SCIENCE CHINA
Information Sciences

• RESEARCH PAPER •

November 2024, Vol. 67, Iss. 11, 212204:1–212204:11
https://doi.org/10.1007/s11432-023-4041-6

Multi-step state-based opacity for unambiguous weighted machines

Zhipeng ZHANG[1], Chengyi XIA[1*], Guoyuan QI[2] & Jun FU[3]

[1]*School of Artificial Intelligence, Tiangong University, Tianjin* 300387*, China;*
[2]*School of Control Science and Engineering, Tiangong University, Tianjin* 300387*, China;*
[3]*State Key Laboratory of Synthetical Automation for Process Industries, Northeastern University, Shenyang* 110819*, China*

Received 19 September 2023/Revised 15 December 2023/Accepted 16 January 2024/Published online 23 October 2024

Abstract Opacity is a central concept in the issue of privacy security and has been studied extensively in fields such as finite automata, probabilistic automata, and stochastic automata. Here, we investigate the problem of validating multi-step opaque properties through unambiguous weighted machines from the perspective of cyber-physical systems. First, the notion of multi-step state-based opacity for unambiguous weighted machines is presented and defined. It includes two variants of delays with a finite K and infinite steps. Subsequently, the weighted state estimate with K (infinite)-step delay is established by abstracting the possible state set that the system could have through these weighted observations. Meanwhile, to keep the observable weighted sequence consistent between the bidirectional observers, the unobserved weights of the reverse weighted machine are assumed to be reserved. Subsequently, the existence conditions are developed, and the corresponding algorithms, termed the weighted bidirectional observer, are generalized to verify these properties. Finally, several numerical examples are illustrated to demonstrate the effectiveness of the proposed method. Taken together, the current approach will be conducive to a deep understanding of the security and privacy of cyber-physical systems.

Keywords logical dynamical systems, weighted state machine, state estimation, opacity, cyber physical systems

1 Introduction

With the extensive applications of intelligent systems [1–5] in the real world, the new technologies, centering on cyber-physical systems, including smart grid, autonomous vehicle, and medical equipment networks, are emerging continuously. However, the remarkable characteristics of the strong interconnections between information space and the physical world also result in some critical information leakages, which present the double challenges of addressing security and privacy [6–10].

At present, cyber-physical systems are becoming more vulnerable to external intruders, which can then lead to the leakage of critical information, including user transaction patterns and usage habits. Hence, the analysis and control of security and privacy issues remains an interesting research topic. Many of these problems can be transformed correspondingly into the system opacity [11–13], which serves as an important information flow characteristic. Opacity, first proposed by [14], was generalized to discrete-event systems to include state-based opacity, and it could be further categorized into two types, namely, language-based [15] opacity and state-based opacity [16], which were used to satisfy different privacy needs. Compared with language-based opacity, state-based opacity will abstract confidential behaviors that need to be hidden inside a collection of secret states and can protect the information from consequent exposure. That is, under the condition that the state-based opacity is satisfied, an external adversary with malicious intentions cannot deduce beyond doubt whether the system is/was in the secret state set following the information of a given system's structure and partially observed events.

To date, the concept of state-based opacity has been extended to a large number of related notions such as initial state-based opacity [17], contemporary state-based opacity [16], K-step state-based

* Corresponding author (email: cyxia@tiangong.edu.cn)

opacity [18], infinite opacity [19, 20], probabilistic opacity [21], networked opacity [22, 23], and initial-and-final opacity [24]. With the development of formal methods, a novel algebraic state space approach based on a semi-tensor product is proposed to verify the related properties effectively [25]. Additionally, if a given system is non-opaque, then how to retrofit it through some kind of control strategy is also an important topic. To date, a variety of control methods have been presented to address the issue, including monitoring theory [26, 27], dynamic masks [28, 29], the specific event insertion mechanism [30–32], and the event editing mechanism [33].

1.1 Related work

In many cases, with the continuous gathering of intrusion observation information on the system's behavior, one can deduce that the system can be in a state of secrecy for the previous steps noted only through their knowledge of observable transition information. Thus, there is a necessity to explore various types of opaque properties such as K-step state-based opacity and infinite opacity. In 2011, Saboori and Hadjicostis [18] established the K-step state-based opacity of logical systems by constructing the delayed state estimator, and the subsequent space complexity resulting from the method was computed. Then, they [19] further analyzed the properties of the infinite state estimator and showed that the task of verifying infinite-step opacity is difficult and PSPACE-hard. After that, Yin and Lafortune [20] constructed a novel algorithm based on the separation principle of state estimation, which demonstrated that the K-step and infinite-step state-based opacity can be reached for partially observed discrete-event systems. As a further development, Yin et al. [21] proposed an innovative finite information structure to extend these two types of state-based opacity into discrete-event systems with stochastic perturbations.

Broadly speaking, the above-mentioned studies mainly focused on the logical or probabilistic system, and the time consumption or cost of complementing a transition is not specified by default. In reality, it is quite common to find that the ability to transition is inadequate and even limited, and weighted machines (WMs) are often taken as an accurate model to characterize the time consumption or cost of executing a string. Compared with the traditional automata in the study of opacity, the opacity problem of WMs takes into account more comprehensive factors, including system behavior, state transition, and cumulative weight, which will require more stringent security requirements. Therefore, much attention is paid to the modeling and analysis of WMs [34]. In specific terms, Lai et al. [35] addressed the existing state estimation problem of max-plus automata with partial event observation. Then, they discussed the verification of detectability for a special WM/unambiguous weighted machine (UWM) [36]; Zhang [37] proposed an innovative operation of concurrent composition for labeled weighted automata over monoids to categorize four classically used concepts of detectability. Recently, Lai et al. [38] studied the initial opacity problem of UWMs in depth by constructing an initial observer, which, to some extent, generalized the current study of opacity into a more advanced scenario. However, many types of opacity of UWMs still need to be studied further.

1.2 Contributions

In this study, we explore the effect of the added weighted value on the verification of finite K step and infinite-step state-based opacity for the UWMs, which extend the current result into a wider context. Based on the aforementioned studies, we further innovate by introducing the notion of multi-step state-based opacity for UWMs, which includes two cases of a K step and an infinite step, and we then generalize the bidirectional observer-based approach and algorithm to characterize the possible states, which are eavesdropped on by malicious observers through K and infinite concurrent observations, so that the restricted problem caused by weighted events may be discussed widely. The main contributions provided in this paper are summarized as follows:

- We establish the weighted state estimation with K delay and infinite delay by abstracting the possible states that the system could have through finite- or infinite-step weighted observations.
- We derive some necessary and sufficient conditions for the established existence of weighted multi-step state-based opacity by then designing the weighted observer.
- We develop the corresponding algorithms to construct the weighted bidirectional observer by then extending the traditionally rendered bidirectional observer.

The remaining sections of this paper are arranged as follows. Section 2 reviews some basic notions of algebraic structure and the system model. Section 3 then formulates the definition of multi-step state-based opacity of WMs and presents the construction process of the algorithm based on the bidirectional

observer. Subsequently, some conditions are established to verify the multi-step state-based opacity of a given UWM. Section 4 gives a comparison between WMs and unweighted ones. Section 5 presents the conclusion of this study and discusses the future direction of research.

2 Preliminaries

In this paper, let Σ^* denote all finite strings over an alphabet set Σ, and for $t \in \Sigma^*$, $|t|$ represents the cardinal number of t. $A_{(i,j)}$ and $\alpha_{(i)}$ represents the element at i-th row and j-th column of A and the i-th element of vector α, in order. In addition, the related notations of the algebraic structure and WMs are introduced as follows.

2.1 Algebraic structure

Generally, an algebraic structure is made up of quadruples $\mathbb{M} = (M, \bar{+}, \bar{\times}, 0, 1)$, such that M is a set; $\bar{+}$ and $\bar{\times}$ thereby denote two binary operational symbols on the set M; 0 and 1 are two constants in M. $\mathbb{M}$ is termed as a semi-ring if these conditions can be then satisfied: (1) $(M, \bar{+}, 0)$ is a commutative monoid; (2) $(M, \bar{\times}, 1)$ is a monoid; (3) $\bar{\times}$ satisfies the distributive laws on $\bar{+}$, i.e., $(\alpha \bar{+} \beta)\bar{\times}\gamma = (\alpha\bar{\times}\gamma)\bar{+}(\beta\bar{\times}\gamma)$, and $\gamma\bar{\times}(\alpha\bar{+}\beta) = (\gamma\bar{\times}\alpha)\bar{+}(\gamma\bar{\times}\beta)$ holds for arbitrary $\alpha, \beta, \gamma \in M$; (4) 0 is therefore the annihilator of $\bar{\times}$, i.e., $0\bar{\times}\alpha = \alpha\bar{\times}0 = 0$ for arbitrary $\alpha \in M$.

For a given semi-ring $\mathbb{M}$, $\mathbb{M}^{a\times b}$ represents the set of all $a \times b$ dimensional matrices over $\mathbb{M}$. For $X, Y \in \mathbb{M}^{a\times b}$ and $Z \in \mathbb{M}^{b\times c}$, $[X\bar{+}Y]_{(i,j)} \triangleq X_{(i,j)}\bar{+}Y_{(i,j)}$; $[X\bar{\times}Z]_{(i,j)} \triangleq \sum_{k=1}^{b} X_{(i,k)}\bar{\times}Z_{(k,j)}$. With perhaps a slight abuse of notations, $\sum$ and $\prod$ thereby represent the successive summation and multiplication, correspondingly.

2.2 Unambiguous weighted machines

A WM over a semi-ring $\mathbb{M} = (M, \bar{+}, \bar{\times}, 0, 1)$ is a quintuple $\mathcal{G} = (Q, \Sigma, \alpha, W, Q_0)$, where Q denotes the set of discrete states; Σ denotes the set of events that can be divided into two mutually exclusive subsets: the set of observable events $\Sigma_{\rm o}$ and the set of unobservable ones $\Sigma_{\rm uo}$; $\alpha \in \mathbb{M}^{1\times|Q|}$ and Q_0 are the initial weighted vector and initial states, in order; $W : \Sigma \to \mathbb{M}^{|Q|\times|Q|}$ is identified as the weighted transition function. Given an event $e \in \Sigma$, the measure of the weight between any state pair can then be expressed as $W(e) \in \mathbb{M}^{|Q|\times|Q|}$. Therefore, for any string $s = e_1e_2\cdots e_k \in \Sigma^*$, its state path from $q_0 \in Q_0$ is $\pi(s) := (q_0, e_1, q_1)(q_1, e_2, q_2)\cdots(q_{k-1}, e_k, q_k)$, and is defined as $q \overset{s}{\rightsquigarrow} q'$, the path set from q to q' with s[1)]. Naturally, for $Q_x, Q_y \subseteq Q$, $Q_x \overset{s}{\rightsquigarrow} Q_y := \bigcup_{q\in Q_x, q'\in Q_y}\{q \overset{s}{\rightsquigarrow} q'\}$, and the weighted transition can be further extended to be $W(s) = W(e_1)\bar{\times}W(e_2)\bar{\times}\cdots\bar{\times}W(e_k)$.

Definition 1. A WM $\mathcal{G} = (Q, \Sigma, \alpha, W, Q_0)$ is said to be completely unambiguous if $\forall q \in Q, \forall s \in \Sigma^*, |Q_0 \overset{s}{\rightsquigarrow} \{q\}| \leqslant 1$.

Given a UWM $\mathcal{G}$ and $s = e_1e_2\cdots e_k \in \Sigma^*$, $\mathbb{W}(\pi)$ denotes the weight of path π, defined as

$$\mathbb{W}(\pi) = \begin{cases} \alpha_{(q_0)}\bar{\times}\prod\limits_{i=1}^{k} W(e_i)_{(q_{i-1},q_i)}, & \text{if } q_0 \in Q_0, \\ \prod\limits_{i=1}^{k} W(e_i)_{(q_{i-1},q_i)}, & \text{else}, \end{cases} \tag{1}$$

where $q_i \in Q$, $e_i \in \Sigma$, and $W(e_i)_{(q_{i-1},q_i)} \neq 0$ for $i = 1, \ldots, k$. Let $\mu(s) \in \mathbb{M}^{1\times|Q|}$ then denote the weight sum of paths from q_0 with the string s, and the q_k-th element is thereby obtained by

$$\mu(s)_{(q_k)} = \sum_{\pi\in Q_0\overset{s}{\rightsquigarrow}q_k} \mathbb{W}(\pi) = \sum_{q_0\in Q_0} \alpha_{q_0}\bar{\times}W(s)_{(q_0,q_k)}. \tag{2}$$

For the path $\pi = (x_0, e_1, x_1)(x_1, e_2, x_2)\cdots(x_{k-1}, e_k, x_k)$, $\mathrm{Seq}(\pi)$ thereby denotes the weighted sequence of π, and

$$\mathrm{Seq}(\pi) = (e_1, c_1)(e_2, c_2)\cdots(e_k, c_k), \tag{3}$$

where $c_i = \mu(e_1e_2\cdots e_i)_{(q_i)}$ and $i = 1, 2, \ldots, k$.

1) $x \overset{s}{\rightsquigarrow} y$ is a null set if $s = \varepsilon$.

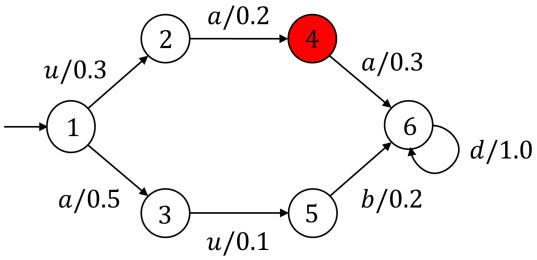

Figure 1 (Color online) UWM $\mathcal{G}$ in Example 1, where $Q = \{1, 2, 3, 4, 5, 6\}$, $\Sigma = \{u, a, b, d\}$, $Q_0 = \{1\}$, $\alpha_{(1)} = 1$, $W(u)_{(1,2)} = 0.3$, $W(a)_{(2,4)} = 0.2$, $W(a)_{(4,6)} = 0.3$, $W(d)_{(6,6)} = 1.0$, $W(a)_{(1,3)} = 0.5$, $W(u)_{(3,5)} = 0.1$, and $W(b)_{(5,6)} = 0.2$.

Finally, based on a UWM $\mathcal{G}$, we then represent the weighted language generated by $\mathcal{G}$ as

$$\mathcal{L}(\mathcal{G}) = \{\gamma \in (\Sigma \times M)^* | \exists q \in Q, \exists s \in \Sigma^*, \exists \pi \in Q_0 \overset{s}{\rightsquigarrow} \{q\} : \gamma = \mathrm{Seq}(\pi)\}. \tag{4}$$

Intuitively, $\mathcal{L}(\mathcal{G})$ includes the totality of all the weighted sequences of the directed paths labeled by string s, which starts at Q_0 and ends at $q \in Q$.

In the analysis of opaque problems, the malicious intruders can only observe the occurrence of events in Σ_o. To capture this intrusive behavior, the natural projection $P : (\Sigma \times M)^* \to (\Sigma_{\mathrm{o}} \times M)^*$ of $\mathcal{G}$ is then introduced, and can then be defined recursively as $\forall \gamma \in (\Sigma \times M)^*, \beta \in (\Sigma \times M)$,

$$P(\gamma\beta) = \begin{cases} P(\gamma)P(\beta), & \text{if } \beta \in \Sigma_{\mathrm{o}}, \\ P(\gamma), & \text{if } \beta \in \Sigma_{\mathrm{uo}}. \end{cases} \tag{5}$$

3 Multi-step state-based opacity of UWM

In this section, the weighted multi-step opacities, which include the K step and the infinite step, are generalized formally, and some verification conditions are derived. Before doing this, some assumptions are made: (1) its reversed WM (described in Subsection 3.2) is also unambiguous; (2) for any state $q \in Q$, there exists an event $e \in \Sigma$ such that $W(e)_{(q,q')} \neq 0$; and no cycle labeled by unobservable events exists. Note that condition (1) will help to construct the reversed UWM, and condition (2) implies that the system $\mathcal{G}$ cannot execute indefinitely to thereby generate weighted sequences.

3.1 Notions of multi-step state-based opacity

For any observable and weighted sequence $\gamma_{\mathrm{o}} = (e_1, c_1)(e_2, c_2) \cdots (e_n, c_n) \in P(\mathcal{L}(\mathcal{G}))$ in a UWM $\mathcal{G}$, there exists at least one weighted-sequence pair $\gamma_1\gamma_2 \in \mathcal{L}(\mathcal{G})$ so that $P(\gamma_1\gamma_2) = \gamma_{\mathrm{o}}$, and let $\hat{Q}_{-K}(\gamma_{\mathrm{o}})$ denote a set of states that are reachable from $q_0 \in Q_0$ through γ_1 within the last K-observations rendered as

$$\begin{aligned} \hat{Q}_{-K}(\gamma_{\mathrm{o}}) = \{q \in Q | \exists q_0 \in Q_0, \exists \gamma_1\gamma_2 \in \mathcal{L}(\mathcal{G}) : q_0 \overset{\gamma_1}{\rightsquigarrow} q \wedge P(\gamma_1) = (e_1, c_1) \cdots (e_{n-K}, c_{n-K}) \\ \wedge P(\gamma_2) = (e_{n-K+1}, c_{n-K+1}) \cdots (e_n, c_n)\}. \end{aligned} \tag{6}$$

Furthermore, given an observable and weighted sequence $\gamma_{\mathrm{o}}\beta_{\mathrm{o}} \in P(\mathcal{L}(\mathcal{G}))$, the resultant weighted state estimate with infinite step can be defined as

$$\hat{Q}_{-\infty}(\gamma_{\mathrm{o}}\beta_{\mathrm{o}}) := \{q \in Q | \exists q_0 \in Q_0, \exists \gamma\beta \in \mathcal{L}(\mathcal{G}) : q_0 \overset{\gamma}{\rightsquigarrow} q \wedge P(\gamma) = \gamma_{\mathrm{o}} \wedge P(\beta) = \beta_{\mathrm{o}}\}. \tag{7}$$

Example 1. Figure 1 shows a specific UWM $\mathcal{G}$, where it is assumed that $\bar{\times} = +$, $\Sigma_{\mathrm{o}} = \{a, b, d\}$. Given that $\gamma_{\mathrm{o}} = (a, 0.5)(b, 0.8) \in P(\mathcal{L}(\mathcal{G}))$, it is not hard to validate that $\hat{Q}_{-1}(\gamma_{\mathrm{o}}) = \{3, 5\}$. Indeed, there is only one path $\pi = (1, a, 3)(3, u, 5)(5, b, 6)$ where $\mathrm{Seq}(\pi) = (a, 0.5)(u, 0.6)(b, 0.8)$ and $P(\mathrm{Seq}(\pi)) = \gamma_{\mathrm{o}}$. The states $\{3, 5\}$ are thereby reachable by $(a, 0.5)$ and $(a, 0.5)(u, 0.6)$, respectively.

After this, according to the weighted state estimate mentioned above, the resultant notions of weighted multi-step state-based opacity are defined below.

Definition 2. Given a UWM $\mathcal{G}$ and a set of secret states Q_S, $\mathcal{G}$ is defined to be weighted K step state-based opacity with regard to Q_S and Σ_{o} if

$$\forall \gamma \in P(\mathcal{L}(\mathcal{G})), \forall k \leqslant \min\{K, |\gamma|\} : \hat{Q}_{-k}(\gamma) \not\subseteq Q_S. \tag{8}$$

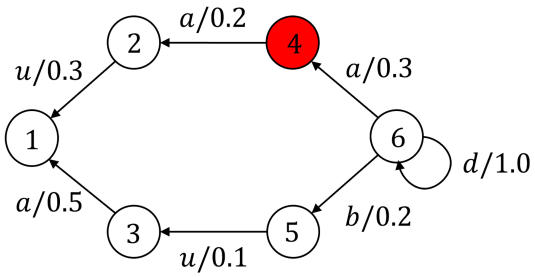

Figure 2 (Color online) Reversed machine $\mathcal{G}_{\mathrm{R}}$ for $\mathcal{G}$.

Definition 3. A UWM $\mathcal{G}$ is defined to be a weighted infinity step state-based opaque with regard to Q_S and Σ_{o} if

$$\forall \gamma_{\mathrm{o}}\beta_{\mathrm{o}} \in P(\mathcal{L}(\mathcal{G})) : \hat{Q}_{-\infty}(\gamma_{\mathrm{o}}\beta_{\mathrm{o}}) \not\subseteq Q_S. \tag{9}$$

Example 2. Recall the system $\mathcal{G}$ in Example 1 with $Q_S = \{4\}$ and $K = 2$. Given $\gamma = (a, 0.5)(a, 0.8)$, we then have $\hat{Q}_{-1}(\gamma) = \{4\}$. That is, when γ is observed, an intruder certainly infers that $\mathcal{G}$ has been in state 4. Therefore, $\mathcal{G}$ is not a 2 step or an infinity step state-based opacity.

3.2 Verification of multi-step state-based opacity

This subsection outlines the way to construct the required weighted bidirectional observer. Firstly, by reversing all transitions in $\mathcal{G}$, we can then construct the reversed machine $\mathcal{G}_{\mathrm{R}}$ over a semi-ring $\mathbb{M} = (M, \bar{+}, \bar{\times}, 0, 1)$ as a quintuple $\mathcal{G}_{\mathrm{R}} = (Q, \Sigma, \alpha_{\mathrm{R}}, W_{\mathrm{R}}, Q_{\mathrm{R},0})$, where $\alpha_{\mathrm{R}} \in \mathbb{M}^{1\times|Q|}$ is the initial weighted vector; $W_{\mathrm{R}} \in \mathbb{M}^{|Q|\times|Q|}$ is thereby the reverse weighted transition function; and $Q_{\mathrm{R},0} = Q$ denotes the initial state set.

It is worth noting that for any $q \in Q$ of $\mathcal{G}_{\mathrm{R}}$, $\alpha_{\mathrm{R}(q)} = 1$, and for $q_1, q_2 \in Q$ and $e \in \Sigma$, $W(e)_{(q_1,q_2)} = W_{\mathrm{R}}(e)_{(q_2,q_1)}$. With a path $\pi = (q_0, e_1, q_1)\cdots(q_{n-1}, e_n, q_n)$ and its sequence $\mathrm{Seq}(\pi) = (e_1, c_1)(e_2, c_2)\cdots(e_n, c_n)$ in $\mathcal{G}$, the reverse path and weighted sequence are $\pi_{\mathrm{R}} = (q_n, e_n, q_{n-1})\cdots(x_1, e_1, q_0)$ and $\mathrm{Seq}(\pi_{\mathrm{R}}) = (e_n, c_n \otimes c_{n-1})(e_{n-1}, c_n \otimes c_{n-2})\cdots(e_1, c_n)$, where $c_j \otimes c_{j-1}$ is obtained by $c_j \otimes c_{j-1} = \{c | c \bar{\times} c_{j-1} = c_j\}$.

Example 3. Considering the system $\mathcal{G}$ in Example 1, its reversed machine $\mathcal{G}_{\mathrm{R}}$ can then be constructed as shown in Figure 2 with $Q_{R,0} = Q$. The reverse weighted transition function $\mathcal{G}_{\mathrm{R}}$ is $W_{\mathrm{R}}(u)_{(2,1)} = 0.3$, $W_{\mathrm{R}}(a)_{(4,2)} = 0.2$, $W_{\mathrm{R}}(a)_{(6,4)} = 0.3$, $W_{\mathrm{R}}(d)_{(6,6)} = 1.0$, $W_{\mathrm{R}}(a)_{(3,1)} = 0.5$, $W_{\mathrm{R}}(u)_{(5,3)} = 0.1$, $W_{\mathrm{R}}(b)_{(6,5)} = 0.2$. Given a path $\pi = (1, a, 3)(3, u, 5)(5, b, 6)$ of $\mathcal{G}$, it is assumed that $\bar{\times} = +$. We then have the weighted sequence $\mathrm{Seq}(\pi) = (a, 0.5)(u, 0.6)(b, 0.8)$. Then, the reversed path is $\pi_{\mathrm{R}} = (6, b, 5)(5, u, 3)(3, a, 1)$, and its weighted sequence is found to be $\mathrm{Seq}(\pi_{\mathrm{R}}) = (b, 0.2)(u, 0.3)(a, 0.8)$.

Next, the reversed projection P_{R} of $\mathcal{G}_{\mathrm{R}}$ can also be defined as

$$P_{\mathrm{R}}\big((s, c_1)(e, c_2)\big) = \begin{cases} P_{\mathrm{R}}\big((s, c_1)\big)P_{\mathrm{R}}\big((e, c_2)\big), & \text{if } e \in \Sigma_{\mathrm{o}}, \\ P_{\mathrm{R}}((s, c_2)), & \text{if } e \in \Sigma_{\mathrm{uo}}. \end{cases} \tag{10}$$

Remark 1. Compared with the natural projection $P(s)$ of $\mathcal{G}$ defined by (5), the weight of an unobservable event is accumulated to its next observable event. When s is reversed, to keep the weights of the two directions consistent, the weight of an unobservable event is, therefore, retained in P_{R}.

Subsequently, the observers in [20] are generalized to the weighted ones by constructing Algorithm 1 as follows.

It is noteworthy that as it relates to observer design, the worst-case time complexity of Algorithm 1 increases exponentially relative to the number of states, and compared with the analysis of finite automata, the weights will bring about a high level of complexity in general. For any weighted sequence $\gamma_{\mathrm{o}} = (e_1, c_1)\cdots(e_n, c_n) \in P(\mathcal{L}(\mathcal{G}))$ (resp. $\gamma_{\mathrm{oR}} = (e_n, c_n)\cdots(e_1, c_1) \in P_{\mathrm{R}}(\mathcal{L}(\mathcal{G}_{\mathrm{R}}))$), let $\gamma_{\mathrm{o}}^{\mathrm{eq}} = (e_1, c_1)(e_2, c_2 \otimes c_1)\cdots(e_n, c_n \otimes c_{n-1})$ (resp. $\gamma_{\mathrm{oR}}^{\mathrm{eq}} = (e_n, c_n)(e_{n-1}, c_{n-1} \otimes c_n)\cdots(e_1, c_2 \otimes c_1) \in \Sigma_{\mathrm{obs,R}}^*$) denote the equivalent representation of γ_{o} in $\mathrm{Obs}(\mathcal{G})$ (resp. γ_{oR} in $\mathrm{Obs}_{\mathrm{R}}(\mathcal{G})$). Formally, $P(\mathcal{L}(\mathcal{G}))^{\mathrm{eq}} := \{\gamma \in (\Sigma_{\mathrm{o}} \times M)^* | \exists \gamma_{\mathrm{o}} \in \mathcal{L}(\mathcal{G}) : \gamma_{\mathrm{o}}^{\mathrm{eq}} = \gamma\}$ (resp. $P_{\mathrm{R}}(\mathcal{L}(\mathcal{G}_{\mathrm{R}}))^{\mathrm{eq}} := \{\gamma \in (\Sigma_{\mathrm{o}} \times M)^* | \exists \gamma_{\mathrm{o}} \in \mathcal{L}(\mathcal{G}) : \gamma_{\mathrm{oR}}^{\mathrm{eq}} = \gamma\}$). Then, according to the conclusion in [36, 38], the following lemma shows the equivalence relationships between the languages of weighted observers.

Lemma 1. Consider the constructed weighted observers, and we have

Algorithm 1 Constructing the weighted observer

Input: A UWM $\mathcal{G}=(Q,\Sigma,f,g,Q_0)$.

Output: $\mathrm{Obs}(\mathcal{G})=(Q_{\mathrm{obs}},\Sigma_{\mathrm{obs}},\delta_{\mathrm{obs}},Q_{\mathrm{obs},0})$ and $\mathrm{Obs_R}(\mathcal{G})=(Q_{\mathrm{obs,R}},\Sigma_{\mathrm{obs,R}},\delta_{\mathrm{obs,R}},Q)$.

(1) Construct a deterministic finite automaton $\mathrm{Obs}(\mathcal{G})=(Q_{\mathrm{obs}},\Sigma_{\mathrm{obs}},\delta_{\mathrm{obs}},Q_{\mathrm{obs},0})$ as follows:

- $Q_{\mathrm{obs},0}=\{Q_0\}\cup\{q\in Q|$ state q is accessible from Q_0 by the sequences in ${\Sigma_{\mathrm{uo}}}^*\}$;
- $Q_{\mathrm{obs}}\subseteq 2^Q$ is the set of states;
- Σ_{obs} is composed of all the weighted labels $(e,c)\in\Sigma_{\mathrm{o}}\times M$ so that $\exists q'\in\bar{Q},\exists q\in Q,\exists i\in\{0,1,\ldots,|Q|-1\}:W(u^ie)_{q',q}=c$, where $\bar{Q}=Q_0\cup\{q\in Q|\exists q'\in Q,\exists e\in\Sigma_{\mathrm{o}}:W(e)_{q',q}\neq 0\}$, and it can then be marked by at least one observable label;
- $\delta_{\mathrm{obs}}:Q_{\mathrm{obs}}\times\Sigma_{\mathrm{obs}}\to Q_{\mathrm{obs}}$ is the deterministic transition function, and it can be defined as

$$\delta_{\mathrm{obs}}(q_{\mathrm{obs}},(e,c))=\{q''\in Q|\exists q\in q_{\mathrm{obs}},\exists(e,c)\in\Sigma_{\mathrm{obs}}:W(u^ie)_{q,q'}=s,q''\in UR(q')\},$$

where $UR(x):=\{y\in Q|\exists x\in Q,\exists i\in\{0,1,\ldots,|Q|-1\}:W(u^i)_{(x,y)}\neq 0\}$;

(2) $\mathrm{Obs_R}(\mathcal{G})=(Q_{\mathrm{obs,R}},\Sigma_{\mathrm{obs,R}},\delta_{\mathrm{obs,R}},Q)$ can be established in the following:

- Q is the initial stare of $\mathcal{G}_{\mathrm{R}}$;
- $Q_{\mathrm{obs,R}}$ is the set of states;
- $\Sigma_{\mathrm{obs,R}}$ is made up of all weighted labels $(e,c)\in\Sigma_{\mathrm{o}}\times M$ such that $\exists q'\in Q,\exists q\in Q,\exists i\in\{0,1,\ldots,|Q|-1\}:W(eu^i)_{q',q}=c$;
- $\delta_{\mathrm{obs,R}}:Q_{\mathrm{obs,R}}\times\Sigma_{\mathrm{obs,R}}\to Q_{\mathrm{obs,R}}$ is the deterministic transition function. $\delta_{\mathrm{obs,R}}(q_{\mathrm{obs,R}},(e,c))$ is defined as

$$\delta_{\mathrm{obs,R}}(q_{\mathrm{obs,R}},(e,c))=\{q''\in Q|\exists q\in q_{\mathrm{obs,R}},\exists(e,s)\in\Sigma_{\mathrm{obs,R}}:W(eu^i)_{(q,q')}=c,q''\in UR^{-1}(q',u^i)\},$$

where $UR^{-1}(x,u^i):=\{y\in Q|\exists x\in Q,\exists i\in\{0,1,\ldots,|Q|-1\}:W(u^i)_{(y,x)}\neq 0\}$.

- $\mathcal{L}(\mathrm{Obs}(\mathcal{G}))=P(\mathcal{L}(\mathcal{G}))^{\mathrm{eq}}$.
- $\mathcal{L}(\mathrm{Obs_R}(\mathcal{G}))=P_{\mathrm{R}}(\mathcal{L}(\mathcal{G}_{\mathrm{R}}))^{\mathrm{eq}}$.

Proposition 1. Given the weighted sequences $\gamma_1,\gamma_2\in\mathcal{L}(\mathcal{G})$, $\gamma_{1\mathrm{R}},\gamma_{2\mathrm{R}}\in\mathcal{L}(\mathcal{G}_{\mathrm{R}})$, we have

- $P_{\mathrm{R}}(\gamma_{1\mathrm{R}})=P_{\mathrm{R}}(\gamma_{2\mathrm{R}})$ if and only if $P(\gamma_1)=P(\gamma_2)$;
- $q_1\overset{\gamma_1}{\rightsquigarrow}q_2$ if and only if $q_2\overset{\gamma_{1\mathrm{R}}}{\rightsquigarrow}q_1$.

This proof can be obtained directly by inducting the length of strings.

Next, we elaborate on the separation principle proposed by Yin and Lafortune in [20], which indicates that the delayed state estimates are the intersection of the states for the original observer and the reversed one.

Theorem 1. For any sequence of observation-weight pairs $\gamma_{\mathrm{o}}\beta_{\mathrm{o}}\in P(\mathcal{L}(\mathcal{G}))$, we have the following equation:

$$\hat{Q}_{-\infty}(\gamma_{\mathrm{o}}\beta_{\mathrm{o}})=\delta_{\mathrm{obs}}(Q_{\mathrm{obs},0},\gamma_{\mathrm{o}}^{\mathrm{eq}})\cap\delta_{\mathrm{obs,R}}(Q,\beta_{\mathrm{oR}}^{\mathrm{eq}}).\tag{11}$$

Proof. Given observable sequence $\gamma_{\mathrm{o}}\beta_{\mathrm{o}}$, we have

$$\begin{aligned}
&\exists q\in\hat{Q}_{-\infty}(\gamma_{\mathrm{o}}\beta_{\mathrm{o}})\\
&\quad\Leftrightarrow\exists q_0\in Q_0,\exists\gamma\beta\in\mathcal{L}(\mathcal{G}):q_0\overset{\gamma}{\rightsquigarrow}q\wedge P(\gamma)=\gamma_{\mathrm{o}}\wedge P(\beta)=\beta_{\mathrm{o}}\\
&\quad\Leftrightarrow[\exists q_0\in Q_0,\exists\gamma\in\mathcal{L}(\mathcal{G}):q_0\overset{\gamma}{\rightsquigarrow}q\wedge P(\gamma)=\gamma_{\mathrm{o}}]\wedge[\exists q'\in Q,\exists\beta\in\mathcal{L}(\mathcal{G}):q\overset{\beta}{\rightsquigarrow}q'\wedge P(\beta)=\beta_{\mathrm{o}}]\\
&\quad\Leftrightarrow[\exists q_0\in Q_0,\exists\gamma\in\mathcal{L}(\mathcal{G}):q_0\overset{\gamma}{\rightsquigarrow}q\wedge P(\gamma)=\gamma_{\mathrm{o}}]\wedge[\exists q'\in Q,\exists\beta_{\mathrm{R}}\in\mathcal{L}(\mathcal{G}_{\mathrm{R}}):q'\overset{\beta_{\mathrm{R}}}{\rightharpoonup}q\wedge P_{\mathrm{R}}(\beta_{\mathrm{R}})=\beta_{\mathrm{oR}}]\\
&\quad\Leftrightarrow q\in\delta_{\mathrm{obs}}(Q_{\mathrm{obs},0},\gamma_{\mathrm{o}}^{\mathrm{eq}})\wedge q\in\delta_{\mathrm{obs,R}}(Q,\beta_{\mathrm{oR}}^{\mathrm{eq}})\\
&\quad\Leftrightarrow q\in\delta_{\mathrm{obs}}(Q_{\mathrm{obs},0},\gamma_{\mathrm{o}}^{\mathrm{eq}})\cap\delta_{\mathrm{obs,R}}(Q,\beta_{\mathrm{oR}}^{\mathrm{eq}}).
\end{aligned}$$

Example 4. Consider the machine $\mathcal{G}$ again and its reversed machine $\mathcal{G}_{\mathrm{R}}$ as illustrated in Figures 1 and 2. According to Algorithm 1, we obtain the weighted observers shown in Figures 3 and 4.

Next, a weighted bi-direction observer (abbreviated as weighted BD-observer) is introduced, which essentially comprises the weighted observer asynchronously and its reversed weighted observer of $\mathcal{G}_{\mathrm{R}}$.

Definition 4. The weighted BD-observer is constructed by combining $\mathcal{G}_{\mathrm{obs}}$ and $\mathcal{G}_{\mathrm{obs,R}}$ as follows:

$$\mathrm{Obs_{BD}}(\mathcal{G})=(Q_{\mathrm{BD}},\Sigma_{\mathrm{BD}},\delta_{\mathrm{BD}},Q_{\mathrm{BD},0}),$$

where $Q_{\mathrm{BD}}\subseteq Q_{\mathrm{obs}}\times Q_{\mathrm{obs,R}}$ is the state set; $\Sigma_{\mathrm{BD}}=(\Sigma_{\mathrm{obs}}\times(\varepsilon,1))\cup((\varepsilon,1)\times\Sigma_{\mathrm{obs,R}})$ is the set of events; $Q_{\mathrm{BD},0}=(Q_{\mathrm{obs},0}\times Q)$ is the set of initial states; $\delta_{\mathrm{BD}}:Q_{\mathrm{BD}}\times\Sigma_{\mathrm{BD}}$ is deterministic, and defined as for $(q_1,q_2)\in Q_{\mathrm{BD}}$ and $e\in\Sigma_{\mathrm{BD}}$,

$$\delta_{\mathrm{BD}}((q_1,q_2),((e,c)\times(\varepsilon,1)))=(\delta_{\mathrm{obs}}(q_1,(e,c)),q_2),$$

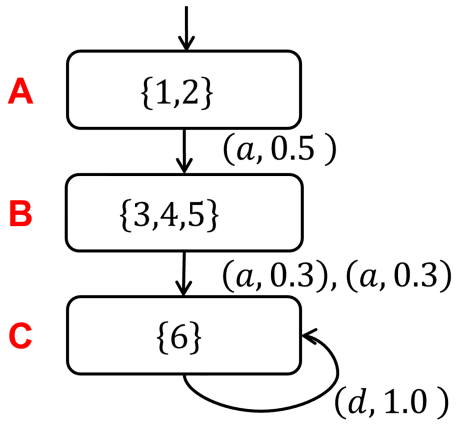

Figure 3 (Color online) Weighted observer $\mathrm{Obs}(\mathcal{G})$ in Example 4.

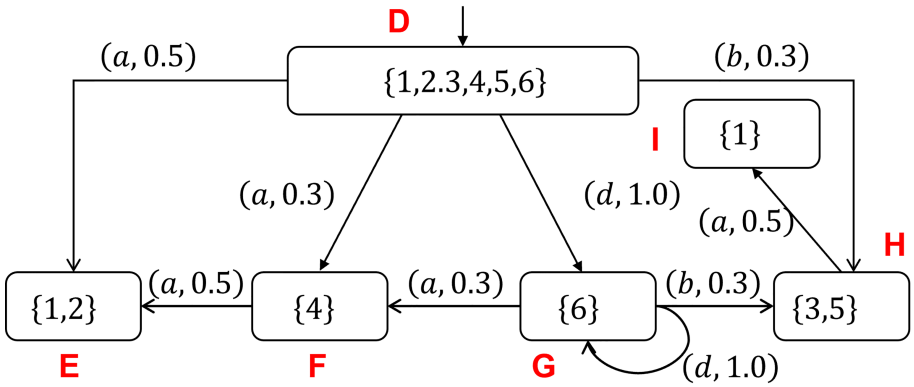

Figure 4 (Color online) Reversed observer $\mathrm{Obs}(\mathcal{G}_{\mathrm{R}})$ in Example 4.

$$\delta_{\mathrm{BD}}((q_1,q_2),((\varepsilon,1)\times(e,c)))=(q_1,\delta_{\mathrm{obs,R}}(q_2,(e,c))).$$

For the weighted sequence $\omega\in\mathcal{L}(\mathrm{Obs}_{\mathrm{BD}}(\mathcal{G}))$, the first and second elements of string ω are labeled as $\mathrm{Pair}_1(\omega)\in\Sigma^*_{\mathrm{obs}}$ and $\mathrm{Pair}_2(\omega)\in\Sigma^*_{\mathrm{obs,R}}$, respectively.

Proposition 2. For $\omega\in\mathcal{L}(\mathrm{Obs}_{\mathrm{BD}}(\mathcal{G}))$, there must exist $\gamma_1\gamma_2\in\mathcal{L}(\mathcal{G})$ that $\mathrm{Pair}_1(\omega)\mathrm{Pair}_2(\omega)_{\mathrm{R}}=[P(\gamma_1)P(\gamma_2)]^{\mathrm{eq}}$ if $\delta_{\mathrm{BD}}(Q_{\mathrm{BD},0},\omega)=(q_1,q_2)$ and $q_1\cap q_2\neq\emptyset$.

Proof. Based on $\mathrm{Obs}_{\mathrm{BD}}(\mathcal{G})$, we can obtain that $q_1=\delta_{\mathrm{obs}}(Q_{\mathrm{obs},0},\mathrm{Pair}_1(\omega))$ and $q_2=\delta_{\mathrm{obs,R}}(Q,\mathrm{Pair}_2(\omega))$. Let $q\in q_1\cap q_2$, and we have that $\exists q_0\in Q_0,\exists\gamma_1\in\mathcal{L}(\mathcal{G}):q_0\overset{\gamma_1}{\rightsquigarrow}q\wedge P(\gamma_1)^{\mathrm{eq}}=\mathrm{Pair}_1(\omega)$ and $\exists q'\in Q,\exists\gamma_2\in\mathcal{L}(\mathcal{G}_{\mathrm{R}}):q'\overset{\gamma_2}{\rightsquigarrow}q\wedge P_{\mathrm{R}}(\gamma_2)^{\mathrm{eq}}=\mathrm{Pair}_2(\omega)$. However, by Proposition 1, $q'\overset{\gamma_2}{\rightsquigarrow}q$ implies that $q\overset{\gamma_{2\mathrm{R}}}{\rightsquigarrow}q'$, and $P_{\mathrm{R}}(\gamma_2)^{\mathrm{eq}}=\mathrm{Pair}_2(\omega)$ means that $P(\gamma_2)^{\mathrm{eq}}=\mathrm{Pair}_2(\omega)_{\mathrm{R}}$. Therefore, it can be inducted that there is $\gamma_1\gamma_2\in\mathcal{L}(\mathcal{G})$ that $[P(\gamma_1)P(\gamma_2)]^{\mathrm{eq}}=\mathrm{Pair}_1(\omega)\mathrm{Pair}_2(\omega)_{\mathrm{R}}$ holds.

Similarly, for any string $\gamma_1\gamma_2\in\mathcal{L}(\mathcal{G})$, the following proposition can be obtained.

Proposition 3. For any string $\gamma_1\gamma_2\in\mathcal{L}(\mathcal{G})$, there must exist $\omega\in\mathcal{L}(\mathrm{Obs}_{\mathrm{BD}}(\mathcal{G}))$ so that $\mathrm{Pair}_1(\omega)=P(\gamma_1)^{\mathrm{eq}}$ and $\mathrm{Pair}_2(\omega)_{\mathrm{R}}=P(\gamma_2)^{\mathrm{eq}}$.

Proof. Let $P(\gamma_1)=(e_1^1,c_1^1)(e_2^1,c_2^1)\cdots(e_k^1,c_k^1)$ and $P(\gamma_2)=(e_1^2,c_1^2)(e_2^2,c_2^2)\cdots(e_n^2,c_n^2)$, and consider the following string:

$$\begin{aligned}\omega=&((e_1^1,c_1^1),(\varepsilon,1))((e_2^1,c_2^1),(\varepsilon,1))\cdots((e_k^1,c_k^1),(\varepsilon,1))((\varepsilon,1),\\&(e_n^2,c_n^2))((\varepsilon,1),(e_{n-1}^2,c_{n-1}^2))\cdots((\varepsilon,1),(e_1^2,c_1^2)).\end{aligned}\tag{12}$$

Since $P(\gamma_1)P(\gamma_2)\in P(\mathcal{L}(\mathcal{G}))$, it can be observed that $P_{\mathrm{R}}(\gamma_{2\mathrm{R}})\in P_{\mathrm{R}}(\mathcal{L}(\mathcal{G}_{\mathrm{R}}))$. Therefore, we find that $P(\gamma_1)^{\mathrm{eq}}\in\mathcal{L}(\mathrm{Obs}(\mathcal{G}))$ and $P_{\mathrm{R}}(\gamma_{2\mathrm{R}})^{\mathrm{eq}}\in\mathcal{L}(\mathrm{Obs}(\mathcal{G}_{\mathrm{R}}))$. Then, by constructing the weighted BD-observer $\mathrm{Obs}_{\mathrm{BD}}(\mathcal{G})$, we find that $\omega\in\mathcal{L}(\mathrm{Obs}_{\mathrm{BD}}(\mathcal{G}))$. Moreover, $\mathrm{Pair}_1(\omega)=P(\gamma_1)^{\mathrm{eq}}$ and $\mathrm{Pair}_2(\omega)_{\mathrm{R}}=P(\gamma_2)^{\mathrm{eq}}$ by the weighted string ω.

Starting from the above-mentioned conclusions, we provide the following theorem to verify the K-step state-based opacity.

Theorem 2. Consider a UWM $\mathcal{G}$ with the observable event set $E_{\rm o}$, the secret state set Q_S, and the weighted BD-observer $\mathrm{Obs}_{\rm BD}(\mathcal{G}) = (Q_{\rm BD}, E_{\rm BD}, \delta_{\rm BD}, Q_{\rm BD,0})$. Then, $\mathcal{G}$ owns the K step state-based opacity with regard to $E_{\rm o}$ and Q_S iff for any string $\omega \in \mathcal{L}(\mathrm{Obs}_{\rm BD}(\mathcal{G}))$ and $\delta_{\rm BD}(Q_{\rm BD,0}, \omega) = (q_1, q_2)$, we have

$$[q_1 \cap q_2 \not\subseteq Q_S \wedge q_1 \cap q_2 \neq \emptyset] \Rightarrow |\mathrm{Pair}_2(\omega)| \geqslant K. \tag{13}$$

Proof. ($\Rightarrow$) This can be proven by contradiction. We assume that there is $\omega \in \mathcal{L}(\mathrm{Obs}_{\rm BD}(\mathcal{G}))$ satisfying $\delta_{\rm BD}(Q_{\rm obs,0}, \omega) = (q_1, q_2)$, $q_1 \cap q_2 \subseteq Q_S$ and $q_1 \cap q_2 \neq \emptyset$ and $\mathrm{Pair}_2(\omega) \leqslant K$. Since $q_1 \cap q_2 \neq \emptyset$, by Proposition 3, it can be obtained directly that there is $\gamma_1\gamma_2 \in \mathcal{L}(\mathcal{G})$, so that $P(\gamma_1)^{\rm eq} = \mathrm{Pair}_1(\omega)$ and $P(\gamma_2)^{\rm eq} = \mathrm{Pair}_2(\omega)_{\rm R}$. Moreover, since $q_1 \cap q_2 = \hat{Q}_{-|P(\gamma_2)|}(P(\gamma_1)P(\gamma_2)) \subseteq Q_S$, and $|\mathrm{Pair}_2(\omega)_{\rm R}| = |P(\gamma_2)| \leqslant K$, and thus $\mathcal{G}$ does not own the K step state-based opacity since Eq. (8) is violated.

($\Leftarrow$) We prove that the contrapositive proposition is true. It is supposed that $\mathcal{G}$ does not own the K step state-based opacity, which means that there is $\gamma_1\gamma_2 \in L(\mathcal{G})$ satisfying $\hat{Q}_{-|P(\gamma_2)|}(P(\gamma_1)P(\gamma_2))$ and $|P(\gamma_2)| \leqslant K$. From Proposition 3, there is a weighted string $\omega \in \mathcal{L}(\mathrm{Obs}_{\rm BD}(\mathcal{G}))$ such that $\mathrm{Pair}_1(\omega) = P(\gamma_1)^{\rm eq}$ and $\mathrm{Pair}_2(\omega)_{\rm R} = P(\gamma_2)^{\rm eq}$. Let $\delta_{\rm BD}(Q_{\rm BD,0}, \omega) = (q_1, q_2)$, Then, we have

$$\begin{aligned} q_1 \cap q_2 &= \delta_{\rm obs}(Q_{\rm obs,0}, P(\gamma_1)) \cap \delta_{\rm obs,R}(Q, P_{\rm R}(\gamma_{2\rm R})^{\rm eq}) \\ &= \hat{Q}_{-|P(\gamma_2)|}(P(\gamma_1)P(\gamma_2)) \subseteq Q_S, \end{aligned}$$

and $|\mathrm{Pair}_2(\omega)| = |P(\gamma_2)| \leqslant K$. Meanwhile, $q_1 \cap q_2 \neq \emptyset$ because $\hat{Q}_{-|P(\gamma_2)|}(P(\gamma_1)P(\gamma_2))$ is not empty. Thus, the contrapositive proof is completed.

As a further step, the following theorem reveals that the weighted BD-observer can also be an effective tool to validate the infinite-step state-based opacity.

Theorem 3. Given a UWM $\mathcal{G}$ with the observable event set $E_{\rm o}$, the secret state set Q_S, and $\mathrm{Obs}_{\rm BD}(\mathcal{G}) = (Q_{\rm BD}, E_{\rm BD}, \delta_{\rm BD}, Q_{\rm BD,0})$, $\mathcal{G}$ is said to own the infinite-step opacity with regard to $E_{\rm o}$ and Q_S iff for any string $\omega \in \mathcal{L}(\mathrm{Obs}_{\rm BD}(\mathcal{G}))$ satisfying $\delta_{\rm BD}(Q_{\rm BD,0}, \omega) = (q_1, q_2)$, we have

$$\forall (q_1, q_2) \in Q_{\rm BD} : q_1 \cap q_2 \not\subseteq Q_S \wedge q_1 \cap q_2 \neq \emptyset. \tag{14}$$

Proof. ($\Rightarrow$) By deploying a contrapositive proposition, it is supposed that there is $(q_1, q_2) \subseteq Q_{\rm BD}$ so that $q_1 \cap q_2 \subseteq Q_S$ and $q_1 \cap q_2 \neq \emptyset$. That is, $\omega \in \mathcal{L}(\mathrm{Obs}_{\rm BD}(\mathcal{G}))$ exists which leads to $(q_1, q_2) \subseteq Q_{\rm BD}$, and $\delta_{\rm BD}(Q_{\rm obs,0}, \omega) = (q_1, q_2)$. Since $q_1 \cap q_2 \neq \emptyset$, according to Proposition 3, there is $\gamma_1\gamma_2 \in \mathcal{L}(\mathcal{G})$ that satisfies $[P(\gamma_1)P(\gamma_2)]^{\rm eq} = \mathrm{Pair}_1(\omega)\mathrm{Pair}_2(\omega)_{\rm R} \in P(\mathcal{L}(\mathcal{G}))^{\rm eq}$.

By constructing the weighted BD-observer $\mathrm{Obs}_{\rm BD}(\mathcal{G})$, it can be obtained that $q_1 = \delta_{\rm obs}(Q_{\rm obs,0}, \mathrm{Pair}_1(\omega))$ and $q_2 = \delta_{\rm obs}(Q, \mathrm{Pair}_2(\omega))$. For $\mathrm{Pair}_1(s)\mathrm{Pair}_2(s)_{\rm R}$, we have

$$\begin{aligned} &\hat{Q}_{-P(\gamma_2)}(P(\gamma_1)P(\gamma_2)) \\ &\quad = \delta_{\rm obs}(Q_{\rm obs,0}, P(\gamma_1)^{\rm eq}) \cap \delta_{\rm obs,R}(Q, P(\gamma_2)^{\rm eq}) \\ &\quad = \delta_{\rm obs}(Q_{\rm obs,0}, \mathrm{Pair}_1(\omega)) \cap \delta_{\rm obs,R}(Q, \mathrm{Pair}_2(\omega)) \\ &\quad = q_1 \cap q_2 \subseteq Q_S. \end{aligned}$$

Therefore, $\mathcal{G}$ does not own the infinite-step state-based opacity since Eq. (7) is violated.

($\Leftarrow$) It is hypothesized that $\mathcal{G}$ is not infinite-step opaque, which implies that there is $\gamma_1\gamma_2 \in L(\mathcal{G})$ satisfying $\hat{Q}_{-|P(\gamma_2)|}(P(\gamma_1)P(\gamma_2)) \subseteq Q_S$. From Proposition 3, there is $\omega \in \mathcal{L}(\mathrm{Obs}_{\rm BD}(\mathcal{G}))$ so that $\mathrm{Pair}_1(\omega) = P(\gamma_1)^{\rm eq}$ and $\mathrm{Pair}_2(\omega)_{\rm R} = P(\gamma_2)^{\rm eq}$. Let $\delta_{\rm BD}(Q_{\rm BD,0}, \omega) = (q_1, q_2)$, and we have

$$\begin{aligned} &\hat{Q}_{-|P(\gamma_2)|}(P(\gamma_1)P(\gamma_2)) \\ &\quad = \delta_{\rm obs}(Q_{\rm obs,0}, \mathrm{Pair}_1(\omega)) \cap \delta_{\rm obs,R}(Q, \mathrm{Pair}_2(\omega)) \\ &\quad = q_1 \cap q_2 \subseteq Q_S. \end{aligned}$$

Thus, the conclusion is proven.

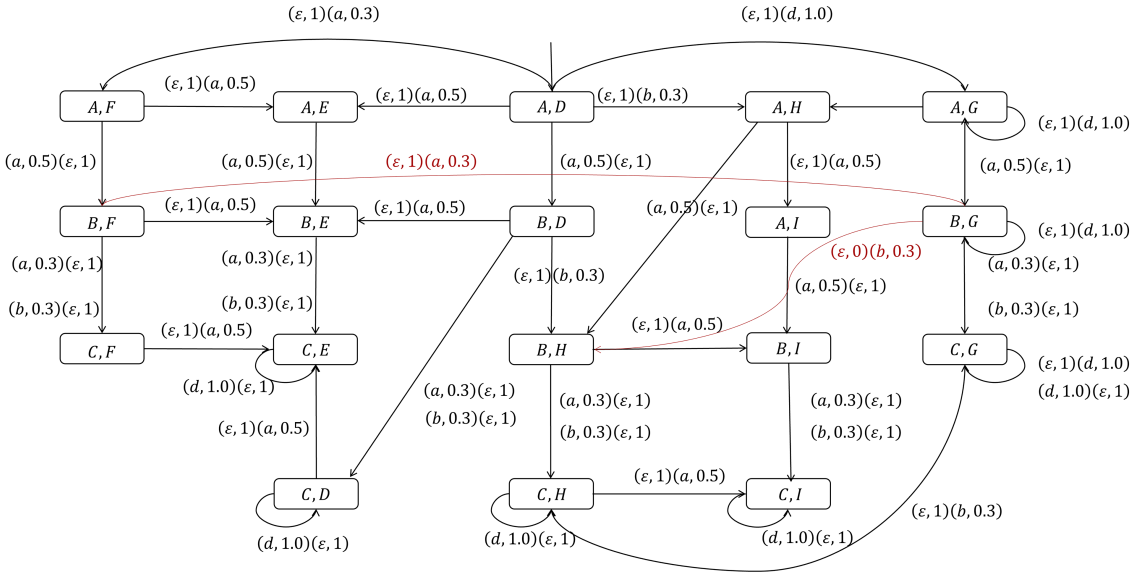

Figure 5 (Color online) Weighted BD-observer $\mathrm{Obs}_{\mathrm{BD}}(\mathcal{G})$ of machine $\mathcal{G}$ is depicted in Figure 1.

Table 1 Various models of logical machine $\mathcal{G}'$

Machine	Symbol
The logical machine	$\mathcal{G}' = (Q, \Sigma', \delta, Q_0)$
The reversed machine	$\mathcal{G}'_{\mathrm{R}} = (Q, \Sigma', \delta_{\mathrm{R}}, Q)$
The observer	$\mathrm{Obs}(\mathcal{G}') = (Q'_{\mathrm{obs}}, \Sigma'_{\mathrm{obs}}, \delta'_{\mathrm{obs}}, Q_{\mathrm{obs},0})$
The reversed observer	$\mathrm{Obs}_{\mathrm{R}}(\mathcal{G}') = (Q'_{\mathrm{obs}}, \Sigma'_{\mathrm{obs}}, \delta'_{\mathrm{obs,R}}, Q)$
The BD-observer	$\mathrm{Obs}_{\mathrm{BD}}(\mathcal{G}') = (Q'_{\mathrm{BD}}, \Sigma'_{\mathrm{BD}}, \delta'_{\mathrm{BD}}, Q_{\mathrm{BD},0})$

Intuitively, for any state in the weighted bidirectional observer, if the state is not empty for the intersection of the first and second components, this means that there is an observable sequence in the weighted system. It is more commonly understood that when the intersection of the first and second components of the weighted bidirectional observer state is not empty, the corresponding string can always be found in the original system.

Example 5. For $\mathcal{G}$ in Figure 1, the corresponding BD-observer $\mathrm{Obs}_{\mathrm{BD}}(\mathcal{G})$ is constructed as shown in Figure 5. It can be found that there is $(B, F) = (\{3, 4, 5\}, \{4\})$, which is reached by $((a, 0.5)(\varepsilon, 1))((\varepsilon, 1)(a, 0.3))$. Since $\{3, 4, 5\} \cap \{4\} \subseteq Q_S$, $\mathcal{G}$ is verified to be not 1-step opaque.

4 Opaque comparison between WMs and unweighted ones

In this section, we elaborate on the difference between WMs and their underlying logical ones and explain what may cause the difference between the two structures.

First, as shown in Table 1, let us define the specification of its underlying logical machine $\mathcal{G}'$ of a WM $\mathcal{G} = (Q, \Sigma, \alpha, W, Q_0)$.

Using the above example, it is not difficult to find that the weighted transition may alter the previously known cognition. $\mathrm{Lab}(\gamma)$ represents the string composed of the first component of the weighted sequence γ. The following proposition describes a state-shunting phenomenon in WMs.

Theorem 4. For any sequence $s \in \mathcal{L}(\mathrm{Obs}_{\mathrm{BD}}(\mathcal{G}'))$, we find that $\delta'_{\mathrm{BD}}(Q_{\mathrm{BD},0}, s) = (q_1, q_2)$ and

$$q_1 \cap q_2 = \{q \in 2^Q | \exists \gamma \in \mathcal{L}(\mathrm{Obs}_{\mathrm{BD}}(\mathcal{G})) : \delta_{\mathrm{BD}}(Q_{\mathrm{BD},0}, \gamma) = (q'_1, q'_2) \wedge q = q'_1 \cap q'_2 \\ \wedge \mathrm{Pair}_{11}(\gamma) = \mathrm{Pair}_1(s) \wedge \mathrm{Pair}_{21}(\gamma) = \mathrm{Pair}_2(s)\},$$

where $\mathrm{Pair}_{11}(\gamma)$ and $\mathrm{Pair}_{21}(\gamma)$ denote the label event of the first and second part for the identity element composing string γ, respectively.

Proof. WMs can recognize the same event table with different weights as distinct event-weighted pairs. Let $s' \in P^{-1}(s)$, and we have the relation between reachable sets of WMs and their underlying logical

ones as

$$\begin{aligned}\delta(q_0,s)=\{q\in Q|\exists s'\in\mathcal{L}(\mathcal{G}'):[\alpha_{(q_0)}\times W(\gamma')]_{(q_0,q)}\neq 0\}\\ \Rightarrow\delta'_{\rm obs}(q_0,P(\gamma))=\{q\in 2^Q|\exists\gamma\in\mathcal{L}(\mathrm{Obs}(\mathcal{G})):q_0\overset{\gamma}{\rightsquigarrow}q\}.\end{aligned}$$

It is similar to the reverse WMs. According to the construction algorithm of the BD-observer, the observer of $\mathcal{G}$ and the corresponding observer of $\mathcal{G}_{\rm R}$ are generated essentially and asynchronously. There must be a sequence $s\in\mathcal{L}(\mathrm{Obs}_{\rm BD}(\mathcal{G}'))$ of the logical BD-observer, such that $\delta'_{\rm BD}(Q_{\rm BD,0},s)=(q_1,q_2)$ and

$$\begin{aligned}q_1\cap q_2=&\{q\in Q|\delta(q_0,\mathrm{Pair}_1(s))\cap\delta(Q,\mathrm{Pair}_2(s))\}\\ =&\{q\in Q|\exists\beta\in\mathcal{L}(\mathcal{G}),\exists t\in\mathcal{L}(\mathcal{G}_{\rm R}):\mathrm{Lab}(\beta)=\mathrm{Pair}_1(s),\mathrm{Lab}(t)=\mathrm{Pair}_2(s),\delta_{\rm obs}(q_0,s)=q'_1,\\ &\delta_{\rm obs,R}(Q,t)=q'_2,q=q'_1\cap q'_2\}\\ =&\{q\in 2^Q|\exists\gamma\in\mathcal{L}(\mathrm{Obs}_{\rm BD}(\mathcal{G})):\delta_{\rm BD}(Q_{\rm BD,0},\gamma)=(q'_1,q'_2)\\ &\wedge q=q'_1\cap q'_2\wedge\mathrm{Pair}_{11}(\gamma)=\mathrm{Pair}_1(s)\wedge\mathrm{Pair}_{21}(\gamma)=\mathrm{Pair}_2(s)\}.\end{aligned}$$

5 Conclusion

This paper presents the concept of multi-step state-based opacity of UWMs, which contain two kinds of opacity with K-step and infinite-step delay. Further, it extends the previously known results and describes them qualitatively. We establish the weighted state estimation with K (infinite)-step delay and derive the conditions for the existence of two classes of opacity properties by constructing the weighted bidirectional observer. Finally, some numerical examples are provided to verify that the method is correct and effective.

Future work could be conducted along the following two lines. On the one hand, we could extend the current approach to a more general class of weighted automata, such as the polynomial ambiguous WM [39]. On the other hand, we can generalize our result with a novel algebraic framework [40–42], that is, illustrate the current notation and results by using the matrix semi-tensor product, which is also an interesting topic. Besides, it is an important topic in the current research field to deal with the limitations in the study of infinite-step and K-step opacity in WMs.

Acknowledgements This work was supported by National Natural Science Foundation of China (Grant Nos. 62203328, 62173247), Tianjin Natural Science Foundation of China (Grant Nos. 21JCQNJC00840, 22JCZDJC00550), and National Key Research and Development Program of China (Grant No. 2018AAA0101603).

References

1 Wang S L, Li H T. Aggregation method to reachability and optimal control of large-size Boolean control networks. Sci China Inf Sci, 2023, 66: 179202
2 Curzon J, Kosa T A, Akalu R, et al. Privacy and artificial intelligence. IEEE Trans Artif Intell, 2021, 2: 96–108
3 Li Z T, Guo Y Q, Gui W H. Asymptotical stability of continuous-time probabilistic logic networks based on transition rate. Sci China Inf Sci, 2023, 66: 132201
4 Zong G, Yang D, Lam J, et al. Fault-tolerant control of switched LPV systems: a bumpless transfer approach. IEEE ASME Trans Mechatron, 2022, 27: 1436–1446
5 Li S, Ahn C K, Guo J, et al. Global output feedback sampled-data stabilization of a class of switched nonlinear systems in the p-normal form. IEEE Trans Syst Man Cybern Syst, 2021, 51: 1075–1084
6 Zhang Z P, Xia C Y, Fu J, et al. Initial-state observability of mealy-based finite-state machine with nondeterministic output functions. IEEE Trans Syst Man Cybern Syst, 2022, 52: 6396–6405
7 Zhou Y R, Chen Z Q, Liu Z X, et al. Strong fault prognosability of partially-observed discrete event systems. Sci China Inf Sci, 2023, 66: 139202
8 Chen H, Zong G, Gao F, et al. Probabilistic event-triggered policy for extended dissipative finite-time control of MJSs under cyber-attacks and actuator failures. IEEE Trans Automat Contr, 2023, 68: 7803–7810
9 Zhao G, Li H. Robustness analysis of logical networks and its application in infinite systems. J Franklin Inst, 2020, 357: 2882–2891
10 Zou W, Ahn C K, Xiang Z. Analysis on existence of compact set in neural network control for nonlinear systems. Automatica, 2020, 120: 109155
11 An L, Yang G H. Opacity enforcement for confidential robust control in linear cyber-physical systems. IEEE Trans Automat Contr, 2020, 65: 1234–1241
12 Badouel E, Bednarczyk M, Borzyszkowski A, et al. Concurrent secrets. Discrete Event Dyn Syst, 2007, 17: 425–446
13 Tong Y, Li Z W, Seatzu C, et al. Verification of state-based opacity using Petri nets. IEEE Trans Automat Contr, 2016, 62: 2823–2837
14 Mazare'E L. Using unification for opacity properties. In: Proceedings of the Workshop on Issues in the Theory of Security, 2004. 165–176
15 Lin F. Opacity of discrete event systems and its applications. Automatica, 2011, 47: 496–503

16 Saboori A, Hadjicostis C N. Notions of security and opacity in discrete event systems. In: Proceedings of the 46th IEEE Conference on Decision and Control, 2007. 5056–5061
17 Saboori A, Hadjicostis C N. Verification of initial-state opacity in security applications of discrete event systems. Inf Sci, 2013, 246: 115–132
18 Saboori A, Hadjicostis C N. Verification of K-step opacity and analysis of its complexity. IEEE Trans Automat Sci Eng, 2011, 8: 549–559
19 Saboori A, Hadjicostis C N. Verification of infinite-step opacity and complexity considerations. IEEE Trans Automat Contr, 2012, 57: 1265–1269
20 Yin X, Lafortune S. A new approach for the verification of infinite-step and k-step opacity using two-way observers. Automatica, 2017, 80: 162–171
21 Yin X, Li Z J, Wang W L, et al. Infinite-step opacity and k-step opacity of stochastic discrete-event systems. Automatica, 2019, 99: 266–274
22 Zhang Z P, Shu S L, Xia C Y. Networked opacity for finite state machine with bounded communication delays. Inf Sci, 2021, 572: 57–66
23 Yang J K, Deng W L, Qiu D W, et al. Opacity of networked discrete event systems. Inf Sci, 2021, 543: 328–344
24 Wu Y C, Lafortune S. Comparative analysis of related notions of opacity in centralized and coordinated architectures. Discrete Event Dyn Syst, 2013, 23: 307–339
25 Wang B, Feng J, Li H, et al. On detectability of Boolean control networks. Nonlinear Anal-Hybrid Syst, 2020, 36: 100859
26 Dubreil J, Darondeau P, Marchand H. Supervisory control for opacity. IEEE Trans Automat Contr, 2010, 55: 1089–1100
27 Yin X, Lafortune S. A uniform approach for synthesizing property-enforcing supervisors for partially-observed discrete-event systems. IEEE Trans Automat Contr, 2016, 61: 2140–2154
28 Cassez F, Dubreil J, Marchand H. Synthesis of opaque systems with static and dynamic masks. Form Methods Syst Des, 2012, 40: 88–115
29 Yin X, Li S. Synthesis of dynamic masks for infinite-step opacity. IEEE Trans Automat Contr, 2020, 65: 1429–1441
30 Ji Y D, Wu Y C, Lafortune S. Enforcement of opacity by public and private insertion functions. Automatica, 2018, 93: 369–378
31 Wu Y C, Lafortune S. Synthesis of insertion functions for enforcement of opacity security properties. Automatica, 2014, 50: 1336–1348
32 Wu B, Dai J, Lin H. Synthesis of insertion functions to enforce decentralized and joint opacity properties of discrete-event systems. In: Proceedings of Annual American Control Conference (ACC), 2018. 3026–3031
33 Ji Y D, Yin X, Lafortune S. Opacity enforcement using nondeterministic publicly known edit functions. IEEE Trans Automat Contr, 2019, 64: 4369–4376
34 Buchholz P, Kemper P. Model checking for a class of weighted automata. Discrete Event Dyn Syst, 2010, 20: 103–137
35 Lai A, Lahaye S, Giua A. State estimation of max-plus automata with unobservable events. Automatica, 2019, 105: 36–42
36 Lai A W, Lahaye S, Giua A. Verification of detectability for unambiguous weighted automata. IEEE Trans Automat Contr, 2020, 66: 1437–1444
37 Zhang K Z. Detectability of labeled weighted automata over monoids. Discrete Event Dyn Syst, 2022, 32: 435–494
38 Lai A W, Lahaye S, Li Z W. Initial-state detectability and initial-state opacity of unambiguous weighted automata. Automatica, 2021, 127: 109490
39 Lai A W, Lahaye S, Komenda J. Observer construction for polynomially ambiguous max-plus automata. IEEE Trans Automat Contr, 2022, 67: 1582–1588
40 Yang X, Li H. Stability analysis of probabilistic Boolean networks with switching discrete probability distribution. IEEE Trans Automat Contr, 2023, 68: 2506–2512
41 Zhao G, Wang Y, Li H. A matrix approach to the modeling and analysis of networked evolutionary games with time delays. IEEE CAA J Autom Sin, 2016, 5: 818–826
42 Yan Y Y, Cheng D Z, Feng J-E, et al. Survey on applications of algebraic state space theory of logical systems to finite state machines. Sci China Inf Sci, 2023, 66: 111201