Available online at www.sciencedirect.com

ScienceDirect

IFAC Papers Online CONFERENCE PAPER ARCHIVE

IFAC PapersOnLine 56-2 (2023) 7899–7905

Verification of Joint Current-State Opacity Using Petri Nets ⋆

Wenjie Zhao * **Alessandro Giua** ** **Zhiwu Li** ***

* *Xidian University, Xi'an 710071, China (e-mail: zhaowenjie2021@gmail.com).*

** *University of Cagliari, 09123 Cagliari, Italy(e-mail:giua@diee.unica.it)*

*** *Macau University of Science and Technology, Taipa, Macau (e-mail: zhwli@xidian.edu.cn)*

Abstract: A *discrete event system* (DES) is said to be opaque if a predefined secret can never be exposed to an intruder who can observe its evolution. In this paper we consider a problem of *joint current-state opacity* for a system modeled by a Petri net and monitored by multiple local intruders, each of which can partially observe the behavior of the system. The intruders can synchronously communicate to a coordinator the state estimate they have computed, but not their observations. We demonstrate that the verification of this property can be efficiently addressed by using a compact representation of the reachability graph, called *basis reachability graph* (BRG), as it avoids the need for exhaustive enumeration of the reachability space. A *joint BRG-observer* is constructed to analyze joint current-state opacity under such a coordinated decentralized architecture.

Keywords: Discrete event system, joint current-state opacity, Petri net, basis reachability graph.

1. INTRODUCTION

Over the past few decades, various critical notions about system security and privacy have been proposed, such as anonymity (Schneider and Sidiropoulos, 1996), noninterference (Focardi and Gorrieri, 1994), non-deductibility (Hadj-Alouane et al., 2005), and opacity (Alur et al., 2006) to ensure that only authorized people in relevant fields have access to secret information. In this work, we are interested in the opacity property, which characterizes whether secret information in the system's behavior is hidden or not from unauthorized persons (called intruders). Since the secret can be a subset of the state space or the generated language of a *discrete event system* (DES), the opacity can be classified accordingly as *state-based opacity* or *language-based opacity*. Research based on opacity is well developed. A comprehensive review on the opacity in DESs is found in (Mazaré, 2004), (Bryans et al., 2005) and (Lafortune et al., 2018).

In this work, we study the verification of *joint current-state opacity* in DESs modeled by bounded Petri nets. We consider *current-state opacity* in a coordinated decentralized architecture, as proposed by Wu and Lafortune (2013). A system is observed by multiple local intruders that share their local state estimates through a single coordinator, called *joint current-state opacity*. Each local intruder, who is viewed as an external observer of a system, is assumed to have full knowledge of the system's structure but generally only a partial observation of the system's behavior. Given a secret described by a subset of the reachability set, the system is said to be jointly current-state opaque if intruders and the coordinator are never able to infer that the current state of the system is within the secret.

Since the development of network technology has led to the increasingly widespread deployment of distributed or decentralized systems, numerous researchers have proposed methods for joint diagnosis or state estimation in the field of DESs. Barrett and Lafortune (2000) propose a novel information structure model to deal with the decentralized control problem for DESs by developing several communicating supervisory controllers so as to achieve a given legal sublanguage of the uncontrolled system's language model, where each controller is with different information. Cabasino et al. (2013) show that, similar to the case with automata, diagnosability is strictly related to the existence of failure ambiguous strings, and propose a method to the diagnosis of Petri nets in a decentralized setting. Ran et al. (2018) report a novel approach to perform codiagnosability analysis of bounded LPNs with a set of sites that observe the system evolution.

Badouel et al. (2007) consider secrecy under multiple observers, however, each observer has an individual secret set. Paoli and Lin (2012) also consider the opacity of languages in two cases with and without coordination in a decentralized framework with several agents. Basile et al. (2015) have considered the decentralized constraints formulated with respect to net transitions, where each local supervisor detects and disables transitions of its own control site only. In contrast to the off-line construction

⋆ This work was partially supported by the Science and Technology Development Funding of Macau SAR, China, under Grant 0064/2021/A2 and the China Scholarship Council under Grant 202106960060.

10.1016/j.ifacol.2023.10.026

of an observer for the verification of opacity, based on *generalized mutual exclusion constraints* (GMECs), a compact and maximally permissive decentralized supervisor for Petri nets is designed in (Cong et al., 2018). To our knowledge, Wu and Lafortune (2013) is the first to extend the notion of current-state opacity to a new coordinated architecture with two intruders, and provide the concept of *joint current-state opacity*. However, the computation of the observer has a complexity of $\mathcal{O}(2^{3n})$ with n being the number of states of the plant.

Petri nets have a richer modeling power than finite automata. One standard analysis technique for bounded Petri nets relies on the construction of the *reachability graph* (RG), which requires an exhaustive enumeration of all reachable markings (i.e., states). This is quite inefficient and can be circumvented by constructing a so-called *basis reachability graph* (BRG). This approach entails enumerating only a subset of reachable markings, i.e., the basis markings, while linear equations represent the other markings that are reachable from these basis markings. In practical situations, as shown by Ma et al. (2017), the BRG can be order of magnitude smaller in size than the RG.

Motivated by this, we propose a approach to verify the joint current-state opacity in a system with multiple local intruders modeled by bounded *labeled Petri nets* (LPNs) under a coordinated decentralized architecture. The idea consists in constructing a *joint BRG-observer* by using basis markings rather than markings. We show that the proposed BRG-based approach is practically more efficient than the one based on reachability analysis as was the case in (Wu and Lafortune, 2013). However, our approach requires that the unobservable subnets of the intruders systems G_1, G_2 be acyclic.

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

1) We define a formal structure, called a joint BRG-observer, that allows one to verify joint current-state opacity in a system modeled by a bounded LPN.
2) Necessary and sufficient conditions for joint current-state opacity with respect to an arbitrary secret and two local intruders are provided based on the analysis of the joint BRG-observer.

2. PRELIMINARIES AND BACKGROUND

This section reviews the formalism used in the paper and some results on reachability analysis of Petri nets, which underpin the entire work of this paper.

2.1 Automata

A *nondeterministic finite automaton* (NFA) is a four-tuple $\mathcal{A} = (X, E, \Delta, x_0)$, where X is the finite set of *states*, $E = \{a, b, \cdots\}$ is the *alphabet* of finite events, $\Delta \subseteq X \times E_\varepsilon \times X$ is the *transition relation* with $E_\varepsilon = E \cup \{\varepsilon\}$ and ε being the empty word associated to unobservable events, $x_0 \in X$ is the *initial state*.

The *Kleene-closure* of E, denoted by E^*, defines the set of all finite sequences of symbols in E, including the empty sequence ε. 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 $\Delta^* \subseteq X \times E^* \times X$: $(x_{j0}, \omega, x_{jk}) \in \Delta^*$ if there exist 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 $\omega \in E^*, x_{ji} \in X$ 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 that $(x_i, e, x_j) \in \Delta$. Generally, write $\Delta(x, \sigma)!$ if $\Delta(x, \sigma)$ is defined.

The behavior of a system modeled by an automaton $\mathcal{A}$ can be characterized by the language that $\mathcal{A}$ generates. The *generated language* of $\mathcal{A} = (X, E, \Delta, x_0)$ is defined as $\mathcal{L}(\mathcal{A}) = \{\omega \in E^* \mid \exists x \in X : (x_0, \omega, x) \in \Delta^*\}$.

Let $\mathcal{A}_1 = (X_1, E_1, \Delta_1, x_{1,0})$ and $\mathcal{A}_2 = (X_2, E_2, \Delta_2, x_{2,0})$ be two NFAs. The synchronous (or parallel) composition is defined as

$$\mathcal{A} = \mathcal{A}_1 \| \mathcal{A}_2 = (X_1 \times X_2, E_1 \cup E_2, \Delta, x_{1,0} \times x_{2,0})$$

where the transition function Δ satisfies

$$\Delta((x_1, x_2), e) = \begin{cases} (\Delta_1(x_1, e), \Delta_2(x_2, e)) \text{ if } \Delta_1(x_1, e)! \& \Delta_2(x_2, e)! \\ (\Delta_1(x_1, e), x_2) \text{ if } \Delta_1(x_1, e)! \& e \notin E_2 \\ (x_1, \Delta_2(x_2, e)) \text{ if } \Delta_2(x_2, e)! \& e \notin E_1 \end{cases}$$

2.2 Petri Nets

A *Petri net* is a four-tuple $N = (P, T, Pre, Post)$, 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*, specifying the arcs from places to transitions, and vice versa. The incidence matrix of a net is represented by $C = Post - Pre$.

A *marking* is a mapping $M : P \to \mathbb{N}$ that assigns to a place a non-negative integer number of tokens, represented by black dots. The marking of place p at a marking M is denoted by $M(p)$, which indicates the number of tokens in place p at M. A marking is also denoted as $M = \sum_{p \in P} M(p) \cdot p$. A net N with an initial marking M_0 is called a *Petri net system*, denoted by $\langle N, M_0 \rangle$.

A transition t is *enabled* at marking M if $M \geq Pre(\cdot, t)$ and may fire yielding a marking M' with $M' = M + C(\cdot, t)$. 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 firing σ at M yields a marking M'. The set of all transition sequences firable from M_0 is denoted as $L(N, M_0)$, i.e., $L(N, M_0) = \{\sigma \in T^* \mid M_0[\sigma\rangle\}$. 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 firing sequence σ such that $M_0[\sigma\rangle M$. The *reachability set* of $\langle N, M_0 \rangle$ is the set of all markings reachable from M_0, 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 four-tuple $G = (N, M_0, E, \ell)$, where $\langle N, M_0\rangle$ is a Petri net system, E is the *alphabet* (a finite set of labels) and $\ell : T \to E \cup \{\varepsilon\}$ is the *labeling function* that assigns a transition $t \in T$ either a symbol from E or the empty word ε. This leads to a partition $T = T_o \dot{\cup} T_u$, where $T_o = \{t \in T \mid \ell(t) \in E\}$ is the set of observable transitions and $T_u = T \backslash T_o = \{t \in T \mid \ell(t) = \varepsilon\}$ is the set of unobservable transitions. In a recursive manner, the labeling function can be extended to $\ell : T^* \to E^*$, which is defined according to: $\ell(\varepsilon) = \varepsilon$; $\ell(t) = \varepsilon$ if $t \in T_u$; $\ell(t) = e$ if $t \in T_o$, $e \in E$; and $\ell(\sigma t) = \ell(\sigma)\ell(t)$ if $\sigma \in T^*$, $t \in T$.

Given an LPN $G = (N, M_0, E, \ell)$, we define its generated language as $\mathcal{L}(G) = \{\omega \in E^* \mid \exists \sigma \in T^* : M_0[\sigma\rangle, \ell(\sigma) = \omega\}$. A string $\omega \in \mathcal{L}(G)$ is called an *observation*. The *set of markings consistent with* ω is denoted as $\mathcal{C}(\omega) = \{M \in \mathbb{N}^m \mid \exists \sigma \in T^*\colon M_0[\sigma\rangle M, \ell(\sigma) = \omega\}$. Since observation ω is generated by the system, set $\mathcal{C}(\omega)$ must be non-empty.

Given two alphabets E' and E with $E' \subseteq E$, the *natural projection* on E', $Pr : E^* \to (E')^*$ is defined according to: $Pr(\varepsilon) = \varepsilon$; $Pr(e) = \varepsilon$ if $e \notin E'$; $Pr(e) = e$ if $e \in E'$; and $Pr(\sigma e) = Pr(\sigma)Pr(e)$ for $\sigma \in E^*$, $e \in E$.

The *inverse projection* of Pr denoted by $Pr^{-1} : (E')^* \to 2^{E^*}$ is defined as $Pr^{-1}(\{s\}) = \{\sigma \in E^* \mid Pr(\sigma) = s\}$, where $s \in (E')^*$.

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 $T \backslash T_u$ from N, where Pre' and $Post'$ are the restrictions of Pre and $Post$ to T_u, respectively. The incidence matrix of the unobservable subnet is defined by $C_u = Post' - Pre'$.

2.3 Some Results on Reachability in Petri Nets

In this subsection, let us recall some key notions of *basis markings* and the construction of *basis reachability graph* (BRG) proposed by (Cabasino et al., 2011) and (Ma et al., 2017).

Given an LPN $G = (N, M_0, E, \ell)$, we denote its BRG as an NFA $\mathcal{B} = (\mathcal{M}_B, E, \Delta, M_0)$, where the set of states $\mathcal{M}_B$ is the set of *basis markings* of the LPN, the alphabet E is the set of labels of observable transitions. $\Delta \subseteq \mathcal{M}_B \times E \times \mathcal{M}_B$ is the transition relation between basis markings, and M_0 is the initial state.

A marking M is reachable in an LPN from the inital marking M_0 with a sequence σ that produces observation ω if and only if the sequence ω in the BRG yields basis marking M_b and M belongs to the unobservable reach of M_b. The unobservable reach of a marking M, denoted by $\mathcal{U}(M)$, is the set of markings reachable from M by firing only unobservable transitions. We use $\mathcal{M}_b(\omega) = \mathcal{C}(\omega) \cap \mathcal{M}_B$ to denote the set of basis markings consistent with ω.

For the convenience of reading, other related definitions can be found in the appendix.

For all observations ω, $\mathcal{M}_b(\omega)$ can be computed by converting an obtained BRG into its equivalent DFA by a standard *determinization procedure* in (Cassandras and Lafortune, 2008). To verify current-state opacity, Tong et al. (2017) have defined the BRG for current-state opacity as $\mathcal{B}_c = (\tilde{\mathcal{M}}_B, E, \Delta, (M_0, \alpha(M_0)))$, where $\tilde{\mathcal{M}}_B \subseteq \mathcal{M}_B \times \{0, 1\}$, and defined the *current-state basis observer* of the BRG $\mathcal{B}_c$ as $Obs(\mathcal{B}_c) = (X_c, E_c, \Delta_c, x_{c,0})$, where each state is a subset of $\tilde{\mathcal{M}}_B$ consistent with an observation, the set of events E_c is a set of all observable events, Δ_c is the transition relation between states in X_c, and $x_{c,0}$ is the initial state.

3. JOINT CURRENT-STATE OPACITY AND PROBLEM FORMULATION

In this section, we review the relevant definitions of current-state opacity and elaborate upon the setting of the problem studied in this work.

Definition 1. An LPN $G = (N, M_0, E, \ell)$ is said to be *current-state opaque* wrt a secret $S \subseteq R(N, M_0)$ if for all observations $\omega \in \mathcal{L}(G)$, $\mathcal{C}(\omega) \nsubseteq S$ holds.

If an LPN is current-state opaque, it implies that an intruder cannot determine whether the current state belongs to the secret based on all possible observations.

In this paper, we will consider joint current-state opacity properties in the framework of coordinated decentralized architecture where multiple intruders work as a team to infer the secret. Specifically, we consider a simplified coordinated architecture with two local intruders communicating with a single coordinator, as shown in Fig. 1. The system is modeled as a bounded LPN $G = (N, M_0, E, \ell)$ and it is assumed to be monitored by two local intruders. The local system observed by each local intruder is defined as $G_i = (N, M_0, E_i, \ell_i), i = 1, 2$, where $\langle N, M_0\rangle$ is a net system, the alphabet of events E_i is a subset of E, associated with two labeling functions $\ell_i(t) = \ell(t)$ if $\ell(t) \in E_i$ else $\ell_i(t) = \varepsilon$. Each local intruder observes the system behavior via their individual labeling function and communicates with the coordinator by sending the results of local state estimates. Finally, the coordinator computes the intersection of the local state estimates it receives: this is called the *coordinated estimate*. We assume that (1) each local intruder knows the structure and the initial marking of the system, but they can only observe the firing of transitions whose label belongs to their own alphabet, (2) the local intruders only communicate with the coordinator and have no knowledge of one another, and there is no delay in communication, and (3) the coordinator does not know the structure of the system.

A system is said to be *jointly opaque* if no coordinated estimate ever reveals the secret information. The notion of joint current-state opacity has originally been defined in automata (Wu and Lafortune, 2013). In this work a set of states is defined as the *secret*, an automaton is jointly current-state opaque under the coordinated architecture if for each string, neither of the two local intruders can ensure whether it ends at a secret state based on their observations. This notion can be naturally rewritten for Petri nets as follows.

Definition 2. An LPN $G = (N, M_0, E, \ell)$ is said to be *jointly current-state opaque* wrt a secret $S \subseteq R(N, M_0)$ and two local intruders if for all transition sequences $\sigma \in L(N, M_0)$, there exists other two sequences $\sigma_1, \sigma_2 \in L(N, M_0)$ such that $\ell_1(\sigma) = \ell_1(\sigma_1) = \omega_1$ with $\omega_1 \in$

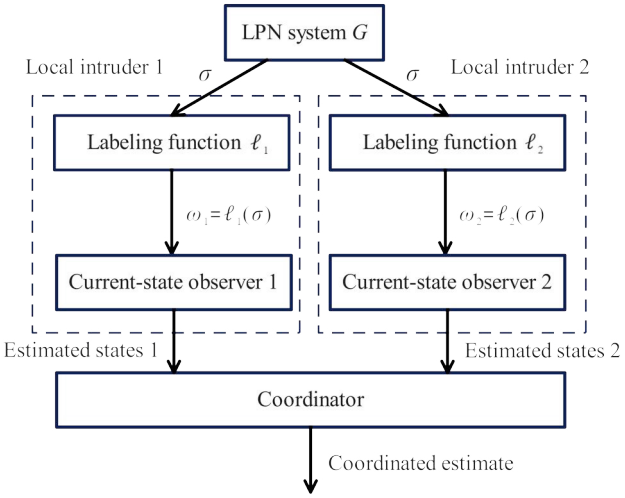

Fig. 1. The coordinated decentralized architecture.

$\mathcal{L}_1(N, M_0)$, $\ell_2(\sigma) = \ell_2(\sigma_2) = \omega_2$ with $\omega_2 \in \mathcal{L}_2(N, M_0)$ and $\mathcal{C}_1(\omega_1) \cap \mathcal{C}_2(\omega_2) \nsubseteq S$ holds [1].

An LPN system that is jointly current-state opaque means that for each transition sequence σ, there exist two other transition sequences σ_1 and σ_2 that leads to some common markings which are not contained in the secret, and two transition sequences are observationally equivalent with σ to intruders 1 and 2, respectively. Note that, if a system is jointly current-state opaque, it must be current-state opaque for each intruder. However, the reverse is not true in general.

Before formalizing the issues involved in the rest of the work, we begin by introducing the following assumptions:

A1) The LPN G is bounded.
A2) The unobservable subnets of G_1 and G_2 are acyclic.

These assumptions will allow the problem under investigation to have some properties on the basis of which we can verify joint current-state opacity of a system. Assumption A1 guarantees that the number of basis markings is finite; thus the algorithm for calculating BRG can halt. Assumption A2 allows us to iteratively compute the basis markings by using the state equation to describe the set of markings reached from the basis markings by firing unobservable transitions. Therefore, the firing of unobservable transitions in a system can be abstracted by using the minimal explanations and the basis markings. This avoids the problem of state explosion and makes it easier to find valid information related to secret states in subsystems.

Problem Statement: Consider a bounded LPN $G = (N, M_0, E, \ell)$ with a secret $S \subseteq R(N, M_0)$ monitored by two local intruders satisfying Assumptions A1 and A2. The local system observed by each local intruder is $G_i = (N, M_0, E_i, \ell_i), i = 1, 2$. Determine the joint current-state opacity property of G.

Example. Consider the LPN system $G = (N, M_0, E, \ell)$ in Fig. 2 monitored by two local intruders. The local system observed by each local intruder i is $G_i = (N, M_0, E_i, \ell_i), i = 1, 2$, where $E_1 = \{a\}$ and $E_2 = \{b\}$. The reachability graph of G under the coordinated architecture, is shown in Fig. 3.

[1] Herein, the subscripts are added to distinguish between languages observed by different local intruders due to different labeling functions.

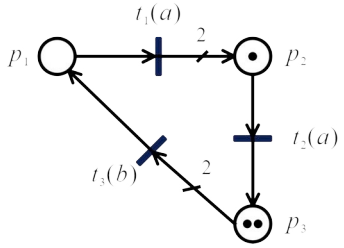

Fig. 2. An LPN G whose unobservable subnet is acyclic.

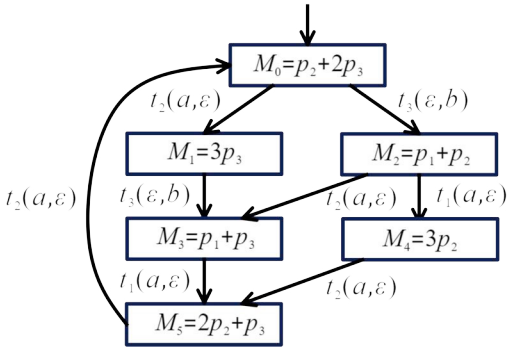

Fig. 3. The reachability graph of G under the coordinated architecture in example.

4. VERIFICATION OF JOINT CURRENT-STATE OPACITY

4.1 Joint BRG-Observer

In this section, we define a formal structure, called a *joint BRG-observer*, that allows one to verify joint current-state opacity in a system modeled by bounded LPN under a coordinated decentralized architecture more efficiently. For the sake of simplicity, we assume that there are two local intruders. The steps are as follows.

Step 1. Define a fictitious global intruder. In our setting there is no global intruder since the coordination among local intruders is restricted. However, for reasons that will be clear in the following, to verify opacity we need to consider a fictitious intruder that can observe all events that are observed by each local intruder, which is called a *global intruder*. We assume that the LPN system known to the global intruder is $G_g = (N, M_0, E_g, \ell_g)$, where $\langle N, M_0 \rangle$ is a net system, the alphabet is $E_g = E_1 \cup E_2$, the labeling function $\ell_g : T \to E_g$ is such that $\ell_g(t) = \ell_1(t)$ if $\ell_1(t) \in E_1$ else $\ell_g(t) = \ell_2(t)$. To facilitate the understanding of the work in this step, we develop two equivalent ways of describing local observations in a decentralized setting in Fig. 4.

Step 2. Construct a BRG for each intruder. *Basis reachability graphs* (BRGs) are compact representation of *reachability graphs* (RGs), which is detailed in the appendix. For a large-size Petri net, constructing its RG will inevitably suffer from the state explosion. Tong et al.

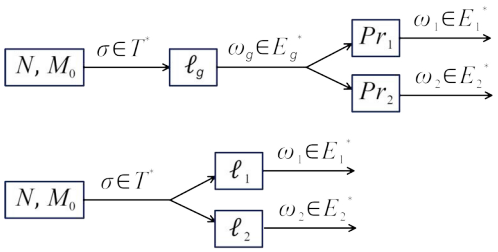

Fig. 4. Two equivalent ways of describing local observations in a decentralized setting.

(2017) shows that current-state opacity can be verified by constructing the BRG (with appropriate modifications) that enables one to avoid RG analysis. The proposed approach exhibits heightened efficiency, as the size of the BRG never surpasses that of the RG, and it becomes even more compact in the presence of unobservable transitions. Note that, since that it is possible to have more than one transition with the same label in system, the BRG is possibly nondeterministic. After this step, we obtain $\mathcal{B}_1, \mathcal{B}_2$ and $\mathcal{B}_g$, which represent, respectively, the BRG for G_1, G_2 and G_g.

Step 3. Construct the observer for each BRG. In this work, we use the *current-state basis observer* to model the knowledge gained by the local intruder i and the global intruder. The current-state basis observer of local intruder i is represented by $Obs(\mathcal{B}_i) := (Y_i, E_i, \Delta_i, y_{i,0}), i = 1, 2$. A state in the set of states Y_i is a set of basis markings of the system G_i. The set of events E_i is a set of all observable events to local intruder i. Δ_i is the transition relation between the states in Y_i. The initial state $y_{i,0}$ is the initial basis markings $\{M_0\}$.

The current-state basis observer of the fictitious global intruder is defined as $Obs(\mathcal{B}_g) := (Y_g, E_g, \Delta_g, y_{g,0})$. The interest of this observer is of generating all words in $Pr_g(\mathcal{L}(G))$.

Step 4. Construct the joint BRG-observer. We define a *joint BRG-observer* as the concurrent composition $Obs(B_1)||Obs(B_2)||Obs(B_g)$. This automaton, denoted as $J = (Y, E, \Delta, y_0)$, has set of states $Y \subseteq Y_1 \times Y_2 \times Y_g$, where each state is denoted by a triple $y = (y_1, y_2, y_g)$. E is the alphabet of events. The initial state is $y_0 = (\{M_0\}, \{M_0\}, \{M_0\})$. The transition relation Δ is defined as follows:

$$\Delta((y_1, y_2, y_g), e) =$$

$$\begin{cases} (\Delta_1(y_1, e), \Delta_2(y_2, e), \Delta_g(y_g, e)) \text{ if } \Delta_1(y_1, e)!\&\Delta_2(y_2, e)! \\ (\Delta_1(y_1, e), y_2, \Delta_g(y_g, e)) \text{ if } \Delta_1(y_1, e)!\&e \notin E_2 \\ (y_1, \Delta_2(y_2, e), \Delta_g(y_g, e)) \text{ if } \Delta_2(y_2, e)!\&e \notin E_1 \end{cases}$$

where $e \in E$, Δ_i is the transition relation of $Obs(\mathcal{B}_i), i = 1, 2$, and Δ_g is the transition relation of $Obs(\mathcal{B}_g)$. By concurrent composition with $Obs(\mathcal{B}_g)$, the behavior of J is restricted within system's observable behavior:

$$\begin{aligned} \mathcal{L}(J) :&= Pr_1^{-1}(\mathcal{L}(Obs(\mathcal{B}_1))) \cap Pr_2^{-1}(\mathcal{L}(Obs(\mathcal{B}_2))) \cap \\ &\quad \mathcal{L}(Obs(\mathcal{B}_g)) \\ &= \mathcal{L}(Obs(\mathcal{B}_g)) = Pr_g(\mathcal{L}(G)) \end{aligned}$$

where the inverse projection is defined as $Pr_i^{-1} : E_i^* \to 2^{E^*}$, for $i = 1, 2$. Consider a word $\omega \in \mathcal{L}(J)$. It means that there exists a state $y = (y_1, y_2, y_g)$ in Y such that $(y_0, \omega, y) \in \Delta^*$, where $y_1 = \mathcal{C}_1(\omega_1)$ and $y_2 = \mathcal{C}_2(\omega_2)$. Note that the state estimates depend only on (y_1, y_2). However, to ensure that in the language of the joint BRG-observer there are no spurious words, i.e., words on E_g that do not correspond to observations produced by the system, we also need to compose the local intruders' observers with $Obs(\mathcal{B}_g)$.

Step 5. Coordinated estimate. Given a joint BRG-observer J, we need to associate with each state $y \in Y$ the *coordinated estimate* of J. To this end, we define the *coordinate estimate function* $f_{ce} : Y \to 2^{|R(N,M_0)|}$ as

$$\begin{aligned} f_{ce}(y) :&= f_{ce}(y_1, y_2, y_g) \\ &= \mathcal{U}_1(y_1) \cap \mathcal{U}_2(y_2) \subseteq R(N, M_0) \end{aligned}$$

where $y \in Y$ satisfying $(y_0, \omega, y) \in \Delta^*$ and $\omega \in \mathcal{L}(J)$. Such a function computes the intersection of two sets where, for $i = 1, 2$, set $\mathcal{U}_i(y_i)$ represents the union for all basis markings $M_b \in y_i$ and the markings reachable from M_b by firing only unobservable transitions in net G_i. Note that, the same basis marking may have different unobservable reaches in different net systems, as shown in Table 1.

Table 1. Unobservable reaches of basis markings in G_1 and G_2

LPN system	Basis Marking	$\mathcal{U}(M)$
G_1	M_0	$\{M_0, M_2\}$
	M_1	$\{M_1, M_3\}$
	M_4	$\{M_4\}$
	M_5	$\{M_5\}$
G_2	M_0	$\{M_0, M_1\}$
	M_2	$\{M_0, M_1, M_2, M_3, M_4, M_5\}$

Let us consider the number of states of the joint BRG-observer in the maximum case as $2^{|\mathcal{M}_{B,1}|+|\mathcal{M}_{B,2}|+|\mathcal{M}_{B,g}|} - 3$. Consequently, the space complexity of the proposed method is $\mathcal{O}(2^{|\mathcal{M}_{B,1}|+|\mathcal{M}_{B,2}|+|\mathcal{M}_{B,g}|})$ with $|\mathcal{M}_B|$ being the number of basis markings of G_1, G_2 and G_g, respectively. However, considering that RG-based methods has a space complexity of $\mathcal{O}(2^{|R(N,M_0)_1|+|R(N,M_0)_2|+|R(N,M_0)_g|})$ with $|R(N, M_0)|$ being the total number of reachable markings of G_1, G_2 and G_g, respectively, and $|\mathcal{M}_B|$ is typically smaller than $|R(N, M_0)|$, we can briefly conclude that BRG-based methods are more efficient compared with the automata based approach by Wu and Lafortune (2013).

Example. Consider the LPN system $G = (N, M_0, E, \ell)$ in Fig. 2 that is monitored by two local intruders with $E_1 = \{a\}$ and $E_2 = \{b\}$. By *Step 2*, we construct the BRG for each intruder in Fig. 5. By *Step 3*, we construct the current-state basis observer to model the knowledge gained by local intruder i and single system intruder which is not real, as shown in Figs. 6 and 7. By *Steps 4* and *5*, we construct the joint BRG-observer J and associate it with the function f_{ce}, as shown in Fig. 8.

4.2 Verifying Joint Current-state Opacity

The following proposition shows that the *coordinated current-state estimate* wrt an observation $\omega \in \mathcal{L}(G)$ such

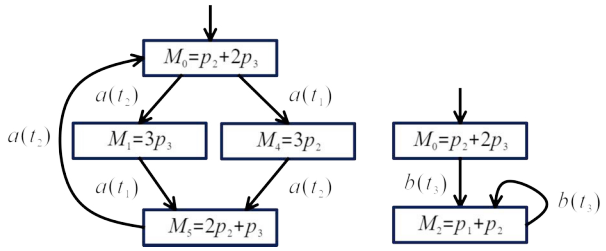

Fig. 5. The BRG of local systems $G_i, i = 1, 2$.

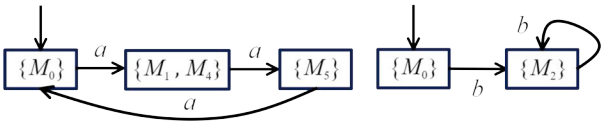

Fig. 6. Current-state basis observer of $\mathcal{B}_i, i = 1, 2$.

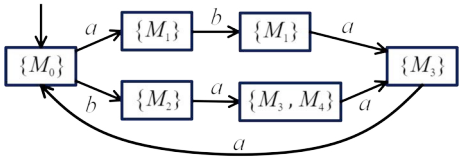

Fig. 7. Current-state basis observer of $\mathcal{B}_g$.

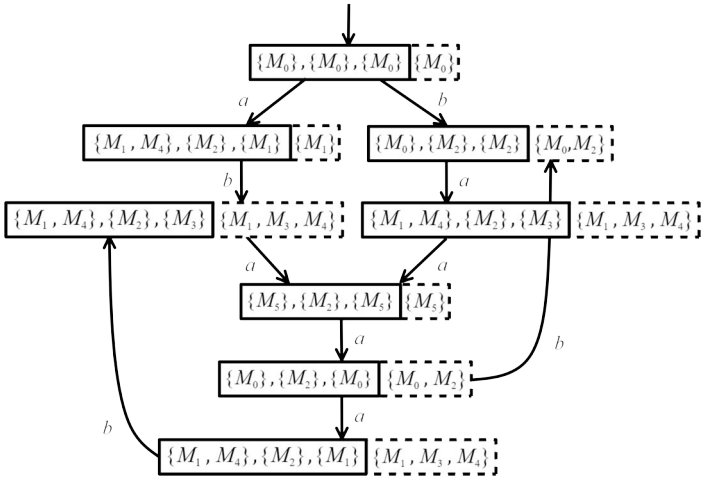

Fig. 8. The joint BRG-observer J in example.

that $\omega = \ell(\sigma)$ and $\sigma \in L(N, M_0)$, denoted as $\hat{X}_{0,coor}(\omega)$, is the *coordinated estimate* associated to a state $y \in Y$ such that $(y_0, \omega, y) \in \Delta^*$ by using f_{ce}. We will show later how to use J with the *coordinate estimate function* f_{ce} to verify the joint current-state opacity property.

Proposition 3. Let $G = (N, M_0, E, \ell)$ be an LPN whose unobservable subnet is acyclic, while is monitored by two local intruders. For all observation $\omega \in \mathcal{L}(G)$ such that $\omega = \ell(\sigma)$ and $\sigma \in L(N, M_0)$, the coordinated current-state estimate $\hat{X}_{0,coor}(\omega)$ is equivalent to the coordinate estimate $f_{ce}(y)$ associated to a state $y \in Y$ such that $(y_0, \omega, y) \in \Delta^*$.

Proof. Consider an observation $\omega \in \mathcal{L}(G)$ such that $\omega = \ell(\sigma)$ and $\sigma \in L(N, M_0)$, $Pr_i(\omega) = \omega_i$, for $i = 1, 2$, and the current-state estimate on an observation ω_i for each local intruder i, denoted as $\hat{X}_{0,i}(\omega_i) = \mathcal{U}_i(\Delta_i(y_{i,0}, \omega_i))$. Thus, the coordinated current-state estimate is $\hat{X}_{0,coor}(\omega) = \hat{X}_{0,1}(\omega_1) \cap \hat{X}_{0,2}(\omega_2) = \mathcal{U}_1(\Delta_1(y_{1,0}, \omega_1)) \cap \mathcal{U}_2(\Delta_2(y_{2,0}, \omega_2)$. On the other hand, the coordinated estimate associate with a state $y \in Y$ reaches by ω in J is

$$\begin{aligned} f_{ce}(y) :&= f_{ce}(y_1, y_2, y_g) \\ &= \mathcal{U}_1(y_1) \cap \mathcal{U}_2(y_2) \\ &= \mathcal{U}_1(\Delta_1(y_{1,0}, \omega_1)) \cap \mathcal{U}_2(\Delta_2(y_{2,0}, \omega_2)) \end{aligned}$$

where the set $\mathcal{U}_i(\Delta_i(y_{i,0}, \omega_i))$ also represents the union for all basis markings $M_b \in y$ with $(y_{i,0}, \omega_i, y) \in \Delta_i^*$ and the markings reachable from M_b by firing only unobservable transitions in local net G_i. Therefore, for an observation $\omega \in \mathcal{L}(G)$, $\hat{X}_{0,coor}(\omega) = f_{ce}(y)$, where $(y_0, \omega, y) \in \Delta^*$ holds.

Based on Proposition 3, we drive the following necessary and sufficient condition for joint current-state opacity.

Theorem 4. Let $G = (N, M_0, E, \ell)$ be an LPN with a secret $S \subseteq R(N, M_0)$, monitored by two local intruders. G is *jointly current-state opaque* wrt a secret $S \subseteq R(N, M_0)$ and two local intruders if and only if for all $y \in Y$ in J, $f_{ce}(y) \nsubseteq S$ holds.

Proof. G is jointly current-state opaque wrt a secret $S \subseteq L(N, M_0)$ and two local intruders if and only if $\hat{X}_{0,coor}(\cdot)$ always contains a non-secret state whenever it contains a secret state. By Proposition 3, $\hat{X}_{0,coor}(\cdot) = \mathcal{U}_1(y_1) \cap \mathcal{U}_2(y_2) = f_{ce}(y)$, where is the intersection of two sets where, for $i = 1, 2$, set $\mathcal{U}_i(y_i)$ represents the union for all basis markings $M_b \in y_i$ and the markings reachable from M_b by firing only unobservable transitions in net G_i. Since J is deterministic and $\mathcal{L}(J) = Pr_g(\mathcal{L}(G))$, every coordinated estimate that is associated with a state reachable in J, corresponds to a valid $\hat{X}_{0,coor}(\cdot)$, and vice-versa. Therefore, the joint current-state opacity property can be verified by examining the coordinated estimate that is associated with each reachable state in J.

Example. Let us go back to the previous Example and take the secret to be $S = \{M_1\}$. The system G is current-state opaque to each local intruder because no state in $Obs(B_1)$ or $Obs(B_2)$ contains only the secret marking without any unobservable reach in the state. However, the system G is not jointly current-state opaque. Due to the collaboration under the coordinated architecture, the team of intruders obtain a coordinated estimate $\{M_1\}$ when $\ell(\sigma) = a$ has occurred, as shown in Fig. 8.

5. CONCLUSION AND FUTURE WORK

This paper, proposes a novel approach to address the verification of joint current-state opacity in the coordinated architecture of discrete event systems by constructing a joint BRG-observer wrt a function to compute the coordinated estimate. In future work, we will focus on simplifying the computation steps and study the verification of other state-based opacity properties in this framework. The approach we have proposed could be combined with integer linear programming tools to avoid exhaustively enumerating the unobservable reach of basis markings.

REFERENCES

Alur, R., Černỳ, P., and Zdancewic, S. (2006). Preserving secrecy under refinement. In *International Colloquium on Automata, Languages, and Programming*, 107–118. Springer.

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

Barrett, G. and Lafortune, S. (2000). Decentralized supervisory control with communicating controllers. *IEEE Transactions on Automatic Control*, 45(9), 1620–1638.

Basile, F., Cordone, R., and Piroddi, L. (2015). A branch and bound approach for the design of decentralized supervisors in Petri net models. *Automatica*, 52, 322–333.

Bryans, J.W., Koutny, M., Mazaré, L., and Ryan, P.Y. (2005). Opacity generalised to transition systems. In *International Workshop on Formal Aspects in Security and Trust*, 81–95. Springer.

Cabasino, M.P., Giua, A., Paoli, A., and Seatzu, C. (2013). Decentralized diagnosis of discrete-event systems using labeled Petri nets. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 43(6), 1477–1485.

Cabasino, M.P., Giua, A., Pocci, M., and Seatzu, C. (2011). Discrete event diagnosis using labeled Petri nets. an application to manufacturing systems. *Control Engineering Practice*, 19(9), 989–1001.

Cassandras, C.G. and Lafortune, S. (2008). *Introduction to discrete event systems*. Springer.

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

Focardi, R. and Gorrieri, R. (1994). A taxonomy of trace-based security properties for ccs. In *Proceedings The Computer Security Foundations Workshop VII*, 126–136. IEEE.

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

Lafortune, S., Lin, F., and Hadjicostis, C.N. (2018). On the history of diagnosability and opacity in discrete event systems. *Annual Reviews in Control*, 45, 257–266.

Ma, Z., Tong, Y., Li, Z., and Giua, A. (2017). Basis marking representation of Petri net reachability spaces and its application to the reachability problem. *IEEE Transactions on Automatic Control*, 62(3), 1078–1093.

Mazaré, L. (2004). Using unification for opacity properties. *Proceedings of the 4th IFIP WG1*, 7, 165–176.

Paoli, A. and Lin, F. (2012). Decentralized opacity of discrete event systems. In *2012 American Control Conference (ACC)*, 6083–6088. IEEE.

Ran, N., Su, H., Giua, A., and Seatzu, C. (2018). Co-diagnosability analysis of bounded Petri nets. *IEEE Transactions on Automatic Control*, 63(4), 1192–1199.

Schneider, S. and Sidiropoulos, A. (1996). Csp and anonymity. In *European Symposium on Research in Computer Security*, 198–218. Springer.

Tong, Y., Li, Z., Seatzu, C., and Giua, A. (2017). Verification of state-based opacity using Petri nets. *IEEE Transactions on Automatic Control*, 62(6), 2823–2837.

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

Appendix A. SOME NOTION OF BASIS REACHABILITY GRAPH (BRG)

Definition 5. Given a marking M and an observable transition $t \in T_o$, we define

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

as the set of *explanations* of t at M, and we define

$$Y(M,t) = \left\{\mathbf{y}_u \in \mathbb{N}^{|T_u|} \mid \exists \sigma \in \Sigma(M,t) : \mathbf{y}_u = \pi(\sigma)\right\}$$

as the set of *explanations vectors*; meanwhile, we define

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

as the set of *minimal explanations* of t at M, and

$$Y_{min}(M,t) = \left\{y_u \in \mathbb{N}^{|T_u|} \mid \exists \sigma \in \Sigma_{min}(M,t) : \mathbf{y}_u = \pi(\sigma)\right\}$$

as the corresponding set of *minimal explanations vectors*.

Definition 6. 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 $M' = M + C(\cdot,t) + \mathcal{C}_u \cdot \mathbf{y}_u$.

Definition 7. Given an LPN $G = (N, M_0, E, \ell)$, its BRG is a deterministic finite state automaton $\mathcal{B}$. The BRG $\mathcal{B}$ is a quadruple $(\mathcal{M}_B, E, \Delta, M_0)$, where

- the state set $\mathcal{M}_B$ is the set of basis markings;
- all events in the event set E are observable;
- $\Delta \subseteq \mathcal{M}_B \times E \times \mathcal{M}_B$ is the transition relation between basis markings;
- the initial state is the initial marking M_0.

Algorithm 1 Construction of the BRG

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

```
M_B := {M_0} and assign no tag to M_0;
while states with no tag exists do
    for all t ∈ T_o and Y_min(M,t) ≠ ∅ do
        for all y_u ∈ Y_min(M,t) do
            M' := M + C_u · y_u + C(·,t);
            if M' ∉ M_B then
                M_B := M_B ∪ {M'};
                assign no tag to M';
            end if
            Δ := Δ ∪ {(M, ℓ(t), M')};
        end for
    end for
    tag node M "old";
end while
Remove all tags.
```

Definition 8. 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 $\mathcal{U}(M) = \{M' \in \mathbb{N}^m \mid \exists \sigma_u \in T_u^* : M\,[\sigma_u\rangle\, M'\}$.