Benchmarks of the CFCE Basis Reachability Graph

Chao Gu, Ziyue Ma, and Zhiwu Li

September 29, 2023

Abstract

In this note, we present a comparative analysis between the CFCE basis reachability graph (CFCE-BRG) and the standard reachability graph (RG). This study adopts four parameterized Petri net benchmarks taken from [1–4], in addition to three modified versions inherited from models in [1, 2, 4]. The algorithms employed are implemented using MATLAB[1] (R2017a version), and the experiments are carried out on a laptop equipped with an Intel i7-5500U 2.40 GHz processor and 8 GB of RAM.

Benchmark I

1.1 The original model

The hospital emergency service system [4] illustrates the entire medical service process, from the arrival of a patient to his/her departure after treatment in the emergency department (TED). This process includes encounters with either a medical doctor (MD) or a registered nurse (RN). Specifically, once a patient has been seen by an MD or RN, the subsequent phases of care can be delineated as follows:

- Prescription for an X-ray or CT scan.
- Waiting for and performing the X-ray or CT scan.
- Patient movement facilitated by an MD, RN or transport staff.
- Waiting for and receiving medical consultation.
- Completing treatment and leaving the hospital.

A schematic of the system is shown in Fig. 1. According to the scheme, the hospital emergency service system is represented by a parameterized marked net $\langle N, M_0 \rangle$ in Fig. 2. Physically, the place p_1 represents the number of patients queuing to visit the TED. The Petri net N consists of 22 places and 22 transitions. Detailed descriptions of these places and transitions can be found in Table 1. As indicated in Fig. 2, the initial marking of the marked net is parameterized as

$$M_0 = [\alpha\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 7\ 9\ 4\ 2\ 2]^T.$$

This initial marking implies that there are 7 medical doctors, 9 registered nurses, 4 available transport staff, 2 accessible CT scanners and 2 operational X-ray scanners. It is worth noting that the only parameter α indicates the number of patients within the patient community who intend to enter the TED, based on the information provided in Table 1.

Let $T_c = \{t_4, t_5, t_6, t_7, t_8, t_{12}, t_{15}\}$ (boxed in red). Further, through the structure of the Petri net we can conclude $T_{conf} = \{t_4, t_5, t_6, t_7, t_8, t_9, t_{14}, t_{15}, t_{16}\}$ holds (marked in shadow). To satisfy the acyclicity of

[1]The source code can be requested by contacting the authors through email (guchao@xidian.edu.cn).

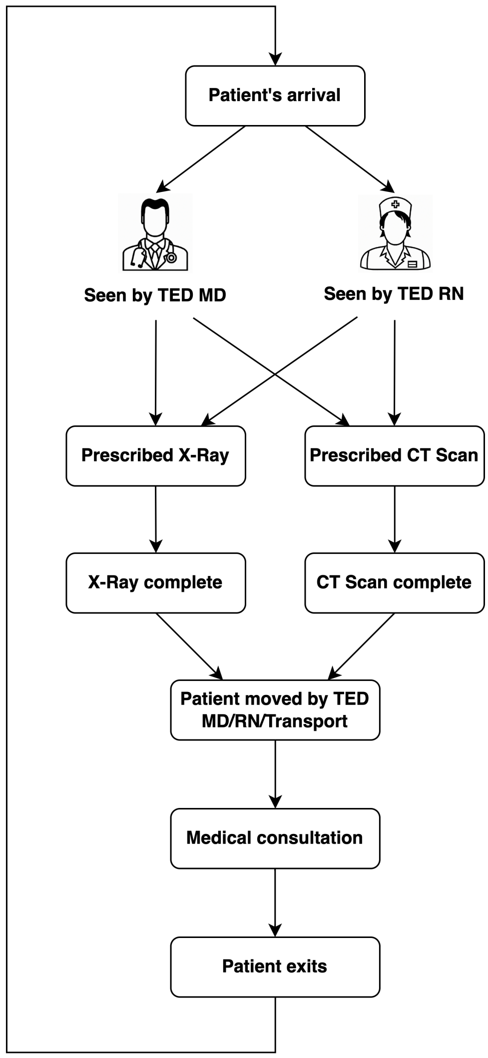

Figure 1: The schematic of the hospital emergency service system.

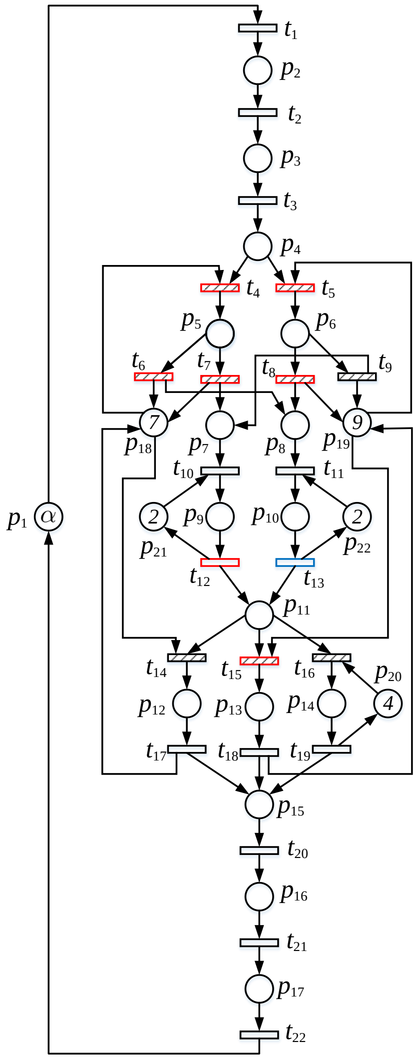

Figure 2: The hospital emergency service system modeled by PN [4].

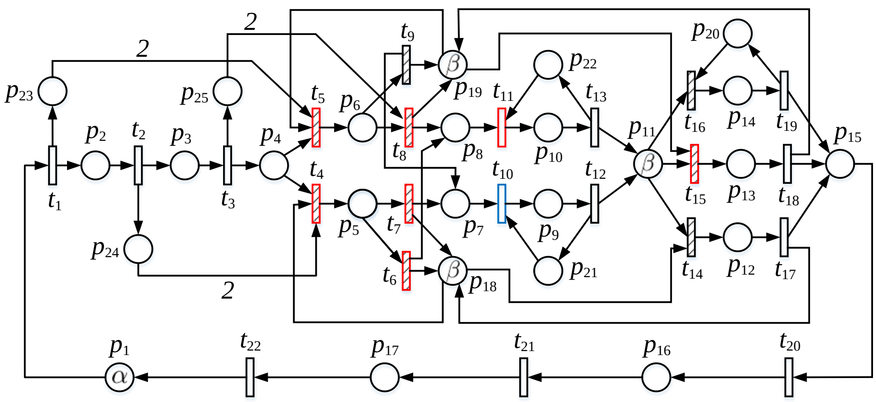

Figure 3: The modified version.

Table 1: Physical interpretations of places and transitions of the Petri net in Fig. 2 [4].

p_1	Patient community
p_2	Patient waiting to be admitted
p_3	Patient waiting to be assigned in the hospital
p_4	Patient waiting to be seen by TED staff
p_5	TED MD seeing patient
p_6	TED RN seeing patient
p_7	Patient waiting for CT Scan
p_8	Patient waiting for X-Ray
p_9	CT Scan being performed
p_{10}	X-Ray being taken
p_{11}	Patient waiting to be moved to medical floor
p_{12}	TED MD moves patient
p_{13}	TED RN moves patient
p_{14}	Transport moves patient
p_{15}	Patient waiting for medical consultation
p_{16}	Patient being consulted
p_{17}	Patient ready to exit the system
p_{18}	TED MD available
p_{19}	TED RN available
p_{20}	Transport available
p_{21}	CT Scanner available
p_{22}	X-Ray available

t_1	Patient enters TED
t_2	Patient admitted
t_3	Space assigned
t_4	Admitted to be seen by TED MD
t_5	Admitted to be seen by TED RN
t_6	Seen by TED MD & prescribed X-Ray
t_7	Seen by TED MD & prescribed CT Scan
t_8	Seen by TED RN & prescribed X-Ray
t_9	Seen by TED RN & prescribed CT Scan
t_{10}	CT Scan start
t_{11}	X-Ray start
t_{12}	CT Scan complete
t_{13}	X-Ray complete
t_{14}	Patient move start by TED MD
t_{15}	Patient move start by TED RN
t_{16}	Patient move start by transport
t_{17}	Patient move complete by TED MD
t_{18}	Patient move complete by TED RN
t_{19}	Patient move complete by transport
t_{20}	Medical consultation starts
t_{21}	Medical consultation complete
t_{22}	Patient exits

the T_I-induced sub-net, we additionally set transition t_{13} be an explicit transition (boxed in blue). As a result, we can obtain a basis partition $\pi = (T_E, T_I)$ where $T_E = T_c \cup T_{conf} \cup \{t_{13}\}$.

Consequently, the CFCE-BRG is able to be constructed. For different values of the parameter α, the number of basis markings $|\mathcal{M}_\mathcal{B}|$ and all reachable markings $|R(N, M_0)|$, as well as their computing times and corresponding ratios, are listed in Table 2. Through the test of this benchmark, we can see that RG cannot be computed within the time limit in runs 3−7 and cannot be obtained with a RAM of 8 GB in the rest of the cases. However, the CFCE-BRG can be computed and is much smaller than the corresponding RG size-wise.

Table 2: Analysis of the RG and CFCE-BRG for the Petri net in Fig. 2.

Run	α	$\lvert R(N, M_0)\rvert$	Time (s)	$\lvert\mathcal{M}_\mathcal{B}\rvert$	Time (s)	$\lvert\mathcal{M}_\mathcal{B}\rvert / \lvert R(N, M_0)\rvert$	Time ratio
1	5	20042	1038	1287	6	6.4%	0.6%
2	6	72659	16706	3003	31	4.1%	0.2%
3	7	235331	o.t.*	6435	136	2.7%	0.06%
4	8	693950	o.t.	14493	702	2.0%	-
5	9	1889762	o.t.	31917	3533	1.7%	-
6	10	4804971	o.t.	66942	16566	1.4%	-
7	11	11506970	o.t.	130876	o.t.	1.1%	-
8	12	-	o.m.**	239320	o.t.	-	-
9	13	-	o.m.	413374	o.t.	-	-

* o.t. represents *overtime*, i.e., the program does not terminate within 43200 seconds (12 hours).
** o.m. represents *out of memory*, i.e., no additional memory can be allocated for use by the program.

We now analyze the deadlock-freeness and liveness of the marked net in Fig. 2 at run 3 (where $|\mathcal{M}_\mathcal{B}| = 6435$); as a contrast, the RG cannot be computed in the given time. First, in the corresponding CFCE-BRG $\mathcal{B} = (\mathcal{M}_\mathcal{B}, \mathrm{Tr}, \Delta, M_0)$, there is no terminal basis marking; hence, the marked net is deadlock-free by Corollary 2 in the manuscript. Second, when viewing the CFCE-BRG $\mathcal{B}$ as a digraph, we can identify a unique *ergodic strongly connected component*[2] denoted as $\mathcal{G}' = (\mathcal{V}', \mathcal{E}')$ with a cardinality of $|\mathcal{V}'| = 3432$,

[2] A strongly connected component $\mathcal{G}'$ of a digraph $\mathcal{G}$ is said to be *ergodic* if there is no edge in $\mathcal{G}$ that goes from a vertex in $\mathcal{G}'$ to a vertex not in $\mathcal{G}'$.

containing vertices $M_{b,121}, M_{b,122}, M_{b,125}, M_{b,132}, \cdots, M_{b,6434}$. Furthermore, our analysis leads to the following conclusion in $\mathcal{G}'$:

$$[(\forall t \in T_E)\ \exists(t,\cdot) \in \mathcal{E}'] \wedge [\sum_{(\cdot,\mathbf{y})\in\mathcal{E}'} \mathbf{y} \geq \mathbf{1}^{|T_I|}].$$

The above expression indicates that every explicit transition in the set T_E and every implicit transition in the set T_I must occur at least once (on the labels of edges) within the ergodic component $\mathcal{G}'$. This observation confirms the liveness of the marked net during run 3, as proved by Corollary 4 in our manuscript.

1.2 The modified model

In the modified model, to enhance the waiting experience for patients at the hospital, we established three dedicated transit waiting rooms situated outside the hospital lobby. Patients are required to wait in these rooms before being admitted for consultation with a doctor, nurse, or X-Ray/CT prescriptions. A healthcare provider will attend to a patient only when there are at least two individuals in the waiting room. This modification aims to streamline the waiting process, ensuring efficient resource allocation. With this in mind, three additional places (i.e., p_{23}, p_{24}, and p_{25}) and six corresponding arcs ($t_1 \to p_{23}, p_{23} \xrightarrow{2} t_5, t_2 \to p_{24}, p_{24} \xrightarrow{2} t_4, t_3 \to p_{25}$, and $p_{25} \xrightarrow{2} t_8$) are attached compared with the Petri net in Fig. 2. The physical meaning of those three additionally added places in our revised version are introduced in Table 3 while the modified Petri net is shown in Fig. 3.

Table 3: Physical interpretations of additional places p_{23}, p_{24}, p_{25} of the Petri net in Fig. 3.

p_{23}	Patient staying in the TED RN waiting room
p_{24}	Patient staying in the TED MD waiting room
p_{25}	Patient staying in the medical prescription waiting room

In the revised model, we adopt an alternative parametrization that characterizes a specific scenario in which all transportation resources (p_{20}), CT scanners (p_{21}), and X-ray devices (p_{22}) are rendered unavailable due to unanticipated power outages. Concurrently, there exist β medical doctors and β registered nurses, with an additional population of β patients awaiting transfer to the medical floor for subsequent consultation services. As a result, in this modified version, the initial marking is parameterized as

$$M_0 = [\alpha\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ \beta\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ \beta\ \beta\ 0\ 0\ 0\ 0\ 0\ 0\ 0]^T.$$

The revised parameterization can serve as a reference for managing healthcare and planning for emergencies when faced with unexpected disruptions. Let $T_c = \{t_4, t_5, t_6, t_7, t_8, t_{11}, t_{15}\}$. From the structure of the Petri net in Fig. 3, we have $T_{conf} = \{t_4, t_5, t_6, t_7, t_8, t_9, t_{14}, t_{15}, t_{16}\}$ (marked in shadow). Also, let t_{10} (boxed in blue) be an explicit transition to guarantee the acyclicity of the T_I-induced subnet. We have a basis partition $\pi = (T_E, T_I)$ for building the CFCE-BRG where $T_E = T_{conf} \cup T_c \cup \{t_{10}\}$ and $T_I = T \setminus T_E$. For different values of parameters α and β, the number of basis markings $|\mathcal{M}_\mathcal{B}|$ and all reachable markings $|R(N, M_0)|$, as well as their computing times and corresponding ratios, are listed in Table 4. The results

Table 4: Analysis of the RG and CFCE-BRG for modified model in Fig. 3.

Run	α	β	$\|R(N, M_0)\|$	Time (s)	$\|\mathcal{M}_\mathcal{B}\|$	Time (s)	$\|\mathcal{M}_\mathcal{B}\|/\|R(N, M_0)\|$	Time ratio
1	5	3	157304	o.t.	4861	52	3.0%	<1.0%
2	6	4	1141871	o.t.	19042	834	1.6%	<1.0%
3	7	5	6325283	o.t.	55786	7556	0.9%	<1.0%
4	8	6	29540437	o.t.	152439	o.t.	0.5%	-
5	9	7	-	o.m.	285768	o.t.	-	-
6	10	7	-	o.m.	570271	o.t.	-	-
7	11	7	-	o.m.	-	o.t.	-	-

indicate that even in the modified scenario, the CFCE-BRG consistently outperforms the RG across all cases, demonstrating both a much smaller structural scale and a much shorter computational time.

Benchmark II

2.1 The original model

The second benchmark is derived from a practical manufacturing process [2], as illustrated in Fig. 4. From this layout, a parameterized Petri net is constructed, as shown in Fig. 5 (referred to as Fig. 5 in [2]).

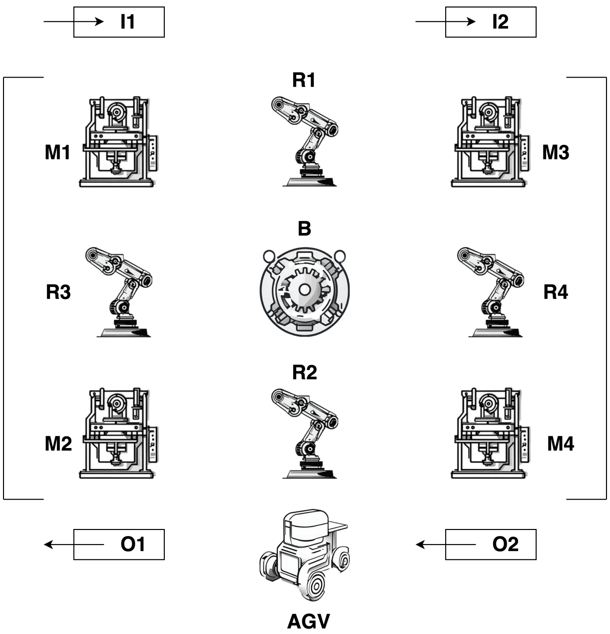

Figure 4: The layout of the manufacturing system [2].

As introduced in [2], the Petri net in Fig. 5 consists of four machines (**M1**, **M2**, **M3** and **M4**), four robots (**R1**, **R2**, **R3** and **R4**), one Autonomous Guided Vehicle (**AGV**) system, one buffer of finite capacity (**B**), two inputs of parts to be processed (**I1** and **I2**) and two outputs for the processed parts (**O1** and **O2**). The two production lines produce two different kinds of final product. There are 46 places and 39 transitions in this marked net. The designation of place p_{40} signifies the count of available slots within the buffer; whereas, the marking of place p_1 (p_{16}) signifies the quantity of items belonging to type 1 (type 2).

In the original model, specific fault events are characterized by distinct transitions, denoted as t_{33}, t_{36}, t_{37}, and t_{38}. For instance, the fault transition t_{33} represents a malfunction in robot **R3**, resulting in the transfer of a component from the output buffer of machine **M1** to the input buffer of machine **M2**, instead of depositing it into buffer **B**. Analogously, the fault transition t_{36} portrays a malfunction in robot **R4**, leading to the movement of a component from the output buffer of machine **M3** to the input buffer of machine **M4**, rather than placing it in buffer **B**. In the original model, the initial marking is parameterized as

$$M_0 = [\alpha\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ \beta\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 1\ 1\ 1\ 1\ 1\ 0\ 1\ 1\ 1\ 8\ 1\ 0\ 0\ 0\ 0\ 0]^T.$$

This parameterization suggests that there are α and β input unprocessed parts, 8 free slots of the buffer; meanwhile, machines **M1**, **M2**, **M3**, and **M4** are all available. Let $T_c = \{t_1, t_7, t_{22}, t_{24}, t_{33}, t_{39}\}$ (marked in red). It can be concluded through the net structure that $T_{conf} = \{t_6, t_7, t_8, t_9, t_{13}, t_{14}, t_{15}, t_{21}, t_{22}, t_{23}, t_{24},$

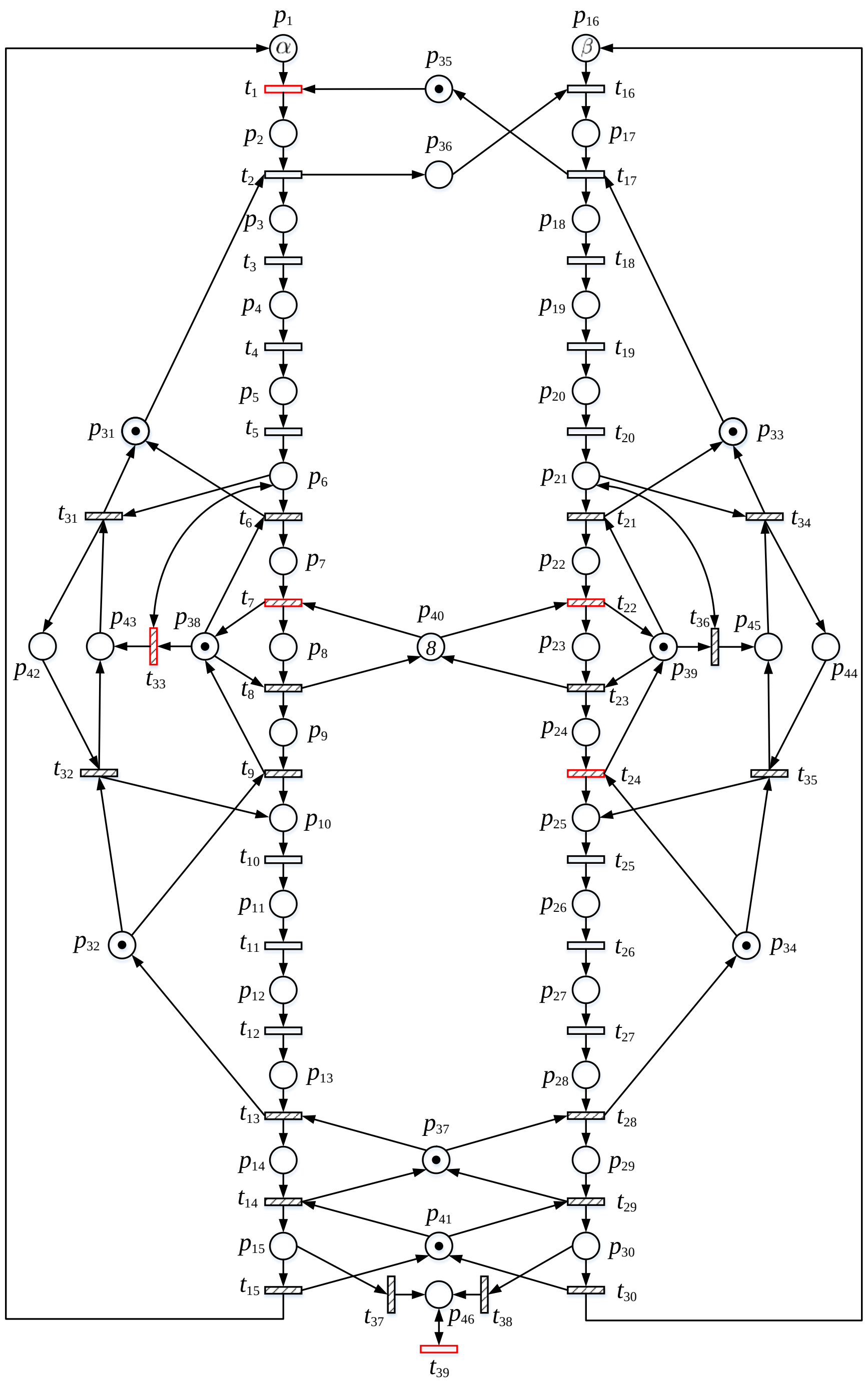

Figure 5: The manufacturing system modeled by PN [2].

$t_{28}, t_{29}, t_{30}, t_{31}, t_{32}, t_{33}, t_{34}, t_{35}, t_{36}, t_{37}, t_{38}\}$ (marked in shadow). Thus, we have basis partition $\pi = (T_E, T_I)$ where $T_E = T_c \cup T_{conf}$. Based on the basis partition π, the correspond CFCE-BRG can be obtained. In Table 5, for different values of α and β, the number of basis markings in the CFCE-BRG, all reachable markings in the RG, and their computing times are listed in columns 1−9. The corresponding ratios (size and time ratios) are reported in columns 8−9. Through this benchmark tests, we conclude that the CFCE-BRG is much smaller in size and costs less computation time than the RG in all cases.

Table 5: Analysis of the RG and CFCE-BRG for the Petri net in Fig. 5.

Run	α	β	$\lvert R(N, M_0)\rvert$	Time (s)	$\lvert\mathcal{M}_{\mathcal{B}}\rvert$	Time (s)	$\lvert\mathcal{M}_{\mathcal{B}}\rvert/\lvert R(N, M_0)\rvert$	Time ratio
1	1	3	35098	2845	4102	43	11.7%	1.0%
2	2	3	205761	o.t.	15091	423	7.3%	-
3	2	4	448306	o.t.	24353	1183	5.4%	-
4	3	3	655472	o.t.	34361	2514	5.2%	-
5	3	4	1383391	o.t.	54761	6582	4.0%	-
6	4	4	2840410	o.t.	93279	19752	3.3%	-
7	5	5	7106562	o.t.	184375	o.t.	2.6%	-
8	6	6	13289726	o.t.	302259	o.t.	2.3%	-
9	7	7	-	o.m.	425140	o.t.	-	-

We exemplify the determination of deadlock-freeness and liveness through the CECF-BRG by run 3, during which the RG computation exceeds the allotted time. First, the absence of a terminal basis marking in the CFCE-BRG $\mathcal{B}$ (with size $|\mathcal{M}_{\mathcal{B}}| = 24353$) constructed in run 3 verifies the deadlock-freeness of the corresponding Petri net (from Corollary 2 in the paper).

Second, Fig. 6 illustrates the existence of an ergodic strongly connected component within CFCE-BRG $\mathcal{B}$. This component is represented as $\mathcal{G}' = (\mathcal{V}', \mathcal{E}')$, where $\mathcal{V}' = \{M_{b,23981}\}$ and $\mathcal{E}' = \{(t_{39}, [0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0]^T)\}$. That is to say, the ergodic strongly connected component $\mathcal{G}'$ consists of a self-loop on the basis marking $M_{b,23981}$. This basis marking is located alongside two other basis markings, $M_{b,23797}$ and $M_{b,23800}$, where

$$M_{b,23797} = [0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 1\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 2\ 1\ 1\ 0\ 0\ 0\ 0\ 0\ 1\ 1\ 1\ 0\ 0\ 1\ 0\ 1\ 0\ 6\ 0\ 0\ 0\ 0\ 0\ 0]^T,$$

$$M_{b,23800} = [0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 2\ 1\ 1\ 0\ 0\ 0\ 0\ 0\ 1\ 0\ 1\ 0\ 0\ 1\ 1\ 1\ 0\ 6\ 0\ 0\ 0\ 0\ 0\ 1]^T,$$

$$M_{b,23981} = [0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 2\ 1\ 1\ 0\ 0\ 0\ 0\ 0\ 1\ 1\ 1\ 0\ 0\ 1\ 0\ 1\ 0\ 6\ 0\ 0\ 0\ 0\ 0\ 1]^T.$$

Furthermore, we can deduce the following relationship within $\mathcal{G}'$:

$$[(\exists t \in T_E)\ (t, \cdot) \notin \mathcal{E}'] \wedge [\sum_{(\cdot, \mathbf{y}) \in \mathcal{E}'} \mathbf{y} \ngeq \mathbf{1}^{|T_I|}].$$

Consequently, as proved in Corollary 4 of the manuscript, we can infer that the marked net in run 3 is not live.

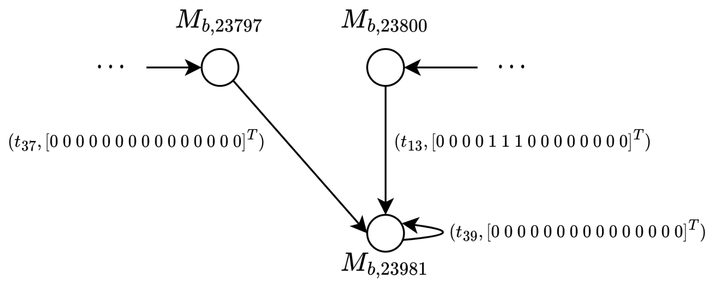

Figure 6: Part of the CFCE-BRG $\mathcal{B}$ in run 3.

2.2 The modified model

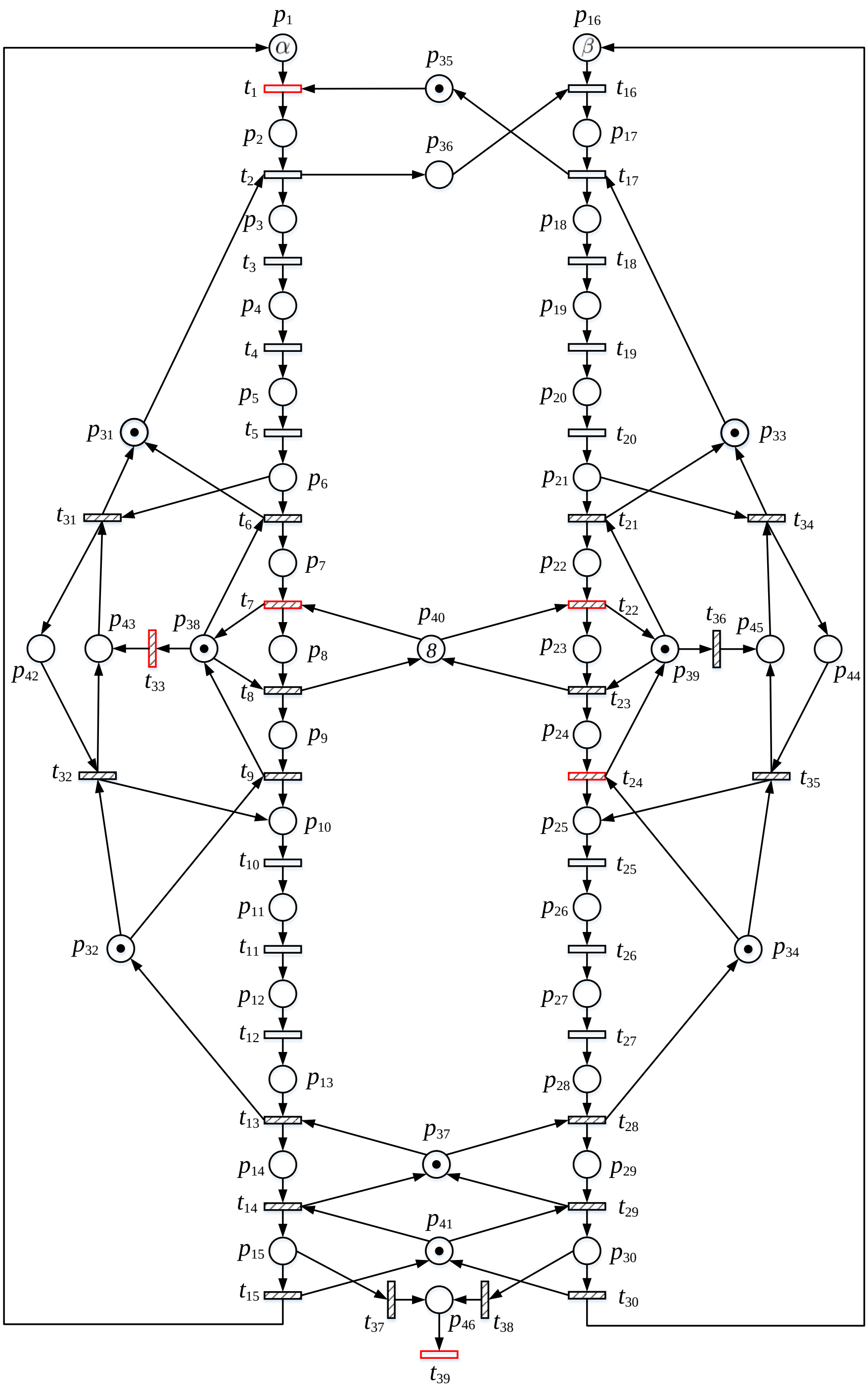

Figure 7: The modified version.

Given that the primary emphasis of our study does not center on the fault diagnosis problem explored in [2], we simplify the original model by excluding the interconnection between fault event t_{33} and the output buffer of machine **M1** with the input buffer of machine **M2**, along with the disconnection between fault event t_{36} and the output buffer of machine **M3** to the input buffer of machine **M4**. Thus, corresponding arcs including $p_6 \to t_{33}, t_{33} \to p_6, p_{21} \to t_{36}$, and $t_{36} \to p_{21}$ are eliminated. For the same rationale, it is unnecessary to observe and record each instance in which a component is moved by the **AGV** subsequent to the occurrence of fault transitions. Consequently, we exclude the arc $t_{39} \rightarrow p_{46}$ from consideration.

The modified Petri net (corresponding to the original one in Fig. 5) is shown in Fig. 7. As illustrated, no additional places nor transitions are added/diminished in the modified one. In the modified model, the initial marking is unchanged and remain parameterized as

$$M_0 = [\alpha\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ \beta\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 1\ 1\ 1\ 1\ 1\ 0\ 1\ 1\ 1\ 8\ 1\ 0\ 0\ 0\ 0\ 0]^T.$$

Let $T_c = \{t_4, t_5, t_6, t_7, t_8, t_{11}, t_{15}\}$. Note that the elimination of the arcs mentioned above does not vary the set $T_{conf} = \{t_6, t_7, t_8, t_9, t_{13}, t_{14}, t_{15}, t_{21}, t_{22}, t_{23}, t_{24}, t_{28}, t_{29}, t_{30}, t_{31}, t_{32}, t_{33}, t_{34}, t_{35}, t_{36}, t_{37}, t_{38}\}$; hence we will use the same basis partition $\pi = (T_E, T_I)$ with the original one, i.e., $T_E = T_c \cup T_{conf}$. In Table 6, the simulation results are presented, demonstrating the better performance of CFCE-BRGs compared to RGs in all scenarios considered, in line with the results of the original model.

Table 6: Analysis of the RG and CFCE-BRG for the modified model in Fig. 7.

Run	α	β	$\|R(N, M_0)\|$	Time (s)	$\|\mathcal{M}_\mathcal{B}\|$	Time (s)	$\|\mathcal{M}_\mathcal{B}\|/\|R(N, M_0)\|$	Time ratio
1	1	1	1966	10	604	2	30.7%	20%
2	1	2	12577	277	2145	11	17.0%	4.0%
3	2	2	76808	12378	7718	105	10.0%	0.8%
4	2	3	262236	o.t.	16438	470	6.2%	-
5	2	4	586604	o.t.	26648	1248	4.5%	-
6	3	3	853850	o.t.	37118	2492	4.3%	-
7	3	4	1837329	o.t.	59315	6449	3.2%	-
8	4	4	3827308	o.t.	101420	19491	2.6%	-
9	5	5	9730140	o.t.	201762	o.t.	2.0%	-

Benchmark III

3.1 The original model

The primary objective of the XML firewall is to execute authentication and authorization validation for incoming requests originating from the application. The parameterized model in Fig. 8 (sourced from [1], Fig. 3) represents an application that invokes two web services concurrently. The places and transitions in the model capture the flow of information and actions between different components of the system, including user authentication, role assignment, access request handling, and web service invocation.

The marked net is devised for a high-level design of the XML firewall implementation. It provides a visual representation of the system's behavior and can be used to analyze properties such as boundedness and liveness. Comprehensive explanations of places and transitions are provided in Table 7.

In the original model, the initial marking is parameterized as

$$M_0 = [\alpha\ 0\ 0\ 0\ \beta\ 0\ 0\ 0\ \gamma\ 0\ 0\ \delta\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0]^T,$$

implying that there are α user login requests, β data in user database, γ user access request, and δ accepted results to be able to used by *computational logic* transition (t_{10}) for further processing.

We set $T_c = \{t_3, t_5, t_7, t_{12}, t_{13}, t_{14}, t_{15}\}$ (boxed in red); further, we conclude $T_{conf} = \{t_2, t_3, t_4, t_5, t_7, t_8, t_9, t_{12}, t_{13}, t_{14}, t_{15}\}$ (shaded) via the structure of the net. As a result, we have a basis partition $\pi = (T_E, T_I)$ to construct the CFCE-BRG where $T_E = \{t_2, t_3, t_4, t_5, t_7, t_8, t_9, t_{12}, t_{13}, t_{14}, t_{15}\}$ and $T_I = T \setminus T_E$. For different parameters of α, β, γ and δ, in Table 8, we report the efficiency of RGs and CFCE-BRGs.

We can verify the deadlock-freeness and liveness through the CFCE-BRG constructed in our benchmarks. For example, at run 3 ($|\mathcal{M}_\mathcal{B}| = 30115$), in the CFCE-BRG $\mathcal{B}$, there are several terminal basis markings such as $M_{b,30090} = [0\ 0\ 0\ 0\ 4\ 4\ 0\ 4\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 4\ 4\ 0]^T$. As another example, in run 4 ($|\mathcal{M}_\mathcal{B}| =$

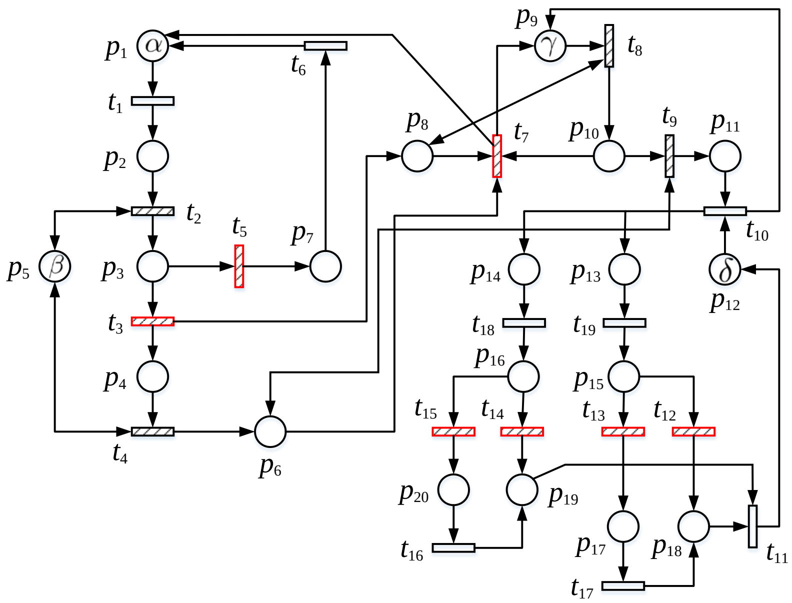

Figure 8: An XML firewall security system modeled by PN [1].

Table 7: Physical interpretations of places and transitions of the Petri net in Fig. 8 [1].

p_1	Login request
p_2	Username password
p_3	Verify user's authenticity
p_4	Login success
p_5	User database
p_6	User details
p_7	Login failure
p_8	Ready to accept request
p_9	User access request
p_{10}	Dispatch request
p_{11}	Request details
p_{12}	Init/result
p_{13}	Request for web service 2
p_{14}	Request for web service 1
p_{15}	Done checking
p_{16}	Done checking
p_{17}	Web service Request
p_{18}	Firewall Result
p_{19}	Firewall Result
p_{20}	Web service request

t_1	Get login request
t_2	Check user database
t_3	Valid
t_4	Get user details
t_5	Not valid
t_6	Access denied
t_7	Logout
t_8	Access request
t_9	Create request
t_{10}	Computational logic
t_{11}	Accept result
t_{12}	Access denied
t_{13}	Request for web service
t_{14}	Access denied
t_{15}	Request for web service
t_{16}	Web service logic
t_{17}	Web service logic
t_{18}	XML Firewall
t_{19}	XML Firewall

56658), there are also terminal basis markings in the corresponding CFCE-BRG $\mathcal{B}$, such as $M_{b,56633} = [0\ 0\ 0\ 0\ 5\ 5\ 0\ 5\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 4\ 4\ 0]^T, M_{b,56640} = [0\ 0\ 0\ 0\ 5\ 5\ 0\ 5\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 1\ 3\ 2\ 2]^T, M_{b,56643} = [0\ 0\ 0\ 0\ 5\ 5\ 0\ 5\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 2\ 2\ 4\ 0]^T$, etc. Based on our results (Corollary 2 in the manuscript), the marked nets in runs 3 and 4 are verified to be non-deadlock-free, i.e. non-live.

Table 8: Analysis of the RG and CFCE-BRG for the Petri net in Fig. 8.

Run	α	β	γ	δ	$\lvert R(N, M_0)\rvert$	Time (s)	$\lvert\mathcal{M}_\mathcal{B}\rvert$	Time (s)	$\lvert\mathcal{M}_\mathcal{B}\rvert/\lvert R(N, M_0)\rvert$	Time ratio
1	2	2	2	2	1439	8	435	0.8	30.2%	10.0%
2	3	3	3	3	28980	3085	4645	53	16.0%	1.7%
3	4	4	4	4	330890	o.t.	30115	2525	9.1%	-
4	5	5	4	4	706580	o.t.	56658	9523	8.0%	-
5	5	6	4	4	706580	o.t.	56658	10406	8.0%	-
6	6	7	4	4	1360716	o.t.	97552	29880	7.2%	-
7	6	6	5	4	4183032	o.t.	232162	o.t.	5.6%	-
8	6	6	6	4	-	o.m.	463022	o.t.	-	-

3.2 The modified model

The modified XML firewall model aims to increase the security and flexibility of the system by redefining the flow and dependencies of actions. To this end, certain arcs in the model are eliminated to streamline the user authentication, access control and request handling processes, optimizing the handling of user information. These modifications also refine the request generation process and improve the flow of request handling and service invocation.

The underlying motivations and consequential implications of these changes are outlined below:

- $t_2 \to p_5$: By removing the direct link between the user database and the *Check user database* operation, we aim to streamline the flow of user authentication and access control within the XML firewall model.
- $t_4 \to p_5$ & $p_5 \to t_4$: This change aims to improve the handling of user information by removing unnecessary links between the *Get user details* operation and the user database.
- $t_3 \to p_8$: This modification aims to improve the authorization and request handling flow by removing the direct connection between the validation process and the readiness to *Ready to accept request.*
- $p_6 \to t_9$: This modification aims to refine the request creation process by preventing the user details from directly triggering the creation of a request.
- $p_8 \to t_8$: This modification aims to improve the request handling and service invocation flow by removing the direct link between the readiness to accept requests and the access request operation.

The modified model is shown in Fig. 9. In this modified version, the initial marking is remain unchanged and parameterized as

$$M_0 = [\alpha\ 0\ 0\ 0\ \beta\ 0\ 0\ 0\ \gamma\ 0\ 0\ \delta\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0]^T.$$

Through the modifications, we can create a new XML firewall security model that can protect web services from unauthorised access and ensure proper authentication and authorisation. It provides a high-level design for XML firewall implementation and allows verification of key properties such as liveness.

Let $T_c = \{t_3, t_5, t_7, t_{12}, t_{13}, t_{14}, t_{15}\}$ (boxed in red) and thus $T_{uc} = T \setminus T_c$. From the modified net structure, it can be concluded that $T_{conf} = \{t_3, t_5, t_7, t_9, t_{12}, t_{13}, t_{14}, t_{15}\}$ (marked with shadow) holds. Based on the CFCE condition, for the basis partition $\pi = (T_E, T_I)$, we set $T_E = \{t_3, t_5, t_7, t_9, t_{12}, t_{13}, t_{14}, t_{15}\}$ and $T_I = T \setminus T_E$.

With different parameters, the number of reachable markings and basis markings, along with the time consumption, are respectively listed in Table 9. The data shows that as the system scale increases, the

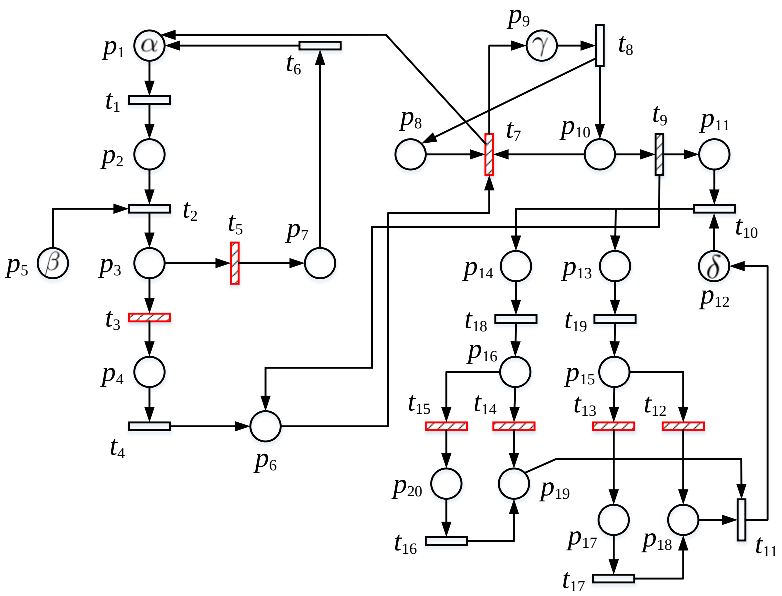

Figure 9: The modified version.

CFCE-BRG is much smaller in size and takes less time to compute than the RG in all cases. Meanwhile, the set of reachable markings cannot be computed in time after case 1 and cannot be obtained in case 7 due to insufficient memory.

Table 9: Analysis of the RG and CFCE-BRG for the modified model in Fig. 9.

Run	α	β	γ	δ	$\lvert R(N, M_0)\rvert$	Time (s)	$\lvert\mathcal{M}_\mathcal{B}\rvert$	Time (s)	$\lvert\mathcal{M}_\mathcal{B}\rvert/\lvert R(N, M_0)\rvert$	Time ratio
1	2	2	2	2	13272	406	910	1	6.8%	0.2%
2	3	3	3	3	1534512	o.t.	8540	122	0.6%	<0.2%
3	4	4	4	4	5051802	o.t.	49945	4937	1.0%	<0.2%
4	5	5	4	4	10293738	o.t.	79912	14553	0.8%	<0.2%
5	5	6	4	4	14827974	o.t.	117271	32791	0.8%	<0.2%
6	6	6	4	4	19274094	o.t.	119868	30857	0.6%	<0.2%
7	6	6	5	4	-	o.m.	285768	o.t.	-	-

Benchmark IV

A Radio Block Center (RBC) is an essential ground system that is responsible for creating messages intended for trains. These messages are based on data from external ground subsystems and onboard systems. RBCs play a crucial role in granting trains the necessary authority to move along their designated routes. Each RBC area is monitored by a single RBC.

Fig. 10 depicts the fourth benchmark including a parameterized marked net, structured to imitate an RBC system [3]. This model encompasses three primary components: a marked net representing the passage of a train through the RBC border, a marked net corresponding to RBC1, and a marked net associated with RBC2. The significance of the three main places in each component is outlined as follows:

- p_1: Indicates the approach of a train to the RBC2 area.
- p_{14}: Signifies the availability of RBC1.
- p_{27}: Indicates the availability of RBC2.

Based on the above-mentioned presentation, our benchmark test employed an initial marking parameterization with

$$M_0 = [\alpha\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ \beta\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ \gamma\ 0\ 0\ 0\ 0\ 0]^T.$$

Let us define the controllable transition set as $T_c = \{t_2, t_4, t_5, t_{16}\}$ (highlighted in red). By examining the network structure, we can deduce that the set T_{conf} is comprised of transitions $t2, t4, t5, t8$, and t_{10} (indicated with shading). Additionally, consider t_{21} (highlighted in blue) as an explicit transition designed to ensure the acyclic nature of the T_I-induced subnet. We establish a CFCE basis partition $\pi = (T_E, T_I)$, where T_E consists of T_{conf}, T_c, and t_{21}. On the other hand, T_I is the complementary set to T_E within the transition set T.

For various parameter values denoted as α, β and γ, we have conducted simulations to compare CFCE-BRG and RG, and the results are presented in Table 10. Through the test of Benchmark IV, it is evident that RG exceeds the computational time limit in the first run and cannot be accommodated within an 8 GB RAM in other instances. In contrast, CFCE-BRG remains computable in all scenarios and consistently exhibits a smaller size compared to RG.

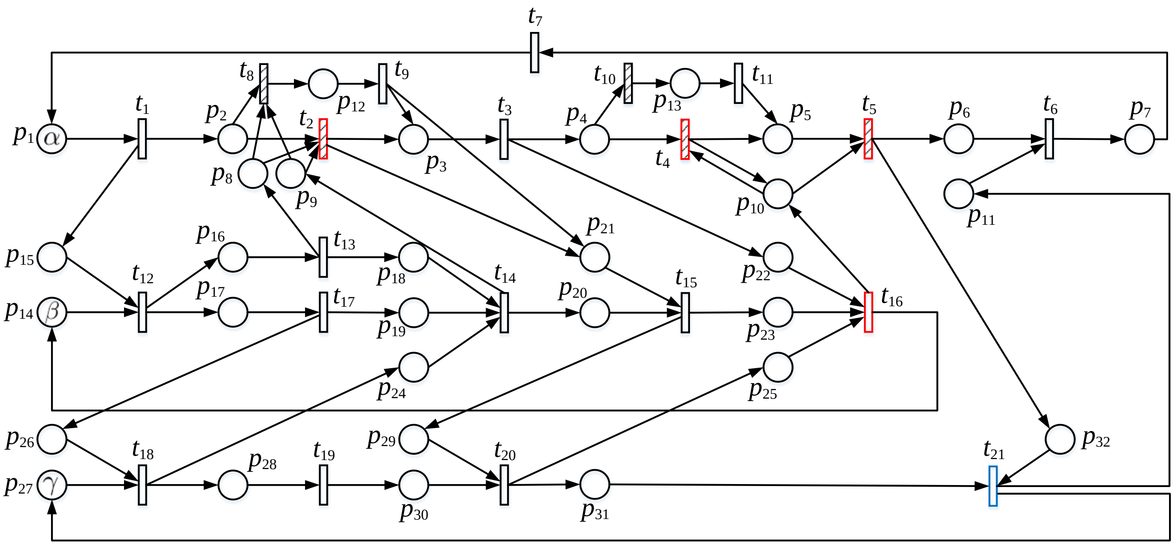

Figure 10: A radio block center system modeled by PN [3].

Table 10: Analysis of the RG and CFCE-BRG for the Petri net in Fig. 10.

Run	α	β	γ	$\lvert R(N, M_0)\rvert$	Time (s)	$\lvert\mathcal{M}_\mathcal{B}\rvert$	Time (s)	$\lvert\mathcal{M}_\mathcal{B}\rvert/\lvert R(N, M_0)\rvert$	Time Ratio
1	6	6	6	1838212	o.t.	3229	21	0.1%	<0.1%
2	10	10	10	-	o.m.	41832	4693	-	-
3	11	11	11	-	o.m.	70004	13575	-	-
4	12	12	12	-	o.m.	113034	43257	-	-
5	13	13	13	-	o.m.	176930	o.t.	-	-

References

[1] M. M. Ayachit and H. P. Xu. A petri net based xml firewall security model for web services invocation. In *Proceedings of the LASTED International Conference Communication, Network, and Information Security*, pages 61–67, 2006.

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

[3] H. Lan, Y. Tong, and C. Seatzu. Crucial states estimation in radio block center handover using Petri nets with unobservable transitions. *IEEE Transactions on Automation Science and Engineering*, 19(2):1268–1276, 2021.

[4] J. Li, M. C. Zhou, T. Guo, Y. H. Gan, and X. Z. Dai. Robust control reconfiguration of resource allocation systems with Petri nets and integer programming. *Automatica*, 50(3):915–923, 2014.