# Decidability of Opacity Verification Problems in Labeled Petri Net Systems ⋆

Yin Tong [a,c], Zhiwu Li [b,a], Carla Seatzu [c], Alessandro Giua [d,c]

[a] *School of Electro-Mechanical Engineering, Xidian University, Xi'an 710071, China*

[b] *Institute of Systems Engineering, Macau University of Science and Technology, Taipa, Macau*

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

[d] *Aix Marseille Univ, Université de Toulon, CNRS, ENSAM, LSIS, Marseille, France*

**Abstract**

A system is said to be *opaque* if an intruder that observes its evolution through a mask cannot infer that the system's evolution belongs to a given secret behavior. Opacity verification is the problem of determining whether the system is opaque with respect to a given secret or not. In this paper we address the decidability of the opacity verification problem. Using reduction approaches, we show that verification of initial-state, current-state, and language opacity is undecidable in labeled Petri nets.

*Key words:* Discrete event systems, Petri nets, opacity, decidability problems.

**Published as**:

Y. Tong, Z.W. Li, C. Seatzu, A. Giua, "Decidability of opacity verification problems in labeled Petri net systems," Automatica, Vol. 80, pp. 48-53, 2017. DOI: 10.1016/j.automatica.2017.01.013.

⋆ This work was supported by the National Natural Science Foundation of China under Grant Nos. 61374068, 61472295, 61673309, the Science and Technology Development Fund, MSAR, under Grant No. 078/2015/A3.

*Email addresses:* yintong@stu.xidian.edu.cn (Yin Tong), zhwli@xidian.edu.cn (Zhiwu Li), seatzu@diee.unica.it (Carla Seatzu), alessandro.giua@lsis.org; giua@diee.unica.it (Alessandro Giua).

## 1 Introduction

Opacity in discrete event systems (DESs) has been extensively investigated over the last decade. For a thorough and comprehensive review on this topic, we refer the reader to (Jacob et al. 2016) and (Wu & Lafortune 2013). Consider a system whose evolution can be observed by an external observer (usually called an intruder in this setting) through a mask that partially hides the event occurrence and the state trajectory. A system is said to be opaque with respect to a given secret behavior when the intruder cannot infer if the system's evolution belongs to the secret based on the available observation. It is typically assumed that the intruder has full knowledge of the system's structure.

Several opacity properties have been defined for DESs, among which we focus on *current-state opacity*, *initial-state opacity* and *language-based opacity*.

- When dealing with current-state opacity, the secret is defined as a set of states and the initial state is (partially) known to the intruder. A system is current-state opaque if the intruder is never able to establish if the current state of the system is within the set of secret states (Bryans et al. 2005, Saboori & Hadjicostis 2007, Tong et al. 2015*a*).
- When dealing with initial-state opacity, the secret is also defined as a set of states and the intruder has no knowledge about the initial state. A system is initial-state opaque if the intruder cannot establish if the evolution of the system has started from a secret state. Initial-state opacity (ISO) has been defined in the Petri net framework by Bryans *et al.* (Bryans et al. 2005). Saboori and Hadjicostis (Saboori & Hadjicostis 2008) proposed a new ISO definition in the automaton framework that we extended to Petri nets in (Tong et al. 2015*b*). In this paper we call it *reach-initial-state opacity* (R-ISO). As discussed in detail in Section 4, R-ISO is a particular case of ISO and may be meaningful in a variety of security problems.
- In the case of language-based opacity, the secret is defined as a language, i.e., a set of event sequences, and the initial state is (partially) known to the intruder. A system is language-based opaque if the intruder cannot establish if the evolution of the system belongs to the secret. Several types of language-based opacity properties have been defined. For instance, *language opacity*, *weak opacity* (Lin 2011) and *strict language opacity* (Tong, Li, Seatzu & Giua 2016*b*).

In the framework of automata two types of observation masks have been investigated in the literature: static and dynamic (Cassez et al. 2012, Lin 2011). A mask is static if the set of events that the intruder can observe is fixed. It is dynamic if the set of observable events changes with the state or the trace of the system. Obviously, the dynamic mask is a generalization of the static one. In Petri nets, similar observation masks have been defined (Tong, Li & Giua 2016). In this work we focus on the opacity problems in (unbounded) labeled Petri nets, i.e., Petri nets with static observation masks.

Opacity verification (Lin 2011, Saboori & Hadjicostis 2011, 2013, Wu & Lafortune 2013, Tong, Li, Seatzu & Giua 2016*b*, Tong et al. 2017) consists in determining whether a system is opaque with respect to a given secret. When opacity is violated, different approaches (Dubreil et al. 2010, Cassez et al. 2012, Wu & Lafortune 2014, Falcone & Marchand 2015, Tong, Li, Seatzu & Giua 2016*a*) have been proposed to turn an unopaque system into an opaque one. In this paper, we study the decidability of opacity verification problems in labeled Petri net systems, focusing on current-state, reach-initial-state and language opacity. In the sequel of this paper we use "opacity problem" to denote "opacity verification problem" for simplicity.

Many contributions related to the decidability of opacity problems in DESs have been proposed in (Bryans et al. 2005, 2008, Cassez 2009, Saboori & Hadjicostis 2010, Jacob et al. 2016). It has been shown that current-state, initial-state and language opacity problems are decidable in finite automata (Bryans et al. 2008). Nonetheless, the current-state opacity problem in probabilistic finite automata and the language-based opacity in timed automata are undecidable (Cassez 2009, Saboori & Hadjicostis 2010). Bryans *et al.* (Bryans et al. 2005) have proven that for *bounded* Petri nets current-state and initial-state opacity problems are decidable. Moreover, general opacity problems in transition systems are undecidable, as well as the initial-state opacity problem in Petri nets (Bryans et al. 2008). Decidability of opacity problems in different systems have been surveyed in (Jacob et al. 2016). However, the decidability of current-state, reach-initial-state and language opacity problems in Petri nets still requires further investigation.

The main contribution of this work consists in proving that current-state, reach-initial-state and language opacity problems are undecidable. All proofs are carried out using reduction.

The rest of the paper is organized as follows. In Section 2 basic notions of Petri nets are recalled. The decidability of the current-state, reach-initial-state and language opacity problems is discussed in Sections 3, 4, and 5, respectively. Finally, conclusions are drawn in Section 6 where we also discuss our future work in this area.

## 2 Preliminaries

In this section we recall the basics of labeled Petri nets. For more details, we refer the reader to (Peterson 1981, Seatzu et al. 2013).

A *Petri net* is a structure $N = (P, T, Pre, Post)$, where $P$ is a set of *places* graphically represented by circles; $T$ is a set of *transitions* graphically represented by bars with $P \cup T \neq \emptyset$ and $P \cap T = \emptyset$; $Pre : P \times T \to \mathbb{N}$, 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, where $\mathbb{N} = \{0, 1, 2, \ldots\}$. The incidence matrix of a net is denoted by $C = Post - Pre$. A transition without any input place is called a *source transition.*

A *marking* is a vector $M : P \to \mathbb{N}$ that assigns to each place of a Petri net a non-negative integer number of tokens, graphically represented by black dots. The marking of place $p$ is denoted by $M(p)$. A marking can also sometimes be represented as a multiset $M = \sum_{p \in P} M(p) \cdot p$. 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 $\sigma$ yields $M'$. We denote $L(N, M_0) = \{\sigma \in T^* | M_0[\sigma\rangle\}$ the set of all transition sequences enabled at $M_0$.

A marking $M$ is *reachable* in $\langle N, M_0 \rangle$ if there exists a sequence $\sigma \in T^*$ 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 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 for any reachable marking $M \in R(N, M_0)$, $M(p) \leq k$ holds.

A *labeled Petri net* (LPN) system is a 4-tuple $G = (N, M_0, E, \ell)$, where $\langle N, M_0 \rangle$ is a Petri net system, $E$ is 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 $\varepsilon$. A transition labeled with a symbol in $E$ is said to be *observable*; a transition labeled with the empty word is *unobservable* (or silent). The labeling function can be extended to sequences $\ell : T^* \to E^*$ as $\ell(\sigma t) = \ell(\sigma)\ell(t)$ with $\sigma \in T^*$ and $t \in T$. Note that $\sigma$ could be the empty sequence (i.e., a sequence of events with length 0) and in this case, $\ell(\sigma) = \varepsilon$. The *generated language* of $G$ is $\mathcal{L}(G) = \{w \in E^* | \exists \sigma \in L(N, M_0) : w = \ell(\sigma)\}$. The *generated language from a marking* $M$ is $\mathcal{L}(N, M) = \{w \in E^* | \exists \sigma \in T^* : M[\sigma\rangle, w = \ell(\sigma)\}$. Therefore, $\mathcal{L}(G) = \mathcal{L}(N, M_0)$. Given a set of markings $\mathcal{M}$, $\mathcal{L}(N, \mathcal{M}) = \bigcup_{M \in \mathcal{M}} \mathcal{L}(N, M)$ is defined.

Finally, we generalize the notion of LPN systems to deal with the case where the net has a set (could be infinite) of initial markings $\mathcal{M}_0 \subseteq \mathbb{N}^m$. In such a case, the LPN system is denoted as $G = (N, \mathcal{M}_0, E, \ell)$, its reachability set is $R(N, \mathcal{M}_0) = \bigcup_{M_0 \in \mathcal{M}_0} R(N, M_0)$, and the generated language of $G$ is $\mathcal{L}(G) = \mathcal{L}(G, \mathcal{M}_0)$.

## 3 Current-State Opacity

In this section we discuss the decidability of the current-state opacity problem in LPN systems. First, we recall the notion of current-state opacity [1] defined in (Bryans et al. 2005).

**Definition 1** *[Petri Net Current-State Opacity] Let $G = (N, \mathcal{M}_0, E, \ell)$ be an LPN system and $S \subseteq R(N, \mathcal{M}_0)$ be a secret set. G is said to be* current-state opaque *(CSO) wrt S if for all $M_0 \in \mathcal{M}_0$, $M \in S$ and $\sigma \in L(N, M_0)$ such that $M_0[\sigma\rangle M$, there exists $M_0' \in \mathcal{M}_0, \sigma' \in L(N, M_0')$ such that $\ell(\sigma') = \ell(\sigma)$ and $M_0'[\sigma'\rangle M' \notin S$.*

An LPN system being current-state opaque means that for every transition sequence $\sigma$ leading to a marking in the secret set, there exists another transition sequence $\sigma'$ whose firing leads to a nonsecret marking, and the two sequences produce the same observation $\ell(\sigma) = \ell(\sigma')$. As a consequence, when the intruder observes the behavior of a current-state opaque LPN system, it cannot conclude whether the current state is contained or not in the secret.

[1] In (Bryans et al. 2005) it is assumed that $\mathcal{M}_0$ is finite, and the property is called *final opacity.* However, "current-state opacity" is used by most of the researchers.

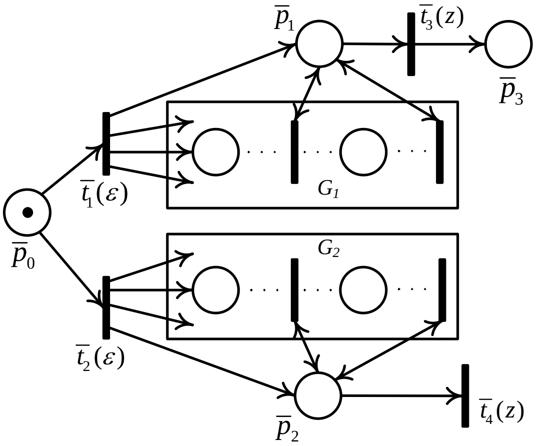

Fig. 1. The LPN system $G$ constructed in the proof of Theorem 3.

We point out that an LPN system with a finite set of initial markings can always be converted into an equivalent LPN system [2] with one initial marking. The procedure requires adding two new places, called $p_0$ and $p_0'$, and $r = |\mathcal{M}_0|$ new unobservable transitions, called $t_{u1}, \ldots, t_{ur}$. The initial marking of the new net assigns a single token to place $p_0$. The firing of a transition $t_{ui}$ (with $i = 1, \ldots, r$) moves the token from $p_0$ to $p_0'$ and produces in the other places a token configuration that coincides with the $i$-th marking in $\mathcal{M}_0$. To prevent transitions (in particular source transitions) from firing before one of the transitions $t_{ui}$ does, self-loops are added between $p_0'$ and all other transitions except $t_{ui}$ for $i = 1, \ldots, r$ (cf. the proof of Theorem 7). Therefore, current-state opacity defined in Definition 1 with a finite set $\mathcal{M}_0$ is equivalent to the one defined in (Tong et al. 2015*a*).

**Definition 2** *[Petri Net Current-State Opacity Problem] Consider an LPN system $G = (N, \mathcal{M}_0, E, \ell)$ and a secret set $S \subseteq R(N, \mathcal{M}_0)$. The* Petri net current-state opacity problem *consists in determining whether $G$ is current-state opaque wrt $S$ or not.*

In (Bryans et al. 2005) it has been proven that if $G$ is bounded, which also implies that $\mathcal{M}_0$ is finite, the Petri net current-state opacity problem is decidable. In the following, we show that in general such a problem is undecidable.

**Theorem 3** *The Petri net current-state opacity problem is undecidable.*

**PROOF.** We preliminarily recall that the Petri net language containment problem, i.e., the problem of determining whether the language generated by an LPN system is contained in the language generated by another LPN system, is not decidable (Reutenauer 1990). We now prove the theorem by showing that the Petri net language containment problem can be reduced to the Petri net current-state opacity problem for a singleton secret set and a single initial marking.

Let $\mathcal{L}(G_1)$ and $\mathcal{L}(G_2)$ be the languages generated by two arbitrary LPN systems $G_1 = (N_1, M_{01}, E_1, \ell_1)$ and $G_2 = (N_2, M_{02}, E_2, \ell_2)$, respectively. Let $P_i$ ($|P_i| = m_i$) and $T_i$ ($|T_i| = n_i$), respectively, be the set of places and transitions of $G_i$, for $i = 1, 2$. We construct a new LPN system $G = (N, M_0, E, \ell)$ based on $G_1$ and $G_2$ by the following steps:

i) Duplicate the structures of $G_1$ and $G_2$ in $G$.
ii) Add to $G$ places: $\overline{p}_0$, $\overline{p}_1$, $\overline{p}_2$, and $\overline{p}_3$, unobservable transitions: $\overline{t}_1$ and $\overline{t}_2$, and observable transitions: $\overline{t}_3$ and $\overline{t}_4$ such that $\ell(\overline{t}_3) = \ell(\overline{t}_4) = z \notin (E_1 \cup E_2)$.
iii) Add new arcs: $Pre(\overline{p}_0, \overline{t}_i) = 1$ for $i = 1, 2$; $Pre(\overline{p}_1, \overline{t}_3) = 1$; $Pre(\overline{p}_2, \overline{t}_4) = 1$; $\forall t \in T_1$, $Pre(\overline{p}_1, t) = 1$, $Post(\overline{p}_1, t) = 1$; $\forall t \in T_2$, $Pre(\overline{p}_2, t) = 1$, $Post(\overline{p}_2, t) = 1$; $Post(\overline{p}_1, \overline{t}_1) = 1$; $Post(\overline{p}_2, \overline{t}_2) = 1$; $Post(\overline{p}_3, \overline{t}_3) = 1$; $\forall p \in P$ such that $M_{01}(p) \neq 0$, $Post(p, \overline{t}_1) = M_{01}(p)$; $\forall p \in P$ such that $M_{02}(p) \neq 0$, $Post(p, \overline{t}_2) = M_{02}(p)$.
iv) $M_0 = \overline{p}_0$.

As a result, the number of places and transitions in $G$ are $|P| = m_1 + m_2 + 4$ and $|T| = n_1 + n_2 + 4$, respectively, and $E = E_1 \cup E_2 \cup \{z\}$. The LPN system $G$ is depicted in Fig. 1. For $i = 1, 2$, the firing of $\overline{t}_i$ initializes $G_i$. Namely, the

[2] "Equivalent" refers to the fact that two nets have the same opacity property.

markings reached after firing $\bar{t}_i$ are $M = \overline{p}_i + \Sigma_{p\in P_i} M_{0i}(p) \cdot p$. Self-loops between $\overline{p}_i$ and transitions in $G_i$ prevent source transitions from firing before $\bar{t}_i$ fires.

Let us consider the secret set $S = \{\overline{p}_3\}$. In the following we prove that

$$\mathcal{L}(G_1) \subseteq \mathcal{L}(G_2) \Leftrightarrow G \text{ is current-state opaque wrt } S.$$

We first prove that if $G$ is current-state opaque wrt $S$, then $\mathcal{L}(G_1) \subseteq \mathcal{L}(G_2)$ holds. Assume that $G$ is current-state opaque wrt $S$. Then for every $\sigma$ leading to the secret marking, there exists $\sigma' \in L(N, M_0)$ that does not lead to the secret but produces the same observation, i.e., $\ell(\sigma) = \ell(\sigma')$. Based on the structure of $G$, the transition sequences that lead to the secret marking take the form $\sigma = \bar{t}_1\sigma_1\bar{t}_3$, where $\sigma_1 \in L(N_1, M_{01})$ and produce observation $\ell(\sigma) = \ell(\sigma_1)z$, where $\ell(\sigma_1) \in \mathcal{L}(G_1)$. Moreover, it appears evident that $\sigma'$ should take the form $\sigma' = \bar{t}_2\sigma_2\bar{t}_4$, where $\sigma_2 \in L(N_2, M_{02})$. Indeed, these are the only sequences that produce an observation ending with $z$ and not leading to the secret marking. This implies that for any $\sigma_1 \in L(N_1, M_{01})$, there exists $\sigma_2 \in L(N_2, M_{02})$ such that $\ell(\sigma_1) = \ell(\sigma_2)$, i.e., $\mathcal{L}(G_1) \subseteq \mathcal{L}(G_2)$.

Analogously, we can prove that if $\mathcal{L}(G_1) \subseteq \mathcal{L}(G_2)$ then $G$ is current-state opaque wrt $S$. Indeed, if $\mathcal{L}(G_1) \subseteq \mathcal{L}(G_2)$, then $L(N_1, M_{01}) \subseteq L(N_2, M_{02})$ and for any sequence $\sigma = \bar{t}_1\sigma_1\bar{t}_3$ that leads to the secret marking, it corresponds a sequence $\sigma' = \bar{t}_2\sigma_2\bar{t}_4$, where $\sigma_1 \in L(N_1, M_{01})$ and $\sigma_2 \in L(N_2, M_{02})$, that produces the same observation but leads to a nonsecret marking, i.e., $G$ is current-state opaque wrt $S$.

Therefore, for the general case where the secret is an arbitrary subset of $R(N, M_0)$ and the initial marking set may not be a singleton, the Petri net current-state opacity problem is undecidable. □

## 4 Initial-State Opacity

The notion of initial-state opacity was first defined for Petri nets by Bryans *et al.* in (Bryans et al. 2005). According to the definition given by Bryans *et al.*, when the intruder starts its observation it does not know in which marking the system is, but simply knows that it belongs to a given set $\mathcal{M}_0$. The secret set $S$ is a subset of $\mathcal{M}_0$. If the system is initial-state opaque, then the intruder cannot infer, based on its observation, whether the evolution has started from a secret marking or a nonsecret one.

**Definition 4** *[Petri Net Initial-State Opacity] Let $G = (N, \mathcal{M}_0, E, \ell)$ be an LPN system and $S \subseteq \mathcal{M}_0$ be a secret set. G is said to be* initial-state opaque *(ISO) wrt $S$ if for all $M \in S$ and for all $w \in \mathcal{L}(N, M)$,*

$$\exists M' \in \mathcal{M}_0 \setminus S : w \in \mathcal{L}(N, M').$$

In simple words, a system is said to be initial-state opaque if for any observation generated from a secret marking, there always exists a nonsecret marking in $\mathcal{M}_0$ from which the same observation can be generated.

Note that $\mathcal{M}_0 \subseteq \mathbb{N}^m$ in Definition 4 could be an infinite set. However, in the original definition of ISO in (Bryans et al. 2005, 2008) $\mathcal{M}_0$ was assumed to be finite. The authors proved that if $R(N, \mathcal{M}_0)$ is finite as well, the problem of determining if $G$ is ISO wrt $S$, is decidable; on the contrary, if $R(N, \mathcal{M}_0)$ is infinite, the problem is undecidable.

In this paper we focus on a particular ISO definition for Petri nets proposed in (Tong et al. 2015*b*), herein called *reach-initial-state opacity.*

**Definition 5** *[Petri Net Reach-Initial-State Opacity] Let $G = (N, M_{st}, E, \ell)$ be an LPN system and $S \subseteq R(N, M_{st})$ be a secret set. G is said to be* reach-initial-state opaque *(R-ISO) wrt $S$ if for all $M \in S$, and for all $w \in \mathcal{L}(N, M)$,*

$$\exists M' \in R(N, M_{st}) \setminus S : w \in \mathcal{L}(N, M').$$

According to Definition 5, a system $G = (N, M_{st}, E, \ell)$ is said to be R-ISO if for any secret marking and any observation generated from such a secret marking, there exists a nonsecret marking in $R(N, M_{st})$ from which the

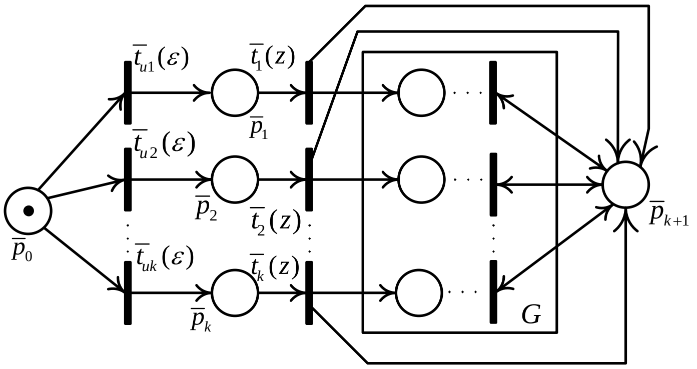

Fig. 2. The LPN system $G'$ constructed in the proof of Theorem 7.

same observation can be generated. Comparing Definition 5 with Definition 4, it is evident that R-ISO is a special case of ISO where $\mathcal{M}_0$ is a subset of $\mathbb{N}^m$ such that $\mathcal{M}_0 = R(N, M_{st})$. Namely, R-ISO only considers a special class of $\mathcal{M}_0$ instead of an arbitrary subset of $\mathbb{N}^m$. However, as discussed in the following, it is still worth studying them separately.

The ISO problem considered in the automaton setting (see Definition 1 in (Saboori & Hadjicostis 2008)) can be summarized as follows: given the structure of an automaton whose initial state is unknown, determine if the intruder can infer if such a state belongs to the secret by observing the system's evolution. Note that the structure of the automaton explicitly contains the full knowledge of the system's state space and thus it is implicitly assumed that the initial state must belong to such a space.

Consider on the contrary a Petri net. The structure of the net $(N, E, \ell)$ is not a dynamical system and contains no information on the state space. We need to associate to the net an initial marking so that the state space can be determined by computing its reachability set. Therefore, the counterpart for Petri nets of the ISO problem defined above can be stated as follows: given a Petri net *system* and its reachability set, assuming its initial marking is unknown, determine if the intruder can infer whether such a marking belongs to the secret by observing the system's evolution. This is what we call R-ISO problem: it is not an artificial problem but the natural Petri net counterpart of the ISO problem in automata.

Therefore, the new definition we propose of R-ISO not only formalizes an important property that so far has not been discussed, but also clarifies the difference between ISO for Petri nets and ISO for automata, that, even if having the same name, are different properties. From a practical point of view, if the R-ISO problem were decidable (unfortunately, as we show later, it is undecidable) and a plant could be proven to enjoy this property, the system's operator could decide (possibly at some extra cost) to block for some time all observations so as to ensure opacity when the observations are re-established.

**Definition 6** *[Petri Net Reach-Initial-State Opacity Problem] Consider an LPN system $G = (N, M_{st}, E, \ell)$ and a secret set $S \subseteq R(N, M_{st})$. The* Petri net reach-initial-state opacity problem *consists in determining whether $G$ is reach-initial-state opaque wrt $S$ or not.*

Based on the results in (Bryans et al. 2005), if the net is bounded, i.e., $R(N, M_{st})$ is finite, the Petri net R-ISO problem is decidable. On the other hand, the undecidability of the Petri net ISO problem does not imply its undecidability for a special class of $\mathcal{M}_0$. Therefore, it is necessary to investigate the decidability of the Petri net R-ISO problem. In the following, we prove its undecidability.

**Theorem 7** *The Petri net reach-initial-state opacity problem is undecidable.*

**PROOF.** It has been proven that the ISO problem in Petri nets is undecidable (Bryans et al. 2008), where $\mathcal{M}_0$ is finite. We prove this theorem by showing that the ISO problem for finite secret sets, which is undecidable, can be reduced into the Petri net R-ISO problem.

Consider an LPN system $G = (N, \mathcal{M}_0, E, \ell)$ with $|P| = m$ and $|T| = n$, where $\mathcal{M}_0 = \{M_0^1, M_0^2, \cdots, M_0^k\} \subseteq \mathbb{N}^m$ is a finite set of initial markings, and a secret set $S = \{M_0^1, M_0^2, \cdots M_0^r\} \subseteq \mathcal{M}_0$ with $r \leq k$. Starting from $G$, let us construct a new LPN system $G' = (N', M'_{st}, E', \ell')$, where $N' = (P', T', Pre', Post')$, by the following steps:

i) Add to $G$ places: $\overline{p}_0, \overline{p}_1, \ldots, \overline{p}_{k+1}$, unobservable transitions $\overline{t}_{u1}, \overline{t}_{u2}, \ldots, \overline{t}_{uk}$, and observable transitions: $\overline{t}_1, \overline{t}_2, \ldots, \overline{t}_k$, such that $\ell(\overline{t}_1) = \cdots = \ell(\overline{t}_k) = z \notin E$.
ii) Add arcs: for $i = 1, 2, \cdots, k$, $Pre(\overline{p}_0, \overline{t}_{ui}) = 1$, $Pre(\overline{p}_i, \overline{t}_i) = 1$, $Post(\overline{p}_i, \overline{t}_{ui}) = 1$, $Post(\overline{p}_{k+1}, \overline{t}_i) = 1$; $\forall p \in P$ such that $M_0^i(p) \neq 0$, $Post(p, \overline{t}_i) = M_0^i(p)$; $\forall t \in T$, $Pre(\overline{p}_{k+1}, t) = 1$, $Post(\overline{p}_{k+1}, t) = 1$.
iii) $M'_{st} = \overline{p}_0$.

The resulting $G'$ is depicted in Fig. 2. Obviously $E' = E \cup \{z\}$. Moreover, the number of places and transitions in $G'$ are $|P'| = m + k + 2$ and $|T'| = n + 2k$, respectively. The firing of $\overline{t}_{ui}\overline{t}_i$ initializes $G$ at $M_0^i$ (for $i = 1, 2, \ldots, k$). Place $\overline{p}_{k+1}$ is added to prevent source transitions in $G$ from firing before the firing of $\overline{t}_{ui}\overline{t}_i$.

Let us consider the secret set $S' = \{\overline{p}_0, \overline{p}_1, \ldots, \overline{p}_r\}$. In the following we prove that

$$G \text{ is ISO wrt S} \Leftrightarrow G' \text{ is R-ISO wrt } S'.$$

First we prove that if $G'$ is R-ISO wrt $S'$, then $G$ is ISO wrt $S$. Assume that $G'$ is R-ISO wrt $S'$. Then for any observation $w$ generated from markings in $S'$, there exists a marking $M' \in R(N', M'_{st}) \setminus S'$ from which the same observation $w$ can be generated, i.e.,

$$\mathcal{L}(N', S') \subseteq \mathcal{L}(N', R(N', M'_{st}) \setminus S'). \tag{1}$$

By the structure of $G'$,

$$\mathcal{L}(N', S') = \{w' \in E'^* | w' = zw, w \in \mathcal{L}(N, S)\} \tag{2}$$

holds. Moreover, the set of words in $\mathcal{L}(N', R(N', M'_{st}) \setminus S')$ having $z$ as the prefix is equal to $\mathcal{L}(N', \{\overline{p}_{r+1}, \ldots, \overline{p}_k\})$. Therefore, by Eq. (1), we have

$$\mathcal{L}(N', S') \subseteq \mathcal{L}(N', \{\overline{p}_{r+1}, \ldots, \overline{p}_k\}). \tag{3}$$

Again by the structure of $G'$, we have

$$\begin{aligned} \mathcal{L}(N', \{\overline{p}_{r+1}, \ldots, \overline{p}_k\}) = \{w' \in E'^* | w' = zw, \\ w \in \mathcal{L}(N, \mathcal{M}_0 \setminus S)\} \end{aligned} \tag{4}$$

By Eqs. (2), (3) and (4), it follows that $\mathcal{L}(N, S) \subseteq \mathcal{L}(N, \mathcal{M}_0 \setminus S)$. Namely, for all $M \in S$, $w \in \mathcal{L}(N, M)$, there exists $M' \in \mathcal{M}_0 \setminus S$ such that $w \in \mathcal{L}(N, M')$, i.e., $G$ is ISO wrt $S$.

Following the same reasoning, we can prove that if $G$ is ISO wrt $S$, then $G'$ is R-ISO wrt $S'$. In more detail, if $G$ is ISO wrt $S$, then $\mathcal{L}(N, S) \subseteq \mathcal{L}(N, \mathcal{M}_0 \setminus S)$ holds. This implies the inclusion relationship in Eq. (3) and, taking into account the structure of $G'$, the inclusion relationship in Eq. (1). Therefore, we conclude that $G'$ is R-ISO wrt $S'$. □

## 5 Language-Based Opacity

Language opacity was first introduced in (Badouel et al. 2007) in the framework of finite automata and then extended to Petri nets (Tong, Li, Seatzu & Giua 2016*b*). In the case of language opacity the secret is defined as a language. In this section we first recall the notion of language opacity in LPN systems, then we formalize the language opacity problem, and finally, we prove that such a problem is undecidable.

**Definition 8** *[Petri Net Language Opacity] Let $G = (N, \mathcal{M}_0, E, \ell)$ be an LPN system and $S \subseteq T^*$ be a secret language. G is said to be* language opaque *(LO) wrt S if for all $\sigma \in L(N, \mathcal{M}_0) \cap S$, there exists $\sigma' \in L(N, \mathcal{M}_0) \setminus S$ such that $\ell(\sigma) = \ell(\sigma')$.*

In other words, a system is language opaque wrt a given secret if for any observation that can be generated by a sequence in the secret, there exists another nonsecret sequence generating the same observation.

**Definition 9** *[Petri Net Language Opacity Problem] Consider an LPN system $G = (N, \mathcal{M}_0, E, \ell)$ and a secret language $S \subseteq T^*$. The* language opacity problem *consists in determining whether $G$ is language opaque wrt $S$ or not.*

**Theorem 10** *The Petri net language opacity problem is undecidable.*

**PROOF.** The proof is carried out by showing that the Petri net current-state opacity problem for finite secret sets, which is proven undecidable by Theorem 3, can be reduced into the Petri net language opacity problem.

Consider an LPN system $G = (N, \mathcal{M}_0, E, \ell)$ and a secret set $S \subseteq R(N, \mathcal{M}_0)$. Let us prove that

$$G \text{ is CSO wrt } S \Leftrightarrow G \text{ is LO wrt } S',$$

where $S' = \{\sigma \in T^* | \exists M_0 \in \mathcal{M}_0, M \in S : M_0[\sigma\rangle M\}$.

First we prove that if $G$ is current-state opaque wrt $S$, then $G$ is language opaque wrt $S'$. Assume that $G$ is current-state opaque wrt $S$. Then for any $M_0 \in \mathcal{M}_0$, $M \in S$ and $\sigma \in T^*$ such that $M_0[\sigma\rangle M$, there exist $M_0' \in \mathcal{M}_0$, $M' \in R(N, \mathcal{M}_0) \setminus S$ and $\sigma' \in T^*$ such that $M_0'[\sigma'\rangle M'$ and $\ell(\sigma) = \ell(\sigma')$. This implies that for all $\sigma \in S'$, there exists $\sigma' \in L(N, \mathcal{M}_0) \setminus S'$ with $\ell(\sigma) = \ell(\sigma')$. Therefore, $G$ is language opaque wrt $S'$.

Now we prove that if $G$ is language opaque wrt $S'$, then $G$ is current-state opaque wrt $S$. Assume that $G$ is language opaque wrt $S'$. Then for any $\sigma \in L(N, \mathcal{M}_0) \cap S'$, there exists at least a firing sequence $\sigma' \in L(N, \mathcal{M}_0) \setminus S'$ such that $\ell(\sigma') = \ell(\sigma)$. Since $\sigma' \notin S'$, $M' \notin S$, where $M_0[\sigma'\rangle M'$ and $M_0 \in \mathcal{M}_0$. Namely, for any transition sequence leading to a marking in $S$, there exists a transition sequence producing the same observation but leading to a marking not in $S$. Therefore, $G$ is current-state opaque wrt $S$. □

## 6 Conclusions and Future Work

In this paper, the decidability of current-state, reach-initial-state and language opacity problems in Petri nets is addressed, where reach-initial-state opacity is a special case of initial-state opacity defined in (Bryans et al. 2005). In particular, showing that all such problems are undecidable for special classes of secrets, we conclude that, in general, Petri net current-state, reach-initial-state, and language opacity problems are undecidable since if a problem is undecidable under special assumptions (e.g., the secret set is finite), the same problem under less restrictive assumptions is obviously undecidable as well.

As a future work, we plan to characterize the classes of Petri nets whose opacity problems can be proven to be decidable. For such classes, we will also try to develop efficient methods for opacity analysis.

## References

Badouel, E., Bednarczyk, M., Borzyszkowski, A., Caillaud, B. & Darondeau, P. (2007), 'Concurrent secrets', *Discrete Event Dynamic Systems* **17**(4), 425–446.

Bryans, J., Koutny, M., Mazaré, L. & Ryan, P. (2008), 'Opacity generalised to transition systems', *International Journal of Information Security* **7**(6), 421–435.

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

Cassez, F. (2009), The dark side of timed opacity, *in* 'Advances in Information Security and Assurance', Springer, pp. 21–30.

Cassez, F., Dubreil, J. & Marchand, H. (2012), 'Synthesis of opaque systems with static and dynamic masks', *Formal Methods in System Design* **40**(1), 88–115.

Dubreil, J., Darondeau, P. & Marchand, H. (2010), 'Supervisory control for opacity', *IEEE Transactions on Automatic Control* **55**(5), 1089–1100.

Falcone, Y. & Marchand, H. (2015), 'Enforcement and validation (at runtime) of various notions of opacity', *Discrete Event Dynamic Systems* **25**(4), 531–570.

Jacob, R., Lesage, J. J. & Faure, J. M. (2016), 'Overview of discrete event systems opacity: models, validation, and quantification', *Annual Reviews in Control* **41**, 135–146.

Lin, F. (2011), 'Opacity of discrete event systems and its applications', *Automatica* **47**(3), 496–503.

Peterson, J. (1981), *Petri net theory and the modeling of systems*, Prentice Hall PTR.

Reutenauer, C. (1990), *The mathematics of Petri nets*, Prentice-Hall, Inc.

Saboori, A. & Hadjicostis, C. (2010), Probabilistic current-state opacity is undecidable, *in* 'Proc. of the 19th International Symposium on Mathematical Theory of Networks and Systems–MTNS', Budapest, Hungary, pp. 477–483.

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

Saboori, A. & Hadjicostis, C. N. (2007), Notions of security and opacity in discrete event systems, *in* 'Proc. of the 46th IEEE Conference on Decision and Control', Louisiana, USA, pp. 5056–5061.

Saboori, A. & Hadjicostis, C. N. (2008), Verification of initial-state opacity in security applications of DES, *in* 'Proc. of the 9th International Workshop on Discrete Event Systems', Göteborg, Sweden, pp. 328–333.

Saboori, A. & Hadjicostis, C. N. (2011), 'Verification of k-step opacity and analysis of its complexity', *IEEE Transactions on Automation Science and Engineering* **8**(3), 549–559.

Seatzu, C., Silva, M. & van Schuppen, J. (2013), *Control of Discrete-Event Systems*, Vol. 433, Springer-Verlag London.

Tong, Y., Li, Z. & Giua, A. (2016), 'On the equivalence of observation structures for Petri net generators', *IEEE Transactions on Automatic Control* **61**(9), 2448–2462.

Tong, Y., Li, Z., Seatzu, C. & Giua, A. (2015*a*), Verification of current-state opacity using Petri nets, *in* 'Proc. of the 2015 American Control Conference', Chicago, USA, pp. 1935–1940.

Tong, Y., Li, Z., Seatzu, C. & Giua, A. (2015*b*), Verification of initial-state opacity in Petri nets, *in* 'Proc. of the 54th IEEE Conference on Decision and Control', Osaka, Japan, pp. 344–349.

Tong, Y., Li, Z., Seatzu, C. & Giua, A. (2016*a*), Supervisory enforcement of current-state opacity with uncomparable observations, *in* 'Proc. of the 13th International Workshop on Discrete Event Systems', Xi'an, China, pp. 313–318.

Tong, Y., Li, Z., Seatzu, C. & Giua, A. (2016*b*), Verification of language-based opacity in Petri nets using verifier, *in* 'Proc. of the 2016 American Control Conference', Boston, USA, pp. 757–763.

Tong, Y., Li, Z. W., Seatzu, C. & Giua, A. (2017), 'Verification of state-based opacity using Petri nets', *IEEE Transactions on Automatic Control* **62**(6). DOI: 10.1109/TAC.2016.2620429. On-line: `http://ieeexplore.ieee.org/document/7637003/`.

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

Wu, Y. & Lafortune, S. (2014), 'Synthesis of insertion functions for enforcement of opacity security properties', *Automatica* **50**(5), 1336–1348.