Automatica 127 (2021) 109490

Contents lists available at ScienceDirect

Automatica

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

Brief paper

Initial-state detectability and initial-state opacity of unambiguous weighted automata[☆]

Aiwen Lai[a,b], Sébastien Lahaye[b,*], Zhiwu Li[c,d]

[a] School of Aerospace Engineering, Xiamen University, 361102 Xiamen, China
[b] Laboratoire Angevin de Recherche en Ingénierie des Systèmes, Université d'Angers, 49000 Angers, France
[c] School of Electro-Mechanical Engineering, Xidian University, 710071 Xi'an, China
[d] Institute of Systems Engineering, Macau University of Science and Technology, Taipa, Macau

ARTICLE INFO

Article history:
Received 3 April 2019
Received in revised form 17 August 2020
Accepted 26 December 2020
Available online xxxx

Keywords:
Weighted automaton
Initial state estimation
Initial-state detectability
Initial-state opacity

ABSTRACT

In this paper, we investigate the verification problem of initial-state detectability (I-detectability) and initial-state opacity (I-opacity) in discrete event systems modeled by unambiguous weighted automata. An I-observer is constructed so as to derive necessary and sufficient conditions for checking strong I-detectability, weak I-detectability, and I-opacity, with exponential complexity. In addition, an approach based on diagnosability analysis is proposed for verifying strong I-detectability. Compared with an I-observer-based approach, the diagnosability-based approach has a lower complexity, and in the case where all the unobservable events in an unambiguous weighted automaton are represented by a unique symbol, the diagnosability-based approach has polynomial complexity.

1. Introduction

I-detectability and I-opacity problems are tightly related to state estimation that has been extensively studied in discrete event systems (DESs) framework. In general, state estimation can be divided into two categories: current-state estimation, e.g., Keroglou and Hadjicostis (2017), Lai et al. (2019) and Shu and Lin (2011) and initial-state estimation, e.g., Saboori and Hadjicostis (2013), Shu and Lin (2013) and Yin (2017). In this paper, we focus on the problem of initial-state estimation and its applications to I-detectability and I-opacity.

Shu and Lin (2013) formulate the initial-state estimation problem of non-deterministic finite state automata (NFAs) as I-detectability. It characterizes whether the initial state of an NFA can be uniquely determined after a finite number of labels have been observed. An exponential (resp. a polynomial-time) complexity algorithm is introduced for checking weak (resp. strong) I-detectability based on the construction of an I-observer (resp. I-detector). Yin (2017) introduces the notion of stochastic initial-state detectability (SI-detectability) by considering the probabilistic sensor failures. SI-detectability characterizes the convergence of the probability for determining the initial-state of a probabilistic finite state automaton. An algorithm with PSPACE-complete complexity is proposed for verifying the SI-detectability.

A system is said to be initial-state opaque if the set of initial states estimated by an intruder for any observation contains at least one element that does not belong to the secret. In Saboori and Hadjicostis (2013), an initial-state estimator is constructed, which can be used to verify I-opacity of an NFA for both invariant-secret and varying-secret. The initial-state estimator has up to 2^{n^2} states, where n is the number of states in the NFA. In addition, when the secret is fixed, the complexity of verifying I-opacity is reduced to $\mathcal{O}(4^n)$ by introducing the notion of verifier. Recently, Wu and Lafortune (2013) prove that the initial state of an NFA can be estimated by the observer of its reverse automaton, and as a result, the verification complexity of I-opacity is reduced to $\mathcal{O}(2^n)$. More work on (initial-state) detectability or opacity can be found in Bryans et al. (2005), Ji et al. (2019), Masopust and Yin (2019a, 2019b), Sasi and Lin (2018), Shu and Lin (2012), Yin and Lafortune (2017), Yin et al. (2019), Zhang (2017) and Zhang et al. (2019).

Weighted automata (WAs) represent a well studied class of DES models (Gaubert, 1995). Unlike classical automata, transitions in WAs carry weights belonging to a semiring. The weight associated with a transition can model, e.g., the cost, the energy, the time needed for executing the transition. WAs have spurred much interest in Computer Science due to their elegant and sound algebraic framework as well as their relevance in practical

☆ This work is partially supported by the National Key R&D Program of China under Grant 2018YFB1700104, and National Natural Science Foundation of China under Grant 61873442. The material in this paper was not presented at any conference. This paper was recommended for publication in revised form by Associate Editor Rong Su under the direction of Editor Christos G. Cassandras.

* Corresponding author.
E-mail addresses: aiwenlai@xmu.edu.cn (A. Lai), sebastien.lahaye@univ-angers.fr (S. Lahaye), zhwli@xidian.edu.cn (Z. Li).

https://doi.org/10.1016/j.automatica.2021.109490
0005-1098/

applications, such as natural language processing, speech recognition and image compression (Droste et al., 2009). From a different perspective, in this paper, we investigate I-detectability and I-opacity verification problems for WAs, which are core problems with the control community. So far, we have found a formal approach to verify these properties for an important class of WAs, namely, unambiguous weighted automata (UWAs), where no two or more paths are labeled by a given string leading to the same state.

To explore the modeling power of UWAs, it is worth mentioning that the relation between max-plus automata (MPAs) and timed Petri nets (TPNs) has been investigated. From a safe TPN under the preselection policy, it is possible to derive an MPA with the same timed behavior (Gaubert & Mairesse, 1999; Lahaye et al., 2015). If the race policy is considered, it has been shown that bounded TPNs can be represented by deterministic max-plus automata (DMPAs) (Komenda et al., 2016; Triska & Moor, 2020). Note that DMPAs constitute a subclass of unambiguous MPAs and the proposed I-detectability and I-opacity approach can be applied. It should also be noted that determinization procedures can be used to transform MPAs into DMPAs with the same timed behavior (Gaubert, 1995; Kirsten, 2008; Lahaye et al., 2020; Mohri, 1997). Using such a transformation, a fairly large class of MPAs can be considered, that is, at least the polynomially ambiguous MPAs having the clones property.

Because of the influence of the transition weights, the I-detectability and I-opacity of a UWA are different from that of its support, i.e., the corresponding logical automaton obtained by removing all the weights in the UWA. For instance, considering the UWA G in Fig. 1, its support is not strongly I-detectable. On the other hand, taking into account quantitative information, it is shown later that G is strongly I-detectable. Besides, if we assume that the set of secret states is $Q_s = \{1, 3\}$, it can be shown that G is not initial-state opaque while its support is initial-state opaque with respect to Q_s.

The above aspects motivate the work in this paper, i.e., the verification of I-detectability and I-opacity for UWAs. The main contributions are as follows. (1) We extend the notion of I-detectability and I-opacity from logical DESs to the framework of WAs. Two types of I-detectability, namely strong I-detectability and weak I-detectability are defined. (2) Given a UWA, a formal procedure is first proposed to construct its initial-state estimator (called I-observer). Then, necessary and sufficient conditions with exponential complexity are developed for verifying I-detectability and I-opacity of the studied UWA based on the constructed I-observer. (3) An approach based on diagnosability analysis is presented for checking strong I-detectability of a UWA. In the case that the unobservable events are not distinguished by an external agent, i.e., all unobservable events in a UWA are represented by a single symbol, the approach is of polynomial complexity.

This paper is organized as follows. Section 2 recalls some basics of WAs. Section 3 formulates the notion of I-detectability and I-opacity. In Section 4.1, the I-observer based approach is proposed to verify strong and weak I-detectability of a UWA. Section 4.2 presents a diagnosability-based approach for verifying strong I-detectability of a UWA. In Section 5, a necessary and sufficient condition is presented for checking I-opacity of a UWA. Finally, conclusions are drawn in Section 6.

2. Preliminaries

In this section we recall some basics of weighted automata (Droste et al., 2009), where transitions carry weights belonging to a semiring $\mathbb{S} = (\mathcal{D}, \oplus, \otimes, \varepsilon, e)$, where ε (resp. e) denotes the neutral element for addition $\oplus$ (resp. multiplication $\otimes$). Typical examples are the tropical semiring $(\mathbb{R} \cup \{+\infty\}, \min, +, +\infty, 0)$ and max-plus semiring $(\mathbb{R} \cup \{-\infty\}, \max, +, -\infty, 0)$.

Let E be an alphabet, i.e., a non-empty set of labels, and E^* be the set of all the finite strings over E including the empty string λ. The set of matrices with m rows and n columns over semiring $\mathbb{S}$ is denoted by $\mathbb{S}^{m\times n}$.

Definition 1. A weighted automaton over a semiring $\mathbb{S} = (\mathcal{D}, \oplus, \otimes, \varepsilon, e)$ is equivalently defined by $G = (Q, E, \alpha, \mu)$ or $G = (Q, E, t, Q_i, \varrho)$, where

- Q and E are respectively a non-empty finite set of states and an alphabet;
- $\alpha \in \mathbb{S}^{1\times|Q|}$ is a row vector specifying the initial weights. A state $q \in Q$ is said to be an initial state iff $\alpha_q \neq \varepsilon$, where α_q is the initial weight of q. We denote by Q_i the set of initial states, and $\varrho : Q_i \to \mathcal{D}$ is the function of initial weights $\varrho(q) \triangleq \alpha_q$ for $q \in Q_i$;
- μ: $E \to \mathbb{S}^{|Q|\times|Q|}$ is a morphism representing the state transitions given by the family of matrices $\mu(a) \in \mathbb{S}^{|Q|\times|Q|}$, $a \in E$. More precisely, we have $\mu(a)_{qq'} \neq \varepsilon$[1] if, and only if, there is a transition labeled by a with a weight of $\mu(a)_{qq'}$ from state q to q'. For any string $\omega = e_1 \cdots e_k \in E^*$, we have $\mu(\omega) = \mu(e_1) \otimes \mu(e_2) \otimes \cdots \otimes \mu(e_k)$. $t : Q \times E \times Q \to \mathcal{D}$ is the transition function with $t(q, a, q') \triangleq \mu(a)_{qq'}$, and for string $\omega = e_1e_2 \cdots e_n \in E^*$, $t(q, \omega, q') = \mu(\omega)_{qq'}$.

Definition 2. Given a WA G, a path of length k is defined as a sequence of transitions $\pi = (q_0, e_1, q_1)(q_1, e_2, q_2) \cdots (q_{k-1}, e_k, q_k)$, where $q_j \in Q$, $j = 0, \ldots, k$, $e_j \in E$ and $\mu(e_j)_{q_{j-1}q_j} \neq \varepsilon$ for $j = 1, \ldots, k$.

Such a path π leads from state q_0 to q_k, and is labeled by $e_1e_2 \cdots e_k \in E^*$. Besides, π is said to be a circuit if q_0 coincides with q_k. We use $p \overset{\omega}{\rightsquigarrow} q$ to represent the set of paths labeled by string $\omega \in E^*$ from state p to q. For $P, R \subseteq Q$, we denote by $P \overset{\omega}{\rightsquigarrow} R$ the union of $p \overset{\omega}{\rightsquigarrow} q$ for all $p \in P$ and $q \in R$.

Definition 3. A WA G is said to be unambiguous if for all $q \in Q$, for all $\omega \in E^*$, $|Q_i \overset{\omega}{\rightsquigarrow} \{q\}| \leq 1$.

In simple words, the unambiguity implies that for any state q of G and any string ω in E^*, there is at most one path labeled by ω leading from an initial state to q.

Remark 1. If $Q_i = Q$, a WA is unambiguous iff any state has no two or more input transitions labeled by the same symbol. In the case of $Q_i \neq Q$, the above characterization provides only a sufficient condition for unambiguity. Besides, a WA is said to be deterministic if it has a unique initial state and from any state, no two or more output transitions are labeled by the same symbol. Determinism implies unambiguity, but the reverse is not true. □

Example 1. Fig. 1 depicts a UWA $G = (Q, E, \alpha, \mu)$, where $Q = \{1, 2, 3, 4, 5, 6, 7\}$, $E = \{u, b, c, d\}$, $\mu(u)_{1,2} = 1$, $\mu(u)_{4,5} = 2$, $\mu(u)_{5,6} = 3$, $\mu(b)_{2,3} = 6$, $\mu(b)_{6,3} = 4$, $\mu(c)_{3,3} = 2$, $\mu(c)_{7,7} = 2$, $\mu(d)_{5,7} = 2$, and $\alpha = (e, \varepsilon, \varepsilon, e, \varepsilon, \varepsilon, \varepsilon)$. All the non-listed coefficients in $\mu(u)$, $\mu(b)$, $\mu(c)$ and $\mu(d)$ are equal to ε, meaning that they do not model possible transitions in the automaton. G is not deterministic since it has two initial states. □

Definition 4. Given an arbitrary path $\pi = (q_0, e_1, q_1)(q_1, e_2, q_2) \cdots (q_{k-1}, e_k, q_k)$ of UWA G with $q_0 \in Q_i$, the weighted sequence $\sigma(\pi) \in (E \times \mathcal{D})^*$ generated by π is defined as: $\sigma(\pi) = (e_1, \tau_1)(e_2, \tau_2) \cdots (e_k, \tau_k)$ where $\tau_1 = \alpha_{q_0} \otimes \mu(e_1)_{q_0q_1}$, $\tau_j = \tau_{j-1} \otimes \mu(e_j)_{q_{j-1}q_j}$ for $j = 2, \ldots, k$.

[1] We assume that the states of G are ordered by positive integers, and by a slight abuse of notation, α_q (resp. $\mu(a)_{qq'}$) is used to denote the qth element of α (resp. the element in the qth row and q'th column of matrix $\mu(a)$).

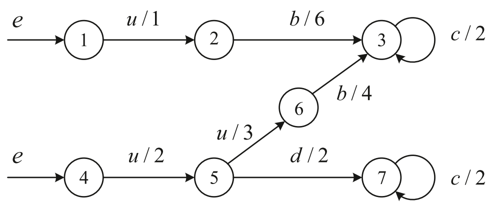

Fig. 1. An unambiguous weighted automaton G.

Here, $\sigma(\pi)$ specifies a sequence of labels and their occurrence weights. We use $q_0 \overset{\sigma(\pi)}{\rightsquigarrow} q_k$ to represent that weighted sequence $\sigma(\pi)$ leads from q_0 to q_k. In the rest of this paper, we focus on semirings where $\otimes$ represents the usual addition, which fits with WAs where weights represent the durations or consumed energy of state transitions. In other words, the weights along an evolution of a WA are interpreted as time or energy accumulated by addition, and an external agent observes this value in addition to events occurrences.

Definition 5. Given a UWA $G = (Q, E, \alpha, \mu)$, the generated weighted language $L(G)$ of G is defined as:

$$\begin{aligned}L(G) =& \{y \in (E \times \mathcal{D})^* \mid \exists q \in Q,\\ &\exists \omega \in E^*, \exists \pi \in Q_i \overset{\omega}{\rightsquigarrow} \{q\} : \sigma(\pi) = y\}.\end{aligned} \tag{1}$$

For any sequence $\sigma \in L(G)$, we denote by $lab_f(\sigma) \in E$ the last label in σ.

Example 2. Consider path $\pi = (1, u, 2)(2, b, 3)(3, c, 3)$ in UWA G in Fig. 1. By Definition 4, we have $\sigma(\pi) = (u, e \otimes \mu(u)_{1,2})(b, e \otimes \mu(u)_{1,2} \otimes \mu(b)_{2,3})(c, e \otimes \mu(u)_{1,2} \otimes \mu(b)_{2,3} \otimes \mu(c)_{3,3}) = (u, e \otimes 1)(b, e \otimes 1 \otimes 6)(d, e \otimes 1 \otimes 6 \otimes 2) = (u, 1)(b, 7)(c, 9)$, and $lab_f(\sigma(\pi)) = c$. $\square$

In this paper, alphabet E is partitioned into two disjoint parts: the unobservable part E_{uo} and the observable part E_o. The projection operator $P : E^* \to E_o^*$ is defined as: $P(\lambda) = \lambda$, where λ represents the empty string; for each $a \in E, \omega \in E^*$, $P(\omega a) = P(\omega)a$ if $a \in E_o$, otherwise, $P(\omega a) = P(\omega)$. We extend $P : E^* \to E_o^*$ to weighted sequences $P : (E \times \mathcal{D})^* \to (E_o \times \mathcal{D})^*$. We denote by $P(L(G))$ the set of all observable weighted sequences for G, and by $\sigma_1\sigma_2$ the concatenation of weighted sequences σ_1 and σ_2. In addition, σ_2 is a prefix of σ_1 if there exists another sequence σ_3 such that $\sigma_1 = \sigma_2\sigma_3$.

3. Notion of I-detectability and I-opacity

As in Lai et al. (2020), without loss of generality, we restrict our attention to a WA $G = (Q, E, \alpha, \mu)$, where the weights of all initial states are equal to e. We make the following assumptions on the studied WA G: (1) G is unambiguous; (2) G is deadlock free, that is, for any state of the system, there exists at least one output transition, i.e., $(\forall q \in Q)(\exists a \in E, q' \in Q)\mu(a)_{qq'} \neq \varepsilon$; (3) There is no circuit labeled only by unobservable labels in G.

(2) implies that the length of a generated weighted sequence becomes infinite as the system evolves indefinitely. (3) implies that the generated sequences of unobservable labels have finite length. Besides, as mentioned in the introductory section, (1) defines the broadest class of WAs for which we have been so far able to handle I-detectability and I-opacity verification.

3.1. Initial-state detectability

Definition 6. Given a UWA G, the set of possible initial states after observing $\sigma_o \in P(L(G))$ is defined as

$$I(\sigma_o) = \{q \in Q_i \mid \exists q' \in Q, \exists \sigma \in L(G) : P(\sigma) = \sigma_o, q \overset{\sigma}{\rightsquigarrow} q'\}. \tag{2}$$

Lemma 1. *Consider a non-empty observation $\sigma_o \in P(L(G))$. Let*

$$\begin{aligned}I'(\sigma_o) = \{&q \in Q_i \mid \exists q' \in Q, \exists \sigma \in L(G) :\\ &P(\sigma) = \sigma_o, q \overset{\sigma}{\rightsquigarrow} q', lab_f(\sigma) = lab_f(\sigma_o)\}.\end{aligned} \tag{3}$$

Then $I(\sigma_o) = I'(\sigma_o)$.

Proof. Let q_i be an initial state with $q_i \in I'(\sigma_o)$. According to Eqs. (2) and (3), $q_i \in I(\sigma_o)$. On the other hand, consider an initial state $q_0 \in I(\sigma_o)$. By Eq. (2), there must exist a path π from q_0 ending with $lab_f(\sigma_o)$ or an unobservable label such that $P(\sigma(\pi)) = \sigma_o$. If π ends with $lab_f(\sigma_o)$, then it is trivial that $q_0 \in I'(\sigma_o)$. When π ends with an unobservable label, we assume that it can be represented as $\pi = (q_0, v_1e_1, q_1)\cdots(q_{n-1}, v_ne_n, q_n)(q_n, v_{n+1}, q_{n+1})$, where $v_1, \ldots, v_{n+1} \in E_{uo}^*$. Let $\pi' = (q_0, v_1e_1, q_1)\cdots(q_{n-1}, v_ne_n, q_n)$. Then π' satisfies Eq. (3). Hence, q_0 belongs to $I'(\sigma_o)$. $\square$

As in a logical DES (Shu & Lin, 2013), in this paper, a possible trajectory of a WA G is represented by an infinite sequence of (label, weight) pairs that G may generate. The set of all possible trajectories of G defines the ω-language $L^\omega(G)$. For any sequence $\sigma \in L^\omega(G)$, we denote by $Pre(\sigma)$ the set of all its prefixes.

Definition 7 (*Strong (Weak) I-detectability*)**.** Given a UWA $G = (Q, E, \alpha, \mu)$, where the set of initial states $Q_i \subseteq Q$ is not empty, i.e., $Q_i \neq \emptyset$, G is strongly (resp. weakly) I-detectable with respect to projection P if, for all (resp. some) trajectories, the set of possible initial states shrinks to a singleton after a finite number of observations, i.e.,

$$\begin{aligned}&(\exists n \in \mathbb{N})(\forall \sigma \text{ (resp. } \exists \sigma) \in L^\omega(G))(\forall \sigma' \in Pre(\sigma))\\ &\qquad |P(\sigma')| > n \Rightarrow |I(P(\sigma'))| = 1.\end{aligned}$$

From the above definition, we know that if a UWA is strongly I-detectable, then it is weakly I-detectable.

3.2. Initial-state opacity

The generated weighted language of a UWA $G = (Q, E, \alpha, \mu)$ from an initial state $q_i \in Q_i$ is defined as

$$\begin{aligned}L(G, q_i) = \{&y \in (E \times \mathcal{D})^* \mid \exists q \in Q,\\ &\exists \omega \in E^*, \exists \pi \in q_i \overset{\omega}{\rightsquigarrow} q : \sigma(\pi) = y\}.\end{aligned} \tag{4}$$

In addition, given a subset $X \subseteq Q_i$, we define the weighted language generated from X as $L(G, X) = \bigcup_{q_i \in X} L(G, q_i)$. Due to unambiguity, if $Q_i = Q_i^1 \cup Q_i^2$, then the generated weighted language of G can be represented by $L(G) = \bigcup_{q_i \in Q_i} L(G, q_i) = L(G, Q_i^1) \cup L(G, Q_i^2)$, and $P(L(G)) = P(L(G, Q_i^1)) \cup P(L(G, Q_i^2))$.

Given a UWA $G = (Q, E, \alpha, \mu)$, an intruder can only observe the projection of the generated language, i.e., $P(L(G))$. Assume that the intruder has full knowledge of the structure of G, and that the secret is described by an arbitrary subset of Q.

Definition 8 (*Initial-state Opacity*)**.** Given a UWA $G = (Q, E, \alpha, \mu)$, projection $P : E^* \to E_o^*$, and a set of secret states $Q_s \subseteq Q$, G is initial-state opaque with respect to Q_s and P, if for all $q \in Q_i \cap Q_s$ and for all $\sigma \in L(G, q)$, there exist $q' \in Q_i \setminus Q_s$ and $\sigma' \in L(G, q')$ such that $P(\sigma') = P(\sigma)$, that is, $P(L(G, Q_i \cap Q_s)) \subseteq P(L(G, Q_i \setminus Q_s))$, or equivalently, $P(L(G)) = P(L(G, Q_i \setminus Q_s))$.

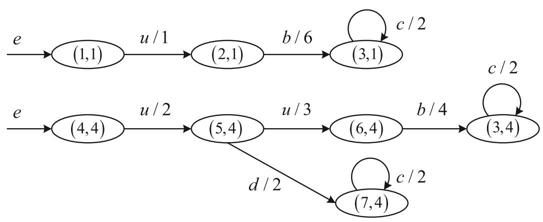

Fig. 2. Augmented automaton G^{aug} of G in Fig. 1.

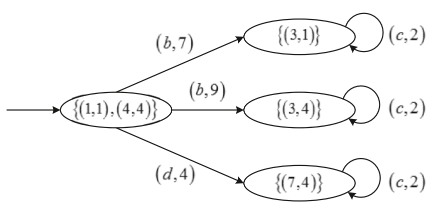

Fig. 3. I-observer G^{aug}_{obs} of G in Fig. 1.

Example 3. Consider again the UWA G in Fig. 1. We assume that the set of secret states is $Q_s = \{3, 4\}$, and u is the only unobservable label. (1) Detectability analysis: Initially, G can be in state 1 and/or state 4. Once an observation is obtained, i.e., $(b, 7)$, $(b, 9)$ or $(d, 4)$, we can uniquely determine the initial state, from which the system starts. Therefore, G is strongly I-detectable and weakly I-detectable. If the weight of transition $(5, u, 6)$ is now changed from 3 to 1, then G is not strongly I-detectable. It can be found that for infinite weighted sequence $(b, 7)(c, 9)(c, 11)(c, 13)\cdots$, we have $I((b, 7)(c, 9)(c, 11)(c, 13)\cdots) = \{1, 4\}$. (2) Opacity analysis: Consider the secret initial state 4 and $\sigma = (u, 2)(d, 4) \in L(G, 4)$. No weighted sequence can be generated by G from non-secret initial state 1 such that its projection is equal to $P(\sigma)$. Therefore G is not initial-state opaque with respect to secret Q_s. □

4. Verification of I-detectability

4.1. I-observer for strong and weak I-detectability

We show that the strong and weak I-detectability of a UWA G can be checked using an I-observer of an augmented automaton obtained from G. The construction of the I-observer extends the approach in Shu and Lin (2013) by using a weighted alphabet that captures the quantitative information associated to observations.

The I-observer $G^{aug}_{obs} = (Q^{aug}_{obs}, E^{aug}_{obs}, \delta^{aug}_{obs}, q^{aug}_{i,obs})$ of a UWA $G = (Q, E, t, Q_i, \varrho)$ is constructed by Algorithm 1, which contains two steps. Step 1 extends G to its augmented version $G^{aug} = \left(Q^{aug}, E, t^{aug}, Q^{aug}_i, \varrho^{aug}\right)$, in which each state $q^{aug} \in Q^{aug}$ is a pair (q_c, q_i), representing that state q_c can be reached in G from initial state q_i. Step 2 computes the observer G^{aug}_{obs} for the augmented automaton G^{aug} by the approach that is first presented in our recent work (Lai et al., 2020). Observer G^{aug}_{obs} is a deterministic finite state automaton over a weighted alphabet $E^{aug}_{obs} \subseteq E_o \times \mathcal{D}$. That is, G^{aug}_{obs} has only one initial state, and from a given state no two transitions of G^{aug}_{obs} are labeled by the same weighted label $(a, t_a) \in E^{aug}_{obs}$.

Example 4. Consider again the UWA G in Fig. 1. By applying Algorithm 1, we obtain the augmented automaton G^{aug} and I-observer G^{aug}_{obs} visualized in Figs. 2 and 3, respectively. □

Algorithm 1 Construction of the I-observer of a UWA

Input: A UWA $G = (Q, E, t, Q_i, \varrho)$.
Output: An I-observer $G^{aug}_{obs} = (Q^{aug}_{obs}, E^{aug}_{obs}, \delta^{aug}_{obs}, q^{aug}_{i,obs})$ of G.

1: Construct an augmented automaton G^{aug} of G as follows:

- $Q^{aug}_i = \{(q, q) \mid q \in Q_i\}$ is the set of initial states;
- $\varrho^{aug} : Q^{aug}_i \to \mathcal{D}$ is the function of initial weights defined as: $\varrho^{aug}((q, q)) = \varrho(q)$;
- $Q^{aug}_1 = \{(q, q_i) \mid q \in Q, q_i \in Q_i\}$;
- $t^{aug} : Q^{aug}_1 \times E \times Q^{aug}_1 \to \mathcal{D}$ is the transition function, where $t^{aug}((q_c, q_i), a, (q'_c, q'_i))$ is defined as: $t^{aug}((q_c, q_i), a, (q'_c, q'_i)) = t(q_c, a, q'_c)$ if $q_i = q'_i$; otherwise, $t^{aug}((q_c, q_i), a, (q'_c, q'_i)) = \varepsilon$;
- Let $G^{aug} = (Q^{aug}, E, t^{aug}, Q^{aug}_i, \varrho^{aug}) = Ac(Q^{aug}_1, E, t^{aug}, Q^{aug}_i, \varrho^{aug})$[2].

2: Compute the observer G^{aug}_{obs} of G^{aug}, i.e., the I-observer of G as follows:

- $q^{aug}_{i,obs} = Q^{aug}_i$;
- E^{aug}_{obs} consists of all weighted labels $(a, \tau) \in E_o \times (\mathcal{D} \setminus \{\varepsilon\})$ for which $\exists q \in Q_1 \cup Q^{aug}_i$, $\exists q' \in Q^{aug}$, $\exists v \in E^*_{uo}$, s.t. $t^{aug}(q, va, q') = \tau$, where $Q_1 = \left\{q \in Q^{aug} \mid \exists q' \in Q^{aug}, \exists a \in E_o : t^{aug}(q', a, q) \neq \varepsilon\right\}$ is the set of states in G^{aug} that have at least one input transition marked by an observable label;
- $\delta^{aug}_{obs} : 2^{Q^{aug}} \times E^{aug}_{obs} \to 2^{Q^{aug}}$ is the state transition function. $\delta^{aug}_{obs}(q^{aug}_{obs}, (a, \tau))$ is defined as:
$$\delta^{aug}_{obs}(q^{aug}_{obs}, (a, \tau)) = \{q' \in Q^{aug} \mid \exists q \in q^{aug}_{obs}, \exists v \in E^*_{uo} : t^{aug}(q, va, q') = \tau\}.$$
- Let $G^{aug}_{obs} = (Q^{aug}_{obs}, E^{aug}_{obs}, \delta^{aug}_{obs}, q^{aug}_{i,obs}) = Ac(2^{Q^{aug}}, E^{aug}_{obs}, \delta^{aug}_{obs}, q^{aug}_{i,obs})$.

Let $(E^{aug}_{obs})^*$ be the set of all the finite strings over weighted alphabet E^{aug}_{obs} including (λ, e). The language generated by the I-observer is

$$L(G^{aug}_{obs}) = \{\omega \in (E^{aug}_{obs})^* \mid \exists q^{aug}_{obs} \in Q^{aug}_{obs} : \delta^{aug}_{obs}(q^{aug}_{i,obs}, \omega) = q^{aug}_{obs}\},$$

which is a subset of $(E^{aug}_{obs})^*$, i.e., $L(G^{aug}_{obs}) \subseteq (E^{aug}_{obs})^*$. For any observed weighted sequence $\sigma_o = (a_1, \tau_1)(a_2, \tau_2)\cdots(a_n, \tau_n) \in P(L(G))$, we define $\sigma^{elem}_o = (a_1, \tau_1)(a_2, \tau_2 - \tau_1)\cdots(a_n, \tau_n - \tau_{n-1})$ to denote its equivalent notation in $(E^{aug}_{obs})^*$. Note that $\tau_k - \tau_{k-1}$ represents the weight for the elementary transition according to a_k for $k = 2, 3, \ldots, n$. We denote by $P(L(G))^{elem}$ the equivalent notation of $P(L(G))$, that is,

$$P(L(G))^{elem} = \{\sigma \in (E_o \times \mathcal{D})^* \mid \exists \sigma_o \in P(L(G)) : \sigma^{elem}_o = \sigma\}.$$

The following lemma states the relationship between the languages generated by G and G^{aug}_{obs}. The proof follows immediately from the construction process of G^{aug}_{obs}, and hence here it is omitted.

Lemma 2. *The language $L(G^{aug}_{obs})$ generated by I-observer G^{aug}_{obs} coincides with $P(L(G))^{elem}$, that is, $L(G^{aug}_{obs}) = P(L(G))^{elem}$.*

Lemma 3. *The possible initial states of UWA G after observing a non-empty weighted sequence $\sigma_o = (a_1, \tau_1)(a_2, \tau_2)\cdots(a_k, \tau_k) \in$*

[2] In this paper, we denote by the $Ac(G)$ the automaton obtained by removing all the states that are not accessible as well as transitions associated with such states in G.

$P(L(G))$ is given by

$$I(\sigma_o) = \{q_i \in Q_i \mid \exists q_c \in Q : (q_c, q_i) \in \delta^{aug}_{obs}(q^{aug}_{i,obs}, (a_1, \tau_1)(a_2, \tau_2 - \tau_1)\cdots(a_k, \tau_k - \tau_{k-1}))\}.$$

Proof.

$$\begin{aligned} I(\sigma_o) &= I'(\sigma_o) \text{ (by Lemma 1)} \\ &= \{q_i \in Q_i \mid \exists q_c \in Q, \exists \sigma \in L(G) : P(\sigma) = \sigma_o, q_i \overset{\sigma}{\rightsquigarrow} q_c, lab_f(\sigma) = lab_f(\sigma_o)\} \\ &= \{q_i \in Q_i \mid \exists q_c \in Q, \exists \sigma \in L(G^{aug}) : P(\sigma) = \sigma_o, (q_i, q_i) \overset{\sigma}{\rightsquigarrow} (q_c, q_i), lab_f(\sigma) = lab_f(\sigma_o)\} \\ &\qquad \text{(by step 1 in Algorithm 1)} \\ &= \{q_i \in Q_i \mid \exists q_c \in Q : (q_c, q_i) \in \delta^{aug}_{obs}(q^{aug}_{i,obs}, (a_1, \tau_1)(a_2, \tau_2 - \tau_1)\cdots(a_k, \tau_k - \tau_{k-1}))\} \\ &\qquad \text{(by Proposition 1 in Lai et al. (2020))} \quad \square \end{aligned}$$

Now we introduce the criteria for checking strong I- detectability and weak I-detectability for UWA G based on its I-observer G^{aug}_{obs}. We denote by S_{ci} the set of all elementary circuits of G^{aug}_{obs} as:

$$S_{ci} = \{(q^{aug}_{obs}, s) \in Q^{aug}_{obs} \times (E^{aug}_{obs})^* \mid \delta^{aug}_{obs}(q^{aug}_{obs}, s) = q^{aug}_{obs} \wedge |s| \geq 1 \wedge [\forall s' \in Pre(s) \text{ s.t. } s' \neq s \wedge |s'| \geq 1 : \delta^{aug}_{obs}(q^{aug}_{obs}, s') \neq q^{aug}_{obs}]\}.$$

Besides, we use $q^{aug}_{obs} \in (q^{aug\prime}_{obs}, s)$ to represent that node q^{aug}_{obs} is visited by circuit $(q^{aug\prime}_{obs}, s)$. Let $Q^{aug}_{I,obs}$ be a subset of Q^{aug}_{obs} consisting of states with the same second element (initial state of G), that is,

$$Q^{aug}_{I,obs} = \{q^{aug}_{obs} \in Q^{aug}_{obs} \mid \exists q \in Q_i, \forall (q_c, q_i) \in q^{aug}_{obs} : q_i = q\}.$$

Theorem 1 (*Criterion for Checking Strong I-detectability*)**.** *A UWA G is strongly I-detectable with respect to projection P iff any node belonging to an elementary circuit of G^{aug}_{obs} is in $Q^{aug}_{I,obs}$. Formally, $\forall q^{aug}_{obs} \in Q^{aug}_{obs}$, if $\exists (q^{aug\prime}_{obs}, s) \in S_{ci}$ such that $q^{aug}_{obs} \in (q^{aug\prime}_{obs}, s)$, then $q^{aug}_{obs} \in Q^{aug}_{I,obs}$.*

Proof. (If) By Algorithm 1, we know that once G reaches a state belonging to $Q^{aug}_{I,obs}$, it will stay in $Q^{aug}_{I,obs}$ forever. Suppose $\forall q^{aug}_{obs} \in Q^{aug}_{obs}$, if $\exists (q^{aug\prime}_{obs}, s) \in S_{ci}$ such that $q^{aug}_{obs} \in (q^{aug\prime}_{obs}, s)$, then $q^{aug}_{obs} \in Q^{aug}_{I,obs}$. Then, I-observer Q^{aug}_{obs} will eventually reach a state in $Q^{aug}_{I,obs}$ after a finite number of observations for all trajectories of G. Hence, by combining Lemma 3, the set of possible initial states is a singleton for all possible continuations, that is, G is strongly I-detectable. (Only If) Assume $\exists q^{aug}_{obs} \in Q^{aug}_{obs}$, $\exists (q^{aug\prime}_{obs}, s) \in S_{ci}$ such that $q^{aug}_{obs} \in (q^{aug\prime}_{obs}, s)$ and $q^{aug}_{obs} \in Q^{aug}_{obs} \setminus Q^{aug}_{I,obs}$. Then a possible evolution of G can iterate indefinitely circuit $(q^{aug\prime}_{obs}, s)$. That is, we cannot determine the initial state of G for such a trajectory forever. Hence, G is not strongly I-detectable. $\square$

Theorem 2 (*Criterion for Checking Weak I-detectability*)**.** *A UWA G is weakly I-detectable with respect to P iff $Q^{aug}_{I,obs} \neq \emptyset$.*

Proof. (If) If $Q^{aug}_{I,obs}$ is not empty, then I-observer Q^{aug}_{obs} can reach a state in $Q^{aug}_{I,obs}$ after a finite number of observations for some trajectories of G. In this case, we can determine the only possible initial state of G for trajectories corresponding to continuations of these observations. Hence, G is weakly I-detectable. (Only If) If $Q^{aug}_{I,obs} = \emptyset$, then the set of possible initial states does not shrink to a singleton whatever the trajectory is, i.e., G is not weakly I-detectable. $\square$

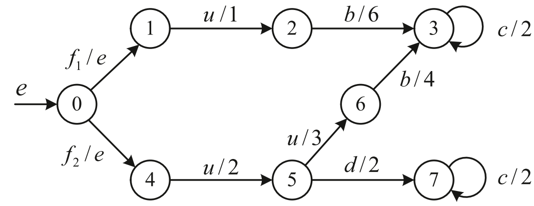

Fig. 4. Modified automaton G' of G in Fig. 1.

Example 5. Consider the I-observer G^{aug}_{obs} in Fig. 3 of UWA G in Fig. 1. There are four states in G^{aug}_{obs}, i.e., $\{(1, 1), (4, 4)\}$, $\{(3, 1)\}$, $\{(3, 4)\}$, $\{(7, 4)\}$, and we have $Q^{aug}_{I,obs} = \{\{(3, 1)\}, \{(3, 4)\}, \{(7, 4)\}\}$. It can be checked that all elementary circuits have all their nodes in $Q^{aug}_{I,obs}$. Therefore, by Theorem 1, G is strongly I-detectable (hence weakly I-detectable). $\square$

Remark 2. For checking strong I-detectability of UWA $G = (Q, E, \alpha, \mu)$, we have to find out all states that belong to an elementary circuit in its I-observer $G^{aug}_{obs} = (Q^{aug}_{obs}, E^{aug}_{obs}, \delta^{aug}_{obs}, q^{aug}_{i,obs})$. This can be done by finding all the strongly connected components in G^{aug}_{obs}, whose complexity is linear in the number of states and transitions of G^{aug}_{obs}, i.e., $\mathcal{O}(|Q^{aug}_{obs}| + |Q^{aug}_{obs}| \times |E^{aug}_{obs}| \times |Q^{aug}_{obs}|)$. By Algorithm 1, $|Q^{aug}_{obs}|$ is bounded by $2^{|Q|^2} - 1$. Hence, the complexity of verifying strong and weak I-detectability using I-observer is $\mathcal{O}(2^{2|Q|^2} \times |E^{aug}_{obs}|)$, where $|E^{aug}_{obs}|$ is usually exponential in $|Q|$. $\square$

4.2. Diagnosability-based approach for strong I-detectability

We present an approach that has lower complexity (compared with the I-observer-based method), but is still exponential, to verify the strong I-detectability of a UWA G. We show that this verification can be done by means of diagnosability analysis of a new UWA G' obtained from G. To perform the diagnosability analysis, we extend the algorithm in Jiang et al. (2001) to build an automaton denoted by G_d from G' with a weighted alphabet.

Definition 9. Given a UWA $G = (Q, E, t, Q_i, \varrho)$, where $Q_i = \{q_1, q_2, \ldots, q_n\}$ is the set of n initial states, a modified UWA $G' = (Q', E', t', Q'_i, \varrho')$ obtained from G is defined by adding a new state $q_w \notin Q$ and $|Q_i|$ new labels $\{f_1, f_2, \ldots, f_{|Q_i|}\} \cap E = \emptyset$ as follows.

- $Q' = Q \cup \{q_w\}$ is the finite set of states;
- $E' = E \cup \{f_1, f_2, \ldots, f_{|Q_i|}\}$;
- $t' : Q' \times E' \times Q' \to \mathcal{D}$ is the transition function defined as: $t'(q_w, f_i, q_i) = e$ for $i = 1, 2, \ldots, |Q_i|$; $t'(q, a, q') = t'(q, a, q')$ if $q, q' \in Q$ and $a \in E$; otherwise, $t'(q, a, q') = \varepsilon$;
- $Q'_i = \{q_w\}$ is the set of initial states;
- $\varrho' : Q'_i \to \mathcal{D}$ is the initial weights function: $\varrho'(q_w) = e$.

In simple words, G' is a UWA obtained from G by adding a new state q_w to become the unique initial state, and by introducing new state transitions (q_w, f_i, q_i) with identity weights for $i = 1, 2, \ldots, |Q_i|$.

Example 6. Consider the UWA G in Fig. 1. The modified automaton G' is depicted in Fig. 4. $\square$

Let f_i, $i = 1, 2, \ldots, |Q_i|$, be unobservable labels belonging to $|Q_i|$ different types of faults, i.e., $E_f = E_{f1} \cup E_{f2} \cup \cdots \cup E_{f|Q_i|} = \{f_1\} \cup \{f_2\} \cup \cdots \cup \{f_{|Q_i|}\}$, and suppose that all labels in E represent normal behavior. We denote by $E'_{uo} = E_{uo} \cup E_f$ the set of unobservable labels in G'. For any weighted sequence $s = (e_1, \tau_1)(e_2, \tau_2)\cdots(e_n, \tau_n) \in (E' \times \mathcal{D})^*$ or any logical sequence $s = e_1 e_2 \cdots e_n \in (E')^*$, we denote by $lab_i(s) = e_1$ the first label in

s. As in logical automata (Sampath et al., 1995), the diagnosability of UWA $G' = (Q', E', t', Q'_i, \varrho')$ can be defined as follows.

Definition 10 (*Diagnosability*). The UWA $G' = (Q', E', t', Q'_i, \varrho')$ is diagnosable with respect to projection $P : (E')^* \to E_o^*$ and $|Q_i|$ different types of faults $E_f = \{f_1, f_2, \ldots, f_{|Q_i|}\}$ if the following holds:

$(\forall f_i \in E_f)(\exists n_i \in \mathbb{N})(\forall v = (f_i, e)t \in L(G'), |t| \geq n_i) \Rightarrow$
$(\forall \omega \in L(G'), P(\omega) = P(v))(lab_i(\omega) = f_i)$.

In simple words, diagnosability requires that when a fault label f_i occurs in G', after a finite number of observations, one can detect its occurrence. The following lemma follows immediately from the construction process of G' given in Definition 9, and the relationship between diagnosability and strong I-detectability.

Lemma 4. *A UWA G is strongly I-detectable iff the modified UWA G' given in Definition 9 is diagnosable with respect to $P : (E')^* \to E_o^*$ and $|Q_i|$ different types of faults $E_f = \{f_1, f_2, \ldots, f_{|Q_i|}\}$.*

Inspired by the work in Jiang et al. (2001), we present an approach for determining if G' is diagnosable with respect to a single fault type $E_{f_i} = \{f_i\}$, $i \in \{1, 2, \ldots, |Q_i|\}$, based on the construction of a finite state automaton $G_d = (Q_d, E_d, \delta_d, q_w^d)$ over a weighted alphabet $E_d \subseteq E_o \times \mathcal{D}$, as defined in Algorithm 2.

Algorithm 2 Construction of G_d for $E_{f_i} = \{f_i\}$

Input: UWA $G' = (Q', E', t', Q'_i, \varrho')$.
Output: NFA $G_d = (Q_d, E_d, \delta_d, q_w^d)$.

1: Construct an NFA G_o from G' as follows:
- $q_w^o = (q_w, N)$;
- $Q'_o = \{(q, f) \mid q \in Q_1 \cup \{q_w\}, f \in \{N, F_i\}\}$ where $Q_1 = \{q \in Q' \mid \exists q' \in Q', \exists a \in E_o : t'(q', a, q) \neq \varepsilon\}$ is the set of states in G' that have at least one input transition marked by an observable label;
- E_d consists of all weighted labels $(a, \tau) \in E_o \times (\mathcal{D} \setminus \{\varepsilon\})$ for which $\exists q \in Q_1 \cup \{q_w\}$, $\exists q' \in Q'$, $\exists v \in (E'_{uo})^*$, s.t. $t'(q, va, q') = \tau$;
- $\delta_o \subseteq Q'_o \times E_d \times Q'_o$ is the set of state transitions. $((q, f), (a, \tau), (q', f')) \in \delta_o$ iff $\exists v \in (E'_{uo})^*$ s.t.
  1) $t'(q, va, q') = \tau$;
  2) $(f' = f) \wedge (|v| = 0 \vee (|v| \geq 1 \wedge lab_i(v) \neq f_i))$ or $(f' = F_i) \wedge (|v| \geq 1 \wedge lab_i(v) = f_i)$.
- Let $G_o = (Q_o, E_d, \delta_o, q_w^o) = Ac(Q'_o, E_d, \delta_o, q_w^o)$.

2: Compute automaton $G_d = G_o \parallel G_o$, the parallel composition of G_o with itself, as follows:
- $q_w^d = (q_w^o, q_w^o) = ((q_w, N), (q_w, N))$;
- $Q'_d = \{(q_o^1, q_o^2) \mid q_o^1, q_o^2 \in Q_o\}$;
- $\delta_d \subseteq Q'_d \times E_d \times Q'_d$ is the set of state transitions. $((p_o^1, p_o^2), (a, \tau), (q_o^1, q_o^2)) \in \delta_d$ iff $(p_o^1, (a, \tau), q_o^1) \in \delta_o$ and $(p_o^2, (a, \tau), q_o^2) \in \delta_o$.
- Let $G_d = (Q_d, E_d, \delta_d, q_w^d) = Ac(Q'_d, E_d, \delta_d, q_w^d)$.

Example 7. Consider the UWA G' in Fig. 4. Assuming that f_1 is the unique fault, by applying Algorithm 2, we can obtain G_o and G_d shown in Figs. 5 and 6, respectively. □

Let S_{cd} be the set of all elementary circuits of G_d. Besides, for $q'_d \in Q_d$ and $(q_d, s) \in S_{cd}$, we use $q'_d \in (q_d, s)$ to represent that node q'_d is visited by circuit (q_d, s).

Theorem 3. *UWA G' is diagnosable with respect to fault type $E_{f_i} = \{f_i\}$, $i \in \{1, 2, \ldots, |Q_i|\}$, iff for every node $((q_d^1, f^1), (q_d^2, f^2)) \in$*

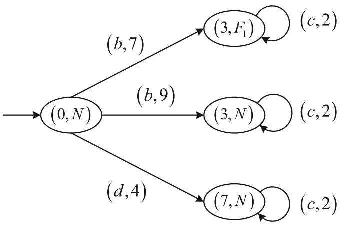

Fig. 5. Diagram of G_o of G' with respect to fault f_1.

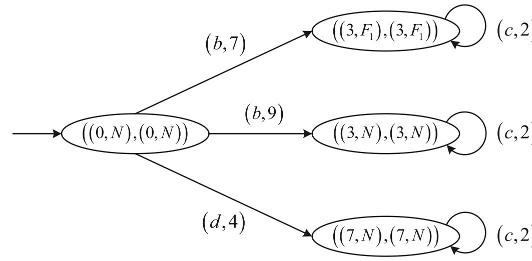

Fig. 6. Diagram of G_d with respect to fault f_1.

Q_d that belongs to an elementary circuit in G_d, we have $f^1 = f^2$. Formally, $\forall((q_i^1, f^1), (q_i^2, f^2)) \in Q_d$, if $\exists(q_d, s) \in S_{cd}$ such that $((q_i^1, f^1), (q_i^2, f^2)) \in (q_d, s)$, then $f^1 = f^2$.

Proof. (If) We suppose that G' is not diagnosable with respect to f_i, $i \in \{1, 2, \ldots, |Q_i|\}$. According to Definition 10 on diagnosability, this implies that there exist two infinite weighted sequences in G' such that they have equal projection, one contains f_i and the other one does not contain f_i. Since G_d is finite, by considering the relationship between G_d and G', there must exist an elementary circuit (q_d, s), where the labels of all the first elements of all nodes are N, and the labels of all the second elements of all nodes are F_i. Hence, $\exists((q_i^1, f^1), (q_i^2, f^2)) \in Q_d$, $\exists(q_d, s) \in S_{cd}$ such that $((q_i^1, f^1), (q_i^2, f^2)) \in (q_d, s)$ and $f^1 \neq f^2$.

(Only If) We assume that $\exists((q_i^1, f^1), (q_i^2, f^2)) \in Q_d$, $\exists(q_d, s) \in S_{cd}$ such that $((q_i^1, f^1), (q_i^2, f^2)) \in (q_d, s)$ and $f^1 \neq f^2$. We can further assume that $f^1 = N$ and $f^2 = F_i$. According to the construction of G_d, the above assumptions imply that for any $((q_j^1, f_j^1), (q_j^2, f_j^2)) \in (q_d, s)$, we have $f_j^1 = f^1 = N$ and $f_j^2 = f^2 = F_i$. Since elementary circuit (q_d, s) can be repeated infinitely, by considering the relationship between G_d and G', there are two infinite weighted sequences γ_1 and γ_2 in G' with the same projection, γ_1 contains fault f_i, and γ_2 does not contain f_i. More precisely, γ_1 and γ_2 lead from the initial state q_w^d to the entry point q_d of circuit (q_d, s) and repeat this circuit infinitely. Assume that q_d is reached by v, i.e., $q_d \in \delta_d(q_w^d, v)$. Then we have $P(\gamma_1)^{elem} = P(\gamma_2)^{elem} = sv^j$, where j is a large enough integer. Therefore, by Definition 10 of diagnosability, G' is not diagnosable. □

Remark 3. Similar to Remark 2, the necessary and sufficient condition in Theorem 3 can be verified by finding all the strongly connected components in $G_d = (Q_d, E_d, \delta_d, q_\omega^d)$, whose complexity is $\mathcal{O}(|Q_d| + |Q_d| \times |E_d| \times |Q_d|)$. From Algorithm 2, the number of states in G_o is bounded by $2 \times (|Q| + 1) = 2|Q| + 2$.

Due to $G_d = G_o \parallel G_o$, $|Q_d|$ is bounded by $(2|Q|+2)^2 = 4|Q|^2 + 8|Q| + 4$. Algorithm 2 should be applied $|Q_i|$ times for testing the diagnosability of G' with respect to $|Q_i|$ different fault types. Therefore, by combining Lemma 4, the complexity of verifying strong I-detectability based on diagnosability for UWA G is $\mathcal{O}(|Q|^4 \times |E_d| \times |Q_i|)$, where $|E_d|$ is exponential in $|Q|$ in general. Note that under the assumption that all the unobservable events of UWA G are represented by a unique symbol, $|E_d|$ is bounded by $|Q|^3 \times |E_o|$, and the above exponential complexity is reduced to polynomial. □

Example 8. Consider G_d presented in Fig. 6. According to Theorem 3, we know that the corresponding UWA G' in Fig. 4 is diagnosable with respect to fault f_1. Similarly, it can be checked that G' is diagnosable with respect to fault f_2 by constructing another G_d on f_2 (here G_d is omitted). Therefore, according to Lemma 4, the original system G in Fig. 1 is strongly I-detectable, which is consistent with the result in Example 5. □

5. Verification of initial-state opacity

In this section, we show that the I-observer constructed in Section 4.1 can be used to check I-opacity of UWAs.

Lemma 5. *Given a UWA $G = (Q, E, \alpha, \mu)$, projection $P : E^* \to E_o^*$, and a set of secret states $Q_s \subseteq Q$, G is initial-state opaque with respect to Q_s and P iff for all $\sigma_o \in P(L(G))$, $I(\sigma_o) \nsubseteq Q_s$ holds.*

Proof.

$$
\begin{aligned}
&(\forall \sigma_o \in P(L(G)))I(\sigma_o) \nsubseteq Q_s \\
&\Leftrightarrow (\forall \sigma_o \in P(L(G)))(\exists q' \in I(\sigma_o))q' \notin Q_s \\
&\Leftrightarrow (\forall \sigma_o \in P(L(G)))(\exists q' \in Q_i \setminus Q_s)(\exists q \in Q) \\
&\qquad\qquad (\exists \sigma' \in L(G))P(\sigma') = \sigma_o \wedge q' \overset{\sigma'}{\rightsquigarrow} q \\
&\quad \text{(by the definition of } I(\sigma_o) \text{ in Eq. (2))} \\
&\Leftrightarrow (\forall \sigma_o \in P(L(G)))(\exists q' \in Q_i \setminus Q_s)(\exists \sigma' \in L(G, q'))P(\sigma') = \sigma_o \\
&\qquad \text{(according to Eq. (4))} \\
&\Leftrightarrow (\forall \sigma_o \in P(L(G, Q_i \cap Q_s)))(\exists q' \in Q_i \setminus Q_s) \\
&\qquad\qquad (\exists \sigma' \in L(G, q'))P(\sigma') = \sigma_o \\
&\text{(by } P(L(G)) = P(L(G, Q_i \cap Q_s)) \cup P(L(G, Q_i \setminus Q_s)) \text{ since} \\
&P(L(G, Q_i \cap Q_s)) \subseteq P(L(G)) \text{ and } \forall \sigma_o \in P(L(G, Q_i \setminus Q_s)), \\
&\exists q' \in Q_i \setminus Q_s, \exists \sigma' \in L(G, q') \text{ s.t. } P(\sigma') = \sigma_o) \\
&\Leftrightarrow (\forall q \in Q_i \cap Q_s)(\forall \sigma \in L(G, q))(\exists q' \in Q_i \setminus Q_s) \\
&\qquad\qquad (\exists \sigma' \in L(G, q'))P(\sigma') = P(\sigma)
\end{aligned}
$$

which is consistent with Definition 8 on I-opacity. □

For any $q_{obs}^{aug} \in Q_{obs}^{aug}$, we define $I(q_{obs}^{aug}) = \{q_i \in Q_i \mid \exists (q_c, q_i) \in q_{obs}^{aug}\}$ as the initial states of automaton G that it contains. The following theorem illustrates that the I-observer G_{obs}^{aug} can be used to verify the I-opacity for UWA G.

Theorem 4. *Given a UWA $G = (Q, E, \alpha, \mu)$, projection $P : E^* \to E_o^*$, and a set of secret states $Q_s \subseteq Q$, G is initial-state opaque with respect to Q_s and P iff*

$$(\forall q_{obs}^{aug} \in Q_{obs}^{aug})I(q_{obs}^{aug}) \nsubseteq Q_s$$

where Q_{obs}^{aug} is the set of states in I-observer G_{obs}^{aug} of G.

Proof. It follows from Lemmas 3 and 5. □

Example 9. Consider the I-observer G_{obs}^{aug} in Fig. 3 of UWA G in Fig. 1. It can be checked that G is always non-opaque with respect to P and an arbitrary secret Q_s so long as $Q_s \cap Q_i \neq \emptyset$. In fact, among the states of G_{obs}^{aug}, we have $I(\{3, 1\}) = \{1\}$ and $I(\{3, 4\}) = I(\{7, 4\}) = \{4\}$. Therefore, for a secret Q_s containing initial state 1 and/or 4, there necessarily exists one state $q_{obs}^{aug} \in Q_{obs}^{aug}$ such that $I(q_{obs}^{aug}) \subseteq Q_s$. □

6. Conclusion

In this paper, an I-observer is constructed to verify the strong I-detectability, weak I-detectability and I-opacity of UWAs. Besides, a diagnosability-based approach, with a lower complexity, is proposed for checking strong I-detectability. Our future work is to explore new techniques that can handle the I-detectability and I-opacity problem for more general classes of WAs.

References

Bryans, J. W., Koutny, M., & Ryan, P. Y. (2005). Modelling opacity using petri nets. *Electronic Notes Theoretical Computer Science*, *121*, 101–115.

Droste, M., Kuich, W., & Vogler, H. (2009). *Handbook of weighted automata*. Springer Science & Business Media.

Gaubert, S. (1995). Performance evaluation of (max,+) automata. *IEEE Transactions on Automatic Control*, *40*(12), 2014–2025.

Gaubert, S., & Mairesse, J. (1999). Modeling and analysis of timed petri nets using heaps of pieces. *IEEE Transactions on Automatic Control*, *44*(4), 683–697.

Ji, Y., Yin, X., & Lafortune, S. (2019). Enforcing opacity by insertion functions under multiple energy constraints. *Automatica*, *108*, Article 108476.

Jiang, S., Huang, Z., Chandra, V., & Kumar, R. (2001). A polynomial algorithm for testing diagnosability of discrete-event systems. *IEEE Transactions on Automatic Control*, *46*(8), 1318–1321.

Keroglou, C., & Hadjicostis, C. N. (2017). Verification of detectability in probabilistic finite automata. *Automatica*, *86*, 192–198.

Kirsten, D. (2008). A burnside approach to the termination of mohri's algorithm for polynomially ambiguous min-plus-automata. *Rairo-Theoretical Information Application*, *42*(3), 553–581.

Komenda, J., Lahaye, S., & Boimond, J. L. (2016). Determinization of timed petri nets behaviors. *Discrete Event Dynamic Systems*, *26*(3), 413–437.

Lahaye, S., Komenda, J., & Boimond, J. L. (2015). Compositions of (max,+) automata. *Discrete Event Dynamic Systems*, *25*(1–2), 323–344.

Lahaye, S., Lai, A., Komenda, J., & Boimond, J. L. (2020). A contribution to the determinization of max-plus automata. *Discrete Event Dynamic Systems*, *30*, 1–20.

Lai, A., Lahaye, S., & Giua, A. (2019). State estimation of max-plus automata with unobservable events. *Automatica*, *105*, 36–42.

Lai, A., Lahaye, S., & Giua, A. (2020). Verification of detectability for unambiguous weighted automata. *IEEE Transactions on Automatic Control*, http://dx.doi.org/10.1109/TAC.2020.2995173.

Masopust, T., & Yin, X. (2019a). Complexity of detectability, opacity and a-diagnosability for modular discrete event systems. *Automatica*, *101*, 290–295.

Masopust, T., & Yin, X. (2019b). Deciding detectability for labeled petri nets. *Automatica*, *104*, 238–241.

Mohri, M. (1997). Finite-state transducers in language and speech processing. *Computational Linguistics*, *23*(2), 269–311.

Saboori, A., & Hadjicostis, C. N. (2013). Verification of initial-state opacity in security applications of discrete event systems. *Information Sciences*, *246*, 115–132.

Sampath, M., Sengupta, R., Lafortune, S., Sinnamohideen, K., & Teneketzis, D. (1995). Diagnosability of discrete-event systems. *IEEE Transactions on Automatic Control*, *40*(9), 1555–1575.

Sasi, Y., & Lin, F. (2018). Detectability of networked discrete event systems. *Discrete Event Dynamic Systems*, *28*(3), 449–470.

Shu, S., & Lin, F. (2011). Generalized detectability for discrete event systems. *Systems & Control Letters*, *60*(5), 310–317.

Shu, S., & Lin, F. (2012). Delayed detectability of discrete event systems. *IEEE Transactions on Automatic Control*, *58*(4), 862–875.

Shu, S., & Lin, F. (2013). I-detectability of discrete-event systems. *IEEE Transactions on Automatic Science and Engineering*, *10*(1), 187–196.

Triska, L., & Moor, T. (2020). Behaviour equivalent max-Plus automata for a class of timed petri nets. In *Proceedings of the workshop on discrete-event systems*.

Wu, Y. C., & Lafortune, S. (2013). Comparative analysis of related notions of opacity in centralized and coordinated architectures. *Discrete Event Dynamic Systems*, *23*(3), 307–339.

Yin, X. (2017). Initial-state detectability of stochastic discrete-event systems with probabilistic sensor failures. *Automatica*, *80*, 127–134.

Yin, X., & Lafortune, S. (2017). A new approach for the verification of infinite-step and k-step opacity using two-way observers. *Automatica*, *80*, 162–171.

Yin, X., Li, Z., Wang, W., & Li, S. (2019). Infinite-step opacity and k-step opacity of stochastic discrete-event systems. *Automatica*, *99*, 266–274.

Zhang, K. (2017). The problem of determining the weak (periodic) detectability of discrete event systems is pspace-complete. *Automatica*, *81*, 217–220.

Zhang, K., Yin, X., & Zamani, M. (2019). Opacity of nondeterministic transition systems: A (bi) simulation relation approach. *IEEE Transactions on Automatic Control*.

Aiwen Lai received the B.S. degree in automation from Xidian University, Xi'an, China, in 2014, the M.S. degree in information systems science from Aix-Marseille University, France, in 2016, and the Ph.D. degree in automatic control from University of Angers, France, in 2019. He is currently an Assistant Professor with the Department of Automation, Xiamen University, Xiamen, China. His current research interests include state estimation, fault diagnosis and opacity of discrete event systems.

Sébastien Lahaye is professor of Automatic Control at Polytech Angers, University of Angers, France. He received the Ph.D. degree in systems and computer engineering in 2000 from the University of Angers, France. His research interests include discrete event systems, complex systems, control, properties analysis and verification, max-plus algebra, Petri nets and automata.

Zhiwu Li received the B.S., M.S., and Ph.D. degrees in mechanical engineering, automatic control, and manufacturing engineering, respectively, all from Xidian University, Xi'an, China, in 1989, 1992, and 1995, respectively. He joined Xidian University, in 1992. He is currently with the Institute of Systems Engineering, Macau University of Science and Technology, Taipa, Macau. He was a Visiting Professor with the University of Toronto, Technion (Israel Institute of Technology), Martin-Luther University, Conservatoire National des Arts et Métiers (Cnam), Meliksah Universitesi, University of Cagliari, University of Alberta, and King Saud University. His current research interests include Petri net theory and application, supervisory control of discrete event systems, workflow modeling and analysis, system reconfiguration, game theory, and data and process mining. He is a fellow of the Institute of Electrical and Electronics Engineers (IEEE).