Yin Tong, Hao Lan, Carla Seatzu

Verification of **K**-step and infinite-step opacity of bounded labeled Petri nets

Automatica

Volume 140, 2022, 110221

The publisher's version is available at:

https://doi.org/10.1016/j.automatica.2022.110221

Verification of K-Step and Infinite-Step Opacity of Bounded Labeled Petri Nets ⋆

Yin Tong [a], Hao Lan [b], Carla Seatzu [c]

[a] *School of Information Science and Technology, Southwest Jiaotong University, Chengdu 611756, China*

[b] *Huawei Technologies Co., Ltd, Chengdu 611731, China*

[c] *Department of Electrical and Electronic Engineering, University of Cagliari, Cagliari 09123, Italy*

Abstract

Opacity is an important information security property. Given a discrete event system, a set of secret states, and an intruder who observes the system evolution through an observation mask, the system is said to be K-step opaque if the intruder is not able to ascertain that the system is or was in a secret state at some time within K steps, namely within the observation of K events. If the intruder is never able to ascertain that the system is or was in a secret state at any time, the system is said to be infinite-step opaque. This work aims at verifying the two opacity properties when the discrete event system is modeled as a bounded labeled Petri net. Using the notion of basis reachability graph, new approaches are proposed to check K-step opacity and infinite-step opacity. The proposed approaches are shown to be more efficient than the standard methods based on the reachability graph.

Key words: Discrete event systems, Petri nets, K-step opacity, Infinite-step opacity.

1 Introduction

Motivated by the concern about security and privacy in cyber-physical systems, opacity has been extensively investigated in the past years (Jacob et al., 2016). Opacity describes the ability of a system to hide a secret behavior to external intruders. Different notions of opacity have been defined for discrete event systems (DESs), including language-based opacity, current-state opacity, initial-state opacity, K-step opacity, infinite-step opacity, etc. In this paper, we focus on *K-step opacity* and *infinite-step opacity*. Given a set of secret states, a system is said to be *K-step opaque* if the intruder is not able to infer that the system is or was in a secret state for any instant within K steps, namely within the observation of K events. Analogously, a system is said to be *infinite-step opaque* if the intruder is not able, and will never be able, to infer if the system is in a secret state, or if it was in a secret state at any time instant.

The notion of K-step opacity was first defined by Saboori and Hadjicostis (2007) in the nondeterministic finite automaton (NFA) framework assuming that the events are partially observable. Then Saboori and Hadjicostis (2009) characterized the notion of infinite-step opacity as an extension of K-step opacity. In Saboori and Hadjicostis (2011), it is shown that given an NFA, its infinite-step opacity can be verified by constructing an observer of the system and a bank of estimators whose elements are the pairs of possible initial state and current state, and the verification of infinite-step opacity is proved to be PSPACE-hard. In Yin and Lafortune (2017), approaches are proposed to check both K-step opacity and infinite-step opacity. Such approaches are based on the construction of a new structure, called *two-way observer* (TW-observer) built through the synchronization of two observers: the observer of the given automaton and the observer of its reversed automaton, called the *initial-state estimator*. Yin and Lafortune (2017) show that the complexity of verifying K-step opacity and infinite-step opacity is exponential in the number of states of the system. In our recent work Lan et al. (2020a), we prove that the two opacity properties can be verified more efficiently by only analyzing the states of the observer and the initial-state estimator, rather than constructing the TW-observer.

Petri nets have been extensively used to model and check different types of opacity, e.g., initial-state opacity (Tong et al., 2017), current-state opacity (Tong et al., 2017; Cong et al., 2018), and language-based opacity (Tong et al., 2016). Moreover, these problems can be solved in the framework of bounded Petri nets using structural analysis and algebraic techniques. However, to the best

⋆ Corresponding author: Yin Tong. This work has been supported by the National Natural Science Foundation of China under Grant No. 61803317, and Project RASSR05871 MOSIMA financed by Region Sardinia, FSC 2014-2020, annuity 2017, Subject area 3, Action Line 3.1.

Email addresses: yintong@swjtu.edu.cn (Yin Tong), haolan8@huawei.com (Hao Lan), seatzu@diee.unica.it (Carla Seatzu).

of our knowledge, K-step opacity and infinite-step opacity have never been studied in the framework of Petri nets.

In this paper, we focus on the formalization and verification of K-step opacity and infinite-step opacity in bounded labeled Petri net systems. The secret is defined as a subset of the reachable markings. The proposed verification approaches are based on the notion of *basis reachability graph* (BRG) that summarizes in a compact form the information contained in the *reachability graph* (RG). Each node in the BRG represents not only the marking associated with it, but also the markings that can be reached from such marking through unobservable transitions. In addition, only markings (called *basis markings*) reachable through observable transitions and the unobservable transition sequences whose firing is necessary to enable them, are enumerated. As a consequence, the size of the BRG is usually smaller than that of the RG, thus the BRG has been efficiently used to verify some opacity properties (Tong et al., 2017). In this paper, under appropriate assumptions, necessary and sufficient conditions for K-step opacity and infinite-step opacity based on the BRG are presented. More precisely, if for any basis marking in the secret, the markings reachable from it through unobservable transitions are also contained in the secret, then the BRG can be used to verify K-step opacity and infinite-step opacity. If such an assumption does not hold, an *extended BRG* (EBRG) is proposed to verify the two opacity properties. Based on the BRG/EBRG of the LPN system, we prove that K-step opacity and infinite-step opacity can be verified by checking the intersections of the states in the observer and the initial-state estimator of the BRG/EBRG. The contributions of the paper can be summarized as follows.

- We investigate the advantages of Petri nets over automata in the verification of K-step and infinite-step opacity. It is shown that under appropriate assumptions, instead of using the RG (i.e., enumerating the whole state space of the system), the BRG can be used to verifying both K-step and infinite-step opacity.
- If the assumptions are not satisfied, a few markings besides the basis markings need to be enumerated. A new structure, called extended BRG (EBRG), is proposed to verify the two opacity properties in the most general case.
- K-step opacity and infinite-step opacity can be checked by analyzing the states in the observer and the initial-state estimator of the BRG/EBRG.

Note that in Lan et al. (2020b) we presented some preliminary results on the formalization and verification of infinite-step opacity in labeled Petri nets, but using a different approach based on language containment.

2 Preliminaries and Background

In this section, we recall the formalisms used in the paper and some results on state estimation in labeled Petri nets.

2.1 Automata

A *nondeterministic finite (state) automaton* (NFA) is a 4-tuple $A = (X, E, f, X_0)$, where X is a finite *set of states*, E is a finite *set of events*, $f : X \times E \to 2^X$ is a (partial) *transition relation*, and $X_0 \subseteq X$ is a set of *initial states*. The transition relation f can be extended to $f : X \times E^* \to 2^X$ in a standard manner. Given an initial state $x_0 \in X_0$ and an event sequence $w \in E^*$, if $f(x_0, w) \neq \emptyset$, then we say that w is defined at x_0 and it is denoted as $f(x_0, w)!$. The generated language of A is $\mathcal{L}(A) = \{w \in E^* | \exists x \in X_0 : f(x, w)!\}$. The *reversed automaton* $A_r = (X, E, f_r, X)$ of A is the automaton obtained by reversing all arcs in A and taking all the states in A as initial states.

Given an NFA, its equivalent DFA, called *observer*, can be constructed following the procedure in Section 2.3.4 of Cassandras and Lafortune (2008). Each state of the observer is a subset of X in which the NFA may be after a certain event sequence has occurred. The complexity of computing the observer is $\mathcal{O}(2^n)$, where n is the number of states of the NFA A. The observer of the reversed automaton A_r is also called the *initial-state estimator* of A (Wu and Lafortune, 2013).

2.2 Petri nets

A *Petri net* is a structure $N = (P, T, Pre, Post)$, where P is a set of m *places*, T is a set of n *transitions*, $Pre : P \times T \to \mathbb{N}$ and $Post : P \times T \to \mathbb{N}$ are the *pre-* and *post-incidence functions* that specify the arcs directed from places to transitions, and from transitions to places, respectively. The *incidence matrix* of a net is denoted by $C = Post - Pre$. A Petri net is *acyclic* if there are no oriented cycles.

A *marking* is a vector $M : P \to \mathbb{N}$ that assigns to each place a non-negative integer number of tokens. The marking of place p is denoted by $M(p)$. A *Petri net system* $\langle N, M_0 \rangle$ is a net N with *initial marking* M_0.

A transition t is *enabled* at marking M if $M \geq Pre(\cdot, t)$ and may fire yielding a new marking $M' = M + C(\cdot, t)$. We write $M[\sigma\rangle$ to denote that the sequence of transitions $\sigma = t_{j1} \cdots t_{jk}$ is enabled at M, and $M[\sigma\rangle M'$ to denote that the firing of σ yields M'. The set of all enabled transition sequences in N from marking M is $L(N, M) = \{\sigma \in T^* | M[\sigma\rangle\}$. Given a transition sequence $\sigma \in T^*$, the function $\pi : T^* \to \mathbb{N}^n$ associates with σ the firing vector $y = \pi(\sigma) \in \mathbb{N}^n$, i.e., $y(t) = k$ if transition t appears k times in σ. The *length* of σ is denoted by $|\sigma|$.

A marking M is *reachable* in $\langle N, M_0 \rangle$ if there exists a transition sequence σ such that $M_0[\sigma\rangle M$. The set of all markings reachable from M_0 defines the *reachability set* $R(N, M_0)$ of $\langle N, M_0 \rangle$. A Petri net system is *bounded* if there exists a non-negative integer $k \in \mathbb{N}$ such that for any place $p \in P$ and any reachable marking $M \in R(N, M_0)$, $M(p) \leq k$ holds.

A *labeled Petri net* (LPN) system is a 4-tuple $G = (N, M_0, E, \ell)$, where $\langle N, M_0 \rangle$ is a Petri net system, E is

the *alphabet* (a set of labels) and $\ell : T \to E \cup \{\varepsilon\}$ is the *labeling function* that assigns to each transition $t \in T$ either a symbol from E or the empty word ε. Therefore, the set of transitions can be partitioned into two disjoint sets $T = T_o \dot{\cup} T_u$, where $T_o = \{t \in T | \ell(t) \in E\}$ is the set of observable transitions and $T_u = T \setminus T_o = \{t \in T | \ell(t) = \varepsilon\}$ is the set of unobservable transitions. We denote $n_o = |T_o|$ (resp. $n_u = |T_u|$) the number of observable (resp. unobservable) transitions. Given a marking $M \in R(N, M_0)$, we define $U(M) = \{M' \in \mathbb{N}^m | M[\sigma_u\rangle M', \sigma_u \in T_u^*\}$ its *unobservable reach*, namely, the set of markings reachable from M through unobservable transitions. Given a subset of markings $Y \subseteq R(N, M_0)$, $U(Y) = \bigcup_{M \in Y} U(M)$.

The labeling function can be extended to transition sequences $\ell : T^* \to E^*$ as $\ell(\sigma t) = \ell(\sigma)\ell(t)$ with $\sigma \in T^*$ and $t \in T$. The *language generated by* G is $\mathcal{L}(G) = \{w \in E^* | \exists \sigma \in L(N, M_0) : w = \ell(\sigma)\}$. It is the set of words that can be observed by the intruder. A word $w \in \mathcal{L}(G)$ is called an *observation*. We denote $\mathcal{C}(w) = \{M \in \mathbb{N}^m | \exists \sigma \in L(N, M_0) : M_0[\sigma\rangle M, \ell(\sigma) = w\}$ the set of markings *consistent* with the observation w.

Given an LPN system $G = (N, M_0, E, \ell)$, the *T_u-induced subnet* $N_u = (P, T_u, Pre_u, Post_u)$ of N, is the net that results by removing all transitions in $T \setminus T_u$ from N, where Pre_u and $Post_u$ are the restrictions of Pre, $Post$ to T_u, respectively. The incidence matrix of the T_u-induced subnet is denoted by $C_u = Post_u - Pre_u$.

2.3 Basis markings

In this subsection, we recall the definitions of basis markings and basis reachability graph. For more details we refer to Ma et al. (2017).

Definition 1 *Given a marking M and an observable transition $t \in T_o$, we define*
$\Sigma(M, t) = \{\sigma \in T_u^* | M[\sigma\rangle M', M' \geq Pre(\cdot, t)\}$
the set of explanations *of t at M, i.e., the set of unobservable transition sequences whose firing at M makes t enabled, and*
$Y(M, t) = \{y_u \in \mathbb{N}^{n_u} | \exists \sigma \in \Sigma(M, t) : y_u = \pi(\sigma)\}$
the corresponding set of e-vectors*, i.e., the set of firing vectors associated with unobservable transition sequences in $\Sigma(M, t)$.* $\diamond$

After firing any unobservable transition sequence in $\Sigma(M, t)$ at M, the transition t is enabled. To provide a compact representation of the reachability set, we are interested in finding the explanations whose firing vector is minimal.

Definition 2 *Given a marking M and an observable transition $t \in T_o$, we define*
$\Sigma_{min}(M, t) = \{\sigma \in \Sigma(M, t) | \nexists \sigma' \in \Sigma(M, t) : \pi(\sigma') \lneqq \pi(\sigma)\}$
the set of minimal explanations *of t at M, and*
$Y_{min}(M, t) = \{y_u \in \mathbb{N}^{n_u} | \exists \sigma \in \Sigma_{min}(M, t) : y_u = \pi(\sigma)\}$
the corresponding set of minimal e-vectors. $\diamond$

Under different assumptions, there are different approaches to calculate $Y_{min}(M, t)$ (e.g., Jiroveanu and Boel (2004), and Boel and Jiroveanu (2004)). In particular, Cabasino et al. (2011) present an approach that only requires algebraic manipulations when the T_u-induced subnet is acyclic.

Definition 3 *Given an LPN system $G = (N, M_0, E, \ell)$, its* basis marking set *$\mathcal{M}_b$ is defined as follows:*

- $M_0 \in \mathcal{M}_b$;
- *if $M \in \mathcal{M}_b$, then $\forall t \in T_o, y_u \in Y_{min}(M, t)$,*
$$M + C(\cdot, t) + C_u \cdot y_u \in \mathcal{M}_b.$$

A marking $M_b \in \mathcal{M}_b$ is called a basis marking of G. $\diamond$

The set of basis markings contains the initial marking and all other markings that are reachable from a basis marking M by firing a transition sequence $\sigma_u t$, where $t \in T_o$ and $\sigma_u \in \Sigma_{min}(M, t)$. By Definition 3, basis markings can be recursively computed from the initial marking if the T_u-induced subnet is acyclic. Note that since $y_u \in Y_{min}(M, t)$, t is enabled at some marking in $U(M)$. Clearly, $\mathcal{M}_b \subseteq R(N, M_0)$ and in practical cases the number of basis markings is smaller than the number of reachable markings (Tong et al., 2017; Ma et al., 2017; Cabasino et al., 2011). The number of basis markings is finite if the LPN system is bounded.

Given an LPN system G, its set of basis markings $\mathcal{M}_b$, and an observation $w \in \mathcal{L}(G)$, in Ma et al. (2017) it is shown that
$$\mathcal{C}(w) = U(\mathcal{M}_b \cap \mathcal{C}(w)). \tag{1}$$

3 K-step opacity and infinite-step opacity

K-step opacity and infinite-step opacity have been defined in the framework of automata. In this section we extend these two opacity properties to labeled Petri net systems.

In the framework of LPNs, the *secret* is a subset of reachable makings $S \subseteq R(N, M_0)$. A marking $M \in S$ is called a *secret marking*.

Definition 4 [**K-Step Opacity**] *Let $G = (N, M_0, E, \ell)$ be an LPN system, $K \in \mathbb{N}$ an integer and $S \subseteq R(N, M_0)$ a secret. System G is* K-step opaque *w.r.t. S if $\forall \sigma_1\sigma_2 \in L(N, M_0)$ with $M_0[\sigma_1\rangle M_1$, $M_1 \in S$ and $|\ell(\sigma_2)| \leq K$, there exists $\sigma_1'\sigma_2' \in L(N, M_0)$ such that $M_0[\sigma_1'\rangle M_1'$, $M_1' \notin S$, $\ell(\sigma_1) = \ell(\sigma_1')$ and $\ell(\sigma_2) = \ell(\sigma_2')$.* $\diamond$

In words, an LPN system is K-step opaque if for any transition sequence σ_1 leading to a secret marking M_1 there exists another transition sequence σ_1' that leads to a non-secret marking M_1' and produces the same observation. Meanwhile, identical observations no longer than K can be generated both from M_1 and M_1'. Namely, after observing $\ell(\sigma_1)$, the intruder cannot infer that the system reached a secret marking at some time instant within the observation of K further events. Note that if $K = 0$, K-step opacity reduces to current-state opacity. When K converges to $+\infty$, K-step opacity becomes infinite-step opacity that is formally defined as follows.

Definition 5 [**Infinite-Step Opacity**] *Let $G = (N, M_0, E, \ell)$ be an LPN system and $S \subseteq R(N, M_0)$*

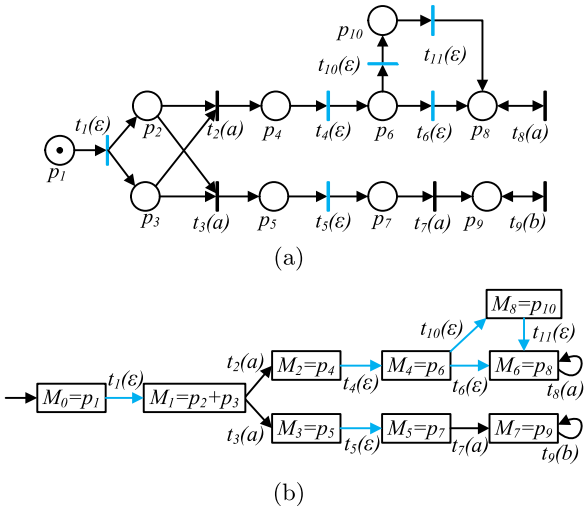

Fig. 1. The LPN system in Example 1 (a), and its RG (b), where the generic marking M is denoted in a compact form by $M = \sum_{p\in P} M(p)\cdot p$. As an example, $M_0 = [1\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0]^T$ is denoted by $M_0 = p_1$.

a secret. System G is infinite-step opaque *w.r.t. S if $\forall \sigma_1\sigma_2 \in L(N, M_0)$ with $M_0[\sigma_1\rangle M_1$ and $M_1 \in S$, there exists $\sigma_1'\sigma_2' \in L(N, M_0)$ such that $M_0[\sigma_1'\rangle M_1'$, $M_1' \notin S$, $\ell(\sigma_1) = \ell(\sigma_1')$ and $\ell(\sigma_2) = \ell(\sigma_2')$.* ◇

Infinite-step opacity implies that based on its observation the intruder can never infer that a secret marking was reached at any time instant.

Example 1 *Let us consider the LPN system in Fig. 1(a) where the set of observable transitions is $T_o = \{t_2, t_3, t_7, t_8, t_9\}$ and the set of unobservable transitions (colored in blue) is $T_u = \{t_1, t_4, t_5, t_6, t_{10}, t_{11}\}$. Transitions t_2, t_3, t_7 and t_8 are labeled a, and transition t_9 is labeled b. The reachability graph (RG) of the LPN system is shown in Fig. 1(b). Let the secret be $S = \{M_3, M_5\}$ and $K = 1$. Transition sequences leading to secret markings are t_1t_3 and $t_1t_3t_5$. Let $\sigma_1 = t_1t_3$ (or $\sigma_1 = t_1t_3t_5$). There exists $\sigma_1' = t_1t_2t_4t_6$ such that $M_0[\sigma_1'\rangle M_6$, $M_6 \notin S$, $\ell(t_1t_2t_4t_6) = \ell(t_1t_3) = \ell(t_1t_3t_5)$, and for any σ_2 with $\sigma_1\sigma_2 \in L(G)$ and $|\ell(\sigma_2)| \leq 1$ (e.g. $\sigma_2 = t_7$) there exists σ_2' such that $\sigma_1'\sigma_2' \in L(G)$ and $\ell(\sigma_2') = \ell(\sigma_2)$ (e.g. $\sigma_2' = t_8$). Therefore, the LPN system is 1-step opaque. Note that the LPN system in Fig. 1(a) is not 2-step opaque. Indeed, for $\sigma_1 = t_1t_3t_5$ and $\sigma_2 = t_7t_9$, there exist no σ_1' and σ_2' such that $M_0[\sigma_1'\rangle M$, $M \notin S$ and $\ell(\sigma_1'\sigma_2') = \ell(\sigma_1\sigma_2)$. This also implies that the LPN system is not infinite-step opaque.*
Suppose transition t_9 is labeled a instead of b. The LPN system is infinite-step opaque w.r.t. S since the intruder will never be able to establish if markings M_3 and M_5 have been visited when observing aa^*. ◇

Let us now provide necessary and sufficient conditions for the two opacity properties. To formalize them, given $w_1, w_2 \in E^*$, let us denote

$$\mathcal{M}(w_1|w_2) = \{M \in R(N, M_0) | \exists \sigma_1\sigma_2 \in L(N, M_0) : M_0[\sigma_1\rangle M, \ell(\sigma_1) = w_1, \ell(\sigma_2) = w_2\} \quad (2)$$

the set of markings consistent with w_1 from which w_2 can be generated in $G = (N, M_0, E, \ell)$. Clearly, $\mathcal{M}(w_1|w_2) \subseteq \mathcal{C}(w_1)$.

By Definitions 4 and 5, it follows that

(1) G is K-step opaque w.r.t S iff $\forall w_1w_2 \in \mathcal{L}(G)$ with $|w_2| \leq K$, $\mathcal{M}(w_1|w_2) \nsubseteq S$;
(2) G is infinite-step opaque w.r.t S iff $\forall w_1w_2 \in \mathcal{L}(G)$, $\mathcal{M}(w_1|w_2) \nsubseteq S$.

Therefore, K-step opacity and infinite-step opacity in LPN systems can be verified by analyzing the marking set $\mathcal{M}(w_1|w_2)$ for all $w_1w_2 \in \mathcal{L}(G)$. In Lan et al. (2020a), it is proven that in the automaton framework all such sets of states are identical to the intersection of the states of the observer of the system and the states of its initial-state estimator. In other words, to calculate $\mathcal{M}(w_1|w_2)$ and to verify K-step and infinite-step opacity, one can construct the RG of the LPN system first and then the observer and the initial-state estimator of the RG. However, it is known that the size of RG is exponential with respect to the size of the net system while the number of states of the observer and of the initial-state estimator are both exponential with respect to the number of reachable markings. Therefore, for RG-based methods state explosion is unavoidable. In the following sections, we propose methods based on the basis reachability graph, whose size is usually smaller than the RG.

4 Verification Using Basis Reachability Graph

In this section, we present preliminary results on verification of the two opacity properties using BRG, which are the basis for the general solutions in Section 5. The usage of BRG requires the satisfaction of the following two assumptions, which are common to all the literature in this area (e.g., Cabasino et al. (2011); Tong et al. (2017); Ma et al. (2017)):
A1) the LPN system is bounded,
A2) its T_u-induced subnet is acyclic.
In the rest of the paper, we always assume that the two assumptions are satisfied.

Given an LPN system $G = (N, M_0, E, \ell)$, its BRG is an NFA, where each state is a basis marking, the set of events is the alphabet of the LPN system, and there is no transition labeled with the empty word. We denote it as $\mathcal{B} = (\mathcal{M}_b, E, f, M_0)$. It is proven that $\mathcal{L}(\mathcal{B}) = \mathcal{L}(G)$. To avoid repeating material already presented in other papers, we refer the reader to Tong et al. (2017) for the algorithm to construct the BRG.

Given a BRG $\mathcal{B} = (\mathcal{M}_b, E, f, M_0)$, we denote:
- $\mathcal{B}_o = (\mathcal{X}_o, E, f_o, X_{o,0})$ the observer of $\mathcal{B}$, and
- $\mathcal{B}_e = (\mathcal{X}_e, E, f_e, X_{e,0})$ the initial-state estimator of $\mathcal{B}$.

Example 2 *Let us consider again the bounded LPN system in Fig. 1(a), whose T_u-induced subnet is acyclic. The BRG of the system is shown in Fig. 2, where there are*

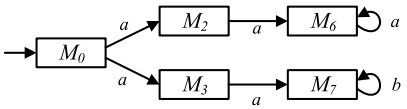

Fig. 2. The BRG $\mathcal{B}$ of the LPN system in Fig. 1.

only five basis markings $\mathcal{M}_b = \{M_0, M_2, M_3, M_6, M_7\}$. $\diamond$

Given an LPN system G and observations $w_1w_2 \in \mathcal{L}(G) = \mathcal{L}(\mathcal{B})$, we denote

$$\mathcal{M}_b(w_1|w_2) = \{M \in \mathcal{M}_b | \exists w_1w_2 \in \mathcal{L}(\mathcal{B}) : M \in f(M_0, w_1) \wedge f(M, w_2)!\}$$

the set of basis markings consistent with w_1 from which w_2 can be generated in the BRG (and thus in the system G). Clearly, $\mathcal{M}_b(w_1|w_2) \subseteq \mathcal{M}(w_1|w_2)$.

Sufficient conditions for K-step opacity and infinite-step opacity can be derived as follows.

Proposition 1 *Let G be an LPN system and S a secret.*

1. *System G is K-step opaque w.r.t. S if $\forall w_1w_2 \in \mathcal{L}(G)$ with $|w_2| \leq K$, $\mathcal{M}_b(w_1|w_2) \nsubseteq S$.*
2. *System G is infinite-step opaque w.r.t. S if $\forall w_1w_2 \in \mathcal{L}(G)$, $\mathcal{M}_b(w_1|w_2) \nsubseteq S$.*

Proof. For any $w_1w_2 \in \mathcal{L}(G)$ with $|w_2| \leq K$, $\mathcal{M}_b(w_1|w_2) \subseteq \mathcal{M}(w_1|w_2)$. If $\mathcal{M}_b(w_1|w_2) \nsubseteq S, \mathcal{M}(w_1|w_2) \nsubseteq S$. Therefore, G is K-step opaque w.r.t. S. When $K = +\infty$, G is infinite-step opaque w.r.t S. □

Conditions in Proposition 1 are not necessary because $\mathcal{M}_b(w_1|w_2) \subseteq S$ does not imply $\mathcal{M}(w_1|w_2) \subseteq S$. However, necessary and sufficient conditions can be derived under the additional assumption:

A3) $M_b \in S \Rightarrow U(M_b) \subseteq S$.

Namely, if a basis marking M_b is a secret marking, then any marking reachable from M_b firing unobservable transitions is also a secret marking.

Under the additional Assumption A3, the conditions in Proposition 1 become necessary and sufficient.

Proposition 2 *Let G be an LPN system, and S a secret satisfying Assumption A3.*

1. *System G is K-step opaque w.r.t. S, if and only if $\forall w_1w_2 \in \mathcal{L}(G)$ with $|w_2| \leq K, \mathcal{M}_b(w_1|w_2) \nsubseteq S$.*
2. *System G is infinite-step opaque w.r.t. S, if and only if $\forall w_1w_2 \in \mathcal{L}(G), \mathcal{M}_b(w_1|w_2) \nsubseteq S$.*

Proof. The If part has been proven in Proposition 1. Now we prove the necessity of the conditions.

Assume that system G is K-step opaque, and this implies that for any $w_1w_2 \in \mathcal{L}(G)$ with $|w_2| \leq K$, $\mathcal{M}(w_1|w_2) \nsubseteq S$. Thus, there exists a marking $M \in \mathcal{M}(w_1|w_2) \setminus S$. By Eq. (1), there exists a basis marking $M_b \in \mathcal{M}_b \cap \mathcal{C}(w_1)$ such that $M \in U(M_b)$. Clearly, $M_b \in \mathcal{M}_b(w_1|w_2)$. Since $M \notin S$, under Assumption A3, it holds that $M_b \notin S$. Therefore, $\mathcal{M}_b(w_1|w_2) \nsubseteq S$.

When $K = +\infty$, then G is infinite-step opaque, and this implies that for any $w_1w_2 \in \mathcal{L}(G)$, $\mathcal{M}_b(w_1|w_2) \nsubseteq S$. □

Proposition 2 reduces the necessary and sufficient conditions on reachable markings to conditions on basis markings. Therefore, the BRG may be used to check K-step opacity and infinite-step opacity of an LPN system. Analogously, based on the results in Lan et al. (2020a), the two conditions can be verified by checking the intersections between pairs of states in the observer and in the initial-state estimator of the BRG.

Theorem 3 *Let G be an LPN system, S a secret satisfying Assumption A3, $\mathcal{B}$ the BRG of G, $\mathcal{B}_o$ the observer of $\mathcal{B}$, and $\mathcal{B}_e$ the initial-state estimator of $\mathcal{B}$.*

1. *System G is K-step opaque w.r.t. S if and only if $\nexists X_o \in \mathcal{X}_o$ and $\nexists X_e \in \mathcal{X}_e^K$ such that $\emptyset \neq (X_o \cap X_e) \subseteq S$, where $\mathcal{X}_e^K = \{X_e \in \mathcal{X}_e | \exists w \in \mathcal{L}(\mathcal{B}_e), |w| \leq K : X_e = f_e(X_{e,0}, w)\}$.*
2. *System G is infinite-step opaque w.r.t. S if and only if $\nexists X_o \in \mathcal{X}_o$ and $\nexists X_e \in \mathcal{X}_e$ such that $\emptyset \neq (X_o \cap X_e) \subseteq S$.*

Proof. Statement 1 follows from Theorem 4 in Lan et al. (2020a) and Proposition 2. Statement 2 follows from Theorem 2 in Lan et al. (2020a) and Proposition 2. □

Under Assumptions A1, A2 and A3, K-step opacity and infinite-step opacity of an LPN system can be verified by constructing the observer and the initial-state estimator of the BRG, which usually has less states compared with the RG. Therefore, the proposed BRG-based method is more efficient than the RG-based method.

5 Verification Using Extended Basis Reachability Graph

In order to provide a more general solution to K/infinite-step opacity verification in Petri nets, we relax Assumption A3 and look for solutions that are still BRG-based.

First, we show that Assumption A3 can be relaxed provided that the notion of basis marking is appropriately extended.

In Section 3, we have shown that K-step opacity and infinite-step opacity can be checked by analyzing whether $\mathcal{M}(w_1|w_2) \nsubseteq S$. According to Proposition 2, if Assumption A3 is satisfied, we only need to check whether $\mathcal{M}_b(w_1|w_2) \nsubseteq S$. If Assumption A3 does not hold, in addition to the markings in $\mathcal{M}_b(w_1|w_2)$, an appropriate set of markings should be explicitly considered, as explained in the following, which in general results in a strict subset of $\mathcal{M}(w_1|w_2)$, with consequent advantages in terms of complexity.

Let us now introduce three sets that depend on the secrete S:

- $\overline{S} = R(N, M_0) \setminus S$ is the set of markings that are reachable and do not belong to the secret. It is called the set of *exposable markings*.

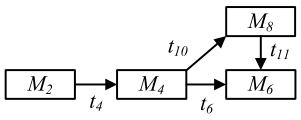

Fig. 3. Reachability graph $R(N', M_2)$.

- $\tilde{S}_b = \{M_b \in \mathcal{M}_b | M_b \in S, U(M_b) \not\subseteq S\}$ is the set of basis markings that do not satisfy Assumption A3, namely the set of secret basis markings whose unobservable reach is not contained in the secret. It is called the set of weakly exposable basis markings.
- $Q_{min} = \bigcup_{M_b \in \tilde{S}_b} \{M \in U(M_b) \setminus S | \nexists M' \in U(M_b) \setminus S : M \in U(M') \wedge M' \neq M\}$ is the set of exposable markings in the unobservable reach of $\tilde{S}_b$ that cannot be reached from other such markings. Clearly, $Q_{min} \subseteq \overline{S}$.

Example 3 *Consider again the LPN system in Fig. 1(a) whose BRG is shown in Fig. 2. Let $S = \{M_2, M_5\}$. Thus, $\tilde{S}_b = \{M_2\}$. To make it more clear, we construct the reachability graph (see Fig. 3) of the Petri net system $\langle N_u, M_2 \rangle$, and denote it as the automaton $R = (U(M_2), T_u, \delta, M_2)$, where the set of states is identical to the unobservable reach of M_2, T_u is the set of events, δ is the transition function and M_2 is the initial state. Since $U(M_2) \setminus S = \{M_4, M_6, M_8\}$ and $M_6, M_8 \in U(M_4)$, $Q_{min} = \{M_4\}$.* $\diamond$

We now prove that the condition $\mathcal{M}(w_1|w_2) \not\subseteq S$ for an arbitrary sequence $w_1 w_2 \in \mathcal{L}(G)$ is equivalent to at least one of the two conditions: $\mathcal{M}_b(w_1|w_2) \not\subseteq S$ or $\mathcal{M}(w_1|w_2) \cap Q_{min} \neq \emptyset$.

Proposition 4 *Let G be an LPN system, and S a secret. Given $w_1 w_2 \in \mathcal{L}(G)$, it holds that $\mathcal{M}(w_1|w_2) \not\subseteq S$ if and only if at least one of the two conditions holds:*

- $\mathcal{M}_b(w_1|w_2) \not\subseteq S$;
- $\mathcal{M}(w_1|w_2) \cap Q_{min} \neq \emptyset$.

Proof. (If) Assume that $\mathcal{M}_b(w_1|w_2) \not\subseteq S$. Since $\mathcal{M}_b(w_1|w_2) \subseteq \mathcal{M}(w_1|w_2)$, $\mathcal{M}(w_1|w_2) \not\subseteq S$.

Assume that $\mathcal{M}_b(w_1|w_2) \subseteq S$ and $\mathcal{M}(w_1|w_2) \cap Q_{min} \neq \emptyset$. Since $Q_{min} \subseteq \overline{S}$, $\mathcal{M}(w_1|w_2) \cap \overline{S} \neq \emptyset$. Thus, $\mathcal{M}(w_1|w_2) \not\subseteq S$.

(Only if) Assume that $\mathcal{M}(w_1|w_2) \not\subseteq S$. This implies that there exists a marking $M \in \mathcal{M}(w_1|w_2) \cap \overline{S}$. By Eq. (1), there exists a basis marking $M_b \in \mathcal{M}_b \cap \mathcal{C}(w_1)$ such that $M \in U(M_b)$. Clearly, $M_b \in \mathcal{M}_b(w_1|w_2)$. Case 1: if $M_b \in \overline{S}$, then $\mathcal{M}_b(w_1|w_2) \not\subseteq S$. Case 2: if $M_b \in S$, then $M_b \in \tilde{S}_b$ since $M \in U(M_b) \setminus S$. By definition of Q_{min}, there must exist a marking $M' \in U(M_b) \setminus S$ such that $M \in U(M')$ and $M' \in Q_{min}$ (Note that M' may be equal to M). Clearly, $M' \in \mathcal{M}(w_1|w_2)$. Therefore, $\mathcal{M}(w_1|w_2) \cap Q_{min} \neq \emptyset$. $\square$

Proposition 4 shows that not only the markings in $\mathcal{M}_b(w_1|w_2)$, but also the markings in $Q_{min} \cap \mathcal{M}(w_1|w_2)$, need to be enumerated. In the rest of the section, we propose a new structure, called *extended basis reachability graph* (EBRG), which includes some new markings to the BRG. Furthermore, we show that the EBRG can be used to verify the conditions for all $w_1 w_2 \in \mathcal{L}(G)$, thus making it an appropriate tool for the verification of the two opacity properties of interest when Assumption A3 does not hold.

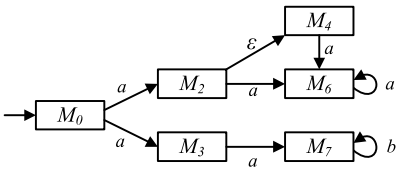

Fig. 4. The EBRG $\mathcal{B}'$ of the LPN system in Fig. 1.

Algorithm 1 Computation of the EBRG

Require: An LPN system $G = (N, M_0, E, \ell)$ and a secret S, which satisfy Assumptions A1 and A2.
Ensure: The EBRG $\mathcal{B}' = (\mathcal{M}'_b, E, f', M_0)$.

1: Construct the BRG $\mathcal{B} = (\mathcal{M}_b, E, f, M_0)$;
2: $\mathcal{M}'_b := \mathcal{M}_b$, $f' := f$, $Q_{min} := \emptyset$.
3: Compute $\tilde{S}_b$ the set of weakly exposable basis markings,
4: **for all** basis markings $M_b \in \tilde{S}_b$, **do**
5: $\quad Q := U(M_b) \setminus S$,
6: $\quad$ **for all** $M \in Q$, **do**
7: $\quad\quad$ **if** $\nexists M' \in Q : M \in U(M') \wedge M \neq M'$ **then**,
8: $\quad\quad\quad f'(M_b, \varepsilon) := f'(M_b, \varepsilon) \cup \{M\}$;
9: $\quad\quad\quad Q_{min} := Q_{min} \cup \{M\}$,
10: $\quad\quad$ **end if**
11: $\quad$ **end for**
12: **end for**
13: $\mathcal{M}'_b := \mathcal{M}'_b \cup Q_{min}$, $Q_{new} := Q_{min}$;
14: **for all** markings $M \in Q_{new}$, **do**
15: $\quad$ **for all** t s.t. $\ell(t) \in E$ and $Y_{min}(M, t) \neq \emptyset$, **do**
16: $\quad\quad$ **for all** $y_u \in Y_{min}(M, t)$, **do**
17: $\quad\quad\quad M' := M + C_u \cdot y_u + C(\cdot, t)$;
18: $\quad\quad\quad f'(M, \ell(t)) := f'(M, \ell(t)) \cup \{M'\}$;
19: $\quad\quad\quad$ **if** $M' \notin \mathcal{M}'_b$, **then**
20: $\quad\quad\quad\quad \mathcal{M}'_b := \mathcal{M}'_b \cup \{M'\}$;
21: $\quad\quad\quad\quad Q_{new} := Q_{new} \cup \{M'\}$;
22: $\quad\quad\quad$ **end if**
23: $\quad\quad$ **end for**
24: $\quad$ **end for**
25: $\quad Q_{new} := Q_{new} \setminus \{M\}$;
26: **end for**

The construction of the EBRG is summarized in Algorithm 1. First, we construct the BRG $\mathcal{B}$, initialize $\mathcal{M}'_b$ as $\mathcal{M}_b$ and $Q_{min} = \emptyset$, and copy the transitions in BRG to EBRG (Steps 1 to 2). Then compute set Q_{min} (Steps 3 to 12) and transitions from basis markings to markings in Q_{min} (Step 8). Then add all the markings in Q_{min} to $\mathcal{M}'_b$ (Step 13). Next, for all markings M in Q_{min}, if there exists an observable transition t for which a minimal explanation exists, we compute the markings reached fir-

ing t and its minimal explanations (Steps 14 to 17). Let M' be one of such markings. We add an edge from M to M' labeled $\ell(t)$ (Step 18). If such a node does not exist in the EBRG, then we add it to $\mathcal{M}'_b$ (Steps 19 to 22). This procedure runs iteratively until all markings in Q_{new} have been explored. Although the EBRG is larger than the BRG, it is still smaller than the RG. Note that the EBRG contains all the basis markings in the BRG, all the markings in Q_{min}, and possibly some non basis markings that can be reached from the markings in Q_{min} firing some observable transitions and the corresponding minimal explanations.

Example 4 *Consider again the LPN system in Fig. 1(a) whose BRG is shown in Fig. 2. Let* $S = \{M_2, M_5\}$. *As shown in Example 3,* $\tilde{S}_b = \{M_2\}$. *For* M_2, $Q = \{M_4, M_6, M_8\}$. *By Steps 6 to 11 of Algorithm 1,* $Q_{min} = \{M_4\}$ *and* $M_4 \in f'(M_2, \varepsilon)$. *By Steps 14 to 26,* $M_6 \in f'(M_4, a)$. *Finally, we compute the EBRG in Fig. 4.* $\diamond$

Although the EBRG contains more markings than the BRG, their generated languages are identical.

Proposition 5 *Let* $\mathcal{B}'$ *be the EBRG of the LPN system* G. *It holds that* $\mathcal{L}(\mathcal{B}') = \mathcal{L}(G)$.

Proof. By Steps 1 and 2 of Algorithm 1, the structure of the BRG is included in the EBRG. In Steps 4 to 12, for each marking $M \in Q_{min}$, there exists a basis marking $M_b \in \mathcal{M}_b$ such that $M \in U(M_b)$ and M is connected with M_b by the empty word. Then in Steps 13 to 26, the transitions from M to M' are computed following the same procedure used to compute the transition between basis markings (ref. Tong et al. (2017)). Namely, any observation generated from M can be generated from M_b in the BRG. Meanwhile, M is reachable from M_b through the empty word. Therefore, $\mathcal{L}(\mathcal{B}') = \mathcal{L}(\mathcal{B}) = \mathcal{L}(G)$. $\square$

Consider the EBRG $\mathcal{B}' = (\mathcal{M}'_b, E, f', M_0)$. We denote

$$\mathcal{M}'_b(w_1|w_2) = \{M \in \mathcal{M}'_b | \exists w_1 w_2 \in \mathcal{L}(\mathcal{B}') : M \in f'(M_0, w_1) \wedge f'(M, w_2)!\}$$

the set of markings consistent with w_1 from which w_2 can be generated in the EBRG. Clearly, $\mathcal{M}_b(w_1|w_2) \subseteq \mathcal{M}'_b(w_1|w_2) \subseteq \mathcal{M}(w_1|w_2)$.

Proposition 6 *Let* G *be an LPN system,* $w_1 w_2 \in \mathcal{L}(G)$, *and* S *a secret. It holds that* $\mathcal{M}(w_1|w_2) \not\subseteq S$ *if and only if* $\mathcal{M}'_b(w_1|w_2) \not\subseteq S$.

Proof. (If) Assume that $\mathcal{M}'_b(w_1|w_2) \not\subseteq S$. Since $\mathcal{M}'_b(w_1|w_2) \subseteq \mathcal{M}(w_1|w_2)$, $\mathcal{M}(w_1|w_2) \not\subseteq S$.

(Only if) Assume that $\mathcal{M}(w_1|w_2) \not\subseteq S$. By Proposition 4, $\mathcal{M}_b(w_1|w_2) \not\subseteq S$ or $\mathcal{M}(w_1|w_2) \cap Q_{min} \neq \emptyset$. Case 1: if $\mathcal{M}_b(w_1|w_2) \not\subseteq S$, since $\mathcal{M}_b(w_1|w_2) \subseteq \mathcal{M}'_b(w_1|w_2)$, then $\mathcal{M}'_b(w_1|w_2) \not\subseteq S$. Case 2: if $\mathcal{M}_b(w_1|w_2) \subseteq S$ and $\mathcal{M}(w_1|w_2) \cap Q_{min} \neq \emptyset$, then there exists a marking $M \in \mathcal{M}(w_1|w_2) \cap \overline{S}$. By Eq. (1), there exists a basis marking $M_b \in \mathcal{M}_b \cap \mathcal{C}(w_1)$ such that $M \in U(M_b)$. Clearly, $M_b \in \mathcal{M}_b(w_1|w_2)$. Since $M \in U(M_b) \setminus S$, $M_b \in \tilde{S}_b$. By Steps 4 to 9 of Algorithm 1, there must exist a marking $M_j \in U(M_b) \setminus S$ such that $M \in U(M_j)$ and $M_j \in f'(M_b, \varepsilon)$. Clearly, $M_j \in \mathcal{C}(w_1)$. Since $M \in U(M_j)$, $f'(M_j, w_2)!$. Thus, $M' \in \mathcal{M}'_b(w_1|w_2)$. Therefore, $\mathcal{M}'_b(w_1|w_2) \not\subseteq S$. $\square$

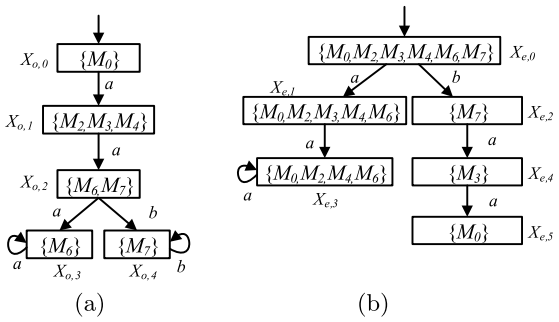

Fig. 5. The observer $\mathcal{B}'_o$ (a) and the initial-state estimator $\mathcal{B}'_e$ (b) of the EBRG $\mathcal{B}'$ in Fig. 4.

Propositions 5 and 6 lead to the conclusion that the EBRG can be used to check K-step opacity and infinite-step opacity of an LPN system. In the following, we show that the two opacity properties can be verified by checking the intersections between pairs of states in the observer and the initial-state estimator of the EBRG.

Theorem 7 *Let* G *be an LPN system,* $\mathcal{B}'$ *the EBRG of an LPN system* G, $\mathcal{B}'_o = (\mathcal{X}'_o, E, f'_o, X'_{o,0})$ *the observer of* $\mathcal{B}'$, $\mathcal{B}'_e = (\mathcal{X}'_e, E, f'_e, X'_{e,0})$ *the initial-state estimator of* $\mathcal{B}'$, *and* S *a secret.*

1. *System* G *is* K*-step opaque w.r.t.* S *if and only if* $\nexists X'_o \in \mathcal{X}'_o$ *and* $\nexists X'_e \in \mathcal{X}'^{K'}_e$ *such that*
$$\emptyset \neq (X'_o \cap X'_e) \subseteq S. \quad (3)$$
where $\mathcal{X}'^{K'}_e = \{X'_e \in \mathcal{X}'_e | \exists w \in \mathcal{L}(\mathcal{B}'_e), |w| \leq K : X'_e = f'_e(X'_{e,0}, w)\}$.
2. *System* G *is infinite-step opaque w.r.t.* S *if and only if* $\nexists X'_o \in \mathcal{X}'_o$ *and* $\nexists X'_e \in \mathcal{X}'_e$ *such that*
$$\emptyset \neq (X'_o \cap X'_e) \subseteq S.$$

Proof. Since the EBRG is an automaton, the set $\mathcal{M}'_b(w_1|w_2)$ can be calculated using the same method in Yin and Lafortune (2017). Based on this, we prove the statement by providing a series of iff conditions.

G is K-step opaque under A1 and A2
$\Leftrightarrow$ $\forall w_1 w_2 \in \mathcal{L}(G)$ with $|w_2| \leq K, \mathcal{M}(w_1|w_2) \not\subseteq S$.
$\Leftrightarrow$ $\forall w_1 w_2 \in \mathcal{L}(\mathcal{B}')$ with $|w_2| \leq K, \mathcal{M}'_b(w_1|w_2) \not\subseteq S$.
(by Propositions 5 and 6)
$\Leftrightarrow$ 1. $\nexists X'_o \in \mathcal{X}'_o, \nexists X'_e \in \mathcal{X}'^{K'}_e : \emptyset \neq (X'_o \cap X'_e) \subseteq S$
(by Theorem 4 in Lan et al. (2020a)).
2. $\nexists X'_o \in \mathcal{X}'_o, \nexists X'_e \in \mathcal{X}'_e : \emptyset \neq (X'_o \cap X'_e) \subseteq S$
(by Theorem 2 in Lan et al. (2020a)). $\square$

Example 5 *Consider again the LPN system in Fig. 1(a). Consider secret* $S = \{M_2, M_5\}$ *that does not satisfy Assumption A3. The EBRG of the LPN system is constructed by Algorithm 1, as shown in Fig. 4. Now,* $\mathcal{M}'_b = \{M_0, M_2, M_3, M_4, M_6, M_7\}$. *The corresponding observer and initial-state estimator are shown in Fig. 5(a) and 5(b), respectively. It holds that for any state* $X'_o \in \mathcal{X}'_o$ *and any state* $X'_e \in \mathcal{X}'_e$, $X'_o \cap X'_e \nsubseteq S$ or $X'_o \cap X'_e = \emptyset$. *Therefore, system* G *is infinite-step opaque w.r.t.* S. ◇

Now, let us discuss the complexity of the above verification approaches. First, the complexity of constructing the EBRG is exponential with respect to the size of the net system (number of places, transitions, and the initial marking) because in the worst case the EBRG coincides with the RG. However, as extensively discussed, in practice $|\mathcal{M}'_b|$ is smaller than $|R(N, M_0)|$. Given a state $X'_o \in \mathcal{X}'_o$ and a state $X'_e \in \mathcal{X}'_e$, the complexity of testing condition (3) is $\mathcal{O}(|\mathcal{M}'_b|)$. In the worst case, there are $2^{|\mathcal{M}'_b|}$ states in $\mathcal{B}'_o$ and $2^{|\mathcal{M}'_b|}$ states in $\mathcal{B}'_e$. Thus, the complexity of verifying infinite-step opacity using the proposed approach is $\mathcal{O}(|\mathcal{M}'_b| \times 2^{|\mathcal{M}'_b|} \times 2^{|\mathcal{M}'_b|})$. Moreover, in the worst case, the number of states in $\mathcal{X}'^{K'}_e$ is bounded by $min\{|E|^K, 2^{|\mathcal{M}'_b|}\}$. Thus, the complexity of verifying K-step opacity using the proposed approach is $\mathcal{O}(min\{|E|^K, 2^{|\mathcal{M}'_b|}\} \times 2^{|\mathcal{M}'_b|} \times |\mathcal{M}'_b|)$.

In summary, since $|\mathcal{M}'_b| < |R(N, M_0)|$, the proposed EBRG-based approaches have advantages over the RG-based approaches in some cases. Two benchmarks are provided in Tong (2021) to show the efficiency of using BRG and EBRG.

Remark: In Tong et al. (2017), a structure called *modified basis reachability graph* (MBRG) is proposed to relax Assumption A3, so that initial-state opacity can be verified by constructing the initial-state estimator of the MBRG. Although MBRG and EBRG are both proposed in order to relax Assumption A3, the two structures are different as the sets Q_{min} are different. Therefore, MBRG can not be used to check K-step opacity and infinite-step opacity.

6 Conclusions

In this paper, we first prove that both K-step and infinite-step opacity of bounded labeled Petri net systems can be verified by constructing the observer and the initial-state estimator of the basis reachability graph if the unobservable subnet is acyclic and the unobservable reach of secret basis markings is still in the secret. To relax the assumption on the unobservable reach of secret basis markings, the extended basis reachability graph is introduced to verify the two opacity properties. The proposed approaches present advantages in terms of complexity over the reachability graph based approaches in the literature, since the enumeration of the whole state space of the system is avoided.

References

Boel, K.R., Jiroveanu, G., 2004. Distributed contextual diagnosis for very large systems. IFAC Proceedings Volumes 37, 333–338. 2004 the 7th Workshop on Discrete Event Systems.

Cabasino, M.P., Giua, A., Pocci, M., Seatzu, C., 2011. Discrete event diagnosis using labeled Petri nets. An application to manufacturing systems. Control Engineering Practice 19, 989–1001.

Cassandras, C.G., Lafortune, S., 2008. Introduction to discrete event systems. Springer.

Cong, X., Fanti, M.P., Mangini, A.M., Li, Z., 2018. Online verification of current-state opacity by Petri nets and integer linear programming. Automatica 94, 205–213.

Jacob, R., Lesage, J.J., Faure, J.M., 2016. Overview of discrete event systems opacity: Models, validation, and quantification. Annual Reviews in Control 41, 135–146.

Jiroveanu, G., Boel, R.K., 2004. Contextual analysis of Petri nets for distributed applications, in: 16th Int. Symp. on Mathematical Theory of Networks and Systems (Leuven, Belgium), p. 136.

Lan, H., Tong, Y., Guo, J., Giua, A., 2020a. Comments on "A new approach for the verification of infinite-step and K-step opacity using two-way observers"[Automatica 80 (2017) 162–171]. Automatica 122, 109290.

Lan, H., Tong, Y., Seatzu, C., 2020b. Verification of infinite-step opacity using labeled Petri nets. IFAC-PapersOnLine 53, 1729–1734. The 21th IFAC World Congress.

Ma, Z., Tong, Y., Li, Z., Giua, A., 2017. Basis marking representation of Petri net reachability spaces and its application to the reachability problem. IEEE Transactions on Automatic Control 62, 1078–1093.

Saboori, A., Hadjicostis, C.N., 2007. Notions of security and opacity in discrete event systems, in: 46th IEEE Conference on Decision and Control, pp. 5056–5061.

Saboori, A., Hadjicostis, C.N., 2009. Verification of infinite-step opacity and analysis of its complexity. IFAC Proceedings Volumes 42, 46–51.

Saboori, A., Hadjicostis, C.N., 2011. Verification of infinite-step opacity and complexity considerations. IEEE Transactions on Automatic Control 57, 1265–1269.

Tong, Y., 2021. Benchmarks of extended basis reachability graphs. Available at: `https://arxiv.org/pdf/2111.10218.pdf`.

Tong, Y., Li, Z., Seatzu, C., Giua, A., 2017. Verification of state-based opacity using Petri nets. IEEE Transactions on Automatic Control 62, 2823–2837.

Tong, Y., Ma, Z., Li, Z., Seatzu, C., Giua, A., 2016. Verification of language-based opacity in Petri nets using verifier, in: American Control Conference, pp. 757–763.

Wu, Y., Lafortune, S., 2013. Comparative analysis of related notions of opacity in centralized and coordi-

nated architectures. Discrete Event Dynamic Systems 23, 307–339.

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.