Verification of State-Based Opacity Using Petri Nets

Yin Tong, *Student Member, IEEE,* Zhiwu Li, *Fellow, IEEE,* Carla Seatzu, *Senior Member, IEEE* and Alessandro Giua, *Senior Member, IEEE*

Abstract

A system is said to be opaque if a given secret behavior remains opaque (uncertain) to an intruder who can partially observe system activities. This work addresses the verification of state-based opacity in systems modeled with Petri nets. The secret behavior of a system is defined as a set of states. More precisely, two state-based opacity properties are considered: *current-state opacity* and *initial-state opacity*. We show that both current-state and initial-state opacity problems in bounded Petri nets can be efficiently solved by using a compact representation of the reachability graph, called *basis reachability graph* (BRG). This approach is practically efficient since the exhaustive enumeration of the reachability space can be avoided.

Index Terms

Discrete event systems, Petri nets, opacity.

To appear as:

Y. Tong, Z.W. Li, C. Seatzu, A. Giua, "Verification of State-Based Opacity Using Petri Nets," IEEE Trans. on Automatic Control, Vol. 62, No. 6, 2017. DOI: 10.1109/TAC.2016.2620429

This work was supported by the National Natural Science Foundation of China under Grants Nos. 61374068, 61472295, the Recruitment Program of Global Experts, the Science and Technology Development Fund, MSAR, under Grant No. 078/2015/A3.

Y. Tong is with the School of Electro-Mechanical Engineering, Xidian University, Xi'an 710071, China (e-mail: yintong@stu.xidian.edu.cn) and also with the Department of Electrical and Electronic Engineering, University of Cagliari, 09123 Cagliari, Italy.

Z. W. Li is with the Institute of Systems Engineering, Macau University of Science and Technology, Taipa, Macau, and also with the School of Electro-Mechanical Engineering, Xidian University, Xi'an 710071, China (e-mail: zhwli@xidian.edu.cn).

C. Seatzu is with the Department of Electrical and Electronic Engineering, University of Cagliari, 09123 Cagliari, Italy (e-mail: seatzu@diee.unica.it)

A. Giua is with Aix Marseille Univ, Université de Toulon, CNRS, ENSAM, LSIS, Marseille, France (email: alessandro.giua@lsis.org) and also with the Department of Electrical and Electronic Engineering, University of Cagliari, 09123 Cagliari, Italy (email: giua@diee.unica.it).

I. INTRODUCTION

Security is one of the most important properties in cyberinfrastructures, ranging from Internet and mobile communication networks to national defense and health service systems. In these systems some information should not be corrupted or acquired by unauthorized people (called intruders). The notion of *opacity* introduced in [1] for transition systems and later developed in [2], formalizes the absence of information flow, or more precisely, the impossibility for an intruder to infer the truth of a predicate representing the secret information. In discrete event systems (DESs), the predicate can be a subset of the state space or a language, therefore, opacity properties can be categorized into two main classes: *state-based opacity* and *language-based opacity*.

In this work, we focus on the verification of two important state-based opacity properties: *current-state opacity* and *initial-state opacity* in DESs modeled by bounded Petri nets. It is assumed that an intruder knows the structure and the initial marking of the system, however, it can only partially observe the occurrence of *events* of the system. To present such an observation structure, the system under consideration is modeled by a *labeled Petri net* (LPN), where the observation function is static and the states are not observable [2], [3], [4]. Given a secret described by a subset of the reachability set, the system is said to be current-state (resp., initial-state) opaque with respect to the secret if the intruder is never able to infer that the current (resp., initial) state of the system is within the secret.

Methods for verifying opacity have been proposed by many researchers in the area of DESs [5], [6], [7], [8], [9], [10], [11]. In a system modeled by a nondeterministic finite automaton (NFA), the verification of both current-state opacity and initial-state opacity is PSPACE-complete [8], [12], [13] with respect to the number n of states in the NFA. On one hand, to verify current-state opacity one needs to convert the NFA into an equivalent deterministic finite automaton (DFA), which has a complexity of $\mathcal{O}(2^n)$ [6], [9]. On the other hand, initial-state opacity in NFA can be verified by the method proposed by Saboori and Hadjicostis [8]. In their approach a DFA called the *initial-state estimator* is constructed with a complexity of $\mathcal{O}(2^{n^2})$. A state of the estimator reached from the initial state following a word w includes all pairs (initial state, current state) of the NFA such that the current state may be reached from the corresponding initial state observing w. As long as an initial-state estimator is built, there is no need to reconstruct it when the secret changes. In their improved method [8], *verifiers* have been introduced to study initial-state opacity. The verifier does not precisely estimate the initial state but only records the possible current states and if such states are reachable from secret/non-secret states, and hence the complexity is reduced to $\mathcal{O}(4^n)$. Furthermore, Wu and Lafortune [9] have shown that the observer of the corresponding reverse automaton can be used to estimate the initial state, which further reduces the complexity of verifying initial-state opacity to $\mathcal{O}(2^n)$.

Petri nets extend the modeling power of finite automata. Nevertheless, few works use this model to deal with state-based opacity. The first contribution is proposed by Bryans *et al*. [2] who proved that the verification of state-based opacity for bounded labeled Petri nets is decidable. Apart from our earlier work [14], [15], [16], so far no efficient opacity analysis method has been reported yet. For bounded Petri nets we may construct its reachability graph (RG) that is an NFA, so that the aforementioned approaches could be applied. Nevertheless, constructing the RG will inevitably suffer from the state explosion that also characterizes automaton models. To overcome such a limitation, in this paper we use the notions of *basis markings* and *explanations*. Such notions have been first introduced in [17], [18], [19], [20], [21] to solve the problems of state estimation, fault diagnosis, diagnosability analysis and reachability analysis in LPNs. They allow one to avoid an exhaustive enumeration of the reachability space. Only a subset of reachable markings, i.e., the basis markings, should be enumerated, while other reachable markings are characterized by linear systems, one for each basis marking. Therefore, the RG can be compactly

represented by the *basis reachability graph* (BRG), a graph describing the transition relation between basis markings.

In this paper we study current-state opacity and initial-state opacity problems in Petri nets. The main contributions of this work can be summarized as follows:

1) Necessary and sufficient conditions for current-state opacity with respect to an arbitrary secret are provided. A novel approach based on the BRG (with appropriate changes) is proposed that enables one to avoid RG analysis. Moreover, if the secret is defined as the intersection of a series of generalized mutual exclusion constraints (GMECs), then current-state opacity can be verified by solving a set of integer linear programming problems (ILPPs) instead of exhaustively enumerating the unobservable reach of basis markings. Finally, if the incidence matrix is totally unimodular, then these ILPPs can be relaxed to linear programming problems (LPPs).
2) We define *exposable* and *weakly exposable* markings. In particular, we prove that if no weakly exposable marking is contained in the secret, then current-state opacity can be efficiently verified without solving ILPPs. Moreover, the proposed approach is extended to the case where the intruder has uncertainties about the initial marking.
3) We provide necessary and sufficient conditions for initial-state opacity with respect to an arbitrary secret. We show that if no weakly exposable marking belongs to the secret, initial-state opacity can be efficiently verified using the BRG. Otherwise, we propose a modified BRG (MBRG) to verify initial-state opacity.
4) A MATLAB tool is developed to implement most of the proposed approaches. Numerical results are illustrated to corroborate their effectiveness.

Note that preliminary results concerning item 1) have been presented in [14] without formal proofs. Furthermore, we already investigated the problem of initial-state opacity in [15] but using a different approach based on language containment.

II. Background on Automata and Petri Nets

In this section we recall the formalisms used in the paper, namely automata and Petri nets. For more details we refer the reader to [22] and [23].

A. Automata

A *nondeterministic finite automaton* (NFA) is a 4-tuple $\mathcal{A} = (X, E, \Delta, X_0)$, where X is the finite *set of states*, $E = \{a, b, \cdots\}$ is the *alphabet* of events, $\Delta \subseteq X \times E_\varepsilon \times X$ is the *transition relation* (here $E_\varepsilon = E \cup \{\varepsilon\}$ and ε is the empty word associated to unobservable events), and $X_0 \subseteq X$ is the *set of initial states*[1]. The transition relation specifies the dynamics of the NFA: if $(x, e, x') \in \Delta$, then from state x the occurrence of event $e \in E_\varepsilon$ yields state x'. The transition relation can be extended to $\Delta^* \subseteq X \times E^* \times X$: $(x_{j0}, w, x_{jk}) \in \Delta^*$ if there exists a sequence of events and states $x_{j0}e_{j1}x_{j1}\cdots x_{jk-1}e_{jk}x_{jk}$ such that $\sigma = e_{j1}\dots e_{jk}$ generates the word $w \in E^*$, $x_{ji} \in X$ for $i = 0, 1, \dots, k$, and $e_{ji} \in E_\varepsilon$, $(x_{ji-1}, e_{ji}, x_{ji}) \in \Delta$ for $i = 1, 2, \dots, k$. Event $e \in E$ is said to be *defined* at state x_i if there exists a state $x_j \in X$ such $(x_i, e, x_j) \in \Delta$.

The *generated language* of an automaton $\mathcal{A} = (X, E, \Delta, X_0)$ from a state $x \in X$ is defined as

$$\mathcal{L}(\mathcal{A}, x) = \{w \in E^* | \exists x' \in X : (x, w, x') \in \Delta^*\}.$$

Generally, given a set of states $Y \subseteq X$, we define

$$\mathcal{L}(\mathcal{A}, Y) = \bigcup_{x \in Y} \mathcal{L}(\mathcal{A}, x)$$

[1]If the set of initial states only contains one state x_0, then $\mathcal{A} = (X, E, \Delta, x_0)$; if the initial states are not specified, then $\mathcal{A} = (X, E, \Delta)$.

the language generated from the states in Y.

B. Petri Nets

A *Petri net* is a structure $N = (P, T, Pre, Post)$, where P is a set of m *places*, graphically represented by circles; T is a set of n *transitions*, graphically represented by bars; $Pre : P \times T \to \mathbb{N}$ 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 vice versa[2]. The incidence matrix of a net is denoted by $C = Post - Pre$.

The input and output sets of a node $x \in P \cup T$ are denoted by ${}^\bullet x$ and $x^\bullet$, respectively. A Petri net $N = (P, T, Pre, Post)$ is a *state machine* (resp. *marked graph*) if $\forall t \in T$, $|{}^\bullet t| = |t^\bullet| \leq 1$ (resp. $\forall p \in P$, $|{}^\bullet p| = |p^\bullet| \leq 1$). A Petri net is said to be *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, graphically represented by black dots. The marking of place p is denoted by $M(p)$. A marking is also denoted as $M = \sum_{p \in P} M(p) \cdot p$. 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'. Given a sequence $\sigma \in T^*$, the function $\pi : T^* \to \mathbb{N}^n$ associates with σ the Parikh vector $y = \pi(\sigma) \in \mathbb{N}^n$, i.e., $y(t) = k$ if transition t appears k times in σ.

A marking M is *reachable* in $\langle N, M_0 \rangle$ if there exists a sequence σ such that $M_0[\sigma\rangle M$. The set of all markings reachable from M_0 defines the *reachability set* of $\langle N, M_0 \rangle$, denoted by $R(N, M_0)$. 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) 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 $T = T_o \cup T_u$, 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. The labeling function can be extended to firing sequences $\ell : T^* \to E^*$, i.e., $\ell(\sigma t) = \ell(\sigma)\ell(t)$ with $\sigma \in T^*$ and $t \in T$.

Given an LPN $G = (N, M_0, E, \ell)$ and a marking $M \in R(N, M_0)$, we define the language generated from M as

$$\mathcal{L}(N, M) = \{w \in E^* | \exists \sigma \in T^* : M[\sigma\rangle \text{ and } \ell(\sigma) = w\}.$$

Furthermore, given a set of markings $Y \subseteq R(N, M_0)$ of G, we define

$$\mathcal{L}(N, Y) = \bigcup_{M \in Y} \mathcal{L}(N, M)$$

the language generated from markings in Y.

A string belonging to $\mathcal{L}(N, M_0)$ is called an *observation*. Let w be an observation of an LPN $G = (N, M_0, E, \ell)$. We define

$$\mathcal{C}(w) = \{M \in \mathbb{N}^m | \exists \sigma \in T^* : M_0[\sigma\rangle M \text{ and } \ell(\sigma) = w\}$$

as the *set of markings consistent with* w. Note that since observation w is generated by the system, set $\mathcal{C}(w)$ must be non-empty.

[2]In this work, we use $\mathbb{N}$, $\mathbb{Z}$ and $\mathbb{R}$ to denote the sets of non-negative integers, integers and real numbers, respectively.

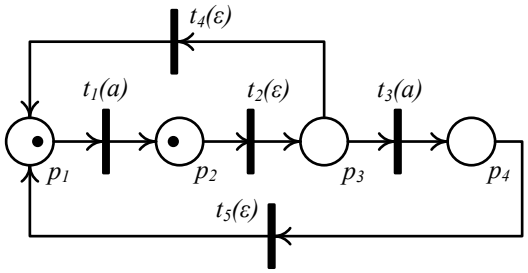

Fig. 1. An LPN whose unobservable subnet is acyclic.

Given an LPN $G = (N, M_0, E, \ell)$ and the set of unobservable transitions T_u, the *unobservable subnet* $N' = (P, T', Pre', Post')$ of G, is the net resulting by removing all transitions in $T \setminus T_u$ from N, where Pre' and $Post'$ are the restriction of Pre, $Post$ to T_u, respectively. The incidence matrix of the unobservable subnet is denoted by $C_u = Post' - Pre'$.

III. Basis Reachability Graph

In [17], [18], a compact way to represent the reachability set of a Petri net was proposed to solve the fault diagnosis problem. Under the assumption that the unobservable subnet is acyclic, only a subset of the reachable markings, called *basis markings*, are computed, while, all non-basis markings are characterized by a set of linear equations associated with each basis marking. Using the notion of basis markings, the *basis reachability graph* (BRG) is defined. It is an NFA in which each state corresponds to a basis marking and all events are observable. The BRG as proposed in [17], [18] also includes some diagnosis information, which are redundant for opacity verification. Herein we redefine it neglecting such information. Before providing the algorithm for its construction, let us recall some key definitions from [18].

Definition 3.1: Given a marking M and an observable transition $t \in T_o$, we define

$$\Sigma(M,t) = \{\sigma \in T_u^* | M[\sigma\rangle M', M' \geq Pre(\cdot,t)\}$$

as the set of *explanations* of t at M and $Y(M,t) = \{\mathbf{y}_u \in \mathbb{N}^{n_u} | \exists \sigma \in \Sigma(M,t) : \mathbf{y}_u = \pi(\sigma)\}$ as the set of *e-vectors*. ◇

Thus $\Sigma(M,t)$ is the set of unobservable sequences whose firing at M enables t and $Y(M,t)$ is the set of firing vectors of the explanations. Among all the explanations, we are interested in finding the minimal ones, i.e., those whose firing vector is minimal.

Definition 3.2: Given a marking M and an observable transition $t \in T_o$, we define

$$\Sigma_{min}(M,t) = \{\sigma \in \Sigma(M,t) | \nexists \sigma' \in \Sigma(M,t) : \pi(\sigma') \lneqq \pi(\sigma)\}$$

as the set of *minimal explanations* of t at M and $Y_{min}(M,t) = \{\mathbf{y}_u \in \mathbb{N}^{n_u} | \exists \sigma \in \Sigma_{min}(M,t) : \mathbf{y}_u = \pi(\sigma)\}$ as the corresponding set of *minimal e-vectors*. ◇

Many approaches can be applied to compute $Y_{min}(M,t)$. In particular, if the unobservable subnet is acyclic the approach proposed by Cabasino *et al.*, namely Algorithm 4.4 in [18], can be efficiently used. Note that since a given place may have two or more unobservable input transitions, i.e., the unobservable subnet is not backward conflict free, the set of minimal explanations is typically not a singleton.

Example 3.3: Let us consider the LPN in Fig. 1, where $M_0 = p_1 + p_2$. Transitions t_1 and t_3 are observable. They are both labeled a. We have $\Sigma(M_0, t_1) = \{\varepsilon, t_2, t_2t_4\}$, $\Sigma_{min}(M_0, t_1) = \{\varepsilon\}$ and $Y_{min} = \{\vec{0}\}$. Let $M = p_2 + p_4$. Then $\Sigma(M, t_1) =$

$\Sigma_{min}(M, t_1) = \{t_2t_4, t_5\}$ and $Y_{min} = \{[1\ 1\ 0]^T, [0\ 0\ 1]^T\}$. ◇

Based on the notion of minimal explanations, the set of basis markings can be recursively defined.

Definition 3.4: Given an LPN $G = (N, M_0, E, \ell)$, its set of basis markings $\mathcal{M}_B$ is a subset of $R(N, M_0)$ such that:

a) $M_0 \in \mathcal{M}_B$;

b) $\forall M \in \mathcal{M}_B, \forall t \in T_o, \forall \mathbf{y}_u \in Y_{min}(M, t)$, it holds $M' \in \mathcal{M}_B$, where $M' = M + C(\cdot, t) + C_u \cdot \mathbf{y}_u$. ◇

In other words, the set of basis markings includes the initial marking and the set of all markings reachable by firing observable transitions together with their minimal explanations. All other intermediate markings reachable by the firing of unobservable transitions are disregarded.

Based on Definition 3.4, the following Algorithm 1 iteratively computes basis markings and constructs the BRG. We denote the BRG as an NFA $\mathcal{B} = (\mathcal{M}_B, E, \Delta, M_0)$, where $\mathcal{M}_B$ is the set of *basis markings* of the LPN, all events are observable, $\Delta \subseteq \mathcal{M}_B \times E \times \mathcal{M}_B$ is the transition relation between basis markings, and M_0 is the initial state.

We now briefly explain how Algorithm 1 works. The set $\mathcal{M}_B$ is initialized at $\mathcal{M}_B = \{M_0\}$. For all markings M in $\mathcal{M}_B$ that have not been studied yet, i.e., with no tag, and for all observable transitions t, we check whether the set of minimal e-vectors $Y_{min}(M, t)$ is not empty. If not, we compute the resulting basis markings. This procedure runs iteratively until there is no unchecked marking in $\mathcal{M}_B$. As Algorithm 1 shows, to construct the BRG one only needs to explore the minimal e-vectors for each basis marking and observable transition. This prevents us from exhaustively exploring the RG.

Algorithm 1 Construction of the BRG

Input: A bounded labeled Petri net $G = (N, M_0, E, \ell)$ whose unobservable subnet is acyclic.
Output: The BRG $\mathcal{B} = (\mathcal{M}_B, E, \Delta, M_0)$

```
1: M_B := {M_0} and assign no tag to M_0;
2: while states with no tag exist, do
3:     select a state M ∈ M_B with no tag;
4:     for all t ∈ T_o and Y_min(M, t) ≠ ∅, do
5:         for all y_u ∈ Y_min(M, t), do
6:             M' := M + C_u · y_u + C(·, t);
7:             if M' ∉ M_B, then
8:                 M_B := M_B ∪ {M'};
9:                 assign no tag to M';
10:            end if
11:            Δ := Δ ∪ {(M, ℓ(t), M')};
12:        end for
13:        tag node M "old";
14:    end for
15: end while
16: Remove all tags.
```

Therefore, the complexity of constructing the BRG is lower than that of constructing the RG. It has been shown that in practical cases the size of the BRG can be order of magnitude smaller than that of the RG [21]. Given a word $w \in \mathcal{L}(\mathcal{B}, M_0)$, based on Algorithm 1, if $(M_0, w, M) \in \Delta^*$ then M is the basis marking reachable from M_0 by firing an observable sequence σ_o that produces w, eventually interleaved with some unobservable transitions whose firing is necessary to enable σ_o. We use $\mathcal{M}_b(w) = \mathcal{C}(w) \cap \mathcal{M}_B$ to denote the set of basis markings consistent with w.

Notice that to apply the BRG approach, two assumptions are made:

A1) the LPN G is bounded, and

A2) the unobservable subnet of G is acyclic.

Assumption A1 guarantees that the number of basis markings is finite thus Algorithm 1 can halt and the BRG can be constructed.

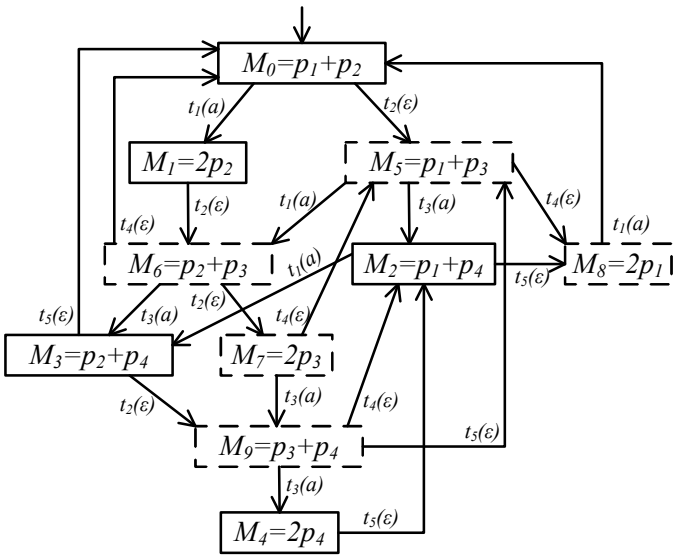

Fig. 2. The RG of the LPN in Fig. 1.

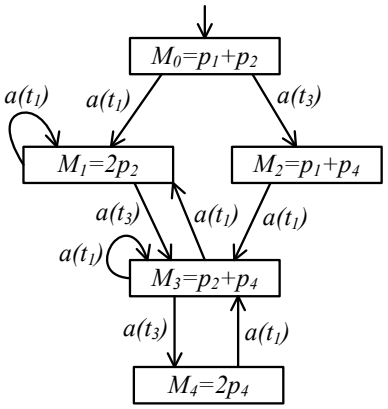

Fig. 3. The BRG of the LPN in Fig. 1.

Assumption A2 allows us to iteratively compute the basis markings and to use the state equation to characterize the set of markings reachable from a basis marking by firing unobservable transitions (as shown in Theorem 3.7).

Example 3.5: Let us consider again the LPN in Fig. 1. It has 10 reachable markings and its RG is shown in Fig. 2. However, there are only 5 basis markings $\mathcal{M}_B = \{M_0 - M_4\}$, and the corresponding BRG is shown in Fig. 3. For clarity of presentation, transitions are added in parenthesis on arcs even if they are not provided by Algorithm 1. Note that they should not be taken into account when establishing whether the BRG is either deterministic or not. ◇

Let us now introduce the following definition that is useful to formalize the main result in this subsection.

Definition 3.6: Given an LPN $G = (N, M_0, E, \ell)$ and a marking $M \in R(N, M_0)$, the *unobservable reach* of M is defined as $\mathcal{U}(M) = \{M' \in \mathbb{N}^m | \exists \sigma_u \in T_u^* : M[\sigma_u\rangle M'\}$. ◇

In simple words, the unobservable reach of a marking M is the set of markings reachable from M by firing only unobservable transitions. In [17], [18], it has been proved that the set of markings consistent with an observation w can be characterized by the unobservable reaches of basis markings in $\mathcal{M}_b(w)$.

Theorem 3.7: [18] Let $G = (N, M_0, E, \ell)$ be an LPN whose unobservable subnet is acyclic. For all $w \in \mathcal{L}(N, M_0)$, it holds

TABLE I
UNOBSERVABLE REACHES OF BASIS MARKINGS IN FIG. 2

Basis Markings	$\mathcal{U}(M)$
M_0	$\{M_0, M_5, M_8\}$
M_1	$\{M_0, M_1, M_5, M_6, M_7, M_8\}$
M_2	$\{M_2, M_8\}$
M_3	$\{M_0, M_2, M_3, M_5, M_8, M_9\}$
M_4	$\{M_2, M_4, M_8\}$

that

$$\begin{aligned}\mathcal{C}(w) &= \bigcup_{M_b \in \mathcal{M}_b(w)} \mathcal{U}(M_b) \\ &= \bigcup_{M_b \in \mathcal{M}_b(w)} \{M \in \mathbb{N}^m | \exists \mathbf{y}_u \in \mathbb{N}^{n_u} : M = M_b + C_u \cdot \mathbf{y}_u\}.\end{aligned}$$

In words, given an LPN whose unobservable subnet is acyclic, and an observation w, a marking M is consistent with w if and only if it belongs to the unobservable reach of a basis marking M_b that is consistent with w. Since the unobservable subnet is acyclic, marking M belonging to $\mathcal{U}(M_b)$ means that $M = M_b + C_u \cdot \mathbf{y}_u$ has a non-negative integer solution $\mathbf{y}_u$.

Example 3.8: Consider again the LPN in Fig. 1. Based on its RG in Fig. 2, the unobservable reaches of basis markings are listed in Table I. One can also compute them by solving the equation in Theorem 3.7.

As discussed above, only markings M_0 to M_4 are basis markings. It can be easily observed that the union of the unobservable reaches of basis markings equals the set of reachable markings. ◇

In the following sections we show how the above definitions and results (particularly Theorem 3.7) may be efficiently used when verifying state-based opacity.

IV. CURRENT-STATE OPACITY

In the framework of LPNs, a secret S is defined as an arbitrary subset of reachable markings, called *secret markings*. It is assumed that the intruder has a complete knowledge of the net system $\langle N, M_0 \rangle$ but only a partial observation of the event occurrences. The current-state opacity property of a system is formally defined as follows.

Definition 4.1: An LPN $G = (N, M_0, E, \ell)$ is said to be *current-state opaque* wrt a secret $S \in R(N, M_0)$ if for all observations $w \in \mathcal{L}(N, M_0)$, $\mathcal{C}(w) \not\subseteq S$ holds. ◇

If an LPN is current-state opaque, it means that for all possible observations, the intruder cannot establish if the current state belongs to the secret.

A. Verifying Current-State Opacity

According to Definition 4.1, to verify current-state opacity of an LPN, we need to check if $\mathcal{C}(w) \not\subseteq S$ holds for all $w \in \mathcal{L}(N, M_0)$, which means that all sets $\mathcal{C}(w)$ need to be computed first. In general, this requires to exhaustively enumerate all sequences of transitions that may fire. For a bounded LPN, this can be done by constructing the DFA equivalent to its RG, which is called *observer*. However, it is known that the complexity of computing a DFA equivalent to a given NFA with $|X|$ states is $\mathcal{O}(2^{|X|})$ [3], [12], [13], [22]. Therefore, if the RG is too large, it may be impossible to construct the observer. In this section, based on the notion of basis markings and explanations, an efficient approach to verifying current-state opacity is proposed. Let us first introduce the following definition.

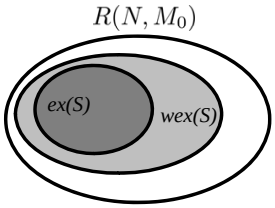

Fig. 4. Inclusion relationships among exposable, weakly exposable, and reachable marking sets.

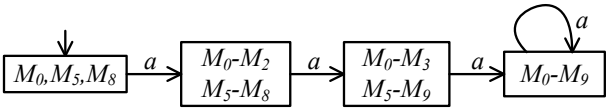

Fig. 5. The observer of the RG.

Definition 4.2: Let $G = (N, M_0, E, \ell)$ be an LPN and $S \in R(N, M_0)$ be a secret. A reachable marking M is said to be *exposable* if it does not belong to the secret, i.e., $M \in R(N, M_0) \setminus S$. The set of exposable markings is $ex(S) = R(N, M_0) \setminus S$. A marking M is said to be *weakly exposable* if there exists a marking $M' \in R(N, M_0)$ such that $M' \in \mathcal{U}(M) \cap ex(S)$. The set of weakly exposable markings is denoted as $wex(S)$. ◇

In simple words, a marking M is weakly exposable if there exists an exposable marking M' that is reachable from it by firing unobservable transitions. Note that the firing sequence of unobservable transitions could be empty. Therefore, all exposable markings are also weakly exposable. Their relations are depicted by the Venn diagram in Fig. 4.

Example 4.3: Consider again the LPN in Fig. 1. Given a secret $S = \{M_2, M_3, M_6, M_7, M_8\}$. The set of exposable markings is $ex(S) = \{M_0, M_1, M_4, M_5, M_9\}$. Since $\mathcal{U}(M_2) \subseteq S$, $\mathcal{U}(M_3) \nsubseteq S$, $\mathcal{U}(M_6) = \{M_0, M_5 - M_8\} \nsubseteq S$, $\mathcal{U}(M_7) = \{M_5, M_7, M_8\} \nsubseteq S$, and $\mathcal{U}(M_8) = \{M_8\} \subseteq S$. Therefore, the set of weakly exposable markings is $wex(S) = \{M_0, M_1, M_3 - M_7, M_9\}$. ◇

From Definitions 4.1 and 4.2, the following fact follows.

Fact 1: G is current-state opaque wrt S iff $\forall w \in \mathcal{L}(N, M_0)$, $\mathcal{C}(w) \cap ex(S) \neq \emptyset$ holds.

Example 4.4: Consider the LPN in Fig. 1. The observer of its RG is shown in Fig. 5. Let $S = \{M_1, M_2, M_5, M_8\}$. The LPN is current-state opaque wrt S since $\forall w \in \mathcal{L}(N, M_0)$, $\mathcal{C}(w) \cap ex(S) \neq \emptyset$. ◇

Based on Theorem 3.7, we derive the following necessary and sufficient condition for current-state opacity.

Theorem 4.5: Let $G = (N, M_0, E, \ell)$ be an LPN whose unobservable subnet is acyclic and $S \in R(N, M_0)$ be a secret. G is current-state opaque wrt S iff $\forall w \in \mathcal{L}(N, M_0)$, $\mathcal{M}_b(w) \cap wex(S) \neq \emptyset$ holds.

Proof: ($\Rightarrow$) Given an arbitrary observation $w \in \mathcal{L}(N, M_0)$, if there exists a basis marking $M_b \in \mathcal{M}_b(w)$ that is weakly exposable, then there is a marking $M \in \mathcal{U}(M_b)$ such that $M \in ex(S)$, and hence $M \in \mathcal{C}(w)$. This indicates that $\mathcal{C}(w) \cap ex(S) \neq \emptyset$. By Fact 1, the system is current-state opaque wrt S.

($\Leftarrow$) Assume that there is an observation $w \in \mathcal{L}(N, M_0)$ and none of the basis markings consistent with w are weakly exposable, i.e., $\forall M_b \in \mathcal{M}_b(w)$, $\mathcal{U}(M_b) \subseteq S$. Based on Theorem 3.7, all markings consistent with observation w belong to the secret, i.e., $\mathcal{C}(w) \cap ex(S) = \emptyset$. By Fact 1, the LPN is not current-state opaque. ■

As a result, instead of exhaustively computing the sets $\mathcal{C}(w)$ for all $w \in \mathcal{L}(N, M_0)$, according to Theorem 4.5, to determine if an LPN is current-state opaque, we only need to compute the set of basis markings $\mathcal{M}_b(w)$ for all observations $w \in \mathcal{L}(N, M_0)$ and to check if it contains a weakly exposable basis marking.

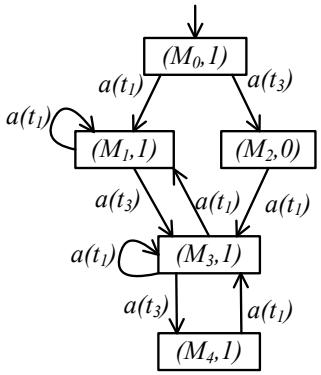

Fig. 6. BRG $\mathcal{B}_c$ for current-state opacity.

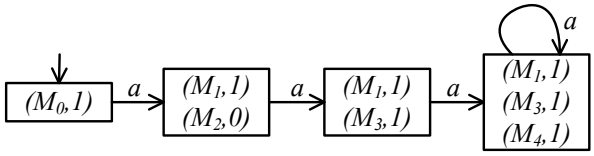

Fig. 7. Current-state basis observer of the BRG $\mathcal{B}_c$ in Fig.6.

B. BRG for Current-State Opacity

In this section, we propose a modified BRG that enables us to verify current-state opacity more efficiently.

Given a bounded LPN G and a secret S, with each node $M_b \in \mathcal{M}_B$ of the BRG $\mathcal{B} = (\mathcal{M}_B, E, \Delta, M_0)$ we associate a binary scalar $\alpha(M_b)$ defined as follows:

$$\alpha(M_b) = \begin{cases} 1 & \text{if } M_b \text{ is weakly exposable;} \\ 0 & \text{otherwise.} \end{cases} \tag{1}$$

The BRG for current-state opacity is denoted as $\mathcal{B}_c = (\tilde{\mathcal{M}}_B, E, \Delta, (M_0, \alpha(M_0)))$, where $\tilde{\mathcal{M}}_B \subseteq \mathcal{M}_B \times \{0,1\}$.

For all observations w, $\mathcal{M}_b(w)$ can be computed by converting the obtained BRG into its equivalent DFA by a standard *determinization procedure* [22]: we do not present it here for the sake of brevity but illustrate it via Example 4.6. In the resulting DFA, called *current-state basis observer*, each state is a subset of $\tilde{\mathcal{M}}_B$ consistent with an observation. According to Theorem 4.5, if all states of the observer have at least a pair $(M, \alpha(M))$ with $\alpha(M) = 1$, the LPN is current-state opaque wrt S; otherwise, the LPN is not current-state opaque.

The number of states of the current-state basis observer in the worst case is $2^{|\mathcal{M}_B|} - 1$. Therefore, the space complexity of the proposed approach is $\mathcal{O}(2^{|\mathcal{M}_B|})$. However, since the RG-based approach has a space complexity of $\mathcal{O}(2^{|R(N,M_0)|})$, and $|\mathcal{M}_B|$ is typically greatly smaller than $|R(N, M_0)|$, we conclude that the BRG-based method is practically much more efficient. Some numerical results that validate this are given in Section VI. Moreover, once the current-state basis observer is constructed, there is no need to reconstruct it when the secret S changes. If S is changed to S', all we need is to update the value of $\alpha(M)$ in the current-basis observer for each basis marking M.

Example 4.6: Consider the LPN in Fig. 1 and the same secret $S = \{M_2, M_3, M_6, M_7, M_8\}$ in Exmaple 4.3. By Eq. (1), the BRG for current-state opacity is illustrated in Fig. 6 and the corresponding observer is shown in Fig. 7. Since all nodes of the observer have at least a pair $(M, \alpha(M))$ with $\alpha(M) = 1$, then by Theorem 4.5, the LPN is current-state opaque wrt S. $\diamond$

The following proposition provides a sufficient but not necessary condition for verifying current-state opacity without constructing the observer of the BRG.

Proposition 4.7: Let $G = (N, M_0, E, \ell)$ be an LPN whose unobservable subnet is acyclic and $S \in R(N, M_0)$ be a secret. If all basis markings $M_b \in \mathcal{M}_B$ of G are weakly exposable, i.e., $\mathcal{M}_B \subseteq wex(S)$, the system is current-state opaque wrt S.

Proof: Since all basis markings are weakly exposable, namely, for all observations $w \in \mathcal{L}(N, M_0)$, there is an exposable marking in $\mathcal{C}(w)$, according to Theorem 4.5, the LPN is current-state opaque. ■

If all states of the BRG have $\alpha(\cdot) = 1$, the LPN is current-state opaque; otherwise, current-state opacity requires further analysis. The result of Example 4.6 shows that the condition in Proposition 4.7 is not necessary for current-state opacity: even though in the BRG there is basis markings $M_2 \in \mathcal{M}_b(a)$ that is not weakly exposable, the LPN is current-state opaque wrt S. When $w = a$ is observed, consistent markings reached from basis marking M_2 belong to the secret. The intruder, however, still does not know for sure if the current state is in the secret, since the current state could be the one that is reachable from $M_1 \in \mathcal{M}_b(a)$ and that does not belong to the secret. For example, the current state could be M_5.

C. Secrets Described by GMECs

Let us now discuss some special cases for which the computation of the scalars $\alpha(M)$ could be simplified. To verify if a marking M is weakly exposable requires to test if there exists a nonsecret marking M' that belongs to its unobservable reach. This can be done exhaustively by solving the reachability problem in its unobservable subnet. If the unobservable subnet is acyclic, this can be done by checking if $M' = M + C_u \cdot \mathbf{y}_u$ has a nonnegative integer solution. However, under special assumptions on the secret and/or the net structure, there may exist a more efficient way to do that. In this subsection we show that such is the case when the secret S is described by a set of *generalized exclusion mutual constraints* (GMECs) [24]. It is well-known that GMECs describe interesting subsets of the state space of a net and many interesting state-based specifications can be represented by GMECs. Furthermore, they allow one to solve analysis and control problems by means of simple linear algebraic tools [25], [26], [27], [28]. We show that in such a case determining if a basis marking is weakly exposable does not require constructing the reachability set of the unobservable subnet, but only finding if a given set of linear integer constraints admits a feasible solution.

Definition 4.8: [24] Given a net N, a *single GMEC* is a pair $(\mathbf{w}, k)$, where $\mathbf{w} \in \mathbb{Z}^m, k \in \mathbb{N}$, defining a set of legal markings $\mathcal{M}_{(\mathbf{w},k)} = \{M \in \mathbb{N}^m \mid \mathbf{w}^T \cdot M \leq k\}$. A *conjunctive GMEC* is a pair (W, K) where $W \in \mathbb{Z}^{r \times m}, K \in \mathbb{N}^r$ defining a set of legal markings $\mathcal{M}_{(W,K)} = \{M \in \mathbb{N}^m \mid W^T \cdot M \leq K\}$. Given a conjunctive GMEC (W, K), we use $(\mathbf{w}_i, k_i)$ to denote the single GMEC $(W(i, \cdot), K(i))$. ◇

In this subsection we assume that the secret is described by a conjunctive GMEC, i.e.,

$$S = \{M \in \mathbb{N}^m \mid W^T \cdot M \leq K\}.$$

Definition 4.9: Let $M \in R(N, M_0)$ be a marking of an LPN $G = (N, M_0, E, \ell)$, $S = \{M \in \mathbb{N}^m | W \cdot M \leq K\}$ be a secret and $(\mathbf{w}_i, k_i)$ be the i-th GMEC of the secret. The (i, M)-*constraint set* is defined as

$$\mathcal{Y}_i(M) = \begin{cases} M' = M + C_u \cdot \mathbf{y}_u \\ \mathbf{w}_i^T \cdot M' > k_i \\ \mathbf{y}_u \in \mathbb{N}^{n_u} \\ M' \in \mathbb{N}^m \end{cases}$$

◇

Proposition 4.10: Let $G = (N, M_0, E, \ell)$ be an LPN whose unobservable subnet is acyclic and $S = \{M \in \mathbb{N}^m | W \cdot M \leq K\}$ be a secret. A reachable marking $M \in R(N, M_0)$ is weakly exposable iff there exists a GMEC $(\mathbf{w}_i, k_i)$ of the secret such that the corresponding (i, M)-constraint set is feasible.

Proof: ($\Rightarrow$) Given a marking $M \in R(N, M_0)$, if there exists a GMEC whose (i, M)-constraint set is feasible, then there exists a marking M' that is reachable from M by firing unobservable transitions and that does not belong to the secret, i.e., M is weakly exposable.

($\Leftarrow$) If M is weakly exposable, then there exists a marking $M' \notin S$ with $M[\sigma\rangle M'$, $\sigma \in T_u^*$. Therefore, there exists a GMEC $(\mathbf{w}_j, k_j)$ such that M' and vector $y = \pi(\sigma)$ is a solution to the (j, M)-constraint set. ■

In other words, when the secret is described by GMECs, verifying if a marking is weakly exposable can be done by solving ILPPs. Therefore, the construction of BRG for current-state opacity requires solving $r \cdot z$ ILPPs, where r is the number of GMECs and z is the number of basis markings. Moreover, for some net structures the complexity of constructing the BRG can be further reduced by relaxing an ILPP into a linear programming problem (LPP).

Lemma 4.11: [29] If A is a totaly unimodular matrix[3] and b is a vector of integers, then a linear programming problem of the form $\min \{c \cdot x \mid A \cdot x \geq b, x \geq 0\}$ or $\max \{c \cdot x \mid A \cdot x \leq b\}$ has an integer optimal solution, for any c.

Proposition 4.12: Let $G = (N, M_0, E, \ell)$ be an LPN whose unobservable subnet is acyclic, the corresponding incidence matrix C_u be a totally unimodular matrix, and $S = \{M \in \mathbb{N}^m | W \cdot M \leq K\}$ be a secret. A reachable marking $M \in R(N, M_0)$ is weakly exposable iff there exists a GMEC $(\mathbf{w}_i, k_i)$ whose (i, M)-constraint set $\mathcal{Y}_i(M)$ is feasible for $y \in \mathbb{R}^{n_u}_{\geq 0}$ and $M' \in \mathbb{R}^m_{\geq 0}$.

Proof: Trivially follows from Proposition 4.10 and Lemma 4.11. ■

Note that there exist many interesting classes of nets whose incidence matrix is totally unimodular: examples are marked graphs and state machines [30].

Example 4.13: Consider again the LPN in Fig. 1 whose unobservable subnet is a state machine. Let the secret be $S = \{M \in \mathbb{N}^4 | M(p_1) + M(p_4) \geq 2\}$, i.e., $W = [\ -1 \quad 0 \quad 0 \quad -1\ ]$ and $K = -2$. Since the observer of the BRG has been constructed in Example 4.6, only the value $\alpha(\cdot)$ of each basis marking needs to be updated. By solving the LPP, we obtain $\alpha(M_0) = 1$, $\alpha(M_1) = 1$, $\alpha(M_2) = 0$, $\alpha(M_3) = 1$, and $\alpha(M_4) = 0$. According to Theorem 4.5, the LPN is current-state opaque wrt the secret S. ◇

Notice that the observer of the BRG still needs to be constructed first. Providing a necessary but not sufficient condition for current-state opacity, Proposition 4.14 can be applied without constructing the observer and only requires solving LPPs.

Proposition 4.14: Let $G = (N, M_0, E, \ell)$ be an LPN whose unobservable subnet is acyclic and $S = \{M \in \mathbb{N}^m | W \cdot M \leq K\}$ be a secret. The LPN is not current-state opaque if for all basis markings $M_b \in \mathcal{M}_B$ and all GMECs $(\mathbf{w}_i, k_i)$, the (i, M_b)-constraint sets $\mathcal{Y}_i(M_b)$ are not feasible for $y \in \mathbb{R}^{n_u}_{\geq 0}$ and $M \in \mathbb{R}^m_{\geq 0}$.

Proof: Given a basis marking M_b, if for all GMECs $(\mathbf{w}_i, k_i)$ the (i, M_b)-constraint sets $\mathcal{Y}_i(M_b)$ is not feasible for $y \in \mathbb{R}^{n_u}_{\geq 0}$ and $M \in \mathbb{R}^m_{\geq 0}$, they are not feasible for $y \in \mathbb{N}^{n_u}_{\geq 0}$ and $M \in \mathbb{N}^m_{\geq 0}$ either. According to Proposition 4.10, basis marking M_b is not weakly exposable. Since none of the basis markings is weakly exposable, by Theorem 4.5, the LPN is not current-state opaque. ■

D. Secrets with No Weakly Exposable Markings

In this subsection we focus on a special class of secrets. More precisely, given an LPN, we assume that the secret satisfies the following additional assumption:

[3]A matrix A is totally unimodular if each subdeterminant of A is 0, 1, or -1.

A3) none of the secret markings is weakly exposable, i.e., $M \in S \Rightarrow \forall M' \in \mathcal{U}(M) : M' \in S$ holds.

This means that if M is a secret marking, all markings in the unobservable reach of M are secret markings as well. This assumption allows to simplify the verification of current-state opacity (as shown by Theorem 4.15). Moreover, it is useful when studying the case of initial-state opacity in Section V-B.

Theorem 4.15: Let $G = (N, M_0, E, \ell)$ be an LPN whose unobservable subnet is acyclic and S be a secret satisfying Assumption A3. The LPN G is current-state opaque wrt S iff $\forall w \in \mathcal{L}(N, M_0)$, $\mathcal{M}_b(w) \cap ex(S_B) \neq \emptyset$ holds, where $ex(S_B) = \mathcal{M}_B \cap ex(S)$.

Proof: ($\Rightarrow$) Let $M_b \in \mathcal{M}_b(w) \cap ex(S_B)$. Therefore, $M_b \in \mathcal{C}(w)$ and $\mathcal{C}(w) \cap ex(S) \neq \emptyset$, i.e., G is current-state opaque wrt S.

($\Leftarrow$) Assume G is opaque. Then $\forall w \in \mathcal{L}(N, M_0), \mathcal{C}(w) \cap ex(S) \neq \emptyset$, i.e., $\exists M \in \mathcal{C}(w) : M \in ex(S)$. According to Theorem 3.7, $\exists M_b \in \mathcal{M}_B \cap ex(S) : M \in \mathcal{U}(M_b)$, otherwise, Assumption A3 would be violated. Therefore, $\mathcal{M}_b(w) \cap ex(S_B) \neq \emptyset$. ■

Example 4.16: Consider again the LPN in Fig. 1. Consider a secret $S = \{M_0, M_2, M_5, M_8, M_9\}$ that satisfies Assumption A3. Then we have $S_B = \{M_0, M_2\}$ and $ex(S_B) = \{M_1, M_3, M_4\}$. Based on the observer of the BRG in Fig. 7, $\forall w \in \mathcal{L}(N, M_0), \mathcal{M}_b(w) \cap ex(S_B) \neq \emptyset$, and therefore, the LPN is current-state opaque wrt S.

In other words, if Assumption A3 is satisfied, then current-state opacity can be verified by simply checking if each state of the current-state basis observer contains at least one basis marking which is exposable (rather than *weakly* exposable). This can be easily done by checking if $\mathcal{M}_b(w) \cap (R(N, M_0) \setminus S) = \emptyset$.

We finally point out that Theorem 4.15 could also be useful when the secret does not satisfy Assumption A3. Indeed, given an arbitrary system G and a secret S, the following proposition shows that we can always find another secret S'' which satisfies Assumption A3 and G has the same current-state opacity property wrt both S and S'', and hence Theorem 4.15 can be applied.

Proposition 4.17: Let $G = (N, M_0, E, \ell)$ be an LPN whose unobservable subnet is acyclic, and $S \in R(N, M_0)$ be a secret. G is current-state opaque wrt S iff G is current-state opaque wrt S'', where $S'' = S \setminus S'$ and $S' = wex(S) \cap S$.

Proof: Assume that G is current-state opaque wrt S''. Therefore, $\forall w \in \mathcal{L}(N, M_0), \mathcal{C}(w) \cap ex(S'') \neq \emptyset$. Suppose that G is not current-state opaque wrt S, i.e., $\exists w \in \mathcal{L}(N, M_0) : \mathcal{C}(w) \cap ex(S) = \emptyset$. Since $ex(S'') = ex(S) \cup S'$, we have $\mathcal{C}(w) \cap ex(S'') = (\mathcal{C}(w) \cap ex(S)) \cup (\mathcal{C}(w) \cap S') = \mathcal{C}(w) \cap S' \neq \emptyset$. Let $M \in \mathcal{C}(w) \cap S'$. Therefore, there exists a marking $M' \in \mathcal{U}(M) : M' \in ex(S)$, and thus $M' \in \mathcal{C}(w) \cap ex(S)$, i.e., G is opaque wrt S.

It is clear that $ex(S) \subseteq ex(S')$ and $ex(S) \subseteq ex(S'')$, since $S' \subseteq S$ and $S'' \subseteq S$. Furthermore, since G is current-state opaque wrt S, i.e., $\mathcal{C}(w) \cap ex(S) \neq \emptyset$, it holds $\mathcal{C}(w) \cap ex(S') \neq \emptyset$ and $\mathcal{C}(w) \cap ex(S'') \neq \emptyset$. Thus G is current-state opaque wrt both S' and S'', respectively. ■

Proposition 4.17 indicates that given a system G and a secret S, to verify if G is current-state opaque wrt S we can pretreat the secret S by simply removing all weakly exposable markings in S to get S'' that satisfies Assumption A3, and then verify if G is current-state opaque wrt S'' using Theorem 4.15.

Example 4.18: Consider again the LPN in Fig.1. Let $S = \{M_1, M_2, M_5, M_8\}$. The secret does not satisfy Assumption A3 since M_1 is weakly exposable. The secret can be partitioned into $S = S' \cup S''$, where $S' = \{M_1\}$ and $S'' = \{M_2, M_5, M_8\}$. Therefore, $S''_B = \{M_2\}$ and $ex(S''_B) = \{M_0, M_1, M_3, M_4\}$. Since $\forall w \in \mathcal{L}(N, M_0)$, $\mathcal{M}_b(w) \cap ex(S''_B) \neq \emptyset$ holds, the LPN is current-state opaque wrt S'', or equivalently, by Proposition 4.17, the LPN is current-state opaque wrt S. ◇

E. Uncertainty on the Initial Marking

In this section we focus on the problem of verifying current-state opacity under the more general assumption that the intruder has only partial knowledge of the initial marking of the net. In more detail, we assume that the intruder simply knows that the initial marking M_0 belongs to a set $\mathcal{M}_0 \subseteq \mathcal{M}_B$, i.e., $M_0 \in \mathcal{M}_0$. Clearly, this is equivalent to assume that the set of possible initial markings for the intruder is $\hat{\mathcal{M}}_0 = \bigcup_{M_b \in \mathcal{M}_0} \mathcal{U}(M_b)$. Obviously, if a Petri net system is current-state opaque wrt a secret when the intruder knows the initial marking M_0, a fortiori it is current-state opaque when the intruder simply knows that the initial marking belongs to set $\hat{\mathcal{M}}_0$. In this subsection, we show that current-state opacity with the above ambiguity on the initial marking can be verified by simply modifying the current-state basis observer.

Given an observation w, we have defined $\mathcal{C}(w)$ (in Sec. II.B) as the set of markings consistent with w, assuming that M_0 is known. Now, we generalize this notion to a given set of initial markings $\hat{\mathcal{M}}_0$, and define

$$\hat{\mathcal{C}}(w) = \{M \in \mathbb{N}^m | \exists M' \in \hat{\mathcal{M}}_0, \exists \sigma \in T^* : \\ M'[\sigma\rangle M \text{ and } \ell(\sigma) = w\},$$

i.e., $\hat{\mathcal{C}}(w)$ is the set of possible current markings estimated by the intruder when observing w. Clearly, if $M_0 \in \mathcal{M}_0$ it holds $\hat{\mathcal{C}}(w) \supseteq \mathcal{C}(w)$, hence the condition in Theorem 4.5 is no longer necessary. Namely, the system could be current-state opaque even if there exists $w \in \mathcal{L}(N, M_0)$ such that $\mathcal{M}_b(w) \cap wex(S) = \emptyset$. If the initial state of the current-state basis observer is initialized at $\mathcal{M}_0$ directly, words that would never be generated by the LPN, i.e., words in $\mathcal{L}(N, \hat{\mathcal{M}}_0) \setminus \mathcal{L}(N, M_0)$, will be generated by the observer. Note that $\mathcal{L}(N, \hat{\mathcal{M}}_0) = \mathcal{L}(N, \mathcal{M}_0)$. As a result, current-state opacity cannot be verified looking at the current-state basis observer. To restrict the language of the current-basis observer to the language of the LPN and separately denote estimations made on the basis of false initial markings $\mathcal{M}_0 \setminus \{M_0\}$ and estimations made on the basis of the real initial marking M_0, as formalized in the following definition, we introduce an extended observer which is the synthesis of two BRG observers, initialized at $\mathcal{M}_0 \setminus M_0$ and M_0, respectively.

Definition 4.19: Let $G = (N, M_0, E, \ell)$ be a bounded LPN whose unobservable subnet is acyclic, $S \in R(N, M_0)$ be a secret, $\mathcal{B}_c = (\tilde{\mathcal{M}}_B, E, \Delta, (M_0, \alpha(M_0)))$ be the corresponding BRG for current-state opacity and $\mathcal{M}_0$ be the intruder's knowledge about the initial marking. The *extended observer* of the BRG is a DFA $\mathcal{V} = (Q, E, \delta, q_0)$, where $Q \subseteq 2^{\tilde{\mathcal{M}}_B} \times 2^{\tilde{\mathcal{M}}_B}$ and $q_0 = (\hat{\mathcal{X}}_0, \mathcal{X}_0)$ with $\hat{\mathcal{X}}_0 = \{(M, \alpha(M)) | M \in \mathcal{M}_0 \setminus \{M_0\}\}$ and $\mathcal{X}_0 = \{(M_0, \alpha(M_0))\}$. The transition function δ is defined as follows: for $e \in E$ and $(\hat{\mathcal{X}}_i, \mathcal{X}_i) \in Q$, if $\exists (M, \alpha(M)) \in \mathcal{X}_i : e$ is defined at $(M, \alpha(M))$, then $((\hat{\mathcal{X}}_i, \mathcal{X}_i), e, (\hat{\mathcal{X}}_j, \mathcal{X}_j)) \in \delta$, where $\hat{\mathcal{X}}_j = \{x' \in \tilde{\mathcal{M}}_B | \exists x \in \hat{\mathcal{X}}_i : \Delta(x, e) = x'\}$ and $\mathcal{X}_j = \{x' \in \tilde{\mathcal{M}}_B | \exists x \in \mathcal{X}_i : \Delta(x, e) = x'\}$. $\diamond$

In plain words, the extended observer characterizes the possible current markings estimated by the intruder. It is first initialized with the uncertainty of the initial marking. To verify current-state opacity we only need to consider the language $\mathcal{L}(N, M_0)$ generated by the LPN, since a word w which can only be generated by some false initial marking will not occur in the actual evolution of the system. The set $\mathcal{X}$ denotes the intruder's estimation with knowledge of the initial marking M_0, while the set $\hat{\mathcal{X}}$ denotes additional estimated markings introduced by uncertainties about the initial marking $\mathcal{M}_0 \setminus \{M_0\}$. Therefore, given an observation $w \in \mathcal{L}(N, M_0)$, the intruder's estimation of the current state is $\hat{\mathcal{X}} \cup \mathcal{X}$, where $(q_0, w, (\hat{\mathcal{X}}, \mathcal{X})) \in \delta$. As a particular case, if $\mathcal{M}_0 = \{M_0\}$, then the intruder knows exactly the initial marking and all the states of the corresponding extended observer have $\hat{\mathcal{X}} = \emptyset$. Therefore, the complexity of constructing the extended observer is $\mathcal{O}(4^{|\mathcal{M}_B|})$.

Theorem 4.20: Let $G = (N, M_0, E, \ell)$ be a bounded LPN whose unobservable subnet is acyclic, $S \in R(N, M_0)$ be a secret and $\mathcal{V} = (Q, E, \delta, q_0)$ be the corresponding extended observer. The LPN is current-state opaque wrt S iff for all states

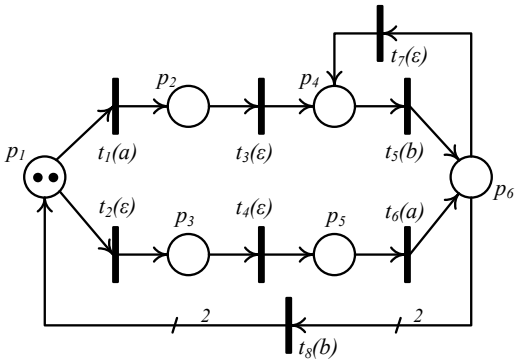

Fig. 8. An LPN whose initial marking is not exactly known by the intruder.

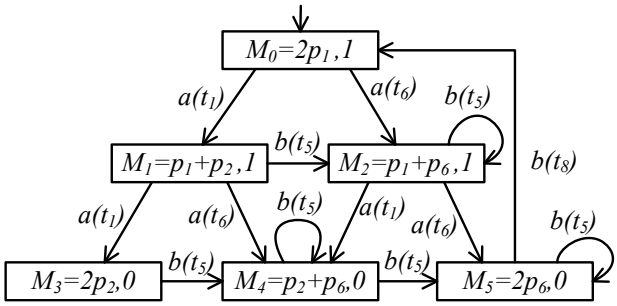

Fig. 9. BRG of the LPN in Example 4.21.

$(\hat{\mathcal{X}}, \mathcal{X}) \in Q$, $\exists (M, \alpha(M)) \in \hat{\mathcal{X}} \cup \mathcal{X}$: $\alpha(M) = 1$.

Proof: Let $(\hat{\mathcal{X}}, \mathcal{X})$ be the state reachable by firing a sequence w, i.e., $(q_0, w, (\hat{\mathcal{X}}, \mathcal{X})) \in \delta$. According to Definition 4.19, the set $\hat{\mathcal{X}} \cup \mathcal{X}$ corresponding to $(\hat{\mathcal{X}}, \mathcal{X})$ is a subset of $\mathcal{M}_B \times \{0, 1\}$ whose markings belong to $\mathcal{C}(w)$. If $\exists (M, \alpha(M)) \in \hat{\mathcal{X}} \cup \mathcal{X}$: M is weakly exposable, for observation w there exists a marking $M' \in \mathcal{U}(M)$ such that $M' \in ex(S)$, i.e., $\mathcal{C}(w) \cap ex(S) \neq \emptyset$. Since this is true for all states of Q, i.e., for all observations $w \in \mathcal{L}(N, M_0)$, the LPN is current-state opaque. Assume there is a state $(\hat{\mathcal{X}}, \mathcal{X})$ of Q reachable by w and $\forall (M, \alpha(M)) \in \hat{\mathcal{X}} \cup \mathcal{X}$: M is not weakly exposable. Therefore, by Theorem 3.7, we have $\mathcal{C}(w) \cap ex(S) = \emptyset$. We conclude that the LPN is not current-state opaque. ■

Example 4.21: Let us consider the LPN in Fig. 8. The BRG of the LPN wrt secret $S = \{M \in \mathbb{N}^6 | M(p_3) + M(p_5) \leq 0\}$ is shown in Fig.9. Assume that the uncertainty about the initial marking is $\mathcal{M}_0 = \{M_0, M_2\}$. The extended observer, as in Definition 4.19, is shown in Fig.10. There are states $(\emptyset; \{(M_3, 0), (M_4, 0), (M_5, 0)\})$ and $(\emptyset; \{(M_4, 0), (M_5, 0)\})$ where all basis markings in $\hat{\mathcal{X}} \cup \mathcal{X}$ satisfy $\alpha(\cdot) = 0$, and therefore, the LPN is not current-state opaque wrt S under $\mathcal{M}_0$. ◇

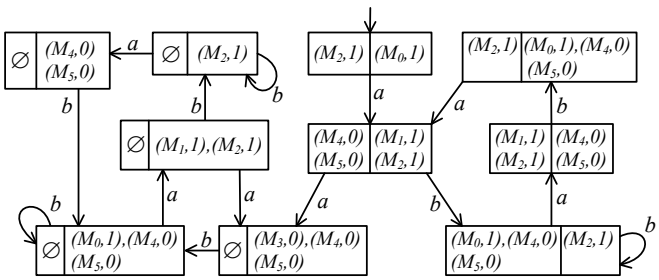

Fig. 10. The extended observer of the BRG in Fig.9.

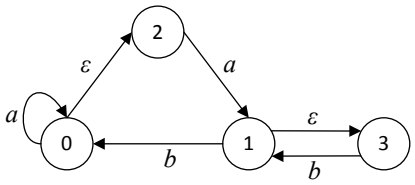

Fig. 11. An automaton $\mathcal{A}$.

V. Initial-State Opacity

In this section another important state-based opacity problem is addressed: *initial-state opacity*. A system is said to be initial-state opaque if the intruder is never able to establish if the initial state belongs to a given secret based on its observation of the system's evolution. Assuming that the intruder knows the net system $\langle N, M_0\rangle$, we extend the notion of initial-state opacity in [8] to Petri nets. It is assumed that originating from M_0, the net system could have reached any marking $M \in R(N, M_0)$ before the observation starts. In this sense, M is the initial state of the observed evolution, not M_0. Thus the definition of observations can be extended to strings $w \in \mathcal{L}(N, R(N, M_0))$. Given an observation w, we define

$$\mathcal{I}(w) = \{M \in R(N, M_0) | \exists \sigma \in T^* : M[\sigma\rangle \text{ and } \ell(\sigma) = w\}$$

as *the set of markings generating* w. Initial-state opacity in Petri nets is formally defined as follows.

Definition 5.1: Let $G = (N, M_0, E, \ell)$ be an LPN and $S \subseteq R(N, M_0)$ be a secret. G is said to be initial-state opaque wrt S if $\forall w \in \mathcal{L}(N, R(N, M_0))$, $\mathcal{I}(w) \not\subseteq S$ holds. $\diamond$

In simple words, an LPN is initial-state opaque if for any observation w, the set of markings generating w is not included in the secret. Note that Definition 5.1 could be applied to either bounded or unbounded Petri net systems.

We also point out that since for $w \in \mathcal{L}(N, R(N, M_0)) \setminus \mathcal{L}(N, S)$, $\mathcal{I}(w) \not\subseteq S$ holds, there is no difference in considering all observations $w \in \mathcal{L}(N, R(N, M_0))$ or only $w \in \mathcal{L}(N, S)$ in Definition 5.1.

A. Initial State Estimation

Given an observation w, the problem of reconstructing the set of possible initial states that can generate w is called *initial-state estimation* [8], [9]. Namely, in the framework of Petri nets the problem is to compute $\mathcal{I}(w)$ for an observed $w \in \mathcal{L}(N, R(N, M_0))$. From Definition 5.1, we have the following fact.

Fact 2: G is initial-state opaque wrt S iff $\forall w \in \mathcal{L}(N, R(N, M_0))$, $\mathcal{I}(w) \cap ex(S) \neq \emptyset$ holds.

In this section we first briefly recall a technique that is used to estimate the set of initial states in automata. In [9] a DFA called an *initial-state estimator* is proposed based on the notion of *reverse automaton*. Given a NFA $\mathcal{A} = (X, E, \Delta)$ where no initial state is specified, the corresponding initial-state estimator $\mathcal{A}^e = (\tilde{\mathcal{X}}, E, \Delta_e, \hat{X}_0)$ is the observer of its reverse automaton $\mathcal{A}^r$, i.e., the automaton obtained by reversing all arcs in $\mathcal{A}$, where $\tilde{\mathcal{X}} \subseteq 2^X$ and $\hat{X}_0 = X$. In $\mathcal{A}^e$, the state reached by a word w' is the set of states from which the word w can be generated in $\mathcal{A}$, where w' is the reverse of w.

Theorem 5.2: [9] Let $\mathcal{A} = (X, E, \Delta)$ be a NFA, $\mathcal{A}^e = (\tilde{\mathcal{X}}, E, \Delta_e, \hat{X}_0)$ be its initial-state estimator, and $w \in \mathcal{L}(\mathcal{A}, X)$ be a word in $\mathcal{A}$. There exist $x, x' \in X : (x, w, x') \in \Delta$ iff $\exists \hat{X}, \hat{X}' \in \tilde{\mathcal{X}} : x \in \hat{X}, x' \in \hat{X}'$ and $(\hat{X}', w', \hat{X}) \in \Delta_e$, where w' is the reverse of w.

Since building a reverse automaton has polynomial complexity, the complexity of constructing the initial-state estimator is $\mathcal{O}(2^{|X|})$.

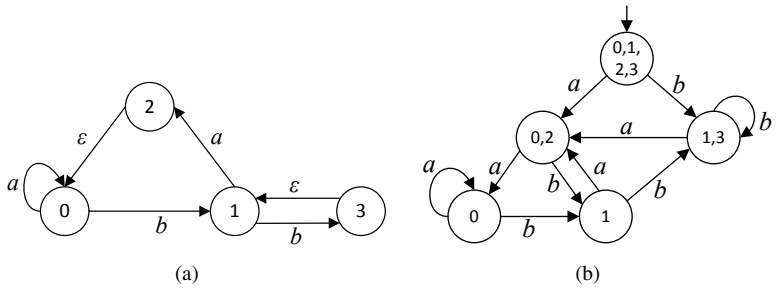

Fig. 12. (a) The reverse automata $\mathcal{A}^r$ and (b) the initial-state estimator $\mathcal{A}^e$.

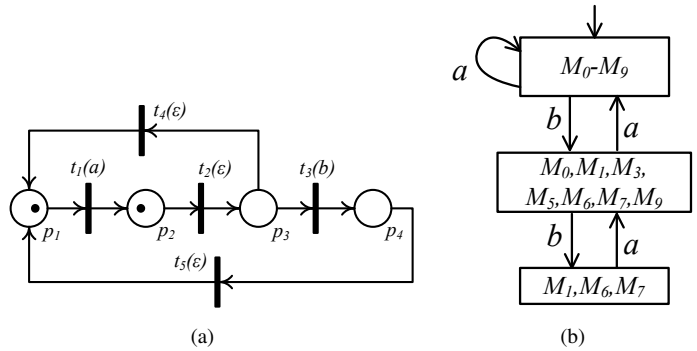

Fig. 13. (a) An LPN where t_3 is labeled by b and (b) The initial-state estimator of the RG.

Example 5.3: Let us consider the automaton $\mathcal{A}$ in Fig. 11 presented in [8]. The set of initial states is unknown. Its reverse automaton $\mathcal{A}^r$ and the corresponding observer $\mathcal{A}^e$, i.e., the initial-state estimator, are shown in Figs. 12(a) and 12(b), respectively. Consider a word $w = ab$. The state reached in the estimator by the reverse word $w' = ba$ is $\{0, 2\}$, which indicates that the state that can generate $w = ab$ in $\mathcal{A}$ is either State 0 or State 2. ◇

B. Verification of Initial-State Opacity

Since the RG of a bounded LPN is finite, the technique applied to automata can also be used to verify initial-state opacity of bounded Petri nets. Let $\mathcal{A}^e = (\tilde{\mathcal{X}}, E, \Delta_e, \hat{X}_0)$ be the initial-state estimator of the RG. If $\exists w' \in E^*$ and $\hat{X} \in \tilde{\mathcal{X}}$ such that $(\hat{X}_0, w', \hat{X}) \in \Delta_e$, then in the LPN we have $\mathcal{I}(w) = \hat{X}$, where w is the reverse of w'.

Corollary 5.4: Given a bounded LPN $G = (N, M_0, E, \ell)$ and a secret $S \subseteq R(N, M_0)$, let $\mathcal{A}^e = (\tilde{\mathcal{X}}, E, \Delta_e, \hat{X}_0)$ be the initial-state estimator of the RG. G is initial-state opaque wrt S iff $\forall \hat{X} \in \tilde{\mathcal{X}}$, $\hat{X} \cap ex(S) \neq \emptyset$ holds.

Proof: Trivially follows from Definition 5.1 and Theorem 5.2. ■

Therefore, by constructing the initial-state estimator of the RG, the complexity of verifying initial-state opacity in bounded Petri nets is $\mathcal{O}(2^{|R(N,M_0)|})$.

Example 5.5: Consider the LPN in Fig. 13(a) whose only difference wrt Fig. 1 is the label assigned to transition t_3 (b rather than a). The initial-state estimator of its RG is shown in Fig. 13(b). Consider a secret $S_1 = \{M_1, M_5, M_6, M_7, M_9\}$ and an observation $w = bbaa$. The state reached by $w' = aabb$, the reverse of w, in the estimator is $\{M_1, M_6, M_7\}$, i.e., $\mathcal{I}(bbaa) = \{M_1, M_6, M_7\}$. Since $\mathcal{I}(bbaa) \cap ex(S_1) = \emptyset$, the LPN is not initial-state opaque wrt S_1.

Consider another secret $S_2 = \{M_1, M_7\}$. Then the LPN is initial-state opaque wrt S_2, since $\forall w \in \mathcal{L}(N, R(N, M_0))$, $\mathcal{I}(w) \cap ex(S_2) \neq \emptyset$. ◇

In the rest of this section an efficient approach to verifying initial-state opacity is proposed based on BRG analysis. Given an LPN $G = (N, M_0, E, \ell)$ and an observation $w \in \mathcal{L}(N, R(N, M_0))$, we denote by $\mathcal{I}_b(w) = \mathcal{I}(w) \cap \mathcal{M}_B$ the set of basis

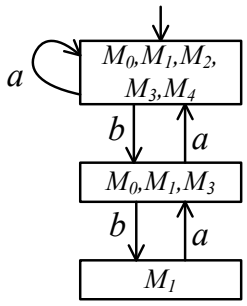

Fig. 14. The initial-state estimator of the BRG in Fig. 3.

markings generating w.

Proposition 5.6: Let $G = (N, M_0, E, \ell)$ be an LPN whose unobservable subnet is acyclic and $S \in R(N, M_0)$ be a secret. If G is initial-state opaque wrt S, then $\forall w \in \mathcal{L}(N, R(N, M_0))$, $\mathcal{I}_b(w) \cap wex(S) \neq \emptyset$ holds, where $wex(S)$ is the set of weakly exposable markings (Def. 4.2).

Proof: Since G is initial-state opaque wrt S, $\forall w \in \mathcal{L}(N, S)$, there exists an exposable marking $M \in ex(S)$ such that $w \in \mathcal{L}(N, M)$. Moreover, according to Theorem 3.7, $\exists M_b \in \mathcal{M}_B : M \in \mathcal{U}(M_b)$. Therefore, $w \in \mathcal{L}(N, M_b)$ and $M_b \in wex(S)$, i.e., $M_b \in \mathcal{I}_b(w)$. ■

The following example shows that Proposition 5.6 provides a necessary but not sufficient condition for initial-state opacity.

Example 5.7: Consider the LPN and the secret S_1 in Example 5.5. According to Table I (it applies to both the nets in Figs. 1 and 13(a)), we have that $\forall M_b \in \mathcal{M}_B$, $\alpha(M_b) = 1$, i.e., all basis markings are weakly exposable. Clearly, $\forall w \in \mathcal{L}(N, R(N, M_0))$, $\mathcal{I}_b(w) \cap wex(S) \neq \emptyset$ holds. However, according to the result in Example 5.5, the LPN is not initial-state opaque wrt S_1. ◇

The reason why Proposition 5.6 is not a sufficient condition is that for an observation w, the possible initial markings that could generate w is generally not the union of all unobservable reach of the possible initial basis markings, i.e., $\mathcal{I}(w) \subseteq \bigcup_{M_b \in \mathcal{I}_b(w)} \mathcal{U}(M_b)$. Therefore $\mathcal{I}(w) \subseteq S$ does not imply that $\bigcup_{M_b \in \mathcal{I}_b(w)} \mathcal{U}(M_b) \subseteq S$. This is different from the case of the current-state opacity problem since $\mathcal{C}(w) = \bigcup_{M_b \in \mathcal{M}_b(w)} \mathcal{U}(M_b)$. However, we show that if Assumption A3 is satisfied, initial-state opacity can be necessarily and sufficiently verified by checking if each $\mathcal{I}_b(w)$ contains at least one basis marking that does not belong to the secret.

Proposition 5.8: Let $G = (N, M_0, E, \ell)$ be an LPN whose unobservable subnet is acyclic and S be a secret satisfying Assumption A3. G is initial-state opaque wrt S iff $\forall w \in \mathcal{L}(N, R(N, M_0))$, $\mathcal{I}_b(w) \cap ex(S_B) \neq \emptyset$ holds.

Proof: ($\Rightarrow$) Assume that $\forall w \in \mathcal{L}(N, R(N, M_0))$, $\mathcal{I}_b(w) \cap ex(S_B) \neq \emptyset$ holds. By $\mathcal{I}_b(w) \subseteq \mathcal{I}(w)$ and $ex(S_B) \subseteq ex(S)$, $\mathcal{I}(w) \cap ex(S) \neq \emptyset$, and Definition 5.1, G is initial-state opaque wrt S.

($\Leftarrow$) Now assume that G is initial-state opaque wrt S. By Definition 5.1, $\forall w \in \mathcal{L}(N, R(N, M_0))$, we have $\mathcal{I}(w) \cap ex(S) \neq \emptyset$. Let $M \in \mathcal{I}(w) \cap ex(S)$. Under Assumption A3, there exists $M_b \in \mathcal{M}_B : M \in \mathcal{U}(M_b)$ and $M_b \in ex(S_B)$ (otherwise it would contradict $M \in ex(S)$). Therefore, $w \in \mathcal{L}(N, M_b)$ and $M_b \in \mathcal{I}(w) \cap ex(S_B)$, i.e., $\mathcal{I}_b(w) \cap ex(S_B) \neq \emptyset$. ■

As a result, initial-state opacity of G can be verified by constructing the initial-state estimator of its BRG $\mathcal{B} = (\mathcal{M}_B, E, \Delta)$ whose complexity is $\mathcal{O}(2^{|\mathcal{M}_B|})$. Since the size of the BRG will never be larger than the RG and it may be much smaller especially when unobservable transitions exist, the proposed approach is practically more efficient.

Example 5.9: Consider again the LPN in Example 5.5. The initial-state estimator of its BRG is shown in Fig. 14. Let $S = \{M_0, M_2, M_5, M_8, M_9\}$ be the secret that satisfies Assumption A3. Then $S_B = \{M_0, M_2\}$ and $ex(S_B) = \{M_1, M_3, M_4\}$.

According to Proposition 5.8, G is initial-state opaque wrt S since no state of the estimator either coincides with S_B or is strictly contained in it. ◇

Note that Assumption A3 is only necessary for the *only if* part of Proposition 5.8 as clarified by the following example.

Example 5.10: Consider the LPN and secret S_2 in Example 5.5. All markings in S_2 are weakly exposable. We have $S_{2B} = \{M_1\}$ and $ex(S_{2B}) = \{M_0, M_2 - M_4\}$. Based on the initial-state estimator of the BRG shown in Fig. 14, we have $\mathcal{I}_b(bb) = \{M_1\}$, i.e., $\exists w : \mathcal{I}_b(w) \cap ex(S_B) = \emptyset$. However, according to the result in Example 5.5, the LPN is initial-state opaque wrt S_2. ◇

C. Relaxation of Assumption A3

Different from the case discussed in Section IV-D, Assumption A3 cannot be relaxed in Proposition 5.8 by simply removing the weakly exposable markings from the secret. In this subsection, we propose a method to relax Assumption A3 by appropriately modifying the BRG definition. The new BRG is called *modified basis reachability graph* (MBRG).

Let us consider the case where Assumption A3 does not hold. Then S can be partitioned into $S' \cup S''$, where $S' = wex(S) \cap S \neq \emptyset$ and $S'' = S \setminus S'$ (Clearly, if Assumption A3 is satisfied, $S' = \emptyset$). The system may be initial-state opaque wrt S even if $\mathcal{I}_b(w) \subseteq S$, since there may exist some marking $M \in (\mathcal{I}(w) \setminus \mathcal{I}_b(w)) \cap ex(S)$. We write $\mathcal{Q} = \bigcup_{M \in S'} \mathcal{U}(M) \cap ex(S)$ to denote the unobservable reach of all markings in S'. The following proposition shows that to decide if the system is initial-state opaque, we need to check if $\mathcal{I}(w) \cap \mathcal{Q} \neq \emptyset$ holds

Proposition 5.11: Let w be an observation in an LPN G whose unobservable subnet is acyclic, $S \in R(N, M_0)$ be a secret, and $\mathcal{I}_b(w) \subseteq S$. $\mathcal{I}(w) \nsubseteq S$ iff $\mathcal{I}(w) \cap \mathcal{Q} \neq \emptyset$.

Proof: ($\Rightarrow$) Assume $\mathcal{I}(w) \cap \mathcal{Q} \neq \emptyset$. Since $\mathcal{Q} \subseteq ex(S)$, $\mathcal{I}(w) \cap ex(S) \neq \emptyset$, i.e., $\mathcal{I}(w) \nsubseteq S$.

($\Leftarrow$) Assume $\mathcal{I}(w) \nsubseteq S$. Since $\mathcal{I}_b(w) \subseteq S$, there exists a marking $M \in (\mathcal{I}(w) \setminus \mathcal{I}_b(w)) \cap ex(S)$. Let $M_b \in \mathcal{M}_B$ be the basis marking such that $M \in \mathcal{U}(M_b)$. Since $\mathcal{I}_b(w) \subseteq S$, we have $M_b \in S'$ and $M \in \mathcal{Q}$, i.e., $\mathcal{I}(w) \cap \mathcal{Q} \neq \emptyset$. ■

In simple words, when Assumption A3 is not satisfied, by checking if either $\mathcal{I}_b(w) \cap ex(S) \neq \emptyset$ or $\mathcal{I}(w) \cap \mathcal{Q} \neq \emptyset$ hold, initial-state opacity can be verified. Let $\mathcal{Q}_{min} \subseteq \mathcal{Q}$ be the subset of Q with the minimal cardinality satisfying the following property: for any $M' \in \mathcal{Q}$, there exists $M \in \mathcal{Q}_{min}$ such that $M' \in \mathcal{U}(M)$. Obviously $\mathcal{Q}_{min}$ is unique.

Proposition 5.12: Let w be an observation in a bounded LPN G whose unobservable subnet is acyclic and $S \in R(N, M_0)$ be a secret. $\mathcal{I}(w) \cap \mathcal{Q} \neq \emptyset$ iff $\mathcal{I}(w) \cap \mathcal{Q}_{min} \neq \emptyset$.

Proof: ($\Rightarrow$) Assume $\mathcal{I}(w) \cap \mathcal{Q}_{min} \neq \emptyset$. Since $\mathcal{Q}_{min} \subseteq \mathcal{Q}$, $\mathcal{I}(w) \cap \mathcal{Q} \neq \emptyset$.

($\Leftarrow$) Assume $\mathcal{I}(w) \cap \mathcal{Q} \neq \emptyset$. Let $M' \in \mathcal{I}(w) \cap \mathcal{Q}$. There exists $M \in \mathcal{Q}_{min}$ such that $M' \in \mathcal{U}(M)$. Therefore, $M \in \mathcal{I}(w)$, i.e., $\mathcal{I}(w) \cap \mathcal{Q}_{min} \neq \emptyset$. ■

Proposition 5.12 shows that we do not need to consider all markings in $\mathcal{Q}$ but only a minimal subset of them. Given a bounded LPN whose unobservable subnet is acyclic, we propose Algorithm 2 to compute $\mathcal{Q}_{min}$. Once $\mathcal{Q}_{min}$ is obtained, a method to verify initial-state opacity by using the MBRG is proposed.

In Algorithm 2, $\mathcal{Q}_{min}$ is initialized at the empty set. Given a marking $M \in S'$, the reachability graph of $\langle N', M \rangle$ is denoted as an automaton $\mathcal{R}(N', M) = (\mathcal{U}(M), T_u, \Delta, M)$: the state space of $\mathcal{R}(N', M)$ is the unobservable reach of M, the initial state is M, and the event set is the set of the unobservable transitions T_u. Since N' is acyclic, the reachable markings can be computed by solving the state equation $M' = M + C_u \cdot y$, where $y \in \mathbb{N}^{n_u}$, and there is no cycle in the reachability graph $\mathcal{R}(N', M)$. We compute the set of exposable markings that are initial vertices of paths in $\mathcal{R}(N', M)$ (Steps 7-11). Finally,

Algorithm 2 Computation of $\mathcal{Q}_{min}$

Input: A bounded LPN $G = (N, M_0, E, \ell)$ whose unobservable subnet N' is acyclic, and a secret S.
Output: $\mathcal{Q}_{min}$

1: $\mathcal{Q}_{min} := \emptyset$;
2: Compute S', the set of weakly exposable markings in S;
3: **while** $S' \neq \emptyset$, **do**
4: select a marking $M \in S'$;
5: construct the reachability graph of $\langle N', M\rangle$, denoted as $\mathcal{R}(N', M) = (\mathcal{U}(M), T_u, \Delta, M)$;
6: $\mathcal{Q}_{temp} := \mathcal{U}(M) \cap ex(S)$.
7: **for all** $M_j \in \mathcal{Q}_{temp}$, **do**
8: **if** $\nexists M_i \in \mathcal{Q}_{temp} : (M_i, \sigma_u, M_j) \in \Delta$, where $\sigma_u \in T_u^*$, **then**
9: $\mathcal{Q}_{min} := \mathcal{Q}_{min} \cup \{M_j\}$;
10: **end if**
11: **end for**
12: $S' := S' \setminus \mathcal{U}(M)$;
13: **end while**

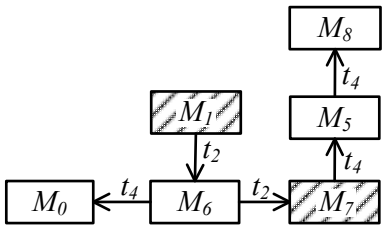

Fig. 15. Reachability Graph $\mathcal{R}(N', M_1)$.

since some markings in S' can be reached from some existing markings in $\mathcal{Q}_{min}$, they are removed from S' to further reduce the computation load in forthcoming iterations.

Example 5.13: Consider again the LPN in Example 5.5 and $S = \{M_1, M_7\}$. The reachability graph of $\langle N', M_1\rangle$ is shown in Fig. 15, and secret markings are in shadowed boxes. We have $S' = \{M_1, M_7\}$. By Algorithm 2, after the first iteration, $\mathcal{Q}_{temp} = \{M_0, M_5, M_6, M_8\}$ and $\mathcal{Q}_{min} = \{M_6\}$ since one can readily verify that all nonsecret markings M_0, M_5, and M_8 in $\mathcal{U}(M_1)$ can be reached from M_6 by firing unobservable transitions. Furthermore, M_7 is removed from S' by Step 12 since $M_7 \in \mathcal{U}(M_1)$ and it is not necessary to check the unobservable reach of M_7. Then Algorithm 2 outputs $\mathcal{Q}_{min} = \{M_6\}$. $\diamond$

In the following, Algorithm 3 is presented to construct the modified BRG (MBRG) $\mathcal{B}' = (\mathcal{M}_{B'}, E, \Delta')$ of a given bounded LPN whose unobservable subnet is acyclic. The method to construct the MBRG is analogous to the method to construct BRG, however, the nodes are initialized by markings in $\{M_0\} \cup \mathcal{Q}_{min}$. Although the MBRG is larger than the BRG, the MBRG is still much smaller than RG. We use $\mathcal{M}_{B'}$ to denote the *extended basis markings* that appear in the MBRG. Correspondingly, we denote by $\mathcal{I}_{b'}(w) = \mathcal{I}(w) \cap \mathcal{M}_{B'}$ the set of markings in $\mathcal{M}_{B'}$ generating w, $S_{B'} = S \cap \mathcal{M}_{B'}$ the set of markings in $\mathcal{M}_{B'}$ that belong to the secret, and $ex(S_{B'}) = ex(S) \cap \mathcal{M}_{B'}$ the set of markings in $\mathcal{M}_{B'}$ that do not belong to the secret.

Proposition 5.14: Let G be an LPN whose unobservable subnet is acyclic, and S be a secret. G is initial-state opaque wrt S iff $\forall w \in \mathcal{L}(N, R(N, M_0))$, $\mathcal{I}_{b'}(w) \cap ex(S_{B'}) \neq \emptyset$ holds.

Proof: ($\Rightarrow$) Assume that $\forall w \in \mathcal{L}(N, R(N, M_0))$, $\mathcal{I}_{b'}(w) \cap ex(S_{B'}) \neq \emptyset$. Since $\mathcal{I}_{b'}(w) \subseteq \mathcal{I}(w)$ and $ex(S_{B'}) \subseteq ex(S)$, $\mathcal{I}(w) \cap ex(S) \neq \emptyset$ holds and, by Definition 5.1, G is initial-state opaque wrt S.

($\Leftarrow$) Now assume that G is initial-state opaque wrt S. According to Definition 5.1, $\forall w \in \mathcal{L}(N, R(N, M_0))$, we have $\mathcal{I}(w) \cap ex(S) \neq \emptyset$, i.e., $\exists M \in \mathcal{I}(w) \cap ex(S)$. Since M must be in the unobservable reach of a basis marking M_b. If $M_b \in ex(S)$ then the proof is concluded. If $M_b \in S$, then M_b is weakly exposable, i.e., $M_b \in S'$. By Algorithm 2 there

Algorithm 3 Construction of the MBRG

Input: A bounded labeled Petri net $G = (N, M_0, E, \ell)$ whose unobservable subnet N' is acyclic, and a secret S.
Output: The modified BRG $\mathcal{B}' = (\mathcal{M}_{B'}, E, \Delta')$.

Construct the BRG $\mathcal{B} = (\mathcal{M}_B, E, \Delta, M_0)$ by using Algorithm 1.
Compute set $\mathcal{Q}_{min}$ by using Algorithm 2.
$\mathcal{M}_{B'} := \mathcal{M}_B \cup \mathcal{Q}_{min}$, $\Delta' := \Delta$.
Tag all $M \in \mathcal{M}_B$ "old".
while states in $\mathcal{M}_{B'}$ with no tag exist, **do**
    select a state $M \in \mathcal{M}_{B'}$ with no tag;
    for all t s.t. $\ell(t) \in E$ and $Y_{min}(M, t) \neq \emptyset$, **do**
        for all $\mathbf{y}_u \in Y_{min}(M, t)$, **do**
            $M' := M + C_u \cdot \mathbf{y}_u + C(\cdot, t)$;
            if $M' \notin \mathcal{M}_B$, **then**
                $\mathcal{M}_{B'} := \mathcal{M}_{B'} \cup \{M'\}$;
                assign no tag to M';
            end if
            $\Delta' := \Delta \cup \{(M, \ell(t), M')\}$;
        end for
        tag node M "old";
    end for
end while
Remove all tags.

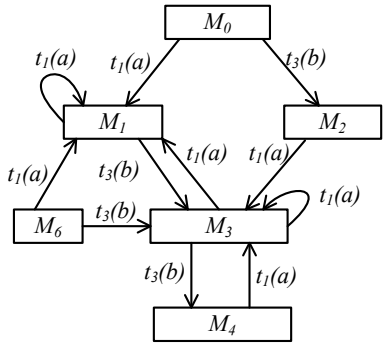

Fig. 16. The MBRG in Example 5.15.

must exist a marking $M' \in \mathcal{Q}_{min} \subseteq \mathcal{M}_{B'}$ such that M is reachable from M' by firing only unobservable transitions, which indicates that $M' \in \mathcal{I}_{b'}(w) \cap ex(S_{B'})$. ■

Proposition 5.14 shows that if Assumption A3 is not satisfied, by constructing the initial-state estimator of the MBRG, initial-state opacity of G can be verified. In this case, the complexity increases to $\mathcal{O}(2^{|\mathcal{M}_{B'}|})$.

Example 5.15: Since secret $S = \{M_1, M_7\}$ does not satisfy Assumption A3, we construct its MBRG by Algorithm 3 which

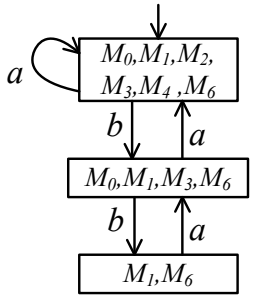

Fig. 17. The initial-state estimator of the MBRG in Fig. 16.

TABLE II
NUMBER OF (BASIS) MARKINGS AND TIME COST

k	$\|R(N,M_0)\|$	T-r	$\|\mathcal{M}_B\|$	T-b
8	220	7.2×10^{-1}	19	4.1×10^{-2}
10	364	2.1×10^{0}	23	5.0×10^{-2}
20	2024	6.3×10^{1}	43	8.0×10^{-2}
40	13244	1.1×10^{3}	83	1.1×10^{-1}
60	o.t.	o.t.	123	3.6×10^{-1}
80	o.t.	o.t.	163	5.3×10^{-1}
100	o.t.	o.t.	203	7.6×10^{-1}
120	o.t.	o.t.	243	9.7×10^{-1}

is shown in Fig. 16. We have $\mathcal{M}_{B'} = \{M_0 - M_4, M_6\}$, $S_{B'} = \{M_1\}$ and $ex(S_{B'}) = \{M_0, M_2 - M_4, M_6\}$. The corresponding initial-state estimator is shown in Fig. 17. Since, $\forall w \in \mathcal{L}(N, R(N, M_0))$, $\mathcal{I}_{b'}(w) \cap ex(S_{B'}) \neq \emptyset$ holds, the LPN is initial-state opaque wrt S. $\diamond$

VI. NUMERICAL EXAMPLES

To compare the approaches of using BRG and RG to verify the state-based opacity properties, a series of numerical examples are presented. Based on the proposed approaches in this work, we developed a MATLAB tool [31] to compute the BRG, the current-state basis observer, the initial-state estimator, and to determine current-state opacity of a bounded LPN. In the following, numerical results are obtained by using the tool.

We still consider the simple LPN G in Fig. 1 but the initial marking in place p_2 is a parameter $k \in \{1, 2, \cdots\}$. Therefore, here we consider not a single LPN but a family of nets parameterized by the initial marking. Based on the structure of the LPN, the number of its reachable markings is

$$|R(N, M_0)| = \frac{1}{6}(k+4)(k+3)(k+2). \tag{2}$$

We still let t_1 and t_3 be the observable transitions. Then the number of basis markings is

$$|\mathcal{M}_B| = 2k + 3. \tag{3}$$

Based on Eqs. (2) and (3), Fig. 18 shows the variation of $|R(N, M_0)|$ and $|\mathcal{M}_B|$ with respect to k. The numerical values for some specific k's together with the computational times are reported in Table II, where Columns 2 and 4 illustrate the number of reachable markings $|R(N, M_0)|$ and basis markings $|\mathcal{M}_B|$, respectively. The corresponding time costs are presented in Columns 3 and 5, respectively. The table shows that when the initial marking of p_2 is larger than or equal to 60, the RG cannot be computed within 8 hours and we use "o.t." to denote the computation is out of time. On the contrary, the BRG can still be constructed in a short time.

For the verification of current-state opacity, let $\ell(t_1) = a$, $\ell(t_3) = a$, and $S = \{M \in \mathbb{N}^4 | M(p_1) + M(p_4) \geq 2\}$, i.e., $W = [\ -1 \quad 0 \quad 0 \quad -1\ ]$ and $K = -2$. For the verification of initial-state opacity, let $\ell(t_1) = a$, $\ell(t_3) = b$. Results are summarized in Tables III and IV, respectively. Columns 2 and 4 present the numbers of states $|\mathcal{X}_{or}|$ and $|\mathcal{X}_{ob}|$ (resp. $|\mathcal{X}_{er}|$ and $|\mathcal{X}_{eb}|$) corresponding to the observers (resp. estimators) of the RG and the BRG. The computation time T-or and T-ob (resp. T-er and T-eb) are shown in Columns 3 and 5, respectively. Note that the computational time for the observer and estimator does not increase fast with respect to k. However, the observer and the estimator of the RG cannot be constructed since the RG is not obtained for $k \geq 60$.

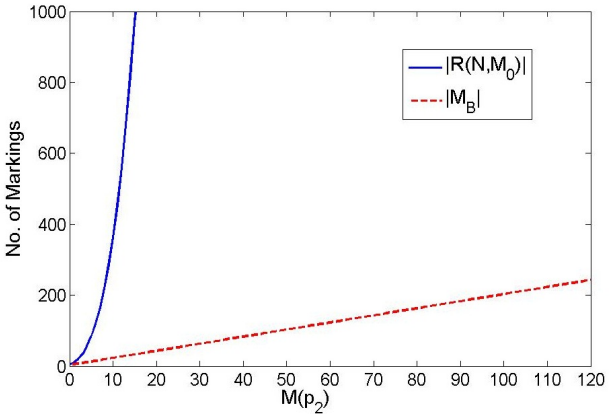

Fig. 18. The sizes of $|R(N, M_0)|$ and $|\mathcal{M}_B|$ changing with k.

TABLE III
NUMBER OF STATES OF THE OBSERVERS AND THE TIME COST

k	$\lvert\mathcal{X}_{or}\rvert$	T-or	$\lvert\mathcal{X}_{ob}\rvert$	T-ob	CSO
8	11	2.0×10^{0}	11	1.6×10^{-2}	Y
10	13	4.2×10^{0}	13	2.2×10^{-2}	Y
20	23	5.5×10^{1}	23	6.8×10^{-2}	Y
40	43	3.5×10^{3}	43	2.1×10^{-1}	Y
60	o.t.	o.t.	63	4.5×10^{-1}	Y
80	o.t.	o.t.	83	7.7×10^{-1}	Y
100	o.t.	o.t.	103	8.7×10^{-1}	Y
120	o.t.	o.t.	123	1.7×10^{0}	Y

From Table III, we notice that the number of states of the observer computed using RG, when computable, is identical to the number of states of the observer relative to the BRG. It can be easily proved that this is a general result validating the effectiveness of the proposed result. Same conclusions can be drawn with regard to the estimator. As a result, we conclude that the proposed approaches are practically efficient especially for large-size Petri nets. The reader can use the MATLAB tool we have developed, which is available on the web [31] to test the proposed approach on other nets.

Two remarks should be done concerning the above numerical examples. The first one relates to initial-state opacity verification, and the other is about the MBRG. When the initial marking (i.e., the value of k) changes, a given secret may not satisfy Assumption A3. Therefore, for initial-state opacity we cannot provide results as a function of parameter k while keeping the secret constant. In simple words, a column analogous to the last column of Table III cannot be obtained. It would be also interesting to compare the size of the MBRG and the RG for different values of k as we did for the BRG. However, this

TABLE IV
NUMBER OF STATES OF THE ESTIMATORS AND THE TIME COST

k	$\lvert\mathcal{X}_{er}\rvert$	T-er	$\lvert\mathcal{X}_{eb}\rvert$	T-eb
8	10	1.8×10^{0}	10	1.1×10^{-1}
10	12	3.6×10^{0}	12	1.1×10^{-1}
20	22	6.0×10^{1}	22	2.8×10^{-1}
40	42	3.7×10^{3}	42	1.7×10^{0}
60	o.t.	o.t.	62	3.7×10^{0}
80	o.t.	o.t.	82	6.5×10^{0}
100	o.t.	o.t.	102	9.8×10^{0}
120	o.t.	o.t.	122	1.4×10^{1}

cannot be done since the structure of MBRG depends not only on the initial marking but also on the secret.

VII. Conclusions and Future Work

This paper addresses current-state and initial-state opacity properties in labeled Petri nets. In the first part of the paper we show that the notion of BRG can be used to verify current-state opacity by constructing the observer of the BRG. This approach has several advantages in terms of computational and space complexity. When the intruder has uncertainty about the initial marking, an extended observer can be used whose initial marking is a subset of the reachability set and the generated language is identical to the language generated by the system. In the second part of the paper we show that under certain assumptions, initial-state opacity can be verified by constructing the initial-state estimator of the BRG. The modified basis reachability graph is introduced to verify initial-state opacity in the general case.

Our future research in this framework will focus on language-based opacity. We plan to first formalize the notion of language opacity in the framework of Petri nets. Second, we plan to study the verification of language opacity using BRG.

References

[1] L. Mazaré, "Using unification for opacity properties," in *Proceedings of the 2004 Workshop on Issues in the Theory of Security*, 2004, pp. 165–176.

[2] J. W. Bryans, M. Koutny, L. Mazaré, and P. Y. Ryan, "Opacity generalised to transition systems," *International Journal of Information Security*, vol. 7, no. 6, pp. 421–435, 2008.

[3] F. Cassez, J. Dubreil, and H. Marchand, "Synthesis of opaque systems with static and dynamic masks," *Formal Methods in System Design*, vol. 40, no. 1, pp. 88–115, 2012.

[4] Y. Tong, Z. W. Li, and A. Giua, "On the equivalence of observation structures for Petri net generators," *IEEE Transactions on Automatic Control*, vol. 61, no. 9, pp. 2448–2462, Sept 2016.

[5] J. W. Bryans, M. Koutny, and P. Y. Ryan, "Modelling opacity using Petri nets," *Electronic Notes in Theoretical Computer Science*, vol. 121, pp. 101–115, 2005.

[6] A. Saboori and C. N. Hadjicostis, "Notions of security and opacity in discrete event systems," in *Proceedings of the 46th IEEE Conference on Decision and Control*. IEEE, 2007, pp. 5056–5061.

[7] F. Cassez, "The dark side of timed opacity," in *Advances in Information Security and Assurance*. Springer, 2009, pp. 21–30.

[8] A. Saboori and C. N. Hadjicostis, "Verification of initial-state opacity in security applications of discrete event systems," *Information Sciences*, vol. 246, pp. 115–132, 2013.

[9] Y. Wu and S. Lafortune, "Comparative analysis of related notions of opacity in centralized and coordinated architectures," *Discrete Event Dynamic Systems*, vol. 23, no. 3, pp. 307–339, 2013.

[10] E. Badouel, M. Bednarczyk, A. Borzyszkowski, B. Caillaud, and P. Darondeau, "Concurrent secrets," *Discrete Event Dynamic Systems*, vol. 17, no. 4, pp. 425–446, 2007.

[11] Y. Falcone and H. Marchand, "Enforcement and validation (at runtime) of various notions of opacity," *Discrete Event Dynamic Systems*, vol. 25, no. 4, pp. 531–570, 2015.

[12] F. Cassez, J. Dubreil, and H. Marchand, "Dynamic observers for the synthesis of opaque systems," in *Automated Technology for Verification and Analysis*. Springer, 2009, pp. 352–367.

[13] R. Jacob, J. Lesage, and J. Faure, "Overview of discrete event systems opacity: Models, validation, and quantification," *Annual Reviews in Control*, vol. 41, pp. 135 – 146, 2016.

[14] Y. Tong, Z. W. Li, C. Seatzu, and A. Giua, "Verification of current-state opacity using Petri nets," in *Proceedings of the 2015 American Control Conference*, July 2015, pp. 1935–1940.

[15] ——, "Verification of initial-state opacity in Petri nets," in *Proceedings of the 2015 IEEE 54th Annual Conference on Decision and Control*, Dec 2015, pp. 344–349.

[16] Y. Tong, Z. Ma, Z. W. Li, C. Seactzu, and A. Giua, "Verification of language-based opacity in Petri nets using verifier," in *Proceedins of the 2016 American Control Conference*, July 2016, pp. 757–763.

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

[18] M. P. Cabasino, A. Giua, M. Pocci, and C. Seatzu, "Discrete event diagnosis using labeled Petri nets. An application to manufacturing systems," *Control Engineering Practice*, vol. 19, no. 9, pp. 989–1001, 2011.

[19] A. Giua, C. Seatzu, and D. Corona, "Marking estimation of Petri nets with silent transitions," *IEEE Transactions on Automatic Control*, vol. 52, no. 9, pp. 1695–1699, Sept 2007.

[20] M. P. Cabasino, A. Giua, and C. Seatzu, "Diagnosability of discrete-event systems using labeled Petri nets," *IEEE Transactions on Automation Science and Engineering*, vol. 11, no. 1, pp. 144–153, 2014.

[21] Z. Ma, Y. Tong, Z. W. Li, and A. Giua, "Basis marking representation of Petri net reachability spaces and its application to the reachability problem," *IEEE Transactions on Automatic Control (to appear)*, vol. 62, no. 3, 2017, DOI: 10.1109/TAC.2016.2574120, On-line: http://ieeexplore.ieee.org/document/7480433/.

[22] C. G. Cassandras and S. Lafortune, *Introduction to discrete event systems*. Springer, 2008.

[23] T. Murata, "Petri nets: Properties, analysis and applications," *Proceedings of the IEEE*, vol. 77, no. 4, pp. 541–580, April 1989.

[24] A. Giua, F. DiCesare, and M. Silva, "Generalized mutual exclusion contraints on nets with uncontrollable transitions," in *Proceedings of the 1992 IEEE International Conference on Systems, Man and Cybernetics*, Oct 1992, pp. 974–979 vol.2.

[25] J. O. Moody and P. J. Antsaklis, "Petri net supervisors for DES with uncontrollable and unobservable transitions," *IEEE Transactions on Automatic Control*, vol. 45, no. 3, pp. 462–476, 2000.

[26] M. V. Iordache and P. J. Antsaklis, "Petri net supervisors for disjunctive constraints," in *Proceedings of the 2007 American Control Conference*. IEEE, 2007, pp. 4951–4956.

[27] J. H. Ye, Z. W. Li, and A. Giua, "Decentralized supervision of Petri nets with a coordinator," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 45, no. 6, pp. 955–966, June 2015.

[28] Z. Y. Ma, Z. W. Li, and A. Giua, "Design of optimal Petri net controllers for disjunctive generalized mutual exclusion constraints," *IEEE Transactions on Automatic Control*, vol. 60, no. 7, pp. 1774–1785, July 2015.

[29] A. Schrijver, *Theory of linear and integer programming*. John Wiley & Sons, 1998.

[30] C. Mahulea, C. Seatzu, M. P. Cabasino, and M. Silva, "Fault diagnosis of discrete-event systems using continuous Petri nets," *IEEE Transactions on Systems, Man and Cybernetics, Part A: Systems and Humans*, vol. 42, no. 4, pp. 970–984, 2012.

[31] Y. Tong, "Matlab tool for verification of state-based opacity," Available: http://www.diee.unica.it/~seatzu/Matlab_tool_opacity.html.