SCIENCE CHINA
Information Sciences

• RESEARCH PAPER •

January 2025, Vol. 68, Iss. 1, 112207:1–112207:20
https://doi.org/10.1007/s11432-023-4108-8

# Decentralized fault diagnosis of discrete-event systems with unreliable sensors using linear temporal logic

Weijie DONG, Shaoyuan LI & Xiang YIN*

*Key Laboratory of System Control and Information Processing, Ministry of Education, Department of Automation, Shanghai Jiao Tong University, Shanghai 200240, China*

Received 3 November 2023/Revised 13 March 2024/Accepted 10 July 2024/Published online 26 December 2024

**Abstract** In this paper, we investigate a decentralized diagnosis problem of a discrete-event system (DES) subject to unreliable sensors, where the sensor observations of local diagnosers may be non-deterministic as a result of possible failures. Existing studies on decentralized robust diagnosis can only deal with different types of sensor failures separately, e.g., all sensors suffer from the same type of sensor failures such as intermittent sensor failures or permanent sensor failures. However, since sensors of different local diagnosers may face different external environments and have different internal characteristics, sensors corresponding to different local diagnosers may also have their own fault features. In this paper, we propose a flexible framework of decentralized diagnosis for DES subject to unreliable sensors such that sensors of different local diagnosers are permitted to have different types of sensor failures. To this end, we extend the existing decentralized diagnosis framework to the case where there exist common sensors broadcasting their observations to all local diagnosers. We apply linear temporal logic (LTL) to constrain infinite behaviors of private sensors of local diagnosers and common sensors. Then, a new notion of $\varphi$-codiagnosability is proposed as the necessary and sufficient condition for the existence of a decentralized diagnoser that works correctly under sensors satisfying LTL-based sensor constraints. Finally, we provide an effective approach to verify the $\varphi$-codiagnosability.

**Keywords** discrete event systems, decentralized diagnosis, codiagnosability, automata

**Citation** Dong W J, Li S Y, Yin X. Decentralized fault diagnosis of discrete-event systems with unreliable sensors using linear temporal logic. Sci China Inf Sci, 2025, 68(1): 112207, https://doi.org/10.1007/s11432-023-4108-8

## 1 Introduction

### 1.1 Backgrounds and motivations

Large-scale cyber physical systems (CPS), such as intelligent transportation systems and flexible manufacturing systems are widely used and safety-critical infrastructures in modern society. They contain millions of concurrent components and intricate operation logic, which make failures volunteer to occur but are too stealthy to detect. Therefore, fault diagnosis is a crucial but challenging task to ensure the security of safety-critical CPS.

In this paper, we investigate the fault diagnosis problem in the context of discrete-event systems (DES). DES is a class of systems with event-triggered discrete dynamic to model high-level logical behaviors of CPS [1]. The research of model-based fault diagnosis applying DES was initialed by [2,3] where the notion of diagnosability was proposed and a system is said to be diagnosable if the occurrence of a fault can always be alarmed within a uniform bound based on partial observations. In the past two decades, fault diagnosis of DES has been extensively developed; see, e.g., some recent studies [4–14], comprehensive survey paper [15,16] and textbook [17].

For many large-scale networked systems, since it may be impossible or very costly to access all observations at a central site, several local stations observe their own local information with different capacities. Therefore, we need to develop diagnosis methodologies for decentralized information architecture. To this end, the decentralized diagnosis of DES was investigated in the seminal paper [18]. Then Refs. [19,20] considered the protocol 3 in [18] and proposed the notion of codiagnosability. It assumed that there

* Corresponding author (email: yinxiang@sjtu.edu.cn)

 

are distributed local diagnosers observing system behaviors from different sites under different sensing capacities and these local diagnosers do not communicate with each other. Then each local diagnoser processes the observed data and sends the diagnostic decision to the coordinator which issues a global diagnostic decision using the local information received. A system is codiagnosable if each fault can always be alarmed by at least one local diagnoser. Following the decentralized scheme, decentralized fault diagnosis has been studied by many studies in the DES literature [21–25].

For models of DES, every event is essentially observed by corresponding sensors. However, the observations of sensors are unreliable in real-world systems because of external noise and communication losses, or internal malfunction. As a result, the observations of events that are supposed to be correct may be missing or wrong in actual circumstances. Thus, taking into consideration the unreliable sensors is necessary to analyze diagnosis problem for real systems.

### 1.2 Literature review on decentralized diagnosis with unreliable sensors

Fault diagnosis of DES subject to unreliable sensors has been intensively studied. In [26], intermittent sensor failures were considered in the centralized diagnosis of DES, where some observable events may become unobservable or recover non-deterministically. Intermittent sensor failures can also be modeled by non-deterministic observations in [27], where Mealy automata with non-deterministic observation function were proposed to model possible observations of the same transition. Then, intermittent sensor failures were considered in decentralized diagnosis for networked DES scheme in [28] where the corresponding notion of codiagnosability was proposed.

In addition, centralized fault diagnosis subject to permanent sensor failures was first studied in [29] where once a sensor fails to observe an event, it will never recover, and it was assumed that every permanent sensor failure can only happen before the first occurrence of the corresponding event. Then decentralized diagnosis for systems subject to permanent sensor failures was investigated in [30]. In [31], centralized diagnosability for systems subject to permanent sensor failures without the above assumption was investigated, which was extended to a disjunctive decentralized diagnosis scheme subject to permanent sensor failures in [32]. In the context of networked DES, failures of communication of sensor have been also investigated and modeled by sensor failures. In [33], $K$-loss sensor failures were considered in the decentralized diagnosis problem, where the communication of sensors was assumed to lose observations only a bounded number of times in a row.

Note that the above approaches only considered individual sensor failure type in each verification procedure. Recently, researchers attempted to unify notions of diagnosability for systems subject to sensor failures. In [34], authors have shown that diagnosability for systems subject to both intermittent and permanent sensor failures can be reduced to the notion of general robust diagnosability [35]. However, different sensors of real systems may have different types of sensor failures. To deal with this situation, in [36], authors proposed a general robust diagnosis framework by modeling the failure mode switching dynamics of sensors into automata, which supports the uniform consideration of different fault types for different sensors. However, the automata that model the sensor observation dynamics are manually designed, which cannot deal with complex and large-scale sensor dynamics. Then, in our previous work [37], we developed a uniform framework for diagnosability analysis of DES subject to unreliable sensors in a centralized observation framework, where linear temporal logic (LTL) was used as a general and user-friendly tool to model unreliable sensors without restricting to specific sensor types.

### 1.3 Our approach and contributions

In the aforementioned studies of decentralized diagnosis for DES subject to unreliable sensors, it is assumed that all the sensors of different local diagnosers can only have the same type of sensor failures. For example, we cannot deal with the case where sensors of one local diagnoser have intermittent sensor failures while sensors of the other local diagnoser have permanent sensor failures. However, in practice, since different local diagnosers observe the system at different sites which may contain different environment conditions and sensors of different local diagnosers have different internal characteristics, sensors of different local diagnosers may have different types of failures. On the other hand, for some crucial events, there may exist common sensors which are dedicated to observing these events and will broadcast their observations to all local diagnosers. However, the existing decentralized diagnosis frameworks cannot analyze codiagnosability with the existence of these common sensors.

Motivated by the above gaps, in this paper, we propose a uniform framework of decentralized diagnosis of DES subject to common sensors and sensor failures. Specifically, we first use Mealy automata with non-deterministic output functions introduced in [27,38] to describe the unconstrained observation space for each local diagnoser. Then, we apply the LTL formula $\varphi_i$ as a modular tool to model how sensors of the $i$th local diagnoser and common sensors should behave in unconstrained observation space, which is dependent on the type of sensor failures. By taking all LTL-based sensor constraints of sensors belonged to each local diagnosers and common sensors into consideration, we propose a new codiagnosability, called $\varphi$-codiagnosability, which serves as a necessary and sufficient condition for the existence of a decentralized diagnoser working correctly under the LTL-based sensor constraints. Finally, we provide an effective procedure for $\varphi$-codiagnosability verification. The complexity of our method is exponential in the length of the sensor constraint formula $\varphi_i$ and the number of local diagnosers, but is only polynomial in the size of the system model.

It is worth noting that analysis of fault diagnosis for DES with assistance of LTL has been investigated in [13, 37, 39–42]. Specifically, in [39, 40], system specification was modeled by LTL formulae and faults of the system were defined as the executions violating this specification. In [13, 41, 42], verification of diagnosability was reduced to an LTL model checking problem. However, different from all the above studies, we apply LTL formulae to specify sensor constraints for sensors of different local diagnosers and common sensors in the context of decentralized diagnosis problem. In [37], an LTL-based uniform framework for the diagnosis of DES subject to unreliable sensors was proposed in a centralized observation framework. In this paper, we extend the results in [37] from a centralized observation scheme to a novel decentralized observation scheme with common sensors and we not only consider the different sensor capacities of different local diagnosers, but also deal with the synchronization of observations of common events observed by common sensors for all local diagnosers.

### 1.4 Organizations

The rest of the paper is organized as follows. Section 2 presents necessary preliminaries of decentralized diagnosis for DES and LTL semantics. In Section 3, we illustrate how to formalize LTL-based sensor constraints for unreliable private sensors of local diagnosers and common sensors. In Section 4, the notion of $\varphi$-codiagnosability is introduced, which is proved to be the necessary and sufficient condition for the existence of a decentralized diagnoser working correctly under LTL-based sensor constraints. In Section 5, we present an effective verification procedure of $\varphi$-codiagnosability. Finally, we conclude the paper in Section 6.

## 2 Preliminaries

### 2.1 Partially-observed discrete event systems

Let $\Sigma$ be a finite set. A sequence $s = \sigma_1\sigma_2\cdots\sigma_n(\cdots)$ is a finite (infinite) string over $\Sigma$ if $\sigma_i \in \Sigma, i = 1, 2, \ldots,$ and $s[j] = \sigma_j$ denotes the $j$th element of $s$. $\Sigma^*$ denotes the set of finite strings over $\Sigma$ with empty string $\epsilon$ and $\Sigma^\omega$ denotes the set of infinite strings over $\Sigma$. We write the union of finite and infinite strings as $\Sigma^+ = \Sigma^* \cup \Sigma^\omega$. For a finite string $s \in \Sigma^*$, $|s|$ is its length, which is the number of components in it, and $|\epsilon| = 0$. For an infinite string $s \in \Sigma^\omega$, $\mathsf{Inf}(s)$ is the set of all components appearing the infinite number of times in $s$. A $*$-language $L \subseteq \Sigma^*$ is a set of finite strings and an $\omega$-language $L \subseteq \Sigma^\omega$ is a set of infinite strings. For any $*$-language $L \subseteq \Sigma^*$, $\overline{L} = \{s \in \Sigma^* : \exists t \in \Sigma^* \text{ s.t. } st \in L\}$ denotes its prefix closure. For any $\omega$-language $L \subseteq \Sigma^\omega$, $\overline{L} = \{s \in \Sigma^* : \exists t \in \Sigma^\omega \text{ s.t. } st \in L\}$ denotes its prefix closure.

In this work, we model the DES by a deterministic finite-state automaton

$$G = (Q, \Sigma, \delta, q_0),$$

where $Q$ is a finite set of states, $\Sigma$ is a finite events set, $q_0 \in Q$ is the initial state and $\delta : Q \times \Sigma \to Q$ is the partial transition function, where for any $q, q' \in Q$ and $\sigma \in \Sigma$, $\delta(q, \sigma) = q'$ means that there exists a transition from state $q$ to $q'$ labeled by $\sigma$. Function $\delta$ is also extended to $\delta : Q \times \Sigma^* \to Q$ recursively by: for any $q \in Q, s \in \Sigma^*$ and $\sigma \in \Sigma$, we have $\delta(q, \epsilon) = q$ and $\delta(q, s\sigma) = \delta(\delta(q, s), \sigma)$. The $*$-language generated by $G$ is $\mathcal{L}(G) = \{s \in \Sigma^* : \delta(q_0, s)!\}$, where "!" means "is defined" and the $\omega$-language generated by $G$ is $\mathcal{L}^\omega(G) = \{s \in \Sigma^\omega : \forall s' \in \overline{\{s\}}, \delta(q_0, s')!\}$. We write $\mathcal{L}^+(G) = \mathcal{L}(G) \cup \mathcal{L}^\omega(G)$. We make a common assumption that system $G$ is live, i.e., for any $q \in Q$, there exists $\sigma \in \Sigma$ such that $\delta(q, \sigma)!$.

For partially-observed DES, the occurrence of events cannot be observed perfectly. The limited observation capability is modeled by an observation mask [1] $P : \Sigma \to \Delta\dot{\cup}\{\epsilon\}$ where $\Delta$ is a set of observation symbols. For an event $\sigma \in \Sigma$, if $P(\sigma) \in \Delta$, then it is observable; otherwise, it is unobservable. The observation mask can also be extended to $P : \Sigma^+ \to \Delta^+$ recursively as usual manner. In the decentralized observation setting, we assume that there are $\boldsymbol{\kappa}$ local diagnosers and $I = \{1, \ldots, \boldsymbol{\kappa}\}$ denotes the index set of local diagnosers. For the local diagnoser $D_i, i \in I$, its local observation symbolic set is denoted by $\Delta_i$. The local observation mask associated with $D_i$ is defined by

$$P_i : \Sigma \to \Delta_i\dot{\cup}\{\epsilon\}. \tag{1}$$

### 2.2 Decentralized observation under unreliable sensors

For real-world plants, sensors are unreliable and the observation of an event may be non-deterministic due to uncertainties. However, the local observation mask in (1) can only capture observations of reliable sensors where for each local diagnoser $D_i, i \in I$, the output of an event $\sigma \in \Sigma$ is always fixed, i.e., $P_i(\sigma)$. To model non-deterministic observations of unreliable sensors for each local diagnoser, we define the local state-dependent non-deterministic observation mapping [27,38] for the local diagnoser $D_i, i \in I$ by

$$\mathcal{O}_i : Q \times \Sigma \to 2^{\Delta_i \cup \{\epsilon\}}. \tag{2}$$

Intuitively, for any state $q \in Q$ and event $\sigma \in \Sigma$, $\mathcal{O}_i(q, \sigma)$ represents the set of possible observations may be obtained by diagnoser $D_i$ whenever event $\sigma$ occurs at state $q$. The local observation mapping $\mathcal{O}_i$ for $D_i, i \in I$, can also be extended to $\mathcal{O}_i : Q \times \Sigma^+ \to 2^{\Delta_i^+}$ in the following manner: for any state $q \in Q$ and event string $s = \sigma_1\sigma_2 \cdots \in \Sigma^+$, we have observation $o_1o_2 \cdots \in \mathcal{O}_i(q, s)$ for diagnoser $D_i, i \in I$, if

$$\forall j = 1, 2, \ldots, o_j \in \mathcal{O}_i(\delta(q, \sigma_1 \cdots \sigma_{j-1}), \sigma_j),$$

where $\sigma_0 = \epsilon$. For the sake of brevity, if state $q$ is the initial state, i.e., $q = q_0$, then we write $\mathcal{O}_i(s)$ to denote $\mathcal{O}_i(q, s)$. Given an event string $s \in \Sigma^+$, we say each string in $\mathcal{O}_i(s)$ is an observation realization of $s$ for local diagnoser $D_i, i \in I$.

**Example 1.** Let us consider system $G$ shown in Figure 1, where $\Sigma = \{a, b, c, d, e, f\}$, $\Delta_1 = \Delta_2 = \{o_1, o_2, o_3, o_4\}$. There are two local diagnosers, i.e., $I = \{1, 2\}$, and each local observation mapping is denoted by the label attached to each transition. For example, $b\backslash\{\epsilon\}\backslash\{o_2, \epsilon\}$ for transition $1 \xrightarrow{b} 2$ represents that (i) with the occurrence of event $b$, the system moves from state 1 to state 2, i.e., $\delta(1, b) = 2$; (ii) the local diagnoser $D_1$ always observes nothing, i.e., $\mathcal{O}_1(1, b) = \{\epsilon\}$; and (iii) the local diagnoser $D_2$ may observe either $o_2$ or nothing, i.e., $\mathcal{O}_2(1, b) = \{o_2, \epsilon\}$. For the finite string $s = bc \in \mathcal{L}(G)$, the observation realization for $D_1$ and $D_2$ are $\mathcal{O}_1(s) = \{o_2, \epsilon\}$ and $\mathcal{O}_2(s) = \{o_2, o_1, o_2o_1, \epsilon\}$, respectively.

**Remark 1.** The local non-deterministic observation mapping is general and can represent many observation models in the literature. For example, consider the standard projection in a decentralized observation setting. For the local diagnoser $D_i, i \in I$, we assume that $\Sigma_o^i \subseteq \Sigma$ is the set of observable events and $\Delta_i = \Sigma_o^i$ is its local observation set. Then, the local non-deterministic observation mapping $\mathcal{O}_i$ can be defined by $\mathcal{O}_i(q, \sigma) = \{\sigma\}$ for all $\sigma \in \Sigma_o^i$ and $\mathcal{O}_i(q, \sigma) = \{\epsilon\}$ for all $\sigma \notin \Sigma_o^i$. Furthermore, intermittent sensor failures, which assume the observations of some sensors may be lost intermittently [43,44], can also be captured by non-deterministic observation mapping. Specifically, in this setting, the event set is partitioned into three disjoint parts for each diagnoser $D_i, i \in I$: $\Sigma = \Sigma_r^i\dot{\cup}\Sigma_{\text{ur}}^i\dot{\cup}\Sigma_{\text{uo}}^i$, where $\Sigma_r^i$ contains reliable events such that their occurrence can always be accurately observed by sensors of $D_i$, $\Sigma_{\text{ur}}^i$ is the set of unreliable events such that their occurrence may be observed or lost by sensors of $D_i$ and $\Sigma_{\text{uo}}^i$ contains unobservable events that can never be observed by sensors of $D_i$. To capture this setting by non-deterministic observation mapping, we assume that $\Delta_i = \Sigma_r^i \cup \Sigma_{\text{ur}}^i$ and for any $q \in Q$ and $\sigma \in \Sigma$, $\mathcal{O}_i$ is defined by

$$\mathcal{O}_i(q, \sigma) = \begin{cases} \{\sigma\}, & \text{if } \sigma \in \Sigma_r^i, \\ \{\sigma, \varepsilon\}, & \text{if } \sigma \in \Sigma_{\text{ur}}^i, \\ \{\varepsilon\}, & \text{if } \sigma \in \Sigma_{\text{uo}}^i. \end{cases} \tag{3}$$

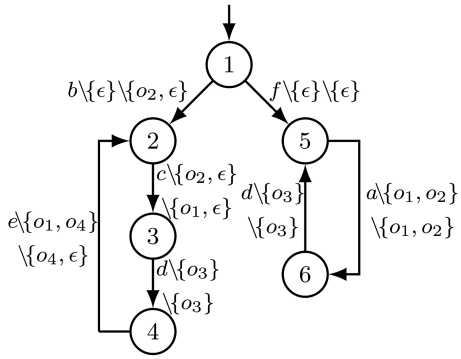


**Figure 1** System $G$.

### 2.3 Decentralized fault diagnosis

In the context of fault diagnosis, we assume there are failures in the system, which are modeled by a set of fault events $\Sigma_F \subset \Sigma$. In this paper, we only consider a single type of fault for the sake of simplicity. A string $s \in \Sigma^+$ is said to be faulty if there is a fault event $\sigma \in \Sigma_F$ in $s$, and we write as $\Sigma_F \in s$ with a slight abuse of notation; otherwise, we say string $s$ is normal. We use $\mathcal{L}_F(G) = \{s \in \mathcal{L}(G) : \Sigma_F \in s\}$ and $\mathcal{L}_F^\omega(G) = \{s \in \mathcal{L}^\omega(G) : \Sigma_F \in s\}$ to denote the sets of all finite and infinite faulty strings generated by $G$, respectively. We define

$$\Psi(G) = \{s \in \mathcal{L}_F(G) : \forall t \in \overline{\{s\}} \setminus \{s\}, \Sigma_F \notin t\}$$

as the set of faulty strings where fault events occur for the first time. Codiagnosability (with nondeterministic observations) [27] is defined as follows.

**Definition 1** (Codiagnosability)**.** System $G$ is said to be codiagnosable w.r.t. mapping $\mathcal{O}_i, i \in I$ and fault events $\Sigma_F$, if

$$(\exists n \in \mathbb{N})(\forall s \in \Psi(G))(\forall st \in \mathcal{L}(G))[|t| \geqslant n \Rightarrow \mathsf{codiag}],$$

where the diagnostic condition codiag is

$$(\exists i \in I)(\forall v \in \mathcal{L}(G))[\mathcal{O}_i(v) \cap \mathcal{O}_i(st) \neq \emptyset \Rightarrow \Sigma_F \in v].$$

Intuitively, the above definition says that a system is codiagnosable if the occurrence of faulty events can always be detected in a bounded number of steps by at least one local diagnoser.

**Example 2.** Consider system $G$ depicted in Figure 1 where the fault event set is $\Sigma_F = \{f\}$. For faulty string $s = f \in \Psi(G)$, it can be extended to an arbitrary long faulty string $s_F = f(da)^n, n \in \mathbb{N}$. The observations of $s_F$ for local diagnoser $D_1$ and $D_2$ are $\mathcal{O}_1(s_F) = \mathcal{O}_2(s_F) = \{[(o_1 + o_2)o_3]^n\}$. However, there is a normal string $v = b(cde)^n$ such that the observation of $v$ for the first local diagnoser satisfies $\mathcal{O}_1(v) \cap \mathcal{O}_1(s_F) = \{o_2o_3(o_1o_3)^{n-1}\}$ and the observation of $v$ for the second local diagnoser satisfies $\mathcal{O}_2(v) \cap \mathcal{O}_2(s_F) = \{(o_1o_3)^n\}$. Therefore, system $G$ is not codiagnosable with respect to $\mathcal{O}_1, \mathcal{O}_2$ and $\Sigma_F$.

### 2.4 Linear temporal logic

Let $\mathcal{AP}$ be a finite set of atomic propositions. An LTL formula is built on atomic propositions, Boolean operators and temporal operators based on the following grammar:

$$\varphi ::= \top \mid p \mid \neg\varphi \mid \varphi_1 \wedge \varphi_2 \mid \bigcirc\varphi \mid \varphi_1 U \varphi_2,$$

where $\top$ denotes `true`, $p \in \mathcal{AP}$ is an atomic proposition, $\neg$ and $\wedge$ represent logical negation and conjunction, while $\bigcirc$ and $U$ denote temporal operators "next" and "until", respectively. The temporal operators $\Diamond$ ("eventually") and $\Box$ ("always") can be induced by above operators: $\Diamond\varphi = \top U \varphi$ and $\Box\varphi = \neg\Diamond\neg\varphi$.

LTL formulae are used to describe temporal properties of infinite words, where an infinite word is an infinite string over the set $2^{\mathcal{AP}}$. For an infinite word $s \in (2^{\mathcal{AP}})^\omega$, $s \models \varphi$ denotes that the word $s$ satisfies LTL formula $\varphi$. We define the set of all words satisfying LTL formula $\varphi$ by $\mathsf{word}(\varphi) = \{s \in (2^{\mathcal{AP}})^\omega : s \models$

$\varphi\}$. The reader is referred to [45] for more details about the semantics of LTL, which are omitted here for the sake of brevity.

To structurally represent all words satisfying an LTL formula, a common tool is the non-deterministic Büchi automaton (NBA), defined as follows.

**Definition 2** (NBA)**.** An NBA is a 5-tupe $\mathcal{B} = (X, X_0, \Sigma_B, \xi, \mathcal{F})$, where $X$ is a finite set of states, $X_0 \subseteq X$ is a finite set of initial states, $\Sigma_B$ is a finite alphabet, $\xi : X \times \Sigma_B \to 2^X$ is a non-deterministic transition function and $\mathcal{F} \subseteq X$ is the set of accepting states.

For an infinite string $s = \sigma_1\sigma_2 \cdots \in {\Sigma_B}^\omega$, an infinite state sequence $\gamma = x_0x_1 \cdots \in X^\omega$ is induced by $s$ if $x_0 \in X_0$ and for any $i = 0, 1, \ldots$, we have $x_{i+1} = \xi(x_i, \sigma_{i+1})$. An infinite state sequence $\gamma \in X^\omega$ is accepted by an NBA $\mathcal{B}$ if it visits accepting states $\mathcal{F}$ for infinite number of times, i.e., $\mathsf{Inf}(\gamma) \cap \mathcal{F} \neq \emptyset$, and we say an infinite string $s$ is accepted by $\mathcal{B}$ if it induces an accepted state sequence. $\mathcal{L}^\omega_m(\mathcal{B})$ denotes the set of all infinite strings accepted by $\mathcal{B}$.

For any LTL formula $\varphi$, we can translate it into an NAB $\mathcal{B}$ with $\Sigma_B = 2^{\mathcal{AP}}$ whose accepting strings is equivalent to the strings satisfying $\varphi$ [45], i.e., $\mathcal{L}^\omega_m(\mathcal{B}) = \mathsf{word}(\varphi)$. We say this NBA $\mathcal{B}$ is associated with $\varphi$. There are well-known tools to calculate this translation such as LTL2BA [46].

## 3 LTL-based constraints of unreliable sensors

### 3.1 Motivation example

In the previous section, the non-deterministic observation mapping under decentralized observation structure $\mathcal{O}_i : Q \times \Sigma \to 2^{\Delta_i \cup \{\epsilon\}}$ essentially captures the possible decentralized observation space in the worst observation case. However, some observation realizations may be infeasible in practice when we have more prior information about sensor failures. For example, we consider the scenario of permanent sensor failures under a decentralized observation setting, where once a sensor fails, it will never repair. For system $G$ in Figure 1, as we discussed in Example 1, there are two local diagnosers. We focus on the first local diagnoser $D_1$ and assume that the sensor of event $c$ has permanent failures, that is, once it fails to observe event $c$, it will never observe event $c$ successfully forever. In this case, for the event string $s = bcdec$, its observation realization $o_3o_1o_2 \in \mathcal{O}_1(s)$ in the non-deterministic mapping is no longer feasible, since the sensor of event $c$ has already failed to observe $o_2$ when $c$ occurs at the first time and it is not possible to observe event $c$ thereafter. Thus, the non-deterministic mapping cannot deal with such a simple scenario of permanent sensor failures. Several approaches have been proposed in the literature to solve this problem in centralized [29, 31, 37] and decentralized [32] observation framework.

However, the existing decentralized robust diagnosis framework of DES still has two gaps to realistic situation. First, it is assumed that all sensors can only have the same type of failures, such as intermittent sensor failures [43], permanent sensor failures [32] and K-loss sensor failures [47]. In practice, as a result of different physical environment conditions, sensors of different local diagnosers may suffer from different types of failures. Thus, it is necessary to develop a uniform framework that can capture different types of sensor failures comprehensively for local diagnosers. Second, the existing framework of decentralized robust diagnosis assumes that there are only private sensors corresponding to each local diagnoser. Namely, it is not able to consider the presence of some sensors that can broadcast observations to all local diagnosers. In many realistic cases with limited resources, there exist some common sensors that broadcast observations to all local diagnosers in the mean time. As a result, the observations of events observed by common sensors are the same for all local diagnosers whenever these events occur.

In this paper, we consider a decentralized scheme with common sensors where sensors of different local diagnosers may have different types of sensor failures. Intuitively, as shown in Figure 2, we assume each local diagnoser $D_i, i \in I$, obtains observations of the plant behaviors through both its private sensors and common sensors. Different local diagnosers own different private sensors and observations, but will receive the same observations from common sensors. To motivate our development, we again consider system $G$ as depicted in Figure 1 and take the scenario where different types of sensor failures are considered comprehensively and there exists a common sensor as an example. As we discussed in Example 1, there are two local diagnosers. Sensors that broadcast observations to all local diagnosers are called common sensors and others are referred to as private sensors. First, we assume that the sensor of event $a$ is common, that is, the observations received by local diagnoser $D_1$ and $D_2$ are the same whenever event $a$ occurs. Note that there are two kinds of possible outputs $\{o_1, o_2\}$ when event $a$ occurs. We assume

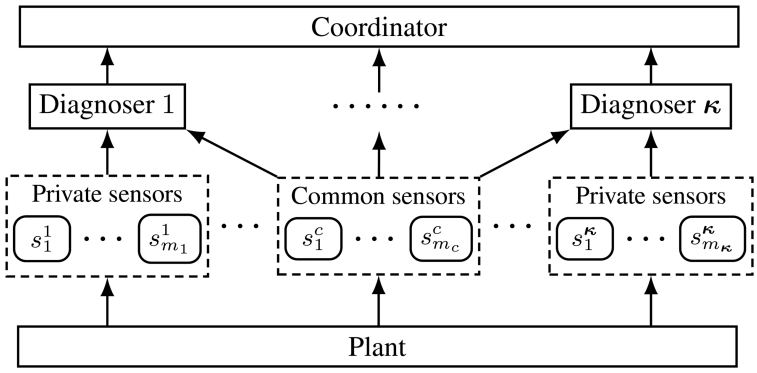


**Figure 2** Decentralized diagnosis scheme with common sensors. For local diagnoser $D_i, i \in I$, $m_i$ denotes the number of its private sensors and $s_j^i$ denotes the $j$th private sensor of $D_i$ where $j = 1, \ldots, m_i$. The number of common sensors is denoted by $m_c$ and $s_j^c$ denotes the $j$th common sensor where $j = 1, \ldots, m_c$.

the common sensor is subject to fairness failures [48], that is, if event $a$ occurs infinitely, the common sensor will observe $o_1$ for infinite times. Second, for local diagnoser $D_1$, the sensor of event $c$ suffers from permanent sensor failures [32], and the sensor of event $e$ has intermittent sensor failures [43], that is, it observes a symbol in $\{o_1, o_4\}$ non-deterministically when event $e$ occurs. Finally, for local diagnoser $D_2$, we assume that private sensors of events $b, c, e$ have intermittent sensor failures. With the above setting, consider the finite string $s = fad \in \mathcal{L}(G)$. It is infeasible for $D_1$ to obtain observation $o_1o_3$ and for $D_2$ to obtain observation $o_2o_3$ at the mean time, since the output of event $a$ should be the same for both local diagnosers. Both local diagnoser $D_1$ and $D_2$ can only receive either $o_1o_3$ or $o_2o_3$ concurrently.

Such complex combinations of different types of sensor failures cannot be analyzed in existing decentralized robust diagnosis frameworks. This gap motivates us to provide a general framework that can deal with the case which considers several types of sensor failures comprehensively and is compatible with the existence of common sensors. Specifically, the basic idea of our approach is as follows:

• First, we construct the unconstrained observation space for each local diagnoser by considering all possible outputs of common sensors and private sensors;

• Then, we further eliminate infeasible observations for each local diagnoser according to how common sensors and private sensors should behave;

• Finally, we consider executions of all local diagnosers comprehensively under the unity of common sensors.

### 3.2 LTL based common and private sensor constraints

In this paper, we assume that the two sets of events observed by common sensors and private sensors are disjoint. In this case, we can partition the event set into two disjoint subsets

$$\Sigma = \Sigma_l \dot{\cup} \Sigma_c,$$

where $\Sigma_l$ is the set of private events which are only observed by private sensors of local diagnosers and $\Sigma_c$ is the set of common events which are only observed by common sensors. Given system $G$, the limited observation mapping of common sensors is defined by $\mathcal{O}_c : Q \times \Sigma_c \to 2^{\Delta_c \dot{\cup} \{\epsilon\}}$, where $\Delta_c$ is the set of observation symbols of common sensors. For the private sensors of local diagnoser $D_i, i \in I$, its observation mapping is defined by $\mathcal{O}_l^i : Q \times \Sigma_l \to 2^{\Delta_l^i \dot{\cup} \{\epsilon\}}$, where $\Delta_l^i$ is the set of output symbols of private sensors corresponding to $D_i$. For the diagnoser $D_i$, its observation symbols set is $\Delta_i = \Delta_l^i \cup \Delta_c$. Then, the observations of all local diagnosers can be obtained by general observation mapping $\mathcal{P} : Q \times \Sigma \to 2^{\Delta_1 \dot{\cup} \{\epsilon\} \times \cdots \times \Delta_\kappa \dot{\cup} \{\epsilon\}}$, which is defined as follows: for any state $q \in Q$ and event $\sigma \in \Sigma$,

$$\begin{aligned}\mathcal{P}(q, \sigma) = \{&(o_1, o_2, \ldots, o_\kappa) \in \Delta_1 \dot{\cup} \{\epsilon\} \times \cdots \times \Delta_\kappa \dot{\cup} \{\epsilon\} : \\ &(\sigma \in \Sigma_c \to o_1 = o_2 = \cdots = o_\kappa \in \mathcal{O}_c(q, \sigma)) \wedge (\forall i \in I)(\sigma \in \Sigma_l \to o_i \in \mathcal{O}_l^i(q, \sigma))\}.\end{aligned}$$

Intuitively, when event $\sigma$ is enabled at state $q$, there are two cases: (i) if the event is a common event, i.e., $\sigma \in \Sigma_c$, all local diagnosers will receive the same observation from the common sensor of $\sigma$, i.e., $o_1 = o_2 = \cdots = o_\kappa = \mathcal{O}_c(q, \sigma)$; (ii) if the event is a private event, each local diagnoser will receive

observation from its own private sensor, i.e., $o_i = \mathcal{O}_l^i(q,\sigma)$. In this case, the observation received by local diagnoser $D_i, i \in I$ is obtained through combining observations from private sensors and common sensors, which is defined by the local observation mapping $\mathcal{P}_i : Q \times \Sigma \to 2^{\Delta_l^i \dot\cup \Delta_c \dot\cup \{\epsilon\}}$, which is formally defined by: for any state $q \in Q$ and event $\sigma \in \Sigma$, we have

$$\mathcal{P}_i(q,\sigma) = \{o \in \Delta_i \cup \{\epsilon\} : (\exists (o_1, o_2, \ldots, o_{\boldsymbol{\kappa}}) \in \mathcal{P}(q,\sigma))(o = o_i)\}.$$

Note that since the common events are observed by common sensors and their outputs will be broadcast to all local diagnosers, every local diagnoser will have the same observation whenever the common event occurs. Therefore, it holds that for any common event $\sigma \in \Sigma_c$ and any state $q \in Q$, $\mathcal{P}_1(q,\sigma) = \cdots = \mathcal{P}_{\boldsymbol{\kappa}}(q,\sigma)$.

In order to capture the relationship among internal states, internal event and external outputs for local diagnoser $D_i, i \in I$, we define the set of local extended events for $D_i$ by $\Sigma_e^i = \Sigma_e^c \dot\cup \Sigma_{e,l}^i$, where $\Sigma_e^c = Q \times \Sigma_c \times (\Delta_c \dot\cup \{\epsilon\})$ is the set of extended events corresponding to common sensors and $\Sigma_{e,l}^i = Q \times \Sigma_l \times (\Delta_l^i \dot\cup \{\epsilon\})$ is the set of extended events corresponding to private sensors owned by $D_i$. A local extended event string $s = (q_0,\sigma_0,o_0)(q_1,\sigma_1,o_1)\cdots \in (\Sigma_e^i)^+$ is generated by system $G$ and corresponding to local diagnoser $D_i, i \in I$, if for any $j = 0,1,\ldots$, we have $\delta(q_j,\sigma_j) = q_{j+1}, o_j \in \mathcal{P}_i(q_j,\sigma_j)$ and $q_0$ is the initial state of $G$. $\mathcal{L}_i(G)$ and $\mathcal{L}_i^\omega(G)$ denote the sets of all finite and infinite extended strings of local diagnoser $D_i, i \in I$, respectively. Then, for any extended string $s = (q_0,\sigma_0,o_0)(q_1,\sigma_1,o_1)\cdots \in (\Sigma_e^i)^+$, $\Theta_Q(s) = q_0 q_1 \cdots \in Q^+$, $\Theta_\Sigma(s) = \sigma_0\sigma_1\cdots \in \Sigma^+$ and $\Theta_\Delta(s) = o_0 o_1 \cdots \in \Delta_i^+$ denote its internal state sequence, internal event string and external observation string, respectively. Note that, the external observation string $\Theta_\Delta(s)$ is an observation realization of $s$ for local diagnoser $D_i$. Then, we define by $\Sigma_{e,F}^i = \{\sigma \in \Sigma_e^i : \Theta_\Sigma(\sigma) \in \Sigma_F\}$ the faulty extended event set for local diagnoser $D_i, i \in I$. Similarly, $\mathcal{L}_{i,F}(G) \subset \mathcal{L}_i(G)$ and $\mathcal{L}_{i,F}^\omega(G) \subset \mathcal{L}_i^\omega(G)$ denote the sets of finite and infinite extended faulty strings for $D_i$.

To model behaviors of common and private sensors, $\mathcal{AP}_c$ denotes the atomic proposition set of common sensors, called common propositions, and for local diagnoser $D_i, i \in I$, $\mathcal{AP}_l^i$ denotes the atomic proposition set of its private sensors, called private propositions of $D_i$. We assume that each set of private propositions and the set of common propositions are disjoint, i.e., $\forall i \in I, \mathcal{AP}_l^i \cap \mathcal{AP}_c = \emptyset$. $\mathcal{AP}_i = \mathcal{AP}_l^i \cup \mathcal{AP}_c$ denotes the set of atomic propositions for local diagnoser $D_i$. We define the common labeling function for common sensors by $\mathsf{label}_c : \Sigma_e^c \to 2^{\mathcal{AP}_c}$ which assigns each extended event a set of common propositions, and we define the private labeling function for private sensors of local diagnoser $D_i, i \in I$, by $\mathsf{label}_l^i : \Sigma_{e,l}^i \to 2^{\mathcal{AP}_l^i}$. Then, by combining common labeling function and private labeling function, we construct the local labeling function of local diagnoser $D_i, i \in I$, by $\mathsf{label}_i : \Sigma_e^i \to 2^{\mathcal{AP}_i}$. Formally, the local labeling function of local diagnoser $D_i, i \in I$, is defined by: for any event $\sigma_e = (q,\sigma,o) \in \Sigma_e^i$, we have

$$\mathsf{label}_i(\sigma_e) = \begin{cases} \mathsf{label}_c(\sigma_e), & \text{if } \sigma_e \in \Sigma_e^c, \\ \mathsf{label}_l^i(\sigma_e), & \text{if } \sigma_e \in \Sigma_{e,l}^i. \end{cases}$$

For any extended string $s = \sigma_1\sigma_2\cdots \in (\Sigma_e^i)^+$, we define its trace as $\mathsf{trace}(s) = \mathsf{label}_i(\sigma_1)\mathsf{label}_i(\sigma_2)\cdots \in (2^{\mathcal{AP}_i})^+$. Based on $\mathcal{AP}_c$, we can describe the constraint of common sensors by an LTL formula $\varphi_c$ over atomic proposition set $\mathcal{AP}_c$. For each local diagnoser $D_i, i \in I$, we can capture constraints of its private sensors by an LTL formula $\varphi_l^i$ over atomic proposition set $\mathcal{AP}_l^i$. Then, $\varphi_i = \varphi_l^i \wedge \varphi_c$ is the sensor constraint of $D_i, i \in I$, which is a conjunction of local sensor constraint $\varphi_l^i$ for local diagnoser $D_i$ and common sensor constraint $\varphi_c$. We say an infinite extended string $s \in (\Sigma_e^i)^\omega$ is $\varphi_i$-compatible, if its trace satisfies $\varphi_i$, i.e., $\mathsf{trace}(s) \models \varphi_i$, and we write $s \models \varphi_i$ if $s$ is $\varphi_i$-compatible, for simplicity. We use

$$\mathcal{L}_i^\varphi(G) = \{s \in \mathcal{L}_i^\omega(G) : s \models \varphi_i\}$$

to denote the set of all $\varphi_i$-compatible infinite extended strings for local diagnoser $D_i, i \in I$, while $\mathcal{L}_{i,F}^\varphi = \mathcal{L}_i^\varphi(G) \cap \mathcal{L}_{i,F}^\omega(G)$ is the set of extended faulty strings that are $\varphi_i$-compatible. We define $\varphi = (\varphi_1, \ldots, \varphi_{\boldsymbol{\kappa}})$ as the set of all sensor constraints for local diagnosers.

**Remark 2.** Intuitively, we use LTL formulae to specify realistic properties of common sensors and private sensors and only infinitely observations that satisfy constraints of sensors are feasible. Specifically, once we specify that the common sensors satisfying constraint $\varphi_c$ and private sensors of $D_i$ satisfying constraint $\varphi_l^i, i \in I$, only behaviors in $\mathcal{L}_i^\varphi(G)$ are feasible in practice. In this case, when local diagnoser $D_i$ online diagnoses system $G$, it only obtains observations of extended strings in $\overline{\mathcal{L}_i^\varphi(G)}$.

To capture the observations received by local diagnoser $D_i, i \in I$, under local sensor constraint $\varphi_i$, we define the local observation function by $\mathcal{M}_i : \Sigma^+ \to \Delta_i^+$ for local diagnoser $D_i$, which is formally defined by: for any $s \in \Sigma^+$,

$$\mathcal{M}_i(s) = \{\rho \in \Delta_i^+ : (\exists s_e \in \mathcal{L}_i^{\varphi}(G) \cup \overline{\mathcal{L}_i^{\varphi}(G)}) \text{ s.t. } [(\Theta_\Sigma(s_e) = s) \wedge (\Theta_\Delta(s_e) = \rho)]\}. \tag{4}$$

Intuitively, $\mathcal{M}_i(s)$ contains all feasible observations obtained by $D_i$ through the sensors satisfying constraint $\varphi_i$ when system $G$ executes $s$. By the above equation, for any $s_e \in \mathcal{L}_i^{\varphi}(G) \cup \overline{\mathcal{L}_i^{\varphi}(G)}$, we also have $\Theta_\Delta(s_e) \in \mathcal{M}_i(\Theta_\Sigma(s_e))$. To comprehensively consider feasible observations of all local diagnosers, we define the infinite general observations of an infinite event string $s \in \Sigma^\omega$ as $\boldsymbol{\kappa}$-table of observations in the form $(\rho_1, \rho_2, \ldots, \rho_{\boldsymbol{\kappa}}) \in \Delta_1^+ \times \cdots \times \Delta_{\boldsymbol{\kappa}}^+$, which can be obtained by infinite general observation function $\mathcal{M}^{\varphi} : \Sigma^\omega \to \Delta_1^+ \times \cdots \times \Delta_{\boldsymbol{\kappa}}^+$ defined as follows: for any $s \in \Sigma^\omega$,

$$\begin{aligned}\mathcal{M}^{\varphi}(s) =& \{(\rho_1, \rho_2, \ldots, \rho_{\boldsymbol{\kappa}}) \in \Delta_1^+ \times \cdots \times \Delta_{\boldsymbol{\kappa}}^+ : (\exists (s_1, s_2, \ldots, s_{\boldsymbol{\kappa}}) \in \mathcal{L}_1^{\varphi}(G) \\ & \times \cdots \times \mathcal{L}_{\boldsymbol{\kappa}}^{\varphi}(G))[(\forall i \in I)(\Theta_\Sigma(s_i) = s \wedge \Theta_\Delta(s_i) = \rho_i) \wedge (\forall j \in \mathbb{N}) \\ & (s[j] \in \Sigma_c \to \Theta_\Delta(s_1[j]) = \Theta_\Delta(s_2[j]) = \cdots = \Theta_\Delta(s_{\boldsymbol{\kappa}}[j]))]\}. \end{aligned} \tag{5}$$

Intuitively, when system executes $s \in \Sigma^\omega$, $\mathcal{M}^{\varphi}(s)$ contains all possible combinations of observations $(\rho_1, \rho_2, \ldots, \rho_{\boldsymbol{\kappa}}) \in \Delta_1^+ \times \cdots \times \Delta_{\boldsymbol{\kappa}}^+$ such that there exists an extended string combination $(s_1, s_2, \ldots, s_{\boldsymbol{\kappa}}) \in \mathcal{L}_1^{\varphi}(G) \times \mathcal{L}_2^{\varphi}(G) \times \cdots \times \mathcal{L}_{\boldsymbol{\kappa}}^{\varphi}(G)$ satisfying that (i) for any $i \in I$, $s_i$ has the internal event string $s$ and the external observation $\rho_i$; (ii) for any $j \in \mathbb{N}$, if $s[j]$ is a common event, the outputs of $s_i[j]$ for all $i \in I$ must be equal. Essentially, general observation function $\mathcal{M}^{\varphi}$ generates the combinations of observations obtained by local diagnosers taking into consideration both constraints of private sensors and common sensors. Then, the finite general observations are the combinations of finite feasible local observations. Formally, finite general observations can be obtained by finite general observation function $\overline{\mathcal{M}}^{\varphi} : \Sigma^* \to \Delta_1^* \times \cdots \times \Delta_{\boldsymbol{\kappa}}^*$ defined as follows: for any $s \in \Sigma^*$,

$$\begin{aligned}\overline{\mathcal{M}}^{\varphi}(s) =& \{(\rho_1, \rho_2, \ldots, \rho_{\boldsymbol{\kappa}}) \in \Delta_1^* \times \cdots \times \Delta_{\boldsymbol{\kappa}}^* : (\exists (s_1, s_2, \ldots, s_{\boldsymbol{\kappa}}) \in \overline{\mathcal{L}_1^{\varphi}(G)} \times \cdots \times \overline{\mathcal{L}_{\boldsymbol{\kappa}}^{\varphi}(G)})[(\forall i \in I)(\Theta_\Sigma(s_i) \\ & = s \wedge \Theta_\Delta(s_i) = \rho_i) \wedge (\forall j \in \mathbb{N})(s[j] \in \Sigma_c \to \Theta_\Delta(s_1[j]) = \Theta_\Delta(s_2[j]) = \cdots = \Theta_\Delta(s_{\boldsymbol{\kappa}}[j]))]\}. \end{aligned}$$

Note that for any string $s \in \Sigma^*$, we have $\overline{\mathcal{M}}^{\varphi}(s) \subseteq \mathcal{M}_1(s) \times \mathcal{M}_2(s) \times \cdots \times \mathcal{M}_{\boldsymbol{\kappa}}(s)$, but the equality does not hold in general since the observations from common sensors have to be equivalent for each local diagnosers. For the system $G$, the set of all infinite and finite general observation is defined as $\mathcal{M}^{\varphi}(\mathcal{L}^\omega(G)) = \bigcup_{s \in \mathcal{L}^\omega(G)} \mathcal{M}^{\varphi}(s)$ and $\overline{\mathcal{M}}^{\varphi}(\mathcal{L}(G)) = \bigcup_{s \in \mathcal{L}(G)} \overline{\mathcal{M}}^{\varphi}(s)$, respectively, and similarly, for each $i \in I$, we define the set of all local observations as $\mathcal{M}_i(\mathcal{L}(G)) = \bigcup_{s \in \mathcal{L}(G)} \mathcal{M}_i(s)$.

Note that how to specify labeling functions and LTL formulae is application-dependent. We use the following example to illustrate this procedure.

**Example 3.** We still consider the system $G$ depicted in Figure 1 where there are two local diagnosers. We consider the motivation example in Subsection 3.1 more specifically. The set of private events can be defined as $\Sigma_l = \{b, c, d, e, f\}$ and the set of common events is $\Sigma_c = \{a\}$. For the common sensor, the observation symbol set is $\Delta_c = \{o_1, o_2\}$ and any symbol in $\Delta_c$ can be observed non-deterministically whenever event $a$ occurs. We assume that the output $o_1$ is fair, that is, if event $a$ occurs infinitely, the common sensor will observe $o_1$ for infinite times. To describe this scenario, we can choose the set of common propositions $\mathcal{AP}_c = \{m_0, m_1\}$, where $m_0$ and $m_1$ represent the observation of event $a$ is $o_1$ and $o_2$, respectively. Then, we define the common labeling function $\mathsf{label}_c : \Sigma_e^c \to 2^{\mathcal{AP}_c}$ by: for any event $\sigma_e = (q, \sigma, o) \in \Sigma_e^c$, we have

$$\mathsf{label}_c(\sigma_e) = \begin{cases} \{m_0\}, & \text{if } \sigma = a \wedge o = o_1, \\ \{m_1\}, & \text{if } \sigma = a \wedge o = o_2, \\ \emptyset, & \text{otherwise.} \end{cases}$$

Then the constraint of common sensor can be formalized as $\varphi_c = (\Box\Diamond(m_0 \vee m_1)) \to (\Box\Diamond m_0)$. Intuitively, the formula $\varphi_c$ means that if event $a$ occurs infinitely, then the observation $o_1$ will be observed for the infinite number of times.

As for local diagnoser $D_1$, the output symbols of its private sensors is $\Delta_l^1 = \{o_1, o_2, o_3, o_4\}$. We assume that (i) the reason why event $c$ may be unobservable is due to permanent sensor failures, that

is, once event $c$ becomes unobservable, diagnoser $D_1$ can never observe it; (ii) the sensor of event $e$ has intermittent sensor failures, that is, diagnoser $D_1$ obtains an output in $\{o_1, o_4\}$ non-deterministically whenever event $e$ occurs. In this case, we define the atomic propositions of private sensors of $D_1$ by $\mathcal{AP}_l^1 = \{m_0^1, m_1^1\}$, where $m_0^1$ and $m_1^1$ represent the sensor of event $c$ has a successful observation $o_2$ and failing one $\epsilon$, respectively. According to the properties of private sensors of $D_1$, we define the private labeling function $\mathsf{label}_l^1 : \Sigma_{e,l}^1 \to 2^{\mathcal{AP}_l^1}$ by: for any event $\sigma_e = (q, \sigma, o) \in \Sigma_{e,l}^1$

$$\mathsf{label}_l^1(\sigma_e) = \begin{cases} \{m_0^1\}, & \text{if } \sigma = c \wedge o = o_2, \\ \{m_1^1\}, & \text{if } \sigma = c \wedge o = \epsilon, \\ \emptyset, & \text{otherwise.} \end{cases}$$

Then the local sensor constraint of diagnoser $D_1$ can be written as $\varphi_l^1 = \Box(m_1^1 \to \Box\neg m_0^1)$. Note that the local sensor constraint $\varphi_l^1$ only restricts the observation of event $c$ explicitly but does not make any constraint on event $e$. This is because the type of sensor fault of event $e$ is an intermittent failure, which means the observation of event $e$ may be any value in a finite set uncertainly when it occurs, and we actually use the true formula to represent this constraint. The sensor constraint of $D_1$ is $\varphi_1 = \varphi_c \wedge \varphi_l^1 = ((\Box\Diamond m_0 \vee m_1) \to (\Box\Diamond m_0)) \wedge (\Box(m_1^1 \to \Box m_0^1))$.

Finally, for local diagnoser $D_2$, its output symbols are $\Delta_l^2 = \Delta_l^1$ and its private sensors of event $\{b, c, e\}$ have intermittent sensor failures. As a result, we can set the atomic propositions of its private sensors as $\mathcal{AP}_l^2 = \emptyset$ and define the local sensor constraint of $D_2$ by $\varphi_l^2 = \top$. In this case, the sensor constraint of $D_2$ is $\varphi_2 = \varphi_c \wedge \varphi_l^2 = \varphi_c$.

Under above mentioned sensor constraints, consider local diagnoser $D_1$. We know that the local extended string $s_1 = (1, b, \epsilon)(2, c, \epsilon)(3, d, o_3)(4, e, o_1)[(2, c, o_2)(3, d, o_3)(4, e, o_1)]^\omega \in (\Sigma_e^i)^\omega$ is not $\varphi_i$-compatible and $s_1 \notin \mathcal{L}_1^\varphi(G)$, since $\mathsf{trace}(s_1) = \emptyset m_1^1 \emptyset\emptyset (m_0^1 \emptyset\emptyset)^\omega \not\models \varphi_1$. Thus, it is impossible for $D_1$ to observe the finite output $o_3 o_1 o_2 o_3 o_1$, since the extended string $s_1' = (1, b, \epsilon)(2, c, \epsilon)(3, d, o_3)(4, e, o_1)(2, c, o_2)(3, d, o_3)(4, e, o_1) \in \overline{\{s_1\}}$ is not included in $\overline{\mathcal{L}_1^\varphi(G)}$. However, the infinite extended string $s_2 = (1, b, \epsilon)(2, c, \epsilon)(3, d, o_3)(4, e, o_1)[(2, c, \epsilon)(3, d, o_3)(4, e, o_1)]^\omega \in (\Sigma_e^i)^\omega$, whose trace is $\mathsf{trace}(s_2) = \emptyset m_1^1 \emptyset\emptyset (m_1^1 \emptyset\emptyset)^\omega \models \varphi_1$, is $\varphi_1$-compatible and $s_2 \in \mathcal{L}_1^\varphi(G)$. Therefore, we have $(o_3 o_1)^\omega \in \mathcal{M}_1(b(cde)^\omega)$.

## 4 Codiagnosability under sensor constraints

In this section, we investigate codiagnosability subject to LTL-based sensor constraints. Specifically, we first modify the existing definition of codiagnosability in Definition 1 to a novel notion, called $\varphi$-codiagnosability. Then, we prove that $\varphi$-codiagnosability is the necessary and sufficient condition for the existence of a set of decentralized diagnosers that work correctly under sensor constraint $\varphi$.

By taking the issues of the sensor constraint $\varphi$ into account, we formally propose a new notion of codiagnosability, called $\varphi$-codiagnosability.

**Definition 3** ($\varphi$-codiagnosability)**.** System $G$ is said to be $\varphi$-codiagnosable w.r.t. local observation mappings $\{\mathcal{P}_i\}_{i\in I}$, fault events $\Sigma_F$ and sensor constraint $\varphi = (\varphi_1, \ldots, \varphi_{\boldsymbol{\kappa}})$, if

$$(\forall s \in \mathcal{L}_F^\omega(G))(\forall(\rho_1, \rho_2, \ldots, \rho_{\boldsymbol{\kappa}}) \in \mathcal{M}^\varphi(s))(\exists i \in I)(\exists \rho \in \overline{\{\rho_i\}})[\varphi\text{-}\mathsf{codiag}], \tag{6}$$

where the $\varphi$-codiagnostic condition $\varphi$-$\mathsf{codiag}$ is

$$(\forall v \in \mathcal{L}(G))[\rho \in \mathcal{M}_i(v) \Rightarrow \Sigma_F \in v].$$

Intuitively, the above definition says that, for any infinite faulty string $s \in \mathcal{L}_F^\omega(G)$ and its general observation $(\rho_1, \rho_2, \ldots, \rho_{\boldsymbol{\kappa}}) \in \mathcal{M}^\varphi(s)$, there is a local diagnoser $D_i, i \in I$ and a finite prefix $\rho$ of $\rho_i$ such that for any finite string $v \in \mathcal{L}(G)$, if the local observation of $v$ contains $\rho$, i.e., $\rho \in \mathcal{M}_i(v)$, then the string $v$ must also be faulty. Essentially, $\varphi$-codiagnosability extends the standard codiagnosability by restricting our attention to local observations that are generated by constrained sensors and taking common sensors into the consideration.

**Remark 3.** Note that LTL sensor constraint $\varphi$ is imposed on infinite strings. As a result, in the definition of $\varphi$-codiagnosability, we can only guarantee that for any infinite faulty string, there is a finite detection bound, while this does not imply the existence of a uniform detection bound for all faulty

strings. In our previous work [37] for the centralized case, we showed that if the LTL formula $\varphi$ is a safety property, then a uniform detection bound exists for all faulty strings. Similar results can also be obtained for our decentralized case.

**Example 4.** Let us still consider the system $G$ shown in Figure 1 with the same setting in Example 3. There is an infinite faulty string $s_F = f(ad)^\omega \in \mathcal{L}^\omega(G)$, along which there are two infinite faulty extended strings $s_1 = s_2 = (1, f, \epsilon)(5, a, o_2)[(6, d, o_3)(5, a, o_1)]^\omega$ for local diagnoser $D_1$ and $D_2$, respectively, such that $\mathsf{trace}(s_1) = \mathsf{trace}(s_2) = \emptyset m_1(\emptyset m_0)^\omega$. Since $\mathsf{trace}(s_1) \models \varphi_1$, we have $\rho_1 = \Theta_\Delta(s_1) = o_2(o_3o_1)^\omega \in \mathcal{M}_1(s)$, and since $\mathsf{trace}(s_2) \models \varphi_2$, we have $\rho_2 = \Theta_\Delta(s_2) \in \mathcal{M}_2(s)$. By (5), the general observation $(\rho_1, \rho_2)$ is included in $\mathcal{M}^\varphi(s)$. On the other hand, consider a normal string $v = b(cde)^\omega \in \mathcal{L}^\omega(G)$. For local diagnoser $D_1$, there is $v_1 = (1, b, \epsilon)(2, c, o_2)[(3, d, o_3)(4, e, o_1)(2, c, \epsilon)]^\omega \in (\Sigma_e^i)^\omega$ such that $\mathsf{trace}(v_1) = \emptyset m_0^1(\emptyset\emptyset m_1^1)^\omega \models \varphi_1$, i.e., $v_1 \in \mathcal{L}_1^\varphi(G)$ and $\Theta_\Delta(v_1) = \rho_1 \in \mathcal{M}_1(v_1)$. For local diagnoser $D_2$, there is $v_2 = (1, b, o_2)(2, c, \epsilon)[(3, d, o_3)(4, e, \epsilon)(2, c\ , o_1)]^\omega \in (\Sigma_e^i)^\omega$ such that $\mathsf{trace}(v_2) = \emptyset^\omega \models \varphi_2$, i.e., $v_2 \in \mathcal{L}_2^\varphi(G)$ and $\Theta_\Delta(v_2) = \rho_2 \in \mathcal{M}_2(v_2)$. Therefore, there exists an infinite faulty string $s \in \mathcal{L}^\omega(G)$ such that one of its general observation $(\rho_1, \rho_2)$ satisfies that for each $i \in \{1, 2\}$ and any prefix $\rho \in \overline{\{\rho_i\}}$, there exists a normal finite string $v' \in \overline{\{v_i\}}$ having the output $\rho$ for diagnoser $D_i$, i.e., $\rho \in \mathcal{M}_i(v')$. By Definition 3, the system $G$ is not $\varphi$-codiagnosable.

The decentralized diagnosis problem of a system with sensors constrained by $\varphi$ requires that the occurrence of any faulty event should be detected by at least one local diagnoser $D_i, i \in I$. Formally, a local diagnoser $D_i, i \in I$ is defined as a function

$$D_i : \mathcal{M}_i(\mathcal{L}(G)) \to \{0, 1\},$$

which assigns each local observation a diagnostic decision. If $D_i$ is sure that a fault has occurred, then "1" is issued; otherwise $D_i$ issues "0". Then, the decentralized diagnoser is a combination of local diagnosers and is defined as $\{D_i\}_{i\in I} : \overline{\mathcal{M}}^\varphi(\mathcal{L}(G)) \to \{0, 1\}$ which issues the decision "1" if at least one local diagnoser issues "1"; otherwise, issues "0". We say that a decentralized diagnoser works correctly subject to sensor constraint $\varphi$ if it satisfies the following conditions:

(C1) For any occurrence of a fault event, the decentralized diagnoser will eventually issue a fault alarm, i.e.,

$$\begin{aligned}&(\forall s \in \mathcal{L}_F^\omega(G))(\forall(\rho_1, \ldots, \rho_{\boldsymbol{\kappa}}) \in \mathcal{M}^\varphi(s))(\exists t \in \overline{\{s\}})(\exists(\rho_1', \ldots, \rho_{\boldsymbol{\kappa}}') \in \overline{\mathcal{M}}^\varphi(t))\\ &[(\forall i \in I)(\rho_i' \in \overline{\{\rho_i\}})] \wedge [\{D_i\}_{i\in I}((\rho_1', \ldots, \rho_{\boldsymbol{\kappa}}')) = 1].\end{aligned}$$

(C2) For any normal execution, the decentralized diagnoser will not issue a false alarm, i.e.,

$$(\forall s \in \mathcal{L}(G) : \Sigma_F \notin s)[(\forall(\rho_1, \ldots, \rho_{\boldsymbol{\kappa}}) \in \overline{\mathcal{M}}^\varphi(s))(\{D_i\}_{i\in I}((\rho_1, \ldots, \rho_{\boldsymbol{\kappa}})) = 0)].$$

The following theorem says that the $\varphi$-codiagnosability in Definition 3 is a necessary and sufficient condition for the existence of a decentralized diagnoser working correctly under sensor constraint $\varphi$.

**Theorem 1.** There exists a decentralized diagnoser $\{D_i\}_{i\in I} : \overline{\mathcal{M}}^\varphi(\mathcal{L}(G)) \to \{0, 1\}$ satisfying conditions (C1) and (C2) if and only if $G$ is $\varphi$-codiagnosable w.r.t. faulty event $\Sigma_F$, local observation mappings $\{\mathcal{P}_i\}_{i\in I}$, and sensor constraint $\varphi$.

*Proof.* ($\Leftarrow$) We prove the necessity by contradiction. Suppose that there exists a diagnoser $\{D_i\}_{i\in I}$ satisfying conditions (C1) and (C2), while, for the sake of contradiction, we assume that system $G$ is not $\varphi$-codiagnosable. Then, there exists an infinite faulty string $s \in \mathcal{L}_F^\omega(G)$ and a general observation $(\rho_1, \rho_2, \ldots, \rho_{\boldsymbol{\kappa}}) \in \mathcal{M}^\varphi(s)$ such that for any $i \in I$ and any prefix $\rho \in \overline{\{\rho_i\}}$, we can find a normal string $v \in \mathcal{L}(G)$ that has the local observation $\rho$ for local diagnoser $D_i$. Therefore, for any $t \in \overline{\{s\}}$, we have $(\rho_1^t, \rho_2^t, \ldots, \rho_{\boldsymbol{\kappa}}^t) \in \overline{\mathcal{M}}^\varphi(t)$ such that for any $i \in I$, $\rho_i^t$ is a prefix of $\rho_i$, and there exists a finite normal string $v' \in \overline{\{v\}}$ having the observation $\rho_i^t$, that is, there is a finite general observation $(\rho_1^{v'}, \ldots, \rho_i^t, \ldots, \rho_{\boldsymbol{\kappa}}^{v'}) \in \overline{\mathcal{M}}^\varphi(v')$. Since diagnoser $\{D_i\}_{i\in I}$ satisfies conditions (C2), we have $\{D_i\}_{i\in I}(\rho_1^{v'}, \ldots, \rho_i^t, \ldots, \rho_{\boldsymbol{\kappa}}^{v'}) = 0$. Thus, we have $D_i(\rho_i^t) = 0$ for any $i \in I$. As a result, $\forall t \in \overline{\{s\}}, \{D_i\}_{i\in I}(\rho_1^t, \rho_2^t, \ldots, \rho_{\boldsymbol{\kappa}}^t) = 0$, i.e., condition (C1) does not hold for diagnoser $\{D_i\}_{i\in I}$, which contradicts the assumption.

($\Rightarrow$) Suppose system $G$ is $\varphi$-codiagnosable. We consider the local diagnoser $D_i : \mathcal{M}_i(\mathcal{L}(G)) \to \{0, 1\}$ given as: for any $\rho \in \mathcal{M}_i(\mathcal{L}(G))$

$$D_i(\rho) = \begin{cases} 1, & \text{if } \forall s \in \mathcal{L}(G) : \rho \in \mathcal{M}_i(s) \Rightarrow \Sigma_F \in s,\\ 0, & \text{otherwise.}\end{cases} \tag{7}$$

Then, we claim that the decentralized diagnoser $\{D_i\}_{i\in I}$ satisfies conditions (C1) and (C2). To see that (C1) holds, we consider any faulty string $s \in \mathcal{L}_F^\omega(G)$. By definition of $\varphi$-codiagnosability, for any general observation $(\rho_1, \rho_2, \ldots, \rho_{\boldsymbol{\kappa}}) \in \mathcal{M}^\varphi(s)$, there exists $i \in I$ and $\rho \in \overline{\{\rho_i\}}$ such that for any string $v \in \mathcal{L}(G)$, if $\rho \in \mathcal{M}_i(v)$, $v$ is faulty. By (7), we have $D_i(\rho) = 1$. Along string $s$, we can find a prefix $t \in \overline{\{s\}}$ and $(\rho_1^t, \rho_2^t, \ldots, \rho_{\boldsymbol{\kappa}}^t) \in \overline{\mathcal{M}}^\varphi(t)$ such that $\rho_i^t = \rho$ and for any $j \in I$, $\rho_j^t$ is a prefix of $\rho_j$. Since $D_i(\rho_i^t) = 1$, we have $\{D_i\}_{i\in I}((\rho_1^t, \rho_2^t, \ldots, \rho_{\boldsymbol{\kappa}}^t)) = 1$. We next show that the diagnoser $\{D_i\}_{i\in I}$ satisfies condition (C2). Consider any normal string $s \in \mathcal{L}(G), \Sigma_F \notin s$. For any $(\rho_1, \ldots, \rho_{\boldsymbol{\kappa}}) \in \overline{\mathcal{M}}^\varphi(s)$, we have $\rho_i \in \mathcal{M}_i(s)$ and $D_i(\rho_i) = 0$ for any $i \in I$. Thus, we have $\{D_i\}_{i\in I}((\rho_1, \ldots, \rho_{\boldsymbol{\kappa}})) = 0$.

## 5 Verification of $\varphi$-codiagnosable

In this section, we investigate how to verify $\varphi$-codiagnosable based on the verification system.

### 5.1 Local augmented system

To consider the dynamic of system and sensor constraints, our first step is to construct the local augment system for each local diagnoser.

**Definition 4** (Local augmented systems)**.** Given system $G = (Q, \Sigma, \delta, q_0)$ with fault events $\Sigma_F$ and local observation mappings $\{\mathcal{P}_i\}_{i\in I}$, we define the local augment system associated with the local diagnoser $D_i$ as a new-tuple

$$\tilde{G}_i = (\tilde{Q}_i, \tilde{q}_{i,0}, \Sigma_e^i, \tilde{\delta}_i), \tag{8}$$

where

- $\tilde{Q}_i \subseteq Q \times \{F, N\}$ is the set of augmented states;
- $\tilde{q}_{i,0} = (q_0, N)$ is the initial augmented state;
- $\Sigma_e^i$ is the set of local extended events;
- $\tilde{\delta}_i : \tilde{Q}_i \times \Sigma_e^i \to \tilde{Q}_i$ is the transition function.

The transition function $\tilde{\delta}_i$ is defined as follows: for any $\tilde{q} = (q, l) \in \tilde{Q}_i$ and $\tilde{\sigma} = (q, \sigma, o) \in \Sigma_e^i$, we have $\tilde{\delta}_i(\tilde{q}, \tilde{\sigma})!$ whenever $\delta(q, \sigma)!$ and $o \in \mathcal{P}_i(q, \sigma)$. Specifically, $\tilde{\delta}_i(\tilde{q}, \tilde{\sigma})$ is defined as

$$\tilde{\delta}_i(\tilde{q}, \tilde{\sigma}) = \begin{cases} (\delta(q, \sigma), N), & \text{if } l = N \wedge \tilde{\sigma} \notin \Sigma_{e,F}^i, \\ (\delta(q, \sigma), F), & \text{otherwise.} \end{cases}$$

By the construction of local augmented systems, similar to [37], we have the following two properties of each local augment system $\tilde{G}_i, i \in I$:

- First, the augment system $\tilde{G}_i$ generates extended event strings of local diagnoser $D_i$. Essentially, $\tilde{G}_i$ associates external observation and emission state information to an internal event, but still tracks the original dynamic of system $G$. Therefore, we have that for any $i \in I, \mathcal{L}(\tilde{G}_i) = \mathcal{L}_i(G)$.
- Second, for each augmented state $(q, l) \in \tilde{Q}_i$, the first component $q \in Q$ is the internal state in system $G$ and the second component $l \in \{N, F\}$ is the label recording whether a fault event has occurred. Specifically, the label is $N$ initially and then transferred to $F$ whenever an extended fault event occurs and the label $F$ will be kept forever. For the local augmented system $\tilde{G}_i$, $\tilde{Q}_i^F = \{(q, l) \in \tilde{Q}_i : l = F\}$ is the set of faulty augmented states and $\tilde{Q}_i^N = \{(q, l) \in \tilde{Q}_i : l = N\}$ is the set of normal augmented states.

**Example 5.** Again, consider system $G$ depicted in Figure 1. Its augmented systems $\tilde{G}_1$ and $\tilde{G}_2$ are depicted in Figures 3(a) and (b), respectively. For any $i \in I$, all states reachable via extended faulty event $(1, f, \epsilon)$ are augmented with "$F$". For the sake of simplicity, we use $\sigma_q^o$ to denote the extended event $(q, \sigma, o)$. Note that each augmented system tracks the actual transitions of the original system $G$ and the observations of the corresponding local diagnoser. For example, consider the augmented system $\tilde{G}_1$. Since there is transition $\delta(4, e) = 2$ and observation $\mathcal{P}_1(4, e) = \{o_1, o_4\}$, we have two transitions in $\tilde{G}_1$: $\tilde{\delta}_i(4N, e_4^{o_1}) = 2N$ and $\tilde{\delta}_i(3N, e_4^{o_4}) = 2N$.

### 5.2 Local observation constrained system

In order to capture feasible extended strings that can be obtained from sensors constrained by $\varphi$, we construct the local observation constrained system of each local diagnoser. First, for any $i \in I$, we translate the sensor constraint $\varphi_i$ into an NBA $\mathcal{B}_{\varphi_i} = (X, X_0, 2^{\mathcal{AP}_i}, \xi, \mathcal{F})$ such that $\mathcal{L}_m^\omega(\mathcal{B}_{\varphi_i}) = \mathsf{word}(\varphi_i)$. Then, the local observation constrained system of $D_i$ is formally defined as follows.

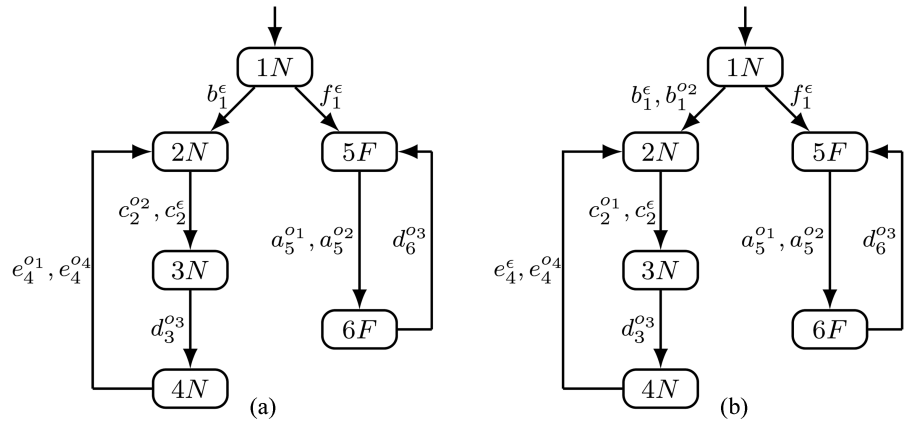


**Figure 3** Augmented systems of system $G$. For simplicity, we also use $\sigma_q^o$ to denote extended event $(q, \sigma, o)$. (a) Augmented system $\tilde{G}_1$; (b) augmented system $\tilde{G}_2$.

**Definition 5** (Local observation constrained system)**.** Given augmented system $\tilde{G}_i = (\tilde{Q}_i, \tilde{q}_{i,0}, \Sigma_e^i, \tilde{\delta}_i)$ and NBA $\mathcal{B}_{\varphi_i} = (X, X_0, 2^{\mathcal{AP}_i}, \xi, \mathcal{F})$, the local observation constrained system of $D_i$ is defined as a new-tuple

$$T_i = (Q_T^i, \Sigma_e^i, \delta_T^i, Q_{0,T}^i, Q_{m,T}^i), \tag{9}$$

where

- $Q_T^i \subseteq \tilde{Q}_i \times X$ is the set of states;
- $\Sigma_e^i$ is still the set of local extended events;
- $\delta_T^i : Q_T^i \times \Sigma_e^i \to 2^{Q_T^i}$ is the non-deterministic transition function defined by

$$\delta_T^i(q_T, \sigma_T) = \left\{ (\tilde{q}', x') : \tilde{q}' = \tilde{\delta}_i(\tilde{q}, \sigma_T) \text{ and } x' \in \xi(x, \mathsf{label}_i(\sigma_T)) \right\}$$

for any $q_T = (\tilde{q}, x) \in Q_T^i$ and $\sigma_T \in \Sigma_e^i$;

- $Q_{0,T}^i = \{\tilde{q}_{i,0}\} \times X_0$ is the set of initial states;
- $Q_{m,T}^i = \{(\tilde{q}, x) \in Q_T^i : x \in \mathcal{F}\}$ is the set of accepting states.

Intuitively, the local observation constrained system $T_i$ is a synchronization of the augmented system $\tilde{G}_i$ and the NBA $\mathcal{B}_{\varphi_i}$ according to labels of extended events. Specifically, for any $q_T = (\tilde{q}, x), q_T' = (\tilde{q}', x') \in Q_T^i$, we have transition $q_T' \in \delta_T^i(q_T, \sigma_T)$ is labeled by extended event $\sigma_T \in \Sigma_e^i$ whenever (i) the internal system state (the first component) $\tilde{q}$ can transfer to $\tilde{q}'$ enabled by extended event $\sigma_T$, i.e., $\tilde{q}' = \tilde{\delta}_i(\tilde{q}, \sigma_T)$; and (ii) the label of the extended event $\sigma_T$ satisfies the transition rules in NBA $\mathcal{B}_{\varphi_i}$, i.e., $x' \in \xi(x, \mathsf{label}_i(\sigma_T))$. Therefore, for any $s \in \mathcal{L}(T_i)$, we have $s \in \mathcal{L}(\tilde{G}_i) = \mathcal{L}_i(G)$, that is, $\mathcal{L}(T_i) \subseteq \mathcal{L}(\tilde{G}_i) = \mathcal{L}_i(G)$, and $\mathsf{trace}(s) \in \mathcal{L}(\mathcal{B}_{\varphi_i})$. By construction, the set of accepting state $Q_{m,T}^i$ contains state $(\tilde{q}, x)$ such that $x$ is the accepting state in $\mathcal{B}_{\varphi_i}$, i.e., $x \in \mathcal{F}$. Therefore, $T_i$ retains all infinite strings in $\tilde{G}_i$ that satisfy the sensor constraint $\varphi_i$, i.e., $\mathcal{L}_m^\omega(T_i) = \mathcal{L}_i^\varphi(G)$.

According to the notion of $\varphi$-codiagnosability in Definition 3, we need to compare local observations in $\mathcal{M}_i(\mathcal{L}(G))$ for every local diagnoser $D_i, i \in I$. To obtain $\mathcal{M}_i(\mathcal{L}(G))$, we need to recognize all finite $\varphi_i$-compatible extended strings $s \in \overline{\mathcal{L}_i^\varphi(G)}$ as defined in (4). By the construction of local observation constrained system $T_i$, we know that a finite extended string $s \in \overline{\mathcal{L}_i^\varphi(G)}$ if and only if it can reach a state in $Q_T^i$ from which $T_i$ can visit accepting states infinitely often. We say that a state $q \in Q_T^i$ is feasible if $\mathcal{L}_m^\omega(T_i(q)) \neq \emptyset$, where $T_i(q) = (Q_T^i, \Sigma_e^i, \delta_T^i, \{q\}, Q_{m,T}^i)$ is the same as $T_i$ except setting the initial state of $T_i$ as state $q$. We use $Q_{\text{feas}}^i \subset Q_T^i$ to denote the feasible state set in local observation constrained system $T_i$. Then, we have the following equivalence:

$$s \in \overline{\mathcal{L}_i^\varphi(G)} \Leftrightarrow \exists q_0 \in Q_{0,T}^i, \delta_T^i(q_0, s) \cap Q_{\text{feas}}^i \neq \emptyset. \tag{10}$$

To indicate whether a fault extended event occurs in word $s \in \mathcal{L}(T_i)$, we use $Q_{N,T}^i = \{(q, l, x) \in Q_T^i : l = N\}$ and $Q_{F,T}^i = \{(q, l, x) \in Q_T^i : l = F\}$ to denote the sets of normal and faulty states in $T_i$, respectively. Then the following equivalence holds: for any $s \in \mathcal{L}(T_i)$, we have

$$\Sigma_{e,F}^i \in s \Leftrightarrow \exists q_0 \in Q_{0,T}^i, \delta_T^i(q_0, s) \cap Q_{F,T}^i \neq \emptyset. \tag{11}$$

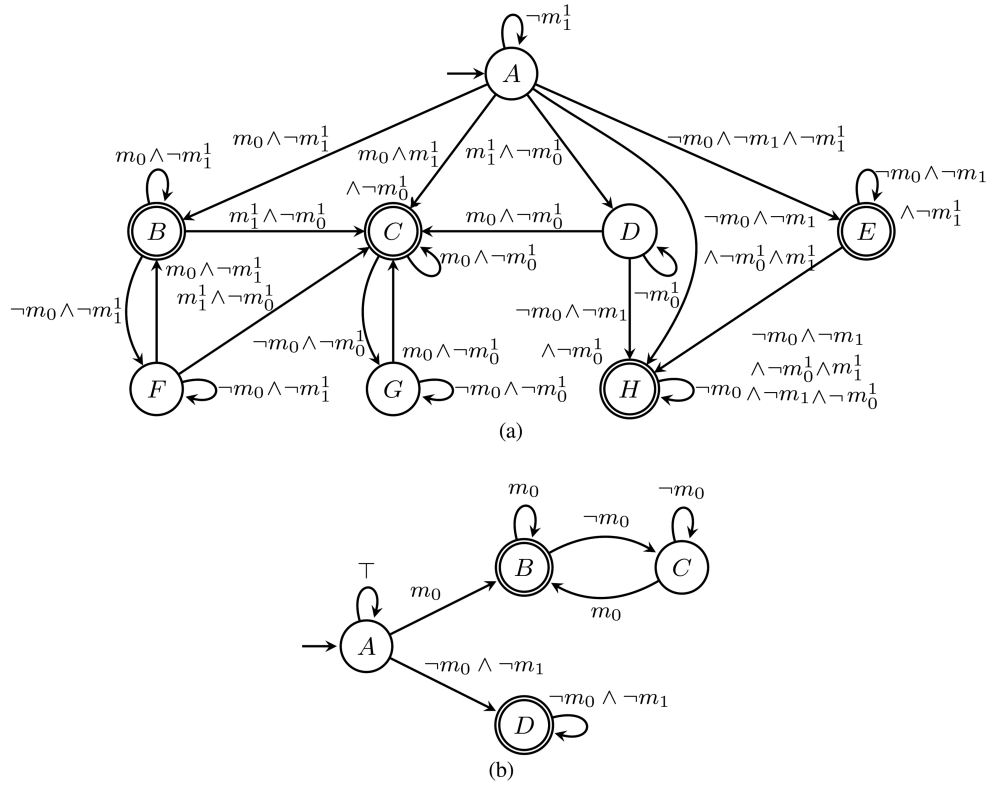


**Figure 4** NBA for specification $\varphi_1 = ((\Box\Diamond m_0 \vee m_1) \to (\Box\Diamond m_0)) \wedge (\Box(m_1^1 \to \Box m_0^1))$ and $\varphi_2 = (\Box\Diamond m_0 \vee m_1) \to (\Box\Diamond m_0)$, where $\mathcal{AP}_1 = \{m_0, m_1, m_0^1, m_1^1\}, \mathcal{AP}_2 = \{m_0^1, m_1^1\}$ and accepting states are highlighted by double circles. Here, we follow the standard abbreviation for drawing NBA over the subset of atomic propositions. For example, $\neg m_0^1$ in $\mathcal{B}_{\varphi_2}$ is the abbreviation of $\{\emptyset, m_1^1\}$ and $\neg m_0^1 \wedge m_1^1$ is the abbreviation of $\{m_1^1\}$. (a) NBA $\mathcal{B}_{\varphi_1}$; (b) NBA $\mathcal{B}_{\varphi_2}$.

**Example 6.** Consider system $G$ in Figure 1 and sensor constraint $\varphi = (\varphi_1, \varphi_2)$ which we have discussed in Example 3. We can translate $\varphi_1$ and $\varphi_2$ in $\mathcal{B}_{\varphi_1}$ and $\mathcal{B}_{\varphi_2}$, as shown in Figures 4(a) and (b), respectively. For any $i \in I$, based on $\tilde{G}_i$ and $\mathcal{B}_{\varphi_i}$, we construct the local constrained observation system $T_i$ which is partially depicted in Figures 5(a) and (b), respectively, where double circles indicate the accepting state in $Q^i_{m,T}$. Since we assume that the system is live, we know that all states appearing in Figures 5(a) and (b) are feasible. For example, we consider the finite string $s = (1, b, \epsilon)(2, c, \epsilon)(3, d, o_3)(4, e, o_1)(2, c, o_2)$ which is included in $\mathcal{L}(\tilde{G}_1)$. However, $s$ is not contained in $\mathcal{L}(T_1)$ since proposition $m_1^1$ has been satisfied by $(2, c, \epsilon)$ and then $m_0^1$ cannot hold anymore, i.e., extended event $(2, c, o_2)$ cannot occur. Hence, we have $s \notin \overline{\mathcal{L}_1^{\varphi}(G)}$.

### 5.3 Verification structure

According to Definition 3, we first construct the local verification system for each local diagnoser $D_i, i \in I$, which captures all pairs of normal strings and faulty strings that have the same observations for diagnoser $D_i$.

**Definition 6** (Local verification system)**.** For the local diagnoser $D_i$, given the local observation constrained system $T_i$, its local verification system is a new tuple

$$V_i = (Q^i_V, \Sigma^i_V, \delta^i_V, Q^i_{0,V}, Q^i_{m,V}), \tag{12}$$

where

- $Q^i_V \subseteq Q^i_T \times Q^i_T$ is the finite set of states;
- $\Sigma^i_V = \Sigma^o_{V_i} \cup \Sigma^{\text{uo}}_{V_i}$ is the finite set of events, where $\Sigma^o_{V_i} = \{(\sigma_1, \sigma_2) \in \Sigma^i_e \times \Sigma^i_e : \Theta_\Delta(\sigma_1) = \Theta_\Delta(\sigma_2) \neq \epsilon\}$, $\Sigma^{\text{uo}}_{V_i} = \{(\sigma_1, \epsilon) \in \Sigma^i_e \times \{\epsilon\} : \Theta_\Delta(\sigma_1) = \epsilon\} \cup \{(\epsilon, \sigma_2) \in \{\epsilon\} \times \Sigma^i_e : \Theta_\Delta(\sigma_2) = \epsilon\}$;
- $\delta^i_V : Q^i_V \times \Sigma^i_V \to 2^{Q^i_V}$ is the non-deterministic transition function defined by

$$\delta^i_V(q_V, \sigma_V) = \delta^i_T(q_1, \sigma_1) \times \delta^i_T(q_2, \sigma_2),$$

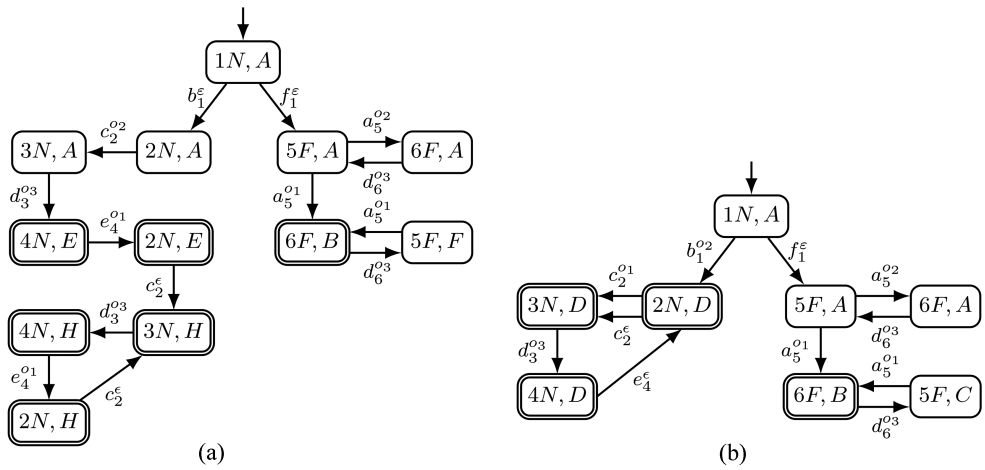


**Figure 5** Local observation constrained systems (a) $T_1$ and (b) $T_2$ for local diagnoser $D_1$ and $D_2$, where accepting states are highlighted by double circles.

for any $q_V = (q_1, q_2) \in Q_V^i$ and $\sigma_V = (\sigma_1, \sigma_2) \in \Sigma_V^i$;

- $Q_{0,V}^i = Q_{0,T}^i \times Q_{0,T}^i$ is the set of initial states;
- $Q_{m,V}^i \subseteq Q_V^i$ is the set of accepting states defined by

$$Q_{m,V}^i = \left\{(q_1, q_2) \in Q_V^i : \ q_1 \in Q_{m,T}^i \cap Q_{F,T}^i \text{ and } q_2 \in Q_{\text{feas}}^i \cap Q_{N,T}^i\right\}.$$

Essentially, the local verification system $V_i$ is a synchronization of the local observation constrained system $T_i$ and its copy based on their observations. For event $\sigma_V = (\sigma_1, \sigma_2) \in \Sigma_V^i$, $\theta_1(\sigma_V) = \sigma_1$ and $\theta_2(\sigma_V) = \sigma_2$ denote the first and second components in $\sigma_V$, respectively. Then, notations $\theta_1$ and $\theta_2$ can also be extended to strings: for any string $s = \sigma_1\sigma_2\cdots \in (\Sigma_V^i)^+$, $\theta_1(s) = \theta_1(\sigma_1)\theta_1(\sigma_2)\cdots$ and $\theta_2(s) = \theta_2(\sigma_1)\theta_2(\sigma_2)\cdots$. By construction, the local verification system $V_i$ has the following properties:

- For any $s \in \mathcal{L}^+(V_i)$, we have $s_1 = \theta_1(s), s_2 = \theta_2(s) \in \mathcal{L}^+(T_i)$ such that $\Theta_\Delta(s_1) = \Theta_\Delta(s_2)$;
- For any pair of extended strings $s_1, s_2 \in \mathcal{L}^+(T_i)$ having the same observation, i.e., $\Theta_\Delta(s_1) = \Theta_\Delta(s_2)$, we have a string $s \in \mathcal{L}^+(V_i)$ such that $\theta_1(s) = s_1$ and $\theta_2(s) = s_2$.

For the accepting state set $Q_{m,V}^i$, there are two conditions to determine if a state $q_V = (q_1, q_2)$ is included in $Q_{m,V}^i$: (i) the first component $q_1$ is faulty and accepting in $T_i$; (ii) the second component $q_2$ is the normal and feasible state. By the first condition, if an infinite string $s \in \mathcal{L}^\omega(V_i)$ can induce an infinite state sequence that visits state $q_V^i \in Q_{m,V}^i$ infinitely and the first component of string $s$ is also infinite, then this first component string will be faulty and $\varphi_i$-compatible. The second condition indicates that any finite string $s \in \mathcal{L}(V_i)$ that can induce a finite state sequence reaching a state in $Q_{m,V}^i$, the second component of $s$ is a normal string in $\overline{\mathcal{L}_i^\varphi(G)}$.

**Example 7.** Consider system $G$ under the same setting in Example 3. We have obtained the local constrained systems in Example 6, as shown in Figures 5(a) and (b). Based on local observation constrained systems $T_1$ and $T_2$, we construct the local verification systems $V_1$ and $V_2$, which are partially shown in Figures 6(a) and (b), respectively. We mark accepting states by double cycles in local verification systems, e.g., in $V_1$, state $\{(6F, B), (2N, E)\}$ is included in $Q_{m,V}^1$ since $(6F, B) \in Q_{m,T}^1 \cap Q_{F,T}^1$ and $(2N, E) \in Q_{\text{feas}}^1 \cap Q_{N,T}^1$.

Then, we need to capture possible general observations of any internal string, which requires us to consider all local outputs of local diagnosers comprehensively under the unity of common sensors. To this end, we construct the verification system.

**Definition 7** (Verification system)**.** Given system $G$ and sensor constraint $\varphi$, its verification system is a new tuple

$$V = (Q_V, \Sigma_V, \delta_V, Q_{0,V}), \tag{13}$$

where

- $Q_V = Q_V^1 \times Q_V^2 \times \cdots \times Q_V^\kappa$ is the finite set of states;

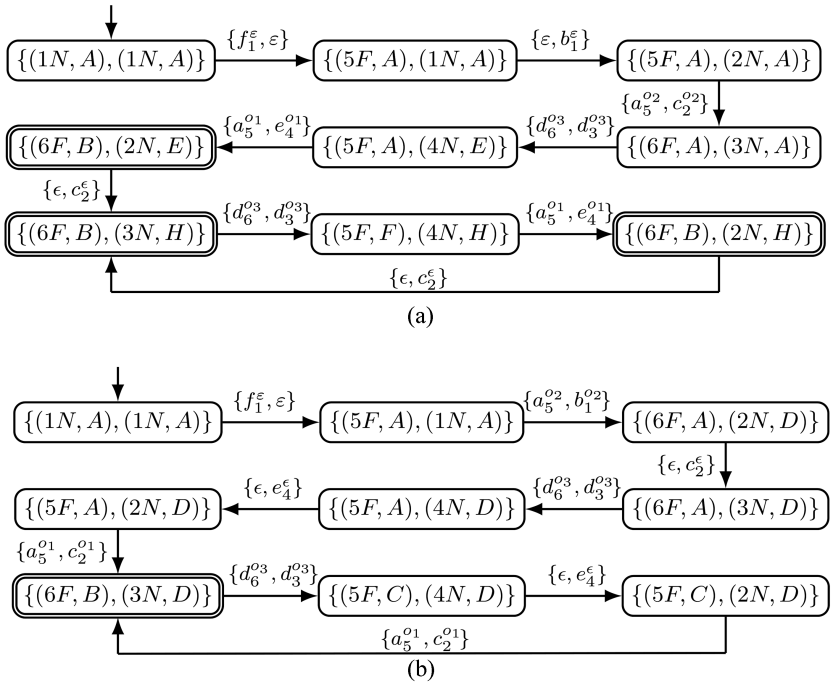


**Figure 6** Local verification system. (a) $V_1$; (b) $V_2$.

• $\Sigma_V \subseteq (\Sigma_V^1 \cup \{\epsilon\}) \times (\Sigma_V^2 \cup \{\epsilon\}) \times \cdots \times (\Sigma_V^{\boldsymbol{\kappa}} \cup \{\epsilon\}) \setminus (\epsilon, \ldots, \epsilon)$ is the set of events, which is defined by

$$\begin{aligned}\Sigma_V =&\{((\sigma_1^l, \sigma_1^r), \ldots, (\sigma_{\boldsymbol{\kappa}}^l, \sigma_{\boldsymbol{\kappa}}^r)) \in (\Sigma_V^1 \cup \{\epsilon\}) \times \cdots \times (\Sigma_V^{\boldsymbol{\kappa}} \cup \{\epsilon\}) \setminus (\epsilon, \ldots, \epsilon) :\\ &\Theta_\Sigma(\sigma_1^l) = \cdots = \Theta_\Sigma(\sigma_{\boldsymbol{\kappa}}^l) \wedge (\Theta_\Sigma(\sigma_1^l) \in \Sigma_c \to \Theta_\Delta(\sigma_1^l) = \cdots = \Theta_\Delta(\sigma_{\boldsymbol{\kappa}}^l))\};\end{aligned}$$

• $\delta_V : Q_V \times \Sigma_V \to 2^{Q_V}$ is the non-deterministic transition function;
• $Q_{0,V} = Q_{0,V}^1 \times \cdots \times Q_{0,V}^{\boldsymbol{\kappa}}$ is the set of initial states.

The non-deterministic transition function $\delta_V$ is defined as follows: for any $q_V = (q_1, \ldots, q_{\boldsymbol{\kappa}}) \in Q_V$ and $\sigma_V = (\sigma_1, \ldots, \sigma_{\boldsymbol{\kappa}}) \in \Sigma_V$, we have $\delta_V(q_V, \sigma_V)!$, if and only if, for each $i \in I$, $\delta_V^i(q_i, \sigma_i)!$ if $\sigma_i \neq \epsilon$. Then, if $\delta_V(q_V, \sigma_V)!$, we have $\delta_V(q_V, \sigma_V) = (q_1', \ldots, q_{\boldsymbol{\kappa}}')$, where, for $i \in I$,

$$q_i' = \begin{cases} \delta_V^i(q_i, \sigma_i), & \text{if } \sigma_i \neq \epsilon,\\ q_i, & \text{otherwise.}\end{cases}$$

Intuitively, the event set $\Sigma_V$ is a subset of $(\Sigma_V^1 \cup \{\epsilon\}) \times (\Sigma_V^2 \cup \{\epsilon\}) \times \cdots \times (\Sigma_V^{\boldsymbol{\kappa}} \cup \{\epsilon\})$ eliminating the case that all components are empty string, i.e., $(\epsilon, \ldots, \epsilon)$. An event $\sigma_V = ((\sigma_1^l, \sigma_1^r), \ldots, (\sigma_{\boldsymbol{\kappa}}^l, \sigma_{\boldsymbol{\kappa}}^r))$ is included in $\Sigma_V$ whenever (i) all extended events $\sigma_i^l, i \in I$, have the same internal event, i.e., $\Theta_\Sigma(\sigma_1^l) = \cdots = \Theta_\Sigma(\sigma_{\boldsymbol{\kappa}}^l)$; (ii) if the internal event of $\sigma_1^l$ is observed by common sensors, the external output of each event $\sigma_i^l, i \in I$, are the same. The first condition makes the verification system capture the observation received by different local diagnosers at the meantime when the original system executes a faulty string. The second condition ensures the outputs of events that are observed by common sensors are the same for all local diagnosers, which models the broadcast of common sensors. For state $q_V = (q_1, \ldots, q_{\boldsymbol{\kappa}}) \in Q_V$, $q_V[i] = q_i$ is the $i$th component in $q_V$; similarly, for event $\sigma_V = (\sigma_1 \cdots \sigma_{\boldsymbol{\kappa}})$, $\sigma_V[i] = \sigma_i$ is the $i$th component in $\sigma_V$, where $i = 1, \ldots, \boldsymbol{\kappa}$. For string $s_V = (\sigma_{1,1}, \ldots, \sigma_{1,\boldsymbol{\kappa}})(\sigma_{2,1}, \ldots, \sigma_{2,\boldsymbol{\kappa}}) \cdots \in \mathcal{L}^+(V)$, $s_V^i = \sigma_{1,i}\sigma_{2,i} \cdots$ is the $i$th-column string of $s_V$. For a state sequence $\gamma_V = (q_{1,1}, \ldots, q_{1,\boldsymbol{\kappa}})(q_{2,1}, \ldots, q_{2,\boldsymbol{\kappa}}) \cdots \in (Q_V)^+$, $\gamma_V^i = q_{1,i}q_{2,i} \cdots \in (Q_V^i)^+$ is the $i$th-column state sequence of $\gamma_V$. By construction, $V$ has the following properties:

• Consider any $s_V \in \mathcal{L}(V)$. For any $i \in I$, we have $s_V^i \in \mathcal{L}(V_i)$ and the following conditions hold: $\Theta_\Sigma(\theta_1(s_V^1)) = \cdots = \Theta_\Sigma(\theta_1(s_V^{\boldsymbol{\kappa}}))$; $(\forall j \in \mathbb{N})(\Theta_\Sigma(\theta_1(s_V^1)[j]) \in \Sigma_c \to \Theta_\Delta(\theta_1(s_V^1)[j]) = \cdots = \Theta_\Delta(\theta_1(s_V^{\boldsymbol{\kappa}})[j]))$.
• For all $i \in I$ and $s_i \in \mathcal{L}^+(V_i)$, if the following conditions hold: $\Theta_\Sigma(\theta_1(s_1)) = \cdots = \Theta_\Sigma(\theta_1(s_{\boldsymbol{\kappa}}))$ and $(\forall j \in \mathbb{N})(\Theta_\Sigma(\theta_1(s_1)[j]) \in \Sigma_c \to \Theta_\Delta(\theta_1(s_1)[j]) = \cdots = \Theta_\Delta(\theta_1(s_{\boldsymbol{\kappa}})[j]))$, there exists $s_V \in \mathcal{L}^+(V)$ such that $s_V^i = s_i$ for any $i \in I$.

### 5.4 Checking $\varphi$-codiagnosability

Now, we show how to verify $\varphi$-codiagnosability by using the verification system $V$. For a verification system $V$, a run in $V$ is a finite sequence $\pi = q_V^1 \xrightarrow{\sigma_V^1} q_V^2 \xrightarrow{\sigma_V^2} \cdots \xrightarrow{\sigma_V^{n-1}} q_V^n$, where $q_V^i \in Q_V, \sigma_V^i \in \Sigma_V$ and $q_V^{i+1} \in \delta_V(q_V^i, \sigma_V^i)$, for $i = 1, \ldots, n-1$. A run is called a cycle if its first state is the same as its last state, i.e., $q_V^1 = q_V^n$. A cycle $\pi$ is reachable if there exists an initial state $q_{0,V} \in Q_{0,V}$ and a finite string $s \in (\Sigma_V)^*$ such that $V$ can reach state $q_V^1$ driven by string $s$ from state $q_{0,V}$, i.e., $q_V^1 \in \delta_V(q_{0,V}, s)$.

We are ready to present the necessary and sufficient conditions for verifying $\varphi$-codiagnosability.

**Theorem 2.** System $G$ is not $\varphi$-codiagnosable w.r.t. fault events $\Sigma_F$, local observation mappings $\{\mathcal{P}_i\}_{i\in I}$ and sensor constraint $\varphi$, if and only if, in the verification system $V$, there exists a reachable cycle

$$\pi = q_V^1 \xrightarrow{\sigma_V^1} q_V^2 \xrightarrow{\sigma_V^2} \cdots \xrightarrow{\sigma_V^{n-1}} q_V^n$$

such that

(1) $\theta_1(\sigma_V^i[1]) \neq \epsilon$ for some $i = 1, \ldots, n-1$;

(2) for any $i \in I$, there exists $q_V^j[i] \in Q_{m,V}^i$ for some $j = 1, \ldots, n-1$.

*Proof.* ($\Leftarrow$) Assume there is a reachable cycle $\pi' = q_V^1 \xrightarrow{\sigma_V^1} q_V^2 \xrightarrow{\sigma_V^2} \cdots \xrightarrow{\sigma_V^{n-1}} q_V^n$ in the verification system $V$ such that for some $i = 1, \ldots, n-1$, $\theta_1(\sigma_V^i[1]) \neq \epsilon$ and for any $i \in I$, there exists $q \in Q_{m,V}^i$ such that $q_V^j[i] = q$ for some $j = 1, \ldots, n$, but the system $G$ is $\varphi$-codiagnosable. Let $s_{V,2} = \sigma_V^1\sigma_V^2 \cdots \sigma_V^{n-1}$. Since cycle $\pi'$ is reachable, we can find a string $s_{V,1} \in \mathcal{L}(V)$ such that $q_V^1 \in \delta_V(q_{0,V}, s_{V,1})$ where $q_{0,V} \in Q_{0,V}$. After repeating the cycle infinitely, we obtain an infinite string $s_V = s_{V,1}(s_{V,2})^\omega \in \mathcal{L}^\omega(V)$, Since there exists $i = 1, \ldots, n-1$ such that $\theta_1(\sigma_V^i[1]) \neq \epsilon$, by the definition of $\Sigma_V$, we know that $\theta_1(\sigma_V^i[j]) \neq \epsilon$ for any $j \in I$. Thus, the first component $s_l^j = \theta_1(s_V^j)$ of sequence $s_V^j$ is an infinite extended string. Along $s_V$ we get an infinite run $\pi = q_V^0 \xrightarrow{\sigma_V^0} \cdots (q_V^1 \xrightarrow{\sigma_V^1} q_V^2 \xrightarrow{\sigma_V^2} \cdots \xrightarrow{\sigma_V^{n-1}} q_V^n)^\omega$. From run $\pi$, we can extract the state sequence $\gamma_V = q_V^0 \cdots (q_V^1 \cdots q_V^n)^\omega$. For any $i$th-column state sequence $\gamma_V^i = q_V^0[i] \cdots (q_V^1[i] \cdots q_V^n[i])^\omega$ of $\gamma_V$, where $i \in I$, an accepting state $q_V^j[i] \in Q_{m,V}^i$ appears infinitely for some $j = 1, \ldots, n$, i.e., $\mathsf{Inf}(\gamma_V^i) \cap Q_{m,V}^i \neq \emptyset$, which means infinite string $s_V^i$ is an accepting in local verification system $V_i$. By definition of $Q_{m,V}^i$, we know that $\theta_1(q_V^j[i]) \in Q_{m,T}^i \cap Q_{F,T}^i$ and $s_l^i = \theta_1(s_V^i)$ is faulty and accepting in system $T_i$, that is, $s_l^i \in \mathcal{L}_i^\varphi(G)$. On the other hand, by $\theta_2(q_V^j[i]) \in Q_{\text{feas},T}^i \cap Q_{N,T}^i$ and (10), the second component string $s_r^i = \theta_2(s_V^i)$ is normal and every prefix of $s_r^i$ is a prefix of an accepting string of $T_i$, that is, $\forall v \in \overline{\{s_r^i\}}, v \in \overline{\mathcal{L}_i^\varphi(G)}$ and $\Sigma_{e,F}^i \notin v$. Thus, by the first property of the local verification system, for any finite prefix $t \in \overline{\{s_l^i\}}$, there exists $v \in \overline{\{s_r^i\}} \subseteq \overline{\mathcal{L}_i^\varphi(G)}$ and $\Sigma_{e,F}^i \notin v$ such that $\Theta_\Delta(t) = \Theta_\Delta(v) \in \mathcal{M}_i(\Theta_\Sigma(v))$. Let $s = \Theta_\Sigma(\theta_1(s_V^1)) = \cdots = \Theta_\Sigma(\theta_1(s_V^{\boldsymbol{\kappa}}))$. Then, we can obtain a general observation $(\rho_1, \rho_2, \ldots, \rho_{\boldsymbol{\kappa}}) \in \Delta_1^+ \times \cdots \times \Delta_{\boldsymbol{\kappa}}^+$ such that for any $i \in I$, $\rho_i = \Theta_\Delta(s_l^i)$. By the first property of the verification system $V$, we know that this general observation $(\rho_1, \rho_2, \ldots, \rho_{\boldsymbol{\kappa}}) \in \mathcal{M}^\varphi(s)$. Thus, for any $i \in I$ and any prefix $\rho \in \overline{\{\rho_i\}}$, there is $v \in \overline{\{\Theta_\Sigma(s_r^i)\}} \in \mathcal{L}(G)$ such that $\rho \in \mathcal{M}_i(v)$ and $\Sigma_F \notin v$, that is, $G$ is not $\varphi$-codiagnosable.

($\Rightarrow$) Suppose the system $G$ is not $\varphi$-codiagnosable. That is, there exists an infinite faulty string $s \in \mathcal{L}_F^\omega(G)$ and a general observation $(\rho_1, \rho_2, \ldots, \rho_{\boldsymbol{\kappa}}) \in \mathcal{M}^\varphi(s)$ such that for any $i \in I$ and any prefix $\rho \in \overline{\{\rho_i\}}$, we can find a normal string $v \in \mathcal{L}(G)$ that can output the observation $\rho$ for local diagnoser $D_i$, i.e.,

$$\begin{aligned}&(\exists s \in \mathcal{L}_F^\omega(G))(\exists(\rho_1, \rho_2, \ldots, \rho_{\boldsymbol{\kappa}}) \in \mathcal{M}^\varphi(s))(\forall i \in I)\\ &(\forall \rho \in \overline{\{\rho_i\}}) : [(\exists v \in \mathcal{L}(G))(\rho \in \mathcal{M}_i(v) \wedge \Sigma_F \notin v)].\end{aligned} \tag{14}$$

Thus, for infinite faulty string $s \in \mathcal{L}_F^\omega(G)$, by (5), there is $(s_1, s_2, \ldots, s_{\boldsymbol{\kappa}}) \in \mathcal{L}_1^\varphi(G) \times \cdots \times \mathcal{L}_{\boldsymbol{\kappa}}^\varphi(G)$ such that (i) for any $i \in I$, we have $\Theta_\Sigma(s_i) = s$ and $\Theta_\Delta(s_i) = \rho_i$; (ii) for any $j \in \mathbb{N}$ such that if $s[j] \in \Sigma_c$, we have that $\Theta_\Delta(s_1[j]) = \Theta_\Delta(s_2[j]) = \cdots = \Theta_\Delta(s_{\boldsymbol{\kappa}}[j]))$. By (14), for any $i \in I$ and any prefix $t_i \in \overline{\{s_i\}}$, there exists a normal string $v \in \mathcal{L}(G)$ and $v_i \in \overline{\mathcal{L}_i^\varphi(G)}$ such that $\Theta_\Sigma(v_i) = v$ and $\Theta_\Delta(t_i) = \Theta_\Delta(v_i)$. By (10), we have $\delta_T^i(q_0, v_i) \cap Q_{\text{feas}}^i \neq \emptyset$. Thus, for any $i \in I$, by $\mathcal{L}_m^\omega(T_i) = \mathcal{L}_i^\varphi(G)$ and the second condition of the local verification system, there exists an infinite string $s_{V_i}$ in local verification system $V_i$ such that $\theta_1(s_{V_i}) = s_i$ and $s_{V_i}$ visits accepting states in $q \in Q_{m,V}^i$ by event $\sigma \in \{\sigma_{V_i} \in \Sigma_V^i : \theta_1(\sigma_{V_i}) \neq \epsilon\}$ for infinite times. By

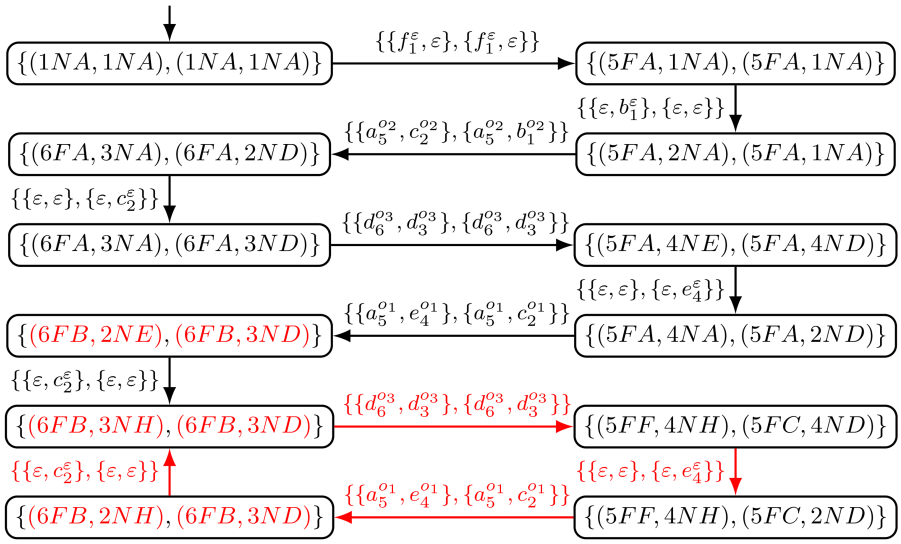


**Figure 7** (Color online) Verification system $V$. For each state, the $i$th component is highlighted in red color if it is included in $Q^i_{m,V}$.

the second property of verification system $V$, there is $s_V \in \mathcal{L}^\omega(V)$ such that, for any $i \in I$, $s^i_V = s_{V_i}$ and $s_V$ visits states in $q \in \{q_V \in Q_V : q_V[i] \in Q^i_{m,V}\}$ by event $\sigma \in \{\sigma_V \in \Sigma_V : \theta_1(\sigma_V[i]) \neq \epsilon\}$ for infinite times. For any $\sigma_V \in \Sigma_V$, since $\Theta_\Sigma(\theta_1(\sigma_V[1])) = \cdots = \Theta_\Sigma(\theta_1(\sigma_V[\boldsymbol{\kappa}])$, the set $\{\sigma_V \in \Sigma_V : \theta_1(\sigma_V[i]) \neq \epsilon\}$ is equivalent to set $\{\sigma_V \in \Sigma_V : \theta_1(\sigma_V[1]) \neq \epsilon\}$. Finally, since the verification system $V$ is finite, by the pigeonhole principle, there exists a cycle $\pi = q^1_V \xrightarrow{\sigma^1_V} q^2_V \xrightarrow{\sigma^2_V} \cdots \xrightarrow{\sigma^{n-1}_V} q^n_V$ such that for any $i \in I$, there exists $j = 1, \ldots, n$ such that $q^j_V[i] \in Q^i_{m,V}$ and $\theta_1(\sigma^j_V[1]) \neq \epsilon$.

**Example 8.** Again, we consider the running example $G$ in Figure 1. As we have discussed in Example 4, system $G$ is not $\varphi$-codiagnosable under the setting in Example 3. We analyze this result more formally through Theorem 2. Based on the local verification systems $V_1$ and $V_2$, which have been constructed in Example 7, we construct the verification system $V$, which is partially shown in Figure 7. For each state, we highlight its component by red color if this component is included in $Q^i_{m,V}$, e.g., component $(6FB, 3NH)$ in state $\{(6FB, 3NH), (6FB, 3ND)\}$ is accepting in local verification $V_1$ and is highlighted by red color. Due to space constraint, we only focus on the reachable cycle satisfying conditions in Theorem 2 and omit other parts without loss of generality for the purpose of falsifying $\varphi$-codiagnosability. Specifically, let us consider the cycle highlighted with red arrows in Figure 7, i.e.,

$$\{(6FB, 3NH), (6FB, 3ND)\} \xrightarrow{\{(d_6^{o3}, d_3^{o3}), (d_6^{o3}, d_3^{o3})\}} \{(5FF, 4NH), (5FC, 4ND)\}$$
$$\xrightarrow{\{(\varepsilon,\varepsilon), (\varepsilon, e_4^\varepsilon)\}} \{(5FF, 4NH), (5FC, 2ND)\} \xrightarrow{\{(a_5^{o1}, e_4^{o1}), (a_5^{o1}, c_2^{o1})\}}$$
$$\{(6FB, 2NH), (6FB, 3ND)\} \xrightarrow{\{(\varepsilon, c_2^\varepsilon), (\varepsilon, \varepsilon)\}} \{(6FB, 3NH), (6FB, 3ND)\}.$$

Note that for state $q^1_V = \{(6FB, 3NH), (6FB, 3ND)\}$, its first component $q^1_V[1] = (6FB, 3NH) \in Q^1_{m,V}$ and second component $q^1_V[2] = (6FB, 3ND) \in Q^2_{m,V}$, and there exists event $\sigma^1_V = \{(d_6^{o3}, d_3^{o3})(d_6^{o3}, d_3^{o3})\}$ such that $\theta_1(\sigma^1_V[1]) \neq \epsilon$. Thus, system $G$ is not $\varphi$-codiagnosable according to Theorem 2.

**Remark 4.** We conclude this section by discussing the complexity of the proposed algorithm to verify $\varphi$-codiagnosability. Note that, for $i \in I$, the local augmented system $\tilde{G}_i$ contains at most $2|Q|$ states and $|\Sigma^i_e| = |Q| \cdot [|\Sigma_c| \cdot (|\Delta_c| + 1) + |\Sigma_l| \cdot (|\Delta^i_l| + 1)]$ events. The local observation constrained system $T_i$ is constructed by composing local augmented system $\tilde{G}_i$ and NBA $\mathcal{B}_{\varphi_i}$. Therefore, $T_i$ is consist of at most $2|Q| \cdot |X_i|$ states, where $|X_i|$ is the number of states in NBA $\mathcal{B}_{\varphi_i}$. It is known that $\mathcal{B}_{\varphi_i}$ has at most $2^{|\varphi_i|} \cdot |\varphi_i|$ states, where $|\varphi_i|$ is the number of operators in formula $\varphi_i$ [45]. Then the local verification system $V_i$ contains at most $4|Q|^2 \cdot |X_i|^2$ states and $(|\Sigma^i_e| + 1)^2 - 1$ events. As a result, the verification $V$ has at most $4^{\boldsymbol{\kappa}}|Q|^{2\boldsymbol{\kappa}} \cdot \prod_{i=1}^{\boldsymbol{\kappa}} |X_i|^2$ states and $\prod_{i=1}^{\boldsymbol{\kappa}}(|\Sigma^i_e| + 1)^2 - 1$ events. Thus, there are at most $4^{\boldsymbol{\kappa}}|Q|^{2\boldsymbol{\kappa}} \cdot \prod_{i=1}^{\boldsymbol{\kappa}} |X_i|^2 \cdot [\prod_{i=1}^{\boldsymbol{\kappa}}(|\Sigma^i_e| + 1)^2 - 1]$ transitions in $V$. Finally, checking whether there exists a cycle satisfying conditions in Theorem 2 is a cycle search problem whose complexity is polynomial in the size

of verification system $V$ [49]. Overall, the complexity of our approach is polynomial in the size of system $G$, and exponential in the length of the sensor constraint formula $\varphi_i$ and the number of local diagnosers.

## 6 Conclusion

In this paper, we provided a uniform framework for the analysis of a robust decentralized diagnosis problem for DES, in which local diagnosers may share common sensors. To this end, we applied LTL formulae as a systematic tool to describe constraints for private sensors of local diagnosers and common sensors, respectively. We proposed a new notion termed as $\varphi$-codiagnosability as the necessary and sufficient condition for the existence of a decentralized diagnoser working correctly under LTL-based sensor constraint. Then an effective verification procedure of $\varphi$-codiagnosability was provided. Our method not only can capture different types of sensor failures of local diagnoser flexibly, but also supports to analyze the effect of common sensors on diagnosis. In the existing literature, decentralized diagnosis methods in DES models have been applied to telecommunication networks [50], railway transportation systems [51] and automated manufacturing systems [52–54]. Extending our theoretical results to real-world systems is under investigation as future work.

**Acknowledgements** This work was supported by National Natural Science Foundation of China (Grant Nos. 62173226, 92367203, 62061136004).

**References**

1 Cassandras C, Lafortune S. Introduction to Discrete Event Systems. Boston: Springer, 2021
2 Sampath M, Sengupta R, Lafortune S, et al. Diagnosability of discrete-event systems. IEEE Trans Automat Contr, 1995, 40: 1555–1575
3 Lin F. Diagnosability of discrete event systems and its applications. Discrete Event Dyn Syst, 1994, 4: 197–212
4 Lin F, Wang L Y, Chen W, et al. N-diagnosability for active on-line diagnosis in discrete event systems. Automatica, 2017, 83: 220–225
5 Yin X, Lafortune S. On the decidability and complexity of diagnosability for labeled Petri nets. IEEE Trans Automat Contr, 2017, 62: 5931–5938
6 Basile F, Cabasino M P, Seatzu C. Diagnosability analysis of labeled time Petri net systems. IEEE Trans Automat Contr, 2017, 62: 1384–1396
7 Lefebvre D, Delherm C. Diagnosis of DES with Petri net models. IEEE Trans Automat Sci Eng, 2007, 4: 114–118
8 Takai S, Kumar R. A generalized framework for inference-based diagnosis of discrete event systems capturing both disjunctive and conjunctive decision-making. IEEE Trans Automat Contr, 2017, 62: 2778–2793
9 Ran N, Su H, Giua A, et al. Codiagnosability analysis of bounded Petri nets. IEEE Trans Automat Contr, 2018, 63: 1192–1199
10 Yin X, Chen J, Li Z, et al. Robust fault diagnosis of stochastic discrete event systems. IEEE Trans Automat Contr, 2019, 64: 4237–4244
11 Hu Y, Ma Z, Li Z, et al. Diagnosability enforcement in labeled Petri nets using supervisory control. Automatica, 2021, 131: 109776
12 Ma Z, Yin X, Li Z. Marking diagnosability verification in labeled Petri nets. Automatica, 2021, 131: 109713
13 Pencole Y, Subias A. Diagnosability of event patterns in safe labeled time Petri nets: a model-checking approach. IEEE Trans Automat Sci Eng, 2022, 19: 1151–1162
14 Su R. A language-based diagnosis framework for permanent and intermittent faults. Automatica, 2023, 154: 111077
15 Zaytoon J, Lafortune S. Overview of fault diagnosis methods for discrete event systems. Annu Rev Control, 2013, 37: 308–320
16 Lafortune S, Lin F, Hadjicostis C N. On the history of diagnosability and opacity in discrete event systems. Annu Rev Control, 2018, 45: 257–266
17 Basilio J C, Hadjicostis C N, Su R. Analysis and control for resilience of discrete event systems: fault diagnosis, opacity and cyber security. FNT Syst Control, 2021, 8: 285–443
18 Debouk R, Lafortune S, Teneketzis D. Coordinated decentralized protocols for failure diagnosis of discrete event systems. Discrete Event Dynamic Syst, 2000, 10: 33–86
19 Qiu W B, Kumar R. Decentralized failure diagnosis of discrete event systems. IEEE Trans Syst Man Cybern A, 2006, 36: 384–395
20 Wang Y, Yoo T S, Lafortune S. Diagnosis of discrete event systems using decentralized architectures. Discrete Event Dyn Syst, 2007, 17: 233–263
21 Viana G S, Basilio J C. Codiagnosability of discrete event systems revisited: a new necessary and sufficient condition and its applications. Automatica, 2019, 101: 354–364
22 Wang W, Girard A R, Lafortune S, et al. On codiagnosability and coobservability with dynamic observations. IEEE Trans Automat Contr, 2011, 56: 1551–1566
23 Yin X, Lafortune S. Codiagnosability and coobservability under dynamic observations: transformation and verification. Automatica, 2015, 61: 241–252
24 Takai S, Kumar R. Implementation of inference-based diagnosis: computing delay bound and ambiguity levels. Discrete Event Dyn Syst, 2018, 28: 315–348
25 Yokota S, Yamamoto T, Takai S. Computation of the delay bounds and synthesis of diagnosers for decentralized diagnosis with conditional decisions. Discrete Event Dyn Syst, 2017, 27: 45–84
26 Carvalho L K, Basilio J C, Moreira M V. Robust diagnosis of discrete event systems against intermittent loss of observations. Automatica, 2012, 48: 2068–2078
27 Takai S, Ushio T. Verification of codiagnosability for discrete event systems modeled by mealy automata with nondeterministic output functions. IEEE Trans Automat Contr, 2012, 57: 798–804
28 Nunes C E V, Moreira M V, Alves M V S, et al. Codiagnosability of networked discrete event systems subject to communication delays and intermittent loss of observation. Discrete Event Dyn Syst, 2018, 28: 215–246

29 Carvalho L K, Moreira M V, Basilio J C, et al. Robust diagnosis of discrete-event systems against permanent loss of observations. Automatica, 2013, 49: 223–231
30 Tomola J H A, Cabral F G, Carvalho L K, et al. Robust disjunctive-codiagnosability of discrete-event systems against permanent loss of observations. IEEE Trans Automat Contr, 2017, 62: 5808–5815
31 Kanagawa N, Takai S. Diagnosability of discrete event systems subject to permanent sensor failures. Int J Control, 2015, 88: 2598–2610
32 Wada A, Takai S. Decentralized diagnosis of discrete event systems subject to permanent sensor failures. Discrete Event Dyn Syst, 2022, 32: 159–193
33 Oliveira V S L, Cabral F G, Moreira M V. K-loss robust codiagnosability of discrete-event systems. Automatica, 2022, 140: 110222
34 Carvalho L K, Moreira M V, Basilio J C. Comparative analysis of related notions of robust diagnosability of discrete-event systems. Annu Rev Control, 2021, 51: 23–36
35 Carvalho L K, Moreira M V, Basilio J C. Generalized robust diagnosability of discrete event systems. IFAC Proc Volumes, 2011, 44: 8737–8742
36 Takai S. A general framework for diagnosis of discrete event systems subject to sensor failures. Automatica, 2021, 129: 109669
37 Dong W, Yin X, Li S. A uniform framework for diagnosis of discrete-event systems with unreliable sensors using linear temporal logic. IEEE Trans Automat Contr, 2024, 69: 145–160
38 Ushio T, Takai S. Nonblocking supervisory control of discrete event systems modeled by mealy automata with nondeterministic output functions. IEEE Trans Automat Contr, 2016, 61: 799–804
39 Jiang S, Kumar R. Failure diagnosis of discrete-event systems with linear-time temporal logic specifications. IEEE Trans Automat Contr, 2004, 49: 934–945
40 Chen J, Kumar R. Fault detection of discrete-time stochastic systems subject to temporal logic correctness requirements. IEEE Trans Automat Sci Eng, 2015, 12: 1369–1379
41 Bittner B, Bozzano M, Cimatti A, et al. Diagnosability of fair transition systems. Artif Intell, 2022, 309: 103725
42 Tuxi T M, Carvalho L K, Nunes E V L, et al. Diagnosability verification using LTL model checking. Discrete Event Dyn Syst, 2022, 32: 399–433
43 Alves M V S, da Cunha A E C, Carvalho L K, et al. Robust supervisory control of discrete event systems against intermittent loss of observations. Int J Control, 2021, 94: 2008–2020
44 Lin F. Control of networked discrete event systems: dealing with communication delays and losses. SIAM J Control Optim, 2014, 52: 1276–1298
45 Baier C, Katoen J. Principles of Model Checking. London: MIT Press, 2008
46 Giannakopoulou D, Lerda F. From states to transitions: improving translation of LTL formulae to Büchi automata. In: Proceedings of International Conference on Formal Techniques for Networked and Distributed Systems, 2002. 308–326
47 Oliveira V S L, Cabral F G, Moreira M V. K-loss robust diagnosability of discrete-event systems. IFAC-PapersOnLine, 2020, 53: 250–255
48 Dong W, Gao S, Yin X, et al. Fault diagnosis of discrete-event systems under non-deterministic observations with output fairness. In: Proceedings of the 61st IEEE Conference on Decision and Control (CDC), 2022. 4256–4262
49 Tarjan R. Depth-first search and linear graph algorithms. SIAM J Comput, 1972, 1: 146–160
50 Pencolé Y, Cordier M O. A formal framework for the decentralised diagnosis of large scale discrete event systems and its application to telecommunication networks. Artif Intell, 2005, 164: 121–170
51 Le Mortellec A, Clarhaut J, Sallez Y, et al. Embedded holonic fault diagnosis of complex transportation systems. Eng Appl Artif Intell, 2013, 26: 227–240
52 Cabasino M P, Giua A, Pocci M, et al. Discrete event diagnosis using labeled Petri nets. An application to manufacturing systems. Control Eng Pract, 2011, 19: 989–1001
53 Veras M Z M, Cabral F G, Moreira M V. Distributed synchronous diagnosis of discrete event systems modeled as automata. Control Eng Pract, 2021, 115: 104892
54 Mayer P C, Cabral F G, Moreira M V. A protocol for decentralized synchronous diagnosis with coordination. Control Eng Pract, 2023, 141: 105732