Verification of Current-State Opacity Using Petri Nets

Yin Tong[1], Zhiwu Li[2], Carla Seatzu[3] and Alessandro Giua[4]

Abstract

This paper addresses the problem of current-state opacity of discrete event systems (DES) modeled with Petri nets. A system is said to be current-state opaque if the intruder who only has partial observations on the system's behavior is never able to infer that the current state of the system is within a set of secret states. Based on the notion of basis markings, an efficient approach to verifying current-state opacity in bounded Petri nets is proposed, without computing the whole reachability set or exhaustively enumerating the set of markings consistent with the observation. An example showing the efficiency of the approach is presented.

Published as:

Y. Tong, Z.W. Li, C. Seatzu, A. Giua, "Verification of Current-State Opacity Using Petri Nets," IEEE American Control Conference (Chicago, IL, USA), July 1-3, 2015. pp. 1935-1940. DOI: 10.1109/ACC.2015.7171016

---

[1]Yin Tong is with the School of Electro-Mechanical Engineering, Xidian University, Xi'an 710071, China yintong@stu.xidian.edu.cn

[2]Zhiwu Li is with the Institute of Systems Engineering, Macau University of Science and Technology, Taipa, Macau, Faculty of Engineering, King Abdulaziz University, Jeddah 21589, Saudi Arabia, and also with the School of Electro-Mechanical Engineering, Xidian University, Xi'an 710071, China zhwli@xidian.edu.cn

[3]Carla Seatzu is with the Department of Electrical and Electronic Engineering, University of Cagliari, 09123 Cagliari, Italy seatzu@diee.unica.it

[4]Alessandro Giua is with Aix Marseille Université, CNRS, ENSAM, Université de Toulon, LSIS UMR 7296, Marseille 13397, France and also with DIEE, University of Cagliari, Cagliari 09124, Italy alessandro.giua@lsis.org; giua@diee.unica.it

I. INTRODUCTION

Motivated by the concern about security and privacy in computer systems, communication protocols etc., various notions of secrecy have been formulated, such as *non-interference* [1], *anonymity* [2], [3] and *opacity* [4], [5], [6], [7], [8]. In this work, we focus on the opacity property that requires a given secret behavior of a system to be hidden from an intruder. According to the definition of "secret", opacity properties can be generally classified as *language-based opacity* and *state-based opacity*. The later includes *initial-state opacity*, *current-state opacity*, *k-step opacity*, etc. [8], [9]. The work in [8] showed that language-based opacity, initial-state opacity, and initial-and-final-state opacity, can be transformed to current-state opacity in polynomial time. In particular, we discuss current-state opacity here.

Current-state opacity defines the secret as a set of states. A system is said to be *current-state opaque* with respect to a given secret if the intruder cannot determine if the current state of the system belongs to the secret. In other words, opacity requires that for any observation the intruder's estimate of the current state, i.e., the set of states consistent with the observation, is not a subset of the secret. In the framework of automata, the intruder is modeled by an external observer who knows the structure of the system but has only partial observation of its revolution. The existing and most intuitive method to verify current-state opacity is to construct the observer automaton [8], each state of which describes the intruder's state estimate after a string is observed. However, the computation of the observer has a complexity of order $\mathcal{O}(2^n)$ with n being the number of states.

In the framework of Petri nets, for the intruder different observation structures can be considered [10], [11]. Herein, we address the verification of current-state opacity in standard *labeled Petri nets* (LPN), i.e., only transitions are observable for the intruder. Structural properties of Petri nets have been used to solving deadlock problems in DES [12], due to its intuitive graphical representation and powerful algebraic formulation. An approach based on *basis markings* [13], [14] has been recently used to solve problems of state estimation and fault diagnosis [15], [16] in LPN. The advantages of this technique that exploits the structural properties of a net are that only part of the reachable markings, i.e., the basis markings, are enumerated and the sets of consistent markings are characterized by linear systems one for each basis marking. As an example, in Section IV we present a net whose number of reachable markings is $\mathcal{O}(k^3)$ times larger than that of basis markings, where k is the initial token content of the net.

We believe that the notion of basis markings can also be used to efficiently solve the opacity problem and in this first work we show that it can be applied to addressing current-state opacity. A necessary and sufficient condition for current-state opacity in bounded Petri nets is proposed. It is shown that based on the notion of basis markings current-state opacity can be verified without an exhaustive enumeration. Furthermore, a modified *basis reachability graph* (BRG) that describes not only all basis markings but also the opacity property of each basis marking, is presented. Compared to the reachability graph, the BRG of a net is generally of smaller size. Finally, by just constructing the observer of the BRG, current-state opacity can be decided.

This paper is structured as follows. The notions of Petri nets and basis markings are recalled in Section II.

The formal definition of current-state opacity and an approach to verifying current-state opacity are proposed in Section III. In Section IV, an example that illustrates the approach is reported. Finally, Section V concludes the paper and discusses future work.

II. BACKGROUND

A. Petri Nets

In this section we recall the formalisms used in the paper. For more details on Petri nets we refer readers to [17].

A *Petri net* (PN) is a structure $N = (P, T, Pre, Post)$, where P is a set of m *places* represented by circles; T is a set of n *transitions* 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[1]. 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 PN $N = (P, T, Pre, Post)$ is a *state machine* (SM) (resp. *marked graph* (MG)) if $\forall t \in T$, $|{}^\bullet t| = |t^\bullet| = 1$ (resp. $\forall p \in P$, $|{}^\bullet p| = |p^\bullet| = 1$). A PN is called *acyclic* if there are no oriented cycles.

A *marking* is a vector $M : P \to \mathbb{N}^m$ that assigns to each place of a PN a non-negative integer number of tokens, graphically represented by black dots. The marking of place p is denoted by $M(p)$. For economy of space, markings can also be 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 an 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 sequences that can fire in a net system $\langle N, M_0 \rangle$ is denoted by $L(N, M_0) = \{\sigma \in T^* | M_0[\sigma\rangle\}$. Given a sequence $\sigma \in T^*$, vector $y = \pi(\sigma) \in \mathbb{N}^n$ is the Parikh vector of σ, 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 firable sequence $\sigma \in L(N, M_0)$ such that $M_0[\sigma\rangle M$. The set of all markings reachable from M_0 defines the *reachability set* of $\langle N, M_0 \rangle$ and is denoted by $R(N, M_0)$. A PN system is *bounded* if there exists a non-negative integer $k \in \mathbb{N}$ such that for any place $p \in P$ and for any reachable marking $M \in R(N, M_0)$, $M(p) \leq k$ holds.

Theorem 2.1: [15] Let $\langle N, M_0 \rangle$ be a PN system where N is an acyclic PN.

(i) If the vector $y \in \mathbb{N}^n$ satisfies the equation $M_0 + C \cdot y \geq \vec{0}$, there exists a firing sequence σ firable from M_0 whose firing vector is $\pi(\sigma) = y$.

(ii) A marking M is reachable from M_0 iff there exists a nonnegative integer solution y satisfying the state equation $M = M_0 + C \cdot y$. $\diamond$

A *labeled Petri net* (LPN) is 4-tuple $G = (N, M_0, E, \ell)$, where $\langle N, M_0 \rangle$ is a PN system, E is an *alphabet* (a set of labels) and $\ell : T \to E \cup \{\varepsilon\}$ is a *labeling function* that assigns to each transition $t \in T$ either a symbol from E or the empty word ε.

[1]In this work, we use $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{R}$ and $\mathbb{R}_{\geq 0}$ to denote the sets of non-negative integers, integers, real numbers and non-negative real numbers, respectively.

We assume that the intruder has full knowledge of the net system $\langle N, M_0\rangle$ but partial observation. Namely, the set of transitions can be partitioned into $T = T_o \cup T_u$ with $T_o \cap T_u = \emptyset$, where T_o (resp. T_u) is the set of $|T_o| = n_o$ (resp. $|T_u| = n_u$) observable (resp. unobservable) transitions whose occurrence can (resp. cannot) be detected by the intruder. For unobservable transitions, the empty word ε is assigned by the labeling function. While, for observable transitions symbols from the alphabet E are assigned to them. The restriction of the incidence matrix to T_o (resp. T_u) is denoted by C_o (resp. C_u).

The labeling function is extended to strings $\ell : T^* \to E^*$ that is recursively defined as $\ell(\sigma t) = \ell(\sigma)\ell(t)$ with $\sigma \in T^*$ and $t \in T$. The set of languages generated by an LPN is denoted as $\mathcal{L}(N, M_0) = \{w \in E^* | \exists \sigma \in L(N, M_0) : \ell(\sigma) = w\}$. The natural projection $P_o : T^* \to T_o^*$ (resp. $P_u : T^* \to T_u^*$) of σ over T_o (resp. T_u) is defined.

Let w be an observed word. We define $\mathcal{S}(w) = \{\sigma \in L(N, M_0) | \ell(\sigma) = w\}$ as the *set of firing sequences consistent with* w and $\mathcal{C}(w) = \{M \in \mathbb{N}^m | \exists \sigma \in \mathcal{S}(w) : M_0[\sigma\rangle M\}$ as the *set of markings consistent with* w. Note that since observation w is generated by the system, sets $\mathcal{S}(w)$ and $\mathcal{C}(w)$ must be non-empty sets.

Given a PN $N = (P, T, Pre, Post)$ and a subset $T' \subseteq T$ of transitions, *T'-induced subnet* $N' = (P, T', Pre', Post')$ of N, denoted by $N' \prec_{T'} N$, is a net that removes all transitions in $T \setminus T'$, where Pre' and $Post'$ are the restriction of Pre, $Post$ to T', respectively.

B. Basis Markings

In this section, a brief review of the notions of basis markings proposed by Cabasino et al. [14] is presented.

Definition 2.2: [14] 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. $\diamond$

Thus $\Sigma(M, t)$ is the set of unobservable transitions sequences whose firing at M enables t. Among all the explanations, we are interested in finding the minimal ones, i.e., the ones whose firing is necessary to enable t.

Definition 2.3: [14] 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 $Y_{min}(M, t) = \pi(\Sigma_{min}(M, t))$ the corresponding set of *minimal e-vectors*. $\diamond$

Many approaches can be applied to computing $Y_{min}(M, t)$. In particular, when the T_u-induced subnet is acyclic the approach proposed by Cabasino et al. [16] only requires algebraic manipulations.

Note that since a given place may have two or more unobservable input transitions, i.e., the T_u-induced subnet is not backward conflict free, the set of minimal explanations is not necessarily a singleton.

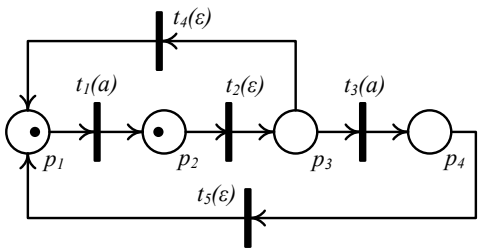

Fig. 1. LPN Model in Example 2.4

Example 2.4: Let us consider the LPN in Fig. 1. The set of explanations of transition t_1 at the initial marking is $\Sigma(M_0, t_1) = \{\varepsilon, t_2, t_2t_4\}$. The corresponding set of minimal explanations is $\Sigma_{min} = \{\varepsilon\}$ and the set of minimal e-vectors $Y_{min}(M_0, t_1) = \{\vec{0}\}$. Let $M = [0\ 1\ 0\ 1]^T$. We have $\Sigma_{min}(M, t_1) = \{t_2t_4, t_5\}$ and $Y_{min}(M, t) = \{[1\ 1\ 0]^T, [0\ 0\ 1]^T\}$. $\diamond$

Definition 2.5: [16] Let $G = (N, M_0, E, \ell)$ be an LPN and $w \in E^*$ be a given observation. We define the set of pairs (σ_o, σ_u) as

$$\begin{aligned}\mathcal{J}(w) =&\{(\sigma_o, \sigma_u) \in T_o^* \times T_u^* | \ell(\sigma_o) = w \\ &[\exists \sigma \in \mathcal{S}(w) : \sigma_o = P_o(\sigma), \sigma_u = P_u(\sigma)] \wedge \\ &[\nexists \sigma' \in \mathcal{S}(w) : \sigma_o = P_o(\sigma'), \sigma'_u = P_u(\sigma) \wedge \\ &\pi(\sigma'_u) \lneqq \pi(\sigma_u)]\},\end{aligned}$$

where σ_u is called a *justification* of w. Moreover, we define $\hat{Y}_{min}(w) = \{(\sigma_o, y) \in T_o^* \times \mathbb{N}^{n_u} | \exists (\sigma_o, \sigma_u) \in \mathcal{J}(w) : \pi(\sigma_u) = y\}$, where y is called a *j-vector*. $\diamond$

In other words, given an observation w, σ_o of a pair $(\sigma_o, \sigma_u) \in \mathcal{J}(w)$ is a sequence of observable transitions that produce w and σ_u is a minimal sequence of unobservable transitions that is needed to fire σ_o. Since more than one transition may be assigned with the same label from E, there are several sequences $\sigma_o \in T_o^*$ corresponding to the same observation w. Finally, basis markings are defined as follows.

Definition 2.6: Given an LPN $G = (N, M_0, E, \ell)$ and an observation w, the marking $M_b = M_0 + C_u \cdot y + C_o \cdot y'$ is called a *basis marking* corresponding to observation w, where $(\sigma_o, \sigma_u) \in \mathcal{J}(w)$, $y = \pi(\sigma_u)$ and $y' = \pi(\sigma_o)$. $\diamond$

Therefore, the basis markings corresponding to an observation w are those reachable from the initial marking by firing an observable sequence σ_o that produces w interleaved with those unobservable transitions whose firings are necessary to enable σ_o. We use $\mathcal{M}_b(w)$ to denote the set of basis markings corresponding to w and $\mathcal{M}_{basis} = \bigcup_{w \in \mathcal{L}(N, M_0)} \mathcal{M}_b(w)$ to denote the set of all basis markings. Clearly, $\mathcal{M}_{basis} \subseteq R(N, M_0)$. If the net is bounded, then the number of basis markings is finite.

Example 2.7: Consider again the LPN in Fig. 1. Assume $w = a$. Then we have $\mathcal{J}(w) = \{(t_1, \varepsilon), (t_3, t_2)\}$ and

correspondingly $\hat{Y}_{min}(w) = \{(t_1, \vec{0}), (t_3, [1\ 0\ 0]^T)\}$. Therefore, for observation w, one basis marking is $M_{b1} = M_0 + C_u \cdot \vec{0} + C_o \cdot [1\ 0]^T = [0\ 2\ 0\ 0]^T$ and the other is $M_{b2} = M_0 + C_u \cdot [1\ 0\ 0]^T + C_o \cdot [0\ 1]^T = [1\ 0\ 0\ 1]^T$, i.e., $\mathcal{M}_b(w) = \{M_{b1}, M_{b2}\}$. $\diamond$

Theorem 2.8: [16] Let $G = (N, M_0, E, \ell)$ be an LPN whose T_u-induced subnet is acyclic. For all $w \in \mathcal{L}(N, M_0)$, it holds that

$$\mathcal{C}(w) = \bigcup_{M_b \in \mathcal{M}_b(w)} \{M \in \mathbb{N}^m | M = M_b + C_u \cdot y : y \in \mathbb{N}^{n_u}\}.$$

$\diamond$

Thanks to the notion of basis markings, the set of markings consistent with an observation can be characterized using linear algebra without an exhaustive marking enumeration. Furthermore, in [12] it was also shown that if the T_u-induced subnet is acyclic, the justification can be recursively computed. Due to limited space, this result is illustrated by Example 2.9.

Example 2.9: Consider the LPN in Fig. 1 whose T_u-induced subnet is acyclic. Let $w = aa = w'l$, where $w' = a$ and $l = a$. From Example 2.7, we have $\mathcal{M}_b(w') = \{M_{b1}, M_{b2}\}$, and the transitions that may produce l are t_1 and t_3. At marking M_{b1}, $Y_{min}(M_{b1}, t_1) = \{e_1 = [1\ 1\ 0]^T\}$ and $Y_{min}(M_{b1}, t_3) = \{e_2 = [1\ 0\ 0]^T\}$; at marking M_{b2}, $Y_{min}(M_{b2}, t_1) = \{e_3 = \vec{0}\}$ and $Y_{min}(M_{b2}, t_3) = \emptyset$. The markings consistent with w are

$$M_{b3} = M_{b1} + C_o(\cdot, t_1) + C_u \cdot e_1 = [0\ 2\ 0\ 0]^T,$$

$$M_{b4} = M_{b1} + C_o(\cdot, t_3) + C_u \cdot e_2 = [0\ 1\ 0\ 1]^T,$$

$$M_{b5} = M_{b2} + C_o(\cdot, t_1) + C_u \cdot e_3 = [0\ 1\ 0\ 1]^T.$$

Therefore, $\mathcal{M}_b(w) = \{[0\ 2\ 0\ 0]^T, [0\ 1\ 0\ 1]^T\}$, and the set of markings consistent with w is $\mathcal{C}(w) = \{M \in \mathbb{N}^4 | M = M_{b3} + C_u \cdot y : y \geq \vec{0}\} \cup \{M \in \mathbb{N}^4 | M = M_{b4} + C_u \cdot y : y \geq \vec{0}\} = \{[0\ 2\ 0\ 0]^T, [0\ 1\ 1\ 0]^T, [1\ 1\ 0\ 0]^T, [0\ 1\ 0\ 1]^T, [0\ 0\ 1\ 1]^T, [1\ 0\ 1\ 0]^T\}$. $\diamond$

To compute basis markings, there is no need to enumerate explanations or justifications but only minimal e-vectors, which can be efficiently computed by matrix operations [16].

III. VERIFYING CURRENT-STATE OPACITY

In this section an approach to verifying current-state opacity of bounded Petri nets is presented.

A. Current-State Opacity

In the framework of LPNs, a secret is defined as a set of markings $S \subseteq R(N, M_0)$. It is assumed that the intruder has the knowledge of the net system $\langle N, M_0 \rangle$ but only has partial observation of the event occurrences.

Definition 3.1: Let G be an LPN and S be a secret. An observation w of G is said to be *current-state opaque* wrt S if $\mathcal{C}(w) \not\subseteq S$ holds. $\diamond$

A current-state opaque observation w implies that the intruder cannot infer that the current state belongs to the secret while observing w, i.e., $\exists M \in \mathcal{C}(w) : M \notin S$.

Based on Definition 3.1, the current-state opacity property of a system is defined.

Definition 3.2: Let G be an LPN and S be a secret. G is said to be *current-state opaque* wrt S if all observations w are current-state opaque wrt S. $\diamond$

B. Verifying Current-State Opacity

According to Definition 3.2, 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. In this section, based on the notion of basis markings an efficient approach to verifying current-state opacity is proposed. Let us first introduce the following definition.

Herein, the set of markings $R(N, M_0) \setminus S$ that do not belong to a secret are called *exposable markings*. Definition 3.3 generalizes this notion.

Definition 3.3: Let $G = (N, M_0, E, \ell)$ be an LPN and S be a secret. A marking $M \in R(N, M_0)$ of G is said to be *weakly exposable* if there exists a marking $M' \in R(N, M_0)$ such that $M[\sigma_u\rangle M'$ with $\sigma_u \in T_u^*$ and $M' \notin S$. $\diamond$

In simple words, a marking is weakly exposable if a marking not in the secret can be reached from it by firing unobservable transitions. Note that the firing sequence of unobservable transitions could be empty. Therefore, the set of weakly exposable markings is a superset of $R(N, M_0) \setminus S$.

Proposition 3.4: Let G be an LPN and S be a secret. An observation w is current-state opaque wrt S iff there exists a weakly exposable marking that belongs to set $\mathcal{C}(w)$. $\diamond$

Proposition 3.4 follows from Definitions 3.1 and 3.3. Based on Theorem 2.8 and Proposition 3.4, we have the following sufficient and necessary condition to verify current-state opacity of an LPN.

Theorem 3.5: Let $G = (N, M_0, E, \ell)$ be an LPN whose T_u-induced subnet is acyclic and S be a secret. G is current-state opaque wrt S iff $\forall w \in \mathcal{L}(N, M_0)$, there exists a basis marking $M_b \in \mathcal{M}_b(w)$ that is weakly exposable. $\diamond$

As a result, instead of exhaustively computing the sets $\mathcal{C}(w)$ for all $w \in \mathcal{L}(N, M_0)$, according to Theorem 3.5, 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 and to check if it contains a weakly exposable basis marking.

C. BRG for current-state opacity

In this section, we introduce the basis reachability graph (BRG) for current-state opacity that characterizes all basis markings and their opacity properties.

Given an LPN G and a secret S, the BRG for current-state opacity of G is a nondeterministic automaton that has as many nodes, i.e., states, as the number of basis markings. To make sure the number of nodes of the BRG is finite, we assume the net is bounded. In this sense, the BRG is a nondeterministic finite automaton (NFA). We denote $B = (X, E, f, x_0)$ the BRG for current-state opacity of a bounded LPN $G = (N, M_0, E, \ell)$. Each node of the BRG is associated with a pair $(M, \alpha(M))$, where $M \in \mathcal{M}_{basis}$ is a basis marking and $\alpha(M)$ is a binary scalar

that is defined as follows:

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

Therefore, $X \subseteq \mathcal{M}_{basis} \times \{0,1\}$. The initial node of the BRG is $x_0 = (M_0, \alpha(M_0))$. The event set of the BRG is identical to the alphabet E. The transition function can be determined by the following rule. If at marking M_b there is an observable transition t for which an explanation exists and the firing of t and one of its minimal explanations lead to M_b', then an edge from node $(M_b, \alpha(M_b))$ to node $(M_b', \alpha(M_b'))$ labeled $\ell(t)$ is defined in the BRG. The procedure to construct the BRG for current-state opacity is summarized in Algorithm 1.

Algorithm 1 Computation of the BRG for current-state opacity

Input: A bounded LPN $G = (N, M_0, E, \ell)$, and a secret S.

Output: The corresponding BRG $B = (X, E, f, x_0)$.

1: Let the initial node be $(M_0, \alpha(M_0))$ and assign no tag to it.
2: **while** nodes with no tag exist, **do**
3: select a node with no tag;
4: let M be the marking in the node;
5: **for all** t s.t. $Y_{min}(M,t) \neq \emptyset$ **do**
6: **for all** $e \in Y_{min}(M,t)$ **do**
7: $M' := M + C_u \cdot e + C(\cdot, t)$;
8: **if** $\nexists$ a node with M', **then**
9: compute $\alpha(M')$ and add a new node $(M', \alpha(M'))$;
10: **end if**
11: add an arc from node $(M, \alpha(M))$ to node $(M', \alpha(M'))$;
12: label the arc with $\ell(t)$;
13: **end for**
14: **end for**
15: tag the node "old".
16: **end while**
17: Remove all tags.

Even though the complexity of constructing a BRG (without considering the computation of $\alpha(M)$) highly depends on the net structure, it will not be worse than computing the RG. Furthermore, the size of the BRG in general is smaller than its corresponding RG, as illustrated by the example in Section IV.

In order to verify Theorem 3.5, it is required to construct the observer of the BRG. Since the intruder knows the initial marking, the observer of the BRG can be constructed by applying the algorithm in [18]. Each state of the observer is a set $\mathcal{M}_b(w)$ of basis markings corresponding to a certain observation. According to Theorem 3.5, if

all states of the BRG 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.

In the worst case, the number of states of the observer is $2^z - 1$, where $z = |\mathcal{M}_{basis}|$ is the number of basis markings. Note that as long as the observer is constructed, there is no need to reconstruct the observer of the BRG when the secret changes. All we need is to update the value of $\alpha(\cdot)$ for each basis marking.

Proposition 3.6 provides a sufficient but not necessary condition for verifying current-state opacity without constructing the observer for the BRG.

Proposition 3.6: Let $G = (N, M_0, E, \ell)$ be an LPN whose T_u-induced subnet is acyclic and S be a secret. If all basis markings $M_b \in \mathcal{M}_{basis}$ of G are weakly exposable, the system is current-state opaque wrt S. $\diamond$

If all states of the BRG have $\alpha(\cdot) = 1$, the LPN is current-state opaque; otherwise, current-state opacity requires further analysis.

D. Verification of Weakly Exposable Markings

It is well-known that GMECs [19] describe interesting subsets of the state space of a net and provide a linear algebra tool for Petri net analysis. To simplify the problem, now we assume that the secret is described by a set of GMECs [19]

$$S = \bigcap_{i=1}^{r} \{M \in \mathbb{N}^m | w_i^T \cdot M \leq k_i\},$$

where $w_i \in \mathbb{Z}^m$ and $k_i \in \mathbb{Z}$ with $i = 1, 2, \cdots, r$. Such a set of GMECs (w_i, k_i) is denoted as $S = \{M \in \mathbb{N}^m | W \cdot M \leq K\}$, where $W = [w_1, w_2, \cdots, w_r]^T$ and $K = [k_1, k_2, \cdots, k_r]^T$. In addition, the following constraint set is also defined.

Definition 3.7: 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 (w_i, k_i) be a GMEC from the secret. The (i, M)-*constraint set* is defined by

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

$\diamond$

By Theorem 2.1, the following result holds.

Proposition 3.8: Let $G = (N, M_0, E, \ell)$ be an LPN whose T_u-induced 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 (w_i, k_i) of the secret such that the corresponding (i, M)-constraint set is feasible. $\diamond$

Based on Proposition 3.8, the construction of the BRG for current-state opacity requires solving integer programming problems (IPP). However, for some net structures the complexity of constructing the BRG can be reduced by relaxing IPP into linear programming problems (LPP). Due to limited space, the complexity reduction part is not presented in this work.

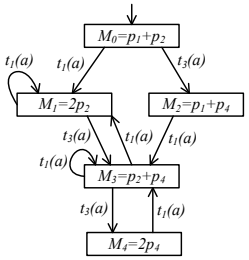

Fig. 2. BRG of the LPN in Fig. 1

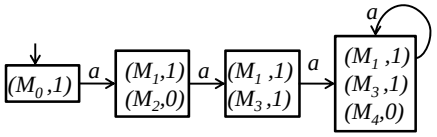

Fig. 3. Observer of the BRG in Fig. 2

Example 3.9: Consider again the LPN in Fig. 1. 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 $K = -2$. The BRG for current-state opacity of the LPN is shown in Fig. 2. For clarity, the corresponding transition is also labeled on the arc. The observer of the BRG is shown in Fig. 3. According to Theorem 3.5, the LPN is current-state opaque wrt the secret S. $\diamond$

Note that when the secret is characterized in other forms, Theorem 3.5 still provides a necessary and sufficient condition for current-state opacity. However, instead of solving IPP, the (i, M)-constraint set may be characterized in a more complex form.

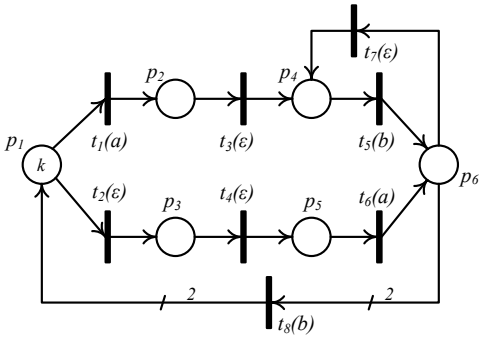

Fig. 4. Communication System

TABLE I

CASE STUDY OF DIFFERENT VALUES OF PARAMETER k

k	$\|R(N, M_0)\|$	$\|\mathcal{M}_{basis}\|$	$\|Obs_B\|$	S	S'
8	1287	45	39	Y	N
9	2002	55	45	Y	N
10	3003	66	54	Y	N
11	4368	78	61	Y	N
12	6188	91	71	Y	N
16	20349	153	111	Y	N
17	26334	171	121	Y	N

IV. EXAMPLE

Let us consider the LPN in Fig. 4. The initial marking of the net depends on the parameter $k \in \{2, 3, \cdots\}$ that describes the number of tokens[2] initially assigned to place p_1. One secret that we consider is $S = \{M \in \mathbb{N}^6 | W \cdot M \leq K\}$ with $W = [\ 0 \quad 1 \quad -1 \quad 1 \quad -1 \quad 0\ ]$ and $K = -1$. The other is $S' = \{M \in \mathbb{N}^6 | W \cdot M \leq K\}$ with $W = [\ 0 \quad 0 \quad 1 \quad 0 \quad 1 \quad 0\ ]$ and $K = 0$.

We use a MATLAB toolbox to compute the reachability graph $R(N, M_0)$, its corresponding observer Obs_R, the BRG for current-state opacity and its observer Obs_B. Several cases have been studied for different initial markings, i.e., different values of k, and the results are shown in Table I.

- Columns 2 and 3 show the cardinalities of the reachability set $R(N, M_0)$ and the set of basis markings $\mathcal{M}_{basis}$; column 4 shows the number of states of the BRG observer[3].
- Columns 5 and 6 show if the LPN is current-state opaque wrt secrets S and S', respectively. Y: the LPN is current-state opaque; N: the LPN is not current-state opaque.

The time in seconds required to compute the reachability graph, the BRG, and the observers are correspondingly illustrated in Table II, where"o.t." (out of time) denotes that the tool did not halt within three hours.

From Tables I and II, we have the following conclusions. The number of reachable markings is larger than that of basis markings, and as k increases, the cardinality of the reachability set grows much faster. Even though the number of states of the observer for the reachability graph is equal to that of the BRG observer, the time needed to compute the observer for the reachability graph is much longer and grows faster than that required to compute the BRG observer. As a result, the tool runs out of time when computing Obs_R with a large value of k. Namely, the time needed to analyze current-state opacity by using the existing method is much longer with respect to the proposed approach, especially when the net has a large initial marking. Last two columns in Table I show that in this example the current-state opacity property wrt secrets S or S' does not depend on the value of k.

[2]When $k = 1$, the LPN is not live.

[3]Since the observer of the reachability graph and the observer of the BRG have the same number of states, the column corresponds to $|Obs_R|$ is not presented in the table.

TABLE II

COMPUTATION TIME

k	$R(N, M_0)$	Obs_R	BRG	Obs_B
8	$2.2 \cdot 10^1$	$2.6 \cdot 10^1$	$1.3 \cdot 10^{-1}$	$1.2 \cdot 10^{-1}$
9	$5.7 \cdot 10^1$	$6.0 \cdot 10^1$	$1.6 \cdot 10^{-1}$	$1.6 \cdot 10^{-1}$
10	$1.3 \cdot 10^2$	$1.5 \cdot 10^2$	$2.0 \cdot 10^{-1}$	$2.4 \cdot 10^{-1}$
11	$2.8 \cdot 10^2$	$3.1 \cdot 10^2$	$2.4 \cdot 10^{-1}$	$3.0 \cdot 10^{-1}$
12	$6.0 \cdot 10^2$	$7.2 \cdot 10^2$	$2.9 \cdot 10^{-1}$	$4.1 \cdot 10^{-1}$
16	o.t.	o.t.	$5.8 \cdot 10^{-1}$	$1.0 \cdot 10^0$
17	o.t.	o.t.	$6.7 \cdot 10^{-1}$	$1.2 \cdot 10^0$

V. CONCLUSIONS AND FUTURE WORK

In this paper, a novel approach to verifying current-state opacity of bounded Petri nets is developed. We show that the notions of basis markings can also be effectively applied to verification of current-state opacity. A modified BRG for current-state opacity is proposed. For Petri nets whose unobservable subnet is acyclic, the current-state opacity property can be decided by just constructing the observer of the BRG rather than computing the observer of the reachability graph, which is generally of larger size. The efficiency of the presented approach is demonstrated by the example in the last section. The future research is to extend such results to other types of opacity properties.

ACKNOWLEDGMENT

This work was supported in part by the National Natural Science Foundation of China under Grant No. 61374068, the Recruitment Program of Global Experts, and the Science and Technology Department Fund, MSAR, under Grant No. 066/2013/A2.

REFERENCES

[1] N. Busi and R. Gorrieri. A survey on non-interference with Petri nets. In *Lectures on Concurrency and Petri Nets*, pages 328–344. Springer, 2004.

[2] M. K. Reiter and A. D. Rubin. Crowds: Anonymity for web transactions. *ACM Transactions on Information and System Security*, 1(1):66–92, 1998.

[3] V. Shmatikov. Probabilistic analysis of an anonymity system. *Journal of Computer Security*, 12(3):355–377, 2004.

[4] N. B. Hadj-Alouane, S. Lafrance, F. Lin, J. Mullins, and M. M. Yeddes. On the verification of intransitive noninterference in mulitlevel security. *IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics*, 35(5):948–958, 2005.

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

[6] A. Saboori and C. N. Hadjicostis. Verification of initial-state opacity in security applications of DES. In *9th International Workshop on Discrete Event Systems*, pages 328–333, 2008.

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

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

[9] Anooshiravan Saboori and Christoforos N Hadjicostis. Notions of security and opacity in discrete event systems. In *Decision and Control, 2007 46th IEEE Conference on*, pages 5056–5061. IEEE, 2007.

[10] Y. Tong, Z. W. Li, and A. Giua. General observation structures for petri nets. In *Emerging Technologies & Factory Automation (ETFA), 2013 IEEE 18th Conference on*, pages 1–4. IEEE, 2013.

[11] Y. Tong, Z. W. Li, and A. Giua. Observation equivalence of petri net generators. In *Discrete Event Systems*, volume 12, pages 338–343, 2014.

[12] ZhiWu Li and MengChu Zhou. Elementary siphons of petri nets and their application to deadlock prevention in flexible manufacturing systems. *Systems, Man and Cybernetics, Part A: Systems and Humans, IEEE Transactions on*, 34(1):38–51, 2004.

[13] A. Giua and C. Seatzu. Fault detection for discrete event systems using Petri nets with unobservable transitions. In *44th IEEE Conference on Decision and Control, 2005 European Control Conference*, pages 6323–6328, 2005.

[14] M. P. Cabasino, A. Giua, and C. Seatzu. Fault detection for discrete event systems using Petri nets with unobservable transitions. *Automatica*, 46(9):1531–1539, 2010.

[15] A. Giua, C. Seatzu, and D. Corona. Marking estimation of Petri nets with silent transitions. *IEEE Transactions on Automatic Control*, 52(9):1695–1699, Sept 2007.

[16] 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*, 19(9):989–1001, 2011.

[17] T. Murata. Petri nets: Properties, analysis and applications. *Procedings of the IEEE*, 77(4):541–580, April 1989.

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

[19] A. Giua, F. DiCesare, and M. Silva. Generalized mutual exclusion contraints on nets with uncontrollable transitions. In *1992 IEEE International Conference on Systems, Man and Cybernetics*, pages 974–979 vol.2, Oct 1992.