Journal Title
XX(X):1–6
©The Author(s) 2025
Reprints and permission:
sagepub.co.uk/journalsPermissions.nav
DOI: 10.1177/ToBeAssigned
www.sagepub.com/
SAGE

Supplementary Document to "Detection of Actuator Enablement Attacks by Time Petri Nets in Supervisory Control"

Zhenhua Yu[1],Yifei Jia[1] and Xuya Cong[1]

In this section, a comparison between the diagnoser and verifier algorithms is conducted under different TPN models. All algorithms are implemented in MATLAB R2023b, and the experimental results are obtained using a laptop computer running the Windows 11 operating system. This device is configured with a 12th Gen Intel (R) Core (TM) i9-12900H processor and 16 GB of RAM.

In this experiment, the algorithms of the diagnoser and verifier for checking AE-safe controllability are compared from the following five aspects: (1) the number of places ($|P|$); (2) the number of states in the original model G ($|X|$); (3) the number of states in the attack-closed controlled system ($|G_M|$); (4) the number of states of the diagnoser ($|X_d|$) or the number of states of the verifier ($|X_T|$); (5) AE-safe controllability.

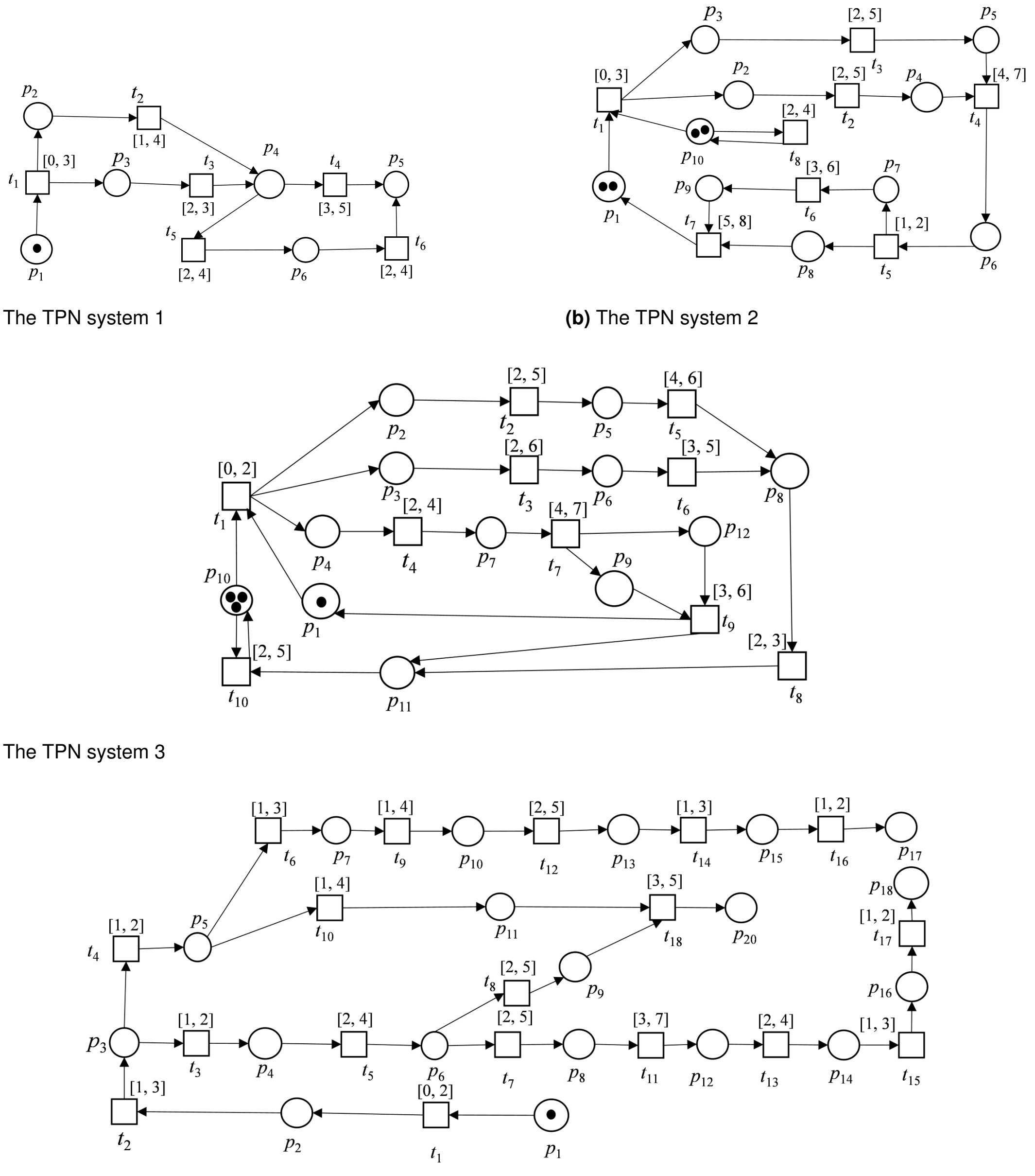
As stated previously, the definitions of event observability and controllability remain consistent with the transitions throughout this paper. To maintain symbol uniformity, we still use α_i to represent both controllable and uncontrollable events. The core parameters for each TPN model (corresponding to Figure 1) are defined as follows:

(1) Figure 1a: The set of controllable events is $\Sigma_c = \{\alpha_1, \alpha_3, \alpha_4\}$, the set of vulnerable-to-attack events is $\Sigma_{c,v} = \{\alpha_3\}$, and the set of unsafe states is $X_f = \{x_{10}\}$. (2) Figure 1b: The set of controllable events is $\Sigma_c = \{\alpha_1, \alpha_5, \alpha_6, \alpha_7, \alpha_8\}$, the set of vulnerable-to-attack events is $\Sigma_{c,v} = \{\alpha_5\}$, and the set of unsafe states is $X_f = \{x_{20}\}$. (3) Figure 1c: The set of controllable events is $\Sigma_c = \{\alpha_1, \alpha_2, \alpha_3, \alpha_5, \alpha_6\}$, the set of vulnerable-to-attack events is $\Sigma_{c,v} = \{\alpha_5, \alpha_6\}$, and the set of unsafe states is $X_f = \{x_{13}, x_{17}\}$. (4) Figure 1d: The set of controllable events is $\Sigma_c = \{\alpha_3, \alpha_4, \alpha_5, \alpha_7, \alpha_8, \alpha_9, \alpha_{12}, \alpha_{15}, \alpha_{16}, \alpha_{17}, \alpha_{18}\}$, the set of vulnerable-to-attack events is $\Sigma_{c,v} = \{\alpha_5, \alpha_7, \alpha_9\}$, and the set of unsafe states is $X_f = \{x_{17}, x_{18}\}$.

The comparative experimental results of AE-safe controllability verification using diagnosers and verifiers under different TPN models are presented in Table 1. From the perspective of basic parameters,

[1] College of Artificial Intelligence and Computer Science, Xi'an University of Science and Technology, Xi'an 710054, China

Corresponding author:
Xuya Cong, College of Artificial Intelligence and Computer Science, Xi'an University of Science and Technology, Xi'an 710054, China.
Email: congxuya@xust.edu.cn



(a) The TPN system 1

(b) The TPN system 2

(c) The TPN system 3

(d) The TPN system 4

Figure 1. The TPN systems 1-4 for the experiment

the number of places ($|P|$), the number of states ($|X|$), and the number of states ($|X_M|$) show an increasing trend with the functional complexity of the models. In terms of diagnosis and verification results, the inspection outcomes of the diagnoser and verifier are consistent. It should be particularly noted that the TPN system 3 encountered a state explosion problem during the construction of the MSCG. The extensive concurrent logic in Figure 1c caused the state space to expand exponentially during iterations, which far exceeded the scope of conventional computing. The state count ($|X|$) of the TPN system 3 is a partial result obtained after setting a maximum iteration limit of 5000 and forcibly terminating the computation, rather than a complete statistic of all reachable states. Affected by the state explosion, the subsequent parameters related to the diagnoser and verifier for TPN system 3 could not be further calculated and presented. This also provides a clear direction for future research on optimizing MSCG construction methods for large-scale TPN systems and mitigating the state explosion issue.

Table 1. Experimental Result Comparison of TPN1 to TPN4

compare	TPN system 1	TPN system 2	TPN system 3	TPN system 4
$\|P\|$	6	10	12	20
$\|X\|$	13	180	21881	22
$\|X_M\|$	20	277	—	35
diagnoser				
$\|X_d\|$	22	348	—	152
AE-safe controllability	false	true	—	true
verifier				
$\|X_T\|$	16	295		138
AE-safe controllability	false	true	—	true

An Example of a Warehouse Order Processing System

The TPN model of the warehouse order processing system is shown in Figure 2. This architecture enables a closed-loop management process from order inflow to completion. In the specific process design, the standard order processing flow includes two branches: sufficient stock and insufficient stock. Expedited orders utilize priority scheduling to optimize resource allocation and shorten the processing cycle. Noted that there are two tokens in p_1, representing two pending order tasks in the current system. To further clarify the practical implications of each core element in the system modeling process, Table 2 and Table 3 provide detailed definitions of the physical scenarios and functions corresponding to the places and transitions in the model, respectively.

The MSCG corresponding to this system, which represents the plant G under investigation, is illustrated in Figure 3. Based on the physical properties of the transitions in Table 3, the system's uncontrollable event set is $\Sigma_{uc} = \{\alpha_5, \alpha_6, \alpha_9\}$. These events are typically automated and dominated by equipment, making external interference extremely difficult. Conversely, the controllable event set is $\Sigma_c = \{\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_7, \alpha_8, \alpha_{10}\}$. The vulnerable event set is $\Sigma_{c,v}^a = \{\alpha_2, \alpha_3, \alpha_8\}$. They are the core targets for attack intervention because they correspond to events that affect critical decision-making,

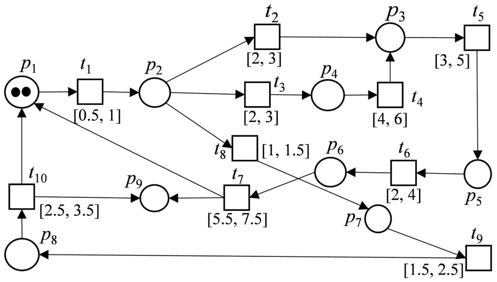


Figure 2. The TPN model of the warehouse order processing system

Table 2. Physical meaning of places.

Places	Meaning
p_1	All pending orders
p_2	Waiting for the system to identify the order priority
p_3	Regular orders with sufficient inventory are pending sorting
p_4	Regular orders are pending stock replenishment
p_5	Regular orders are pending quality inspection
p_6	Regular orders are pending packaging
p_7	Rush orders with sufficient inventory are pending sorting
p_8	Rush orders are pending packaging
p_9	Order completed

Table 3. Physical meaning of transitions.

Transition	Meaning
t_1	Classification of pending orders
t_2	Check on sufficient inventory for regular orders
t_3	Check on insufficient inventory for regular orders
t_4	Regular order replenishment
t_5	Regular order sorting process
t_6	Regular order quality inspection process
t_7	Package regular orders and process new orders
t_8	Rush order inventory check
t_9	Rush order sorting
t_{10}	Package rush orders and process new orders

such as order flow direction and prioritization. The two types of states, “Regular Order with Sufficient Inventory Pending Sorting” and “Rush Order with Sufficient Inventory Pending Sorting,” serve as the core nodes connecting order decision-making and physical execution. Anomalies in these states directly lead to the stagnation of the warehouse sorting function and the interruption of the supply chain flow, thereby disrupting the normal operational logic of the warehouse. Therefore, the unsafe state set for this system is defined as $X_f = \{x_2, x_3, x_7\}$. These states are critical for accurately describing the threats to system stability.

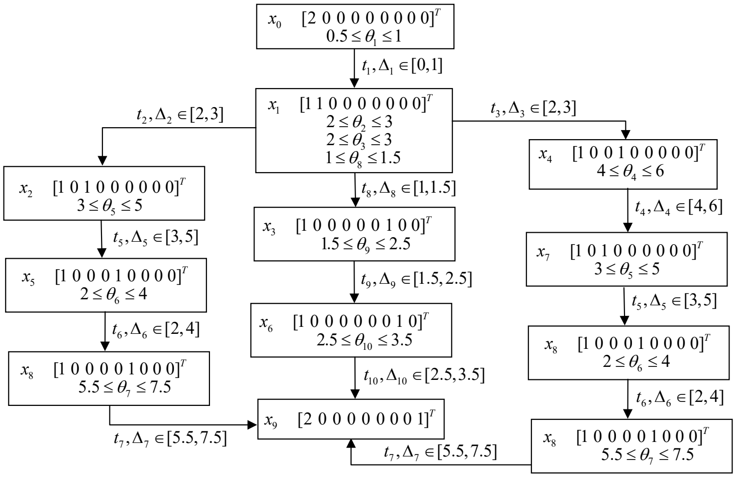

x_0 $[2\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0]^T$ $0.5 \le \theta_1 \le 1$
$t_1, \Delta_1 \in [0,1]$
x_1 $[1\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 0]^T$ $2 \le \theta_2 \le 3$ $2 \le \theta_3 \le 3$ $1 \le \theta_8 \le 1.5$
$t_2, \Delta_2 \in [2,3]$
$t_3, \Delta_3 \in [2,3]$
x_2 $[1\ 0\ 1\ 0\ 0\ 0\ 0\ 0\ 0]^T$ $3 \le \theta_5 \le 5$
$t_8, \Delta_8 \in [1,1.5]$
x_4 $[1\ 0\ 0\ 1\ 0\ 0\ 0\ 0\ 0]^T$ $4 \le \theta_4 \le 6$
x_3 $[1\ 0\ 0\ 0\ 0\ 0\ 1\ 0\ 0]^T$ $1.5 \le \theta_9 \le 2.5$
$t_4, \Delta_4 \in [4,6]$
$t_5, \Delta_5 \in [3,5]$
x_7 $[1\ 0\ 1\ 0\ 0\ 0\ 0\ 0\ 0]^T$ $3 \le \theta_5 \le 5$
x_5 $[1\ 0\ 0\ 0\ 1\ 0\ 0\ 0\ 0]^T$ $2 \le \theta_6 \le 4$
$t_9, \Delta_9 \in [1.5,2.5]$
$t_5, \Delta_5 \in [3,5]$
x_6 $[1\ 0\ 0\ 0\ 0\ 0\ 0\ 1\ 0]^T$ $2.5 \le \theta_{10} \le 3.5$
$t_6, \Delta_6 \in [2,4]$
x_8 $[1\ 0\ 0\ 0\ 1\ 0\ 0\ 0\ 0]^T$ $2 \le \theta_6 \le 4$
x_8 $[1\ 0\ 0\ 0\ 0\ 1\ 0\ 0\ 0]^T$ $5.5 \le \theta_7 \le 7.5$
$t_{10}, \Delta_{10} \in [2.5,3.5]$
$t_6, \Delta_6 \in [2,4]$
x_9 $[2\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 1]^T$
x_8 $[1\ 0\ 0\ 0\ 0\ 1\ 0\ 0\ 0]^T$ $5.5 \le \theta_7 \le 7.5$
$t_7, \Delta_7 \in [5.5,7.5]$
$t_7, \Delta_7 \in [5.5,7.5]$

Figure 3. The MSCG of the TPN system in Figure 2

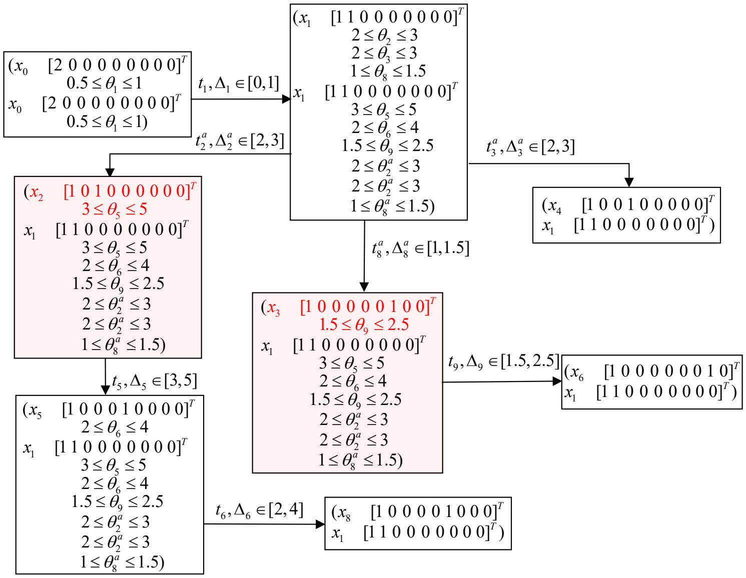
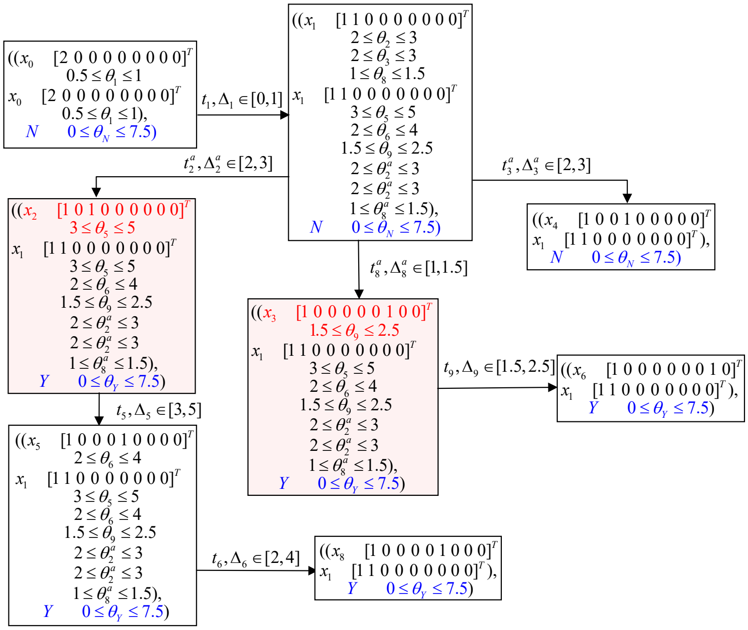

$(x_1$ $[1\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 0]^T$ $2 \le \theta_2 \le 3$ $2 \le \theta_3 \le 3$ $1 \le \theta_8 \le 1.5$ x_1 $[1\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 0]^T$ $3 \le \theta_5 \le 5$ $2 \le \theta_6 \le 4$ $1.5 \le \theta_9 \le 2.5$ $2 \le \theta_2^a \le 3$ $2 \le \theta_2^a \le 3$ $1 \le \theta_8^a \le 1.5)$
$(x_0$ $[2\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0]^T$ $0.5 \le \theta_1 \le 1$ x_0 $[2\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0]^T$ $0.5 \le \theta_1 \le 1)$
$t_1, \Delta_1 \in [0,1]$
$t_2^a, \Delta_2^a \in [2,3]$
$t_3^a, \Delta_3^a \in [2,3]$
$(x_2$ $[1\ 0\ 1\ 0\ 0\ 0\ 0\ 0\ 0]^T$ $3 \le \theta_5 \le 5$ x_1 $[1\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 0]^T$ $3 \le \theta_5 \le 5$ $2 \le \theta_6 \le 4$ $1.5 \le \theta_9 \le 2.5$ $2 \le \theta_2^a \le 3$ $2 \le \theta_2^a \le 3$ $1 \le \theta_8^a \le 1.5)$
$(x_4$ $[1\ 0\ 0\ 1\ 0\ 0\ 0\ 0\ 0]^T$ x_1 $[1\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 0]^T)$
$t_8^a, \Delta_8^a \in [1,1.5]$
$(x_3$ $[1\ 0\ 0\ 0\ 0\ 0\ 1\ 0\ 0]^T$ $1.5 \le \theta_9 \le 2.5$ x_1 $[1\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 0]^T$ $3 \le \theta_5 \le 5$ $2 \le \theta_6 \le 4$ $1.5 \le \theta_9 \le 2.5$ $2 \le \theta_2^a \le 3$ $2 \le \theta_2^a \le 3$ $1 \le \theta_8^a \le 1.5)$
$t_5, \Delta_5 \in [3,5]$
$t_9, \Delta_9 \in [1.5,2.5]$
$(x_6$ $[1\ 0\ 0\ 0\ 0\ 0\ 0\ 1\ 0]^T$ x_1 $[1\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 0]^T)$
$(x_5$ $[1\ 0\ 0\ 0\ 1\ 0\ 0\ 0\ 0]^T$ $2 \le \theta_6 \le 4$ x_1 $[1\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 0]^T$ $3 \le \theta_5 \le 5$ $2 \le \theta_6 \le 4$ $1.5 \le \theta_9 \le 2.5$ $2 \le \theta_2^a \le 3$ $2 \le \theta_2^a \le 3$ $1 \le \theta_8^a \le 1.5)$
$t_6, \Delta_6 \in [2,4]$
$(x_8$ $[1\ 0\ 0\ 0\ 0\ 1\ 0\ 0\ 0]^T$ x_1 $[1\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 0]^T)$

Figure 4. Attacked closed-loop system model G_M

To prevent an increase in analysis complexity due to an excessively large attack time span, the time interval for the occurrence of attack events in this example is set to be the same as the firing time interval of the transitions. According to Algorithm 1, the attacked model G_a and the attacked supervisor H_a are constructed, respectively. By calculating $G_a \otimes H_a$, the attacked closed-loop controlled system G_M of this case is obtained, as shown in Figure 4.

Since this system is a small-scale system, a diagnoser is used to determine the AE-safe controllability of the system. The diagnoser G_d is shown in Figure 5. According to Step 7 of Algorithm 2, we can obtain $\{((x_2, x_1), Y), ((x_3, x_1), Y)\} \in FC$. Since this set contains the unsafe states x_2 and x_3, the system does not satisfy the AE-safe controllability.



((x0 [2 0 0 0 0 0 0 0 0]^T 0.5 ≤ θ1 ≤ 1
x0 [2 0 0 0 0 0 0 0 0]^T 0.5 ≤ θ1 ≤ 1), N 0 ≤ θN ≤ 7.5)
t1, Δ1 ∈ [0,1]
((x1 [1 1 0 0 0 0 0 0 0]^T 2 ≤ θ2 ≤ 3 2 ≤ θ3 ≤ 3 1 ≤ θ8 ≤ 1.5
x1 [1 1 0 0 0 0 0 0 0]^T 3 ≤ θ5 ≤ 5 2 ≤ θ6 ≤ 4 1.5 ≤ θ9 ≤ 2.5 2 ≤ θ2^a ≤ 3 2 ≤ θ2^a ≤ 3 1 ≤ θ8^a ≤ 1.5), N 0 ≤ θN ≤ 7.5)
t2^a, Δ2^a ∈ [2,3]
t3^a, Δ3^a ∈ [2,3]
((x4 [1 0 0 1 0 0 0 0 0]^T x1 [1 1 0 0 0 0 0 0 0]^T), N 0 ≤ θN ≤ 7.5)
((x2 [1 0 1 0 0 0 0 0 0]^T 3 ≤ θ5 ≤ 5
x1 [1 1 0 0 0 0 0 0 0]^T 3 ≤ θ5 ≤ 5 2 ≤ θ6 ≤ 4 1.5 ≤ θ9 ≤ 2.5 2 ≤ θ2^a ≤ 3 2 ≤ θ2^a ≤ 3 1 ≤ θ8^a ≤ 1.5), Y 0 ≤ θY ≤ 7.5)
t8^a, Δ8^a ∈ [1,1.5]
((x3 [1 0 0 0 0 0 1 0 0]^T 1.5 ≤ θ9 ≤ 2.5
x1 [1 1 0 0 0 0 0 0 0]^T 3 ≤ θ5 ≤ 5 2 ≤ θ6 ≤ 4 1.5 ≤ θ9 ≤ 2.5 2 ≤ θ2^a ≤ 3 2 ≤ θ2^a ≤ 3 1 ≤ θ8^a ≤ 1.5), Y 0 ≤ θY ≤ 7.5)
t9, Δ9 ∈ [1.5, 2.5]
((x6 [1 0 0 0 0 0 0 1 0]^T x1 [1 1 0 0 0 0 0 0 0]^T), Y 0 ≤ θY ≤ 7.5)
t5, Δ5 ∈ [3,5]
((x5 [1 0 0 0 1 0 0 0 0]^T 2 ≤ θ6 ≤ 4
x1 [1 1 0 0 0 0 0 0 0]^T 3 ≤ θ5 ≤ 5 2 ≤ θ6 ≤ 4 1.5 ≤ θ9 ≤ 2.5 2 ≤ θ2^a ≤ 3 2 ≤ θ2^a ≤ 3 1 ≤ θ8^a ≤ 1.5), Y 0 ≤ θY ≤ 7.5)
t6, Δ6 ∈ [2,4]
((x8 [1 0 0 0 0 1 0 0 0]^T x1 [1 1 0 0 0 0 0 0 0]^T), Y 0 ≤ θY ≤ 7.5)

Figure 5. The diagnoser G_d