Automatica 80 (2017) 48–53

Contents lists available at ScienceDirect

Automatica

journal homepage: www.elsevier.com/locate/automatica

Brief paper

Decidability of opacity verification problems in labeled Petri net systems☆

Yin Tong [a,c], Zhiwu Li [b,a,1], 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

ARTICLE INFO

Article history:
Received 9 November 2015
Received in revised form
5 January 2017
Accepted 22 January 2017
Available online 28 March 2017

Keywords:
Discrete event systems
Petri nets
Opacity
Decidability problems

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.

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, Lesage, and Faure (2016) and Wu and 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, Koutny, & Ryan, 2005; Saboori & Hadjicostis, 2007; Tong, Li, Seatzu, & Giua, 2015a).
- 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. (2005). Saboori and Hadjicostis (2008) proposed a new ISO definition in the automaton framework that we extended to Petri nets in Tong, Li, Seatzu, and Giua (2015b). 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, 2016b).

☆ 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. The material in this paper was not presented at any conference. This paper was recommended for publication in revised form by Associate Editor Bart De Schutter under the direction of Editor Christos G. Cassandras.

E-mail addresses: yintong@stu.xidian.edu.cn (Y. Tong), zhwli@xidian.edu.cn (Z. Li), seatzu@diee.unica.it (C. Seatzu), alessandro.giua@lsis.org, giua@diee.unica.it (A. Giua).

[1] Corresponding author. Tel.: +86 29 88201986; fax: +86 29 88202456.

http://dx.doi.org/10.1016/j.automatica.2017.01.013
0005-1098/

In the framework of automata two types of observation masks have been investigated in the literature: static and dynamic (Cassez, Dubreil, & Marchand, 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; Tong et al., 2016b; Tong, Li, Seatzu, & Giua, 2017; Wu & Lafortune, 2013) consists in determining whether a system is opaque with respect to a given secret. When opacity is violated, different approaches (Cassez et al., 2012; Dubreil, Darondeau, & Marchand, 2010; Falcone & Marchand, 2015; Tong, Li, Seatzu, & Giua, 2016a; Wu & Lafortune, 2014) 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, Koutny, Mazaré, and Ryan (2008); Bryans et al. (2005), Cassez (2009), Jacob et al. (2016) and Saboori and Hadjicostis (2010). 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. (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 has 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 3–5, 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) and Seatzu, Silva, and van Schuppen (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 σ 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 ε. 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 σ 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[2] 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 exist $M_0' \in \mathcal{M}_0$, $\sigma' \in L(N, M_0')$ 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 σ leading to a marking in the secret set, there exists another transition sequence σ' 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.

We point out that an LPN system with a finite set of initial markings can always be converted into an equivalent LPN system[3] 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

[2] 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.

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