IEEE Access
Multidisciplinary : Rapid Review : Open Access Journal

Received 10 August 2023, accepted 29 August 2023, date of publication 6 September 2023, date of current version 15 September 2023.

*Digital Object Identifier 10.1109/ACCESS.2023.3312542*

RESEARCH ARTICLE

# Decentralized Marking Fault Diagnosis of Labeled Petri Nets

**ZHENHUA YU, (Member, IEEE), YINYIN QI, AND XUYA CONG, (Member, IEEE)**
College of Computer Science and Technology, Xi'an University of Science and Technology, Xi'an 710054, China

Corresponding author: Xuya Cong (congxuya@xust.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant 62303375, Grant 62273272, and Grant 61873277, in part by the Key Research and Development Program of Shaanxi Province under Grant 2023-YBGY-243, in part by the Natural Science Foundation of Shaanxi Province under Grant 2022JQ-606 and Grant 2020-JQ758, in part by the Research Plan of Department of Education of Shaanxi Province under Grant 21JK0752, and in part by the Youth Innovation Team of Shaanxi Universities.

**ABSTRACT** A decentralized marking fault diagnosis method is proposed to solve the problem that increasing the number of unobservable transitions may result in the inability to diagnose faulty markings, in a class of decentralized systems modeled by labeled Petri nets. Assuming that each local site knows the structure of the labeled Petri net, and the subnet induced by unobservable transitions is acyclic. The decentralized architecture consists of a set of local sites communicating with a coordinator that determines whether the faults have occurred in the system, which are modeled by markings. First, each local site constructs the corresponding dual verifier and calculates the local marking fault diagnosis state according to the local observations. Then, it exchanges the corresponding information with the coordinator according to the two proposed diagnosis protocols. Finally, the coordinator calculates the global diagnosis state according to the received information. In addition, the marking diagnosability under both protocols is analyzed. A sufficient and necessary condition for marking fault diagnosis in the decentralized architecture under the second protocol is proved.

**INDEX TERMS** Discrete event systems, marking fault diagnosis, labeled petri nets, verifier.

## I. INTRODUCTION

Discrete event system [32], [33] is a dynamic system whose state evolutions are driven by discrete events. If a sensor detects the occurrence of a specific event in a discrete event system, the state of it changes accordingly. Many intelligent information systems can be regarded as discrete event systems, such as power systems [1], manufacturing systems [2], communication systems [3], logistics sorting systems [4] and image processing systems [34]. If a fault occurs in a discrete event system, the performance and productivity of the system will be reduced, and even a major production accident may occur. Fault diagnosis in discrete event systems can determine whether some faulty events have occurred in accordance with the current observation, so that timely measures can be taken to restore the system to normal operation. Since fault diagnosis in discrete event systems is highly relevant to the safety of the system [35], a lot of works have been done in the past decades [36], [5], [6], [7], [8], [9]. In the related literature, fault detection and diagnosis have been extensively studied in centralized systems [10], [11], [12], [13], [14], [15]. Due to the distributed nature of many large real systems, several methods have been proposed to solve the problem of fault diagnosis in the decentralized settings by building relevant models through automata [16], [17], [18], [19], [20]. These class of methods build a diagnoser by an automaton from the model indicating whether the paths generated so far have faulty events. However, with the growth of system size, the construction of diagnosers inevitably encounters the problem of state space explosion. Petri nets [21], [22] can describe the system behavior with more compact structures without expounding the entire state space. The distributed characteristics of Petri nets reduce the computational complexity of fault diagnosis problems. Therefore, some

The associate editor coordinating the review of this manuscript and approving it for publication was Lei Shu.

works [23], [24], [25], [26], [27], [28], [37] use Petri nets as modeling tools to study fault diagnosis problems of distributed systems.

Cabasino et al. [23] propose a method to verify diagnosability of Petri nets in a decentralized setting, and prove that the system without failure ambiguous strings is diagnosable. The work in [24] defines three protocols, and proves that diagnosability of the decentralized system is strictly related to the existence of failure ambiguous strings. Under the assumptions that the unobservable subnet is acyclic and the structure of the net is known to each site, Cong et al. [25] propose an online diagnosis method for Petri net systems using integer linear programming. Specifically, the study in [25] proposes two protocols and proves a necessary and sufficient condition for the second protocol to be able to successfully diagnose faults in the decentralized setting. Ran et al. [26] solve the problem of codiagnosability of labeled Petri nets by constructing a verifier, which avoids the exhaustive enumeration of the set of reachable markings by using the concept of basis markings. In addition, this work [26] extends the notion of $K$-step diagnosability to $K$-step codiagnosability and gives an algorithm to compute the minimum $K$ value. On the basis of [26], the work in [27] extends the method to unbounded Petri nets and gives the necessary and sufficient conditions for $K$-step codiagnosability. Recently, Ran et al. [37] enforce the codiagnosability of systems by adding appropriate sensors. Bonhomme [28] proposes a state estimation method in a decentralized system to evaluate the occurrence of each specific fault, but the complexity of the proposed algorithm is exponential in the centralized and decentralized settings.

All of the above approaches consider the fault as an event in a Petri net or automaton. In many practical situations, the operator of a system may expect to know whether the system has or has ever reached an important state, rather than recognizing an event. For example, in a logistics sorting system, the buffer may often exceed the threshold. In order to get the attention of the operator, an alarm needs to be raised in a finite number of steps after the threshold is exceeded. Therefore, Ma et al. [29] study marking-based fault diagnosis in centralized systems. The work solves the problem of marking-based fault diagnosis by expressing the fault with a specific state. Since systems are distributed in reality, we extend this work to decentralized systems. Unlike centralized systems, which perform marking fault diagnosis regarding the system directly, decentralized systems are monitored by series of sites that perform marking fault diagnosis locally. A coordinator communicates with sites and outputs the diagnosis states. Since each site can only observe part of the system's events, and the increase of the number of unobservable events may lead to the failure to diagnose the existing faults. We propose protocols to define the information that can be exchanged between the coordinator and the local sites to realize the marking fault diagnosis of the decentralized system.

The main contributions of this paper are summarized as follows: (1) The marking fault diagnosis under the existing centralized discrete event systems is extended to the decentralized systems, which are more in line with the characteristics of the real systems. (2) Two diagnosis protocols are proposed to verify the marking diagnosability of decentralized systems, and a necessary and sufficient condition for marking fault diagnosis in the decentralized architecture under the second protocol is proved.

We remark that two diagnosis protocols proposed in [25] are only applicable to event-based faults. In order to meet the requirement that system operators only expect to know whether the system has reached the faulty state, this paper proposes two marking-based fault diagnosis protocols to realize the marking fault diagnosis of decentralized systems.

The rest of this paper is structured as follows. First, some basic definitions and notations needed in this paper are recalled in Section II. The marking fault diagnosis for the local sites is formalized in Section III. In Section IV, two protocols are proposed to solve the problem of marking fault diagnosis in decentralized systems, and we analyze their diagnosability. The diagnosability of the two protocols is verified by an example of logistics sorting system in Section V. Section VI concludes the paper.

## II. PRELIMINARIES

### A. PETRI NETS AND LABELED PETRI NETS

A Petri net is a net structure $N = (P, T, Pre, Post)$, where $P$ is a set of $m$ places, $T$ is a set of $n$ transitions, $Pre : P \times T \to \mathbb{N}$ and $Post : P \times T \to \mathbb{N}$ are the pre- and post-incidence matrices, respectively. The incidence matrix of $N$ is defined as $C = Post - Pre$. We use $C(\cdot, t)$ to represent the corresponding column of the transition $t$ in the incidence matrix. For a transition $t \in T$, the set of input places is defined as ${}^\bullet t = \{p \in P \mid Pre(p, t) > 0\}$ and the set of output places is defined as $t^\bullet = \{p \in P \mid Post(p, t) > 0\}$.

A marking is a function $M : P \to \mathbb{N}$. It can also be represented as a column vector $M$. At a marking $M$, the number of tokens in place $p$ is denoted as $M(p)$. A Petri net system $\langle N, M_0\rangle$ is a net $N$ with an initial marking $M_0$.

For a transition $t$, if $\forall p \in {}^\bullet t, M(p) \geq Pre(p, t)$, it is said to be enabled at a marking $M$, denoted by $M[t\rangle$. Enabled transition $t$ may fire and yield a new marking $M' = M_0 + C(\cdot, t)$. This fact is denoted as $M[t\rangle M'$. We say that $M'$ is reachable from $M$, if a transition sequence $\sigma = t_1 t_2 \ldots t_k \in T^*$ fires at a marking $M$ and its occurrence finally generates $M'$, where $T^*$ is the Kleene-closure [30] of $T$. The notation $M[\sigma\rangle M'$ is used to denote this fact. The reachability set of $\langle N, M_0\rangle$ is composed of the markings set reachable from the initial marking $M_0$ denoted by $R(N, M_0)$. The language of $\langle N, M_0\rangle$ is defined as $L(N, M_0) = \{\sigma \in T^* \mid M_0[\sigma\rangle\}$. Given a sequence $\sigma \in T^*$, we denote its firing vector as $\mathbf{y}$. The times of occurrence of a transition $t$ in $\sigma$ is denoted by $y(t)$. For any sequence $\sigma \in T^*$, the prefix-closure of $\sigma$ is defined as $Pr(\sigma) = \{\sigma' \in T^* \mid (\exists \sigma'' \in T^*)\sigma = \sigma'\sigma''\}$ [29]. If a sequence $\bar{\sigma} \in T^*$ such that $\bar{\sigma} \in Pr(\sigma)$ and $\bar{\sigma} \neq \sigma$, it is called a strict prefix of $\sigma$.

Given a Petri net $N = (P, T, Pre, Post)$, a subset $P' \subseteq P$ of its places and a subset $T' \subseteq T$ of its transitions, if $Pre'$ is the restriction of $Pre$ to $P' \times T'$ and $Post'$ is the restriction of $Post$ to $P' \times T'$, a subnet of $N$ is denoted by a new net $N' = (P', T', Pre', Post')$. If $N' = (P, T', Pre', Post')$ then $N'$ is said to be the $T'$-induced subnet.

A labeled Petri net is defined as $G = (N, M_0, E, \ell)$, where $\langle N, M_0 \rangle$ represents a Petri net system, the set $E$ represents an alphabet, and the labeling function is denoted as $\ell : T \rightarrow E \cup \{\varepsilon\}$ that assigns each transition $t \in T$ either a symbol from $E$ or the empty word $\varepsilon$. The set of transitions $T$ is partitioned into $T_o \cup T_u$, where $T_o = \{t \in T \mid \ell(t) \in E\}$ is the set of observable transitions, and $T_u = \{t \in T \mid \ell(t) = \varepsilon\}$ is the set of silent or unobservable transitions.

The labeling function can be extended to $\ell : T^* \rightarrow E^*$, where $E^*$ is the Kleene-closure of $E$, as follows:

(1) $\ell(\varepsilon) = \varepsilon$;

(2) $\ell(\sigma t) = \ell(\sigma)\ell(t)$, where $\sigma \in T^*$ and $t \in T$.

The observation of $\sigma$ is represent by $\omega = \ell(\sigma) \in E^*$ if a string $\sigma \in T^*$ fires. The inverse projection of an observation $\omega \in E^*$ of a labeled Petri net $G$ is denoted by $\ell^{-1}(\omega) = \{\sigma \in L(N, M_0) \mid \ell(\sigma) = \omega\}$. Moreover, $L(G) = \{\ell(\sigma) \mid \sigma \in L(N, M_0)\}$ is called the language of $G = (N, M_0, E, \ell)$.

### B. BASIS REACHABILITY GRAPH

We review some definitions on basis reachability graph (BRG) proposed in [31]. In a Petri net $N = (P, T, Pre, Post)$, if $T_I \subseteq T$, $T_E = T \backslash T_I$, and the $T_I$-induced subnet is acyclic, then the set of transitions can be partitioned into $T_E$ and $T_I$, denoted by $\pi = (T_E, T_I)$. $T_E$ and $T_I$ represent the set of explicit transitions and the set of implicit transitions, respectively.

In brief, the basis partition is to divide $T$ into $T_E$ and $T_I$ such that the $T_I$-induced subnet is acyclic. It is important to note that the terms "explicit" and "implicit" are not related to the physical meaning of the transitions.

*Definition 1:* Consider a Petri net $N = (P, T, Pre, Post)$ with a basis partition $\pi = (T_E, T_I)$, and a transition $t \in T$, the set of explanations of $t$ at a marking $M$ is defined as:

$$\sum(M, t) = \{\sigma \in {T_I}^* \mid M[\sigma\rangle M', M' \geq Pre(\cdot, t)\}.$$

The set of explanation vectors of $t$ at a marking $M$ is defined as:

$$Y(M, t) = \{y_\sigma \in \mathbb{N}^{|T_I|} \mid \sigma \in \sum(M, t)\}.$$

The set of explanation vectors is called the minimal explanation vector of $t$ if $\sigma$ is the minimal unobservable transition sequence. The set of minimal explanation vectors is denoted by $Y_{min}(M, t)$.

*Definition 2:* Consider a Petri net $N = (P, T, Pre, Post)$ with an initial marking $M_0$ and a basis partition $\pi = (T_E, T_I)$, the set of its basis markings consists of the initial marking $M_0$ and the set of markings $M' \in \mathcal{M}$ such that $\forall t \in T_E, \forall y \in Y_{min}(M, t)$ and $\forall M \in \mathcal{M}$ satisfing $M' = M + C \cdot y + C(\cdot, t)$.

Based on the above definitions, the BRG can be defined as a finite state automaton $\mathcal{B} = (\mathcal{M}, Tr, \Delta, M_0)$, where (1) $\mathcal{M}$ is the set of basis markings; (2) $Tr$ is the set of transitions $t \in T_E$; (3) the transition relation $\Delta$ is $\Delta = \{(M_1, (t, y), M_2) \mid y \in Y_{min}(M_1, t), t \in T_E, M_2 = M_1 + C \cdot y + C(\cdot, t)\}$; (4) $M_0$ is the initial state.

For the sake of expression, we use $\phi = (t_{i_1}, y_{i_1})(t_{i_2}, y_{i_2}) \cdots (t_{i_n}, y_{i_n})$ to denote a word of transitions of arcs in a BRG. A path $M_{b,1} \rightarrow M_{b,2} \rightarrow \cdots \rightarrow M_{b,n}$ in a BRG labeled by $(t_{i_1}, y_{i_1})(t_{i_2}, y_{i_2}), \ldots, (t_{i_n}, y_{i_n})$ is denoted by $\ell(\phi) = \ell(t_{i_1} t_{i_2} \cdots t_{i_n})$.

## III. BASICS OF DECENTRALIZED MARKING FAULT DIAGNOSIS

The marking fault diagnosis in a decentralized setting studied in this paper is depicted in Fig. 1, where a set $\mathcal{J} = \{1, 2, \ldots, J\}$ of local sites performing local marking fault diagnosis supervise the whole system. Each site knows the structure and initial marking of the net, but it only observes a subset of its transitions. The subset of transitions observed by each site is different, and all sites observe the system together. For each local site $j \in \mathcal{J}$, we use $T_{o,j} \subseteq T_o$ and $T_{u,j} = T \backslash T_{o,j}$ to denote the set of the locally observable and unobservable transitions, respectively.

The labeling function for each local site $j \in \mathcal{J}$ can be defined as:

$$\ell_j(t) = \begin{cases} \ell(t), & t \in T_{o,j} \\ \varepsilon, & \text{otherwise,} \end{cases}$$

where $\omega_j = \ell_j(\sigma)$ is the string associated with the transition sequence $\sigma$ observed by the $j$th site.

As shown in Fig. 1, each site locally performs marking fault diagnosis after observing the string $\omega_j = \ell_j(\sigma)$. Each site computes a local marking fault diagnosis state $\mathcal{A}_j(\omega_j)$ once it gets its own observation. According to the results, the local sites exchange specific information with a coordinator through a given communication protocol. The coordinator analyzes the information sent by different sites and infers whether the fault has occurred according to the related protocol. Finally, the coordinator generates a global marking fault diagnosis state $\mathcal{A}(\omega)$.

In this paper, decentralized marking fault diagnosis is studied under the following assumptions:

(1) The net is deadlock-free;

(2) For any site $j \in \mathcal{J}$, the $T_{u,j}$-induced subnet is acyclic;

(3) The coordinator knows the set of transitions that each local site can observe;

(4) At least one local site can observe all transitions labeled $e$;

(5) Before the coordinator performs any polling, each site must receive a projection of $\omega$ that a sequence of observable events generated by the Petri net on its local alphabet.

Assumption 1 is a common assumption in partially observable Petri net analysis. According to it, at any reachable marking at least one transition can fire, which guarantees the complete constructions of the positive and negative BRGs in proposed protocols. Assumption 2 is a standard assumption in fault diagnosis of Petri nets [25]. There are

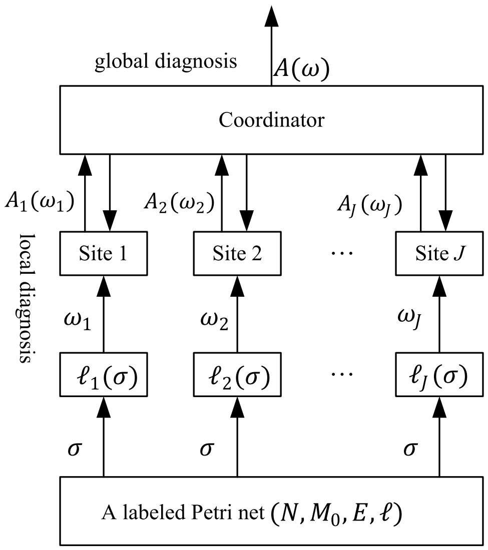



**FIGURE 1.** **Decentralized marking fault diagnosis architecture.**

no cycles of unobservable events in each site for local marking fault diagnosis in proposed protocols. Assumption 3 determines which information the coordinator knows. It is necessary for the polling strategy of proposed protocols. Assumption 4 guarantees that all transitions corresponding to each observable event can be observed by at least one local site. Assumption 5 assures that the information exchanges between the coordinator and the local sites is relative to the same sequence $\omega$. The last two assumptions guarantee correct transmission of diagnosis state between the site and the coordinator in proposed protocols.

To represent the set of faulty markings of the system, we need to use the definition of a generalized mutually exclusive constraint (GMEC) [29]. A GMEC is a function that is defined as a pair $(w, k)$, where $w \in \mathbb{Z}^m$ and $k \in \mathbb{Z}$, which determine a marking set $\mathcal{L}_{(w,k)} = \{M \in \mathbb{N}^m \mid w^T \cdot M \leq k\}$. At a marking $M$, the number of tokens of GMEC $(w, k)$ is the value of $w^T \cdot M$. We use the quantity $w^T \cdot C(\cdot, t)$ to denote the influence of $t$.

In order to verify the marking diagnosability of centralized systems, the work in [29] proposes the definition of fault language and marking diagnosability. For the sake of verifying the marking diagnosability of decentralized systems, we extend these definitions to local sites.

*Definition 3:* For a given set of faulty markings $F$, the fault language for a local site $j \in \mathcal{J}$ at a marking $M$ is defined as:

$$L_{j_{M,F}} = \{\sigma_j \in L(N, M) \mid \exists \bar{\sigma}_j \in Pr(\sigma_j), M[\bar{\sigma}_j\rangle M' \in F\},$$

where $\sigma_j$ is the sequence observed by a site $j$, $\bar{\sigma}_j$ is a strict prefix of $\sigma_j$.

Briefly speaking, this definition only requires that a marking $M'$ generated by at least one prefix of the fired transition sequence $\sigma_j$ belongs to the set of faulty markings $F$. Moreover, $L_{j_{M_0,F}}$ is called the fault language of the initial marking. The fault language of the system is similarly defined as $L_{M,F}$, and it is $L_{M_0,F}$ at the initial marking.

According to the above definition, a labeled Petri net $G = (N, M_0, E, \ell)$ with a set of faulty markings $F$ is diagnosable (w.r.t. $F$) if for the markings generated by any $\sigma$ from the initial marking $M_0$ reach $F$, there exists an integer $K_\sigma \in \mathbb{N}$ satisfing the following condition: $\forall \sigma' \in \ell^{-1}(\ell(\sigma)), \forall \sigma'' \in T^* : \sigma'\sigma'' \in L(N, M_0) \wedge |\sigma''| \geq K_\sigma \Rightarrow \sigma'\sigma'' \in L_{M_0,F}$.

*Definition 4:* Given a labeled Petri net $G = (N, M_0, E, \ell)$ monitored by a set $\mathcal{J} = \{1, 2, \ldots, J\}$ of local sites with a set of faulty markings $F = \mathcal{L}_{(w,k)}$, the set of explicit (resp., implicit) transitions for each site is $T_{E,j}$ (resp., $T_{I,j}$). The set of transitions whose influence is greater than 0 is $T_{p,j} = \{t \mid w^T \cdot C(\cdot, t) > 0\}$, and the set of transitions whose influence is less than 0 is $T_{n,j} = \{t \mid w^T \cdot C(\cdot, t) < 0\}$. For a local site $j \in \mathcal{J}$, we define the BRG w.r.t. a basis partition $\pi_j^+ = (T_{E,j}^+, T_{I,j}^+)$ as its positive BRG, where $T_{E,j}^+ = T_{o,j} \cup T_{p,j}$, which is denoted by $\mathcal{B}_j^+ = (\mathcal{M}^+, Tr_j^+, \Delta_j^+, M_0)$. The BRG w.r.t. a basis partition $\pi_j^- = (T_{E,j}^-, T_{I,j}^-)$ is defined as its negative BRG, where $T_{E,j}^- = T_{o,j} \cup T_{n,j}$, which is denoted by $\mathcal{B}_j^- = (\mathcal{M}^-, Tr_j^-, \Delta_j^-, M_0)$. We use $M_{b,j}^+$ and $M_{b,j}^-$ to represent basis markings in a positive and negative BRG of a site $j$, respectively. The relevant definitions ($T_p$, $T_n$, $T_E^+$ and $T_E^-$) of the positive (resp., negative) BRG $\mathcal{B}^+$ (resp., $\mathcal{B}^-$) of the system are defined similarly to those for the local sites.

In order to sign whether faulty markings are reachable in the positive and negative BRGs for local sites, we extend the propositions of signing faulty markings for centralized systems in [29] to decentralized systems.

*Proposition 1:* Given a labeled Petri net $G = (N, M_0, E, \ell)$ monitored by a set $\mathcal{J} = \{1, 2, \ldots, J\}$ of local sites with a set of faulty markings $F = \mathcal{L}_{(w,k)}$ and a negative BRG of a site $j$, there exists a sequence $\sigma_j \in T^*$ that satisfies $M_0[\sigma_j\rangle M \in F$ if and only if a path $\Phi_j$ in $\mathcal{B}_j^-$ holds $M_0 \xrightarrow{\Phi_j} M_{b,j}^- \in F$ and $\ell(\sigma_j) = \ell(\Phi_j)$.

*Definition 5:* A labeled Petri net $G = (N, M_0, E, \ell)$ monitored by a set $\mathcal{J} = \{1, 2, \ldots, J\}$ of local sites with a set of faulty markings $F = \mathcal{L}_{(w,k)}$ and a positive BRG of a site $j$, if $M_{b,j}^+ + C_{I,j} \cdot y \leq k$ then an arc $M_{b,j}^+ \xrightarrow{(t,y)}$ is called a faulty arc.

*Proposition 2:* Given a labeled Petri net $G = (N, M_0, E, \ell)$ monitored by a set $\mathcal{J} = \{1, 2, \ldots, J\}$ of local sites with a set of faulty markings $F = \mathcal{L}_{(w,k)}$ and a positive BRG of a site $j$, there exists a sequence $\sigma_j \in L(N, M_0) \setminus L_{j_{M_0,F}}$ if and only if in $\mathcal{B}_j^+$ a path holds: (1) $M_{b_0,j} \xrightarrow{(t_{i1},y_1)} M_{b_1,j}^+ \xrightarrow{(t_{i2},y_2)} \cdots M_{b_{n-1},j}^+ \xrightarrow{(t_{in},y_n)} M_{b_n,j}^+$ satisfies $\ell(\sigma_j) = \ell(\Phi_j)$, $\Phi_j = (t_{i1}, y_1) \cdots (t_{in}, y_n)$; (2) each arc is not a faulty arc on this path.

*Definition 6:* The dual-next function $\Omega_{d,j} : (\mathcal{M}^+ \times \Gamma_j) \times (\mathcal{M}^- \times \Gamma_j) \times (E_j \cup \{\varepsilon\}) \to (\mathcal{M}^+ \times \Gamma_j) \times (\mathcal{M}^- \times \Gamma_j)$, where $\Gamma_j = \{0, 1\}$ for a local site $j$, is denoted by: $\Omega_{d,j}((M_{b,j}^+, \gamma_j^+), (M_{b,j}^-, \gamma_j^-), e) = \{(\hat{M}_{b,j}^+, \hat{\gamma}_j^+), (\hat{M}_{b,j}^-, \hat{\gamma}_j^-)\}$

where

$$\begin{cases} (M_{b,j}^{+},(t^{+},y^{+}),\hat{M}_{b,j}^{+})\in\Delta_j^{+},(M_{b,j}^{-},(t^{-},y^{-}),\hat{M}_{b,j}^{-})\in\Delta_j^{-},\\ \ell_j^{+}(t)=\ell_j^{-}(t)=e,\\ \hat{\gamma}_j^{+}=\begin{cases}0, & \text{if } \hat{\gamma}_j^{+}=0\wedge M_{b,j}^{+}\xrightarrow{(t^{+},y^{+})} \text{ is not a faulty arc,}\\ 1, & \text{otherwise}\end{cases}\\ \hat{\gamma}_j^{-}=\begin{cases}0, & \text{if } \hat{\gamma}_j^{-}=0\wedge M_{b,j}^{-}\notin F,\\ 1, & \text{otherwise.}\end{cases}\end{cases}$$

According to Definition 6, given a labeled Petri net $G = (N, M_0, E, \ell)$ monitored by a set $\mathcal{J} = \{1, 2, \ldots, J\}$ of local sites with a set of faulty markings $F = \mathcal{L}_{(w,k)}$, the dual verifier for a site $j$ is defined as a nondeterministic automaton $\mathcal{D}_j = (D_j, E_j, \delta_j, d_0)$, where (1) $D_j \subseteq (\mathcal{M}^+ \times \Gamma_j) \times (\mathcal{M}^- \times \Gamma_j)$ is the state set, where $\Gamma_j = \{0, 1\}$; (2) $E_j$ is an alphabet; (3) the nondeterministic transition relation $\delta_j$ is defined as: for each $e \in E_j \cup \{\varepsilon\}$: $\delta_j(((M_b^+, \gamma_j^+), (M_b^-, \gamma_j^-)), e) = \Omega_{d,j}((M_b^+, \gamma_j^+), (M_b^-, \gamma_j^-), e)$; (4) $d_0 = ((M_0, 0), (M_0, 0))$ is the initial state. $\delta_j^*$ is the extension of $\delta_j$ when the observation is $\omega_j$. In the dual verifier of a site $\mathcal{D}_j$, the state such that $\gamma_j^+ = 1$ or $\gamma_j^- = 1$ is denoted by $D_{F,j}$. The dual verifier of the system is denoted by $\mathcal{D} = (D, E, \delta, d_0)$. The state such that $\gamma^+ = 1$ or $\gamma^- = 1$ is denoted by $D_{F,j}$. $\delta^*$ is the extension of $\delta$ when the observation is $\omega$.

*Definition 7:* Given a labeled Petri net $G = (N, M_0, E, \ell)$ monitored by a set $\mathcal{J} = \{1, 2, \ldots, J\}$ of local sites with $T_E^+$ and $T_E^-$, at initial marking $M_0$, if the last transition $t$ of the fired transition sequence $\sigma$ satisfies $t \in T_E \cap T_u$, then the set of basis markings is denoted by $\mathcal{M}_u(\sigma) = \{M \in \mathbb{N}^m \,|M_0[\sigma\rangle M\}$. The corresponding set of states of dual verifier is denoted by $D_u(\sigma) = \{(M^+, M^-) \,|\, M^+ \in \mathcal{M}_u(\sigma) \wedge M^- \in \mathcal{M}_u(\sigma)\}$. If the fired transition sequence is unobservable, the generated basis markings set is denoted as $M_{ui}(\sigma)$, and the corresponding set of states of dual verifier is denoted as $D_{ui}(\sigma)$. Similarly, we can get the definitions of $\mathcal{M}_{u,j}(\sigma)$, $D_{u,j}(\sigma)$, $\mathcal{M}_{ui,j}(\sigma)$ and $D_{ui,j}(\sigma)$ of a local site.

*Definition 8:* A cycle $d_{j,1} \rightarrow d_{j,2} \rightarrow \cdots \rightarrow d_{j,n} \rightarrow d_{j,1}$ in a dual verifier of a local site $j$ is called a confused cycle if $d_{j,i} = ((M_{b_i,j}^+, 0), (M_{b_i,j}^-, 1))$ for all $i = 1, \ldots, n$.

A centralized system is diagnosable if and only if there is no confused cycle in its dual verifier [29]. Similarly, we can get a theorem that a local site is diagnosable about the fault marking set $F$.

*Theorem 1:* Given a labeled Petri net $G = (N, M_0, E, \ell)$ monitored by a set $\mathcal{J} = \{1, 2, \ldots, J\}$ of local sites with a set of faulty markings $F = \mathcal{L}_{(w,k)}$, a local site $j$ is diagnosable w.r.t. to $F$ if and only if there are no confused cycles in the corresponding dual verifier $\mathcal{D}_j = (D_j, E_j, \delta_j, d_0)$.

## IV. DECENTRALIZED MARKING FAULT DIAGNOSIS PROTOCOLS AND DIAGNOSABILITY ANALYSIS

In this section, two protocols are presented to solve the marking fault diagnosis problem in a decentralized setting. Then, the diagnosability of the two protocols are analyzed.

### A. MARKING FAULT DIAGNOSIS PROTOCOLS

The diagnosis state is defined as a function $\mathcal{A} : L(\mathcal{D}) \rightarrow \{A, N, F\}$, where $L(\mathcal{D}) = \{\omega \in E^* \mid d \in D : (d_0, \omega, d) \in \delta^*\}$. Given an observation $\omega \in L(\mathcal{D})$, the corresponding diagnosis states are as follows:

$$\mathcal{A}(\omega) = \begin{cases} A, \text{ if the corresponding path of } \omega \text{ has a confused cycle}\\ N, \text{ if all corresponding paths of } \omega \text{ do not pass } F\\ F, \text{ if all corresponding paths of } \omega \text{ pass } F. \end{cases}$$

Similarly, the diagnosis state for a local site $j \in \mathcal{J}$ is defined as a function $\mathcal{A}_j : L(\mathcal{D}_j) \rightarrow \{A, N, F\}$, where $L(\mathcal{D}_j) = \{\omega_j \in E_j^* \mid d \in D : (d_0, \omega_j, d) \in \delta_j^*\}$. Given an observation $\omega \in L(\mathcal{D}_j)$, the corresponding diagnosis states are as follows:

$$\mathcal{A}_j(\omega_j) = \begin{cases} A, \text{ if the corresponding path of } \omega_j \text{ has a confused cycle}\\ N, \text{ if all corresponding paths of } \omega_j \text{ do not pass } F\\ F, \text{ if all corresponding paths of } \omega_j \text{ pass } F. \end{cases}$$

*Proposition 3:* In a labeled Petri net $G = (N, M_0, E, \ell)$, given a fired transition sequence $\sigma$ at $M_0$, for each local site $j \in \mathcal{J}$, there exists $D_u(\sigma) \subseteq D_{u,j}(\sigma)$.

*Proof:* For each local site $j \in \mathcal{J}$, there exists $T_u^+ \subseteq T_{u,j}^+$ and $T_u^- \subseteq T_{u,j}^-$ in $T_{E,j}^+ \subseteq T_E^+$ and $T_{E,j}^- \subseteq T_E^-$. According to Definition 7, we can know that $\mathcal{M}_u(\sigma) \subseteq \mathcal{M}_{u,j}(\sigma)$. Then, we can infer that $D_u(\sigma) \subseteq D_{u,j}(\sigma)$. ■

The following proposition is the rule by which the coordinator determines whether the system is normal based on the information from the local sites.

*Proposition 4:* Given a labeled Petri net $G = (N, M_0, E, \ell)$, considering the words $\omega \in L(G)$ observed at $M_0$, if there exists a local site $j \in \mathcal{J}$ whose diagnosis state is $\mathcal{A}_j(\omega_j) = N$, then the diagnosis state of the system is $\mathcal{A}(\omega) = N$.

*Proof:* If there is a local site $j \in \mathcal{J}$ whose diagnosis state is $\mathcal{A}_j(\omega_j) = N$, then according to the definition of $\mathcal{A}(\omega)$, it has no confused cycles in its dual verifier and none of its paths are passed faulty markings. According to the Proposition 3, there are also no confused cycles in the dual verifier of the system and none of the paths are passed faulty markings. Therefore, the diagnosis state of the system is $\mathcal{A}(\omega) = N$. ■

In Protocol 1, after a new transition $t \in T_{o,j}$ fires, each local site $j \in \mathcal{J}$ receives an observable event associated with this transition. Then, each site computes the corresponding positive BRG $\mathcal{B}_j^+$, negative BRG $\mathcal{B}_j^-$ and dual verifier $\mathcal{D}_j$. If there exists a confused cycle in $\mathcal{D}_j$, the site $j \in \mathcal{J}$ sends $\mathcal{A}_j(\omega_j) = A$ to the coordinator. If no confused cycle exists in $\mathcal{D}_j$, the site $j \in \mathcal{J}$ sends $F$ to the coordinator when $(\gamma_j^+, \gamma_j^-) = (1, 1)$, otherwise the site $j$ sends $N$. If there is an confused cycle in the local site $j \in \mathcal{J}$, then there is also a confused cycle in the system. Therefore, we cannot determine whether a fault has occurred, and the coordinator updates the diagnosis state to $\mathcal{A}(\omega) = A$. If the local site $j \in \mathcal{J}$ detects a fault, then the system is faulty and the coordinator updates the

**Algorithm 1** Protocol

**Input:** A labeled Petri net $G = (N, M_0, E, \ell)$ and a set of faulty markings $F$.

**Output:** $\mathcal{A}(\omega)$.

1: Wait until a new observable transition $t \in T_o$ fires;
2: Steps performed by each site $j \in \mathcal{J}$:
3: Let $\omega_j' := \omega_j$ and $\omega_j := \omega_j'\ell_j(t)$;
4: Site $j$ computes the positive BRG $\mathcal{B}_j^+$ and the negative BRG $\mathcal{B}_j^-$;
5: Site $j$ computes the dual verifier $\mathcal{D}_j$;
6: **if** there exist confused cycles in $\mathcal{D}_j$ **then**
7: Site $j$ transmits $\mathcal{A}_j(\omega_j) = A$ to the coordinator;
8: **end if**
9: **if** there are no confused cycles in $\mathcal{D}_j$ **then**
10: **if** $(\gamma_j^+, \gamma_j^-) = (1, 1)$ **then**
11: Site $j$ transmits $\mathcal{A}_j(\omega_j) = F$ to the coordinator;
12: **else**
13: Site $j$ transmits $\mathcal{A}_j(\omega_j) = N$ to the coordinator;
14: **end if**
15: **end if**
16: Steps performed by the coordinator:
17: **if** $\mathcal{A}_j(\omega_j) = A$ **then**
18: Outputs $\mathcal{A}(\omega) = A$, terminates the algorithm;
19: **end if**
20: **if** $\mathcal{A}_j(\omega_j) = F$ **then**
21: Outputs $\mathcal{A}(\omega) = F$;
22: **end if**
23: **if** $\mathcal{A}_j(\omega_j) = N$ **then**
24: Outputs $\mathcal{A}(\omega) = N$, go to Step 1.
25: **end if**

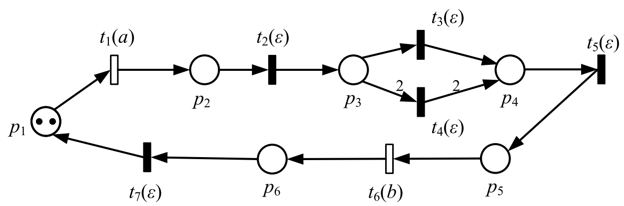



**FIGURE 2.** A labeled Petri net.

diagnosis state to $\mathcal{A}(\omega) = F$. If the behavior of the local site $j \in \mathcal{J}$ is normal, then so is the system, and the coordinator updates the diagnosis state to $\mathcal{A}(\omega) = N$. In this case, the algorithm goes to step 1 and continues to wait for a new event to occur.

*Example 1:* Consider the labeled Petri net with a set of faulty markings $F = \mathcal{L}_{(w,k)} = \{M \in \mathbb{N}^6 \mid M(p_2)+2M(p_3) \geq 3\}$ in Fig. 2, where $w = [0, -1, -2, 0, 0, 0]^T$, $k = -3$. Assume that the sets of the positive explicit transitions and the negative explicit transitions of the site 1 (resp., 2) are $T_{E,1}^+ = \{t_1, t_3, t_4\}$ and $T_{E,1}^- = \{t_1, t_2\}$ (resp., $T_{E,2}^+ = \{t_3, t_4, t_6\}$ and $T_{E,2}^- = \{t_1, t_2, t_6\}$). The positive basis markings of the site 1 are $M_0^+ = [2, 0, 0, 0, 0, 0]^T$, $M_1^+ = [1, 1, 0, 0, 0, 0]^T$,

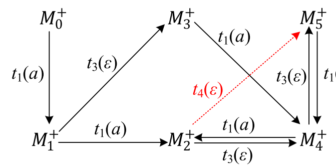



**FIGURE 3.** The positive BRG $\mathcal{B}_1^+$ of the local site 1. The faulty arcs are marked by dashed arcs.

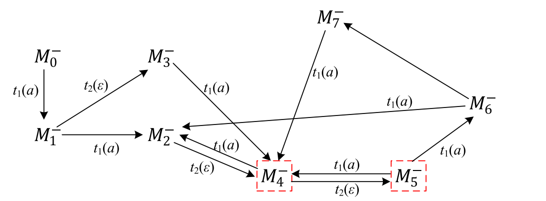



**FIGURE 4.** The negative BRG $\mathcal{B}_1^-$ of the local site 1. The dashed boxs denote the fault markings.

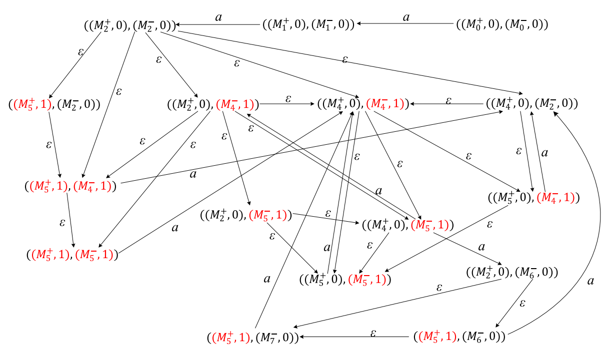


**FIGURE 5.** Part of the dual verifier of the local site 1.

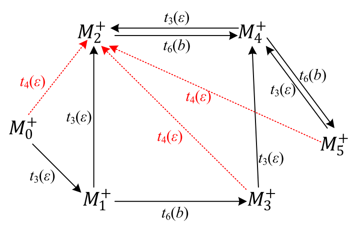



**FIGURE 6.** The positive BRG $\mathcal{B}_2^+$ of the local site 2.

$M_2^+ = [0, 2, 0, 0, 0, 0]^T$, $M_3^+ = [1, 0, 0, 1, 0, 0]^T$, $M_4^+ = [0, 1, 0, 1, 0, 0]^T$, $M_5^+ = [0, 0, 0, 2, 0, 0]^T$. The negative basis markings of the site 1 are $M_0^- = [2, 0, 0, 0, 0, 0]^T$, $M_1^- = [1, 1, 0, 0, 0, 0]^T$, $M_2^- = [0, 2, 0, 0, 0, 0]^T$, $M_3^- = [1, 0, 1, 0, 0, 0]^T$, $M_4^- = [0, 1, 1, 0, 0, 0]^T$, $M_5^- = [0, 0, 2, 0, 0, 0]^T$, $M_6^- = [0, 1, 0, 1, 0, 0]^T$, $M_7^- = [0, 0, 1, 1, 0, 0]^T$. The positive basis markings of the site 2 are $M_0^+ = [2, 0, 0, 0, 0, 0]^T$, $M_1^+ = [1, 0, 0, 1, 0, 0]^T$, $M_2^+ = [0, 0, 0, 2, 0, 0]^T$, $M_3^+ = [1, 0, 0, 0, 0, 1]^T$, $M_4^+ = [0, 0, 0, 1, 0, 1]^T$, $M_5^+ = [0, 0, 0, 0, 0, 2]^T$. The negative

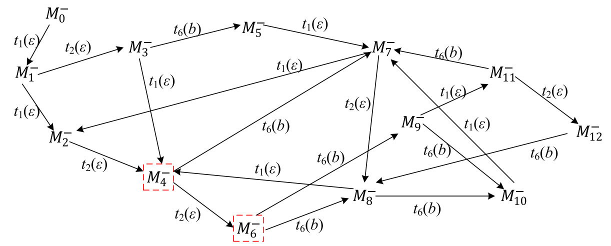



**FIGURE 7.** The negative BRG $\mathcal{B}_2^-$ of the local site 2.

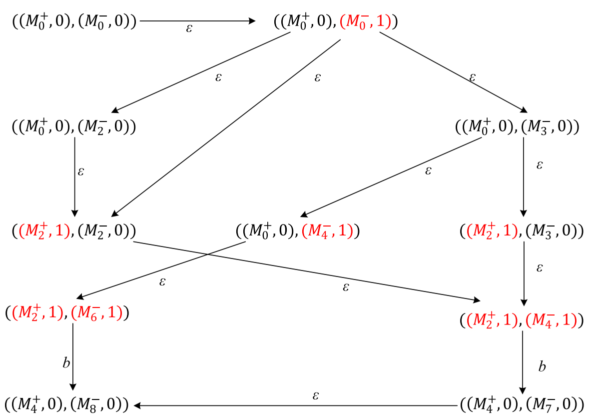



**FIGURE 8.** Part of the dual verifier of the local site 2.

basis markings of the site 2 are $M_0^- = [2, 0, 0, 0, 0, 0]^T$, $M_1^- = [1, 1, 0, 0, 0, 0]^T$, $M_2^- = [0, 2, 0, 0, 0, 0]^T$, $M_3^- = [1, 0, 1, 0, 0, 0]^T$, $M_4^- = [0, 1, 1, 0, 0, 0]^T$, $M_5^- = [1, 0, 0, 0, 0, 1]^T$, $M_6^- = [0, 0, 2, 0, 0, 0]^T$, $M_7^- = [0, 1, 0, 0, 0, 1]^T$, $M_8^- = [0, 0, 1, 0, 0, 1]^T$, $M_9^- = [0, 0, 0, 1, 0, 1]^T$, $M_{10}^- = [0, 0, 0, 0, 0, 2]^T$, $M_{11}^- = [0, 1, 0, 1, 0, 0]^T$, $M_{12}^- = [0, 0, 1, 1, 0, 0]^T$. There are 25 states in the dual verifier of the site 1. Fig. 5 only shows part of it. There are 66 states in the dual verifier of the site 2, and Fig. 8 only shows part of it.

The dual verifier of the site 1 has a path $((M_2^+, 0), (M_4^-, 1)) \xrightarrow{\varepsilon} ((M_4^+, 0), (M_4^-, 1)) \xrightarrow{\varepsilon} ((M_4^+, 0), (M_5^-, 1)) \xrightarrow{a} ((M_2^+, 0), (M_4^-, 1))$ that is a confused cycle, then the system cannot detect the faults. The dual verifier of the site 2 has no confused cycles, and the system can determine some faulty markings. Finally, the faults can only be determined by the site 2.

It is worth noting that when the diagnosis state of the coordinator by using Protocol 1 is $\mathcal{A}(\omega) = A$, the centralized diagnosis state is $F$, indicating that the capability of marking fault diagnosis in a decentralized setting under Protocol 1 is weaker than that in a centralized setting. Therefore, we propose Protocol 2 to further improve the diagnosis capability of marking fault diagnosis in a decentralized setting.

In Protocol 2, after a new transition $t \in T_{o,j}$ fires, each local site $j \in \mathcal{J}$ receives an observable event associated with this transition. Then, each site computes the corresponding positive BRG $\mathcal{B}_j^+$, negative BRG $\mathcal{B}_j^-$ and dual verifier $\mathcal{D}_j$. If there exists a confused cycle in $\mathcal{D}_j$, the site $j \in \mathcal{J}$ sends $\mathcal{A}_j(\omega_j) = A$, $Y^+_{min,j}(M, t)$ and $Y^-_{min,j}(M, t)$ to the coordinator. If no confused cycle exists in $\mathcal{D}_j$, the site $j \in \mathcal{J}$ sends $F$ to the coordinator when $(\gamma_j^+, \gamma_j^-) = (1, 1)$, otherwise the site $j$ sends $N$. If there is a confused cycle in the local site $j \in \mathcal{J}$, the coordinator determines whether the fired transition $t$ and transitions in $Y^+_{min,j}(M, t)$ and $Y^-_{min,j}(M, t)$ are observable for the system but unobservable for the site $j \in \mathcal{J}$. If there is such a transition, then the coordinator deletes the corresponding arcs in $\mathcal{D}_j$ and the algorithm goes to step 1. If there is no such a transition, then there is also a confused cycle in the system. Therefore, the system is undiagnosable, and the coordinator updates the diagnosis state to $\mathcal{A}(\omega) = A$. If the behavior of the local site $j \in \mathcal{J}$ is normal, then so is the system, and the

---

**Algorithm 2** Protocol

**Input:** A labeled Petri net $G = (N, M_0, E, \ell)$ and a set of faulty markings $F$.
**Output:** $\mathcal{A}(\omega)$.

```
1:  Wait until a new observable transition t ∈ T_o fires;
2:  Steps performed by each site j ∈ J:
3:  Let ω'_j := ω_j and ω_j := ω'_j ℓ_j(t);
4:  Site j computes the positive BRG B_j^+ and the negative BRG B_j^-;
5:  Site j computes the dual verifier D_j;
6:  if there exist confused cycles in D_j then
7:      Site j transmits A_j(ω_j) = A, Y^+_{min,j}(M, t) and Y^-_{min,j}(M, t) to the coordinator;
8:  end if
9:  if there are no confused cycles in D_j then
10:     if (γ_j^+, γ_j^-) = (1, 1) then
11:         Site j transmits A_j(ω_j) = F to the coordinator;
12:     else
13:         Site j transmits A_j(ω_j) = N to the coordinator;
14:     end if
15: end if
16: Steps performed by the coordinator:
17: if A_j(ω_j) = A then
18:     if the transition t is observable for system but unobservable for the local site j ∈ J or the transitions in Y^+_{min,j}(M, t) or Y^-_{min,j}(M, t) are observable for system but unobservable for the local site j ∈ J then
19:         Delete the corresponding arcs, go to Step 1;
20:     else
21:         Outputs A(ω) = A, terminates the algorithm;
22:     end if
23: end if
24: if A_j(ω_j) = F then
25:     Outputs A(ω) = F;
26: end if
27: if A_j(ω_j) = N then
28:     Outputs A(ω) = N, go to Step 1.
29: end if
```

coordinator updates the diagnosis state to $\mathcal{A}(\omega) = N$. In this case, the algorithm goes to step 1 and continues to wait for a new event to occur.

*Example 2:* Consider the labeled Petri net with a set of faulty markings $F = \mathcal{L}_{(w,k)} = \{M \in \mathbb{N}^6 \mid M(p_2) + 2M(p_3) \geq 3\}$ in Fig. 2 again. The assumptions are the same as Example. 1. The dual verifier of the site 1 that is not processed by Protocol 2 is shown in Fig. 5. The dual verifier of the site 2 that is not processed by Protocol 2 is shown in Fig. 8. The dual verifier of the site 1 has a path $((M_2^+, 0), (M_4^-, 1)) \xrightarrow{\varepsilon} ((M_4^+, 0), (M_4^-, 1)) \xrightarrow{\varepsilon} ((M_4^+, 0), (M_5^-, 1)) \xrightarrow{a} ((M_2^+, 0), (M_4^-, 1))$ that is a confused cycle. Since the minimal explanation vectors of the fired transition $t_1$ in the path $((M_4^+, 0), (M_5^-, 1)) \xrightarrow{a} ((M_2^+, 0), (M_4^-, 1))$ contain the transition $t_6$ which is observable for the system but unobservable for the site 1, according to Protocol 2, the corresponding arc is deleted. Similarly, such arcs in confused cycles $((M_2^+, 0), (M_4^-, 1)) \xrightarrow{\varepsilon} ((M_2^+, 0), (M_5^-, 1)) \xrightarrow{\varepsilon} ((M_4^+, 0), (M_5^-, 1)) \xrightarrow{a} ((M_2^+, 0), (M_4^-, 1))$ and $((M_4^+, 0), (M_4^-, 1)) \xrightarrow{a} ((M_5^+, 0), (M_5^-, 1)) \xrightarrow{a} ((M_4^+, 0), (M_4^-, 1))$ are deleted. Then, the faulty markings can be detected. The dual verifier of the site 2 has no confused cycles, and the system can determine some faulty markings.

In Protocols 1 and 2, when each local site $j \in \mathcal{J}$ computes positive and negative BRGs, in the worst case, if all transitions in the Petri net belong to the explicit transitions set, the computational complexity is the same as the complexity of constructing reachable graphs. For a positive BRG and negative BRG with $|M_1|$ and $|M_2|$ basis markings of each local site $j \in \mathcal{J}$, the dual verifier of the site $j$ has at most $2 \cdot |M_1| \cdot |M_2|$ states. The complexity of constructing the dual verifier of each site $j$ is $O(|M_1| \cdot |M_2|)$. Since the two protocols simply exchange information between the sites and the coordinator, the complexity of each diagnosis protocol is the same as the complexity of constructing the dual verifier.

### B. DIAGNOSABILITY ANALYSIS

By using Protocol 1, we prove a sufficient condition for the system to realize marking fault diagnosis in a decentralized setting, which is proved below.

*Proposition 5:* Given a labeled Petri net $G = (N, M_0, E, \ell)$ with faulty markings $F = \mathcal{L}_{(w,k)}$ supervised by a set $\mathcal{J} = \{1, 2, \ldots, J\}$ of local sites. According to Protocol 1, if the site $j \in \mathcal{J}$ is diagnosable, then the decentralized system is diagnosable.

*Proof:* According to Theorem 1, the site $j$ is diagnosable w.r.t. $F$ if its dual verifier does not contain any confused cycles. Therefore, it is only necessary to prove that there are no confused cycles in the dual verifier $\mathcal{D}_j$ of any local sites, then there are no confused cycles in the dual verifier $\mathcal{D}$ of the system. If the site $j \in \mathcal{J}$ is diagnosable, there are no confused cycles in its dual verifier $\mathcal{D}_j$. According to Proposition 3, $\mathcal{M}_{ui}(\sigma) \subseteq \mathcal{M}_{ui,j}(\sigma)$ and $D_F \subseteq D_{F,j}$. Therefore, if there are no confused cycles in the dual verifier $\mathcal{D}_j$ of sites, there are no confused cycles in the system. That is, the system is diagnosable. ∎

We prove a sufficient and necessary condition for marking fault diagnosis in a decentralized architecture by applying Protocol 2. The following proposition proves diagnosability regarding Protocol 2.

*Proposition 6:* Given a labeled Petri net $G = (N, M_0, E, \ell)$ with faulty markings $F = \mathcal{L}_{(w,k)}$ supervised by a set $\mathcal{J} = \{1, 2, \ldots, J\}$ of local sites. The system is diagnosable, if and only if any one site is diagnosable by Protocol 2.

*Proof:* According to Theorem 4.1 in [29], the labeled Petri net is diagnosable if its dual verifier does not contain any confused cycles. Therefore, it is only necessary to prove that there are no confused cycles in the dual verifier of the system, if and only if there are no confused cycles in the dual verifier of any sites.

*If*: The proof is the same as that of Proposition 5.

*Only if*: If the system is diagnosable, there are no confused cycles in its dual verifier $\mathcal{D}$. If the fault markings $M_f \in F$ are present in the positive and negative BRGs, the corresponding tag ($\gamma^+$ or $\gamma^-$) in the dual verifier changes from 0 to 1. Since $T_{p,j} = T_p$ and $T_{n,j} = T_n$, if a fault occurs, both the system and the sites can reach state (1,1). Since there are no confused cycles in the dual verifier $\mathcal{D}$ of the system, the dual verifier $\mathcal{D}_j$ of the local site $j$ also has no confused cycles for the part of the system corresponding to the state (1,1). In Protocol 2, if there are confused cycles in the dual verifier $\mathcal{D}_j$ of the site $j$, but there are transitions in fired transition sequence or the minimal explanation vectors set of the sequence in confused cycles are observable for the system but unobservable for some sites, then the corresponding arcs are deleted. Thus, the dual verifier of each site $j$ does not contain confused cycles. The decentralized system is diagnosable by Protocol 2. ∎

In Protocol 1, the local sites only send diagnosis states to the coordinator and receive no information from the coordinator when calculating diagnosis states. Thus, the existence of no confused cycles is a necessary condition for the diagnosability of decentralized systems. In Protocol 2, the local sites do not only send diagnosis states to the coordinator, but also send the minimal explanation vectors of the fired transition sequence when there are confused cycles. Then they generate new diagnosis states according to the feedback information of the coordinator. Therefore, we can determine whether the decentralized system is diagnosable even if there is an confused cycle in the local site.

## V. EXAMPLE

A labeled Petri net describing the process in logistics sorting system is depicted in Fig. 9.

Tokens in place $p_1$ mean that the logistics center is ready to sort packages. Transitions $t_1 - t_3$ are the operations before sorting. Transitions $t_4 - t_6$ describe the process of manually scanning the code into the system of small packages and other packages that are not convenient to use conveyor belts. Transitions $t_7 - t_{10}$ denote the process of scanning information of other packages transported to the package supply station through the conveyor belt. Transition $t_{11}$ indicates the gate to which the system confirms the package should be shipped.

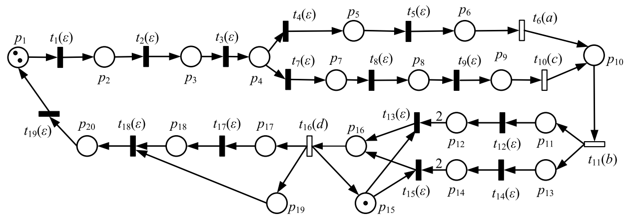



**FIGURE 9.** A labeled Petri net describing the process in logistics sorting system.

**TABLE 1.** The place meaning of labeled Petri net model of process in logistics sorting system.

| Place | Meaning |
|---|---|
| $p_1$ | goods arrived |
| $p_2$ | completion of unloading |
| $p_3$ | security check completed |
| $p_4$ | safety zone |
| $p_5$ | wait for scanning information after unwrapping |
| $p_6$ | information scan completed |
| $p_7$ | sorting completed |
| $p_8$ | Packages have been put onto the conveyor belt |
| $p_9$ | arrive at the packet supply station |
| $p_{10}$ | information scan completed |
| $p_{11}, p_{13}$ | The gate to be delivered has been confirmed |
| $p_{12}, p_{14}$ | The package has been delivered to the correct gate |
| $p_{15}$ | staff in place |
| $p_{16}$ | seal wrap completed |
| $p_{17}$ | information scan completed |
| $p_{18}$ | loading completed |
| $p_{19}$ | stow weighing completed, wait for temporary storage |
| $p_{20}$ | delivery completed |

Transitions $t_{12} - t_{15}$ represent the process of two sorting lines moving packages to the correct grid and sealing the bags. Transitions $t_{16} - t_{19}$ represent the process of scanning packages, loading vehicles, and notifying the arrival of new goods. The place meaning of labeled Petri net model of process in logistics sorting system is shown in Table 1. The transition meaning of labeled Petri net model of process in logistics sorting system is shown in Table 2. Each grid has a maximum capacity of two tokens. In the sorting process, if the number of tokens of the grid $(p_{12}, p_{14})$ is greater than or equal to 2, the faults have occurred. The set of faulty markings of this system is $F = \{M \mid M(p_{12}) \geq 2 \text{ or } M(p_{14}) \geq 2\}$. The set of observable transitions is $T_o = \{t_6, t_{10}, t_{11}, t_{16}\}$. There are four sensors in the system that can observe the signal change and output the symbols $a, b, c, d$. The set of labels of observable events is $E = \{a, b, c, d\}$. Site 1 communicates with the corresponding sensors to observe the output of labels $a, c, d$. Site 2 communicates with the corresponding sensors to observe the output of labels $b, d$.

The set of observable transitions of site 1 is $T_{o,1} = \{t_6, t_{10}, t_{16}\}$, where the set of positive explicit transitions is $T^+_{E,1} = \{t_6, t_{10}, t_{13}, t_{15}, t_{16}\}$, and the set of negative explicit transitions is $T^-_{E,1} = \{t_6, t_{10}, t_{12}, t_{14}, t_{16}\}$. The dual verifier has 119 states, and does not contain confused cycles. Finally, it can arrive the state $((M^+_3, 1), (M^-_8, 1))$ that is tagged by double 1, and faults can be detected.

**TABLE 2.** The transition meaning of labeled Petri net model of process in logistics sorting system.

| Transition | Meaning |
|---|---|
| $t_1$ | unload |
| $t_2$ | security check |
| $t_3$ | transport to safety zone |
| $t_4$ | unwrap small packages |
| $t_5$ | scan the package message |
| $t_6$ | enter the information into the system |
| $t_7$ | sort non-small packages |
| $t_8$ | put packages on the conveyor belt |
| $t_9$ | transport packages to packet supply stations |
| $t_{10}$ | scan the package information by the machine |
| $t_{11}$ | confirm package sorting gate |
| $t_{12}, t_{14}$ | deliver the package to the correct gate |
| $t_{13}, t_{15}$ | wrap bag of package |
| $t_{16}$ | scan bags information |
| $t_{17}$ | load bags |
| $t_{18}$ | dispatch |
| $t_{19}$ | send a message to let new goods in |

The set of observable transitions of site 2 is $T_{o,2} = \{t_{11}, t_{16}\}$, where the set of positive explicit transitions is $T^+_{E,2} = \{t_{11}, t_{13}, t_{15}, t_{16}\}$, and the set of negative explicit transitions is $T^-_{E,2} = \{t_6, t_{10}, t_{12}, t_{14}, t_{16}\}$. The dual verifier has 119 states, and does not contain confused cycles. Finally, it can arrive the state $((M^+_4, 1), (M^-_8, 1))$ that is tagged by double 1, and faults can be detected.

According to Protocol 1, there are no confused cycles in the dual verifiers of the two local sites, $(\gamma^+_1, \gamma^-_1) = (1, 1)$ and $(\gamma^+_2, \gamma^-_2) = (1, 1)$. The two sites all send the diagnosis state $\mathcal{A}_j(\omega_j) = F$ to the coordinator. The faulty markings can be detected. By Protocol 2, site 1 reaches the state $(\gamma^+_1, \gamma^-_1) = (1, 1)$, and site 2 reaches the state $(\gamma^+_2, \gamma^-_2) = (1, 1)$. The dual verifiers of the two local sites have no confused cycles, then they send the diagnosis state $\mathcal{A}_j(\omega_j) = F$ to the coordinator. The faulty markings can also be detected.

## VI. CONCLUSION

In this paper, a new diagnosis strategy in the decentralized setting is proposed. We extend the centralized marking fault diagnosis method proposed in [29] to the decentralized setting. In order to achieve this, two protocols executed by a set of local sites and a coordinator are proposed. Under the first protocol, the coordinator simply accepts the diagnosis states sent by the local sites. Applying Protocol 2, the coordinator makes global decisions by the diagnosis states and information sent by the local sites. Therefore, Protocol 2 has better diagnosis capability than Protocol 1. Future work will focus on on-line marking fault diagnosis.

## REFERENCES

[1] M. Bahrami, M. Fotuhi-Firuzabad, and H. Farzin, "Reliability evaluation of power grids considering integrity attacks against substation protective IEDs," *IEEE Trans. Ind. Informat.*, vol. 16, no. 2, pp. 1035–1044, Feb. 2020.

[2] B. A. Nesrine, A. Said, and M. Hassani, "Switching models and control of Petri nets with shared resources under marking constraints," *Int. J. Comput. Integr. Manuf.*, vol. 35, no. 2, pp. 113–128, Feb. 2022.

[3] F. Lin, W. Wang, L. Han, and B. Shen, "State estimation of multichannel networked discrete event systems," *IEEE Trans. Control Netw. Syst.*, vol. 7, no. 1, pp. 53–63, Mar. 2020.

[4] C. Gerini and A. Sciomachen, "Evaluation of the flow of goods at a warehouse logistic department by Petri nets," *Flexible Services Manuf. J.*, vol. 31, no. 2, pp. 354–380, Jun. 2019.

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

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

[7] A. Al-Ajeli and D. Parker, "Fault diagnosis in labelled Petri nets: A Fourier–Motzkin based approach," *Automatica*, vol. 132, Oct. 2021, Art. no. 109831.

[8] L. Cao, S. Shu, F. Lin, Q. Chen, and C. Liu, "Weak diagnosability of discrete-event systems," *IEEE Trans. Control Netw. Syst.*, vol. 9, no. 1, pp. 184–196, Mar. 2022.

[9] G. Zhu, L. Feng, Z. Li, and N. Wu, "An efficient fault diagnosis approach based on integer linear programming for labeled Petri nets," *IEEE Trans. Autom. Control*, vol. 66, no. 5, pp. 2393–2398, May 2021.

[10] L. Belkacem, L. Mhamdi, Z. Simeu-Abazi, H. Messaoud, and E. Gascard, "Diagnosis of hybrid dynamical systems through hybrid automata," *IFAC-PapersOnLine*, vol. 49, no. 12, pp. 990–995, 2016.

[11] Y. Hu, Z. Ma, Z. Li, and A. Giua, "Diagnosability enforcement in labeled Petri nets using supervisory control," *Automatica*, vol. 131, Sep. 2021, Art. no. 109776.

[12] Z. Zhao, P. X. Liu, and J. Gao, "Model-based fault diagnosis methods for systems with stochastic process—A survey," *Neurocomputing*, vol. 513, pp. 137–152, Nov. 2022.

[13] S. Li, S. Zhou, L. Yin, and R. Jiang, "Robust diagnosability analysis using basis reachability graph," *IEEE Access*, vol. 11, pp. 9751–9762, 2023.

[14] D. Lefebvre, Z. Li, and Y. Liang, "Diagnosis of timed patterns for discrete event systems by means of state isolation," *Automatica*, vol. 153, Jul. 2023, Art. no. 111045.

[15] Z. He, Z. Li, A. Giua, F. Basile, and C. Seatzu, "Some remarks on 'State estimation and fault diagnosis of labeled time Petri net systems with unobservable transition,'" *IEEE Trans. Autom. Control*, vol. 64, no. 12, pp. 5253–5259, Dec. 2019.

[16] G. S. Viana, M. V. S. Alves, and J. C. Basilio, "Codiagnosability of networked discrete event systems with timing structure," *IEEE Trans. Autom. Control*, vol. 67, no. 8, pp. 3933–3948, Aug. 2022.

[17] V. D. L. Oliveira, F. G. Cabral, and M. V. Moreira, "$K$-loss robust codiagnosability of Discrete-Event Systems," *Automatica*, vol. 140, Jun. 2022, Art. no. 110222.

[18] G. S. Viana and J. C. Basilio, "Codiagnosability of discrete event systems revisited: A new necessary and sufficient condition and its applications," *Automatica*, vol. 101, pp. 354–364, Mar. 2019.

[19] M. Z. M. Veras, F. G. Cabral, and M. V. Moreira, "Distributed synchronous diagnosis of discrete event systems modeled as automata," *Control Eng. Pract.*, vol. 115, Oct. 2021, Art. no. 104892.

[20] A. Wada and S. Takai, "Decentralized diagnosis of discrete event systems subject to permanent sensor failures," *Discrete Event Dyn. Syst.*, vol. 32, no. 2, pp. 159–193, Jun. 2022.

[21] X. Cong, M. P. Fanti, A. M. Mangini, and Z. Li, "Critical observability verification and enforcement of labeled Petri nets by using basis markings," *IEEE Trans. Autom. Control*, early access, Jul. 5, 2023, doi: 10.1109/TAC.2023.3292747.

[22] W. Shi, Z. He, Z. Ma, N. Ran, and X. Yin, "Security-preserving multi-robot path planning for Boolean specification tasks using labeled Petri nets," *IEEE Control Syst. Lett.*, vol. 7, pp. 2017–2022, 2023.

[23] M. P. Cabasino, A. Giua, A. Paoli, and C. Seatzu, "Decentralized diagnosability analysis of discrete event systems using Petri nets," *IFAC Proc. Volumes*, vol. 44, no. 1, pp. 6060–6066, Jan. 2011.

[24] M. P. Cabasino, A. Giua, A. Paoli, and C. Seatzu, "Decentralized diagnosis of discrete-event systems using labeled Petri nets," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 43, no. 6, pp. 1477–1485, Nov. 2013.

[25] X. Cong, M. P. Fanti, A. M. Mangini, and Z. Li, "Decentralized diagnosis by Petri nets and integer linear programming," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 48, no. 10, pp. 1689–1700, Oct. 2018.

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

[27] N. Ran, J. Hao, Z. Dong, Z. He, Z. Liu, Y. Ruan, and S. Wang, "K-codiagnosability verification of labeled Petri nets," *IEEE Access*, vol. 7, pp. 185055–185062, 2019.

[28] P. Bonhomme, "Decentralized state estimation and diagnosis of P-time labeled Petri nets systems," *Discrete Event Dyn. Syst.*, vol. 31, no. 1, pp. 137–162, Mar. 2021.

[29] Z. Ma, X. Yin, and Z. Li, "Marking diagnosability verification in labeled Petri nets," *Automatica*, vol. 131, Sep. 2021, Art. no. 109713.

[30] C. G. Cassandras and S. Lafortune, *Introduction to Discrete Event Systems*, 3rd ed. Cham, Switzerland: Springer, 2021.

[31] Z. Ma, Y. Tong, Z. Li, and A. Giua, "Basis marking representation of Petri net reachability spaces and its application to the reachability problem," *IEEE Trans. Autom. Control*, vol. 62, no. 3, pp. 1078–1093, Mar. 2017.

[32] Z. Yu, X. Duan, X. Cong, X. Li, and L. Zheng, "Detection of actuator enablement attacks by Petri nets in supervisory control systems," *Mathematics*, vol. 11, no. 4, Feb. 2023, Art. no. 943.

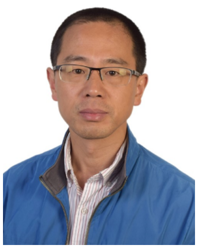
[33] X. Cong, M. P. Fanti, A. M. Mangini, and Z. Li, "Critical observability of labeled time Petri net systems," *IEEE Trans. Autom. Sci. Eng.*, vol. 20, no. 4, pp. 2063–2074, Jul. 2023.

[34] Z. Yu, A. Sohail, M. Jamil, O. A. Beg, and J. M. R. S. Tavares, "Hybrid algorithm for the classification of fractal designs and images," *Fractals*, 2022, doi: 10.1142/S0218348X23400030.

[35] N. Ran, J. Hao, and C. Seatzu, "Prognosability analysis and enforcement of bounded labeled Petri nets," *IEEE Trans. Autom. Control*, vol. 67, no. 10, pp. 5541–5547, Oct. 2022.

[36] Z. Yu, H. Gao, X. Cong, N. Wu, and H. H. Song, "A survey on cyber-physical systems security," *IEEE Internet Things J.*, 2023, doi: 10.1109/JIOT.2023.3289625.

[37] N. Ran, T. Li, Z. He, and C. Seatzu, "Codiagnosability enforcement in labeled Petri nets," *IEEE Trans. Autom. Control*, vol. 68, no. 4, pp. 2436–2443, Apr. 2023.



**ZHENHUA YU** (Member, IEEE) received the B.S. and M.S. degrees from Xidian University, Xi'an, China, in 1999 and 2003, respectively, and the Ph.D. degree from Xi'an Jiaotong University, Xi'an, in 2006. He is currently a Professor with the College of Computer Science and Technology, Institute of System Security and Control, Xi'an University of Science and Technology, Xi'an. He has authored more than 30 technical articles in conferences and journals and holds two invention patents. His research mainly focuses on cyber-physical systems, unmanned aerial vehicles, multi-agent systems, artificial intelligence system security, and nonlinear dynamical systems.

**YINYIN QI** received the B.S. degree in e-commerce from Weinan Normal University, Weinan, China, in 2020. She is currently pursuing the M.S. degree in computer science and technology with the Xi'an University of Science and Technology, Xi'an, China. Her current research interests include discrete event systems, labeled petri nets, and fault diagnosis.

**XUYA CONG** (Member, IEEE) received the B.S. degree in automation from Xidian University, Xi'an, China, in 2014, and the dual Ph.D. degrees in control theory and control engineering and in electrical and information engineering from Xidian University and the Polytechnic University of Bari, Bari, Italy, in 2020. He is currently a Lecturer with the College of Computer Science and Technology, Xi'an University of Science and Technology, Xi'an. His current research interests include critical observability, opacity, supervisory control, state estimation of discrete event systems, and cyber-physical systems.