IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received November 17, 2017, accepted December 24, 2017, date of publication January 23, 2018, date of current version March 9, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2792012

Event Feedback Supervision for a Class of Petri Nets With Unobservable Transitions

NING RAN[1], SHOUGUANG WANG[2], (Senior Member, IEEE), AND WENHUI WU[2]

[1]Machine Vision Engineering Research Center of Hebei Province, College of Electronic and Information Engineering, Hebei University, Baoding 071000, China
[2]School of Information and Electronic Engineering, Zhejiang Gongshang University, Hangzhou 310018, China

Corresponding author: Shouguang Wang (wsg5000@hotmail.com)

This work was supported in part by the Hebei University through "One province one university" Special Fund, in part by the National Natural Science Foundation of China under Grant 61603154 and Grant 61472361, and in part by the Zhejiang Natural Science Foundation under Grant LY15F030003.

ABSTRACT In this paper, we propose a method to design an on-line event feedback supervisor (EFS) for a class of Petri nets whose augmented unobservable subnets are acyclic forward synchronization and backward conflict-free (FSBCF) nets. In more detail, an FSBCF net is an ordinary Petri net in which each place has at most one output transition, and each transition has at most one input place. The designed EFS is able to compute a set of transitions that need to be forbidden based on the current observation of the system. In particular, the EFS is maximally permissive, i.e., it ensures that the controlled system never enters into illegal markings while minimally restricting its behavior. Finally, we use an example to illustrate the effectiveness of the proposed method.

INDEX TERMS Discrete event systems, Petri nets, forbidden states, supervisory control.

I. INTRODUCTION

With the improvement of resource utilization efficiency, the problem of preventing certain states (called *forbidden states*) often arises in a discrete event system (DES). Putting the system in such states may reduce the production efficiency or even result in a catastrophic consequence. Solving the *forbidden state problem* consists in designing a supervisor to prevent the system entering into forbidden states. Due to the intuitive graphical representation and powerful algebraic formulation, Petri nets have been widely used in dealing with such a problem [1]–[21].

In the Petri net framework, the set of legal states is typically formalized as *generalized mutual exclusion constraints (GMECs)* [4]. In detail, a GMEC is defined as a constraint that limits a weighted sum of tokens contained in a subset of places. The markings that satisfy the given GMECs are said to be *legal markings*, otherwise they are called *illegal (forbidden) markings*. If the transitions in a Petri net are all controllable and observable, the given GMECs can be easily enforced on the Petri net by a set of additional places, called *monitors*, which guarantees maximal permissiveness. Yamalidou *et al.* [5] design monitors using the notion of place invariance.

For a Petri net with uncontrollable transitions, the complexity of the forbidden state problem is enhanced since it is possible that a legal marking reaches a forbidden marking by firing uncontrollable transitions. In such a case, the designed supervisor must restrict the evolution of the system within the set of *admissible markings*. Moody and Antsaklis [7] present the notion of *admissible GMECs*, which describes a subset of admissible markings. They provide an algorithm to transform given inadmissible GMECs into admissible ones, which can be directly enforced on the net in the form of monitors using the place invariance approach proposed in [5].

Chen [11] proposes the concept of *uncontrollable influence subnet*, and proves that GMECs can be transformed in terms of the uncontrollable influence subnet only. It significantly reduces the computational complexity of the problem. Luo *et al.* [12] transform GMECs into admissible GMECs for Petri nets whose uncontrollable influence subnets are *forward conflict-free (FCF) nets*. Although the transformation is optimal, it is based on the notion of *crux path* whose computation is exponential w.r.t. the structure of the Petri nets. To reduce the computational complexity of the method in [12], Wang *et al.* [13] propose a new optimal transformation method with polynomial complexity for the Petri nets whose uncontrollable influence subnets are FSBCF nets.

Since the firing of an unobservable transition cannot be detected, all unobservable transitions are also implicity

uncontrollable [7]. Literature that focuses on forbidden state problem of Petri nets with unobservable transitions is insufficient either in breadth or in depth. Luo and Zhou [14] propose a method based on constraint transformation to enforce linear constraints on Petri nets with unobservable transitions and uncontrollable transitions. In particular, they provide an algorithm to equivalently transform linear constraints into admissible dynamic constraints for a Petri net whose uncontrollable subnet is a state machine.

In this paper we design an on-line *event feedback supervisor* to enforce a given GMEC on a Petri net whose *augmented unobservable subnet* is an acyclic FSBCF net. In more detail, the supervisor takes advantage of the structural properties of such type of nets, and computes the set of transitions that need to be forbidden according to the current observation. It minimally restricts the behavior of the net while ensuring that the closed-loop system never reaches the set of forbidden markings.

The paper is organized as follows. Section II provides some background on Petri nets and introduces the notations used in the paper. In Section III, we first recall the notions of GMEC and augmented unobservable subnet, then introduce the notion of event feedback supervisor. Section IV provides an algorithm for designing a maximally permissive event feedback supervisor. An example is given in Section V to illustrate the effectiveness of the algorithm. Finally, Section VI concludes the paper and points out the line of our future research in this area.

II. PRELIMINARIES

In this section, some basic notions of Petri nets are reviewed. They are taken from [22] and [23].

An ordinary Petri net (PN) is a 3-tuple $N = (P, T, F)$, where P is the set of places and T is the set of transitions. $F \subseteq (P \times T) \cup (T \times P)$ is called the flow relation of the net. Let $a \in P \cup T$ be a node of net N. The preset of a is defined as ${}^\bullet a = \{b \in P \cup T \mid (b, a) \in F\}$. While the postset of a is defined as $a^\bullet = \{b \in P \cup T \mid (a, b) \in F\}$. A transition without any input (output) place is called a source (sink) transition. A place without any input (output) transition is called a source (sink) place. $\forall A \subseteq P \cup T$, ${}^\bullet A = \bigcup_{a \in A} {}^\bullet a$, and $A^\bullet = \bigcup_{a \in A} a^\bullet$. The incidence matrix $[N]$ of N is a $|P| \times |T|$ integer matrix such that $[N](p, t) = 1$ if $p \in t^\bullet \setminus {}^\bullet t$, $[N](p, t) = -1$ if $p \in {}^\bullet t \setminus t^\bullet$, otherwise, $[N](p, t) = 0$. For a place p (transition t), its incidence vector is denoted by $[N](p, \cdot)$ ($[N](\cdot, t)$).

A marking m of a PN N is a mapping from P to $\mathbb{N} = 0, 1, 2, \ldots$: $m(p)$ denotes the number of tokens in place p. (N, m_0) denotes a PN system with an initial marking m_0.

A transition t is enabled at a marking m if $\forall p \in {}^\bullet t$, $m(p) \geq 1$. This fact is denoted by $m[t\rangle$, while $m[\sigma\rangle$ is used to denote that the transition sequence $\sigma = t_1 t_2 \ldots t_k$ is enabled at m. We denote $\pi : T^* \to \mathbb{N}^{|T|}$ the function that associates to σ a vector $y = \pi(\sigma) \in \mathbb{N}^{|T|}$, namely the firing vector of σ, where $y(t) = k$ if transition t is contained k times in σ. The set of all sequences that are enabled at the initial marking m_0 is denoted by $L(N, m_0)$, i.e., $L(N, m_0) = \{\sigma \in T^* \mid m_0[\sigma\rangle\}$. ε is used to denote the empty sequence.

Firing t yields a new marking m' such that $\forall p \in P$, $m'(p) = m(p) + [N](p, t)$, which is denoted by $m[t\rangle m'$. Marking m'' is said to be reachable from m if there exists a transition sequence σ such that $m[\sigma\rangle m''$. The set of markings reachable from m in N is called the reachability set of (N, m) and is denoted by $R(N, m)$.

A string $a_1, a_2, \ldots, a_n$ is called a path if $a_{i+1} \in a_i^\bullet$, where $a_i \in P \cup T$ and $i \in \{1, 2, \ldots, n-1\}$. If there exists a path from a_i to a_j, we say that a_i can access a_j, or a_j can be accessed from a_i. Note that each node can access itself. A circuit is a path in which the first and last nodes are identical. A PN with no directed circuits is said to be acyclic.

A transition is called uncontrollable if its firing cannot be forbidden, and a transition is called unobservable if its firing cannot be detected. Since the firing of an unobservable transition cannot be detected, all unobservable transitions are also implicity uncontrollable. On the other hand, an uncontrollable transition may or may not be unobservable [7]. Therefore, the set T of transitions in a PN is partitioned into three disjoints subsets: $T = T_{co} \cup T_{ouc} \cup T_{uo}$, where T_{co} is the set of controllable and observable transitions, T_{ouc} is the set of observable but uncontrollable transitions, and T_{uo} is the set of unobservable transitions. In this paper, we study a class of PNs whose observable transitions are also controllable, i.e., $T_{ouc} = \emptyset$ and $T_{co} = T_o$, where T_o is the set of observable transitions. Hence, we simply write $T = T_o \cup T_{uo}$.

Given a transition sequence $\sigma \in T^*$, we denote $P_o(\sigma)$ the projection of σ over T_o, and $\nu = P_o(\sigma)$ the corresponding (observed) word. Word $u \in T_o^*$ is a *prefix* of $\nu \in T_o^*$ if there exists $u' \in T_o^*$ such that $\nu = uu'$.

Given a word $\nu \in (T_o)^*$, we denote

$$\mathcal{S}(\nu) = \{\sigma \in L(N, m_0) \mid P_o(\sigma) = \nu\}$$

the set of transition sequences *consistent* with ν; and

$$\mathcal{C}(\nu) = \{m \mid m_0[\sigma\rangle m,\ \sigma \in \mathcal{S}(\nu)\}$$

the set of reachable markings *consistent* with ν.

A *forward synchronization and backward conflict-free (FSBCF)* net is an ordinary PN in which each place has at most one output transition, and each transition has at most one input place. Since there is no transition has more than one input places in an FSBCF net, a token may flow downstream along each unobservable path, no matter what the distribution of the other tokens is [12].

III. PROBLEM STATEMENT

In this section, we first recall the notions of GMEC, then propose the definition of augmented unobservable subnet and the definition of event feedback supervisor.

A. GMEC

In the PN framework, a control specification may be typically formalized as GMECs [4].

Definition 1 [4]: A *generalized mutual exclusion constraint (GMEC)* is a couple (ω, k), where $\omega \in \mathbb{N}^{1 \times |P|}$ is

a vector that assigns to each place a non-negative number; $k \in \mathbb{N}$, such that $\omega \cdot m \leq k$.

We denote $\omega(p)$ the number assigned to place p, and $P_f = \{p \in P \mid \omega(p) \neq 0\}$ the set of *forbidden places*. For the sake of simplicity, we assume that there is only one forbidden place in the PN, i.e., $P_f = \{p_f\}$, where p_f is the forbidden place.

Given a PN system (N, m_0) with a GMEC (ω, k), the set of *legal markings* is

$$\mathcal{L}(\omega, k) = \{m \in R(N, m_0) \mid \omega \cdot m \leq k\}.$$

The set of *illegal (forbidden) markings* is

$$\overline{\mathcal{L}}(\omega, k) = \{m \in R(N, m_0) \mid \omega \cdot m > k\}.$$

In fact, some legal markings may inevitably reach forbidden markings by firing only unobservable transitions. In the following we call the legal marking set not containing such markings *admissible marking set*, which is denoted by $\mathcal{A}(\omega, k)$, i.e., it is

$$\mathcal{A}(\omega, k) = \{m \in \mathcal{L}(\omega, k) \mid \nexists \sigma \in (T_{uo})^* : m[\sigma\rangle m' \wedge m' \in \overline{\mathcal{L}}(\omega, k)\}.$$

To guarantee safeness it is necessary to restrict the net's evolution within the admissible marking set.

B. AUGMENTED UNOBSERVABLE SUBNET

Now we introduce the definition of augmented unobservable subnet.

Definition 2: Let (N, m_0) be a PN with a GMEC (ω, k), and P_f the set of forbidden places. $(N_\omega, \widetilde{m}_0)$ is the *augmented unobservable subnet* of N, where $N_\omega = (P_\omega, T_\omega, F_\omega)$ and

- $P_\omega \subseteq P$ is the set of places that satisfy the following conditions:
  - $P_f \subseteq P_\omega$;
  - If $p \in P_\omega$ and $t \in {}^\bullet p \cap T_{uo}$, then ${}^\bullet t \subseteq P_\omega$;
  - If $p \in P_\omega$ and $t \in p^\bullet \cap T_{uo}$, then $t^\bullet \subseteq P_\omega$.
- $T_\omega = {}^\bullet P_\omega \cup P_\omega{}^\bullet$;
- F_ω is the restriction of F to $(P_\omega \times T_\omega) \cup (T_\omega \times P_\omega)$;
- $\forall p \in P_\omega,\ \widetilde{m}_0(p) = m_0(p)$.

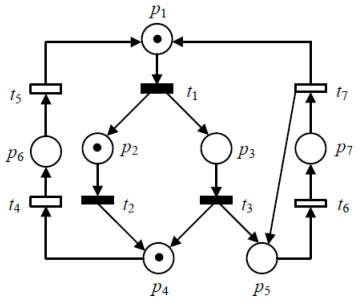


FIGURE 1. A PN system.

Example 1: Consider the PN system shown in Fig. 1 with a GMEC (ω, k), where $T_o = \{t_4 - t_7\}$, $T_{uo} = \{t_1 - t_3\}$, $\omega = (0, 0, 1, 0, 0, 0, 0)$ and $k = 2$. The forbidden place is p_3. The augmented unobservable subnet $(N_\omega, \widetilde{m}_0)$ is shown in Fig. 2, where $P_\omega = \{p_1 - p_5\}$, $T_\omega = \{t_1 - t_7\}$.

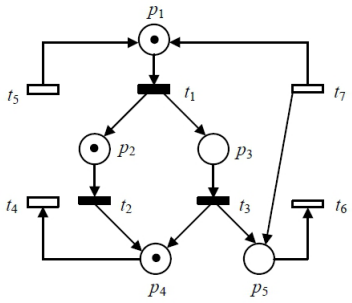


FIGURE 2. The augmented unobservable subnet of the PN in Fig 1.

By Definition 2, we know that a source unobservable transition in N_ω is also a source transition in N. Since a source unobservable transition cannot be detected and forbidden by an external agent, it may be impossible to design an admissible supervisor to enforce a GMEC on the PN. In the remaining discussion, we assume that N_ω contains no source unobservable transitions.

C. EVENT FEEDBACK SUPERVISOR

We define a *control input* as a subset $\gamma \subseteq T_o$, in which all transitions are forbidden to occur. An event feedback supervisor is defined as follows.

Definition 3: Let $\Gamma \subseteq 2^{T_o}$ be the set of all possible control inputs. An *event feedback supervisor (EFS)* is a mapping:

$$f : (T_o)^* \to \Gamma.$$

In other words, an EFS consists in selecting a set γ of observable transitions to forbid, in response to an observed word $\nu \in (T_o)^*$. In the following, we denote $(N, m_0)|f$ the *controlled PN system*, i.e., the PN system that is under the supervision of the EFS f.

A word $\nu \in (T_o)^*$ is said to be *admissible* if $\forall \nu' \in prefix(\nu),\ \mathcal{C}(\nu') \in \mathcal{A}(\omega, k)$.

Definition 4: An EFS f is *admissible* if all words generated by $(N, m_0)|f$ are admissible.

In other words, an EFS is admissible if $(N, m_0)|f$ evolves only within the admissible marking set.

Definition 5: An EFS f is *maximally permissive* if

1) It is admissible, and
2) For any admissible EFS f' and for any admissible word ν, it holds that $f(\nu) \subseteq f'(\nu)$.

Given a PN system $(N, m_0, \mathcal{L})$ whose augmented unobservable subnet is an FSBCF net, and a GMEC (ω, k), our objective is to design a maximally permissive EFS f to enforce the GMEC on the PN system. In particular, we make the following assumptions.

A1) The structure of PN N and the initial marking m_0 are known, and m_0 is admissible, i.e., $m_0 \in \mathcal{A}(\omega, k)$.
A2) There is only one forbidden place in the PN.
A3) The augmented unobservable subnet is acyclic.

Remark 1: From [13], we know that there may exist *A-circuits* in an FSBCF net, which may produce at most an infinite number of tokens. Assumption A3 is necessary to avoid dealing with such a case.

IV. MAIN RESULTS

In this section, we propose a method to design a maximally permissive EFS.

A. BASIC NOTATIONS

Given two nodes $a, b \in P_\omega \cup T_\omega$, we use $\Pi(a, b)$ to denote the set of paths in $(N_\omega, \widetilde{m}_0)$ satisfying the following three conditions:

1) $a \neq b$,
2) the head node and the ending node of the path are a and b, respectively,
3) between a and b (except a and b) there are no transitions in the path, or between a and b (except a and b) all transitions in the path are unobservable.

Example 2: Consider again the augmented unobservable subnet in Fig. 2, we have $\Pi(t_7, p_5) = \{t_7p_1t_1p_3t_3p_5, t_7p_5\}$ and $\Pi(t_7, t_4) = \{t_7p_1t_1p_2t_2p_4t_4, t_7p_1t_1p_3t_3p_4t_4\}$.

After observing a word ν, since p_f may acquire or lose tokens via unobservable paths, we need to compute the maximum number of tokens that may contained in p_f (denoted by $\mathcal{M}_{p_f}(\nu)$ hereinafter). Obviously, by Definition 2, the observable transitions whose firing may influence such a number belong to T_ω.

We define the following notions of *increasing place* (the place that can access p_f via an unobservable path), *increasing transition* (the observable transition that is the input of p_f or that can access p_f via an unobservable path) and *decreasing transition* (the observable transition that is the output of p_f or that can be accessed from p_f via an unobservable path).

Definition 6: Let p_f be a forbidden place. We define the set of

- *increasing places* of p_f as

$$\mathcal{P}_I(\cdot, p_f) = \{p \in P_\omega \mid \Pi(p, p_f) \neq \emptyset\}. \tag{1}$$

- *increasing transitions* of p_f as

$$\mathcal{T}_I(\cdot, p_f) = \{t \in T_\omega \cap T_o \mid \Pi(t, p_f) \neq \emptyset\}. \tag{2}$$

- *decreasing transitions* of p_f as

$$\mathcal{T}_D(p_f, \cdot) = \{t \in T_\omega \cap T_o \mid \Pi(p_f, t) \neq \emptyset\}. \tag{3}$$

The forbidden place p_f can obtain tokens from the places in $\mathcal{P}_I(\cdot, p_f)$ and the firing of transitions in $\mathcal{T}_I(\cdot, p_f)$. In particular, since N_ω is an acyclic FSBCF net, a token may flow downstream into p_f along each unobservable path, no matter what the distribution of the other tokens is. We denote $\Phi(\nu)$ as the maximum number of tokens that p_f can obtain from the places in $\mathcal{P}_I(\cdot, p_f)$ and the firing of transitions in $\mathcal{T}_I(\cdot, p_f)$ after a word ν. Clearly, the following two equations hold:

$$\Phi(\varepsilon) = \sum_{p \in \mathcal{P}_I(\cdot, p_f)} \widetilde{m}_0(p) \cdot |\Pi(p, p_f)|, \tag{4}$$

$$\Phi(\nu) = \sum_{p \in \mathcal{P}_I(\cdot, p_f)} \widetilde{m}_0(p) \cdot |\Pi(p, p_f)| + \sum_{t \in \mathcal{T}_I(\cdot, p_f)} y(t) \cdot |\Pi(t, p_f)|, \tag{5}$$

where $y = \pi(\nu)$.

Example 3: Consider again the augmented unobservable subnet in Fig. 2. By Definition 6, we have $\mathcal{P}_I(\cdot, p_3) = \{p_1\}$, $\mathcal{T}_I(\cdot, p_3) = \{t_5, t_7\}$ and $\mathcal{T}_D(p_3, \cdot) = \{t_4, t_6\}$. Moreover, $\Phi(\varepsilon) = 1$ and $\Phi(t_5t_7) = 3$.

The firing of an increasing transition can increase the maximum number of tokens in p_f for sure. However, the firing of a decreasing transition t does not necessarily decrease the maximum number of tokens in p_f. The reason consists in some places or the firing of some transitions may also increase the number of tokens in the set ${}^\bullet t$ of places via unobservable paths.

Given two nodes $a, b \in P_\omega \cup T_\omega$, we use $\widetilde{\Pi}(a, b)$ to denote the set of paths in $(N_w, \widetilde{m}_0)$ satisfying the following four conditions:

1) $a \neq b$,
2) the head node and the ending node of the path are a and b, respectively,
3) between a and b (except a and b) there are no transitions in the path, or between a and b (except a and b) all transitions in the path are unobservable,
4) the path does not contain forbidden places.

Example 4: Reconsider the augmented unobservable subnet in Fig. 2. We have $\widetilde{\Pi}(t_7, p_5) = \{t_7p_5\}$ and $\widetilde{\Pi}(t_7, t_4) = \{t_7p_1t_1p_2t_2p_4t_4\}$.

Now we define the following notions of *influencing place* (the place that is the input of t or that can access t via an unobservable path in which each place is not a forbidden place) and *influencing transition* (the observable transition that can access t via an unobservable path in which each place is not a forbidden place).

Definition 7: Let t be a decreasing transition of p_f. i.e., $t \in \mathcal{T}_D(p_f, \cdot)$. We define the set of

- *influencing places* of t as

$$\mathcal{P}_{ID}(\cdot, t) = \{p \in P_\omega \setminus P_f \mid \widetilde{\Pi}(p, t) \neq \emptyset\}. \tag{6}$$

- *influencing transitions* of t as

$$\mathcal{T}_{ID}(\cdot, t) = \{t' \in T_\omega \cap T_o \mid \widetilde{\Pi}(t', t) \neq \emptyset\}. \tag{7}$$

For any $t \in \mathcal{T}_D(p_f, \cdot)$, the place in ${}^\bullet t$ is able to obtain tokens from i) the place p_f, ii) the places in $\mathcal{P}_{ID}(\cdot, t)$, and iii) the firing of transitions in $\mathcal{T}_{ID}(\cdot, t)$. We denote $\Psi_t(\nu)$ the maximum number of tokens in the place in ${}^\bullet t$ that obtained from the places in $\mathcal{P}_{ID}(\cdot, t)$ and the firing of transitions in $\mathcal{T}_{ID}(\cdot, t)$. Clearly, the followings two equations hold:

$$\Psi_t(\varepsilon) = \sum_{p \in \mathcal{P}_{ID}(\cdot, t)} \widetilde{m}_0(p) \cdot |\widetilde{\Pi}(p, t)|, \tag{8}$$

$$\Psi_t(v) = \sum_{p\in\mathcal{P}_{ID}(\cdot,t)} \widetilde{m}_0(p)\cdot|\widetilde{\Pi}(p,t)| + \sum_{t'\in\mathcal{T}_{ID}(\cdot,t)} y(t')\cdot|\widetilde{\Pi}(t',t)|, \quad (9)$$

where $y = \pi(v)$.

Example 5: Consider again the augmented unobservable subnet in Fig. 2. By Definition 7, we have $\mathcal{P}_{ID}(\cdot,t_4) = \{p_1,p_2,p_4\}$, $\mathcal{P}_{ID}(\cdot,t_6) = \{p_5\}$, $\mathcal{T}_{ID}(\cdot,t_4) = \{t_5,t_7\}$ and $\mathcal{T}_{ID}(\cdot,t_6) = \{t_7\}$. Moreover, $\Psi_{t_4}(\varepsilon) = 3$ and $\Psi_{t_4}(t_5t_7) = 5$.

Theorem 1: Let $(N_\omega,\widetilde{m}_0)$ be an augmented unobservable subnet, v be an observed word and $y = \pi(v)$. Let $\mathcal{M}_{p_f}(v)$ be the maximum number of tokens in p_f after the observed word v.

1) Let $v = \varepsilon$, it holds that

$$\mathcal{M}_{p_f}(\varepsilon) = \widetilde{m}_0(p_f) + \Phi(\varepsilon). \quad (10)$$

2) Let $t \in \mathcal{T}_I(\cdot,p_f)$, it holds that

$$\mathcal{M}_{p_f}(vt) = \mathcal{M}_{p_f}(v) + |\Pi(t,p_f)|. \quad (11)$$

3) Let $t \in \mathcal{T}_{ID}(\cdot,t)\setminus\mathcal{T}_I(\cdot,p_f)$, it holds that

$$\mathcal{M}_{p_f}(vt) = \mathcal{M}_{p_f}(v). \quad (12)$$

4) Let $t \in \mathcal{T}_D(p_f,\cdot)$, we have

a) if

$$[\Phi(v) - \mathcal{M}_{p_f}(v)]\cdot|\Pi(p_f,t)| + \Psi_t(v) - y(t) > 0, \quad (13)$$

then it holds that

$$\mathcal{M}_{p_f}(vt) = \mathcal{M}_{p_f}(v). \quad (14)$$

b) if

$$[\Phi(v) - \mathcal{M}_{p_f}(v)]\cdot|\Pi(p_f,t)| + \Psi_t(v) - y(t) \le 0, \quad (15)$$

then it holds that

$$\mathcal{M}_{p_f}(vt) = \mathcal{M}_{p_f}(v) - 1. \quad (16)$$

Proof: Conditions 1) to 3) follow from the fact that N_ω is an acyclic FSBCF net, and a token may flow downstream along each unobservable path no matter what the distribution of the other tokens is.

After the word v, the place in ${}^\bullet t$ obtains at most $[\Phi(v) - \mathcal{M}_{p_f}(v)]\cdot|\Pi(p_f,t)|$ tokens from p_f, and at most $\Psi_t(v)$ tokens from the places in $\mathcal{P}_{ID}(\cdot,t)$ and the firing of transitions in $\mathcal{T}_{ID}(\cdot,t)$. Therefore, the number of tokens in the place in ${}^\bullet t$ is at most $[\Phi(v) - \mathcal{M}_{p_f}(v)]\cdot|\Pi(p_f,t)| + \Psi_t(v) - y(t)$. Inequation (13) means that the place in ${}^\bullet t$ may have enough tokens to enable t. Otherwise, at least a token in p_f flows downstream into the place in ${}^\bullet t$ to enable t. Hence, condition 4) holds. □

B. ON-LINE EFS DESIGN

An admissible EFS f must ensure that any observed word v generated by $(N,m_0)|f$ satisfies:

$$\omega(p_f)\cdot\mathcal{M}_{p_f}(v) \le k. \quad (17)$$

We design the EFS f using Algorithm 1.

Algorithm 1 [On-Line EFS Design]

Input: A system $(N,m_0,\mathcal{L})$ with a GMEC (ω,k).
Output: An on-line EFS f.
1. Compute the augmented unobservable subnet $(N_\omega,\widetilde{m}_0)$.
2. Compute the sets $\mathcal{P}_I(\cdot,p_f)$, $\mathcal{T}_I(\cdot,p_f)$ and $\mathcal{T}_D(p_f,\cdot)$.
3. For all $t\in\mathcal{T}_D(p_f,\cdot)$, compute $\mathcal{P}_{ID}(\cdot,t)$ and $\mathcal{T}_{ID}(\cdot,t)$.
4. Let $v=\varepsilon$ and $f(v)=\emptyset$.
5. Compute $\Phi(v)$ and $\mathcal{M}_{p_f}(v)$ using (4) and (10), respectively.
6. **While** *true*, **do**
6.1 **for** all $t\in\mathcal{T}_I(\cdot,p_f)$, **do**
- compute $\mathcal{M}_{p_f}(vt)$ using (11).
- **if** $\mathcal{M}_{p_f}(vt)\cdot\omega(p_f) > k$, **then**
  $f(v) = f(v)\cup\{t\}$.
  end if

end for
6.2 all transitions in $f(v)$ are forbidden to occur, and wait until a new observable transition $t\in T_o\setminus f(v)$ fires.
6.3 **if** $t\in\mathcal{T}_I(\cdot,p_f)$, **then**
- compute $\mathcal{M}_{p_f}(vt)$ using (11).

end if
6.4 **if** $t\in\mathcal{T}_{ID}(\cdot,t)\setminus\mathcal{T}_I(\cdot,p_f)$, **then**
- compute $\mathcal{M}_{p_f}(vt)$ using (12).

end if
6.5 **if** $t\in\mathcal{T}_D(p_f,\cdot)$, **then**
- compute $\Phi(v)$ and $\Psi_t(v)$ using (5) and (9), respectively.
- **if** (13) holds, **then**
  compute $\mathcal{M}_{p_f}(vt)$ using (14).
  else
  compute $\mathcal{M}_{p_f}(vt)$ using (16).
  end if

end if
6.6 let $v = vt$ and $f(v)=\emptyset$.
end while.

Theorem 2: Let (N,m_0) be a PN system with a GMEC (ω,k). The EFS f designed by Algorithm 1 is maximally permissive.

Proof: The proof includes two parts, i.e., 1) the EFS f is admissible, and 2) for any admissible EFS f' and any admissible word v, it holds that $f(v)\subseteq f'(v)$.

Condition 1) follows from the facts that m_0 is admissible (by assumption A1), and that after each observation all observable transitions leading the system to a non-admissible

marking are forbidden to occur (by Step 6.1 and Step 6.2 of Algorithm 1).

By contradiction, assume that there exists an admissible EFS f' and an admissible word ν such that $f(\nu) \supset f'(\nu)$. Let $t \in f(\nu) \setminus f'(\nu)$. The transition t is allowed to occur by f' but forbidden to occur by f. By Algorithm 1, it must hold that

$$\mathcal{M}_{p_f}(\nu t) \cdot \omega(p_f) > k.$$

In other words, the controlled PN system $(N, m_0)|f'$ may enter into a forbidden marking after the word νt. Therefore, f' is not admissible. This is a contradiction. □

We conclude this section with a brief discussion on the complexity of the proposed method. From Algorithm 1, we know that the most burdensome part consists in computing the sets: $\mathcal{P}_I(\cdot, p_f)$, $\mathcal{T}_I(\cdot, p_f)$, $\mathcal{T}_D(p_f, \cdot)$, $\mathcal{P}_{ID}(\cdot, t)$ and $\mathcal{T}_{ID}(\cdot, t)$, whose complexity is polynomial w.r.t. the sum of the number of nodes and the number of arcs in the PN. In fact, the computation of such sets is quite simple since the augmented unobservable subnet is an acyclic FSBCF net. In particular, this part may be moved off-line. The on-line part of the EFS is also with low computational cost since it only performs some simple algebraic operations after each observed transition.

V. EXAMPLE

In this section, we continue to consider the PN system in Example 1, where $\omega = (0, 0, 1, 0, 0, 0, 0)$ and $k = 2$. We design the EFS f using Algorithm 1. The procedures are detailed as follows.

1) We first compute the sets introduced in Section IV-A:
   - $\mathcal{P}_I(\cdot, p_3) = \{p_1\}$ and $\Pi(p_1, p_3) = \{p_1 t_1 p_3\}$.
   - $\mathcal{T}_I(\cdot, p_3) = \{t_5, t_7\}$, $\Pi(t_5, p_3) = \{t_5 p_1 t_1 p_3\}$ and $\Pi(t_7, p_3) = \{t_7 p_1 t_1 p_3\}$.
   - $\mathcal{T}_D(p_3, \cdot) = \{t_4, t_6\}$, $\Pi(p_3, t_4) = \{p_3 t_3 p_4 t_4\}$ and $\Pi(p_3, t_6) = \{p_3 t_3 p_5 t_6\}$.
   - $\mathcal{P}_{ID}(\cdot, t_4) = \{p_1, p_2, p_4\}$, $\widetilde{\Pi}(p_1, t_4) = \{p_1 t_1 p_2 t_2 p_4 t_4\}$, $\widetilde{\Pi}(p_2, t_4) = \{p_2 t_2 p_4 t_4\}$, $\widetilde{\Pi}(p_4, t_4) = \{p_4 t_4\}$; $\mathcal{P}_{ID}(\cdot, t_6) = \{p_5\}$, $\widetilde{\Pi}(p_5, t_6) = \{p_5 t_6\}$.
   - $\mathcal{T}_{ID}(\cdot, t_4) = \{t_5, t_7\}$, $\widetilde{\Pi}(t_5, t_4) = \{t_5 p_1 t_1 p_2 t_2 p_4 t_4\}$, $\widetilde{\Pi}(t_7, t_4) = \{t_7 p_1 t_1 p_2 t_2 p_4 t_4\}$; $\mathcal{T}_{ID}(\cdot, t_6) = \{t_7\}$, $\widetilde{\Pi}(t_7, t_6) = \{t_7 p_5 t_6\}$.
2) Let $\nu = \varepsilon$. It is $\mathcal{M}_{p_3}(\varepsilon) = 1$. Let $\nu' = t_5$ and $\nu'' = t_7$.
   - Consider the sequence ν'. We compute $\mathcal{M}_{p_3}(t_5)$ using (11) and $\mathcal{M}_{p_3}(t_5) = 2$.
   - Consider the sequence ν''. We compute $\mathcal{M}_{p_3}(t_7)$ using (11) and $\mathcal{M}_{p_3}(t_7) = 2$.

   By Algorithm 1, $f(\nu) = \emptyset$.
3) Let $\nu = t_7$. Compute $\mathcal{M}_{p_3}(t_7)$ using (11) and $\mathcal{M}_{p_3}(t_7) = 2$. Let $\nu' = t_7 t_5$ and $\nu'' = t_7 t_7$.
   - Consider the sequence ν'. We compute $\mathcal{M}_{p_3}(\nu')$ using (11) and $\mathcal{M}_{p_3}(\nu') = 3$.
   - Consider the sequence ν''. We compute $\mathcal{M}_{p_3}(\nu'')$ using (11) and $\mathcal{M}_{p_3}(\nu'') = 3$.

   By Algorithm 1, both t_5 and t_7 should be forbidden to occur, i.e., $f(\nu) = \{t_5, t_7\}$.
4) Let $\nu = t_7 t_6$. By (5) and (9), we have $\Phi(t_7) = 2$ and $\Psi_{t_6}(t_7) = 1$. Since $[\Phi(t_7) - \mathcal{M}_{p_3}(t_7)] \cdot 1 + \Psi_{t_6}(t_7) - 0 > 0$, we compute $\mathcal{M}_{p_3}(t_7 t_6)$ using (14) and $\mathcal{M}_{p_3}(t_7 t_6) = \mathcal{M}_{p_3}(t_7) = 2$. Let $\nu' = t_7 t_6 t_5$ and $\nu'' = t_7 t_6 t_7$.
   - Consider the sequence ν'. We compute $\mathcal{M}_{p_3}(\nu')$ using (11) and $\mathcal{M}_{p_3}(\nu') = 3$.
   - Consider the sequence ν''. We compute $\mathcal{M}_{p_3}(\nu'')$ using (11) and $\mathcal{M}_{p_3}(\nu'') = 3$.

   By Algorithm 1, both t_5 and t_7 should be forbidden to occur, i.e., $f(\nu) = \{t_5, t_7\}$.
5) Let $\nu = t_7 t_6 t_6$. By (5) and (9), we have $\Phi(t_7 t_6) = 2$ and $\Psi_{t_6}(t_7 t_6) = 1$. Since $[\Phi(t_7 t_6) - \mathcal{M}_{p_3}(t_7 t_6)] \cdot 1 + \Psi_{t_6}(t_7 t_6) - 1 = 0$, we compute $\mathcal{M}_{p_3}(t_7 t_6)$ using (16) and $\mathcal{M}_{p_3}(t_7 t_6 t_6) = \mathcal{M}_{p_3}(t_7 t_6) - 1 = 1$. Let $\nu' = t_7 t_6 t_6 t_5$ and $\nu'' = t_7 t_6 t_6 t_7$.
   - Consider the sequence ν'. We compute $\mathcal{M}_{p_3}(\nu')$ using (11) and $\mathcal{M}_{p_3}(\nu') = 2$.
   - Consider the sequence ν''. We compute $\mathcal{M}_{p_3}(\nu'')$ using (11) and $\mathcal{M}_{p_3}(\nu'') = 2$.

   By Algorithm 1, $f(\nu) = \emptyset$.

VI. CONCLUSIONS

This paper proposes an on-line EFS for a class of PNs whose augmented unobservable subnets are acyclic FSBCF nets. The EFS takes advantage of the structural properties of such class of nets, and selects a set of transitions to forbid in response to each observation. It minimally restricts the behavior of the PN while ensuring that the closed-loop system evolves only within the set of legal markings. Our future work will focus on extending the method to more general classes of PNs.

REFERENCES

[1] T. Ushio and R. Matsumoto, "State feedback and modular control synthesis in controlled Petri nets," in *Proc. 27th IEEE Conf. Decision Control*, vol. 2. Dec. 1988, pp. 1502–1507.
[2] T. Ushio, "On the controllability of controlled Petri nets," *Control-Theory Adv. Technol.*, vol. 5, no. 3, pp. 265–275, Sep. 1989.
[3] L. E. Holloway, B. H. Krogh, and A. Giua, "A survey of Petri net methods for controlled discrete event systems," *Discrete Event Dyn. Syst.*, vol. 7, no. 2, pp. 151–190, 1997.
[4] A. Giua, F. DiCesare, and M. Silva, "Generalized mutual exclusion constraints on nets with uncontrollable transitions," in *Proc. IEEE Int. Conf. Syst., Man Cybern.*, vol. 2. Oct. 1992, pp. 974–979.
[5] K. Yamalidou, J. Moody, M. Lemmon, and P. Antsaklis, "Feedback control of Petri nets based on place invariants," *Automatica*, vol. 32, no. 1, pp. 15–28, 1996.
[6] A. Giua, "Petri nets as discrete event models for supervisory control," M.S. thesis, Rensselaer Polytechn. Inst., Troy, NY, USA, 1992.
[7] J. O. Moody and P. J. Antsaklis, "Petri net supervisors for DES with uncontrollable and unobservable transitions," *IEEE Trans. Autom. Control*, vol. 45, no. 3, pp. 462–476, Mar. 2000.
[8] F. Basile, P. Chiacchio, and A. Giua, "Suboptimal supervisory control of Petri nets in presence of uncontrollable transitions via monitor places," *Automatica*, vol. 42, no. 6, pp. 995–1004, 2006.
[9] A. Ghaffari, N. Rezg, and X. Xie, "Design of a live and maximally permissive Petri net controller using the theory of regions," *IEEE Trans. Robot. Autom.*, vol. 19, no. 1, pp. 137–141, Feb. 2003.
[10] J. O. Moody and P. J. Antsaklis, *Supervisory Control of Discrete Event Systems Using Petri Nets*. Norwell, MA, USA: Kluwer, 1998.
[11] C. Haoxun, "Net structure and control logic synthesis of controlled Petri nets," *IEEE Trans. Autom. Control*, vol. 43, no. 10, pp. 1446–1450, Oct. 1998.

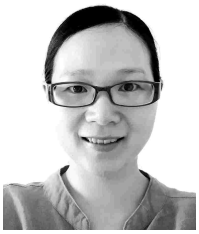
[12] J. Luo, W. Wu, H. Su, and J. Chu, "Supervisor synthesis for enforcing a class of generalized mutual exclusion constraints on Petri nets," *IEEE Trans. Syst., Man, Cybern. A, Syst., Humans*, vol. 39, no. 6, pp. 1237–1246, Nov. 2009.
[13] S. Wang, C. Wang, and M. Zhou, "Design of optimal monitor-based supervisors for a class of Petri nets with uncontrollable transitions," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 43, no. 5, pp. 1248–1255, Sep. 2013.
[14] J. Luo and M. Zhou, "Petri-net controller synthesis for partially controllable and observable discrete event systems," *IEEE Trans. Autom. Control*, vol. 62, no. 3, pp. 1301–1313, Mar. 2017.
[15] S. Wang, D. You, and C. Wang, "Optimal supervisor synthesis for Petri nets with uncontrollable transitions: A bottom-up algorithm," *Inf. Sci.*, vol. 363, pp. 261–273, Oct. 2016.
[16] S. Wang, D. You, M. Zhou, and C. Seatzu, "Characterization of admissible marking sets in Petri nets with uncontrollable transitions," *IEEE Trans. Autom. Control*, vol. 61, no. 7, pp. 1953–1958, Jul. 2016.
[17] N. Ran, H. Su, and S. Wang, "An improved approach to test diagnosability of bounded Petri nets," *IEEE/CAA J. Autom. Sinica*, vol. 4, no. 2, pp. 297–303, Apr. 2017.
[18] D. You, S. Wang, W. Dai, and W. Wu, "An approach for enumerating minimal siphons in a subclass of Petri nets," *IEEE Access*, to be published, doi: 10.1109/ACCESS.2017.2763783.
[19] S. Wang, D. You, and M. Zhou, "A necessary and sufficient condition for a resource subset to generate a strict minimal siphon in S^4PR," *IEEE Trans. Autom. Control*, vol. 62, no. 8, pp. 4173–4179, Aug. 2017.
[20] S. Wang, D. You, and C. Seatzu, "A novel approach for constraint transformation in Petri nets with uncontrollable transitions," *IEEE Trans. Syst., Man, Cybern., Syst.*, to be published, doi: 10.1109/TSMC.2017.2665479.
[21] D. You, S. Wang, Z. Li, and C. Wang, "Computation of an optimal transformed linear constraint in a class of Petri nets with uncontrollable transitions," *IEEE Access*, vol. 5, pp. 6780–6790, 2017.
[22] N. Ran, H. Su, A. Giua, and C. Seatzu, "Codiagnosability analysis of bounded Petri nets," *IEEE Trans. Autom. Control*, to be published, doi: 10.1109/TAC.2017.2742659.
[23] T. Murata, "Petri nets: Properties, analysis and applications," *Proc. IEEE*, vol. 77, no. 4, pp. 541–580, Apr. 1989.

NING RAN received the B.S. degree in automation from Hebei University, Baoding, China, in 2010, the M.S. degree in control theory and control engineering from North China Electric Power University, Baoding, in 2013, and the Ph.D. degree in control science and engineering from Zhejiang University, Hangzhou, China, in 2017. He joined Hebei University in 2017, where he is currently a Lecturer with the College of Electronic and Information Engineering. His current research interests include fault diagnosis of Petri nets and supervisory control of discrete event systems.

He was a Visiting Ph.D. Student with the Electrical and Electronic Engineering Department, University of Cagliari, Cagliari, Italy, from 2015 to 2016.

SHOUGUANG WANG (M'10–SM'12) received the B.S. degree in computer science from the Changsha University of Science and Technology, Changsha, China, in 2000, and the Ph.D. degree in electrical engineering from Zhejiang University, Hangzhou, China, in 2005. He joined Zhejiang Gongshang University in 2005, where he is currently a Professor with the School of Information and Electronic Engineering, the Director of the Discrete-Event Systems Group, and the Dean of the System Modeling and Control Research Institute. He has authored or co-authored over ten papers in the IEEE TRANSACTIONS. His current research interests include Petri net theory and application and supervisory control of discrete event systems. He is currently an Associate Editor of the IEEE ACCESS and the IEEE/CAA JOURNAL OF AUTOMATICA SINICA.

He was a Visiting Professor with the Department of Electrical and Computer Engineering, New Jersey Institute of technology, Newark, NJ, USA, from 2011 to 2012. He was the Dean of the Department of Measuring and Control Technology and Instrument from 2011 to 2014. He was a Visiting Professor with the Electrical and Electronic Engineering Department, University of Cagliari, Cagliari, Italy, from 2014 to 2015.



WENHUI WU received the B.S. and M.S. degrees from Zhejiang Normal University, China, in 2003 and 2006, respectively. She is currently a Senior Lab Master with the School of Information and Electronic Engineering, Zhejiang Gongshang University. Her main interests include Petri net theory and application and supervisory control of discrete event systems.