Additional contents of the paper

State-based Opacity Verification of Networked Discrete Event Systems Using Labeled Petri Nets
(Paper ID: JAS-2023-0480)

1 Variable List

N	A Petri net, $N = (P, T, Pre, Post)$
P	The set of places of a Petri net
T	The set of transitions of a Petri net
$\mathbb{N}$	The set of non-negative integers
Pre	The pre-incidence function of a Petri net
$Post$	The post-incidence function of a Petri net
C	The incidence matrix of a Petri net
$\bar{C}$	The converse incidence matrix of a Petri net
M	A marking of a Petri net
$\langle N, M_0\rangle$	A Petri net system
σ	A sequence of transitions
$R(N, M_0)$	The reachability set of a Petri net system $\langle N, M_0\rangle$
G	A labeled Petri net, $G = (N, M_0, \Sigma, l)$
Σ	An alphabet
l	A labeling function assigning to each transition with a symbol or the empty word ε
T_o	The set of observable transitions
T_u	The set of unobservable transitions
$\mathcal{L}(N, M)$	The language generated from M of a labeled Petri net
w	An observation
$\mathcal{C}(w)$	The set of markings consistent with w
$\hat{T}$	A subset of T
$\mathcal{N}$	A next-state function
$\mathcal{N}^R$	A conversely next-state function
$\mathcal{M}$	A set of markings
F	A multi-valued decision diagram, $F = (Q, D, q_0, q_t, q_f, \delta_t)$
H	A matrix diagram, $H = (Q, \mathcal{D}, q_0, q_t, q_f, \delta_t)$
$\mathcal{K}(F)$	The set of the label sequences of all top-bottom paths ending with the true terminal vertex in F
$\mathcal{K}(H)$	The set of the label sequences of all top-bottom paths ending with the true terminal vertex in H
$F_1 \cup F_2$	Union of two MDDs F_1 and F_2
$F_1 \cap F_2$	Intersection of two MDDs F_1 and F_2
$F \otimes H$	Relational product of an MDD F and a matrix diagram H
$pr(\sigma)$	The prefix of σ
$su(\sigma)$	The suffix of σ
$pr(w)$	The prefix of w
$su(w)$	The suffix of w

κ_L	The mapping representing communication losses
κ_D	The mapping representing communication delays
κ_{DL}	The mapping representing both communication losses and delays
X	A delay upper bound
$\mathcal{C}_L(w)$	The current-state estimation with respect to w and κ_L
$\mathcal{C}_D(w)$	The current-state estimation with respect to w and κ_D
$\mathcal{C}_{DL}(w)$	The current-state estimation with respect to w and κ_{DL}
$\mathcal{I}_L(w)$	The initial-state estimation with respect to w and κ_L
$\mathcal{I}_D(w)$	The initial-state estimation with respect to w and κ_D
$\mathcal{I}_{DL}(w)$	The initial-state estimation with respect to w and κ_{DL}
$\mathcal{D}_L(w_1\|w_2)$	The delayed state estimation with respect to w and κ_L
$\mathcal{D}_D(w_1\|w_2)$	The delayed state estimation with respect to w and κ_D
$\mathcal{D}_{DL}(w_1\|w_2)$	The delayed state estimation with respect to w and κ_{DL}
$\mathcal{G} = (Q_o, \Sigma, \delta_o, q_{o0})$	The observer of G under the consideration of the mapping κ_{DL}
$\mathcal{U}(\mathcal{M}_r)$	Unobservable reach of a set of markings $\mathcal{M}_r$
$\bar{\mathcal{N}}_\varepsilon$	The matrix diagram decided by all unobservable transitions
$\mathcal{G}_L = (Q_o^L, \Sigma, \delta_o^L, q_{o0}^L)$	The observer $\mathcal{G}$ under the consideration of the mapping κ_L
$\mathcal{R}(\mathcal{M}, \alpha)$	The reversed α-reach of $\mathcal{M}$
$\mathcal{R}(\mathcal{M})$	The reversed unobservable reach of $\mathcal{M}$
$\mathcal{J} = (Q_e, \Sigma, \delta_e, q_{e0})$	The estimator of G under the consideration of the mapping κ_{DL}
$\bar{\mathcal{N}}$	The matrix diagram that is decided by all transitions in T
$\bar{\mathcal{N}}_t^R$	The matrix diagram decided by transition t under the reversed transition relation
$\mathcal{T} = (Q_{tw}, D_{tw}, \delta_{tw}, q_{tw0})$	A modified two-way observer of G
$\lambda_1(\tau_i) \in \Sigma^*$	The first components of τ_i
$\lambda_2(\tau_i) \in \Sigma^*$	The second components of τ_i
$d_{ij}[2]$	The second entry of the label d_{ij}
$\lambda_2^R(\tau_i)$	The reversed sequence of $\lambda_2(\tau_i)$
$\mathcal{IO} = (\mathcal{T}, V_{io})$	The I-observer of G with respect to $\mathcal{T}$, κ_{DL}, and S
$\mathcal{G}_{\mathcal{M}} = (Q_o', \Sigma, \delta_o', \hat{\mathcal{M}})$	An observer initialized at a set of markings $\mathcal{M}$
$\mathcal{X}^X(\mathcal{D}_L(w_1\|w_2), w_2)$	The set of $\mathcal{D}_L(w_1\|w_2)$-reachable markings with respect to X
$\mathcal{X}_{w_2}(\mathcal{D}_L(w_1\|w_2), w_2)$	The set of markings that can be reached from $\mathcal{D}_L(w_1\|w_2)$ after firing transition sequences σ with $w_2 \in \kappa_L(\sigma)$
$\mathcal{Y}(\mathcal{G}_{\mathcal{M}}, L)$	The set of vertices that is generated from $\hat{\mathcal{M}}$ within L steps
$\mathcal{Y}_U(\mathcal{G}_{\mathcal{M}}, L)$	The union of all vertices contained in $\mathcal{Y}(\mathcal{G}_{\mathcal{M}}, L)$
$h[i]$	The i-th entry of the tuple h

2 Main Algorithms

In this section, three critical algorithms as well as their explanations and computational complexity analysis are presented. Particularly, Algorithms 1, 2, and 3 are designed for the construction of an observer $\mathcal{G}$, an estimator $\mathcal{J}$, and an I-observer $\mathcal{T}$ that are utilized for the verification of current-state opacity, initial-state opacity, and infinite-step (or K-step) opacity of an LPN system G, respectively.

Algorithm 1: Construction of a symbolic observer $\mathcal{G}$

Input: An LPN $G = (N, M_0, \Sigma, l)$ with $N = (P, T, Pre, Post)$ and a mapping κ_{DL} associated with a delay upper bound $X \in \mathbb{N}$.

Output: Observer $\mathcal{G} = (Q_o, \Sigma, \delta_o, q_{o0})$ of G.

Initialize $G' = (P, T', Pre', Post')$ with $T' \leftarrow T$, $Pre' \leftarrow Pre$, $Post' \leftarrow Post$;
for all $t \in T_l$ **do**
  $T' \leftarrow T' \cup \{t'\}$ with $l(t') = \varepsilon$ defined;
  for all $p \in P$ **do**
    $Pre'(p, t') \leftarrow Pre(p, t)$;
    $Post'(p, t') \leftarrow Post(p, t)$;
$\hat{\mathcal{M}}_r \leftarrow \{\hat{M}_0\}$;
repeat
  $\hat{\mathcal{M}}_{temp} \leftarrow \hat{\mathcal{M}}_r$;
  $R \leftarrow$ Relational-product($\hat{\mathcal{M}}_{temp}, \bar{\mathcal{N}}_\varepsilon$);
  $\hat{\mathcal{M}}_r \leftarrow$ Union($\hat{\mathcal{M}}_{temp}, R$);
until $\hat{\mathcal{M}}_{temp} = \hat{\mathcal{M}}_r$;
$q_{o0} \leftarrow \hat{\mathcal{M}}_r$; $Q_o \leftarrow \{q_{o0}\}$;
Assign the vertex q_{o0} with a "new" tag;
while *vertices with a tag "new" exist* **do**
  Select a vertex q_o tagged with "new";
  for all $\alpha \in \Sigma$ **do**
    $\hat{\mathcal{M}}_\alpha \leftarrow$ Relational-product($q_o, \bar{\mathcal{N}}_\alpha$);
    repeat
      $\hat{\mathcal{M}}_{temp} \leftarrow \hat{\mathcal{M}}_\alpha$;
      $R \leftarrow$ Relational-product($\hat{\mathcal{M}}_{temp}, \bar{\mathcal{N}}_\varepsilon$);
      $\hat{\mathcal{M}}_\alpha \leftarrow$ Union($\hat{\mathcal{M}}_{temp}, R$);
    until $\hat{\mathcal{M}}_{temp} = \hat{\mathcal{M}}_\alpha$;
    $q'_o \leftarrow \hat{\mathcal{M}}_\alpha$;
    if $q'_o \notin Q_o$ *and* $\mathcal{M}_\alpha \neq \emptyset$ **then**
      $Q_o \leftarrow Q_o \cup \{q'_o\}$;
      $\delta_o(q_o, \alpha) = q'_o$ is defined;
      Assign "new" tag to q'_o;
  Tag q_o "old";
for all $q_o \in Q_o$ **do**
  for all *paths* $\tau_o = \alpha_1\alpha_2 \cdots \alpha_r$ *(*$|\tau_o| = X$*) s.t.* $\delta_o(q_{oi}, \alpha_i) = q_{o(i+1)}$ *(*$i = 1, 2, \ldots, r$ *and* $q_{o1} = q_o$*)* **do**
    $q_o \leftarrow \bigcup_{i=1,2,\ldots,r+1} q_{oi} \cup q_o$;

Algorithm 1: At the beginning of Algorithm 1, we initialize the LPN G' with G. Then, for all potentially lost transitions $t \in T_l$, we add a new unobservable transition t', i.e., $l(t') = \varepsilon$ to T', with ${}^\bullet t' = {}^\bullet t$ and $t'^\bullet = t^\bullet$. Then, the LPN G' is obtained. We then compute the observer of G' by a symbolic approach. The initial marking M_0 is represented by an MDD and assigned to $\hat{\mathcal{M}_r}$[1]. The codes in lines 8–12 compute the unobservable reach of $\mathcal{M}_r$, i.e., $\mathcal{U}(\mathcal{M}_r) = \bigcup_{M\in\mathcal{M}_r}\{M' \in \mathbb{N}^m \mid (\exists\sigma_u \in T_u^*)\ M[\sigma_u\rangle M'\}$ (the notation $\bar{\mathcal{N}_\varepsilon}$ in line 10 denotes the matrix diagram decided by all unobservable transitions). We assign $\hat{\mathcal{M}_r}$ to the initial vertex q_{o0} and $\{q_{o0}\}$ to Q_o. For any vertex that is not visited and for any label contained in Σ, we calculate the α-reach of q_o, i.e., $\mathcal{M}_\alpha = \mathcal{N}(\check{q}_o, \hat{T}_\alpha)$[2], where $\hat{T}_\alpha$ represents the set of transitions labeled by α and then compute the unobservable reach of $\hat{\mathcal{M}_\alpha}$ that is assigned to q_o' with the codes in lines 19–24. If q_o' is not included in Q_o and the set of markings $\mathcal{M}_\alpha$ with $\hat{\mathcal{M}_\alpha} = q_o'$ is not empty, q_o' is added to Q_o and $\delta_o(q_o,\alpha) = q_o'$ is defined. The set of vertices Q_o is iteratively computed until all vertices are tagged with "old".

For all vertices $q_o \in Q_o$ and for all label sequences $\tau_o = \alpha_1\alpha_2\cdots\alpha_r$ with $|\tau_o| = r = X$[3] such that $\delta_o(q_{o1},\alpha_1) = q_{o2}$, $\delta_o(q_{o2},\alpha_2) = q_{o3}, \ldots, \delta_o(q_{or},\alpha_r) = q_{o(r+1)}$ starting at q_o ($q_o = q_{o1}$), we add the union of the sets of markings $q_{o1} \cup q_{o2} \cup \cdots \cup q_{o(r+1)}$ to q_o.

Note that in lines 1–29 of Algorithm 1, we compute a part of the observer $\mathcal{G}$ under the consideration of the mapping κ_L, i.e., only communication losses are considered, which is denoted as $\mathcal{G}_L = (Q_o^L, \Sigma, \delta_o^L, q_{o0}^L)$. The codes in lines 30–32 consider communication delays for the construction of $\mathcal{G}$.

The computational complexity of Algorithm 1 can be divided into two parts, i.e., the computation of $\mathcal{G}_L$ and $\mathcal{G}$. For the former, its complexity is mainly derived from the alternative computation of the unobservable reach of a set of markings in lines 8–12 and 19–23, i.e., $\mathcal{O}(N_r \times (\sum_{i=1}^{m} |Q_i'|_{max} \times |Q_i''|_{max}))$, where N_r represents the number of loops until the arrival of a fixed point, i.e., the terminal condition, while $|Q_i'|_{max}$ and $|Q_i''|_{max}$ with $i = 1, 2, \ldots, m$ (m is the number of places) represent the maximum numbers of vertices at level i for all the operations associated with two symbolic structures (MDDs or matrix diagrams). The complexity for constructing $\mathcal{G}_L$ is $\mathcal{O}(|Q_o| \times |\Sigma| \times N_{max} \times (\sum_{i=1}^{m} |Q_i'|_{max} \times |Q_i''|_{max}))$, where $|Q_o|$ is the number of vertices in $\mathcal{G}$, $|\Sigma|$ is the number of symbols in Σ, and N_{max} represents the maximum number of loops for all the computations of unobservable reach of a set of markings. After the construction of $\mathcal{G}_L$, the complexity for computing $\mathcal{G}$ is $\mathcal{O}(|Q_o| \times |\Sigma|^X \times (\sum_{i=1}^{m} |Q_i'|_{max} \times |Q_i''|_{max}))$.

Algorithm 2: The construction of Algorithm 2 for computing an estimator of an LPN G is based on on Theorem 2. We now show the details of Algorithm 2. In line 2 of Algorithm 2, we construct G' by adding unobservable transitions according to the potentially lost transitions. Then we assign the MDD that represents the initial marking M_0 to $\hat{\mathcal{M}_r}$ and symbolically compute the reachable markings of G' with $\mathcal{M}_r = R(N, M_0)$ in lines 4–8 (the notation $\bar{\mathcal{N}}$ represents the matrix diagram that is decided by all transitions in T). The MDD $\hat{\mathcal{M}_r}$ is assigned to the initial vertex q_{e0} with a "new" tag. For all transitions $t \in T$, we compute the markings generated from $R(N, M_0)$ after the firing of t, i.e., $\mathcal{M}_t = \mathcal{N}(R(N, M_0), \{t\})$ (note that $\bar{\mathcal{N}_t}$ in line 12 represents the matrix diagram decided by t).

Then we randomly select a vertex tagged with "new" and for all $\alpha \in \Sigma$, assign the empty set to $\mathcal{M}_\alpha$. For all the transitions $t \in T$ labeled by α, we obtain the intersection of $\mathcal{M}_t$ and $\check{q}_e$ to indicate that under the firing of transition t at some markings, the markings contained in $\mathcal{M}_t' = \mathcal{M}_t \cap \check{q}_e$ are generated. If $\mathcal{M}_t'$ is not empty, we compute a set of markings after the converse firing of transition t, i.e., $\mathcal{M}_t^r = \mathcal{N}^R(\mathcal{M}_t', \{t\})$ and extend $\hat{\mathcal{M}_\alpha}$ with $\hat{\mathcal{M}_t^r} \cup \hat{\mathcal{M}_\alpha}$ (the notation $\bar{\mathcal{N}_t^R}$ in line 20 represents the matrix diagram decided by transition t under the reversed transition relation).

[1]The symbol "ˆ" over a notation denoting a set of markings implies that the set is represented by an MDD.

[2]The symbol "ˇ" over a notation denoting an MDD is a set of markings represented by the MDD. Here, $\check{q}_o$ is a set of markings represented by the MDD q_o.

[3]With a slight abuse of notation, write $|\cdot|$, where "$\cdot$" denotes a sequence, to represent the length, i.e., the number of elements in a default sequence.

Algorithm 2: Construction of an estimator of an LPN

Input: An LPN $G = (N, M_0, \Sigma, l)$ with $N = (P, T, Pre, Post)$ and a mapping κ_{DL} associated with a delay upper bound $X \in \mathbb{N}$.

Output: Estimator $\mathcal{J} = (Q_e, \Sigma, \delta_e, q_{e0})$ of G.

1 Initialize $G' = (P, T', Pre', Post')$ with $T' \leftarrow T$, $Pre' \leftarrow Pre$, $Post' \leftarrow Post$;
2 Add unobservable transitions for the potentially lost transitions using the codes in lines 2–6 of Algorithm 1;
3 $\hat{\mathcal{M}}_r \leftarrow \{\hat{M}_0\}$;
4 **repeat**
5     $\hat{\mathcal{M}}_{temp} \leftarrow \hat{\mathcal{M}}_r$;
6     $R \leftarrow$ Relational-product$(\hat{\mathcal{M}}_{temp}, \bar{\mathcal{N}})$;
7     $\hat{\mathcal{M}}_r \leftarrow$ Union$(\hat{\mathcal{M}}_{temp}, R)$;
8 **until** $\hat{\mathcal{M}}_{temp} = \hat{\mathcal{M}}_r$;
9 $q_{e0} \leftarrow \hat{\mathcal{M}}_r$; $Q_e \leftarrow \{q_{e0}\}$;
10 Assign the vertex q_{e0} with a "new" tag;
11 **for all** $t \in T$ **do**
12     $\hat{\mathcal{M}}_t \leftarrow$ Relational-product$(q_{e0}, \bar{\mathcal{N}}_t)$;
13 **while** *vertices with a tag "new" exist* **do**
14   Select a vertex q_e tagged with "new";
15   **for all** $\alpha \in \Sigma$ **do**
16         $\mathcal{M}_\alpha \leftarrow \emptyset$;
17   **for all** $t \in T$ *with* $l(t) = \alpha$ **do**
18             $\hat{\mathcal{M}}'_t \leftarrow$ Intersection$(\hat{\mathcal{M}}_t, q_e)$;
19   **if** $\mathcal{M}'_t \neq \emptyset$ **then**
20                 $\hat{\mathcal{M}}^r_t \leftarrow$ Relational-product$(\hat{\mathcal{M}}'_t, \bar{\mathcal{N}}^R_t)$;
21                 $\hat{\mathcal{M}}_\alpha \leftarrow$ Union$(\hat{\mathcal{M}}_\alpha, \hat{\mathcal{M}}^r_t)$;
22         $\hat{\mathcal{M}}_\varepsilon \leftarrow \hat{\mathcal{M}}_\alpha$;
23   **repeat**
24             $\hat{\mathcal{M}}_{temp} \leftarrow \hat{\mathcal{M}}_\varepsilon$;
25   **for all** $t \in T$ *with* $l(t) = \varepsilon$ **do**
26                 $R_1 \leftarrow$ Intersection$(\hat{\mathcal{M}}_{temp}, \hat{\mathcal{M}}_t)$;
27                 $R_2 \leftarrow$ Relational-product$(R_1, \bar{\mathcal{N}}^R_t)$;
28                 $\hat{\mathcal{M}}_\varepsilon \leftarrow$ Union$(\hat{\mathcal{M}}_\varepsilon, R_2)$;
29   **until** $\hat{\mathcal{M}}_\varepsilon = \hat{\mathcal{M}}_{temp}$;
30         $q'_e \leftarrow \hat{\mathcal{M}}_\varepsilon$;
31   **if** $q'_e \notin Q_e$ *and* $\mathcal{M}_\varepsilon \neq \emptyset$ **then**
32             $Q_e \leftarrow Q_e \cup \{q'_e\}$;
33             $\delta_e(q_e, \alpha) = q'_e$ is defined;
34   Assign "new" tag to q'_e;
35   Tag q_e "old";

In lines 23–29, we iteratively compute the set of markings that can reach a marking in $\mathcal{M}_\alpha$ after firing unobservable transitions. In particular, in an *until* loop and for all unobservable transitions $t \in T_u$, we compute the possible markings that can generate a marking in $\mathcal{M}_\varepsilon$ after firing unobservable transitions. The *until* loop reaches to a fixed point when $\hat{\mathcal{M}}_\varepsilon = \hat{\mathcal{M}}_{temp}$, and we assign $\hat{\mathcal{M}}_\varepsilon$ to q'_e. If $\check{q}'_e \neq \emptyset$ and q'_e is not contained in Q_e, q'_e is assigned to Q_e and $\delta_e(q_e, \alpha) = q'_e$ is defined.

The most burdensome part of Algorithm 2 is the computation of the reversed unobservable reach of a set of markings in lines 23–29, which has the complexity of $\mathcal{O}(N_r \times |T_u| \times (\sum_{i=1}^{m} |Q'_i|_{max} \times |Q''_i|_{max}))$, where N_r represents the number of loops until the arrival of a fixed point, and $|T_u|$ is the number of unobservable transitions. The complexity for constructing $\mathcal{J}$ is $\mathcal{O}(|Q_e| \times |\Sigma| \times N_{max} \times |T_u| \times (\sum_{i=1}^{m} |Q'_i|_{max} \times |Q''_i|_{max}))$.

Algorithm 3: As for the calculation of Algorithm 3, we initially assign the empty set to V_{io} to initialize $\mathcal{IO}$ (note that the two-way observer $\mathcal{T} = (Q_{tw}, D_{tw}, \delta_{tw}, q_{tw0})$ can be obtained directly by Definition 7). For all the vertices (q_o^L, q_e) contained in Q_{tw} such that $\check{q}_o^L \cap \check{q}_e \neq \emptyset$ and $\check{q}_o^L \cap \check{q}_e \subseteq S$, i.e., the intersection of two MDDs q_o^L and q_e is an MDD that represents a non-empty set contained in the secret S, and for all paths $\tau_i = (\varepsilon, \alpha_1)(\varepsilon, \alpha_2) \cdots (\varepsilon, \alpha_m) \in D_{tw}^*$ starting at (q_o^L, q_{e1}) and ending at (q_o^L, q_e) such that $\delta_{tw}((q_o^L, q_{e1}), (\varepsilon, \alpha_1)) = (q_o^L, q_{e2})$, $\delta_{tw}((q_o^L, q_{e2}), (\varepsilon, \alpha_2)) = (q_o^L, q_{e3})$,. . ., $\delta_{tw}((q_o^L, q_{em}), (\varepsilon, \alpha_m)) = (q_o^L, q_{e(m+1)})$ with $(q_o^L, q_{e(m+1)}) = (q_o^L, q_e)$, we have two cases:

1) If $|\tau_i| = X$, we reversely traverse τ_i from m to 1 by computing the set of markings reached from the markings in $\check{q}_o^L \cap \check{q}_e$ by firing the transitions labeled by α_j interleaved with all possible unobservable transitions. Then the tuple $h = (\tau_i, (q_o^L, q_{e1}), 1, \check{\mathcal{Z}})$ is assigned to H, where $h[3] = 1$ indicates that the length of τ_i equals X;

2) If $|\tau_i| < X$ and $q_{e1} = q_{e0}$, i.e., the path τ_i starts at the vertex (q_o^L, q_{e0}), we reversely traverse τ_i and update $\mathcal{Y}$ and $\mathcal{Z}$ by $\mathcal{Y} \cap q_{ej}$ and $\mathcal{Z} \cup \mathcal{Y}$, respectively. Then, we compute the observer $\mathcal{G}_\mathcal{Y} = (Q'_o, \Sigma, \delta'_o, \mathcal{Y})$ by Algorithm 1. For all paths $\tau_o = \beta_1 \cdots \beta_n$ in $\mathcal{G}_\mathcal{Y}$ such that $\delta'_o(\mathcal{Y}, \tau_o) = q'_o$ and $n \leq X - |\tau_i|$, we update $\mathcal{Z}$ with $\mathcal{Z} \cup q'_o$. Then $h = (\tau_i, (q_o^L, q_{e0}), 0, \check{\mathcal{Z}})$ is assigned to H, where $h[3] = 0$ indicates that the length of τ_i is less than X.

At the end of Algorithm 3, after the calculation of H, we assign $((q_o^L, q_e), H)$ to the set V_{io}. For the complexity of Algorithm 3, the maximum number of paths τ_i is $|Q_{tw}| \times |\Sigma|^X$ by assuming that all vertices $q_{tw} = (q_o^L, q_e) \in Q_{tw}$ satisfy $\check{q}_o^L \cap \check{q}_e \neq \emptyset$ and $\check{q}_o^L \cap \check{q}_e \subseteq S$. If $|\tau_i| = X$, the complexity for computing h with $h[1] = \tau_i$ is $\mathcal{O}(X \times N_{max} \times (\sum_{i=1}^{m} |Q'_i|_{max} \times |Q''_i|_{max}))$. If $|\tau_i| < X$, the computational complexity for h is $\mathcal{O}_1(\mathcal{MDD} \times |\tau_i|) + \mathcal{O}_2(\mathcal{MDD} \times |Q'_o| \times |\Sigma|^X) + \mathcal{O}_3(|\Sigma|^n \times \mathcal{MDD})$, where $\mathcal{MDD} = N_{max} \times (\sum_{i=1}^{m} |Q'_i|_{max} \times |Q''_i|_{max})$ represents the operations associated with MDDs and matrix diagrams.

3 Supplementary Contents for Case Study

This section presents some additional contents for the case study, i.e., Section VII of the paper. Particularly, when considering the LPN $G = (N, M_0, \Sigma, l)$ with $N = (P, T, Pre, Post)$ in Fig. 9, and its observer $\mathcal{G}_L = (Q_o^L, \Sigma, \delta_o^L, q_{o0}^L)$ and estimator $\mathcal{J} = (Q_e, \Sigma, \delta_e, q_{e0})$ shown in Figs. 10 and 11, respectively (Figs. 9, 10, and 11 are shown in the paper), the symbolic two-way observer of G obtained by Definition 7 is illustrated in Fig. 1 of the supplementary file. Note that due to the limited space, we write (i, j) in Fig. 1 to represent the vertex (q_{oi}^L, q_{ej}), where $q_{oi}^L \in Q_o^L$ and $q_{ej} \in Q_e$ $(i = 0, 1, \ldots, 6$ and $j = 0, 1, \ldots, 9)$. Table 1 details the reachable markings of the Petri net portrayed in Fig. 9.

Algorithm 3: Construction of an I-observer of an LPN

Input: A two-way observer $\mathcal{T} = (Q_{tw}, D_{tw}, \delta_{tw}, q_{tw0})$ of G, a mapping κ_{DL} associated with a delay upper bound $X \in \mathbb{N}$, and a secret S.

Output: I-observer $\mathcal{IO} = (\mathcal{T}, V_{io})$.

Initialize $\mathcal{IO} = (\mathcal{T}, V_{io})$ with $V_{io} \leftarrow \emptyset$;

for all $(q_o^L, q_e) \in Q_{tw}$ *s.t.* $\check{q}_o^L \cap \check{q}_e \neq \emptyset$ *and* $\check{q}_o^L \cap \check{q}_e \subseteq S$ **do**

  $H \leftarrow \emptyset$;

  for all *paths* $\tau_i = (\varepsilon, \alpha_1)(\varepsilon, \alpha_2) \cdots (\varepsilon, \alpha_m) \in D_{tw}^*$ *s.t.* $\delta_{tw}((q_o^L, q_{e1}), (\varepsilon, \alpha_1)) = (q_o^L, q_{e2})$, $\delta_{tw}((q_o^L, q_{e2}), (\varepsilon, \alpha_2)) = (q_o^L, q_{e3}), \ldots,$ $\delta_{tw}((q_o^L, q_{em}), (\varepsilon, \alpha_m)) = (q_o^L, q_{e(m+1)})$ $((q_o^L, q_{e(m+1)}) = (q_o^L, q_e))$ **do**

    $\mathcal{Y} \leftarrow q_o^L \cap q_e$; $\mathcal{Z} \leftarrow q_o^L \cap q_e$;

    if $|\tau_i| = X$ **then**

      for $j = m$ to 1 **do**

        Update $\mathcal{Y}$ with its unobservable reach using the codes in lines 8–12 of Algorithm 1;

        Update $\mathcal{Y}$ with its α_j-reach and unobservable reach using the codes in lines 17–23 of Algorithm 1;

        $\mathcal{Y} \leftarrow \mathcal{Y} \cap q_{ej}$;

        $\mathcal{Z} \leftarrow \mathcal{Z} \cup \mathcal{Y}$;

      $H \leftarrow H \cup (\tau_i, (q_o^L, q_{e1}), 1, \check{\mathcal{Z}})$;

    else if $|\tau_i| < X$ *and* $q_{e1} = q_{e0}$ **then**

      for $j = m$ to 1 **do**

        Update $\mathcal{Y}$ with its unobservable reach using the codes in lines 8–12 of Algorithm 1;

        Update $\mathcal{Y}$ with its α_j-reach and unobservable reach using the codes in lines 17–23 of Algorithm 1;

        $\mathcal{Y} \leftarrow \mathcal{Y} \cap q_{ej}$;

        $\mathcal{Z} \leftarrow \mathcal{Z} \cup \mathcal{Y}$;

      Compute the observer $\mathcal{G}_{\mathcal{Y}} = (Q_o', \Sigma, \delta_o', \mathcal{Y})$ by Algorithm 1 by replacing $\{\hat{M}_0\}$ with $\mathcal{Y}$ in its line 7;

      for all $\tau_o = \beta_1 \cdots \beta_n \in \Sigma^*$ *s.t.* $\delta_o'(\mathcal{Y}, \tau_o) = q_o'$ *and* $n \leq X - |\tau_i|$ **do**

        $\mathcal{Z} \leftarrow \mathcal{Z} \cup q_o'$;

      $H \leftarrow H \cup (\tau_i, (q_o^L, q_{e0}), 0, \check{\mathcal{Z}})$;

  $V_{io} \leftarrow V_{io} \cup \{((q_o^L, q_e), H)\}$;

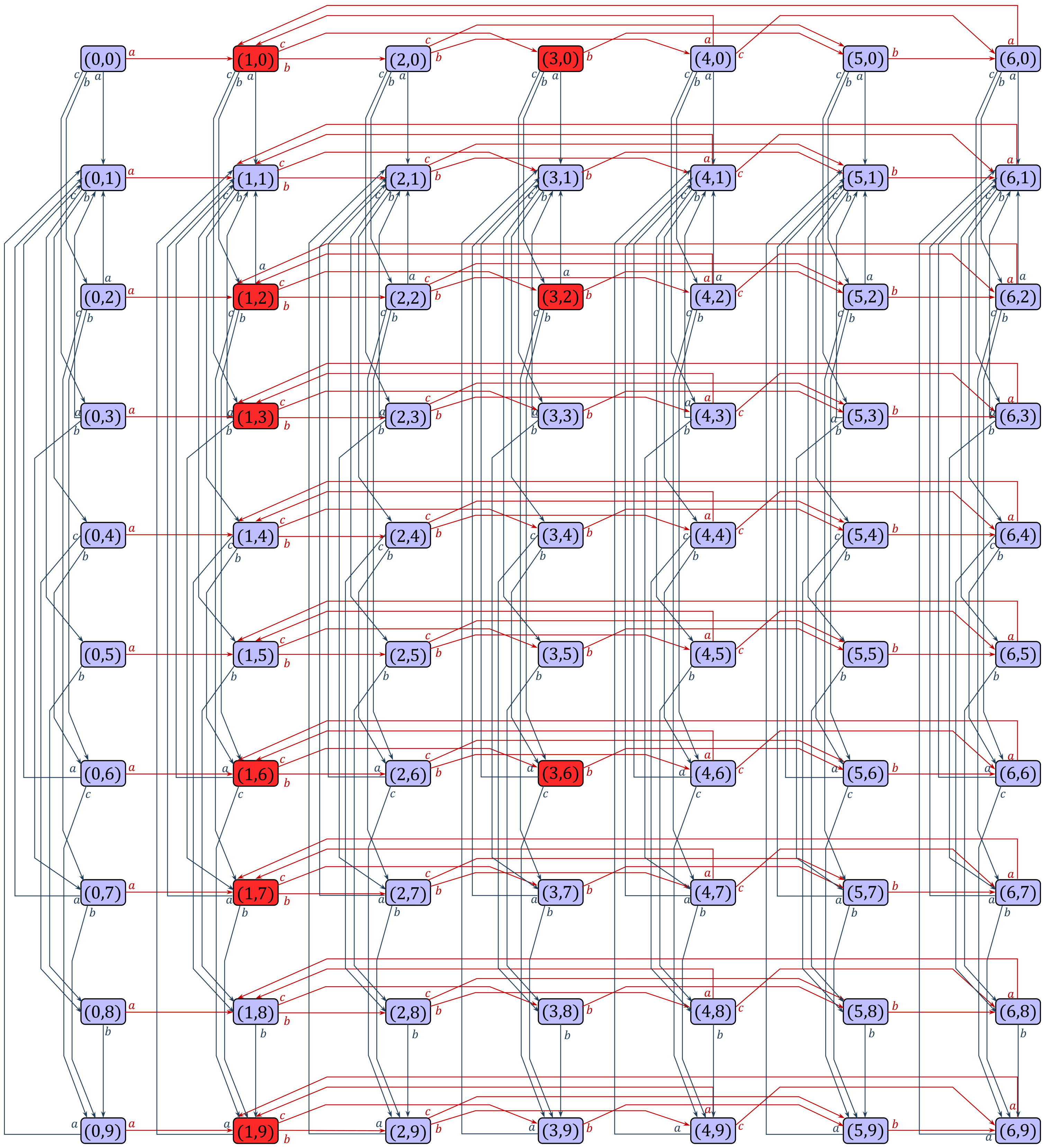

Figure 1: Symbolic two-way observer $\mathcal{T}$ of G shown in Fig. 9 of the paper.

Table 1: Reachable markings of the Petri net illustrated in Fig. 9 with the initial marking $M_0 = 3p_1$

Markings	Token locations	Markings	Token locations	Markings	Token locations
M_0	$3p_1$	M_{42}	$p_6 + p_8 + p_{10}$	M_{83}	$p_1 + p_5 + p_6$
M_1	$p_2 + p_6 + p_9$	M_{43}	$p_1 + p_4 + p_9$	M_{84}	$p_6 + p_8 + p_{12}$
M_2	$p_3 + p_6 + p_9$	M_{44}	$p_4 + p_8 + p_{10}$	M_{85}	$p_1 + p_4 + p_{11}$
M_3	$p_2 + p_7 + p_9$	M_{45}	$p_4 + p_7 + p_{11}$	M_{86}	$p_4 + p_8 + p_{12}$
M_4	$p_2 + p_6 + p_{10}$	M_{46}	$p_4 + p_6 + p_{12}$	M_{87}	$p_1 + p_4 + p_7$
M_5	$p_4 + p_6 + p_9$	M_{47}	$p_1 + p_3 + p_{10}$	M_{88}	$p_1 + p_3 + p_{12}$
M_6	$p_3 + p_7 + p_9$	M_{48}	$p_3 + p_8 + p_{11}$	M_{89}	$p_1 + p_3 + p_8$
M_7	$p_3 + p_6 + p_{10}$	M_{49}	$p_3 + p_7 + p_{12}$	M_{90}	$2p_1 + p_2$
M_8	$p_2 + p_8 + p_9$	M_{50}	$p_1 + p_3 + p_6$	M_{91}	$2p_1 + p_{10}$
M_9	$p_2 + p_7 + p_{10}$	M_{51}	$p_1 + p_2 + p_{11}$	M_{92}	$p_1 + p_8 + p_{11}$
M_{10}	$p_2 + p_6 + p_{11}$	M_{52}	$p_2 + p_8 + p_{12}$	M_{93}	$p_1 + p_7 + p_{12}$
M_{11}	$p_5 + p_6 + p_9$	M_{53}	$p_1 + p_2 + p_7$	M_{94}	$2p_1 + p_6$
M_{12}	$p_4 + p_7 + p_9$	M_{54}	$p_1 + p_8 + p_9$	M_{95}	$p_1 + p_5 + p_{11}$
M_{13}	$p_4 + p_6 + p_{10}$	M_{55}	$p_1 + p_7 + p_{10}$	M_{96}	$p_5 + p_8 + p_{12}$
M_{14}	$p_3 + p_8 + p_9$	M_{56}	$p_1 + p_6 + p_{11}$	M_{97}	$2p_8 + p_{11}$
M_{15}	$p_3 + p_7 + p_{10}$	M_{57}	$p_1 + p_5 + p_9$	M_{98}	$p_{10} + 2p_{12}$
M_{16}	$p_3 + p_6 + p_{11}$	M_{58}	$p_5 + p_8 + p_{10}$	M_{99}	$p_1 + p_9 + p_{12}$
M_{17}	$p_1 + p_2 + p_9$	M_{59}	$2p_8 + p_9$	M_{100}	$p_1 + p_5 + p_7$
M_{18}	$p_2 + p_8 + p_{10}$	M_{60}	$p_5 + p_7 + p_{11}$	M_{101}	$p_7 + p_8 + p_{12}$
M_{19}	$p_2 + p_7 + p_{11}$	M_{61}	$p_7 + p_8 + p_{10}$	M_{102}	$p_1 + p_6 + p_8$
M_{20}	$p_2 + p_6 + p_{12}$	M_{62}	$p_5 + p_6 + p_{12}$	M_{103}	$p_1 + p_4 + p_{12}$
M_{21}	$p_1 + p_6 + p_9$	M_{63}	$p_6 + p_8 + p_{11}$	M_{104}	$p_1 + p_4 + p_8$
M_{22}	$p_1 + p_7 + p_9$	M_{64}	$p_1 + p_4 + p_{10}$	M_{105}	$2p_1 + p_3$
M_{23}	$p_5 + p_6 + p_{10}$	M_{65}	$p_4 + p_8 + p_{11}$	M_{106}	$2p_1 + p_{11}$
M_{24}	$p_6 + p_8 + p_9$	M_{66}	$p_4 + p_7 + p_{12}$	M_{107}	$p_1 + p_8 + p_{12}$
M_{25}	$p_4 + p_8 + p_9$	M_{67}	$p_1 + p_4 + p_6$	M_{108}	$2p_1 + p_7$
M_{26}	$p_4 + p_7 + p_{10}$	M_{68}	$p_1 + p_3 + p_{11}$	M_{109}	$p_1 + p_5 + p_{12}$
M_{27}	$p_4 + p_6 + p_{11}$	M_{69}	$p_3 + p_8 + p_{12}$	M_{110}	$p_1 + p_5 + p_8$
M_{28}	$p_1 + p_3 + p_9$	M_{70}	$p_1 + p_3 + p_7$	M_{111}	$2p_8 + p_{12}$
M_{29}	$p_3 + p_8 + p_{10}$	M_{71}	$p_1 + p_2 + p_{12}$	M_{112}	$p_{11} + 2p_{12}$
M_{30}	$p_3 + p_7 + p_{11}$	M_{72}	$p_1 + p_2 + p_8$	M_{113}	$p_1 + p_{10} + p_{12}$
M_{31}	$p_3 + p_6 + p_{12}$	M_{73}	$2p_1 + p_9$	M_{114}	$p_1 + p_7 + p_8$
M_{32}	$p_1 + p_2 + p_{10}$	M_{74}	$p_1 + p_8 + p_{10}$	M_{115}	$2p_1 + p_4$
M_{33}	$p_2 + p_8 + p_{11}$	M_{75}	$p_1 + p_7 + p_{11}$	M_{116}	$2p_1 + p_{12}$
M_{34}	$p_2 + p_7 + p_{12}$	M_{76}	$p_1 + p_6 + p_{12}$	M_{117}	$2p_1 + p_8$
M_{35}	$p_1 + p_2 + p_6$	M_{77}	$p_1 + p_5 + p_{10}$	M_{118}	$2p_1 + p_5$
M_{36}	$p_1 + p_7 + p_9$	M_{78}	$p_5 + p_8 + p_{11}$	M_{119}	$p_1 + 2p_8$
M_{37}	$p_1 + p_6 + p_{10}$	M_{79}	$2p_8 + p_{10}$	M_{120}	$3p_{12}$
M_{38}	$p_5 + p_8 + p_9$	M_{80}	$p_9 + 2p_{12}$	M_{121}	$p_1 + p_{11} + p_{12}$
M_{39}	$p_5 + p_7 + p_{10}$	M_{81}	$p_5 + p_7 + p_{12}$	M_{122}	$p_1 + 2p_{12}$
M_{40}	$p_7 + p_8 + p_9$	M_{82}	$p_7 + p_8 + p_{11}$	M_{123}	$3p_{13}$
M_{41}	$p_5 + p_6 + p_{11}$				