Diagnosability Verification in Petri Nets Under Unknown Initial Marking

Yushan Li[1], Shaopeng Hu[2], Yufeng Chen[1], and Zhiwu Li[1]

Abstract— **This paper formalizes and addresses the diagnosability verification for discrete event systems modeled with Petri nets under unknown initial markings, where part or all of the places are unobservable at an initial marking. A minimal initial marking model is constructed to verify the diagnosability of the original system. Specifically, the model contains the least initial total number of tokens and allows that any transition can be potentially fired. This procedure employs a nondeterministic finite state automaton, called an extended verifier, that is derived from the reachability graph of the proposed model. We prove that a plant under unknown initial markings is diagnosable if and only if the verifier does not contain some particular paths. Examples are presented to demonstrate the proposed method.**

Index Terms— **Diagnosability verification, discrete event system, Petri net, unknown initial marking**

I. Introduction

Ensuring the timely detection and accurate identification of faults is essential for the reliable functioning of discrete-event systems (DESs) [1]. Such systems are commonly encountered in a variety of application domains, including automated manufacturing environments, electrical power networks, and urban transportation infrastructures. In Petri nets, the initial marking may be unknown or uncertain, which can lead to difficulties in analyzing and verifying the behavior of the system [2]. The objective of diagnosis, as studied in [3]–[6], is to determine whether unobservable fault events take place in a system based on the observations available to an external observer. A partially observed discrete event system is considered diagnosable if every fault can be identified within a finite observation delay after its occurrence.

Related problems of diagnosability verification in DESs have been extensively studied over the past decades [7]–[11]. As far as we know, the works in [7]–[8] first verify diagnosability in DESs by designing a diagnoser. However, the structural complexity of establishing a diagnoser is exponential wrt the state size of the considered plant. In order to reduce the computational burden, the studies in [9] and [10] propose a structure, called a verifier, to test the diagnosability, which has polynomial complexity wrt the state size of a plant. In contrast to the above graph-based analysis [7]–[10], diagnosability in DESs can be tested by constructing and solving an integer linear programming (ILP) [11].

Since the structural analysis and abstraction techniques can reduce computational overheads and facilitate system development, the diagnosability verification problem is usually considered in Petri nets. Diagnosability [12] and prognosability [13] are studied in unbounded Petri nets by establishing a basis coverability graph. The work in [14] tests diagnosability in time Petri nets by constructing an ILP problem with polynomial complexity wrt the size of a plant. The work in [15] diagnoses a stochastic Petri net by computing its probabilities of consistent trajectories. Moreover, diagnosability verification has recently been generalized to address a variety of challenging settings, including attack-related scenarios [16], observation delay and loss [17], and decentralized frameworks [18].

For Petri nets under unknown initial markings, as far as we know, there are few results that solve the diagnosability verification problem in such Petri nets. In this way, one needs to decide diagnosability for all initial markings in a Petri net under unknown initial markings. In the framework of Petri nets under unknown initial markings, the authors in [19] and [20] deal with the problem of initial state opacity verification by using a graph-based approach and constructing an ILP problem, respectively. The research in [21] achieves marking estimation by calculating a set of minimum initial markings. The study in [22] touches upon the problem of structural sequence detectability in interpreted Petri nets by using the output information and structural analysis.

This paper develops a minimal initial marking model to achieve diagnosability verification in Petri nets under unknown initial markings, which avoids testing diagnosability for each initial marking. The main contributions of this paper are summarized as follows.

- We generalize the notion of diagnosability to Petri nets under unknown initial markings. To avoid testing diagnosability for each initial marking, this paper proposes a minimal initial marking model to verify diagnosability for the original system. Diagnosability analysis at a minimal initial marking is addressed in [21], requiring that considered plant does not contain unobservable transitions. However, the proposed method can be applied to Petri nets with unobservable transition cycles.
- This paper proves that a plant under unknown initial markings is diagnosable iff the extended verifier established from the minimal initial marking model does not have a basis fault path. In this way, we do not need to calculate (basis) reachability graphs of the original Petri net for all initial markings.

*This work is supported by the Science Technology Development Fund, MSAR under Grant No. 0029/2023/RIA1. (*Corresponding author: Shaopeng Hu.*)

[1]Institute of Systems Engineering, Macau University of Science and Technology, Taipa, Macau 2240027337@student.must.edu.mo; chyf01@163.com; zwli@must.edu.mo

[2]School of Electro-Mechanical Engineering, Xidian University, Xi'an 710071, China sphu@stu.xidian.edu.cn

The rest of this paper is organized as follows. Section II reviews the basics of Petri nets. Section III articulates the definition of unknown initial markings and diagnosability. Section IV proposes a structure called an extended verifier to test the diagnosability of a Petri net under unknown initial markings. Section V concludes this paper.

II. Petri net

A Petri net is a four-tuple $\mathcal{N} = (P, T, Pre, Post)$, where P (resp. T) is a finite and non-empty set of places (resp. transitions), graphically represented by circles (resp. bars) with $P \cap T = \emptyset$. Pre: $P \times T \to \mathbb{N}$ and $Post$: $P \times T \to \mathbb{N}$ are the pre- and post- incidence functions that specify the arcs directed from places to transitions and transitions to places, respectively, where $\mathbb{N} = \{0, 1, 2, \dots\}$ is the set of non-negative integers. Functions Pre and $Post$ can be represented by matrices indexed by P and T. Let $C = Post - Pre$ be the incidence matrix of a Petri net $\mathcal{N}$. A Petri net is called an ordinary net if for all $(x, y) \in (T \times P) \cup (P \times T)$, $Post(x, y) \neq 0 \Rightarrow Post(x, y) = 1$ and $Pre(x, y) \neq 0 \Rightarrow Pre(x, y) = 1$; otherwise, a Petri net is called a generalized net.

A marking of a Petri net is a mapping $M : P \to \mathbb{N}$, and $M(p)$ denotes the number of tokens (graphically represented by black dots) in place p at marking M. $\langle \mathcal{N}, M_0 \rangle$ is a net system, where M_0 is called an initial marking. Given a sequence $\sigma \in T^*$, $\mathbf{y}_\sigma$ indicates the firing vector of σ, i.e., $\mathbf{y}_\sigma(t) = n$ if the transition t appears n times in σ. By a slight abuse of notation, write $t \in \sigma$ if σ contains the transition t. We use $[\sigma] = \{t \in T \mid t \in \sigma\}$ to denote the support of σ.

A transition t in a net system is said to be enabled at a marking M if $M \geq Pre(\cdot, t)$. An enabled transition t can fire, yielding a marking $M' = M + C(\cdot, t)$, denoted by $M[t\rangle$. Given a transition sequence $\sigma = t_1 t_2 t_3 \cdots t_n \in T^*$, σ is said to be enabled at a marking M if there exist markings $M_1, M_2, \dots, M_n$ such that $M[t_1\rangle M_1[t_2\rangle M_2 \dots M_{n-1}[t_n\rangle M_n$ holds, denoted by $M[\sigma\rangle M_n$. In this case, M_n is said to be reachable from M. The set of all markings reachable from M_0, denoted by $R(\mathcal{N}, M_0)$, defines the reachability set of $\langle \mathcal{N}, M_0 \rangle$, i.e., $R(\mathcal{N}, M_0) = \{M \in \mathbb{N}^{|P|} \mid (\exists \sigma \in T^*) M_0[\sigma\rangle M\}$. The set of all sequences that are enabled at the initial marking M_0 is defined as $L(\mathcal{N}, M_0) = \{\sigma \in T^* \mid M_0[\sigma\rangle\}$. Let $L(\mathcal{N}, M_0)/\sigma = \{\sigma' \in T^* \mid \sigma\sigma' \in L(\mathcal{N}, M_0)\}$ be the post-language of $L(\mathcal{N}, M_0)$ after $\sigma \in T^*$.

Given a net system $\langle \mathcal{N}, M_0 \rangle$, a non-empty set $P_s \subseteq P$ is a siphon if ${}^\bullet P_s \subseteq P_s^\bullet$. A non-empty set $P_t \subseteq P$ is a trap if $P_t^\bullet \subseteq {}^\bullet P_t$. A siphon (trap) is minimal if there is no siphon (trap) contained in it as a proper subset. Let $J \in 2^P$ be the set of all minimal siphons and traps.

Given a net system $\langle \mathcal{N}, M_0 \rangle$, the set of transitions T can be partitioned into two disjoint sets T_o and T_{uo}, representing the collections of observable and unobservable transitions, respectively, i.e., $T = T_o \dot{\cup} T_{uo}$. The set of unobservable transitions T_{uo} can be further partitioned into two disjoint subsets, i.e., $T_{uo} = T_f \dot{\cup} T_{reg}$, where T_f is the set of fault transitions and T_{reg} is the set of regular unobservable transitions.

Given $T_o, T_{uo} \subseteq T$ with $T = T_o \dot{\cup} T_{uo}$, the natural projection $\mathcal{P}$ is a function $\mathcal{P} : T^* \to T_o^*$ defined as (1) $\mathcal{P}(\varepsilon) = \varepsilon$; (2) $\mathcal{P}(t) = t$ if $t \in T_o$; (3) $\mathcal{P}(t) = \varepsilon$ if $t \in T_{uo}$; (4) $\mathcal{P}(\sigma t) = \mathcal{P}(\sigma)\mathcal{P}(t)$, where $\sigma \in T^*$ and $t \in T$. The inverse projection of $\mathcal{P}$, $\mathcal{P}^{-1} : 2^{T_o^*} \to 2^{T^*}$, can be accordingly defined. Specifically, given $A \in 2^{T_o^*}$, $\mathcal{P}^{-1}(A) = \cup_{s \in A}\{t \in T^* \mid \mathcal{P}(t) = s\}$. By a slight abuse of notation, given $s \in T_o^*$, write $\mathcal{P}^{-1}(\{s\})$ as $\mathcal{P}^{-1}(s)$ for simplicity.

Net system $\langle \mathcal{N}, M_0 \rangle$ is said to be *deadlock-free* if for all $M \in R(\mathcal{N}, M_0)$, there exists $t \in T$ such that $M[t\rangle$. $\langle \mathcal{N}, M_0 \rangle$ is said to be *reversible* if for all $M \in R(\mathcal{N}, M_0)$, M_0 is reachable from M. $\langle \mathcal{N}, M_0 \rangle$ is said to be *bounded* if for all places $p \in P$ there exists a positive integer $b \in \mathbb{N}$ such that for all $M \in R(\mathcal{N}, M_0)$, $M(p) \leq b$ holds.

III. Problem Statement

A. Petri nets under unknown initial marking

Given a net system $\langle \mathcal{N}, M_0 \rangle$, some places are assumed to be unobservable at the initial marking M_0. Specifically, the sets of observable and unobservable places at the initial marking are respectively denoted as $P_o = \{p_{o_1}, p_{o_2}, \dots, p_{o_n}\} \subseteq P$ and $P_u = \{p_{u_1}, p_{u_2}, \dots, p_{u_m}\} \subseteq P$, where $n, m \in \mathbb{N}$. Let on_i be the number of initial tokens in place p_{o_i} and b be the upper bound of the tokens in any place $p \in P$. The net system under unknown initial markings is denoted as $\langle \mathcal{N}, \mathcal{M}_0 \rangle$, where $\mathcal{M}_0 = \{M_0 \in \mathbb{N}^{|P|} | (\forall i = 1, \dots, n)(\forall j = 1, \dots, m)\ M_0(p_{o_i}) = on_i, M_0(p_{u_j}) \leq b\}$ is the initial marking set. If none of the places at the initial marking is observable, the initial marking set reduces to $\mathcal{M}_0 = \{M_0 \in \mathbb{N}^{|P|} | (\forall j = 1, \dots, |P|)\ M_0(p_j) \leq b\}$.

B. Diagnosability

Consider a net system with uncertain initial markings, denoted by $\langle \mathcal{N}, \mathcal{M}_0 \rangle$. The set of fault transitions T_f can be partitioned into h disjoint subsets T_{f_i} $(i \in 1, 2, \dots, h)$, each corresponding to a distinct fault category, where $h \in \mathbb{N}$. To simplify the presentation, we restrict our attention to the single-fault-class case (i.e., $h = 1$). Nevertheless, following a similar line of reasoning as in [23], the proposed framework can be extended to handle multiple fault classes with trivial adjustments. Given an initial marking $M_0 \in \mathcal{M}_0$, define the set of admissible transition sequences that terminate with a fault transition $t_f \in T_f$ as $\Psi(T_f) = \{\sigma t_f \in L(\mathcal{N}, M_0) \mid \sigma \in L(\mathcal{N}, M_0), t_f \in T_f\}$.

In order to deal with the diagnosability verification problem in Petri nets under unknown initial markings, the considered system $\langle \mathcal{N}, \mathcal{M}_0 \rangle$ satisfies the following assumptions.
(A1) $\langle \mathcal{N}, M_0 \rangle$ is bounded and reversible for all $M_0 \in \mathcal{M}_0$.
(A2) $\mathcal{N}$ is an ordinary net.

Assumption (A1) guarantees that for all $M_0 \in \mathcal{M}_0$, the set of reachable markings $R(\mathcal{N}, M_0)$ is finite and does not enter deadlocks. Assumption (A2) is used to simplify the representation of the results. For the sake of brevity, this paper assumes that any transition $t \in T$ can be potentially fired in $\langle \mathcal{N}, M_0 \rangle$ for all $M_0 \in \mathcal{M}_0$. However, by simply removing the set of transitions that cannot be fired from the considered plant, our approach can be extended to verify diagnosability under such a condition.

The definition of diagnosability in Petri nets on the premise that all places are observable at the initial marking is proposed in [12]. Based on this notion, we generalize the diagnosability in Petri nets under unknown initial markings

Definition 1: Let $\langle \mathcal{N}, \mathcal{M}_0 \rangle$ be a net system under unknown initial markings and $M_0 \in \mathcal{M}_0$ be a given initial marking. $\langle \mathcal{N}, M_0 \rangle$ is diagnosable w.r.t. T_f if

$(\forall s' \in \Psi(T_f))(\forall s'' \in L(\mathcal{N}, M_0)/s')(\exists K \in \mathbb{N})\ |s''| \geqslant K \implies (\forall s \in \mathcal{P}^{-1}(\mathcal{P}(s's'')))\ (\exists t_f \in T_f)\ t_f \in s.$

$\langle \mathcal{N}, \mathcal{M}_0 \rangle$ is said to be diagnosable if it is diagnosable for any $M_0 \in \mathcal{M}_0$. □

Definition 1 is a classical notion of diagnosability if $\mathcal{M}_0 = \{M_0\}$. In other words, to verify diagnosability for a net system under unknown initial markings, one needs to test the diagnosability for any $M_0 \in \mathcal{M}_0$.

IV. Solution Procedure

A. Minimal initial marking

In this paper, we propose a minimal initial marking (MIM) to verify the diagnosability in Petri nets under unknown initial markings, which avoids testing diagnosability for any marking $M_0 \in \mathcal{M}_0$. A similar notion of MIM is developed in [21]. However, we will shortly see that for the purpose of diagnosability, the notion of MIM proposed in this paper is more reasonable.

Definition 2: Given a Petri net $\mathcal{N}$, an initial marking $M_0^m \in \mathbb{N}^{|P|}$ is said to be a minimal initial marking for $\mathcal{N}$ if the following two conditions hold: (1) any transition $t \in T$ in $\langle \mathcal{N}, M_0^m \rangle$ can be potentially fired; (2) there does not exist an initial marking $M \in \mathbb{N}^{|P|}$ satisfying condition (1) and $\sum_{p \in P} M(p) < \sum_{p \in P} M_0^m(p)$. A Petri net under an MIM is called a minimal initial marking model, i.e., $\langle \mathcal{N}, M_0^m \rangle$. □

In simple words, for all transitions $t \in T$, there exists a marking $M \in R(\mathcal{M}, M_0^m)$ such that $M[t\rangle$ holds and the total number of tokens in places $p \in P$ at the marking M_0^m is minimal. The work in [21] represents an MIM based on a given observation sequence. However, the notion of MIM proposed in [21] is not applicable if the considered plant contains unobservable transitions.

Fact 1: Let $M \in R(\mathcal{N}, M_0)$ be a reachable marking, where $M_0 \in \mathcal{M}_0$ is a given initial marking and $P_t \subseteq P$ be a trap. If $M(P_t) > 0$, then for all $M' \in R(\mathcal{N}, M)$, $M'(P_t) > 0$.

Proposition 1: Given a reversible net system under unknown initial markings, the set of places P is a trap.

Proof: By contrapositive, suppose that the set of places P is not a trap, i.e., $P^\bullet \nsubseteq {}^\bullet P$. Then there necessarily exists a transition $t \in P^\bullet$ such that $t \notin {}^\bullet P$. For any $M_0 \in \mathcal{M}_0$, there exists a reachable marking $M \in R(\mathcal{N}, M_0)$ such that $M[t\rangle$ since for all $t' \in T$, there exists a marking $M \in R(\mathcal{N}, M_0)$ such that $M[t'\rangle$. Further, by firing sufficiently enough times of t from M, the system reaches a state $M' \in \mathbf{0}^{|P|}$. However, since $\langle \mathcal{N}, M_0 \rangle$ is bounded, $M_0 \notin \mathbf{0}^{|P|}$. Thus, $\langle \mathcal{N}, M_0 \rangle$ is not necessarily reversible, which is inconsistent with Assumption (A3) and thus completes the proof. ■

Fact 1 states that if a trap is marked at a given marking, then it will remain marked in all markings that are reachable thereafter. Proposition 1 implies that any transition $t \in T$ may be potentially fired under an initial marking if a transition can be fired under the initial marking.

In this paper, an MIM can be established by solving an integer linear programming problem (ILPP). Assume that there exist $k \in \mathbb{N}^+$ distinct minimal siphons and traps in J, i.e., $P_j^i \in J$ for all $i \in \{1, 2, \ldots k\}$. In the following, a set of linear inequalities $\mathcal{C}$ for any element in J to calculate MIM can be established:

$$\mathcal{C} = \begin{cases} M_0(p_{j1}^1) + M_0(p_{j2}^1) + M_0(p_{j3}^1) \cdots \geq 1 \\ M_0(p_{j1}^2) + M_0(p_{j2}^2) + M_0(p_{j3}^3) \cdots \geq 1 \\ \ldots \\ M_0(p_{j1}^k) + M_0(p_{j2}^k) + M_0(p_{j3}^k) \cdots \geq 1 \end{cases}$$

where places $p_{j1}^i, p_{j2}^i, p_{j3}^i \in P_j^i$ for all $i \in \{1, 2, \ldots, k\}$.

Given a Petri net $\mathcal{N}$, there may exist a set of MIMs satisfying Definition 2. An MIM is established by solving the following ILPP:

$$min \sum_{p \in P} M_0(p) \text{ subject to constraint set } \mathcal{C} \tag{1}$$

Proposition 2: Given a net system under unknown initial markings $\langle \mathcal{N}, \mathcal{M}_0 \rangle$, any transition $t \in T$ can be potentially fired in the minimal initial marking model $\langle \mathcal{N}, M_0^m \rangle$.

Proof: By contradiction, suppose that for all transitions $t \in T$, there exists at least a place $p \in {}^\bullet t$ such that $M_0^m(p) = 0$. By Proposition 1, there necessarily exists a minimal trap P. Thus, there at least exists a place $p_i \in P$ such that $M_0^m(p_i) > 0$ by the set $\mathcal{C}$. Then there necessarily exists another place $p_j \in P$ with $p_i \neq p_j$ and $p_i^\bullet \cap p_j^\bullet \neq \emptyset$ such that $M_0^m(p_j) = 0$. Since $\langle \mathcal{N}, \mathcal{M}_0 \rangle$ is reversible, there must be a transition t_j with $Post(t_j, p_j) = 1$ by Assumption (A2). Then there is a new trap $P_t \subseteq P$ with $p_j \in P_t$ and $P_t \cap {}^\bullet t_j \neq \emptyset$. By the set $\mathcal{C}$, $M_0^m(p_j) + M_0^m({}^\bullet t_j) \geq 1$. The transition $t \in p_i^\bullet \cap p_j^\bullet$ can be fired if $M_0^m(p_j) = 1$; the transition t_j can be fired otherwise. By Fact 1 and Proposition 1, we conclude that any transition $t \in T$ can be potentially fired in $\langle \mathcal{N}, M_0^m \rangle$. ■

Example 1: Consider the net system under unknown initial markings $\langle \mathcal{N}, \mathcal{M}_0 \rangle$ in Fig. 1, where $T_o = \{t_1, t_2, t_4, t_5\}$ graphically presented by black bars and $T_{uo} = \{t_3, t_6\}$ presented grey bars. There exists a fault class $T_f = \{t_6\}$. The sets of observable places and unobservable places at the initial marking are $P_o = \{p_5\}$ graphically represented by white circles and $P_u = \{p_1, p_2, p_3, p_4, p_6\}$ represented by grey circles, respectively. The initial marking set is $\mathcal{M}_0 = \{M_0 \in \mathbb{N}^6 | (\forall p \in P \setminus \{p_5\})\ M_0(p_5) = 4, M_0(p) \leq 10\}$.

There are two minimal siphons or traps, i.e., $P_{t_1} = \{p_1, p_2, p_3, p_4\}$ and $P_{t_2} = \{p_5, p_6\}$. By the set $\mathcal{C}$, we have $M_0^m(p_5) + M_0^m(p_6) \geq 1$ and $M_0^m(p_1) + M_0^m(p_2) + M_0^m(p_3) + M_0^m(p_4) \geq 1$. Thus, an MIM can be given by

$M_0^m = p_2 + p_5$. By Proposition 2, any transition $t \in T$ is potentially fired in $\langle \mathcal{N}, M_0^m \rangle$. Note that there are other MIMs, i.e., $M_0^{m1} = p_1 + p_6$ and $M_0^{m2} = p_4 + p_6$. ■

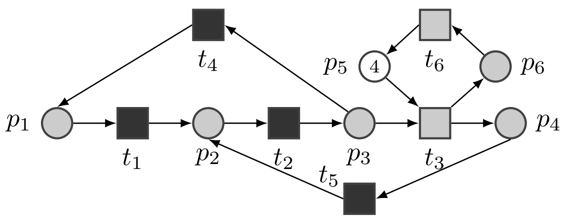

Fig. 1: Net system under unknown initial markings $\langle \mathcal{N}, \mathcal{M}_0 \rangle$ of Example 1.

B. Extended verifier

For a bounded net system $\langle \mathcal{N}, M_0 \rangle$ with $M_0 \in \mathcal{M}_0$, its reachability graph can be represented as a deterministic finite automaton (DFA). Based on this observation, a structure derived from the DFA, referred to as a verifier, was introduced in [6] to check diagnosability with polynomial complexity. Consequently, the problem of verifying diagnosability for a net system can be equivalently reduced to analyzing the corresponding verifier.

Let $x = |R(\mathcal{N}, M_0)|$ be the total number of reachable markings from a given initial marking $M_0 \in \mathcal{M}_0$ in a net system with uncertain initial states. According to [6], the constructed verifier contains no more than $4x^2$ states. Later, an unfolded verifier was proposed in [23], which reduces the state size to at most $2x^2 + 1$, thereby improving computational efficiency. This improvement is achieved by eliminating redundant symmetric paths during the construction process. However, the approach requires generating two (basis) reachability graphs, corresponding to the original net and an auxiliary non-failure net.

Motivated by the above development, this paper introduces an extended verifier via Algorithm 1, which also guarantees an upper bound of $2x^2 + 1$ states, while avoiding the need to explicitly construct a non-failure net system.

Definition 3: Given an MIM model $\langle \mathcal{N}, M_0^m \rangle$, the reachability graph is a DFA $G = (\mathcal{M}, T, Tr, M_0^m)$, where $\mathcal{M} = R(\mathcal{N}, M_0^m)$ is the state set, T is the event set, $Tr = \{(M, t, M') \mid M, M' \in R(\mathcal{N}, M_0^m), M[t\rangle M'\}$ is the transition relation, and M_0^m is the initial state. □

Definition 4: Given a reachability graph G, an extended verifier $G_v = (\mathcal{V}, \Sigma, \Delta, V_0)$ is a DFA, where

- $\mathcal{M}_v = \mathcal{M} \times \mathcal{M} \times \{N, F\}$ is the set of states,
- $\Sigma = \{(t_1, t_2) | t_1, t_2 \in (T \cup \{\varepsilon\}) \setminus T_f\} \cup \{(t_3, t_f) | t_f \in T_f, t_3 \in (T_{reg} \cup \{\varepsilon\})\}$ is the set of event pairs,
- $\Delta \subseteq \mathcal{V} \times \Sigma \times \mathcal{V}$ is the transition relation, and
- $V_0 = (M_0^m, M_0^m; N)$ is the initial state. □

Given an extended verifier G_v, a state of the form $(M_1, M_2; q) \in \mathcal{V}$ is referred to as a q-state, where $q \in \{N, F\}$. A cycle in the extended verifier G_v is defined as a q-cycle if all states along the cycle share the same label q. Furthermore, an N-cycle is considered uncertain if there exists at least one state on the cycle from which an F-state is reachable through some event sequence $\sigma \in \Sigma^*$.

Algorithm 1: Construction Procedure of the Extended Verifier G_v

Input: A net system $\langle \mathcal{N}, \mathcal{M}_0 \rangle$ under unknown initial markings and ILPP (1).
Output: An extended verifier $G_v = (\mathcal{V}, \Sigma, \Delta, V_0)$.

Determine an MIM M_0^m by solving the ILPP (1);
Initialize the label set $q \in \{N, F\}$;
Set $\mathcal{V} := \{(M_0^m, M_0^m; N)\}$, $\Delta := \emptyset$, $\Sigma := \emptyset$, and leave $(M_0^m, M_0^m; N)$ unlabeled;
while *there exists an unlabeled state in* $\mathcal{V}$ **do**
  choose an unlabeled state $V = (M_1, M_2; q) \in \mathcal{V}$;
  for ***each*** $t_1, t_2 \in (T \cup \{\varepsilon\}) \setminus T_f$ **do**
    construct $V' := (\Delta(M_1, t_1), \Delta(M_2, t_2); q)$;
    if $V' \notin \mathcal{V}$ **then**
      update $\mathcal{V} := \mathcal{V} \cup \{V'\}$;
       $\Sigma := \Sigma \cup \{(t_1, t_2)\}$;
      $\Delta := \Delta \cup \{V, (t_1, t_2), V'\}$;
      mark V' as unlabeled.
    end
  end
  for ***each*** $t_1 \in T_{reg} \cup \{\varepsilon\}$ *and* $t_2 \in T_f$ **do**
    construct $V' := (\Delta(M_1, t_1), \Delta(M_2, t_2); F)$;
    if $V' \notin \mathcal{V}$ **then**
      update $\mathcal{V} := \mathcal{V} \cup \{V'\}$;
       $\Sigma := \Sigma \cup \{(t_1, t_2)\}$;
      $\Delta := \Delta \cup \{V, (t_1, t_2), V'\}$;
      mark V' as unlabeled.
    end
  end
end
Remove all state labels.

The research in [23] shows that a Petri net under a given initial marking is diagnosable if and only if its verifier established from the basis reachability graph does not contain any F-cycles. This conclusion also holds by simply replacing the basis reachability graph with the reachability graph.

Corollary 1: [23] A net system $\langle \mathcal{N}, M_0 \rangle$, with $M_0 \in \mathcal{M}_0$ is diagnosable iff the extended verifier established from the reachability graph of $\langle \mathcal{N}, M_0 \rangle$ has no F-cycles.

Based on Corollary 1, to verify diagnosability for a net system $\langle \mathcal{N}, \mathcal{M}_0 \rangle$ under unknown initial markings, one needs to establish an extended verifier for any initial marking $M_0 \in \mathcal{M}_0$ and determine whether there exists an F-cycle for all unfolded verifiers [23].

In the framework of diagnosability verification for $\langle \mathcal{N}, \mathcal{M}_0 \rangle$, to avoid the additional computational burden caused by constructing extended verifiers for all $M_0 \in \mathcal{M}_0$, this paper proposes a notion called a basis fault path composed of uncertain N-cycles and F-cycles.

Definition 5: A path $\hat{\sigma}_f = M_0(t_1, t_1')M_1(t_2, t_2') \ldots M_{k-1} (t_k, t_k')M_k \in (\mathcal{V} \cdot \Sigma)^*$ of G_v, where $\mathcal{V} \cdot \Sigma$ is the catenation of $\mathcal{V}$ and Σ, is called a basis fault path if, defining $\sigma_p = t_1 t_2 \ldots t_r$, $\sigma_q = t_{r+1} \ldots t_s$, $\sigma_j = t_s \ldots t_k$, $\sigma_p' = t_1' \ldots t_r'$, $\sigma_q' = t_{r+1}' \ldots t_s'$, and $\sigma_j' = t_s' \ldots t_k'$, the following statements

hold:
(1) $\Delta_e(M_0, \sigma_p) = M'$, $\Delta_e(M', \sigma_q) = M'$ and $\Delta_e(M', \sigma_j) = M''$ with $M', M'' \in \{M_0, M_1, \ldots, M_k\}$;
(2) $\Delta_e(M_0, \sigma'_p) = M^1$, $\Delta_e(M^1, \sigma'_q) = M^1$ and $\Delta_e(M^1, \sigma'_j) = M^2$ with $M^1, M^2 \in \{M_1, M_2, \ldots, M_k\}$;
(3) $t_f \in t_1 t_2 \ldots t_k$;
(4) $\mathcal{P}(\sigma_p) = \mathcal{P}(\sigma_p)'$, $\mathcal{P}(\sigma_q) = \mathcal{P}(\sigma_q)'$ and $\mathcal{P}(\sigma_j) = \mathcal{P}(\sigma_j)'$;
(5) σ_p, σ'_p, σ_j and σ'_j can be empty;
(6) no prefix of $\hat{\sigma}$ satisfies items (1)–(5). □

Equivalently, a basis fault path is defined as a path that originates from the initial state of G_v and terminates either at the first occurrence of a repeated F-state, or at the first F-state reached after traversing an N-cycle. In addition, such a path is regarded as an F-cycle when it satisfies the condition specified in item (5) of Definition 5.

Given a set of sequences T^*, define $Z : T^* \to T^*$ recursively as follows: $Z(\varepsilon) = \varepsilon$, and for any $s \in T^*$ and $\alpha \in \Sigma$, $Z(s\alpha) = Z(s)\alpha$ if $\alpha \notin [Z(s)]$, and $Z(s\alpha) = Z(s)$ otherwise. That is, $Z(s)$ is obtained by retaining only the first occurrence of each symbol in s, while preserving their order of appearance. For example, given $s = \beta\alpha\beta\gamma\alpha$, we have $Z(s) = \beta\alpha\gamma$.

Proposition 3: A net system $\langle \mathcal{N}, \mathcal{M}_0 \rangle$ under unknown initial markings is diagnosable if the verifier constructed by the reachability graph of the minimal initial marking model $\langle \mathcal{N}, M_0^m \rangle$ does not contain basis fault paths.

Proof: By contrapositive, suppose that the system under an initial marking $M_0 \in \mathcal{M}_0$, i.e., $\langle \mathcal{N}, M_0 \rangle$, is nondiagnosable. It follows that there exist two sufficient sequences $\sigma_1 = t_1 t_2 \cdots$ and $\sigma_2 = t'_1 t'_2 \cdots$ in $L(\mathcal{N}, M_0)$ such that their projections are identical, i.e., $\mathcal{P}(\sigma_1) = \mathcal{P}(\sigma_2)$. Moreover, the fault transition $t_f \in T_f$ appears in σ_1 but does not occur in σ_2.

If all transitions in σ_1 and σ_2 are distinct, except for the pairs (t_1, t_n) and (t'_1, t'_n), then $\sigma_1 = s_1\sigma'_1, \sigma_2 = s_2\sigma'_2 \in L(\mathcal{N}, M_0^m)$ by Definition 2. Thus, by Definitions 3 and 4, G_v has an F-cycle, i.e., $(M, M'; F) \xrightarrow{(\sigma'_1, \sigma'_2)} (M, M'; F)$, where $(M, M'; F) = \Delta((M_0^m, M_0^m; N), (s_1, s_2))$. Actually, an F-cycle is a basis fault path by Definition 5.

If some transitions in either σ_1 or σ_2 occur more than once, i.e., there exist $t, t' \in T$ such that $\mathbf{y}\sigma_1(t) > 1$ or $\mathbf{y}\sigma_2(t') > 1$, then one can derive two transition sequences $Z(\sigma_1) = s\sigma_{z1}$ and $Z(\sigma_2) = s'\sigma_{z2}$. If there are two sequences $Z(\sigma_1) \in L(\mathcal{N}, M_0^m)$ and $Z(\sigma_2) \in L(\mathcal{N}, M_0^m)$, by Definition 4, there exists an F-cycle in G_v, i.e., $(M, M'; F) \xrightarrow{(\sigma_{z1}, \sigma_{z2})} (M, M'; F)$, where $(M, M'; F) = \Delta((M_0^m, M_0^m; N), (s, s'))$. By Definition 5, there exists a basis fault path in G_v.

If $Z(\sigma_1) \notin L(\mathcal{N}, M_0^m)$ or $Z(\sigma_2) \notin L(\mathcal{N}, M_0^m)$, there necessarily exist four sequences $\sigma_3, s_4\sigma_4, \sigma'_3, s'_4\sigma'_4 \in L(\mathcal{N}, M_0^m)$ with $\mathbf{y}_{\sigma_3}(t_f) > 0$, $\mathbf{y}_{s_4\sigma_4}(t_f) = \mathbf{y}_{\sigma'_3}(t_f) = \mathbf{y}_{s'_4\sigma'_4}(t_f) = 0$, $\mathcal{P}(\sigma_3) = \mathcal{P}(\sigma'_3)$ and $\mathcal{P}(s_4\sigma_4) = \mathcal{P}(s'_4\sigma'_4)$ such that $[\sigma_3] \cap [s_4\sigma_4] \cap [Z(\sigma_1)] \neq \emptyset$ and $[\sigma'_3] \cap [s'_4\sigma'_4] \cap [Z(\sigma_2)] \neq \emptyset$ by Definition 2. Hence, an N-cycle must exist in G_v, that is, there is a state $(M, M'; N)$ that can reach itself via (σ_4, σ'_4). This state is reachable from the initial state $(M_0^m, M_0^m; N)$ through (s_4, s'_4) as defined in Definition 4. Moreover, one can identify a pair of sequences (s_1, s_2) with $s_1 \in [\sigma_3] \cap [\sigma_4]$ and $s_2 \in [\sigma'_3] \cap [\sigma'_4]$ such that $M_0^m[s_1 t_f\rangle$ and $M_0^m[s_2\rangle$, where $t_f \in T_f$ by Definition 4. Thus, there exists a basis fault path in G_v by Definition 5. This contradicts the initial assumption, thereby concluding the proof. ■

Proposition 3 offers a criterion for checking diagnosability of a net system $\langle \mathcal{N}, \mathcal{M}_0 \rangle$ under unknown initial markings that may contain unobservable transition cycles without establishing its reachability graphs for all $M_0 \in \mathcal{M}_0$. However, the absence of basis fault paths cannot be directly concluded from the diagnosability of $\langle \mathcal{N}, \mathcal{M}_0 \rangle$. Under an additional assumption, Proposition 3 can be reversed. Specifically, consider the following condition:
(A4) For any $M_0 \in \mathcal{M}_0$, there does not exist a transition cycle $\sigma \in L(\mathcal{N}, M_0)$ with for all $t_f \in T_f$, $t_f \notin \sigma$ such that for all $\sigma' \in \Psi(T_f)$, σ cannot be fired at the marking $M_0[\sigma'\rangle$.

Theorem 1: Given a net system $\langle \mathcal{N}, \mathcal{M}_0 \rangle$ under unknown initial markings that satisfies Assumptions (A1)–(A4), $\langle \mathcal{N}, \mathcal{M}_0 \rangle$ is diagnosable iff G_v constructed by the reachability graph of $\langle \mathcal{N}, M_0^m \rangle$ has no basis fault paths.

Proof: (Only if) By contrapositive, suppose that there exists a basis fault path in G_v. If it is an F-cycle, i.e., the condition in item (5) of Definition 5 holds, we have two transition sequences $\sigma_1, \sigma_2 \in L(\mathcal{N}, M_0^m)$ with $t_f \in T_f$, $t_f \in \sigma_1$, $t_f \notin \sigma_2$ and $\mathcal{P}(\sigma_1) = \mathcal{P}(\sigma_2)$ by Definition 4. If $M_0^m \in \mathcal{M}_0$, then $\langle \mathcal{N}, M_0^m \rangle$ is nondiagnosable by Corollary 1. If $M_0^m \notin \mathcal{M}_0$, then for all $M_0 \in \mathcal{M}_0$, $M_0 = M_0^m + I$ holds by Definition 2, where $I \in \mathbb{N}^{|P|}$. Thus, $\sigma_1, \sigma_2 \in L(\mathcal{N}, M_0)$ for all $M_0 \in \mathcal{M}_0$. By Definition 1, $\langle \mathcal{N}, \mathcal{M}_0 \rangle$ is not diagnosable.

If the basis fault path is not an F-cycle, we have two transition sequences $(s_1, s_2) \in \Sigma^*$ and two sequences $\sigma_3 = s_3 s_4, \sigma_4 = s_5 s_6 \in L(\mathcal{N}, M_0^m)$ with $t_f \in s_4$, $\mathbf{y}_{s_3}(t_f) = \mathbf{y}_{s_5}(t_f) = \mathbf{y}_{s_6}(t_f) = 0$, $s_3 \in [s_1]$, $s_5 \in [s_2]$, $\mathcal{P}(s_3) = \mathcal{P}(s_5)$ and $\mathcal{P}(s_4) = \mathcal{P}(s_6)$ by Definition 4. Since for all $M_0 \in \mathcal{M}_0$, $M_0 = M_0^m + I$ holds by Definition 2, where $I \in \mathbb{N}^{|P|}$, s_1, s_2, $\sigma_3, \sigma_4 \in L(\mathcal{N}, M_0)$ for all $M_0 \in \mathcal{M}_0$. By Assumption (A4), we have two sufficiently long sequences $s_1\sigma_3(s_1)^n$, $s_2\sigma_4(s_2)^n \in L(\mathcal{N}, M_0)$, where $n \in \mathbb{N}$. By Definition 1, $\langle \mathcal{N}, \mathcal{M}_0 \rangle$ is not diagnosable.

(If) This is a special case of Proposition 3. ■

According to Theorem 1, the diagnosability verification problem for a net system $\langle \mathcal{N}, \mathcal{M}_0 \rangle$ with unknown initial markings reduces to checking whether the corresponding extended verifier G_v, constructed from the reachability graph of $\langle \mathcal{N}, M_0^m \rangle$, contains at least one basis fault path.

Example 2: Consider the net system again under unknown initial markings $\langle \mathcal{N}, \mathcal{M}_0 \rangle$ shown in Fig. 1. By Example 1, we have an MIM $M_0^m = p_2 + p_5$. In this way, the reachability graph of the MIM model $\langle \mathcal{N}, M_0^m \rangle$ is depicted in Fig. 2(a), where $M_0 = p_2 + p_5$, $M_1 = p_3 + p_5$, $M_2 = p_1 + p_5$, $M_3 = p_4 + p_6$, $M_4 = p_2 + p_6$ and $M_5 = p_4 + p_5$.

By Definition 4, the initial state is $V_0 = (M_0, M_0; N)$. By firing the event (t_2, t_2), it reaches a state $(M_1, M_1; N)$. Then, we have an N-state $(M_2, M_2; N)$ if the event (t_4, t_4) has occurred. Thus, we find an N-cycle, i.e., from $(M_0, M_0; N)$ through $(M_1, M_1; N)$ and $(M_2, M_2; N)$, the plant reaches again $(M_0, M_0; N)$. By Algorithm 1, the extended verifier G_v is shown in Fig. 2(b). There exist two basis fault paths since the state $(M_1, M_1; N)$ belongs to an N-cycle and reaches the F-states $(M_4, M_5; F)$ and $(M_4, M_0; F)$. Therefore, $\langle \mathcal{N}, \mathcal{M}_0 \rangle$ is nondiagnosable by Theorem 1. ■

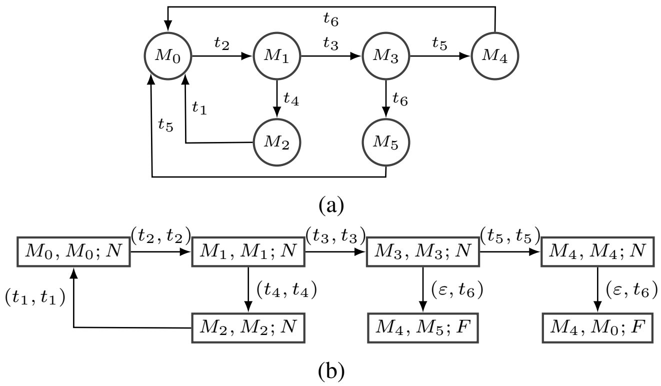

Fig. 2: The extended verifier G_v of Example 2.

C. Computational complexity

In this section, we analyze the computational complexity of each step in the proposed framework.

- Construction of an MIM M_0^m: To derive M_0^m, all minimal siphons and traps must be computed. In the worst case, this step has complexity of $O(2^{|P|})$. Nevertheless, in practice, this computation can be efficiently carried out using the open-source tool INA.
- Construction of the extended verifier G_v: The size of the state space of G_v depends on the reachability graph of $\langle \mathcal{N}, M_0^m \rangle$. In general, the complexity of reachability graph construction is determined by the net structure and the initial token distribution. Since M_0^m corresponds to the minimal total number of tokens among all possible initial markings, the resulting reachability graph is expected to be smaller, and thus less expensive to compute, than that obtained from any $M_0 \in \mathcal{M}_0$.
- Construction of all basis fault paths: Let $x = |\mathcal{M}|$ denote the number of reachable markings of $\langle \mathcal{N}, M_0^m \rangle$. In the worst case, G_v contains at most $2x^2+1$ states, and each state enables at most $|T|^2 - 1$ event pairs according to Algorithm 1. Consequently, the total number of basis fault paths is bounded by $O\big((|T|^2 - 1)^{2x^2+1}\big)$.

V. Conclusion

In this paper, we propose a minimal initial marking model to verify diagnosability for Petri nets under unknown initial markings without testing diagnosability for each initial marking. It is shown that the original system is diagnosable if and only if the extended verifier established from the reachability graph of the minimal initial marking model has no basis fault paths. Finally, we formally discuss the complexity of the proposed approach.

Our future research under this framework will focus on diagnosability enforcement in Petri nets under unknown initial markings. Furthermore, it would be interesting to consider extensions to timed Petri nets.

References

[1] C. G. Cassandras, and S. Lafortune, *Introduction to Discrete Event Systems*. New York, NY, USA: Springer, 2008.

[2] A. Giua, C. Seatzu, and F. Basile, "Observer-based state-feedback control of timed Petri nets with deadlock recovery," *IEEE Trans. Autom. Control*, vol. 49, no. 1, pp. 17–29, 2004.

[3] J. Chen, and R. Kumar, "Failure detection framework for stochastic discrete event systems with guaranteed error bounds," *IEEE Trans. Autom. Control*, vol. 60, no. 6, pp. 1542–1553, 2015.

[4] M. P. Cabasino, A. Giua, and C. Seatzu, "Fault detection for discrete event systems using Petri nets with unobservable transitions," *Automatica*, vol. 46, no. 9, pp. 1531–1539, 2010.

[5] Y. Wu, and C. N. Hadjicostis, "Algebraic approaches for fault identification in discrete-event systems," *IEEE Trans. Autom. Control*, vol. 50, no. 12, pp. 2048–2055, 2005.

[6] C. N. Hadjicostis, *Estimation and Inference in Discrete Event Systems*. Switzerland: Springer, 2020.

[7] F. Lin, "Diagnosability of discrete event systems and its applications," *Discrete Event Dynamic Systems*, vol. 4, no. 2, pp. 197–212, 1994.

[8] 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, 1995.

[9] T.-S. Yoo, and S. Lafortune, "Polynomial-time verification of diagnosability of partially observed discrete-event systems," *IEEE Trans. Autom. Control*, vol. 47, no. 9, pp. 1491–1495, 2002.

[10] S. Hu, and Z. Li, "A digital twin approach for enforcing diagnosability in Petri nets," *IEEE Transactions on Automation Science and Engineering*, vol. 21, no. 4, pp. 6068–6080, 2024.

[11] G. Zhu, Z. W. Li, and N. Wu, "Model-based fault identification of discrete event systems using partially observed Petri nets," *Automatica*, vol. 96, pp. 201–212, 2018.

[12] S. Hu, Y. Hu, D. Liu, M. P. Fanti, and Z. Li, "Diagnosability verification and enforcement for unbounded Petri nets by online supervisors," *IEEE Trans. Autom. Sci. Eng.*, vol. 22, pp. 9061–9074, 2026.

[13] S. Hu, R. Liu, M. P. Fanti, and Z. Li, "Optimal sensor selection for K-step prognosability verification and enforcement of unbounded Petri nets," *IEEE Trans. Autom. Control*, 2026. Available online: https://ieeexplore.ieee.org/document/11479826.

[14] F. Basile, M. P. Cabasino, and C. Seatzu, "State estimation and fault diagnosis of labeled time Petri net systems with unobservable transitions," *IEEE Trans. Autom. Control*, vol. 60, no. 4, pp. 997–1009, 2015.

[15] R. Ammour, E. Leclercq, E. Sanlaville, and D. Lefebvre, "Datation of faults for markovian stochastic DESs," *IEEE Trans. Autom. Control*, vol. 64, no. 7, pp. 2961–2967, 2019.

[16] S. Hu, Y. Hu, J. Komenda, and Z. Li, "Supervisory control for active diagnosis in labeled Petri nets under coordinated sensor and actuator attacks," *IEEE Trans. Autom. Control*, vol. 71, no. 5, pp. 2873–2886, 2026.

[17] S. Hu, W. Duan, D. Liu, and Z. Li, "Supervisory control for active diagnosis in labeled Petri nets under observation and control delays," *IEEE Trans. Autom. Control*, 2026. Available online: https://ieeexplore.ieee.org/abstract/document/11359496.

[18] G. Zhu, T. Chang, L. Yin, N. Wu, and Z. Li, "Decentralized fault diagnosis of labeled Petri nets," *IEEE Trans. Autom. Control*, 2026. Available online: https://ieeexplore.ieee.org/abstract/document/11397297.

[19] Y. Tong, Z. W. Li, C. Seatzu, and A. Giua, "Verification of state-based opacity using verifier nets," *IEEE Trans. Autom. Control*, vol. 62, no. 6, pp. 2823–2837, 2016.

[20] X. Cong, M. P. Fanti, A. Mangini, and Z. W. Li, "Critical observability of Petri nets with unknown initial marking," in *IEEE 58th Conference on Decision and Control*, pp. 2003–2008, 2019.

[21] L. Li, and C. N. Hadjicostis, "Minimum initial marking estimation in labeled Petri nets," *IEEE Trans. Autom. Control*, vol. 58, no. 1, pp. 198–203, 2012.

[22] S. A. Nuño-Sánchez, A. R. Treviño, and J. R. León, "Structural sequence detectability in free choice interpreted Petri nets," *IEEE Trans. Autom. Control*, vol. 61, no. 1, pp. 198–203, 2015.

[23] N. Ran, H. Su, A. Giua, and C. Seatzu, "Enforcement of diagnosability in labeled Petri nets via optimal sensor selection," *IEEE Trans. Autom. Control*, vol. 64, no. 7, pp. 2997–3004, 2019.