# Supplementary material to the paper "$K$-step and Definite Critical Observability in Networked Discrete Event Systems Under Replacement Attacks via Labeled Petri Nets"

Xuya Cong, Zhenhua Yu, Maria Pia Fanti, Agostino Marcello Mangini, and Zhiwu Li

## I. Main Algorithms

In this section, three algorithms as well as their explanations are presented.

**Algorithm 1:** Algorithm 1 is used to compute $R(M, k)$ for given $M$ and $k$, which is the set of basis markings in an RABRG reachable from marking $M$ through $k$ events in $E$. Note that if $k = 0$, we have $R(M, k) = UR(M)$.

---

**Algorithm 1** Computation of $R(M, k)$ in an RABRG

---

**Input:** An RABRG $\mathcal{B}_A = (\mathcal{M}_B, Tr, \delta_A, M_0)$, a basis marking $M$, and an integer $k \in \mathbb{N} \setminus \{0\}$

**Output:** $R(M, k)$

$S_n := \{(M, 0)\}$ and $R(M, k) := \emptyset$;<br>
**while** $S_n \neq \emptyset$ **do**<br>
 pop a pair $(M', i) \in S_n$;<br>
 **for** all $(t, \vec{y}_\sigma) \in \Gamma_A(M')$ **do**<br>
  **if** $\lambda((t, \vec{y}_\sigma)) \in E$ **then**<br>
   $i := i + 1$ and $y := \{(\hat{M}', i) | \hat{M}' \in \delta_A(M', (t, \vec{y}_\sigma))\}$;<br>
  **else if** $\lambda((t, \vec{y}_\sigma)) = \varepsilon$ **then**<br>
   $y := \{(\hat{M}', i) | \hat{M}' \in \delta_A(M', (t, \vec{y}_\sigma))\}$;<br>
  **end if**<br>
  **if** $i < k$ **then**<br>
   **for** all $(\hat{M}', i) \in y$ **do**<br>
    $S_n := S_n \cup \{(\hat{M}', i)\}$;<br>
   **end for**<br>
  **else if** $i = k$ **then**<br>
   $R(M, k) := R(M, k) \cup UR(\delta_A(M', (t, \vec{y}_\sigma)))$;<br>
  **end if**<br>
 **end for**<br>
**end while**

---

**Algorithm 2:** Algorithm 2 is used to compute a set of fully-critical basis markings $\mathcal{F}$, a set of partially critical basis markings $\mathcal{P}$, and a set of non-critical basis markings $\mathcal{N}$, which directly follows from Definition 10 and Proposition 4.

**Algorithm 2** Computing the sets $\mathcal{F}$, $\mathcal{P}$, and $\mathcal{N}$

**Input:** The set of basis markings $\mathcal{M}_B$ of an RABRG and a set of critical markings $C_R$

**Output:** Sets $\mathcal{F}$, $\mathcal{P}$, and $\mathcal{N}$

$\mathcal{F} := \emptyset$, $\mathcal{P} := \emptyset$, and $\mathcal{N} := \emptyset$;
$\hat{\mathcal{M}}_B := \mathcal{M}_B$;
**while** $\hat{\mathcal{M}}_B \neq \emptyset$ **do**
    select a basis marking $M \in \hat{\mathcal{M}}_B$;
    $\hat{\mathcal{M}}_B := \hat{\mathcal{M}}_B \setminus \{M\}$;
    **if** the set of constraints (1) is feasible **then**
        assign $M$ with tag "1";
    **else if** the set of constraints (1) is infeasible **then**
        assign $M$ with tag "2";
    **end if**
    **if** the set of constraints (2) is feasible **then**
        assign $M$ with tag "3";
    **else if** the set of constraints (2) in is infeasible **then**
        assign $M$ with tag "4";
    **end if**
**end while**
**while** $\mathcal{M}_B \neq \emptyset$ **do**
    select a basis marking $M \in \mathcal{M}_B$;
    $\mathcal{M}_B := \mathcal{M}_B \setminus \{M\}$;
    **if** ($M$ is with tag "1" and "3") $\vee$ ($M$ is with tag "2" $\wedge$ there exists $\phi \in (Tr'_u)^*$ such that $M' \in \delta_A(M, \phi)$ and $M'$ is with tag "1") $\vee$ ($M$ is with tag "4" $\wedge$ there exists $\phi \in (Tr'_u)^*$ such that $M' \in \delta_A(M, \phi)$ **then** and $M'$ is with tag "3")
        $\mathcal{P} := \mathcal{P} \cup \{M\}$;
    **else if** ($M$ is with tag "2" $\wedge$ for all $\phi \in (Tr'_u)^*$ such that $M' \in \delta_A(M, \phi)$ and $M'$ is with tag "2") **then**
        $\mathcal{F} := \mathcal{F} \cup \{M\}$;
    **else if** ($M$ is with tag "4"$\wedge$ for all $\phi \in (Tr'_u)^*$ such that $M' \in \delta_A(M, \phi)$ and $M'$ is with tag "4") **then**
        $\mathcal{N} := \mathcal{N} \cup \{M\}$;
    **end if**
**end while**

**Algorithm 3** Computing maximal $k$ for $k$-CO w.r.t. a replacement attack, a communication delay, and a critical marking set

**Input:** A bounded LPN $G = (PN, M_0, E, \lambda)$ w.r.t. a labeling function $A_D$ associated with a replacement attack $\mathcal{A}$ and a delay upper bound $N \in \mathbb{N}$, and a set of critical markings $C_R$

**Output:** A maximal $k$ such that $G$ is $k$-CO w.r.t. $A_D$ and $C_R$, or "NA"

Compute the robust basis $n$-extended networked detector $\hat{\mathcal{B}}_{d,n}$, where $n = |\mathcal{M}_B|^2 - 1$;
find all the negative cycles in the corresponding underlying digraph $\mathcal{B}$ of $\hat{\mathcal{B}}_{d,n}$;
**if** there exists no negative cycle on any path from $z'$ to $z$ for all the states $z' \in Z_0$ and $z \in Z_v$ **then**
  output "def-CO" and exit;
**end if**
$i := 1$ and $j := |\mathcal{M}_B|^2 - 1$;
**while** $i <= j$ **do**
  $k := \lfloor \frac{1}{2}(i+j) \rfloor$, where $\lfloor \frac{1}{2}(i+j) \rfloor$ represents the largest integer not greater than $\frac{1}{2}(i+j)$;
  compute the robust basis $k$-extended networked detector $\hat{\mathcal{B}}_{d,k}$, find all the negative cycles in the corresponding underlying digraph $\mathcal{B}$ of $\hat{\mathcal{B}}_{d,k}$;
  **if** there exists a negative cycle on a path from $z'$ to $z$ for a state $z' \in Z_0$ and a state $z \in Z_v$ **then**
    $j := k - 1$ and $flag := 1$;
  **else**
    $i := k + 1$ and $flag := 2$;
  **end if**
**end while**
**if** $flag = 1$ **then**
  **if** $k \neq 1$ **then**
    output $k-1$; "$(k-1)$-CO" and exit;
  **else**
    output "NA" and exit;
  **end if**
**else**
  output $k$, "$k$-CO" and exit;
**end if**

**Algorithm 3:** Algorithm 3 is used to compute a maximal $k$ for $k$-CO w.r.t. a labeling function $A_D$ associated with a replacement attack $\mathcal{A}$ and a delay upper bound $N \in \mathbb{N}$, and a set of critical markings $C_R$ (if it exists). Now we briefly explain how Algorithm 3 works. First, steps 1 to 5 check def-CO by constructing the robust basis $(|\mathcal{M}_B|^2 - 1)$-extended networked detector and checking whether there exists no negative cycle on any path from $z'$ to $z$ for all the states $z' \in Z_0$ and $z \in Z_v$. If the LPN is not def-CO w.r.t. $A_D$ and $C_R$, then steps 6 to 24 compute a maximal $k$ for $k$-CO by using the binary search. In particular, step 6 initializes the lower and upper bounds of the search interval as $i = 1$ and $j = |\mathcal{M}_B|^2 - 1$, respectively. Step 8 computes the midpoint of the interval $[i, j]$ as $k$; step 9 determines whether the LPN $G$ is $k$-CO w.r.t. $A_D$ and $C_R$. If $G$ is not $k$-CO w.r.t. $A_D$ and $C_R$, by Proposition 2, it cannot be $k'$-CO for any $k' > k$. Thus, step 11 sets the upper bound as $j = k - 1$. If $G$ is $k$-CO, then step 13 sets the lower bound as $i = k + 1$. Steps 7 to 15 execute iteratively until the lower bound is greater than the upper bound. Finally, if $G$ is verified to be not $k$-CO in the final iteration, step 18 outputs $k - 1$ as the maximal value if $k \neq 1$, and step 19 outputs "NA" if $k = 1$. If $G$ is verified to be $k$-CO in the final iteration, step 23 outputs $k$ as the maximal value.

## II. Proofs for the Main Results

*Proposition 1:* If an LPN $G$ is $(k, l)$-CO w.r.t. a labeling function $A_D$ associated with a replacement attack $\mathcal{A}$ and a delay upper bound $N \in \mathbb{N}$, and a set of critical markings $C_R$, then $G$ is $(k, l')$-CO w.r.t. $A_D$ and $C_R$ for any $l' \geq l$.

**Proof:** Since $G$ is $(k, l)$-CO w.r.t. $A_D$ and $C_R$, for all $s' = uvw' \in A_D(L_G(k, l')) \subseteq A_D(L_G(k, l))$ with $|v| = k$ and $|w'| \geq l'$, Condition (1) or (2) holds. Thus, $G$ is also $(k, l')$-CO w.r.t. $A_D$ and $C_R$. □

*Proposition 2:* If an LPN $G$ is $k$-CO w.r.t. a labeling function $A_D$ associated with a replacement attack $\mathcal{A}$ and a delay upper bound $N \in \mathbb{N}$, and a set of critical markings $C_R$, then $G$ is $k'$-CO for any $k' \leq k$ w.r.t. $A_D$ and $C_R$.

**Proof:** Suppose that $G$ is $(k, l)$-CO w.r.t. $A_D$ and $C_R$, i.e., for any $s = uvw \in A_D(L(G))$ with $|v| = k$ and $|w| \geq l$, Condition (1) or (2) in Definition 1 holds. Let $k' \in \mathbb{N}$ be an integer less than or equal to $k$. Due to $A_D(L_G(k, l)) = A_D(L_G(k', l + (k - k')))$, Condition (1) or (2) holds for any $s = uvw = uv'w'$ with $|v'| = k'$ and $|w'| \geq l + (k - k')$. □

*Proposition 3:* Given an LPN $G$ under a replacement attack $\mathcal{A}$, let $\mathcal{B}_A = (\mathcal{M}_B, Tr, \delta_A, M_0)$ be the RABRG w.r.t. $\pi = (T_E, T_I)$ with $T_E \supseteq T_o$. The following two statements are equivalent:

1) there is a path in the RABRG $\mathcal{B}_A$:

$$M_0 \xrightarrow{(t_1,\vec{y}_{\sigma_1})} M_1 \xrightarrow{(t_2,\vec{y}_{\sigma_2})} \cdots \xrightarrow{(t_n,\vec{y}_{\sigma n})} M_n;$$

2) there exists a marking $M$ and a firing sequence $\sigma = \sigma_1 t'_1 \cdots \sigma_n t'_n \sigma_{n+1}$ , where $\sigma_i \in T_I^*$ for all $i \in \{1, \ldots, n+1\}$, and $t'_i \in T_E$ for all $i \in \{1, \ldots, n\}$ such that $M_0[\sigma\rangle M$, $M \in R_I(M_n)$, $\lambda(t'_1) \in A(\lambda(t_1))$, …, and $\lambda(t'_n) \in A(\lambda(t_n))$.

**Proof:** This result follows from Theorem 1 in [1] by considering the transition function assignment in Definition 6. □

*Theorem 1:* Given an LPN $G = (PN, M_0, E, \lambda)$, a set of critical markings $C_R$, a labeling function $A_D$ associated with a replacement attack $\mathcal{A}$ and a delay upper bound $N \in \mathbb{N}$, and two nonnegative integers $k, l \in \mathbb{N}$, $G$ is $(k, l)$-CO w.r.t. $A_D$ and $C_R$ if and only if for all $z \in D_l(\hat{\mathcal{B}}_{d,k})$, $z \in Z_s$ holds.

**Proof:** (If) By contrapositive, suppose that $G$ is not $(k, l)$-CO w.r.t. $A_D$ and $C_R$. There exist two event sequences $s = uvw \in A_D(L(G))$ and $s' = uv'w \in A_D(L(G))$ such that $\widehat{\mathcal{C}}_D(s) \cap C_R \neq \emptyset$ and $\widehat{\mathcal{C}}_D(s') \cap R(PN, M_0) \setminus C_R \neq \emptyset$ with $|v| = |v'| = k$, and $|w| \geq l$. Then, we have two sequences $\sigma_1\sigma_2$ and $\sigma'_1\sigma'_2$ such that $M_0[\sigma_1\rangle M_1[\sigma_2\rangle M_2 \in C_R$, $M_0[\sigma'_1\rangle M'_1[\sigma'_2\rangle M'_2 \notin C_R$ with $uv \in A(\lambda(\sigma_1))$, $uv' \in A(\lambda(\sigma'_1))$, $w \in A_D(\lambda(\sigma_2)) \cap A_D(\lambda(\sigma'_2))$. Since all confusable pairs of basis markings in $\mathcal{B}_A$ are in $R(\Omega(\mathcal{B}_A), k)$ as soon as the communication loss stage completes, there exists a state $(\hat{M}_1, \hat{M}'_1)$ in $R(\Omega(\mathcal{B}_A, k))$ such that $M_1 \in R_I(\hat{M}_1)$ and $M'_1 \in R_I(\hat{M}'_1)$ based on Proposition 3. Moreover, by the construction of a robust basis $k$-extended networked detector, there exists a path $z \xrightarrow{\phi} z'$ such that $(\hat{M}_1, \hat{M}'_1) \in z$, $(\hat{M}_2, \hat{M}'_2) \in z'$, $M_2 = R_I(\hat{M}_2)$ and $M'_2 = R_I(\hat{M}'_2)$ with $|\lambda(\phi)| \geq l$ and $w \in A_D(\lambda(\phi))$ based on Proposition 3. Thus, we have $z' \in Z_v$.

(Only if) By contrapositive, suppose that there exists a state $z \in D_l(\hat{\mathcal{B}}_{d,k})$ with $z \in Z_v$. Then, we have $(\hat{M}, \hat{M}') \in z'$, and one of the following two conditions holds: 1) $\hat{M} \in \mathcal{F}$ and $\hat{M}' \in \mathcal{N}$; 2) $\hat{M} \in \mathcal{P}$ based on Definition 11.

For the first case, there exists a path $z \xrightarrow{\phi} z'$ with $(\hat{M}_1, \hat{M}'_1) \in z$, $(\hat{M}, \hat{M}') \in z'$, and $(\hat{M}_1, \hat{M}'_1) \in R(\Omega(\mathcal{B}_A, k))$ such that $M \in R_u(\hat{M}) \cap C_R$ and $M' \in R_u(\hat{M}') \cap (R(PN, M_0) \setminus C_R)$ according to Definition 10 and the condition $T_I \subseteq T_u$. Based on Proposition 3 and the construction of a robust basis $k$-extended networked detector, we have $\hat{M}_1[\sigma\rangle M$ and $\hat{M}'_1[\sigma'\rangle M'$ such that $w \in A_D(\lambda(\sigma)) \cap A_D(\lambda(\sigma'))$ and $|w| \geq l$. Moreover, since $R(\Omega(\mathcal{B}_A), k)$ contains all confusable pairs in $\mathcal{B}_A$ as soon as the communication loss stage completes, there exist two event sequences

$s = uv$ and $s' = uv'$ such that $\hat{M}_1 \in \widehat{\mathcal{C}}(s)$ and $\hat{M}_1' \in \widehat{\mathcal{C}}(s')$. Based on Proposition 3, we have two sequences $\sigma_1$ and $\sigma_1'$ such that $uv \in A(\lambda(\sigma_1))$, $uv' \in A(\lambda(\sigma_1'))$, and $|v| = |v'| = k$. By Definition 1, $G$ is not $(k, l)$-CO w.r.t. $A_D$ and $C_R$.

For the second case, there exists a path $z \xrightarrow{\phi} z'$ with $(\hat{M}_1, \hat{M}_1') \in z$, $(\hat{M}, \hat{M}') \in z'$, and $(\hat{M}_1, \hat{M}_1') \in R(\Omega(\mathcal{B}_A, k))$ such that $M \in R_u(\hat{M}) \cap C_R$ and $M' \in R_u(\hat{M}) \cap (R(PN, M_0) \setminus C_R)$ according to Definition 10 and the condition $T_I \subseteq T_u$. Based on Proposition 3 and the construction of a robust basis $k$-extended networked detector, we have $\hat{M}_1[\sigma\rangle M$ and $\hat{M}_1[\sigma'\rangle M'$ such that $w \in A_D(\lambda(\sigma)) \cap A_D(\lambda(\sigma'))$ and $|w| \geq l$. Moreover, due to $(\hat{M}_1, \hat{M}_1') \in R(\Omega(\mathcal{B}_A, k))$, there exist two event sequences $s = uv$ and $s' = uv'$ such that $\hat{M}_1 \in \widehat{\mathcal{C}}(s) \cap \widehat{\mathcal{C}}(s')$. Based on Proposition 3, we have two sequences $\sigma_1$ and $\sigma_1'$ such that $uv \in A(\lambda(\sigma_1))$, $uv' \in A(\lambda(\sigma_1'))$, and $|v| = |v'| = k$. By Definition 1, $G$ is neither $(k, l)$-CO w.r.t. $A_D$ and $C_R$. $\square$

## III. Case of multiple communication losses

In this section, we present the procedure to apply the proposed method in [3] recursively to the case where there exists more than one communication loss stage. Given a sequence $s = uv_1w_1v_2w_2 \cdots v_nw_n \in A_D(L(G))$ in an LPN $G$ under a replacement attack and a communication delay, and the communication losses occur for all $v_i$ substrings for $n$ times, where $|v_i| = k_i$ and $|w_i| = l_i$ for $i = 1, 2, \cdots, n$. Now, the following steps are used to check critical observability in a general case.

1) No communication failure state N: compute the set $\Omega(\mathcal{B}_A)$ of all confusable basis marking pairs under $\mathcal{A}$.
2) Communication loss stage L1: compute the $k_1$-step reach $L_1 = R(\mathcal{B}_A, k_1)$.
3) Communication recover state R1: construct the robust basis $k_1$-extended detector $\mathcal{B}_{d,k_1}$ starting from the set of initial markings $L_1$, and then compute the $l_1$-step reach of $L_1$ in $\mathcal{B}_{d,k_1}$, denoted as $R_1 = R(L_1, l_1)$.
4) Communication loss stage L2: compute the $k_2$-step reach $L_2 = R(R_1, k_2)$.
5) Communication recover stage R2: construct the robust basis $k_2$-extended detector $\mathcal{B}_{d,k_2}$ starting from the set of initial markings $L_2$, and then compute the $l_2$-step reach of $L_2$ in $\mathcal{B}_{d,k_2}$, denoted as $R_2 = R(L_2, l_2)$.
6) ...
7) Communication loss stage Ln: compute the $k_n$-step reach $L_n = R(R_{n-1}, k_n)$.

8) Communication delay stage D: construct the robust basis $k_n$-extended networked detector $\hat{\mathcal{B}}_{d,k_n}$ starting from the set of initial markings $L_n$.

For brevity, after constructing the set $\Omega(\mathcal{B}_A)$, we iteratively compute the corresponding $k_i$-step reach for $n$ times, and the $l_i$-step reach in the corresponding robust basis extended detector for $n-1$ times, and check if the final robust basis extended networked detector $\hat{\mathcal{B}}_{d,k_n}$ satisfies the condition in Theorem 1.

*Example 1:* Let us consider the LPN in Fig. 1(a). Let $C_R = \{M_c^1 = [0\,0\,1\,0\,0\,0\,0\,0\,0\,1]^T\}$, $A_D$ be a labeling function associated with a replacement attack $\mathcal{A} = \{(b, c)\}$ and a delay upper bound $N = 1$. First, we construct the replacement attack basis reachability graph (RABRG) in Fig. 1(b). Assume that the communication loss occur twice and $k_1 = 1$, $k_2 = 2$, $l_1 = 1$, and $l_2 = 2$.

1) No communication failure state to Communication recover stage R1: According to the robust basis 1-extended detector $\mathcal{B}_{d,1} = Ac(X_d, Tr', \delta_d, X_{d,0})$ shown in Fig. 2, we obtain $R_1 = R(X_{d,0}, 1) = \{(M_2, M_2), (M_2, M_4), (M_4, M_2), (M_4, M_4), (M_3, M_3), (M_2, M_3), (M_3, M_2), (M_4, M_3), (M_3, M_4)\}$, i.e., after observing one observable event, the set of confusable basis marking pairs are collected in $R_1$.
2) Communication loss stage L2: compute $L_2 = R(R_1, 2) = R_1$, i.e., the set of confusable basis marking pairs are collected in $L_2$ after losing two observable events.
3) Communication delay state D: construct the robust basis 2-extended networked detector $\hat{\mathcal{B}}_{d,2}$ shown in Fig. 3. By Theorem 1, the plant is not critically observable due to the existence of a negative cycle from $z_0 \in Z_0$ to $z_3 \in Z_v$ in the underlying digraph $\mathcal{B}$ of $\hat{\mathcal{B}}_{d,2}$.

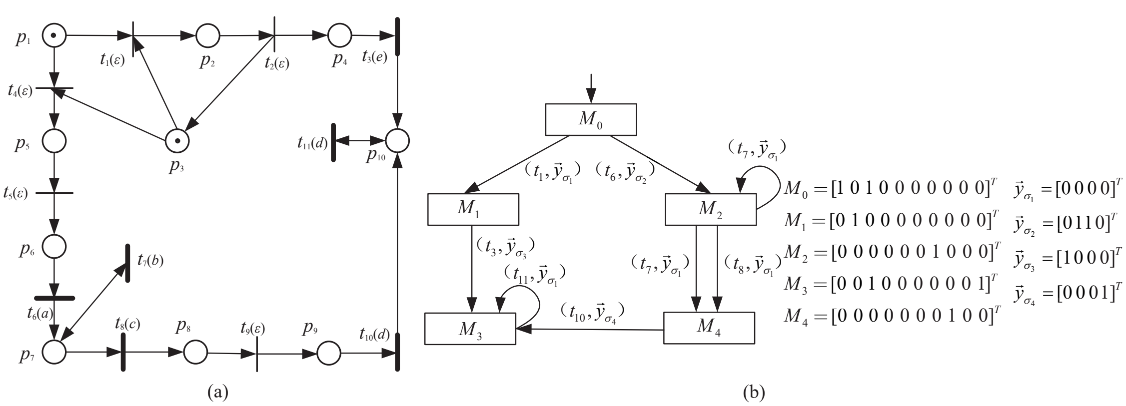


Fig. 1: (a) A bounded LPN under a replacement attack and (b) its RABRG.

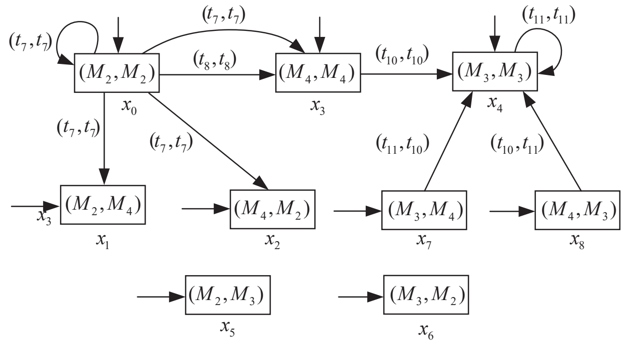


Fig. 2: The robust basis 1-extended detector.

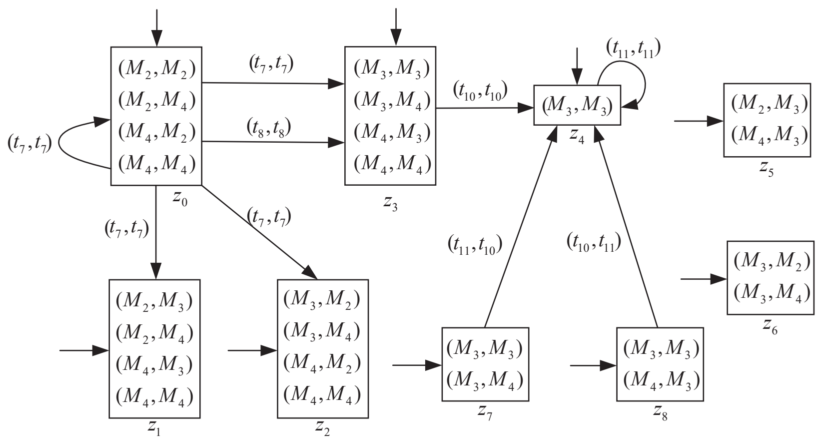


Fig. 3: The robust basis 2-extended networked detector.

Note that the operator of a plant net may not know the forthcoming disturbance a priori. That is to say, it does not know the exact communication loss times in practice. Thus, if the communication suffers from multiple communication losses, it is more realistic to consider def-CO. In particular, if an LPN is def-CO, then it is critically observable for all $n$, $k_1, \cdots, k_n$, and $l_1, \cdots, l_n$. In a word, the $k$-CO defined in [3] characterizes the robustness of a system against casual single-time communication loss, and the def-CO defined in [3] characterizes the robustness against multiple communication losses.

## IV. Case study

Some experimental results are provided in this section about the application of the proposed methodology for the $k$-CO verification in NDESs under replacement attacks. The results are obtained by a laptop under Windows 10 operating system with Intel CPU 2.3 GHz and 16 GB memory.

To this aim, we take into account two groups of LPNs with fixed numbers of places and transitions. For each group of the nets, we consider the same net structure with two different initial markings. In particular, the net systems presented in this section can model two different communication systems [4]. More precisely, each place of LPNs 1–4 can represent the replay station that implements the information transfer. Each marking $M(p_i) = 1$ ($M(p_i) = 0$) indicates the busy (free) status of each relay station. For the safety of the information transfer in the system, the situations of some important information shared by some particular stations are regarded as the critical states in the system.

The net structure of the first group of LPNs is shown in Fig. 4, which has 19 places and 11 transitions (five observable transitions and six unobservable transitions). There are four labels in this net structure. Assuming that the set of critical markings for LPNs 1 and 2 is $C_R = \{M \in \mathbb{N}^{19} | M(p_2) + M(p_4) + M(p_6) + M(p_{19}) \geq 1\}$. Let $k = 1$ and $A_D$ be a labeling function associated with a replacement attack $\mathcal{A} = \{(a, b)\}$ and a delay upper bound $N = 1$.

The net structure of the second group of LPNs is shown in Fig. 5, which has 23 places and 23 transitions (four observable transitions and 19 unobservable transitions). There are four labels in this net structure. Assuming the set of critical markings for LPNs 3 and 4 is $C_R = \{M \in \mathbb{N}^{23} | M(p_5) + M(p_6) \geq 1\}$. Let $k = 1$ and $A_D$ be a labeling function associated with a replacement attack $\mathcal{A} = \{(a, b)\}$ and a delay upper bound $N = 1$.

Table I shows the performance of the proposed method applied to LPNs 1–4: column two represents the number of tokens in $p_1$ for LPNs 1–4, columns three and four represent the number of basis markings and that of arcs in the RABRGs that associate with LPNs 1–4, respectively. Column five and six represent the number of markings and that of arcs in the reachability graphs of LPNs 1–4 under replacement attacks by using the PN analysis software TINA [5], and the last column shows whether the LPN is $k$-CO w.r.t. $A_D$ and $C_R$. From the experimental results shown in Table I, we can see that the proposed method is more efficient than the one generating the full state space.

## References


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

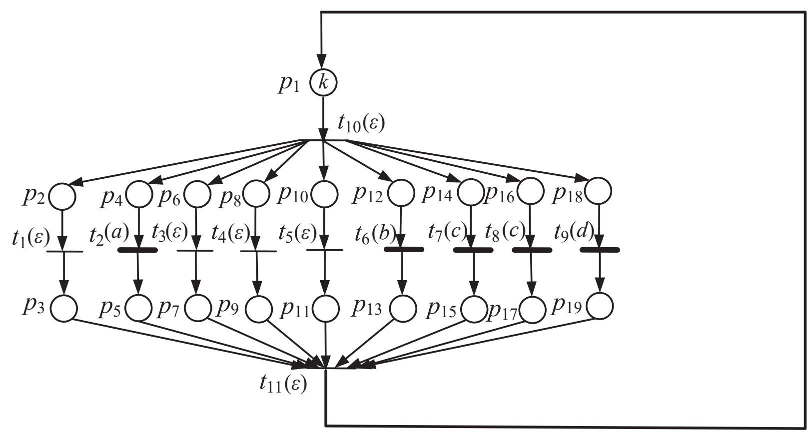


Fig. 4: Net structure of LPNs 1 and 2.

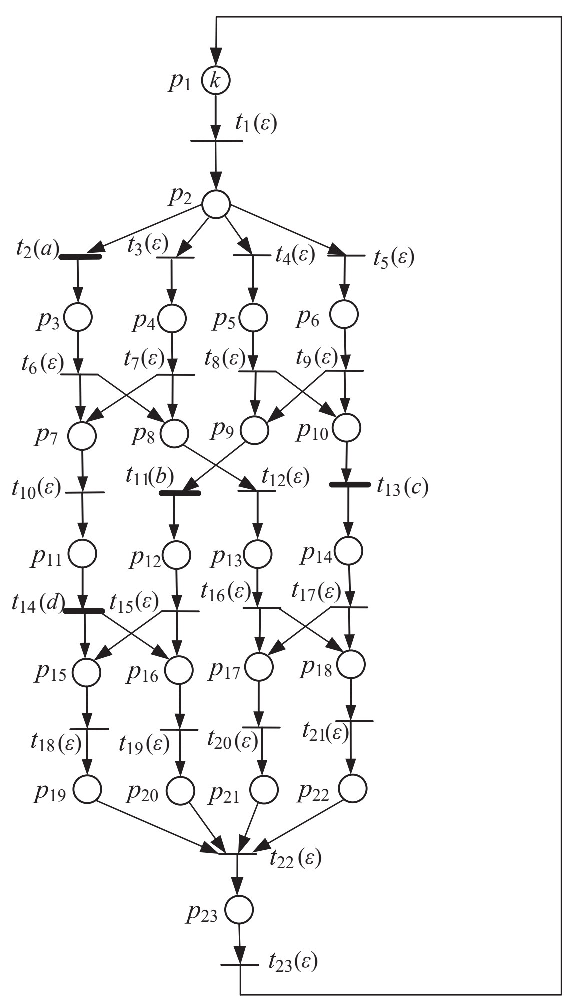


Fig. 5: Net structure of LPNs 3 and 4.

TABLE I: Experimental results for the LPNs 1–4

| | $k$ | $\|\mathcal{M}_B\|$ | $\|\delta_A\|$ | $\|R_A(PN, M_0)\|$ | $\|\bar{\delta}_A\|$ | $K$-CO |
|---|---|---|---|---|---|---|
| LPN1 | 1 | 33 | 90 | 513 | 2562 | Yes |
| LPN2 | 2 | 276 | 1071 | 20196 | 134806 | Yes |
| LPN3 | 1 | 7 | 14 | 63 | 129 | Yes |
| LPN4 | 2 | 55 | 185 | 1683 | 6159 | Yes |


[2] Cong, X., Fanti, M. P., Mangini, A. M., & Li, Z. (2023). Critical observability verification and enforcement of labeled Petri nets by using basis markings. *IEEE Transactions on Automatic Control*, 68(12), 8158–8164.

[3] Cong, X., Yu, Z., Fanti, M. P., Mangini, A. M., & Li, Z. (2025). $K$-step and definite critical observability in networked discrete event systems under replacement attacks via labeled Petri nets, submitted to *Automatica*.

[4] Cong, X., Fanti, M. P., Mangini, A. M. & Li, Z. (2022). Critical observability of discrete-event systems in a Petri net framework. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 52(5), 2789–2799.

[5] TINA (Version 3.8.0): Time Petri Net Analyzer 2024. [Online]. Available: http://projects.laas.fr/tina//download.php