mathematics

IMPACT FACTOR 2.4

CITESCORE 3.5

Article

Verification of Current-State Opacity in Discrete Event Systems by Using Basis Coverability Graphs

Haoming Zhu, Ahmed M. El-Sherbeeny, Mohammed A. El-Meligy, Amir M. Fathollahi-Fard and Zhiwu Li

MDPI

https://doi.org/10.3390/math11081798

mathematics

MDPI

Article

Verification of Current-State Opacity in Discrete Event Systems by Using Basis Coverability Graphs

Haoming Zhu [1], Ahmed M. El-Sherbeeny [2], Mohammed A. El-Meligy [2], Amir M. Fathollahi-Fard [3] and Zhiwu Li [1,*]

[1] Institute of Systems Engineering, Macau University of Science and Technology, Taipa, Macao SAR, China
[2] Industrial Engineering Department, College of Engineering, King Saud University, P.O. Box 800, Riyadh 11421, Saudi Arabia
[3] Peter B. Gustavson School of Business, University of Victoria, P.O. Box 1700, Victoria, BC V8P 5C2, Canada
* Correspondence: zwli@must.edu.mo

Abstract: A new approach to the verification of current-state opacity for discrete event systems is proposed in this paper, which is modeled with unbounded Petri nets. The concept of opacity verification is first extended from bounded Petri nets to unbounded Petri nets. In this model, all transitions and partial places are assumed to be unobservable, i.e., only the number of tokens in the observable places can be measured. In this work, a novel basis coverability graph is constructed by using partial markings and quasi-observable transitions. By this graph, this research finds that an unbounded net system is current-state opaque if, for an arbitrary partial marking, there always exists at least one regular marking in the result of current-state estimation with respect to the partial marking not belonging to the given secret. Finally, a sufficient and necessary condition is proposed for the verification of current-state opacity. A manufacturing system example is presented to illustrate that the concept of current-state opacity can be verified for unbounded net systems.

Keywords: basis coverability graph; discrete event system; Petri net; current-state opacity

MSC: 93-08

Citation: Zhu, H.; El-Sherbeeny, A.M.; El-Meligy, M.A.; Fathollahi-Fard, A.M.; Li, Z. Verification of Current-State Opacity in Discrete Event Systems by Using Basis Coverability Graphs. *Mathematics* **2023**, *11*, 1798. https://doi.org/10.3390/math11081798

Academic Editor: António Lopes

Received: 19 January 2023
Revised: 21 March 2023
Accepted: 23 March 2023
Published: 10 April 2023

1. Introduction

In recent decades, with the rapid development of information technology and computer science, the security of cyber–physical systems has become a hot research direction in interdisciplinary areas, which include many human-built infrastructures. Discrete event systems (DESs) serve as the technical generalization of such human-made systems that are usually computer-integrated and evolve with the predefined regulations. Typically, almost all the production systems fall into this category. In discrete event systems, similar to controllability, observability, diagnosability, and detectability, opacity is one of the basic attributes of DESs [1], which reflects the confidentiality of a system. To be specific, when unauthorized external observers (or intruders) observe the evolution of the system, they cannot infer that the predicate representing secret information is true.

In the context of DESs, a secret predicate can be either a subset of the state space or a subset of the language generated by a system [2,3]. Opacity can be accordingly divided into two categories: state-based opacity and language-based opacity. Furthermore, state-based opacity can be categorized into current-state opacity (CSO) [4,5], initial-state opacity [6,7], *k*-step, and infinite-step opacity [8–11]. Opacity verification can be conducted in a centralized or decentralized framework [12], under different formalisms such as fuzzy or stochastic DESs [13,14].

In this work, the concept of current-state opacity is verified by using an unbounded system, i.e., the number of times a transition is triggered is no longer set with an upper limit. A basis coverability graph (BCG) is constructed to address the CSO verification of a

DES modelled with unbounded Petri nets (UPNs); such a system cannot be modelled with a finite state automaton. A condition in [6] is extended, i.e., some unobservable transitions can be detected in a partially observed DES. Moreover, an external observer (or intruder) is assumed to know the overall structure and initial state of the unbounded net model, but only part of places can be observable, i.e., the number of tokens in such a place can be explicitly measured or counted. Under such a setting, it becomes much more challenging to estimate the current state of an unbounded system. This paper constructs a BCG for an unbounded Petri net to determine the possible current state of the system according to the derived quasi-observable transitions and partial observable places.

Compared with finite-state automata (FSA), Petri nets are a more popular tool for modelling and controlling DESs [15]. By changing the number of tokens in places, the system behaviors are observed for further investigations [16] of interesting system properties or behavior. Petri nets have been extensively used to study the diagnosability analysis [17,18], state estimation [19], and supervisory control of DESs. In [17], a programming problem is formulated to perform fault diagnosis in a bounded Petri net, while the work in [18] reports a verifier net to derive a fault diagnosis method for DESs.

However, the existing results in the framework of bounded Petri nets usually need to construct reachability graphs [17–19], which suffer from the notorious state explosion problem. In other words, it is difficult to enumerate all the states for real-world systems due to their large sizes [20]. To mitigate this issue, a new type of reachability graph is proposed by Cabasino et al. [21], called a basis reachability graph (BRG). The authors, as well as the followers in the DES domain, apply BRG to many DES problems such as fault diagnosis, diagnosability analysis, supervisory control, and critical observability, opacity verification and enforcement.

In the research on DESs based on Petri nets, there are few studies on unbounded net systems. Ushio et al. [22] reported a method of fault diagnosis by using a partially observed UPN, where all transitions are unobservable and partial places are observable. In [22], two diagnosers, a simple diagnoser and an ω-diagnoser, were constructed to analyze the diagnosability of an underlying system by monitoring the token counts and their changes in observable places. Moreover, the work in [23] improved the results in [18] by extending the diagnosability analysis in bounded net systems to unbounded net systems using a verifier net. In addition, when analyzing the state space of an unbounded net system, its coverability graph [24–26] has to be considered. In [27], Lefaucheux et al. extended the concept of BRGs to unbounded net systems. The authors analyzed the relationship between coverability sets and reachability sets. After the definition of BCGs was proposed, the relationship between BCGs and BRGs was further analyzed. Based on the proposed BCGs, the diagnosability analysis for unbounded net systems was significantly improved by the team who originally developed the notion of BRG with a deluge of results. For example, it was shown that an unbounded net system is diagnosable iff there does not exist any cycle in the BCG with the relevant set of fault transitions. However, the investigation of further applications of the BCGs is still open.

Opacity verification and enforcement have been extensively studied and applied to real applications [5–7,28,29], i.e., no matter what information is observed by a malicious intruder from outside, some non-secret information and secret information cannot be identified. In this case, the intruder cannot decide whether the possible current system states reasoned from the current observation so far belong to the pre-defined secret of the system.

In [30], the concept of opacity in finite transition systems was proposed for the first time, which was then extended to Petri nets [31]. For the verification of CSO, Tong et al. [4] used a BRG to verify the CSO of a bounded labeled Petri net, which was extended in [6] by representing a secret as generalized mutual exclusion constraints. In addition, a secret with no weakly exposed markings and uncertainty of the initial marking were also considered. The work in [5] verified the CSO in a partially observed bounded Petri net, where the unobservable transitions were divided into quasi-observable transitions and

truly unobservable transitions, which were used to analyze the behavior of the system such that more information regarding the system evolution can be precisely captured. However, as far as we know, no work has been reported on the opacity verification of DESs modeled by UPNs.

In this paper, we touch upon the verification of opacity of a DES modeled with unbounded Petri nets by borrowing the methods in [5,6]. The major contributions of this work are stated as follows.

1. A new type of basis coverability graph is proposed. The work by Lefaucheux et al. in [27] is extended to propose a new BCG based on the partially observable places only. In short, based on the number change of tokens in all observable places, the system can determine whether the (unobservable) transitions in their pre/post-sets are fired. This approach releases the frequently adopted assumption that observable transitions necessarily exist in a plant. Furthermore, this newly constructed BCG is readily applicable to the formulation of control laws for large and complex systems. A method of state estimation based on this BCG is also presented;
2. A verification approach for CSO based on BCG is proposed. A sufficient and necessary condition is developed for the verification of opacity based on the current-state estimation and proves that the CSO can be verified in unbounded net systems.

This paper is organized into five sections. Section 2 conceptualizes partial markings and basis coverability graphs. In Section 3, we introduce a method to estimate the current state by using the newly proposed BCG. Section 4 details the verification of CSO in partially observed UPNs. To show that our method is effective and feasible, an example of a real-world system is shown in Section 5. Finally, the paper is concluded in Section 6.

2. Construction of BCG

The concepts of partial markings and BCGs are reviewed in this section, and a new type of BCG is proposed. Due to the limited space, we suppose that readers are familiar with the preliminaries of the Petri net theory and the related concepts. To facilitate the reading and understanding of this research, the Petri net notations and notions used in this paper can be seen in [32]. In addition, the system considered in this work is assumed to be self-loop free.

2.1. Partial Markings

A marking $M \in R(N, M_0)$ restricted to P_o is represented by a vector $\tilde{M}$ with j entries, called the partially observable marking of the marking M [33]. Then, a partially observable marking (partial marking for simplicity) can be readily calculated by

$$A \cdot M = \tilde{M},$$

where A is a $j \times h$ matrix, called the observability mapping matrix with $A(i,i) = 1$ for $i = 1, 2, \ldots, j$, and the other entries are 0. Similarly, the matrix A is used to project a marking M of a Petri net onto a partial marking based on the set of observable places P_o.

Example 1. *A marking of a partially observed UPN is denoted as* $M = [p_{o1}, p_{o2}, p_{o3}, p_{uo1}, p_{uo2}]^T = [1,1,0,1,0]^T$. *By assuming that the mapping matrix* A_1 *is*

$$A_1 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix},$$

the partial marking of $M = [1,1,0,1,0]^T$ *is* $\tilde{M} = [1,1,0]^T$, *whose entries correspond to places* p_{o1}, p_{o2}, *and* p_{o3}, *respectively, i.e.,* $\tilde{M}(p_{o1}) = 1$, $\tilde{M}(p_{o2}) = 1$, *and* $\tilde{M}(p_{o3}) = 0$.

In order to construct the BCG for a UPN with partially observable markings, a coverability set of partial markings is defined as

$$CS_o(N, M_0) = \{\tilde{M} \mid \exists M \in CS(N, M_0), A \cdot M = \tilde{M}\}.$$

Although all the transitions are assumed to be unobservable in a UPN in this paper, the transitions whose firing can be detected and inferred by the token changes in observable places are called quasi-observable transitions. Given an unbounded net system $\langle N, M_0 \rangle$, the set of quasi-observable transitions is defined as

$$\hat{T}_q = \{t \in T \mid ({}^\bullet t \cup t^\bullet) \cap P_o \neq \emptyset\}.$$

Similarly, the transitions that are not in $\hat{T}_q$ are called truly unobservable transitions. Given an unbounded net system $\langle N, M_0 \rangle$, the set of truly unobservable transitions is $\hat{T}_u = T \setminus \hat{T}_q$.

Given a transition sequence $\sigma \in T^*$, we use $\mathcal{P}$ to denote the natural projection with respect to quasi-observable transitions, i.e., $\mathcal{P} : T^* \to \hat{T}_q^*$, which is defined as

$$\begin{cases} \mathcal{P}(\varepsilon) = \varepsilon \\ \mathcal{P}(\sigma) = \sigma, \sigma \in \hat{T}_q^* \\ \mathcal{P}(\sigma) = \varepsilon, \sigma \in \hat{T}_u^* \\ \mathcal{P}(\sigma s) = \mathcal{P}(\sigma)\mathcal{P}(s), \sigma \in T^*, s \in T. \end{cases}$$

The inverse projection $\mathcal{P}^{-1} : \hat{T}_q^* \to 2^{T^*}$ is defined as $\mathcal{P}^{-1}(w) = \{\sigma \in L(N, M_0) | \sigma = \mathcal{P}(w)\}$, i.e., $\mathcal{P}^{-1}(w)$ consists of all transition sequences in $L(N, M_0)$ whose observations are w.

Example 2. *A partially observed unbounded Petri net is considered as shown in Figure 1, where p_{uo} is an unobservable place. Its coverability graph is shown in Figure 2, where a marking is denoted by $M = (p_{o1}, p_{o2}, p_{uo})^T$. Note that p_{o2} is unbounded and that the set of quasi-observable transitions is $\hat{T}_q = \{t_1, t_2\}$.*

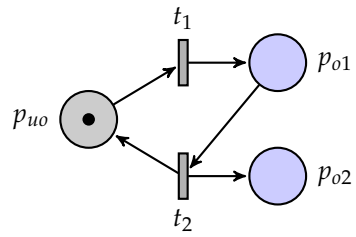

Figure 1. A partially observed unbounded Petri net.

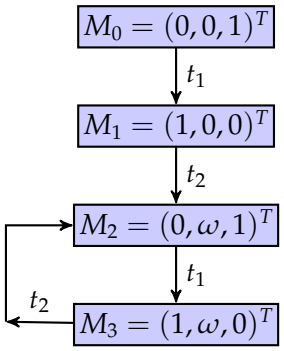

Figure 2. The coverability graph.

Note that, in this investigation, the number of tokens in unbounded places is denoted by ω. Therefore, if there are some unbounded places that are observable, the system's

administrators or intruders can detect the change in the number of tokens in these places. In simpler terms, for some unbounded places, which are denoted by ω, if they are observable, their pre-sets and post-sets are detectable and quasi-observable.

Algorithm 1 is used to identify the quasi-observable and the truly unobservable transitions in an unbounded Petri net. Moreover, given a quasi-observable string w and a partial marking $\tilde{M}$, let us define the set of states that are possibly reachable by detecting and observing w and $\tilde{M}$ as

$$\mathcal{C}(w, \tilde{M}) = \{M | \exists \sigma \in \mathcal{P}^{-1}(w) : M_0[\sigma\rangle M, A \cdot M = \tilde{M}\}$$

which is a collection of markings consistent with w and $\tilde{M}$.

Algorithm 1: Classification of transitions.

Input: A UPN (N, M_0), and a set of observable places P_o.
Output: Set of quasi-observable transitions $\hat{T}_q$, and that of truly unobservable transitions $\hat{T}_u$.

```
Let T̂_q = ∅, and T̂_u = ∅;
if the set of observable places is an empty set, i.e., P_o = ∅ then
    T̂_q = ∅;
    T̂_u = T;
else
    for all transitions t ∈ T do
        if (•t ∪ t•) ∩ P_o ≠ ∅ then
            if t ∉ T̂_q then
                T̂_q = T̂_q ∪ {t};
        else
            if t ∉ T̂_u then
                T̂_u = T̂_u ∪ {t};
```

2.2. Basis Coverability Graph in Partially Observed UPNs

Different from the work in [27], where an approach based on the labeled Petri nets and their markings is proposed, the concepts of quasi-observable transitions, truly unobservable transitions, and partial markings are used to construct our novel BCGs. In addition, the definition of an unobservable transition subnet [6,20] is extended to truly unobservable transitions.

Definition 1. *Let (N, M_0) be a UPN. Additionally, $\hat{T}_u$ is a set of truly unobservable transitions. The truly unobservable subnet $N' = (P, T', Pre', Post')$ of N is obtained by removing $T \setminus \hat{T}_u$, where Pre' and $Post'$ are the restrictions of Pre and $Post$ to $\hat{T}_u$, respectively. The incidence matrix of this subnet is denoted by $C_{\hat{u}} = Post' - Pre'$.*

Therefore, based on the above definition, we assume that the truly unobservable subnet is acyclic.

As shown in Figure 3, a partially observed UPN is considered. Table 1 and Figure 4 show the list of markings and its coverability graph, respectively, where a regular marking is denoted as $M = (p_{o1}, p_{o2}, p_{o3}, p_{uo1}, p_{uo2}, p_{uo3}, p_{uo4})^T$.

Definition 2. *Given a partially observed UPN (N, M_0) with its truly unobservable subnet being acyclic, a partial markings $\tilde{M}$, and a transition $t_q \in \hat{T}_q$,*

$$\Gamma(\tilde{M}, t_q) = \{\sigma \in \hat{T}_u^* | M[\sigma\rangle M', M' \geq Pre(\cdot, t_q), A \cdot M = \tilde{M}\}$$

is defined as a set of explanations of quasi-observable transition t_q at partial marking $\tilde{M}$, and $Y(\tilde{M}, t_q) = \{y_\sigma \in \mathbb{N}^{|\hat{T}_u|} | \exists \sigma \in \Gamma(\tilde{M}, t_q) : y_\sigma = \pi(\sigma)\}$ is defined as the corresponding set of explanation vectors.

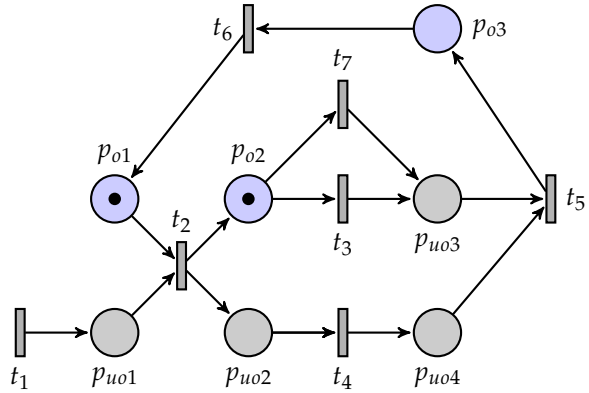

Figure 3. An unbounded Petri net.

Table 1. Markings list of Figure 3.

M	***Vector***	***M***	***Vector***
M_0	$(1,1,0,0,0,0,0)^T$	M_6	$(0,2,0,\omega,0,0,1)^T$
M_1	$(1,1,0,\omega,0,0,0)^T$	M_7	$(0,0,0,\omega,1,2,0)^T$
M_2	$(1,0,0,0,1,0,0)^T$	M_8	$(0,1,0,\omega,0,1,1)^T$
M_3	$(0,2,0,\omega,1,0,0)^T$	M_9	$(0,0,0,\omega,0,2,1)^T$
M_4	$(1,0,0,\omega,0,1,0)^T$	M_{10}	$(0,1,1,\omega,0,0,0)^T$
M_5	$(0,1,0,\omega,1,1,0)^T$	M_{11}	$(0,0,1,\omega,0,1,0)^T$

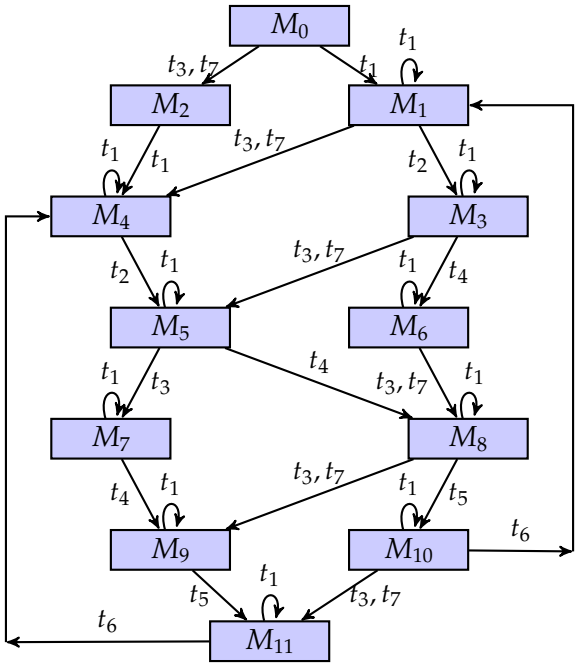

Figure 4. A coverability graph of the unbounded net system.

Definition 3. *Given a partially observed UPN* (N, M_0) *with the acyclic truly unobservable subnet, a partial marking* $\tilde{M} \in CS_o(N, M_0)$*, and a transition* $t_q \in \hat{T}_q$*,*

$$\Gamma_{min}(\tilde{M}, t_q) = \{\sigma \in \Gamma(\tilde{M}, t_q) | \nexists \sigma' \in \Gamma(\tilde{M}, t_q) : \pi(\sigma') \lneq \pi(\sigma)\}$$

is defined as a set of minimum explanations of quasi-observable transition t_q *at partial marking* $\tilde{M}$ *and* $Y_{min}(\tilde{M}, t_q) = \{y_\sigma \in \mathbb{N}^{|\hat{T}_u|} | \exists \sigma \in \Gamma_{min}(\tilde{M}, t_q) : y_\sigma = \pi(\sigma)\}$ *is defined as the corresponding set of minimum explanation vectors.*

Therefore, there necessarily exists a set of basis markings in a BRG regardless of whether the transition set of a labeled Petri net is partitioned [6]. However, in a partially observed UPN, the markings are no longer applicable to constructing the BCG. Instead, the partial markings are only used for this graph. In the following, the definition of a set of basis partial markings is proposed.

Definition 4. *For an unbounded net system* $\langle N, M_0 \rangle$ *and an initial partial marking* $\tilde{M}_0$*, a set of basis partial markings* $\mathcal{M}_b$ *is defined as follows:*

1. $\tilde{M}_0 \in \mathcal{M}_b$;
2. $\forall \tilde{M} \in \mathcal{M}_b, \forall t_q \in \hat{T}_q, \forall \sigma' \in \Gamma_{min}(M, t)$ *and* $y_\sigma = \pi(\sigma')$*, it holds* $\tilde{M}' \in \mathcal{M}_b$*, where* $\tilde{M}' = \tilde{M} + C(\cdot, t_q) + C_{\hat{u}} \cdot y_\sigma$.

In other words, the set of basis partial markings includes the initial partial marking and a set of all of the partial markings reachable by firing quasi-observable transitions and minimum explanations of truly unobservable transitions.

Based on the above definitions, an algorithm is proposed to construct a BCG for partially observed UPNs. We follow the work in [6] by using an NFA $\mathbb{C} = (\mathcal{M}_b, \hat{T}_q, \Delta, \tilde{M}_0)$ to represent the novel BCG, where $\mathcal{M}_b$ is the set of basis partial markings, $\hat{T}_q$ is a set of quasi-observable transitions, and Δ is a transition function defined as $\Delta : \mathcal{M}_b \times \hat{T}_q \to \mathcal{M}_b$.

Algorithm 2 can be briefly explained. In the first step, the set of basis partial markings $\mathcal{M}_b$ is initialized at $\mathcal{M}_b = \{\tilde{M}_0\}$. For all non-visited basis partial markings $\tilde{M}$ and all quasi-observable transitions $\hat{T}_q$, we need to determine whether its minimum explanation vector $Y_{min}(\tilde{M}, t)$ is a nonempty set. If it is not empty, a new basis partial marking can be calculated. The algorithm runs repeatedly until all basis partial markings are calculated.

Algorithm 2: Construction of BCG for a partially observed UPN.

Input: A UPN (N, M_0), a set of partial markings $CS_o(N, M_0)$, and a set of quasi-observable transitions $\hat{T}_q$.
Output: A BCG $\mathbb{C} = (\mathcal{M}_b, \hat{T}_q, \Delta, \tilde{M}_0)$.

```
1  M̂ = {M̃_0} and assign no label to M̃_0;
2  while states with no label exist do
3      select a partial marking M̃ ∈ M_b with no label;
4      for all t_q ∈ T̂_q do
5          if Y_min(M̃, t_q) ≠ ∅ then
6              for all y_σ ∈ Y_min(M̃, t_q) do
7                  M̃' = M̃ + C(·, t_q) + C_û · y_σ;
8                  if M̃' ∉ M_b then
9                      M_b = M_b ∪ {M̃'};
10                 Δ = Δ ∪ {M̃, t_q, M̃'};
11             Assign a label "done" to M̃;
12 Remove all labels.
```

Example 3. *The partially observed unbounded Petri net is considered again as shown in Figure 3. Table 1 is the marking list of the net system, where a marking is denoted as* $M = [p_{o1}, p_{o2}, p_{o3}, p_{uo1}, p_{uo2}, p_{uo3}, p_{uo4}]^T$*; Figure 4 is the coverability graph of the net system. The places* p_{uo1}*, ,* p_{uo2}*,* p_{uo3}*, and* p_{uo4} *are assumed to be unobservable. Therefore, the set of quasi-observable transitions is* $\hat{T}_q = \{t_2, t_3, t_5, t_6, t_7\}$*, and the others are truly unobservable transitions. Moreover, a new mapping matrix* A_2 *is assumed as*

$$A_2 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

The novel BCG is shown in Figure 5. Since t_1 and t_4 are truly unobservable transitions, if an intruder observes a new partial marking $\tilde{M}_2$ from $\tilde{M}_0$, the set of explanations with respect to $\tilde{M}_o$ may be $\{t_1^n\}$, where $n \in \mathbb{N}$. Therefore, there is one minimum explanation, i.e., $\Gamma_{min} = \{t_1\}$.

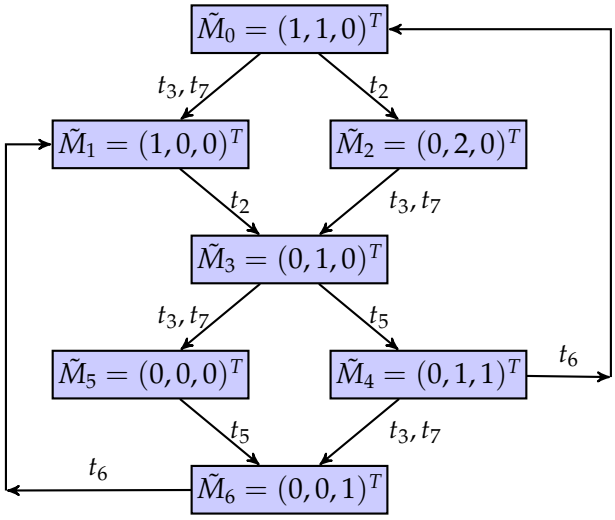

Figure 5. A BCG of the unbounded net system.

A special situation should be noted in this work: Given two quasi-observable transitions $t_1, t_2 \in \hat{T}_q$, they are said to be confused if $Pre(p, t_1) = Pre(p, t_2)$, or $Post(p, t_1) = Post(p, t_2)$, where p is an arbitrary observable place, with $p \in {}^\bullet t_1 \cap {}^\bullet t_2$ or $p \in t_1^\bullet \cap t_2^\bullet$. In other words, there may be multiple quasi-observable transitions in the net system that can lead to the same change in the observable places. This change makes the intruders unable to determine which transition is fired. Therefore, in the novel BCG, there may exist two or even more quasi-observable transitions that are tagged on an arc from one node to another node. In simpler terms, the system administrators do not need to determine which quasi-observable transition is fired. They only need to determine that one of them has been fired.

Example 4. *As shown in Figures 3 and 5, the partially observed UPN and its BCG are considered again. From the initial partial marking $\tilde{M}_0 = (1,1,0)^T$, if a new partial marking $\tilde{M}_1 = (1,0,0)^T$ is observed, there are two situations: $\tilde{M}_0 \times t_3 \to \tilde{M}_1$ and $\tilde{M}_0 \times t_7 \to \tilde{M}_1$, i.e., transitions t_3 and t_7 are confused. Therefore, for the set of quasi-observable transitions $\{t_3, t_7\}$, we conclude that one of the transitions t_3 and t_7 must have been fired.*

3. Current-State Estimation

Based on the new BCG, the concept of current-state estimation is discussed in this section. Let us now introduce the following statements that are useful to formalize the main result.

Given a marking M, $A \cdot M = \tilde{M}$, which is reached by firing a quasi-observable transition $t_q \in \hat{T}_q$, i.e., $M_0[\sigma t_q\rangle M$, where $\sigma \in T^*$, a new set of markings is defined as $\mathcal{U}(\tilde{M}) = \{M' | \exists \sigma' \in \hat{T}_u^* : M[\sigma'\rangle M'\}$, called the unobservable reach of the partial marking $\tilde{M}$.

Given a partial marking $\tilde{M}$ and a quasi-observable transition t_q, we assume that the firing of an enabled quasi-observable transition t_q at partial marking $\tilde{M}$ yields a partial marking $\tilde{M}' = \tilde{M} + C(\cdot, t_q) + C_{\hat{u}} \cdot \pi(\sigma_u)$, where $\sigma_u \in \Gamma_{min}(\tilde{M}, t_q)$, which is denoted by $\tilde{M}[t_q\rangle \tilde{M}'$. A quasi-observable string $w = \mathcal{P}(\sigma) = t_{q1} t_{q2} \dots t_{qn} \in \hat{T}_q^*$, is enabled at partial marking $\tilde{M}$ if there exist partial markings $\tilde{M}_1, \tilde{M}_2, \dots, \tilde{M}_n$ such that $\tilde{M}[t_{q1}\rangle \tilde{M}_1[t_{q2}\rangle \dots \tilde{M}_{n-1}[t_{qn}\rangle \tilde{M}_n$,

denoted as $\tilde{M}[w\rangle\tilde{M}_n$, where $\sigma \in T^*$, and $n \in \mathbb{N}$. Specifically, if a quasi-observable string w is an empty string, then $\tilde{M}[w\rangle\tilde{M}$ holds.

Theorem 1. *Consider a UPN (N, M_0) with $N = (P, T, Pre, Post)$, whose truly unobservable subnet is acyclic, and a marking M' that is reached by firing a quasi-observable transition. For arbitrary partial markings $\tilde{M} \in CS_o(N, M_0)$ and an explanation vector $y_\sigma \in Y(\tilde{M}, t)$, it holds that*

$$\begin{aligned}\mathcal{C}(w, \tilde{M}) &= \mathcal{U}(\tilde{M}) \\ &= \{M | M = M' + C_{\hat{u}} \cdot y_\sigma, A \cdot M' = A \cdot M = \tilde{M}\}.\end{aligned}$$

Proof. This proof is extended from [33]. We prove this result by induction on the length of the string w, where there is a transition sequence σ, $\mathcal{P}(\sigma) = w$.

In the case that w is an empty string, then the result is true.

Assume that the result is valid for v. We prove that it is also true for $w = vt_q$, where $t_q \in \hat{T}_q$.

In fact, there is a transition sequence $\sigma \in T^*$ such that $M_0[\sigma\rangle M'$ with $\mathcal{P}(\sigma) = w$, and $y_\sigma = \pi(\sigma)$. Then, there are two sequences σ', σ'' such that

$$M_0[\sigma'\rangle M'[t_q\rangle M''[\sigma''\rangle M'''.$$

where $\mathcal{P}(\sigma') = v$ and $\sigma'' \in \hat{T}_u^*$. Therefore, one has

$$A \cdot M_0 \neq A \cdot M' \neq A \cdot M'' \neq A \cdot M'''.$$

By induction, there is a partial marking $\tilde{M} \in CS_o(N, M_0)$ such that

$$M_0[\sigma_a\rangle M[\sigma_b\rangle M'[t_q\rangle M''[\sigma'\rangle M''', \tag{1}$$

where $\mathcal{P}(\sigma_a) = v$, $\sigma_b \in \hat{T}_u^*$ and there is a transition sequence $\sigma_u \in \hat{T}_u$ such that $\pi(\sigma_u) = y_\sigma$ and $\pi(\sigma_a) = \pi(v) + y_\sigma$. In addition, we have

$$A \cdot M = A \cdot M' = \tilde{M}.$$

By definition of minimal explanations, there is a transition sequence $\sigma_c \in \Gamma(\tilde{M}, t_q)$ such that

$$M[\sigma_c\rangle M_c[t_q\rangle M_d \tag{2}$$

with $A \cdot M = A \cdot M_c$ and $\pi(\sigma_c) \leq \pi(\sigma_b)$.

We now claim that there is a transition sequence σ_d with $\pi(\sigma_b) = \pi(\sigma_c) + \pi(\sigma_d)$ enabled at M_d. In fact, from Equation (1), it follows that

$$\begin{aligned}M'' &= M + C_{\hat{u}} \cdot \pi(\sigma_b) + C(\cdot, t_q) \\ &= M + C_{\hat{u}} \cdot \pi(\sigma_c) + C_{\hat{u}} \cdot \pi(\sigma_d) + C(\cdot, t_q),\end{aligned}$$

while from Equation (2), it follows that

$$M_d = M + C_{\hat{u}} \cdot \pi(\sigma_c) + C(\cdot, t_q).$$

The last two equations imply that

$$M_d = M + C_{\hat{u}} \cdot \pi(\sigma_d) \geq 0,$$

and since the truly unobservable subnet is acyclic, it holds that

$$M_d[\sigma_d\rangle M'', \tag{3}$$

$$A \cdot M_d = A \cdot M'', \tag{4}$$

Combining Equations (1)–(4), we can write

$$M_0[\sigma_a\rangle M[\sigma_c\rangle M_c[t_q\rangle M_d[\sigma_d\rangle M''[\sigma''\rangle M'''.$$

This completes the proof. □

In simpler terms, for an unbounded net system, if there is a marking that is reached by firing a quasi-observable transition t_q, we need to find some markings that still have the same measurement results after firing some truly unobservable transitions, i.e., these markings all have the same partial marking.

Example 5. *As shown in Figure 3, we continue to consider the unbounded net system. Table 2 is a list of all potential markings for all partial markings.*

Since the solution of y_σ is a non-negative solution, given an initial marking M_0 with its partial marking being $\tilde{M}_0$, the potential markings are M_0 and M_1 due to $M_0[t_1\rangle M_1$, where $t_1 \in \hat{T}_u$, and $A_2 \cdot M_0 = A_2 \cdot M_1 = \tilde{M}_0$. On the other hand, given a marking M_3, the partial marking of M_3 is $\tilde{M}_2$. The other potential marking with respect to $\tilde{M}_2$ is $\{M_6\}$, thanks to $M_3[t_1\rangle M_3$ and $M_3[t_4\rangle M_6$, where $t_1, t_4 \in \hat{T}_u$ and $A_2 \cdot M_3 = A_2 \cdot M_6 = \tilde{M}_2$.

Based on Table 2 and the above examples, a BCG-based observer is constructed in Figure 6.

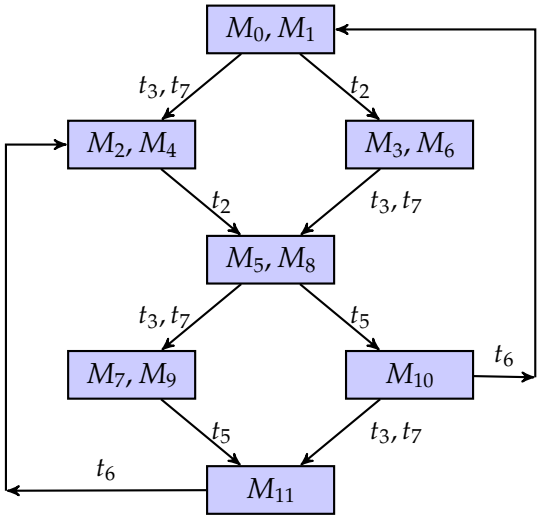

Figure 6. An observer of the unbounded net system.

Table 2. Set of markings with respect to $\tilde{M}$.

$\tilde{M}$	$\mathcal{C}(w, \tilde{M})$
$\tilde{M}_0 = (1,1,0)^T$	M_0, M_1
$\tilde{M}_1 = (1,0,0)^T$	M_2, M_4
$\tilde{M}_2 = (0,2,0)^T$	M_3, M_6
$\tilde{M}_3 = (0,1,0)^T$	M_5, M_8
$\tilde{M}_4 = (0,1,1)^T$	M_{10}
$\tilde{M}_5 = (0,0,0)^T$	M_7, M_9
$\tilde{M}_6 = (0,0,1)^T$	M_{11}

Based on Algorithm 2 and the above definitions of explanations and current-state estimation, the necessity of the truly unobservable subnet needs to be explained. For the partially observed unbounded net systems studied in this work, we can only infer the evolution process of the system state by observing the partial markings composed of partially observable places. In other words, the markings cannot be used to construct a complete coverability graph to obtain complete information about the system. Therefore, it is necessary for us to build novel BCGs to help us complete the acquisition of system information. However, if we do not require that the truly unobservable transition subnet should not constitute a circuit, then the construction of our BCGs may never be complete,

i.e., the net system remains in a circuit without any quasi-observable transition being fired. This situation makes it impossible to obtain a complete result of the current-state estimation. Based on this situation, we insist that, for building a BCG, the unobservable transition subnet needs to be acyclic. In the next section, the above results are used to verify the opacity problem.

4. Current-State Opacity Verification

In this section, a method is proposed for verifying the CSO by using the BCG.

4.1. CSO on Unbounded Net Systems

In this part, the set of secret S is defined as a subset of the arbitrary markings. For this work, since all transitions are unobservable, we not only need to estimate the current state of the system but also predict the transitions in its pre-set or pro-set through a few observable places. In this regard, a new definition of CSO is proposed.

Definition 5. *Given a UPN (N, M_0) with the truly unobservable subnet being acyclic and a set of secret $S \subseteq R(N, M_0)$, the unbounded net system $\langle N, M_0 \rangle$ is said to be current-state opaque with respect to S if for any transition sequence $\sigma \in T^*$, $\mathcal{P}(\sigma) = w$ such that $\tilde{M}_0[w\rangle \tilde{M}$, and $\mathcal{C}(w, \tilde{M}) \nsubseteq S$ holds.*

In simpler terms, an unbounded net system is current-state opaque if, for an arbitrary partial marking that is reached by firing a quasi-observable string, there exists at least one marking that does not belong to the secret in the result of the current-state estimation.

Example 6. *The unbounded net system is considered again as shown in Figure 3. Let the secret be $S = \{M_3, M_5\}$. Suppose that an intruder detects a quasi-observable string $w = t_2t_3$, i.e., $\tilde{M}_0[t_2\rangle \tilde{M}_2\ [t_3\rangle \tilde{M}_3$. Then, the system is current-state opaque since $\mathcal{C}(w_0, \tilde{M}_0) \nsubseteq S$, $\mathcal{C}(w_1, \tilde{M}_2) \nsubseteq S$, and $\mathcal{C}(w_2, \tilde{M}_3) \nsubseteq S$, where w_0 is an empty string, $w_1 = t_2$, and $w_2 = t_2t_3$.*

Moreover, given a UPN (N, M_0) with the truly unobservable subnet being acyclic, and secret S, a marking M is said to be exposed if $M \in CS(N, M_0) \setminus S$. Furthermore, the set of exposed markings is defined as $E(S) = CS(N, M_0) \setminus S$.

Example 7. *The unbounded net system is considered again as shown in Figure 3. Let the secret states be $S_1 = \{M_0, M_2, M_3, M_5, M_7\}$. Then, the set of exposed markings is $E(S_1) = \{M_1, M_4, M_8 - M_{11}\}$.*

The above example intuitively explains what markings do not belong to the secret. However, this would be inadequate. More details should be considered. Given a UPN (N, M_0) with the truly unobservable subnet being acyclic, and secret S, a marking M with $A \cdot M = \tilde{M}$ is said to be weakly exposed if M is an exposed marking, and $M \in \mathcal{U}(\tilde{M})$. Furthermore, the set of weakly exposed markings consistent with partial marking $\tilde{M}$ is defined as $WE(S, \tilde{M}) = E(S) \cap \mathcal{U}(\tilde{M})$.

Example 8. *The above example is extended here. For a partial marking $\tilde{M}_3$, the marking M_8 is a weakly exposed marking, since $M_8 \in E(S_1)$, $M_5[t_4\rangle M_8$, and $A_2 \cdot M_5 = A_2 \cdot M_8$. At the same time, $WE(S_1, \tilde{M}_0) = \{M_1\}$, $WE(S_1, \tilde{M}_1) = \{M_4\}$, $WE(S_1, \tilde{M}_2) = \{M_6\}$, $WE(S_1, \tilde{M}_4) = \{M_{10}\}$, $WE(S_1, \tilde{M}_5) = \{M_9\}$, and $WE(S_1, \tilde{M}_6) = \{M_{11}\}$.*

Note that some markings, such as M_{11}, are reached by firing one of the quasi-observable transitions in $\{t_3, t_5, t_7\}$. At the same time, there exists a truly unobservable transition that can be fired, e.g., $M_{11}[t_1\rangle M_{11}$, so these markings also belong to $WE(S, \tilde{M})$.

Based on the above definitions and theorem, the following necessary and sufficient condition is proposed for CSO.

Theorem 2. *Given a UPN $\langle N, M_0\rangle$ with $N = (P, T, Pre, Post)$, whose truly unobservable subnet is acyclic, and a secret $S \subseteq R(N, M_0)$, the system is current-state opaque with respect to S if and only if for all $\sigma \in T^*$ with $\mathcal{P}(\sigma) = w$ and $\tilde{M}_0[w\rangle\tilde{M}$, $\mathcal{C}(w, \tilde{M}) \cap WE(S, \tilde{M}) \neq \emptyset$ holds.*

Proof. ($\Rightarrow$) Given an arbitrary sequence $\sigma \in T^*$ such that $\mathcal{P}(\sigma) = w$ and $\tilde{M}_0[w\rangle\tilde{M}$, if the set of weakly exposed markings consistent with $\tilde{M}$ is not an empty set, then there is a marking $M \in \mathcal{U}(\tilde{M})$, $M \in E(S)$, i.e., $M \in \mathcal{U}(\tilde{M}) \cap E(S) = WE(S, \tilde{M})$, and hence, $M \in \mathcal{C}(w, \tilde{M})$. This indicates that $\mathcal{C}(w, \tilde{M}) \cap WE(S, \tilde{M}) \neq \emptyset$. By the definition of the set of exposed markings, the system is current-state opaque with respect to S.

($\Leftarrow$) On the contrary, given an unbounded net system that is current-state opaque, we assume that an intruder detects a quasi-observable string w such that $\tilde{M}_0[w\rangle\tilde{M}$, and none of the markings consistent with $\tilde{M}$ are weakly exposed. Based on Theorem 1 and the definition of exposed markings, all markings consistent with partial marking $\tilde{M}$ belong to the secret, i.e., $\mathcal{C}(w, \tilde{M}) \cap WE(S, \tilde{M}) = \emptyset$, i.e., the system is not opaque. This indicates that this assumption contradicts the definition of opacity, which completes the proof. □

As stated in the above theorem, if the system administrators need to verify whether an unbounded net system is current-state opaque, they just need to find out whether there exists at least one weakly exposed marking in partial markings, instead of exhausting all the states.

4.2. CSO Verification on BCG

This subsection deals with the CSO verification based on the BCG. Since the purpose of this work is to extend the existing opacity verification methods to UPNs, some existing methods [5,6] can be referred to and used. Given a UPN (N, M_0) with the truly unobservable subnet being acyclic, and a secret S, a binary scalar $a(\tilde{M})$ is defined as follows:

$$a(\tilde{M}) = \begin{cases} 1 & \mathcal{C}(w, \tilde{M}) \cap WE(S, \tilde{M}) \neq \emptyset; \\ 0 & otherwise. \end{cases}$$

The BCG is combined with binary scalar $a(\tilde{M})$ to construct a new non-deterministic automaton (NFA), i.e., a new observer $\hat{\mathbb{C}} = (\hat{\mathcal{M}}_b, \hat{T}_q, \Delta, \tilde{M}_0)$, where $\hat{\mathcal{M}}_b \subseteq \mathcal{M}_b \times \{0, 1\}$. Compared with the observer in [6], their spatial complexity is approximate. The spatial complexity of the new non-deterministic automaton observer $\hat{\mathbb{C}}$ is $\mathcal{O}(2^{|\tilde{M}|})$. In general, the number of partial markings is less than or equal to that of markings, i.e., $|CS_o(N, M_0)| \leq |CS(N, M_0)|$. Moreover, if the secret S is changed to S', we only need to change the scalar $a(\tilde{M})$ of all partial markings. In the following, a proposition for the CSO verification problem is proposed by using the BCG.

Proposition 1. *Given a UPN (N, M_0) with the truly unobservable subnet being acyclic, and a secret $S \subseteq R(N, M_0)$, for all nodes in the new non-deterministic automaton observer, if the binary scalar is always $a(\tilde{M}) = 1$, then the unbounded net system $\langle N, M_0\rangle$ is current-state opaque with respect to secret S.*

Proof. Based on the contrapositive, assume that the system is not current-state opaque. If the binary scalars of all nodes in an unbounded net system are equal to 1, i.e., for all partial markings $\tilde{M}$, $a(\tilde{M}) = 1$, we can find that there is at least one weakly exposed marking in the result of any state estimation. According to Theorem 2, the unbounded net system is current-state opaque with respect to S. However, this contradicts the original hypothesis, which completes the proof. □

In simpler terms, according to Theorem 2 and Proposition 1, if all the binary scalars are 1, i.e., $a(\cdot) = 1$, the net system is current-state opaque; otherwise, we require further analysis. According to the above proposition, an example is present to illustrate the novel method.

Example 9. *As shown in Figure 3, the unbounded net system is considered again. The secret set of Example 7 is considered again. Figure 7 is the new BCG-based observer of the unbounded net system using the non-deterministic automaton. Since the binary scalar of all nodes in this automaton is* $a(\tilde{M}) = 1$. *It represents that the unbounded net system* $\langle N, M_0 \rangle$ *is current-state opaque.*

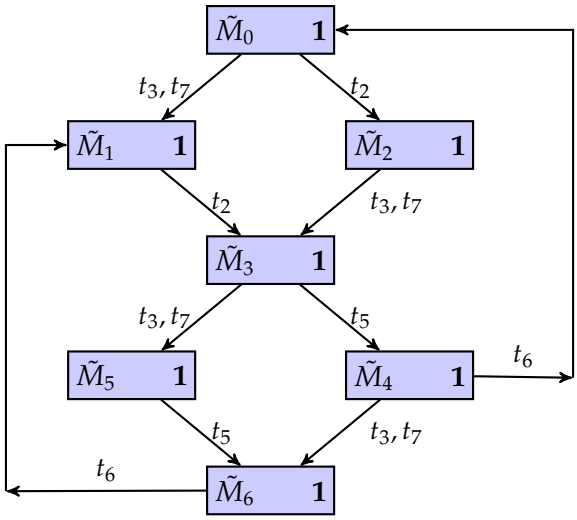

Figure 7. A BCG-based new observer of the unbounded net system.

In other words, for any quasi-observable string, if there exists at least one weakly exposed marking associated with the arbitrary partial marking, then it means that the unbounded net system is current-state opaque.

5. An Example of Real Systems

In this section, the novel methodology will be applied to a real system that can be of help to illustrate the idea underlying this research. We hope that the explanation of this example can show that our method has a certain engineering guiding significance such that a practitioner may be interested in this study.

A small but comprehensive flexible manufacturing cell [34] is considered as shown in Figure 8. The reason that we choose a manufacturing cell as an example lies in the fact that such an example is easy to understand and captures the methods developed in this paper. The system is composed of one robot, one input buffer, one output buffer, and two machines. The robot and the machines can only deal with one part when the system is working. Specifically, the buffer can be regarded as an infinite bin, i.e., its space capacity is unlimited, which is different from the traditional modeling methods that assume such a buffer is bounded. The workflow of this system is as follows: When a sensor detects that the goods to be processed enter the input buffer if the robot and Machine 1 are available, the robot will put the goods into Machine 1 for processing. When the work of Machine 1 is completed, the robot puts the goods into the buffer for storage. Machine 2 will regularly use the robot to process goods. The robot will put the goods into Machine 2 from the buffer. If the buffer is empty, the robot will directly put the goods into Machine 2 from Machine 1. When Machine 2 finishes the processing, the robot transfers the goods to the output.

The system is modeled by Petri nets in Figure 9, where places $\{p_{uo1}, \ldots, p_{uo6}\}$ and all transitions are unobservable. Furthermore, the meanings of all places and transitions are displayed in Table 3. A coverability graph is shown in Figure 10, where a marking of the system is denoted as $M = (p_{o1}, p_{o2}, p_{o3}, p_{o4}, p_{o5}, p_{o6}, p_{uo1}, p_{uo2}, p_{uo3}, p_{uo4}, p_{uo5}, p_{uo6})^T$. Based on the set of unobservable places, we can infer that the set of truly unobservable transitions is $\hat{T}_u = \{t_8, t_9\}$, and $\hat{T}_q = T \setminus \hat{T}_u$. Moreover, the mapping matrix A_3 is assumed as follows by using the technique presented, as aforementioned:

$$A_3 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

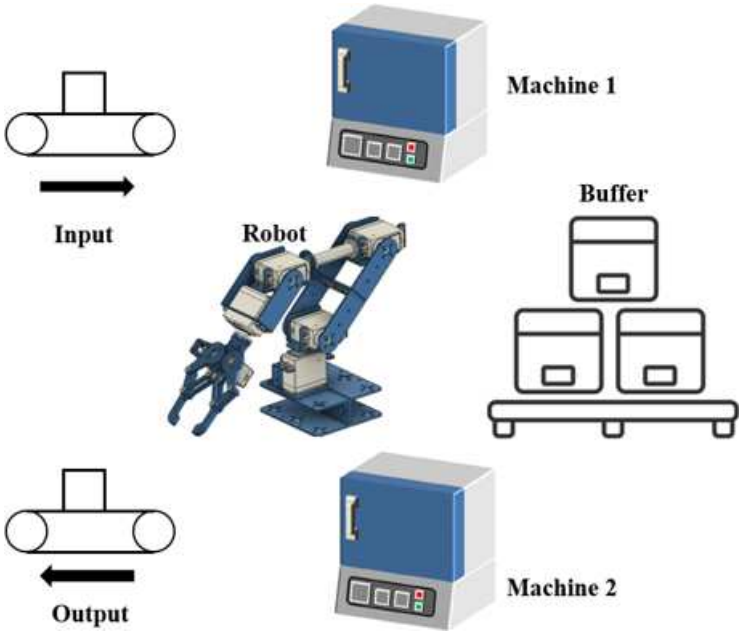

Figure 8. A small flexible manufacturing cell.

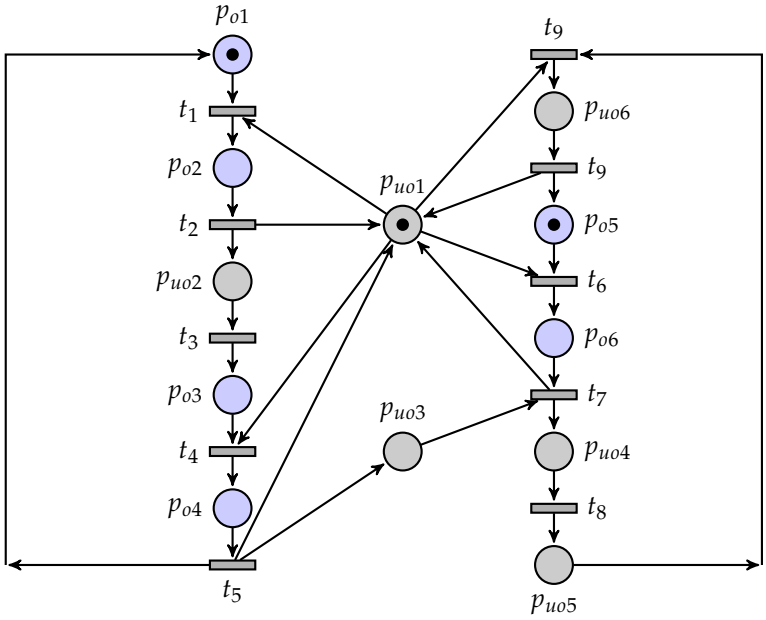

Figure 9. The Petri net model.

Figure 11 is a BCG of the flexible manufacturing cell using the partial markings and quasi-observable transitions. The results of the current-state estimation with partial markings are shown in Figure 12. In this work, we assume that the process of Machine 2 is the confidential information of the system, i.e., the secret states are $S = \{M_7, M_8\}$.

Its BCG-based observer, as shown in Figure 13, is constructed to verify if the system is current-state opaque.

Table 3. Meaning of transitions and places.

T	*Meaning*	*P*	*Meaning*
t_1	Goods detected	p_{o1}	Machine 1 waiting
t_2	Load over	p_{o2}	Loading
t_3	Machine 1 over	p_{uo2}	Machine 1 processing
t_4	Ready to move	p_{o3}	Wait robot
t_5	Buffer entered	p_{o4}	Move to buffer
t_6	Robot requested	p_{uo3}	Buffer
t_7	Move to Machine 2	p_{o5}	Machine 2 waiting
t_8	Machine 2 over	p_{o6}	Robot holding
t_9	Product detected	p_{uo4}	Machine 2 processing
t_{10}	Unload over	p_{uo5}	Wait robot
		p_{uo6}	Unload
		p_{uo1}	Robot

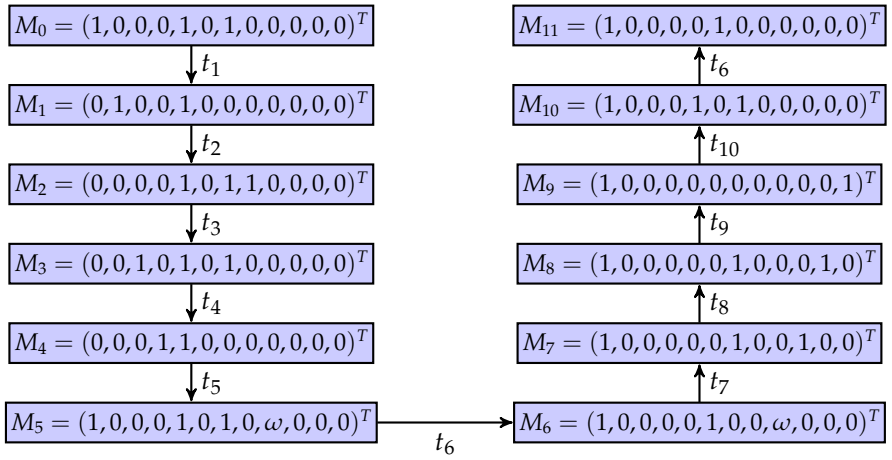

Figure 10. A coverability graph of the net system.

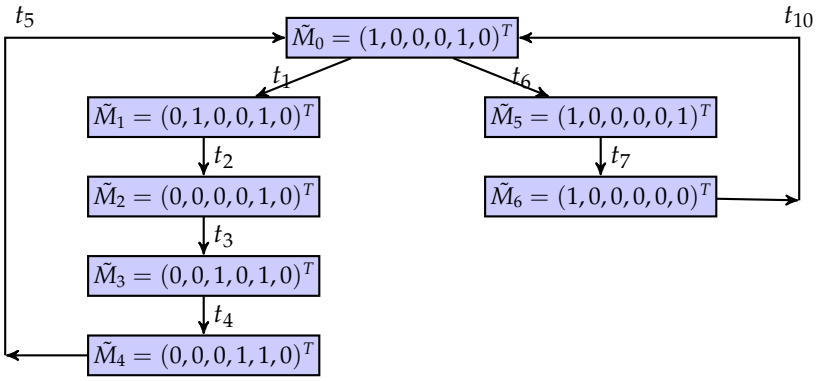

Figure 11. A BCG of the net system.

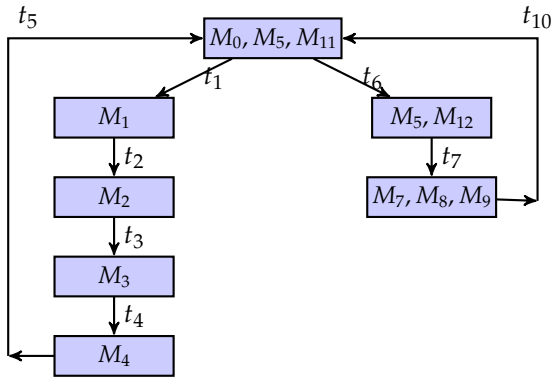

Figure 12. The result of state estimation.

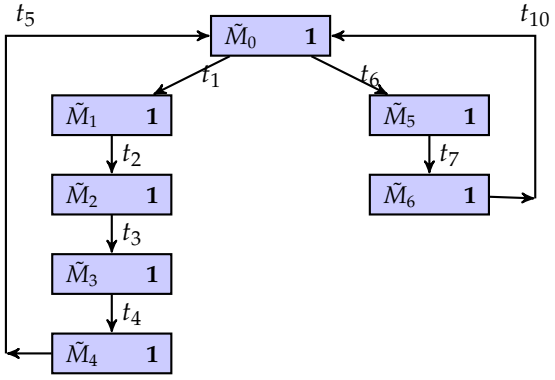

Figure 13. The BCG-based observer.

There is a possibility that when the system is invaded by intruders, the system can keep secret information. Specifically, an intruder can infer the system's quasi-observable transitions and build the corresponding BCG of the system. When they observe that the evolution of the system is $t_1t_2t_3t_4t_5t_6t_7$, the corresponding partial marking of the system is $\tilde{M}_6$, and at the same time, $\mathcal{C}(w, \tilde{M}_6) \cap WE(S, \tilde{M}_6) \neq \emptyset$, and $a(\tilde{M}_6) = 1$. This means that the intruder cannot determine whether the current state of the system must be a secret state. On the other hand, for other partial marks, there is no possible secret state in their current state estimation results. In other words, in the BCG-based observer of the system, the binary scalar of any node is equal to one, i.e., $a(\cdot) = 1$. Therefore, the flexible manufacturing cell is current-state opaque.

Based on this example, we can find that for a manufacturing system, because goods are constantly transported, loaded, and unloaded, a real system is in general not bounded, as it is reasonable to assume that the production is continuous without any interruption. In other words, unbounded systems are more common than bounded systems. Furthermore, the method reported in this particular research not only is successfully applied to the proposed example but also shows that this method can be closer to the conditions of unbounded systems in the real world. Therefore, this method is more effective in solving the problem of confidentiality of confidential information in the real world.

6. Conclusions

This paper deals with the verification of CSO in partially observed unbounded Petri nets, where the truly unobservable subnet is acyclic. The coverability problem and complete state estimation problem are explored by using the novel basis coverability graph. This research proves that the BCG can verify the CSO problems by constructing a BCG-based observer. This approach is characterized by the fact that the CSO problem can be accomplished based on only a few observations. Specific examples are presented and illustrate that this approach is effective.

However, based on the real-world example, one deficiency in this research is also recognized. From the viewpoint of graph theory, Petri nets are a topological structure of a real system, and their nodes correspond to the components of the system. This phenomenon leads to the necessity of reusing Petri nets for modeling if the structure of the system or topology is changed. To help system administrators analyze system performance, adaptive modeling methods developed for system structure changes will become a new research topic.

In future work, unbounded Petri nets and their basis coverability graphs are still our research interest. All the typical problems arising in the domain of discrete event systems modeled with unbounded Petri nets will be continuously explored, such as the verification of initial-state opacity and language-based opacity, the analysis of detectability [35,36], the enforcement of opacity based on supervisory control [37], and fault diagnosis and diagnosability analysis [38]. It is also interesting to address various scheduling problems of automated production systems [39] with the opacity property being guaranteed.

Author Contributions: Conceptualization, H.Z., and Z.L.; methodology, H.Z.; validation, H.Z., and Z.L.; Formal analysis, A.M.E.-S.; Resources, M.A.E.-M.; Writing—original draft, H.Z.; Writing—review & editing, Z.L.; Supervision, A.M.F.-F., and Z.L.; Project administration, A.M.E.-S., M.A.E.-M., and Z.L. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the Science and Technology Fund, FDCT, Macau SAR, under grant 0064/2021/A2, and by the Special Fund for Scientific and Technological Innovation Strategy of Guangdong Province under grant No. 2022A0505030025. The authors extend their appreciation to King Saud University, Saudi Arabia, for funding this work through Researchers Supporting Project number (RSP2023R133), King Saud University, Riyadh, Saudi Arabia.

Data Availability Statement: Date are contained within the article.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Lin, F. Opacity of discrete event systems and its applications. *Automatica* **2011**, *47*, 496–503. [CrossRef]
2. Mazaré, L. Using unification for opacity properties. In Proceedings of the 4th IFIP WGI, Baracelona, Spain, 5–7 April 2004; Volume 7, pp. 165–176.
3. Jacob, R.; Lesage, J.-J.; Faure, J.-M. Overview of discrete event systems opacity: Models, Validation, and Quantification. *Annu. Rev. Control* **2016**, *41*, 135–146. [CrossRef]
4. Tong, Y.; Li, Z.; Seatzu, C.; Giua, A. Verification of current-state opacity using Petri nets. In Proceedings of the American Control Conference, Chicago, IL, USA, 1–3 July 2015; pp. 1935–1940.
5. Saadaoui, I.; Li, Z.; Wu, N. Current-state opacity modelling and verification in partially observed Petri nets. *Automatica* **2020**, *116*, 108907. [CrossRef]
6. Tong, Y.; Li, Z.; Seatzu, C.; Giua, A. Verification of state-based opacity using Petri nets. *IEEE Trans. Autom. Control* **2017**, *62*, 2823–2837. [CrossRef]
7. Tong, Y.; Li, Z.; Seatzu, C.; Giua, A. Verification of initial-state opacity in Petri nets. In Proceedings of the 54th IEEE Conference on Decision and Control, Osaka, Japan, 15–18 December 2015; pp. 344–349.
8. Saboori, A.; Hadjicostis, C.N. Verification of *k*-step opacity and analysis of its complexity. *IEEE Trans. Autom. Sci. Eng.* **2011**, *8*, 549–559. [CrossRef]
9. Falcone Y.; Marchand, H. Runtime enforcement of *k*-step opacity. In Proceedings of the 52nd IEEE Conference on Decision and Control, Firenze, Italy, 10–13 December 2013; pp. 7271–7278.
10. Yin X.; Li, S. Synthesis of dynamic masks for infinite-step opacity. *IEEE Trans. Autom. Control* **2020**, *65*, 1429–1441. [CrossRef]
11. Ma, Z.; Yin, X.; Li, Z. Verification and enforcement of strong infinite-step and *k*-step opacity using state recognizers. *Automatica* **2021**, *133*, 109838. [CrossRef]
12. Paoli, A.; Lin, F. Decentralized opacity of discrete event systems. In Proceedings of the America Control Conference, Montreal, QC, Canada, 27–29 June 2012; Volume 99, pp. 6083–6088.
13. Deng, W.; Yang, J.; Jiang, C.; Qiu, D. Opacity of fuzzy discrete event systems. In Proceedings of the Chinese Control and Decision Conference, Nanchang, China, 3–5 June 2019; pp. 1840–1845.
14. Cong, X.; Fanti, M.; Mangini, M.; Li, Z. On-line verification of current-state opacity by Petri nets and integer linear programming. *Automatica* **2018**, *94*, 205–213. [CrossRef]
15. Zhang, C.; Tian, G.; Fathollahi-Fard, A.M.; Wang, W.; Wu, P.; Li, Z. Interval-valued intuitionistic uncertain linguistic cloud Petri net and its application to Risk assessment for subway fire accident. *IEEE Trans. Autom. Sci. Eng.* **2022**, *19*, 163–177. [CrossRef]

16. Cassandras, C.G.; Lafortune, S. *Introduction to Discrete Event Systems*, 2nd ed.; Springer Science & Business Media: New York, NY, USA, 2009.
17. Zhu, G.; Feng, L.; Li, Z.; Wu, N. An efficient fault diagnosis approach based on integer linear programming for labeled Petri nets. *IEEE Trans. Autom. Control* **2021**, *66*, 2393–2398. [CrossRef]
18. Cabasino, M.P.; Giua, A.; Seatzu, C. Diagnosability of bounded Petri nets. In Proceedings of the 48th IEEE Conference on Decision and Control Held Jointly with 28th Chinese Control Conference, Shanghai, China, 15–18 December 2009; pp. 1254–1260.
19. Lin, F.; Wang, W.; Han, L.; Shen, B. State estimation of multichannel networked discrete event systems. *IEEE Trans. Control Netw. Syst.* **2020**, *7*, 53–63. [CrossRef]
20. Ma, Z.; Tong, Y.; Li, Z.; Giua, A. Basis marking representation of Petri net reachability spaces and its application to the reachability problem. *IEEE Trans. Autom. Control* **2017**, *62*, 1078–1093. [CrossRef]
21. Zhu, G.; Li, Z.; Wu, N. Model-based fault identification of discrete event systems using partially observed Petri nets. *Automatica* **2018**, *96*, 201–212. [CrossRef]
22. Ushio, T.; Onishi, I.; Okuda, K. Fault detection based on Petri net models with faulty behaviors. In Proceedings of the IEEE International Conference on Systems, Man, and Cybernetics, San Diego, CA, USA, 14 October 1998; pp. 113–118.
23. Cabasino, M.P.; Giua, A.; Lafortune, S.; Seatzu, C. Diagnosability analysis of unbounded Petri nets. In Proceedings of the 48th IEEE Conference on Decision and Control Held Jointly with 28th Chinese Control Conference, Shanghai, China, 15–18 December 2009; pp.1267–1272.
24. Finkel, A. *The Minimal Coverability Graph for Petri Nets*; Springer: Berlin/Heidelberg, Germany, 1991; pp. 210–243.
25. Valmari, A.; Hansen, H. Old and new algorithms for minimal coverability sets. *Fundam. Inform.* **2014**, *131*, 1–25. [CrossRef]
26. Wang, S.; Zhou, M.; Li, Z.; Wang, C. A new modified reachability tree approach and its applications to unbounded Petri nets. *IEEE Trans. Syst. Man Cybern. Syst.* **2013**, *43*, 932–940. [CrossRef]
27. Lefaucheux, E.; Giua, A.; Seatzu, C. Basis coverability graph for partially observable Petri nets with application to diagnosability analysis. In Proceedings of the International Conference on Applications and Theory of Petri Nets and Concurrency, Bratislava, Slovakia, 24–29 June 2018; pp. 164–183.
28. Tong, Y.; Ma, Z.; Li, Z.; Seactzu, C.; Giua, A. Verification of language-based opacity in Petri nets using verifier. In Proceedings of the American Control Conference, Boston, MA, USA, 6–8 July 2016; pp. 757–763.
29. Zhu, H.; Yin, L.; Wu, N.; Li, Z. Verification of current-state opacity for discrete event systems modeled with unbounded Petri nets. In Proceedings of the 8th International Conference on Control, Decision and Information Technologies, Istanbul, Turkey, 17–20 May 2022; pp. 1261–1266.
30. Bryans, J.W.; Koutny, M.; Ryan, P.Y. Modelling opacity using Petri nets. *Electron. Notes Theor. Comput. Sci.* **2005**, *121*, 101–115. [CrossRef]
31. Bryans, J.W.; Koutny, M.; Mazaré, L.; Ryan, P.Y. Opacity generalised to transition systems. *Int. J. Inf. Secur.* **2008**, *7*, 421–435. [CrossRef]
32. Zhu, H. Preliminaries of Petri Nets. Available online: https://github.com/Zhiwuli/Zhiwu-must/blob/master/Preliminaries%20of%20Petri%20nets.pdf (accessed on 18 January 2023).
33. Cabasino, M.P.; Giua, A.; Seatzu, C. Fault detection for discrete event systems using Petri nets with unobservable transitions. *Automatica* **2010**, *46*, 1531–1539. [CrossRef]
34. Lu, F.; Zeng, Q.; Zhou, M.; Bao, Y.; Duan, H. Complex reachability trees and their application to deadlock detection for unbounded Petri nets. *IEEE Trans. Syst. Man Cybern. Syst.* **2019**, *49*, 1164–1174. [CrossRef]
35. Shu, S.; Lin, F.; Ying, H. Detectability of discrete event systems. *IEEE Trans. Autom. Control* **2007**, *52*, 2356–2359. [CrossRef]
36. Lan, H.; Tong, Y.; Guo, J.; Seatzu, C. Verification of C-detectability using Petri nets. *Inf. Sci.* **2020**, *528*, 294–310. [CrossRef]
37. Saboori, A.; Hadjicostis, C.N. Opacity-enforcing supervisory strategies via state estimator constructions. *IEEE Trans. Autom. Control* **2012**, *57*, 1155–1165. [CrossRef]
38. Cabasino, M.P.; Giua, A.; Lafortune, S.; Seatzu, C. A new approach for diagnosability analysis of Petri nets using verifier nets. *IEEE Trans. Autom. Control* **2012**, *57*, 3104–3117. [CrossRef]
39. Tian, Z.; Jiang, X.; Liu, W.; Li, Z. Dynamic energy-efficient scheduling of multi-variety and small batch flexible job-shop: A case study for the aerospace industry. *Comput. Ind. Eng.* **2023**, *178*, 109111. [CrossRef]