Proceedings of the 17th World Congress
The International Federation of Automatic Control
Seoul, Korea, July 6-11, 2008

Fault Accommodation for Discrete Event Systems Using Petri Nets with Application to Traffic Light Control [1]

Hao Yang [*,**], **Bin Jiang** [*], **Vincent Cocquempot** [**]

[*] *College of Automation Engineering, Nanjing University of Aeronautics and Astronautics, Nanjing, 210016, P.R. China*

[**] *LAGIS-CNRS, UMR 8146 Université des Sciences et Technologies de Lille, 59655 Villeneuve d'Ascq cedex, France*

Abstract: This paper discusses the fault tolerant control problem for discrete event systems modeled by Petri nets. The fault is represented by the unobservable transitions. Firstly, an observer-based fault diagnosis method is proposed to estimate the marking with unknown initial markings and meanwhile, to diagnose the faulty behavior. Then, an adaptive fault tolerant controller is designed to maintain the general mutual exclusion constraints (GMEC) property of the system. The proposed method is applied to the control of traffic lights.

1. INTRODUCTION

Petri nets (PNs) are widely used for modeling discrete event systems, e.g., autonomous manufacturing, traffic control, chemical process. Such model can capture system's behaviors including concurrency, synchronization and conflicts, see Murata (1989).

Faults may lead to abnormal system behaviors. Fault diagnosis includes detecting, isolating and estimating the faults, while Fault tolerant control (FTC) is aimed at achieving the system goal in spite of faults (see Blanke et al. (2003), Jiang et al. (2006)). To the best of our knowledge, until now, only a few literatures have been devoted to FTC for discrete event systems modeled by PNs such as Balduzzi and Febbraro (2001), Hsieh (2004), where the FTC goal is to prevent the system from deadlock. However, fruitful results of diagnosis methods for PNs can be used as the basis of the further FTC research. In Benveniste et al. (2003), an unfolding based diagnosis approach is provided for asynchronous discrete-event systems. A diagnoser is given based on the concept of basis markings in Giua and Seatzu (2005). Ramirez-Trevino et al. (2007) proposes an on-line diagnosis method based on interpreted PN, where the output information of markings has to be used. The method derived in Lefebvre and Delherm (2007) is based on marking variation and causality relationships. In Wu and Hadjicostis (2005), the parity space method is extended to Petri net. In most of these literatures, the partial marking is measurable or the initial marking is known, such that the current marking just before faults occur can be calculated. Giua et al. (2004) considers the marking estimation from event observations with unknown initial marking, but no fault is considered.

The faulty behavior in this paper is represented as unobservable and uncontrollable transitions as in Giua and Seatzu (2005),Lefebvre and Delherm (2007), which may violate the general mutual exclusion constraints (GMEC) of PN that is the basic requirement for system's stability. We propose an observer-based FTC scheme to maintain the GMEC property of the system. The main contributions of this work are as follows:

1. An observer-based fault diagnosis method is proposed for PN with unknown initial marking, which estimates the unmeasurable markings and meanwhile, diagnoses the fault.
2. Based on the marking estimates, an adaptive FTC scheme is designed to maintain the GMEC, which is updated according to fault behavior. The general condition for controller design that the GMEC is not affected by unobservable transitions is relaxed.
3. The proposed method is effectively applied to the control of traffic lights.

The rest of the paper is organized as follows: Section 2 gives some preliminaries and problem formulation. In Section 3, fault diagnosis and observer design is discussed. FTC is analyzed in Section 4. The application is described in section 5, and simulation results are given. Some concluding remarks end the paper.

2. PRELIMINARIES

2.1 Background on Petri nets

This section recalls the PNs formalism used in this paper. The reader can find a more detailed presentation of PNs

[1] This work is partially supported by National Natural Science Foundation of China (60574083), National "863" program of China (2006AA12A108), Aeronautics Science Foundation of China (2007ZC52039) and Graduate innovation research funding of Jiangsu Province(CX07B-112z).

Email: younghao82@yahoo.com.cn. (H. Yang), binjiang@nuaa.edu.cn (B. Jiang), vincent.cocquempot@univ-lille1.fr (V. Cocquempot).

in Murata (1989). A PN structure is the 4-tuple $N = (P, T, Pre, Post)$, where P is a set of m places, T is a set of n transitions. $Pre_{i,j} : P \times T \to \mathbb{N}$ that assigns a weight to any arc between a transition t_j and its input place p_i, where $\mathbb{N}$ the field of natural numbers. $Post_{i,j} : P \times T \to \mathbb{N}$ that assigns a weight to any arc between a transition t_j and its output place p_i. The preset and postset of a node $X \in P \cup T$ are denoted ${}^\bullet X$ and $X^\bullet$.

The marking of a PN is the function $M : P \to \mathbb{N}$ which assigns a nonnegative integer number of tokens to each place.

A transition $t \in T$ is enabled, if $M \geq Pre(\cdot, t)$ and may fire yielding $M' = M + C(\cdot, t)$, where $C(p, t) = Post(p, t) - Pre(p, t)$. Firing of t_j lasts d_j time units, where d_j is a nonnegative deterministic number. Denote $M[\omega\rangle M'$ such that the enabled sequence of transitions ω may fire at M yielding M'.

The set of faults is denoted as T_f , where $T = T_N \cup T_f$ with T_N the set of normal transition, T_f the set of faults.

From a graphical point of view, places are represented by circles, transitions are represented by thick bars (thin bars denote the immediate discrete transitions i.e., $d = 0$). The marking are represented by the dot in places.

2.2 Control of traffic lights

The application in this work is the control of traffic lights at the terminator of the bridge as shown in Fig.1, where six roads are interconnected with the bridge. The roads r_1^{out}, r_2^{out} and r_3^{out} are the output roads to which the vehicles go from bridge, whereas the roads r_1^{in}, r_2^{in} and r_3^{in} are the input roads from which vehicles go to the bridge.

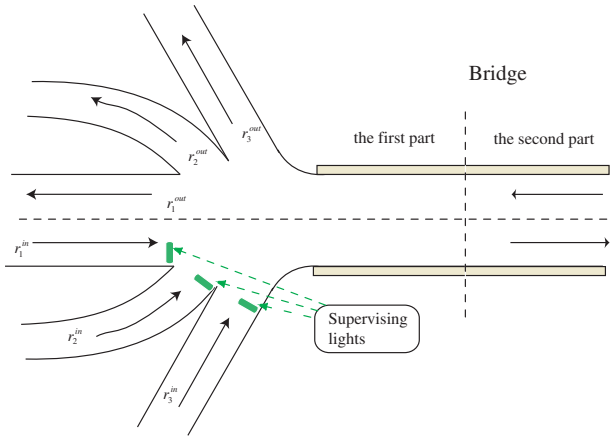

Fig. 1. One terminator of the bridge

The control specification can be described as P1 : the vehicles from different input roads never get into the bridge simultaneously. This is the basic requirement on the initial performance, which must be guaranteed, otherwise the vehicles may crash. The fault considered in this system represents the abnormal behavior of the traffic lights, i.e. the lights do not work as prescribed.

The PN model of the traffic lights system related to Fig.1 is shown in Fig.2, a detailed description of places is given in Table 1. Compared with the PN model in Febbraro et al. (2004), red lights are considered in ours, which is more suitable for fault modeling and FTC design.

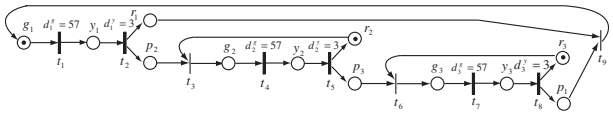

Fig. 2. PN model of traffic lights system

Tablel 1 : Places of the PN in Fig.2

Place	Meaning
g_i	green period of i th input road
y_i	yellow period of i th input road
r_i	red period of i th input road

From Fig. 2, it is more clear that the FTC objective is to reconfigure the PN such that at each time, only one green light is activated in spite of faults.

We impose the following hypothesis which always hold throughout the paper.

H1. All $t \in T_N$ is controllable and observable. All $t \in T_f$ is uncontrollable and unobservable.
H2. $\forall p \in P$, $t \in T$, $Pre(p, t) = Post(p, t)$. If $\exists t_1, t_2 \in T_f$ and ${}^\bullet t_1 = {}^\bullet t_2$, $t_1^\bullet = t_2^\bullet$, then $t_1 = t_2$.
H3. $\forall p \in P$, $M(p)$ is unmeasurable. The initial marking is unknown while the initial macromarking (defined in Section 3) is known.

3. FAULT DIAGNOSIS AND MARKING ESTIMATION

In this section, we consider the problem of fault diagnosis and observer design.

3.1 Fault diagnosability

The diagnosability definition of finite state machine in Sampath et al. (1998) is extended to PN as follows:

Definition 1: A PN is *diagnosable* with respect to $t \in T_f$, if $\exists n \in \mathbb{N}$, and an observable transition sequence ω, such that $\|\omega\| \geq n \Rightarrow t \in \psi(t)\omega$, where $\psi(t)$ denotes the sequence that ends in t, $\|\omega\|$ is the length of the sequence ω. □

The above definition of diagnosability means the following: Let $\psi(t)$ be any transition sequence that ends in a fault $t \in T_f$, and let ω be any sufficiently long continuation of $\psi(t)$. $t \in \psi(t)\omega$ means that every transition sequence, that produces the same record of observable transitions as the sequence $\psi(t)\omega$, should contain a fault in it. This implies that along every continuation ω of $\psi(t)$, one can detect the occurrence of a fault t with a finite delay (n steps).

Before giving the diagnosability result of PN, the following definitions are introduced.

Definition 2: Given a PN N, and a subset $T' \subseteq T$ of its transitions, we define the *T'-induced subnet* of N as the new net $N' = (P, T', Pre', Post')$ where Pre' $Post'$ are the restriction of $Pre, Post$ to T'. □

The net N' can also be thought as obtained from N by removing all transitions in $T \setminus T'$.

Definition 3: An unobservable transitions subset of PN is *acyclic* if no oriented cycle of sequence occurs that contains only unobservable transitions in this subset. □

Definition 4: A PN is *forward conflict* (FC) if there exist two transitions which have at least one common input place. A PN is *backward conflict* (BC) if there exist two transitions which have at least common output place. A PN is *absolutely conflict* (AC) if it is both FC and BC. □

We also say that a PN is forward (resp. backward) conflict free (FCF (resp. BCF)) if it is not forward (resp. backward) conflict.

Lemma 1: A PN is *diagnosable* with respect to $t \in T_f$, if 1) T_f-induced subnet is acyclic. 2) T_f-induced subnet N_f is not AC. 3) the initial marking $M_0(p_b) = M_0(p_a) = 0$, where $p_b \in^\bullet t$, $p_a \in t^\bullet$. 4) ${}^\bullet p_a \setminus t$ do not fire before $p_b^\bullet \setminus t$ or $p_a^\bullet$ fire. 5) After one transition from ${}^\bullet p_b$ fired, ${}^\bullet p_b$ do not fire again before $p_b^\bullet$ fire.

Proof: From the graph point of view, there exist two transition sets ${}^\bullet p_b$ and $p_a^\bullet$ before and after t. Condition 3) implies that a transition $t_b \in^\bullet p_b$ must fire before t since $M_0(p_b) = 0$. Condition 1) means that the occurrence of fault must be interconnected with the firing of normal transitions. Under the condition 2), three cases are considered as follows:

Case 1: The N_f is FCF and BCF. Since $Pre(p,) = Post(p,)$ from H1 and $M_0(p_b) = 0$, Condition 5) implies that if $\exists \varrho \in p_b^\bullet \setminus t$ fires, then t must not occur. On the other hand, $M_0(p_a) = 0$, Condition 4) means that before we determined whether the fault occurs or not, ${}^\bullet p_a \setminus t$ do not fire, i.e., $M_0(p_a)$ do not change due to the firing of ${}^\bullet p_a \setminus t$. Thus t can be diagnosed once $t_a \in p_a^\bullet$ fires.

Case 2: The N_f is FC and BCF. Several faults share one same input place. The fault t may not be identified from t_b, while a smaller region than T_f in which the fault belongs to can be determined. The property of BCF ensures that t can still be diagnosed once t_a fires.

Case 3: The N_f is BC and FCF. Since each fault has one different input place, the fault that may occur can be distinguished from t_b. Although several faults share one same output place, t can be diagnosed once t_a fires. □

3.2 Observer design

The purpose of the observer design for PN is to provide the marking estimates in the presence of faults. The following definition describes *consistent markings* as in Giua et al. (2004)

Definition 5: After the transition sequence ω has been observed, we define the set of *ω-consistent markings* $\mathcal{C}(\omega) = \{M | \exists M \in \mathbb{N}^{m^d}, M'[\omega\rangle M\}$ as the set of all markings in which the system may be given the observed behavior and the initial marking. □

Similarly to Giua et al. (2004), the partial information of the initial marking in discrete places is available in the form of macromarking defined as follows.

Definition 6: Assume that the set of places P^D can be written as the union of $r+1$ subsets: $P^D = P_0 \cup P_1 \cup \ldots \cup P_r$ such that $P_0 \cap P_j = \emptyset$, $\forall j > 0$. The number of tokens contained in $P_j (j > 0)$ is known to be b_j, while the number of tokens in P_0 is unknown. For each P_j, let v_j be its characteristic vector, i.e., $v_j(p) = 1$ if $p \in P_j$, else $v_j(p) = 0$. Let $V = [v_1, \ldots, v_r]$ and $b = [b_1, \ldots, b_r]$. The *macromarking* is defined as the set $\mathcal{V}(V, b) = \{M \in \mathbb{N}^{m^d} | V^T M = b\}$. □

Denote $\psi(\overrightarrow{t})$ as the set of all transition sequences that $\overrightarrow{t}$ may follow, with $\overrightarrow{t} = \{t_1, \ldots\}$ the set of faults (F1) that may fire after $\psi(\overrightarrow{t})$.

Assumption 1: If $\omega_i \in \psi(\overrightarrow{t})$, then all the faults in $\overrightarrow{t}$ share the same input place. □

Assumption 1 means that after we determine whether a fault from an input place occurs or not, the fault from another input place may fire. Otherwise, we just take into account the possible faults from one input place.

Based on the conditions in Lemma 1 and Assumption 1, the following algorithm provides the marking estimates in the form of consistent markings iteratively in spite of faults.

Algorithm 1: Marking estimation with event observation, initial macromarking and faults

1. *Let the initial estimates $M^e_{\omega_0}(p) = 0$, the initial complementary estimates $M^c_{\omega_0} = M^e_{\omega_0}$.*
2. *Let the initial bound $B_{\omega_0} = b - V^T M^e_{\omega_0}$, the initial complementary bound $B^c_{\omega_0} = B_{\omega_0}$.*
3. *Let $i = 1$.*
4. *Wait until $t_{\alpha i}$ fires.*
   If for $i \geq 2$, $t_{\alpha i} \in t_j^{\bullet\bullet}$, then
   $M^e_{\omega_{i-1}} = M^{cj}_{\omega_i}$, $B_{\omega_{i-1}} = B^{cj}_{\omega_i}$, go to 6.
   end if.
5. *If for $i \geq 2$, $\omega_i \in \psi(\overrightarrow{t})$ then*
   Let $M'_{\omega_i}(p) = \max\{M^e_{\omega_{i-1}}(p), Pre(p, t_{\alpha i})\}$,
   Let $M^e_{\omega_i} = M'_{\omega_i} + C(\cdot, t_{\alpha i})$, $B_{\omega_i} = B_{\omega_{i-1}} - V^T \cdot (M'_{\omega_i} - M^e_{\omega_{i-1}})$.
   Let $M^{cj\prime}_{\omega_{i+1}}(p) = \max\{M^{cj}_{\omega_i}(p), Pre(p, t_{\alpha i})\}$,
   Let $M^{cj}_{\omega_{i+1}} = M^{cj\prime}_{\omega_{i+1}} + C(\cdot, t_{\alpha i})$, $B^{cj}_{\omega_{i+1}} = B^{cj}_{\omega_i} - V^T \cdot (M^{cj\prime}_{\omega_{i+1}} - M^{cj}_{\omega_i})$, go to 9.
   end if.
6. *Let $M'_{\omega_i}(p) = \max\{M^e_{\omega_{i-1}}(p), Pre(p, t_{\alpha i})\}$.*
7. *Let $M^e_{\omega_i} = M^c_{\omega_i} = M'_{\omega_i} + C(\cdot, t_{\alpha i})$, $B_{\omega_i} = B^{cj}_{\omega_i} = B_{\omega_{i-1}} - V^T \cdot (M'_{\omega_i} - M^e_{\omega_{i-1}})$.*
8. *If $\exists \bar{p} \in t^\bullet_{\alpha i}$, and $t_1, \ldots, t_q \in T_f$, such that $\bar{p} \in^\bullet t_j, (1 \leq j \leq q)$ then*
   Let $M^{cj\prime}_{\omega_{i+1}}(\bar{p}) = \max\{M^e_{\omega_i}(\bar{p}), Pre(\bar{p}, t_j)\}$.
   Let $M^{cj}_{\omega_{i+1}} = M^{ci\prime}_{\omega_{i+1}} + C(\cdot, t_j)$, $B^{cj}_{\omega_{i+1}} = B^{cj}_{\omega_i} - V^T \cdot (M^{ci\prime}_{\omega_{i+1}} - M^{cj}_{\omega_i})$
   Let $M^c_{\omega_i} = \bigcup M^{cj}_{\omega_i}$, $B^c_{\omega_i} = \bigcup B^{cj}_{\omega_i}$.
   end if.
9. *Let $i = i + 1$, go to 4.* ■

Algorithm 1 is an extension of the algorithm in Giua et al. (2004) to the faulty case.The main idea behind Algorithm 1 is that, when we predicate that a fault may occur at next transition (steps 8 and 5), we consider all the possible markings that may be reached under this fault, which are recorded in the complementary marking estimates M^c_ω. When we determine the fault has occured (Step 4), M^c_ω will

be used to update the marking estimates M^e_ω. Otherwise, keep M^e_ω not changed (steps 6 and 7).

Remark 1: Algorithm 1 can also be extended to the case that the fault from m input places may occur. $2^m - 1$ complementary markings estimates need to be designed in this case. ◊

The set of consistent markings provided by Algorithm 1 is as follows.

Theorem 1: Suppose that Assumption 1 and all the conditions in Lemma 1 hold. Consider a PN with initial macromarking $\mathcal{V}(V, b)$, an observed transition sequence ω_i, the fault transition $t \in T_f$, and $M^e_{\omega_i}$, B_{ω_i} $M^c_{\omega_{i+1}}$, $B^c_{\omega_{i+1}}$ computed by Algorithm 1. The set of ω_i-consistent markings is

$$\mathcal{C}(\omega_i|V,b) = \begin{cases} \mathcal{C}_1 & \text{if } \omega_i \notin \psi(\overrightarrow{t}) \\ \mathcal{C}_1 \cup \mathcal{C}_2, & \text{if } \omega_i \in \psi(\overrightarrow{t}) \end{cases} \quad (1)$$

where $\mathcal{C}_1 \triangleq \left\{M \in N^{m^d} | V^T M = V^T M^e_{\omega_i} + B_{\omega_i}, M \geq M^e_{\omega_i}\right\}$, $\mathcal{C}_2 \triangleq \left\{M \in N^{m^d} | V^T M = V^T M^{cj}_{\omega_{i+1}} + B^{cj}_{\omega_{i+1}}, M \geq \min_j\{M^{cj}_{\omega_{i+1}}\}\right\}$.

Proof: For the case $\omega_i \notin \psi(\overrightarrow{t})$, i.e., no fault occurs. The proof is similar to Giua et al. (2004), which is omitted.

For the case $\omega_i \in \psi(\overrightarrow{t})$, we first consider that the T_f-subnet is FCF, i.e., only one possible fault t may occur after ω_i. In this case, ω_i-consistent markings $\mathcal{C}(\omega_i|V,b)$ should include the marking that may be reached under $\omega_i t$, This can be provided by $M^c_{\omega_i}$ and $B^c_{\omega_i}$ as follows.

Steps 6 and 7 in Algorithm 1 ensure $M^e_{\omega_i} = M^c_{\omega_i}$ and $B_{\omega_i} = B^c_{\omega_i}$ before t occurs. Let us show that $\mathcal{C}(\omega_i|V,b) = \{M \in N^{m^d} | V^T M = V^T M^c_{\omega_i} + B^c_{\omega_i}, M \geq M^e_{\omega_i}\} \Rightarrow \mathcal{C}(\omega_i t|V,b) = \{M \in N^{m^d} | V^T M = V^T M^c_{\omega_{i+1}} + B^c_{\omega_{i+1}}, M \geq M^e_{\omega_{i+1}}\}$. In fact, $\mathcal{C}(\omega_i t|V,b) = \{M \in N^{m^d} | \exists M' \in \mathcal{C}(\omega_i|V,b), M' \geq Pre(\cdot,t), M = M' + C(\cdot,t)\} = \{M \in N^{m^d} | \exists M', V^T M' = V^T M^c_{\omega_i} + B^c_{\omega_i}, M' \geq M^e_{\omega_i}, M' \geq Pre(\cdot,t), M = M' + C(\cdot,t)\}$, which together with the step 8 of Algorithm 1, leads to $M' \geq M^{c\prime}_{\omega_i}$. We further have from the step 8 that $V^T M^c_{\omega_i} + B^c_{\omega_i} = V^T M^{c\prime}_{\omega_{i+1}} + B^c_{\omega_{i+1}}$. Therefore, $\mathcal{C}(\omega_i t|V,b) = \{M \in N^{m^d} | \exists M', V^T M' = V^T M^{c\prime}_{\omega_{i+1}} + B^c_{\omega_{i+1}}, M' \geq M^e_{\omega_i}, M = M' + C(\cdot,t)\} = \{M \in N^{m^d} | V^T M = V^T M^c_{\omega_{i+1}} + B^c_{\omega_{i+1}}, M \geq M^e_{\omega_{i+1}}\}$.

For the case that the T_f-subnet is FC, it can be seen from the analysis above that $\mathcal{C}(\omega|V,b)$ defined in (1) includes all markings that may be reached by any fault t_j. Once we determined whether the fault occurs or not from Lemma 1, $\mathcal{C}(\omega|V,b)$ will be updated as in Algorithm 1, which always gives the set of all markings in which the system may be given the observed behavior. This completes the proof. □

Some properties about the observer of Algorithm 1 can also be discussed similar to Giua et al. (2004). We give the following two properties without proving them.

Proposition 1: Let ω_i be an observed transition sequence. The estimates computed by Algorithm 1 is a lower bound of actual marking. i.e., $\forall i, M^e_{\omega_i} \leq M'_{\omega_{i+1}} \leq M_{\omega_i}$. □

Proposition 2: Given M_{ω_i} and $M^e_{\omega_i}$, the estimation error $e(M_{\omega_i}, M^e_{\omega_i}) = \sum_{p \in P^D}(M_{\omega_i}(p) - M^e_{\omega_i}(p))$ is a monotonically nonincreasing function of ω_i. i.e., $e(M_{\omega_i}, M^e_{\omega_i}) \geq e(M_{\omega_{i+1}}, M^e_{\omega_{i+1}})$. □

4. FTC DESIGN

We first give the definition of generalized mutual exclusion constraints (GMEC) that have been considered in Giua et al. (2004), Iordache and Antsaklis (2006).

Definition 7: Given an integer matrix $L = [l_1 \dots l_s]$ with $l_j \in \mathbb{Z}^{m^d}$ and an integer vector $k = [k_1, \dots, k_s]$ with $l_j \in \mathbb{Z}$, a *GMEC* of the PN (L, k) defines the set of legal markings $\mathcal{L} = \{M \in \mathbb{N}^{m^d} | L^T \cdot M \leq k\}$. □

For the FTC objective of our application described in Section 2.2, we consider a set of *forbidden markings* $\mathcal{F} = \{M \in \mathbb{N}^{m^d} | M \notin \mathcal{L}\}$. Forbidden markings violate $\mathcal{L}$, which must be prevented from being reached (e.g., in the traffic light control, no more than one green light can be activated simultaneously).

4.1 Adaptive FTC scheme using observer

Based on the marking estimates and fault information provided by the observer of Algorithms 1, an adaptive FTC scheme is designed for PN as follows.

Assumption 2: The initial actual marking $M_0 \in \mathcal{L}$ □

Assumption 2 is quite general, if the initial situation violates the GMEC, the system would be destroyed at the beginning.

Algorithm 2: Computation of the PN based fault tolerant controller using observer

1. *Given the observed ω_i, solve for each $j (1 \leq j \leq s)$ the IPP*

$$\begin{cases} \max L_j^T \cdot M \\ s.t. \\ M \in \mathcal{C}(\omega_i|V,b) \\ M \in \mathcal{L} \end{cases} \quad (2)$$

and let h_j be its optimal solution.

2. *Update the FTC controller with*

$$\begin{cases} C_{cj} = -L_j C \\ M_{cj} = k_j - h_j \end{cases} \quad (3)$$

where C_{cj} and M_{cj} denote the incidence matrix and markings of the controller.

3. *Let $i = i + 1$, go to 1.* ■

Compared with the logical control design in Giua et al. (2004), Holloway and Krogh (1990), the control law (3) is based on place invariants Iordache and Antsaklis (2006), which is updated based on the consistent markings of the observer at each time when a normal discrete transition fires. Under this controller, some controllable discrete transitions are disabled such that $\mathcal{F}$ is never reached. The separate computation as in Holloway and Krogh (1990) is not required.

Theorem 2: Supposed that Assumptions 2 and all the conditions in Theorem 1 hold. The controller (3) guarantees that $\mathcal{F}$ is never reached in spite of fault $t \in p^\bullet$, if

$$M_{\omega_i t_j} \in \mathcal{L}, \forall t_j \in p^\bullet \tag{4}$$

Proof: Since $M_0 \in \mathcal{L}$ from Assumption 2, and the fault does not occur as the first transition from Lemma 1, based on the result in Iordache and Antsaklis (2006), the controller (3) ensure $M_{\omega_1} \in \mathcal{L}$.

As for $i \geq 2$, assume that t may follow ω_i, condition (4) guarantees that once a fault from input place p occurs, the GMEC is still not violated. On the other hand, under Assumption 1, only the faults from one input place is considered before it is determined to occur or not. So the controller (3) only disables the controllable normal transition rather than the fault transitions at each step. From Theorem 1, $\mathcal{C}(\omega_i|V,b)$ includes all markings that may be reached by possible faults after observed ω_i, which together with the result in Iordache and Antsaklis (2006) leads to that $\mathcal{F}$ is never reached in spite of faults. □

Remark 2 : The condition (4) is less restrictive than the general condition in most literatures e.g.,Iordache and Antsaklis (2006), where $L \cdot C(,T_{uo}) = 0$, i.e. the unobservable transition $t_{uo} \in T_{uo}$ can not change the markings in places that related to the GMEC. Our method can be applied even if $L \cdot C(,T_f) \neq 0$ as shown in the application. ◊

If T_f-subset is FC, i.e. some faults share the same input discrete place, then $\mathcal{C}(\omega_i|V,b)$ has to include more possible markings, which would lead to more restrictive controller. The following result can help to analyze the permissiveness of the controller.

Proposition 3: Suppose that the conditions in Theorem 2 holds. Let $\mathcal{C}(\omega_i)_{FC}$, $\mathcal{C}(\omega_i)_{FCF}$ be two sets of ω_i-consistent markings for the case that T_f-subset is FC and FC free respectively. The controller (3) based on $\mathcal{C}(\omega_i)_{FCF}$ is at least as permissive as that based on $\mathcal{C}(\omega_i)_{FC}$.

Proof: For all ω_i, Theorem 1 implies that $\mathcal{C}(\omega_i)_{FCF} \subseteq \mathcal{C}(\omega_i)_{FC}$, it follows that $h_{jFCF} \leq h_{jFC}$, where h_{jFCF}, h_{jFC} denote the solution of Algorithm 3 with respectively $\mathcal{C}(\omega_i)_{FCF}$ and $\mathcal{C}(\omega_i)_{FC}$, which, together with (3), leads to $M_{cjFCF} \leq M_{cjFC}$ i.e., the marking in control places under $\mathcal{C}(\omega_i)_{FCF}$ is equal to or less than that under $\mathcal{C}(\omega_i)_{FC}$. Based on the result in Iordache and Antsaklis (2006), it holds that more controllable transitions may be disabled under $\mathcal{C}(\omega_i)_{FC}$. This complete the proof. □

Remark 3: The observer-based controller may be more restrictive than that obtained when the actual marking is known. This may lead to a deadlock. The concept of *Siphon* can be used to prevent the PN from the deadlock as in Hsieh (2004),Giua et al. (2004),Iordache and Antsaklis (2006). ◊

5. APPLICATION

This section applies the proposed method to the traffic light control system as described in Section 2.2.

Let us come back to the PN model in Fig. 2. It can be obtained that $\mathcal{L} = \{M \in \mathbb{N}^{12} | M(g_1) + M(g_2) + M(g_3) \leq 1\}$, i.e., only one green light can be activated at one time. $\mathcal{L}_i = \{M \in \mathbb{N}^{12} | M(g_i) + M(r_j) + M(r_h) = 3, M(y_p) + M(r_q) + M(r_m) = 3, i \neq j \neq h, p \neq q \neq m$, with the green light sequence $g_1 \rightarrow g_2 \rightarrow g_3 \rightarrow g_1$, and $d_i^g = 57s, d_i^y = 3s, d_i^r = 120s\}$, i.e., if one green light or one yellow light is activated, the other two should be red lights. We also suppose that if more than one green light can be activated simultaneously, the green light that satisfies the prescribed sequence is chosen to avoid the conflict.

5.1 Healthy case

We first consider the fault-free case to show the performance of observer-based controller. The macromarking is

$$\begin{cases} M(g_1) + M(y_1) + M(r_1) = 1 \\ M(g_2) + M(y_2) + M(r_2) = 1 \\ M(g_3) + M(y_3) + M(r_3) = 1 \end{cases} \tag{5}$$

The initial marking is (100000100010) which is unknown. Fig. 3 shows the evolution of the estimation based on Algorithm 1, which shows that the estimates is the low bound of actual marking, and equal to the actual marking after t_6 fires, which verifies propositions 1 and 2. The Fig. 4 shows the controller designed from Algorithm 2. In the healthy case, the marking always belongs to $\mathcal{L}$.

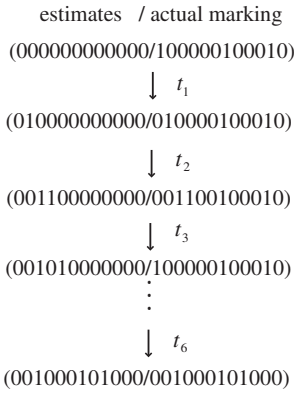

Fig. 3. Marking estimation

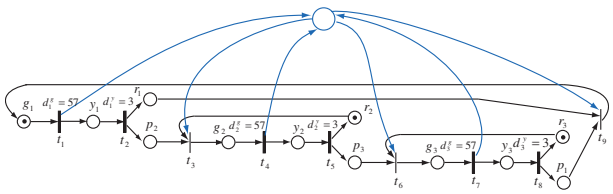

Fig. 4. PN in the healthy case

5.2 Faulty cases

We consider the following 2 faulty cases

Case 1: $t_f^1 \in T_f : r_1 \rightarrow y_1$ as shown in Fig. 5. In this case, after t_2 fired, more consistent markings have to be provided. Note that Assumption 1 is satisfied, since after t_2 fired, t_2 is impossible to fire again before t_9 or t_f^1 fires. If $t_f^1 : r_1 \rightarrow y_1$ really occurs, it can be diagnosed once t_2 fires as shown in Lemma 1. If t_9 fires before t_2, then it is determined that t^1 does not occur. The fault tolerant controller after t_2 fired is also given in Fig. 5. Such that t_f^1 does not violate the GMEC.

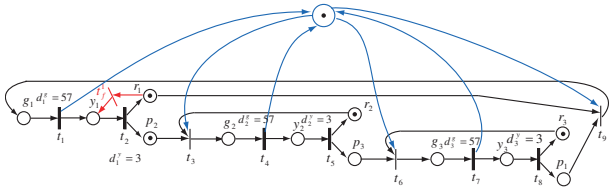

Fig. 5. PN in the faulty case 1

Case 2: $t_f^1 \in T_f : r_1 \rightarrow y_1$ and $t_f^2 : r_1 \rightarrow g_1$ as shown in Fig. 6. Note that $LC(, t_f^2) \neq 0$, which violate the condition in Iordache and Antsaklis (2006). The T_f-subnet is FC since t_f^1 and t_f^2 share the same input place r_1. Similarly more consistent markings will be provided by the observer after t_2 fired. However, the controller after t_2 fired, shown in Fig. 6 is less permissive than that in Case 1, due to possible fault t_f^2 which may activate g_1, the controller must disable t_3, i.e., the green light g_2 can not be activated. This verifies the Proposition 3. In fact, under t_f^2, the system gets deadlock unless t_f^2 really occurs.

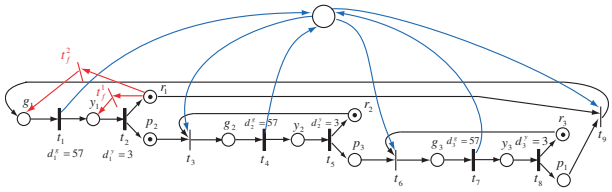

Fig. 6. PN in the faulty case 2

6. CONCLUSION

This paper discusses the FTC problem for discrete event systems modeled by PN with application to the traffic light control problem. The proposed observer-based adaptive FTC scheme has been shown effective to accommodate the fault represented by unobservable transitions. The future work will be focused on the FTC design for more general faults, e.g., marking variation due to faults in each place.

REFERENCES

F. Balduzzi and A. D. Febbraro. Combining fault detection and process optimization in manufacturing systems using first-order hybrid petri nets. pages 40–45. Proc. of IEEE International Conference Robotics and Automation, 2001.

A. Benveniste, E. Fabre, S. Haar, and C. Jard. Diagnosis of asynchronous discrete-event systems: an unfolding approach. *IEEE Trans. on Automatic Control*, 48(5): 714–727, 2003.

M. Blanke, M. Kinnaert, J. Lunze, and M. Staroswiecki. *Diagnosis and Fault-Tolerant Control*. Springer Verlag, Berlin, 2003.

A. D. Febbraro, D. Giglio, and N. Sacco. Urban traffic control structure based on hybrid petri nets. *IEEE Trans. on Intelligent Transportation Systems*, 5(4):224–237, 2004.

A. Giua and C. Seatzu. Fault detection for discrete event systems using petri nets with unobservable transitions. pages 6323–6328. Proc. of the joint 44th IEEE Conference on Decision and Control, European Control Conference, 2005.

A. Giua, C. Seatzu, and F. Basile. Observer-based state-feedback control of timed petri nets with deadlock recovery. *IEEE Trans. on Automatic Control*, 49(1): 17–29, 2004.

L. E. Holloway and B. H. Krogh. Synthesis of feedback logic for a class of controlled petri nets. *IEEE Trans. on Automatic Control*, 35(5):514–523, 1990.

F-S Hsieh. Fault-tolerant deadlock avoidance algorithm for assembly processes. *IEEE Trans. on Systems, Man, and Cybernetics-Part A: Systems and Humans*, 34(1): 65–79, 2004.

M. V. Iordache and P. J. Antsaklis. Supervision based on place invariants: a survey. *J. Discrete Event Dynamic Systems:Theory and Applications*, 16(4):451–492, 2006.

B. Jiang, M. Staroswiecki, and V. Cocquempot. Fault accommodation for a class of nonlinear dynamic systems. *IEEE Trans. on Automatic Control*, 51(9):1578–1583, 2006.

D. Lefebvre and C. Delherm. Diagnosis of des with petri net models. *IEEE Trans. on Automation Science and Engineering*, 4(1):114–118, 2007.

T. Murata. Petri nets: properties, analysis and applications. *Proc. IEEE*, 77(4):541–580, 1989.

A. Ramirez-Trevino, E. Ruiz-Beltran, I. Rivera-Rangel, and E. Lopez-Mellado. Online fault diagnosis of discrete event systems: a petri net-based approach. *IEEE Trans. on Automation Science and Engineering*, 4(1):31–39, 2007.

M. Sampath, S. Lafortune, and D. Teneketzis. Active diagnosis of discrete event systems. *IEEE Trans. Automatic Control*, 43(7):908–929, 1998.

Y. Wu and C. N. Hadjicostis. Algebraic approaches for fault identification in discrete-event systems. *IEEE Trans. on Automatic Control*, 50(12):2048–205, 2005.