^G, \sigma), \delta^H(p_3^H, \sigma), \delta^H(p_4^H, \sigma)), \\ (\delta^G(p_1^G, \sigma), \delta^H(p_1^H, \sigma), \delta^G(p_2^G, \sigma), \delta^H(p_2^H, \sigma), \\ \quad \delta^G(p_3^G, \sigma), \delta^H(p_3^H, \sigma), \delta^H(p_4^H, \sigma)), \\ (p_1^G, \Lambda_1, p_2^G, \Lambda_2, p_3^G, \Lambda_3, p_4^H), \quad \text{if Condition (D0) holds.} \end{cases}$$

(v) For $\sigma \in (\Sigma_{1,o} \cap \Sigma_{2,o}) \setminus \Sigma_{3,o}$,

$$\delta^{M_d}((p_1^G, p_1^H, p_2^G, p_2^H, p_3^G, p_3^H, p_4^H), \sigma) = \begin{cases} (\delta^G(p_1^G, \sigma), \delta^H(p_1^H, \sigma), \delta^G(p_2^G, \sigma), \delta^H(p_2^H, \sigma), \\ \quad p_3^G, p_3^H, \delta^H(p_4^H, \sigma)), \\ (p_1^G, p_1^H, p_2^G, p_2^H, \delta^G(p_3^G, \sigma), \delta^H(p_3^H, \sigma), p_4^H), \\ (\delta^G(p_1^G, \sigma), \delta^H(p_1^H, \sigma), \delta^G(p_2^G, \sigma), \delta^H(p_2^H, \sigma), \\ \quad \delta^G(p_3^G, \sigma), \delta^H(p_3^H, \sigma), \delta^H(p_4^H, \sigma)), \\ (p_1^G, \Lambda_1, p_2^G, \Lambda_2, p_3^G, \Lambda_3, p_4^H), \quad \text{if Condition (D0) holds.} \end{cases}$$

(vi) For $\sigma \in (\Sigma_{1,o} \cap \Sigma_{3,o}) \setminus \Sigma_{2,o}$,

$$\delta^{M_d}((p_1^G, p_1^H, p_2^G, p_2^H, p_3^G, p_3^H, p_4^H), \sigma) = \begin{cases} (\delta^G(p_1^G, \sigma), \delta^H(p_1^H, \sigma), p_2^G, p_2^H, \\ \quad \delta^G(p_3^G, \sigma), \delta^H(p_3^H, \sigma), \delta^H(p_4^H, \sigma)), \\ (p_1^G, p_1^H, \delta^G(p_2^G, \sigma), \delta^H(p_2^H, \sigma), p_3^G, p_3^H, p_4^H), \\ (\delta^G(p_1^G, \sigma), \delta^H(p_1^H, \sigma), \delta^G(p_2^G, \sigma), \delta^H(p_2^H, \sigma), \\ \quad \delta^G(p_3^G, \sigma), \delta^H(p_3^H, \sigma), \delta^H(p_4^H, \sigma)), \\ (p_1^G, \Lambda_1, p_2^G, \Lambda_2, p_3^G, \Lambda_3, p_4^H), \quad \text{if Condition (D0) holds.} \end{cases}$$

(vii) For $\sigma \in (\Sigma_{2,o} \cap \Sigma_{3,o}) \setminus \Sigma_{1,o}$,

$$\delta^{M_d}((p_1^G, p_1^H, p_2^G, p_2^H, p_3^G, p_3^H, p_4^H), \sigma) = \begin{cases} (\delta^G(p_1^G, \sigma), \delta^H(p_1^H, \sigma), p_2^G, p_2^H, p_3^G, p_3^H, p_4^H), \\ (p_1^G, p_1^H, \delta^G(p_2^G, \sigma), \delta^H(p_2^H, \sigma), \\ \quad \delta^G(p_3^G, \sigma), \delta^H(p_3^H, \sigma), \delta^H(p_4^H, \sigma)), \\ (\delta^G(p_1^G, \sigma), \delta^H(p_1^H, \sigma), \delta^G(p_2^G, \sigma), \delta^H(p_2^H, \sigma), \\ \quad \delta^G(p_3^G, \sigma), \delta^H(p_3^H, \sigma), \delta^H(p_4^H, \sigma)), \\ (p_1^G, \Lambda_1, p_2^G, \Lambda_2, p_3^G, \Lambda_3, p_4^H), \quad \text{if Condition (D0) holds.} \end{cases}$$

(viii) For $\sigma \in (\Sigma_{1,o} \cap \Sigma_{2,o} \cap \Sigma_{3,o})$,

$$\delta^{M_d}((p_1^G, p_1^H, p_2^G, p_2^H, p_3^G, p_3^H, p_4^H), \sigma) = \begin{cases} (\delta^G(p_1^G, \sigma), \delta^H(p_1^H, \sigma), \delta^G(p_2^G, \sigma), \delta^H(p_2^H, \sigma), \\ \quad \delta^G(p_3^G, \sigma), \delta^H(p_3^H, \sigma), \delta^H(p_4^H, \sigma)), \\ (p_1^G, \Lambda_1, p_2^G, \Lambda_2, p_3^G, \Lambda_3, p_4^H), \quad \text{if Condition (D0) holds.} \end{cases}$$

(ix) $\delta^{M_d}((p_1^G, p_1^H, p_2^G, p_2^H, p_3^G, p_3^H, p_4^H), \sigma)$ is undefined if $p_1^H = f$ or $p_2^H = f$ or $p_3^H = f$.

In M_d, if $q^{M_d} = (p_1^G, p_1^H, \ldots, p_n^G, p_n^H, p_{n+1}^H)$ and $\delta^{M_d}(q_0^{M_d}, t) = q^{M_d}$, then there are $s_1, \ldots, s_n, s \in \Sigma^*$ with $P_i(s) = P_i(s_i)$, where each s_i leads to p_i^G and p_i^H, s leads to p_{n+1}^H, and $i \in I$. If both conditions (D0) and (Di) are satisfied, then there is $\sigma \in \widetilde{\Sigma}_c \cap \Sigma_{c,d}$ and $s \in L(H)$ such that $i \notin A_{s,\sigma}$. So $i \notin A_{s,\sigma}$ is characterized by conditions (D0) and (Di) in this case, where $i \in I$.

Definition 14. For state $q^{M_d} = (p_1^G, p_1^H, \ldots, p_n^G, p_n^H, p_{n+1}^H)$, each p_i^H is a *component in H* of q^{M_d}. In particular, p_i^H is called *an f-component* if $p_i^H = f$, where $i \in I$; and q^{M_d} is *a j-f state of* M_d if there are j f-components in q^{M_d}, where $1 \le j \le n$.

Definition 15. *The marked state set of the $\Sigma_{c,d}$-discriminator M_d is* defined as

$$Q_m^{M_d} = \bigcup_{j=k}^{n} \left\{ q^{M_d} \in Q^{M_d} : q^{M_d} \text{ is a } j\text{-}f \text{ state} \right\}. \tag{11}$$

Proposition 2. (1) *Let $q^{M_e} = (p_1, \ldots, p_n, p_{n+1}, p_{n+2}) \in Q^{M_e}$. Assume that q^{M_e} is a j-f state of M_e whose ℓ_1th, …, ℓ_jth components are f-components, where $\ell_1, \ldots, \ell_j \in I$. Then there is $q'^{M_e} = (p'_1, \ldots, p'_n, p_{n+1}, p_{n+2}) \in Q^{M_e}$ without containing any f-component, and, there are $s_1, \ldots, s_n, s \in \Sigma^*$ and $\sigma \in \widetilde{\Sigma}_c \cap \Sigma_{c,e}$ satisfying $\delta^H(q_0^H, s) = p_{n+1}$, $\delta^G(q_0^G, s) = p_{n+2}$, and for each $i \in I$, $\delta^H(q_0^H, s_i) = p'_i$ and $P_i(s) = P_i(s_i)$. Moreover, for each ℓ_r, either $\sigma \notin \Sigma_{\ell_r,c}$ or $\delta^H(p'_{\ell_r}, \sigma)$ and $\delta^G(p_{n+2}, \sigma)$ are defined but $\delta^H(p_{n+1}, \sigma)$ is undefined, where $r = 1, \ldots, j$.*

(2) *Let $q_1^{M_d} = (p_{11}^G, p_{11}^H, \ldots, p_{1n}^G, p_{1n}^H, p_{n+1}^H) \in Q^{M_d}$. Assume that q^{M_d} is a j-f state of M_d whose ℓ_1th, …, ℓ_jth components are f-components, where $\ell_1, \ldots, \ell_j \in I$. Then there is $q_2^{M_d} = (p_{21}^G, p_{21}^H, \ldots, p_{2n}^G, p_{2n}^H, p_{n+1}^H) \in Q^{M_d}$ without containing any f-component, and, there are $s_1, \ldots, s_n, s \in \Sigma^*$ and $\sigma \in \widetilde{\Sigma}_c \cap \Sigma_{c,d}$ satisfying $\delta^H(q_0^H, s) = p_{n+1}^H$, and for each $i \in I$, $\delta^G(q_0^G, s_i) = p_{2i}^G$, $\delta^H(q_0^H, s_i) = p_{2i}^H$ and $P_i(s) = P_i(s_i)$. Moreover, for each ℓ_r, either $\sigma \notin \Sigma_{\ell_r,c}$ or $\delta^H(p_{n+1}^H, \sigma)$ and $\delta^G(p_{2\ell_r}^G, \sigma)$ are defined but $\delta^H(p_{2\ell_r}^H, \sigma)$ is undefined, where $r = 1, \ldots, j$.*

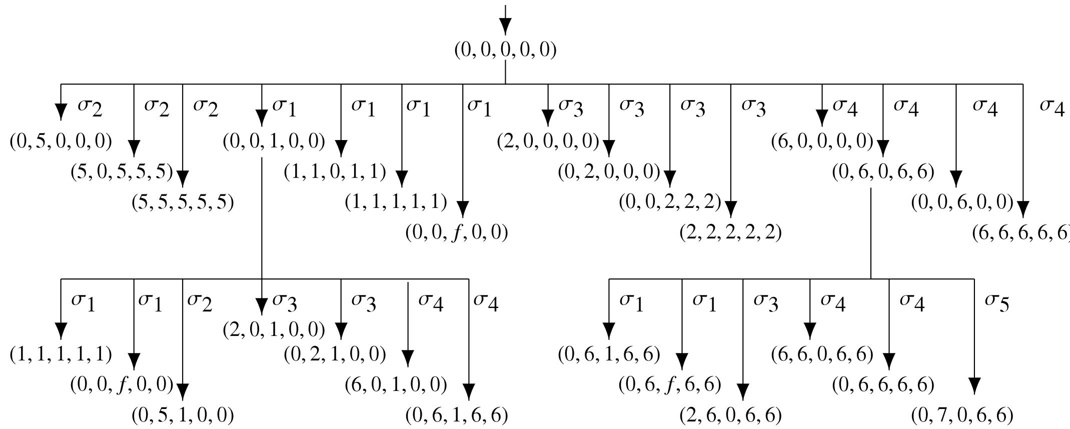


Fig. 1. $\Sigma_{c,e}$-discriminator of 2-reliable $\widetilde{\Sigma}_c$-coobservability M_e in Example 2.

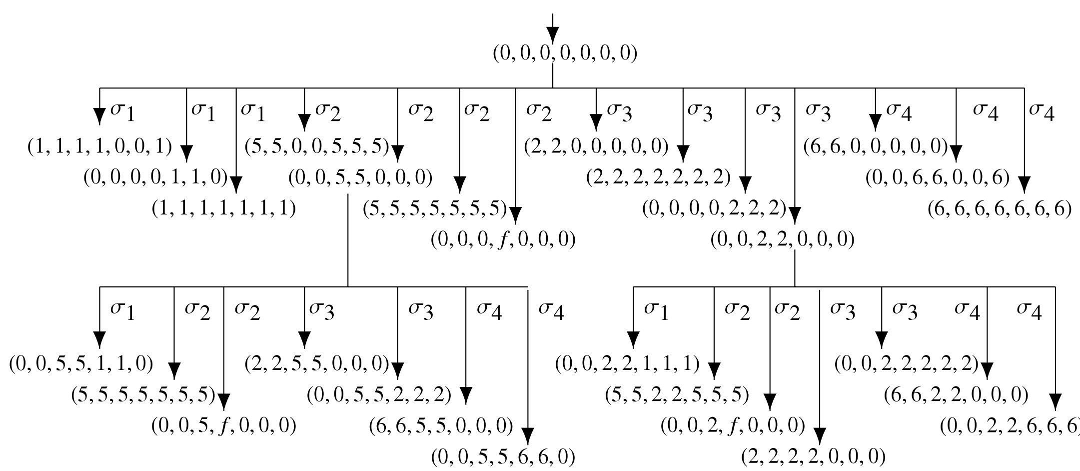


Fig. 2. $\Sigma_{c,d}$-discriminator of 2-reliable $\widetilde{\Sigma}_c$-coobservability M_d in Example 2.

Proof. (1) Denote $\delta^{M_e}(q_0^{M_e}, t) = q'^{M_e}$ and $\delta^{M_e}(q_0'^{M_e}, \sigma) = q^{M_e}$, where $t \in \Sigma^*$, $\sigma \in \Sigma$, and $q'^{M_e} = (p'_1, \ldots, p'_n, p_{n+1}, p_{n+2}) \in Q^{M_e}$. Since in M_e, no transition is defined in the states with f-components, q'^{M_e} does not contain any f-component. Let $\delta^H(q_0^H, s_i) = p'_i$ $(i \in I)$, $\delta^H(q_0^H, s) = p_{n+1}$, and $\delta^G(q_0^G, s) = p_{n+2}$. Then Definition 9(i)–(viii) guarantee $P_i(s) = P_i(s_i)$ for each $i \in I$. Due to the ℓ_1th, …, ℓ_jth components of q^{M_e} being f-components, Conditions (C0) and (Cℓ_1), …, (Cℓ_j) hold. That is, $\sigma \in \widetilde{\Sigma}_c \cap \Sigma_{c,e}$, and for each ℓ_r, either $\sigma \notin \Sigma_{\ell_r,c}$ or $\delta^H(p'_{\ell_r}, \sigma)$ and $\delta^G(p_{n+2}, \sigma)$ are defined but $\delta^H(p_{n+1}, \sigma)$ is undefined.

(2) It can be similarly proved according to Definition 13. □

Theorem 2. *$L_m(H)$ is k-reliably $\widetilde{\Sigma}_c$-coobservable if and only if $L_m(M_e) = L_m(M_d) = \emptyset$.*

Proof. ($\Rightarrow$) If $L_m(M_e) \neq \emptyset$, then there is a marked state in M_e, denoted as $q^{M_e} = (p_1, \ldots, p_n, p_{n+1}, p_{n+2})$. From Eq. (9), q^{M_e} must contain j f-components, where $k \leq j \leq n$. Without loss of generality, we denote the j f-components as $p_{\ell_1}, \ldots, p_{\ell_j}$, where $\ell_1, \ldots, \ell_j \in I$. By Proposition 2(1), there is $q'^{M_e} = (p'_1, \ldots, p'_n, p_{n+1}, p_{n+2}) \in Q^{M_e}$ without containing any f-component, and, there are $s_1, s_2, \ldots, s_n, s \in \Sigma^*$ and $\sigma \in \widetilde{\Sigma}_c \cap \Sigma_{c,e}$ such that $\delta^H(q_0^H, s) = p_{n+1}$, $\delta^G(q_0^G, s) = p_{n+2}$, and $\delta^H(q_0^H, s_i) = p'_i$, $P_i(s) = P_i(s_i)$ for each $i \in I$. Moreover, for each ℓ_r, either $\ell_r \notin In(\sigma)$ or $s_{\ell_r}\sigma \in L(H)$ and $s\sigma \in L(G)$ but $s\sigma \notin L(H)$. According to Eq. (6), $\ell_r \notin A_{s,\sigma}$ for all $r \in \{1, 2, \ldots, j\}$. Consequently, $|A_{s,\sigma}| \leq n - j \leq n - k$ due to $k \leq j \leq n$. By Definition 7, $L_m(H)$ is not k-reliably $\widetilde{\Sigma}_c$-coobservable.

If $L_m(M_d) \neq \emptyset$, then there is a marked state $q_1^{M_d} = (p_{11}^G, p_{11}^H, \ldots, p_{1n}^G, p_{1n}^H, p_{n+1}^H)$ in M_d. From Eq. (11), $q_1^{M_d}$ must contain j f-components, where $k \leq j \leq n$. Without loss of generality, we denote the j f-components as $p_{\ell_1}, \ldots, p_{\ell_j}$, where $\ell_1, \ldots, \ell_j \in I$. By Proposition 2(2), there is $q_2^{M_d} = (p_{21}^G, p_{21}^H, \ldots, p_{2n}^G, p_{2n}^H, p_{n+1}^H)$ without containing any f-component, and, there are $s_1, s_2, \ldots, s_n, s \in \Sigma^*$ and $\sigma \in \widetilde{\Sigma}_c \cap \Sigma_{c,d}$ such that $\delta^H(q_0^H, s) = p_{n+1}^H$, and $\delta^G(q_0^G, s_i) = p_{2i}^G$, $\delta^H(q_0^H, s_i) = p_{2i}^H$, $P_i(s) = P_i(s_i)$ for each $i \in I$. Moreover, for each ℓ_r, either $\ell_r \notin In(\sigma)$ or $s\sigma \in L(H)$, $s_{\ell_r}\sigma \in L(G)$ but $s_{\ell_r}\sigma \notin L(H)$. From Eq. (6), $\ell_r \notin A_{s,\sigma}$ for all $r \in \{1, 2, \ldots, j\}$. As a result, $|A_{s,\sigma}| \leq n - j \leq n - k$ due to $k \leq j \leq n$. By Definition 9, $L_m(H)$ is not k-reliably $\widetilde{\Sigma}_c$-coobservable.

($\Leftarrow$) If $L_m(H)$ is not k-reliably $\widetilde{\Sigma}_c$-coobservable, then by Definition 9, there are $s \in L(H)$ and $\sigma \in \widetilde{\Sigma}_c$ such that $|A_{s,\sigma}| \leq n - k$. If $\sigma \in \Sigma_{c,e}$, then $|A_{s,\sigma}| \leq n - k$ implies that there are $\ell_1, \ldots, \ell_k \in I - A_{s,\sigma}$. Thus, for each ℓ_j $(1 \leq j \leq k)$, either $\sigma \notin \Sigma_{\ell_j,c}$ or there is $s_{\ell_j} \in P_{\ell_j}^{-1}P_{\ell_j}(s)$ such that $s_{\ell_j}\sigma \in L(H)$ although $s\sigma \in L(G) - L(H)$. By Definition 9, there is a state in M_e where the ℓ_1th, …, ℓ_kth components are f-components. Therefore, $L_m(M_e) \neq \emptyset$. If $\sigma \in \Sigma_{c,d}$, then from $|A_{s,\sigma}| \leq n-k$, we know that there are $\ell_1, \ldots, \ell_k \in I - A_{s,\sigma}$. So for each ℓ_j $(1 \leq j \leq k)$, either $\sigma \notin \Sigma_{\ell_j,c}$ or there is $s_{\ell_j} \in P_{\ell_j}^{-1}P_{\ell_j}(s) \cap L(H)$ with $s_{\ell_j}\sigma \in L(G) - L(H)$ although $s\sigma \in L(H)$. Therefore, by Definition 13, there is a state in M_d where the ℓ_1th, …, ℓ_kth components are f-components. So $L_m(M_d) \neq \emptyset$. □

Remark 4. Theorem 2 shows that deciding the k-reliable $\widetilde{\Sigma}_c$-coobservability of $L_m(H)$ is equivalent to checking if $L_m(M_e)$ and

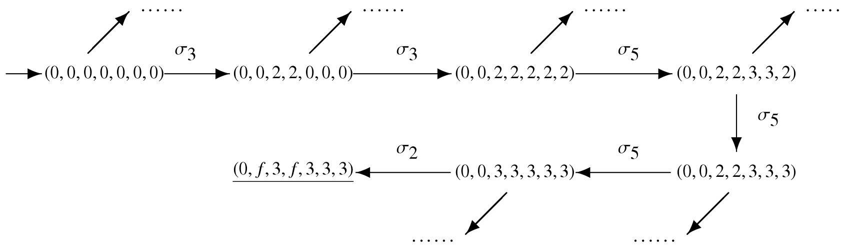


Fig. 3. $\Sigma_{c,d}$-discriminator of 2-reliable $\widetilde{\Sigma}_c$-coobservability M_d in Example 3.

$L_m(M_d)$ are empty. With a similar analysis of Theorem 3.1 in Rudie and Willems (1995), not only constructing M_e and M_d but also searching the paths from the initial state to the marked states (i.e., the strings in $L_m(M_e)$ and $L_m(M_d)$) can be done in polynomial time with respect to $|Q^G|$ and $|Q^H|$ for a fixed number of the local supervisors. Therefore, together with the aforementioned fact that the test of the $\widetilde{\Sigma}_{uc}$-controllability is polynomial, we can check the existence of a k-reliable decentralized supervisor in polynomial time with respect to $|Q^G|$ and $|Q^H|$.

In order to illustrate the approach proposed above, we provide an example.

Example 2. We consider the DES G and specification K given in Example 1. The sets of local observable and controllable events are the same as those of Example 1. In the following, we first verify the 2-reliable $\widetilde{\Sigma}_c$-coobservability of K by Theorem 2, and then prove that there is a 2-reliable decentralized supervisor.

According to Definitions 8 and 12, the $\Sigma_{c,e}$-discriminator M_e and the $\Sigma_{c,d}$-discriminator M_d of 2-reliable $\widetilde{\Sigma}_c$-coobservability are constructed as Figs. 1 and 2, respectively, in which for simplicity, only a part of M_e and a part of M_d are displayed. The 2-f and 3-f states are marked states of M_e and M_d.

Notice that there are no 2-f or 3-f states in M_e and M_d shown in Figs. 1 and 2, i.e., $L_m(M_e) = L_m(M_d) = \emptyset$. Consequently, by Theorem 2, we have the conclusion that K is 2-reliably $\widetilde{\Sigma}_c$-coobservable.

On the other side, K is $\widetilde{\Sigma}_{uc}$-controllable since $\overline{K}\widetilde{\Sigma}_{uc} \cap L(G) = \{\sigma_3, \sigma_4, \sigma_3\sigma_5, \sigma_4\sigma_5\} \subseteq \overline{K}$, where $\widetilde{\Sigma}_{uc} = \{\sigma_3, \sigma_4, \sigma_5\}$. By Theorem 1, we have the same result obtained in Example 1 that there is a 2-reliable decentralized supervisor. □

Example 3. We consider the same DES G and the same local observable and controllable event sets as those in Example 1, but the specification is changed into $K = \sigma_4\sigma_5 + \sigma_3\sigma_5\sigma_2$, then the $\Sigma_{c,d}$-discriminator M_d of 2-reliable $\widetilde{\Sigma}_c$-coobservability is constructed as Fig. 3, where for simplicity, only part of M_d is displayed. The 2-f and 3-f states are marked states of M_d.

Notice that there is a 2-f state $(0, f, 3, f, 3, 3, 3)$ in M_d (labeled by an underline in Fig. 3), i.e., $L_m(M_d) \neq \emptyset$. By Theorem 2, K is not 2-reliably $\widetilde{\Sigma}_c$-coobservable. So, there is no 2-reliable decentralized supervisor by Theorem 1. □

5. Conclusion

In this paper, the reliable decentralized supervisory control problem under the general architecture was addressed. A existence condition of reliable decentralized supervisors was proposed by using the notions of $\widetilde{\Sigma}_{uc}$-controllability and k-reliable $\widetilde{\Sigma}_c$-coobservability. We further presented a polynomial-time algorithm to verify the k-reliable $\widetilde{\Sigma}_c$-coobservability.

Based on these results, it is interesting to compute the supremal or infimal $\widetilde{\Sigma}_{uc}$-controllable and $\widetilde{\Sigma}_c$-coobservable sublanguage for a given specification language that is neither $\widetilde{\Sigma}_{uc}$-controllable nor k-reliably $\widetilde{\Sigma}_c$-coobservable. We will investigate this problem in subsequent work.

Acknowledgements

We thank Professor Ian Petersen, the Editor, the Associate Editor, and the reviewers for their invaluable comments that greatly helped us improve the quality of this paper.

References

Cassandras, C. G., & Lafortune, S. (1999). *Introduction to discrete event systems*. Boston, MA: Kluwer.

Kumar, R., & Takai, S. (2007). Inference-based ambiguity management in decentralized decision-making: decentralized control of discrete event systems. *IEEE Transactions on Automatic Control*, *52*(10), 1783–1794.

Liu, F., Qiu, D., Xing, H., & Fan, Z. (2008). Decentralized diagnosis of stochastic discrete event systems. *IEEE Transactions on Automatic Control*, *53*(2), 535–546.

Liu, F., & Lin, H. (2009). Reliable decentralized supervisory control of discrete event systems with communication delays. In: *Proc. 2009 IEEE/ASME conference on advanced intelligent mechatronics*, Singapore, July 14–17.

Liu, F., & Lin, H. (2009). A General architecture for reliable decentralized supervisory control of discrete event systems. In: *Proc. joint 48th IEEE conference on decision and control and 28th Chinese control conference*, Shanghai, China, December 16–18.

Park, S. J., & Cho, K. H. (2007). Decentralized supervisory control of discrete event systems with communication delays based on conjunctive and permissive decision structures. *Automatia*, *43*, 738–743.

Rohloff, K., & Lafortune, S. (2003). On the synthesis of safe control policies in decentralized control of discrete event systems. *IEEE Transactions on Automatic Control*, *48*(6), 1064–1068.

Rudie, K., & Willems, J. (1995). The computational complexity of decentralized discrete-event control problems. *IEEE Transactions on Automatic Control*, *40*(7), 1313–1319.

Takai, S., & Ushio, T. (2000). Reliable decentralized supervisory control of discrete event systems. *IEEE Transactions on Systems, Man and Cybernetics, Part B (Cybernetics)*, *30*(5), 661–667.

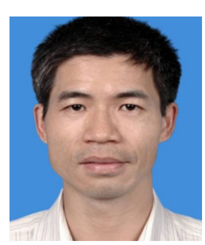
Takai, S., & Ushio, T. (2003a). Reliable decentralized supervisory control for marked language specifications. *Asian Journal of Control*, *5*(1), 160–167.

Takai, S., & Ushio, T. (2003b). Reliable decentralized supervisory control of discrete event systems with the conjunctive and disjunctive fusion rules. In: *Proc. 2003 Amer. contr. conf.*, June 2003 (pp. 1050–1055).

Yoo, T.-S., & Lafortune, S. (2002). A general architecture for decentralized supervisory control of discrete-event systems. *Discrete Event Dynamic Systems: Theory and Applications*, *12*(3), 335–377.

Yoo, T.-S., & Lafortune, S. (2004). Decentralized supervisory control with conditional decisions: Supervisor existence. *IEEE Transactions on Automatic Control*, *49*(11), 1886–1904.

Zhang, H., Guan, Z., & Feng, G. (2008). Reliable dissipative control for stochastic impulsive systems. *Automatica*, *44*(4), 1004–1010.



Fuchun Liu received the B.S. and M.S. degrees in mathematics from Jiangxi Normal University, China in 1994 and 1997, respectively. He was awarded the Ph.D. degree in Engineering from Sun Yat-Sen University, Guangzhou, China in 2008. He has been an associate professor at Faculty of Computer, Guangdong University of Technology, Guangzhou, China since 2005. He worked as a research fellow at National University of Singapore starting from 2009. His research interests include supervisory control and failure diagnosis for discrete event systems, mathematical logic, fuzzy systems, and rough set theory.

Hai Lin is currently an assistant professor in the National University of Singapore, Electrical and Computer Engineering Department. He received the B.S. degree from University of Science and Technology, Beijing, China in 1997, the M.Eng. degree from Chinese Academy of Science, China in 2000, and the Ph.D. degree from the University of Notre Dame, USA in 2005. He has been the chair of the IEEE SMC Singapore Chapter since 2009, and serves in several editorial board and conference organizing committee. His research interests are in the multidisciplinary study of the problems at the intersection of control, communication, computation and life sciences. His current research thrust is on hybrid control systems, multi-robot coordination and systems biology.