Reliable Decentralized Failure Diagnosis of Discrete Event Systems

Shuhei NAKATA * and Shigemasa TAKAI *

Abstract: In most existing works on decentralized diagnosis of discrete event systems, it is implicitly assumed that diagnosis decisions of all local diagnosers are available to detect the failure. However, it may be possible that some local diagnosis decisions are not available due to some causes. Letting \( n \) be the number of local diagnosers, the notion of \((n,k)\)-reliable codiagnosability guarantees that any occurrence of the failure can be detected by using arbitrary more than or equal to \( k \) local diagnosis decisions within a uniformly bounded number of steps. In other words, even if at most \( n - k \) local diagnosis decisions are not available, the failure can be detected by using the remaining diagnosis decisions.

In this paper, a method for verifying \((n,k)\)-reliable codiagnosability for any \( k \) is presented. Then, the delay bound within which any occurrence of the failure can be detected by using arbitrary more than or equal to \( k \) local diagnosis decisions is computed.

Key Words: discrete event system, decentralized diagnosis, reliable codiagnosability, verification, delay bound.

1. Introduction

Failure diagnosis is one of the active research topics for discrete event systems (DESs). A language based approach for failure diagnosis of DESs is proposed in [1]. In this approach, the failure is represented by the occurrence of an unobservable failure event, and the task of a diagnoser is to detect any occurrence of a failure event within a uniformly bounded number of steps. The diagnosability property introduced in [1] guarantees that this required task can be performed by a diagnoser. Polynomial algorithms for verifying diagnosability are developed in [2]–[4]. Diagnosability allows the existence of a finite delay in detection of the failure. For a diagnosable system, it is important to compute the delay bound within which any occurrence of the failure can be detected. In [4], this delay bound is computed by finding the shortest path in a certain weighted directed graph.

The approach of [1] has been extended to decentralized failure diagnosis where \( n \) local diagnosers jointly perform the task of diagnosis [5]. In [6], decentralized failure diagnosis is studied in a general case where a nonfailure specification language is specified, and the failure is modeled by violation of the specification language. A notion of codiagnosability is defined to characterize a class of diagnosable systems in the decentralized setting, and an algorithm for verifying codiagnosability is developed [6]. The computational complexity for verifying codiagnosability based on the abstracted models are derived [8]. Further, several extended versions of codiagnosability have been studied [9]–[15]. Also, for a codiagnosable system, computation of the delay bound is studied [6].

In the previous works on decentralized diagnosis mentioned above, it is implicitly assumed that diagnosis decisions of all local diagnosers are available to detect the failure. However, it may be possible that some local diagnosis decisions are not available due to some causes including breakdown of local diagnosers and disconnection of the network. In the context of supervisory control of DESs initiated by Ramadge and Wonham [16], a reliable decentralized supervisory control problem is formulated in [17]. This problem requires synthesizing a decentralized supervisor which achieves the legal behavior even if control decisions of some local supervisors are not available. When \( n \) is the number of local supervisors, the notion of \((n,k)\)-reliable coobservability \((1 \leq k \leq n)\) introduced in [17] guarantees that, for each controllable event, there are at least \( n - k + 1 \) local supervisors which make the correct control decisions. In other words, even if at most \( n - k \) local control decisions are not available, the correct control actions can be determined by using the remaining control decisions. In this sense, the decentralized supervisor has reliability. Verification of \((n,k)\)-reliable coobservability is studied in [18].

In [19], reliable decentralized failure diagnosis is firstly studied. Letting \( n \) be the number of local diagnosers, the notion of \( R_l \)-robust codiagnosability \((1 \leq l < n)\) is introduced to characterize a class of systems for which any occurrence of an unobservable failure event can be detected even if diagnosis decisions of arbitrary \( l \) local diagnosers are not available. An efficient algorithm for verifying \( R_1 \)-robust codiagnosability in the presence of codiagnosability is developed. In this paper, a notion of \((n,k)\)-reliable codiagnosability, which is equivalent to \( R_{n-k} \)-robust codiagnosability, is introduced in the general case where the failure is modeled by violation of the specification language, and a method for verifying \((n,k)\)-reliable codiagnosability for any \( k \) is presented without assuming that codiagnosability holds. Therefore, the verification result of this paper is more general than that of [19]. Further, the delay bound is computed in the case where arbitrary more than or equal to \( k \) local diagnosis decisions are available. Note that computation of the delay bound is not addressed in [19].
2. Preliminaries

A DES to be diagnosed is modeled by an automaton $G = (X, \Sigma, \alpha, x_0)$, where $X$ is the set of states, $\Sigma$ is the finite set of events, $\alpha : X \times \Sigma \rightarrow X$ is the partial state transition function, and $x_0 \in X$ is the initial state. Let $\Sigma^*$ be the set of all prefixes of strings in $\Sigma$, including the empty string $\epsilon$. The domain of the state transition function $\alpha$ can be extended from $X \times \Sigma$ to $X \times \Sigma^*$ in the usual way. For each $s \in \Sigma^*$, $|s|$ denotes its length. (Note that, for a finite set $A$, $|A|$ denotes the number of its elements.) The generated language of $G$, denoted by $L(G)$, is defined as $L(G) = \{ s \in \Sigma^* | \alpha(x_0, s) \}$, where, for each $x \in X$ and $s \in \Sigma^*$, $\alpha(x, s)$ denotes that $s$ is defined at $x$. Also, for each $s \in L(G)$, the postlanguage of $L(G)$ after $s$ is defined as $L(G)/s = \{ t \in \Sigma^* | st \in L(G) \}$. Further, the set of deadlocking strings is defined as $L_d(G) = \{ s \in L(G) | \{ \sigma \Sigma \cap L(G) = \emptyset \}$.

For a string $s \in \Sigma^*$, the set of all prefixes of $s$ is denoted by $pr(s)$, that is, $pr(s) = \{ t \in \Sigma^* | \exists u \in \Sigma^* : tu = s \}$. Let $L \subseteq \Sigma^*$ be a language. The set of all prefixes of strings in $L$ is defined as $pr(L) = \bigcup_{s \in L} pr(s) = \{ t \in \Sigma^* | \exists u \in \Sigma^* : tu \in L \}$.

If $L = pr(L)$, then $L$ is said to be (prefix-)closed.

Let $I = \{ 1, 2, \ldots, n \}$ be the index set of local diagnosers which jointly diagnose a DES $G$. The $i$th local diagnoser observes the occurrence of an event through the local observation mask $M_i : \Sigma \rightarrow \Delta_i \cup \{ \epsilon \} (i \in I)$, where $\Delta_i$ is the set of symbols observed by the $i$th diagnoser. An event $\sigma \in \Sigma$ with $M_i(\sigma) = \epsilon$ is unobservable to the $i$th local diagnoser. An observation mask $M_i$ is extended to $M_i : \Sigma^* \rightarrow \Delta_i^* \subseteq \Sigma^*$ inductively as follows:

- $M_i(\epsilon) = \epsilon$,
- $\forall s \in \Sigma^* \forall \tau \in \Sigma$, $M_i(\sigma \tau) = M_i(s)M_i(\tau)$.

Strings $s_1, s_2 \in \Sigma^*$ are said to be indistinguishable (under $M_i$) if $M_i(s_1) = M_i(s_2)$. Also, the inverse observation mask, denoted by $M_i^{-1} : \Delta_i^* \rightarrow 2^{\Sigma^*}$, is defined as

$$M_i^{-1}(t) = \{ s \in \Sigma^* | M_i(s) = t \}$$

for each $t \in \Delta_i^*$. This is the set of strings on $\Sigma$ which are observed as $t \in \Delta_i$ by the $i$th diagnoser.

It is assumed that a nonempty closed sublanguage $K \subseteq L(G)$, called a nonfailure specification language, represents the normal behavior of $G$. The failure behavior of $G$ is represented by the language $L(G) - K$. That is, in this paper, the failure means the occurrence of a string in $L(G) - K$. The notion of codiagnosability [6] plays an important role in decentralized diagnosis.

Definition 1 [6] The system $G$ is said to be codiagnosable with respect to a nonempty closed language $K \subseteq L(G)$ if

$$\exists m \in N \forall s \in L(G) - K \forall t \in L(G)/s \\ [|t| \geq m \ \vee \ st \in L_d(G)] \Rightarrow \exists i \in I : M_i^{-1}(st) \cap L(G) \subseteq L(G) - K,$$

where $N$ is the set of nonnegative integers.

The notion of codiagnosability means that the occurrence of a failure string in $L(G) - K$ can be detected by at least one local diagnoser within a uniformly bounded number of steps.

3. Reliable Codiagnosability

In this paper, a situation in which diagnosis decisions of some local diagnosers are not available by some causes is considered. In order to guarantee that the failure is detected within a uniformly bounded number of steps in such a situation, a stronger notion of codiagnosability is required.

Example 1 We consider a DES $G$ with $L(G) = pr[\{ a^h b^l a^m \in \Sigma^* | h, l \geq 0 \}]$ and a nonempty closed language $K = \{ a^k \in \Sigma^* \ | \ h \geq 0 \}$. That is, the event $f$ represents the occurrence of the failure. Since $G$ is deadlock-free, $L_d(G) = \emptyset$. Let $\Delta_1 = \{ a \}, \Delta_2 = \{ b \}$, and the observation masks $M_1$ and $M_2$ be given as

$$M_1(\sigma) = \begin{cases} a, & \text{if } \sigma = a \\ \epsilon, & \text{otherwise} \end{cases}$$

and

$$M_2(\sigma) = \begin{cases} b, & \text{if } \sigma = b \\ \epsilon, & \text{otherwise} \end{cases}$$

respectively.

For any $s \in L(G) - K$ and $t \in L(G)/s$ with $|t| \geq 1$, $st$ can be written as $st = a^h b^l$, where $h \geq 0$ and $l > 0$. We have $M_1^{-1}(st) \cap L(G) = \{ a^h b^l | h \geq 0 \} \subseteq L(G) - K$, which implies that $G$ is codiagnosable with respect to $K$, and the occurrence of the failure is detected by the second diagnoser. However, if the diagnosis decision of the second diagnoser is not available due to some causes, the failure cannot be detected since the first diagnoser cannot distinguish any failure string $st = a^h b^l$ ($h \geq 0$, $l \geq 0$) from a nonfailure one $a^h K$.

For each failure string $w \in L(G) - K$, let

$$I(w) = \{ i \in I | M_i^{-1}(st) \cap L(G) \subseteq L(G) - K \}$$

be the index set of local diagnosers for which all strings indistinguishable from $w$ are failure strings in $L(G) - K$. That is, the index set $I(w)$ specifies local diagnosers which can detect the occurrence of the failure after $w$ is executed. Then, a notion of $(n, k)$-reliable codiagnosability, which guarantees that any occurrence of the failure is detected even if at most $n - k$ local diagnosis decisions are not available, is defined as follows.

Definition 2 Assume that $1 \leq k \leq n$. The system $G$ is said to be $(n, k)$-reliably codiagnosable with respect to a nonempty closed language $K \subseteq L(G)$ if

$$\exists m \in N \forall s \in L(G) - K \forall t \in L(G)/s \ [ |t| \geq m \ \vee \ st \in L_d(G) ] \Rightarrow [ |st| \geq n - k + 1 ]$$

be true.

The $(n, k)$-reliable codiagnosability condition requires that there exists a nonnegative integer $m \in N$ such that, for any failure string $s \in L(G) - K$ and any extension $t \in L(G)/s$ with $|t| \geq m$ or $st \in L_d(G)$, at least $n - k + 1$ local diagnosers can detect the occurrence of the failure. For any subset $I' \subseteq I$ with $|I'| \geq k$, $I(st) \cap I' \neq \emptyset$ when $|st| \geq n - k + 1$. That is, $(n, k)$-reliable codiagnosability guarantees that if arbitrary more than or equal to $k$ local diagnosis decisions are available, any occurrence of the failure can be detected.

Remark 1 The notion of reliable codiagnosability is originally introduced as robust codiagnosability in [19] in a special case where the failure is represented by the occurrence of an unobservable failure event.

Remark 2 When $n = k$, the $(n, k)$-reliable codiagnosability condition is reduced to the conventional codiagnosability condition of Definition 1.
4. Verification of Reliable Codiagnosability

In this section, verification of \((n,k)\)-reliable codiagnosability is studied. In [19], a method for verifying \((n,n-1)\)-reliable codiagnosability in the presence of \((n,n)\)-reliable codiagnosability is developed. In this paper, by generalizing the verification result for codiagnosability [6], \((n,k)\)-reliable codiagnosability is verified for any \(k\) \((1 \leq k \leq n)\) without assuming that \(G\) is \((n,n)\)-reliably codiagnosable.

In the rest of this paper, it is assumed that the system state \(X\) of the system \(G\) is finite and a nonfailure specification language \(K \subseteq L(G)\) is generated by a finite automaton \(H = (Y, \Sigma, \beta, y_0)\), that is, \(L(H) = K\). Then, \(H\) is augmented by adding the failure state \(F \notin Y\) as \(H' = (Y, \Sigma, \tilde{\beta}, y_0)\), where \(\tilde{Y} = Y \cup \{F\}\) and the transition function \(\tilde{\beta} : \tilde{Y} \times \Sigma \to \tilde{Y}\) is defined as

\[
\tilde{\beta}(\tilde{y}, \sigma) = \begin{cases} 
\beta(\tilde{y}, \sigma), & \text{if } \tilde{y} \in Y \land \beta(\tilde{y}, \sigma)!
F, & \text{otherwise}
\end{cases}
\]

for each \(\tilde{y} \in \tilde{Y}\) and \(\sigma \in \Sigma\). Since \(\tilde{\beta}(\tilde{y}, \sigma)\) for any \(\tilde{y} \in \tilde{Y}\) and \(\sigma \in \Sigma, L(H') = \Sigma^*\) holds. Further, for any \(\sigma \in \Sigma^*\), \(s \notin K\) if and only if \(\tilde{\beta}(y_0, s) = F\).

To verify \((n,k)\)-reliable codiagnosability for any \(k\) \((1 \leq k \leq n)\), a testing automaton

\[
T = (Z, \Sigma_T, \gamma, z_0)
\]

is constructed by composing \(G\) and \(n - 1\) copies of \(H\), where \(Z\) is the finite set of states, \(z_0 \in Z\) is the initial state, \(\Sigma_T\) is the finite set of events, and \(\gamma : Z \times \Sigma_T \to Z\) is the partial state transition function. They are defined as follows:

- \(Z = (X \times \tilde{Y}) \times \tilde{Y} \times \tilde{Y} \times \cdots \times \tilde{Y}\) \(n\) times
- \(z_0 = (x_0, y_0, y_0, \ldots, y_0)\)
- \(\Sigma_T = (\Sigma \cup \{x\}) \times (\Sigma \cup \{x\}) \times \cdots \times (\Sigma \cup \{x\}) - \{(\varepsilon, \ldots , \varepsilon)\}\) \(n\) times
- For any \(z = (x, \tilde{y}_1, \tilde{y}_2, \ldots , \tilde{y}_n) \in Z\) and \(\sigma_T = (\sigma, \sigma_1, \sigma_2, \ldots , \sigma_n) \in \Sigma_T\), \(\gamma(z, \sigma_T)\) if and only if
  - \((\forall i \in I) M_i(\sigma) = M_i(\sigma_t)\), and
  - \(\sigma \neq \varepsilon \Rightarrow \alpha(x, \sigma)!\).

If \(\gamma(z, \sigma_T)!\) then \(\gamma(x', \sigma_T) = (x', \tilde{y}_1', \tilde{y}_2', \ldots , \tilde{y}_n')\), where

\[
x' = \begin{cases} 
\alpha(x, \sigma), & \text{if } \sigma \neq \varepsilon \\
x, & \text{otherwise}
\end{cases}, \quad \tilde{y}' = \begin{cases} 
\tilde{\beta}(\tilde{y}, \sigma), & \text{if } \sigma \neq \varepsilon \\
\tilde{y}, & \text{otherwise}
\end{cases}, \quad \tilde{y}_i' = \begin{cases} 
\tilde{\beta}(\tilde{y}_i, \sigma_i), & \text{if } \sigma_i \neq \varepsilon \\
\tilde{y}_i, & \text{otherwise}
\end{cases} \quad (\forall i \in I).
\]

The projection functions \(P : \Sigma_T \to \Sigma^*\) and \(P_i : \Sigma_T \to \Sigma^* \quad (i \in I)\) are inductively defined as follows:

- \(P(\varepsilon) = \varepsilon, P_i(\varepsilon) = \varepsilon\),
- \((\forall s_T \in \Sigma_T^*)(\forall \sigma_T = (\sigma, \sigma_1, \sigma_2, \ldots , \sigma_n) \in \Sigma_T)\)
  \[
  P(s_T, \sigma_T) = P(s_T) \sigma; P_i(s_T, \sigma_T) = P_i(s_T, \sigma_i)
  \]

By construction of \(T\), we have

\[
(Vi \in I) M_i(P_i(s_T)) = M_i(P_i(s_T))
\]

for any \(s_T \in L(T)\). Also, for any strings \(s \in L(G)\) and \(s_i \in \Sigma^* \quad (i \in I)\) which satisfy

\[
(Vi \in I) M_i(s) = M_i(s_i),
\]

there exists \(s_T \in L(T)\) such that \(P(s_T) = s\) and \(P_i(s_T) = s_i\) for all \(i \in I\).

A sequence of transitions

\[
\gamma(1)^{(1)} \rightarrow \gamma(2)^{(1)} \rightarrow \cdots \rightarrow \gamma(g)^{(1)} \rightarrow \gamma(g + 1)^{(1)} \quad (g \geq 1)
\]

satisfies \(\gamma(p) = \gamma(z)^{(p)}\), \(\gamma(1)^{(p)}\) for any \(p \in \{1, 2, \ldots , q\} \in \Sigma\) \(\gamma(1)^{(p)} = \gamma(1)^{(1)}\) is called a cycle in \(T\).

**Definition 3** Let \(J_1(K)\) be the set of \(j(0 \leq j \leq n)\) such that there exists a reachable cycle \(\gamma(1)^{(1)} \rightarrow \gamma(2)^{(1)} \rightarrow \cdots \rightarrow \gamma(g)^{(1)} \rightarrow \gamma(1)^{(1)}\) in the testing automaton \(T\) which satisfies

\[
(3p \in \{1, 2, \ldots , q\}) \gamma(p)^{(p)} = F \land \gamma(p)^{(p)} \neq \varepsilon \land ||i \in I| |\gamma(p)^{(p)} = F| = j,
\]

where we let \(\gamma(p)^{(p)} = (x^{(p)}, y^{(p)}, y_1^{(p)}, y_2^{(p)}, \ldots , y_n^{(p)}) \in Z\) and \(\sigma_T^{(p)} = (\sigma^{(p)}, \sigma_1^{(p)}, \sigma_2^{(p)}, \ldots , \sigma_n^{(p)}) \in \Sigma_T\) for each \(p \in \{1, 2, \ldots , q\}\).

Also, let \(J_2(K)\) be the set of \(j(0 \leq j \leq n)\) such that there exists a reachable state \((x, \tilde{y}_1, \tilde{y}_2, \ldots , \tilde{y}_n) \in Z\) in the testing automaton \(T\) which satisfies

\[
x \in X_d \land \tilde{y} = F \land ||i \in I| |\gamma(p)^{(1)} = F| = j,
\]

where \(X_d\) is the set of deadlocking states of \(G\) defined as \(X_d = \{x \in X \mid \forall \sigma \in \Sigma : \alpha(x, \sigma)\}!\).

Intuitively, when \(\min(j) = (J_1(K) \cup J_2(K)) > 0\), for any sufficiently long or deadlocking failure string, there exist at least \(\min(j) \leq J_1(K) \cup J_2(K)\) local diagnosers which can detect the occurrence of the failure. Also, if \(\min(j) = J_1(K) \cup J_2(K)) = 0\), there exists a sufficiently long or deadlocking failure string for which any local diagnoser cannot detect the occurrence of the failure. The following theorem presents a necessary and sufficient condition for \(G\) not to be \((n,k)\)-reliably codiagnosable with respect to \(K\).

**Theorem 1** For any \(k(1 \leq k \leq n)\), the system \(G\) is not \((n,k)\)-reliably codiagnosable with respect to \(K\) if and only if

\[
k < n - \min(j) \leq J_1(K) \cup J_2(K)) + 1.
\]

**Proof:** \((\Rightarrow)\) By (13), we have

\[
\min(j) \leq J_1(K) \cup J_2(K)) < n - k + 1.
\]

First, we consider the case where \(\min(j) \leq J_1(K) \cup J_2(K)) \in J_1(K)\), which implies that there exists a reachable cycle \(\gamma(1)^{(1)} \rightarrow \gamma(2)^{(1)} \rightarrow \cdots \rightarrow \gamma(g)^{(1)} \rightarrow \gamma(1)^{(1)}\) in \(T\) which satisfies

\[
(3p \in \{1, 2, \ldots , q\}) \gamma(p)^{(p)} = F \land \gamma(p)^{(p)} \neq \varepsilon \land ||i \in I| |\gamma(p)^{(p)} = F| < n - k + 1.
\]

Then, there exists a string \(s_T \in L(T)\) which satisfies \(\gamma(z_0, s_T) = \gamma(1)^{(1)}\), where \(\alpha(x_0, P_i(s_T)) = \gamma(1)^{(1)}, \beta(y_0, P_i(s_T)) = y(1)^{(1)}\), and
where $\tilde{P}(y, P(s_T)) = \tilde{y}^{(i)}$. Once the state of $\tilde{H}$ becomes $F$, it remains there. Since $\tilde{y}^{(0)} = F$, we have $\tilde{y}^{(1)} = F$. Letting $s = P(s_T)$, we have $\alpha(x_0, s) = x^{(1)}$ and $\tilde{P}(y_0, s) = \tilde{y}^{(1)} = F$. It follows that $s \in L(G) - K$.

For any $m \in N$, we let $\tilde{t} = (\alpha^{(1)} \alpha^{(2)} \cdots \alpha^{(p)})^{\infty}$. Letting $t = P(s_T) = (\alpha^{(1)} \alpha^{(2)} \cdots \alpha^{(p)})^{\infty}$, we have $\|i\| \geq m$ since $\alpha^{(p)} \neq e$. We consider a string $s_T \in L(T)$. We have $s = P(s_T)$ and let $u_i = \tilde{P}(s_T \tilde{t})$. Then, we have $\alpha(x_0, s) = x^{(1)}$, $\tilde{P}(y_0, s) = \tilde{y}^{(1)}$, and $\tilde{P}(y_0, u_i) = \tilde{y}^{(i)}$ (i.e., from $|i| \in \{1, 2, \ldots, p\}$, we have $|i| \in \{1, 2, \ldots, p\}$, and $\tilde{P}(y_0, s) = \tilde{y}^{(i)} = F$). Therefore, we have $|i| \in \{1, 2, \ldots, p\} \neq F$, which implies that $|i| \in \{1, 2, \ldots, p\} \neq F$, and hence, $G$ is not $(n, k)$-reliably diagonalizable with respect to $K$.

Next, consider the case where $\min \{j \mid j \in J_1(K) \cup J_2(K)\} \in J_3(K)$, which implies that there exists a reachable state $z = (x, \tilde{y}, \tilde{y}_1, \tilde{y}_2, \ldots, \tilde{y}_n)$ in $T$ such that $x \in X_d$ and $\tilde{y} = F \wedge |i| \in \{1, 2, \ldots, p\} \neq F$, and hence, $G$ is not $(n, k)$-reliably diagonalizable with respect to $K$.

Thus, there exists a string $s_T^{(i)} \in L(T)$ such that $\gamma(s_0, s_T^{(i)}) = z$. It follows that $\alpha(x_0, P(s_T^{(i)})) = x$, $\tilde{P}(y_0, P(s_T^{(i)})) = \tilde{y}$, and $\tilde{P}(y_0, u_i) = \tilde{y}^{(i)}$ (i.e., from $|i| \in \{1, 2, \ldots, p\}$, we have $|i| \in \{1, 2, \ldots, p\} \neq F$, and hence, $G$ is not $(n, k)$-reliably diagonalizable with respect to $K$.

Since $\gamma(s_0, s_T^{(i)}) = z$, we have $|i| \in \{1, 2, \ldots, p\} \neq F$, and hence, $G$ is not $(n, k)$-reliably diagonalizable with respect to $K$.

Suppose that $G$ is not $(n, k)$-reliably diagonalizable with respect to $K$. Then, for any $m \in N$, there exist strings $s \in L(G) - K$ and $L(G)/s$ which satisfy

$$[|i| \geq m \vee st \in L(G)/s] \wedge [|i| \in \{1, 2, \ldots, p\}] \neq F, \quad n \neq k + 1.$$

For each $i \in L(T)$, we consider any $u_i \in \Sigma^*$ which satisfies $M_i(s_0) = M_i(u_i)$. Also, for any $i \notin L(T)$, there exist $u_i \in K$ which satisfies $u_i \in M_i(s_0) \wedge L(G)$ such that $M_i(s_0) \wedge L(G)$ is not $(n, k)$-reliably diagonalizable with respect to $K$. Then, for any $m \in N$, there exist strings $s \in L(G) - K$ and $L(G)/s$ which satisfy

$$[|i| \geq m \vee st \in L(G)/s] \wedge [|i| \in \{1, 2, \ldots, p\}] \neq F, \quad n \neq k + 1.$$

This contradicts the assumption that $G$ is $(n, k)$-reliably diagonalizable with respect to $K$. Therefore, the complexity of verifying the condition of Theorem 1 is $O(\|X\| \times \|Y\|^{p+1} \times \|\Sigma\|^{p+1})$. The complexity of the method of [6] for verifying the conventional diagnosability condition is $O(\|X\| \times \|Y\|^{p+1} \times \|\Sigma\|^{p+1})$. Hence, the complexity of the presented method for verifying $(n, k)$-reliably diagnosability is the same as that for verifying diagnosability condition.
failure can be detected if local diagnosis decisions of at least $k$ conditions, that is, $K$ with respect to $\mathcal{M}$.

By Definition 2, if the system $G$ is $(n,k)$-reliably codiagnosable, any occurrence of the failure can be detected within $m_1^*(K)$ steps by using arbitrary more than or equal to $k$ local diagnosis decisions. For any $m' \in \mathcal{M}$ with $m' < m_1^*(K)$, there exist $s \in L(G) - K$ and $t \in L(G)/s$ such that $|t| \geq m'$ and $|l(st)| < n - k + 1$. That is, there exist at least $k$ local diagnosers which cannot detect the occurrence of the failure within $m'$ steps. Therefore, $m_1^*(K)$ can be regarded as the delay bound.

In this section, we assume that the system $G$ is $(n,k)$-reliably codiagnosable with respect to $K$, and develop an algorithm for computing the delay bound $m_1^*(K)$ by generalizing the result of [4] for computing the delay bound in centralized failure diagnosis.

**Algorithm 1** Computation of the delay bound $m_1^*(K)$.

1. Construct the testing automaton $T = (Z, \Sigma_T, \gamma, z_0)$ defined in Section 4.

2. By using the testing automaton $T$, construct a weighted directed graph $G_{T_k} = (V, E, W)$, where $V$ is the set of vertices, $E \subseteq V \times V$ is the set of edges, and $W : E \rightarrow \{-1,0\}$ is the weighting function. They are defined as follows:
   - $V = \{(x, \bar{y}, \bar{y}_1, \bar{y}_2, \ldots, \bar{y}_n) \in Z \mid |\{i \in I \mid \bar{y}_i = F\}| \leq n-k\}$.
   - $E = \{(z, z') \in V \times V \mid \exists \sigma_T \in \Sigma_T : \gamma(z, \sigma_T) = z'\}$.
   - For any $(z, z') \in E$,
     \[
     W(z, z') = \begin{cases} 
     -1, & \text{if } \exists \sigma_T \in \Sigma_T : \gamma(z, \sigma_T) = z' \\
     0, & \text{otherwise}
     \end{cases}
     \]
     where $z = (x, \bar{y}, \bar{y}_1, \bar{y}_2, \ldots, \bar{y}_n)$ and $\sigma_T = (\sigma_1, \sigma_1', \sigma_2, \ldots, \sigma_n)$

3. A path of $G_{T_k}$ is a finite string $p = (z_0, z_1)(z_1, z_2) \cdots (z_{l-1}, z_l) \in E^*$ ($l \geq 1$) initiated at the initial state $z_0$ of $T$, and its weight denoted by $l(p)$ is defined as
   \[
   l(p) = \sum_{k=0}^{l-1} W(z_k, z_{k+1}).
   \]
   Then, compute
   \[
   d_k = \min\{l(p) \mid p \in L_p(G_{T_k})\},
   \]
   where $L_p(G_{T_k})$ is the set of all paths of $G_{T_k}$.

4. If there exists a vertex $z = (x, \bar{y}, \bar{y}_1, \bar{y}_2, \ldots, \bar{y}_n) \in V$ with $\bar{y} = F$, which is reachable from $z_0$ in $G_{T_k}$, then $d_k' := |d_k| + 1$; otherwise, $d_k' := |d_k|$. Output $d_k'$ as $m_1^*(K)$.

**Remark 5** By Theorem 1, since $G$ is $(n,k)$-reliably codiagnosable, any cycle reachable from $z_0$ in $G_{T_k}$ does not include an edge whose weight is $-1$. Therefore, $d_k$ is well-defined in Step 5 of Algorithm 1, and can be computed by using an algorithm which solves the shortest path problem [20].
Remark 6 In the weighted directed graph \(G_{T,k}\), the weight \(-1\) is introduced to count the number of steps after the occurrence of the failure. Intuitively, at most \(|d_t|\) events occur before the failure is detected by at least \(n-k+1\) local diagnosers (unless the failure is detected without delay). Therefore, any occurrence of the failure can be detected by at least \(n-k+1\) local diagnosers within \(|d_t| + 1\) steps.

The following lemma is needed to prove the correctness of Algorithm 1.

**Lemma 1** If \(d_t^* > 0\), then, for any \(m' \in N\) with \(0 \leq m' < d_t^*\),

\[(3s \in L(G) - K) (\exists \bar{t} \in L(G)/s) [t] \geq m' \land [l(st)] \leq n - k).

**Proof:** Since \(d_t^* > 0\), there exists \(z = (x, \bar{y}, \bar{y}_1, \bar{y}_2, \ldots, \bar{y}_k) \in V\) with \(\bar{y} = F\), which is reachable from \(z_0\) in \(G_{T,k}\). This implies that \(|d_t| = d_t^* - 1\).

We first consider the case where \(m' = 0\). For any \(z = (x, \bar{y}, \bar{y}_1, \bar{y}_2, \ldots, \bar{y}_k) \in V\) with \(\bar{y} = F\), which is reachable from \(z_0\) in \(G_{T,k}\), there exists \(s_T \in L(G)/s\) such that \(g(z_0, s_T) = z\).

The following lemma is needed to prove the correctness of \(G_{T,k}\). Now, we show that \(|l(st)| \leq n - k\). Thus, for \(P(s_T)\) in \(L(G) - K\) and \(s \in L(G)/s\), we have \(|s| = 0\) and \([l(P(s_T))] \leq n - k\).

We next consider the case where \(0 < m' \leq |d_t|\). There exists a sequence \(z_0 = t^{(1)} \rightarrow t^{(2)} \rightarrow \cdots \rightarrow t^{(q)}\) of transitions in \(T\) such that \(t^{(i)} = F\) and \(P(t^{(i)}) = m'\) for some \(r \in \{1, 2, \ldots, q\}\), where \(t^{(i)} = (x^{(i)}, \bar{y}, \bar{y}_1^{(i)}, \bar{y}_2^{(i)}, \ldots, \bar{y}_k^{(i)})\).

Since \(t^{(i)} = F\), we have \(s_T = P(t^{(i)})\). Also, let \(t^{(i)} = (x^{(i)}, \bar{y}^{(i)}, \bar{y}_1^{(i)}, \bar{y}_2^{(i)}, \ldots, \bar{y}_k^{(i)})\) and \(t = P(s_T)\). Then, we have \(t \in L(G)/s\) and \([l(P(T))] = m'\).

Further, since \([l([i \in I \mid t^{(i)} = F])] \geq n - k\), we have \([l(st)] \leq [l([i \in I \mid t^{(i)} = F])] \geq n - k\). That is,

\[(\exists s \in L(G) - K) (\exists \bar{t} \in L(G)/s) [t] \geq m' \land [l(st)] \leq n - k).

\[\square\]

**Theorem 2** Assume that the system \(G\) is \((n, k)\)-reliably codiagnosable with respect to \(K\). Then, \(m_2(K) = d_t^*\) holds.

**Proof:** First, we consider the case where \(d_t^* = 0\). Since \(|d_t| = d_t^* = 0\), we have \(d_t = 0\). It follows from \(d_t = 0\) that no vertex \(z = (x, \bar{y}, \bar{y}_1, \bar{y}_2, \ldots, \bar{y}_k) \in V\) with \(\bar{y} = F\) is reachable from \(z_0\) in \(G_{T,k}\).

Now, we show that \((\forall s \in L(G) - K) (\forall t \in L(G)/s) [l(st)] \geq n - k + 1\).

We suppose for contradiction that there exist \(s \in L(G) - K\) and \(t \in L(G)/s\) such that \([l(st)] \leq n - k\). For any \(i \in I\) with \(i \in I\), we consider any \(u_i \in \Sigma^*\) with \(M_i(s) = M_i(u_i)\). Also, for any \(i \in I\) with \(i \in I\), we consider any \(u_i \in \Sigma^*\) with \(M_i(s) = M_i(u_i)\) and \(L(G)\). Since \(M_i(s) = M_i(u_i)\) for any \(i \in I\), there exists \(s_T \in L(T)\) such that \(P(s_T) = s\) and \(P(s_T) = u_i\) for any \(i \in I\).

Since \(s \in K\) and \(s_T \in L(G) - K\), we have \([l(st)] = [s_T]\). Let \(s_T = \sigma_T^{(1)}\sigma_T^{(2)}\cdots\sigma_T^{(q)}\) (\(q \geq 1\)). Then, there exists a sequence \(z_0 = \sigma_T^{(1)}\sigma_T^{(2)}\cdots\sigma_T^{(q)}\) of transitions in \(T\) such that \(\sigma_T^{(i)} = F\) and \(P(\sigma_T^{(i)}) = m'\) for some \(r \in \{1, 2, \ldots, q\}\), where \(\sigma_T^{(i)} = (x^{(i)}, \bar{y}, \bar{y}_1^{(i)}, \bar{y}_2^{(i)}, \ldots, \bar{y}_k^{(i)})\).

Since \([l(st)] \leq n - k\) and \([l(st)] \leq n - k\) for any \(i \in I\), we have \([l([i \in I \mid \sigma_T^{(i)} = F])] \leq n - k\).

Letting \(\sigma_T^{(i)} = (x^{(i)}, \bar{y}, \bar{y}_1^{(i)}, \bar{y}_2^{(i)}, \ldots, \bar{y}_k^{(i)})\), we have \(\bar{y}_k^{(i)} = F\) and \(\bar{y}^{(i)} = F\).

Since \([l(st)] \leq n - k\), we have \([l([i \in I \mid \sigma_T^{(i)} = F])] \leq n - k + 1\).

Thus, \((\forall s \in L(G) - K) (\forall t \in L(G)/s) [l(st)] \geq n - k + 1\) holds.

\[\square\]

**Example 3** We consider the setting of Example 2, where \(G\) is \((3, 2)\)-reliably codiagnosable with respect to \(K\).

We compute the delay bound \(m_2(K)\). From the testing automaton \(T\) shown in Fig. 3, the weighted directed graph \(G_{T,k}\) is constructed as shown in Fig. 4. By Fig. 4, \(d_t^* = 0\) holds. Also, there is no reachable vertex \(z = (x, \bar{y}, \bar{y}_1, \bar{y}_2, \bar{y}_3) \in V\) with \(\bar{y} = F\), which implies that \(d_t^* = d_t = 2\). Thus, we have \(m_2(K) = 0\).

6. Conclusions

In this paper, reliable decentralized failure diagnosis of DESs has been studied. First, a method for verifying \((n, k)\)-reliably codiagnosability for any \(k \leq n \leq k\) has been developed.
Next, an algorithm for computing the delay bound within which any occurrence of the failure can be detected by using arbitrary more than or equal to $k$ local diagnosis decisions has been presented.

The decentralized diagnosis architecture used in this paper can be regarded as the disjunctive architecture. Reliable decentralized failure diagnosis in the conjunctive architecture introduced in [9] is important future work.

Acknowledgments

This work was supported in part by JSPS Grant-in-Aid for Scientific Research (No. 24560547).

References


