Supplementary material concerning the paper

Supervisory Control of Petri Nets in the Presence of Replacement Attacks

Dan You, ShouGuang Wang, MengChu Zhou, *Fellow, IEEE*, and Carla Seatzu

I. NOMENCLATURE

$\mathbb{N}$	$\{0, 1, 2, \ldots\}$
$\mathbb{N}^+$	$\{1, 2, \ldots\}$
$\mathbb{Z}$	set of integers
N	(P, T, F, W), a PN
$[N]$	*incidence matrix* of N
${}^\bullet x$	$\{y\in P\cup T \mid (y, x)\in F\}$, the set of *inputs* of $x\in P\cup T$
$x^\bullet$	$\{y\in P\cup T \mid (x, y)\in F\}$, the set of *outputs* of $x\in P\cup T$
${}^\bullet X$	$\bigcup_{x\in X} {}^\bullet x$, the set of *inputs* of $X\subseteq P\cup T$
$X^\bullet$	$\bigcup_{x\in X} x^\bullet$, the set of *outputs* of $X\subseteq P\cup T$
m	$P\rightarrow\mathbb{N}$, a *marking* or *state*
$m(p)$	the number of *tokens* in place p at marking m
$m[t\rangle$	transition $t\in T$ is *enabled* at a marking m
$En(m)$	set of transitions enabled at m
$\mathcal{M}$	set of markings
$En(\mathcal{M})$	$\bigcup_{m\in\mathcal{M}} En(m)$
$m[t\rangle m'$	marking m' is reached from m by firing t
m_t	marking reached by firing t at m
m_α	marking reached by firing a transition sequence $\alpha\in T^*$ at m
m_0	*initial marking* of a PN
(N, m_0)	*net system* with initial marking m_0
$L(N, m_0)$	$\{\alpha\in T^* \mid m_0[\alpha\rangle\}$, the *language* of (N, m_0)
$R(N, m_0)$	$\{m \mid \exists\alpha\in T^*, m_0[\alpha\rangle m\}$, the set of all reachable markings of N from m_0
$L_o(N, m_0)$	observed language of (N, m_0)
$\mathcal{P}_r(\alpha)$	$\{\alpha'\in T^* \mid \exists\alpha''\in T^* \text{ s.t. } \alpha=\alpha'\alpha''\}$, the set of all *prefixes* of a transition sequence $\alpha\in T^*$
ρ	$L_o(N, m_0)\rightarrow 2^T$, a *control policy* of a PN system (N, m_0)
δ	an observation $\delta\in L_o(N, m_0)$
$\rho(\delta)$	*disabled set* associated with the observation δ
$(N, m_0)\vert_\rho$	system (N, m_0) supervised under policy ρ
$R(N, m_0)\vert_\rho$	reachability set of $(N, m_0)\vert_\rho$
$L(N, m_0)\vert_\rho$	language of $(N, m_0)\vert_\rho$
$L_o(N, m_0)\vert_\rho$	observed language of $(N, m_0)\vert_\rho$
$\rho_1\succ\rho_2$	policy ρ_1 is *more permissive* than policy ρ_2
(ω, k)	GMEC
$\mathcal{L}_{(\omega, k)}$	$\{m\in\mathbb{N}^{\vert P\vert} \mid \omega\cdot m\leq k\}$, the *legal marking set* of (ω, k)
ϖ	$\omega\cdot[N]$
Ω	$\{(\omega_1, k_1), (\omega_2, k_2), \ldots, (\omega_n, k_n)\}$, a set of GMECs
$\wedge\Omega$	the *conjunction* of GMECs in Ω
$\mathcal{L}_{\wedge\Omega}$	$\bigcap_{(\omega,k)\in\Omega}\mathcal{L}_{(\omega,k)}$, the *legal marking set* of $\wedge\Omega$
$\mathcal{A}$	$\mathcal{A}\in 2^{T\times T}$, a *replacement attack*
(t, t')	action disguising the firing of transition t as the firing of transition t'
$A(t)$	set of all possible observed transitions when transition t really fired
$A^{-1}(t)$	set of all possible really fired transitions producing the observation t
$\Gamma_{(\omega, k)}(\mathcal{M})$	$\{t\in En(\mathcal{M}) \mid \exists m\in\mathcal{M}, \text{ s.t. } \omega\cdot m_t > k\}$, the set of *violating transitions* at $\mathcal{M}$ related to GMEC (ω, k)
(N^c, m_0^c)	*monitor-controlled PN system*
$[N^c]$	*incidence matrix* of N^c
p_c	monitor
m^c	marking of the monitor-controlled PN N^c
m_{pc}	marking of the monitor place p_c
$Dis(m_{pc})$	$\{t\in p_c^\bullet \mid m_{pc}<W^c(p_c, t)\}$, the set of *monitor-disabled transitions* related a marking m_{pc}
$\Psi(m^c)$	$Dis(m_{pc})\cap En(m)$, where $[m^T\ m_{pc}^T]^T= m^c$
$\mathcal{M}^c$	set of markings of N^c
$\Psi(\mathcal{M}^c)$	$\bigcup_{m^c\in\mathcal{M}^c}\Psi(m^c)$

II. PROOF OF THEOREM 3

Let (N^c, m_0^c) be the monitor-controlled PN system w.r.t. (N, m_0) and (ω, k). By Property 1, $\forall m^c\in R(N^c, m_0^c)$, $\omega\cdot m+m_{pc}=k$ and $Dis(m_{pc})=\{t\in T \mid \omega\cdot m+\varpi(t)>k\}$.

Let ρ be the policy computed by Method 3. By assumption, m_0 is legal. Let m_{pc0} be the marking of monitor p_c such that $m_0^c=[m_0, m_{pc0}]$. Since $\rho(\varepsilon)=Dis(m_{pc0})$, any firable transition t at m_0 satisfies the inequality: $\omega\cdot m_0+\varpi(t)\leq k$, i.e., any marking reachable from m_0 by firing a transition is legal.

Let t_1 be the first observed transition. Suppose that t_1' is the really fired transition producing observation t_1. Let m_1 and m_1^c be the markings reached by N and N^c after firing t_1' from m_0 and m_0^c, respectively. It is $m_1^c=[m_1, m_{pc1}]$, where $m_{pc1}=k-\omega\cdot m_1$ and $m_{pc1}=m_{pc0}+[N^c](p_c, t_1')$. Let $m_{pc1}^*= m_{pc0}+\min_{t'\in T_{real}}[N^c](p_c, t')$, where $T_{real}=A^{-1}(t_1)\cap En(m_0^c)$ since Flag=True. We can see that $m_{pc1}^*\leq m_{pc1}$ since $t_1'\in T_{real}$. Hence, $Dis(m_{pc1}^*)\supseteq Dis(m_{pc1})$. We observe that $\omega m_1 \leq k$ and $Dis(m_{pc1})=\{t\in T | \omega m_1+\varpi(t)>k\}$. Since $\rho(t_1)=Dis(m_{pc1}*)$, any firable transition t at m_1 satisfies the condition: $\omega m_1+\varpi(t)\leq k$, i.e., any marking reachable from m_1 by firing a transition is legal.

If Flag is still "True", when the next transition is observed, by repeating the above reasoning, the reachable markings in the next step are all legal. Let us consider now the case that Flag is changed to "False". Let t_2 be the next observed transition. Suppose that t_2' is the really fired transition producing observation t_2. Let m_2 and m_2^c be the markings reached by N and N^c after firing t_2' from m_1 and m_1^c, respectively. Clearly, $m_2^c=[m_2, m_{pc2}]$, where $m_{pc2}=k-\omega m_2$ and $m_{pc2}=m_{pc1}+[N^c](p_c, t_2')$. Let $m_{pc2}*=m_{pc1}*+\min_{t'\in T_{real}}[N^c](p_c, t')$, where $T_{real}=A^{-1}(t_2)\backslash\rho(t_1)$ since Flag=False. Since $m_{pc1}*\leq m_{pc1}$ and $t_2'\in T_{real}$, it holds that $m_{pc2}*\leq m_{pc2}$. Hence, $Dis(m_{pc2}*)\supseteq Dis(m_{pc2})$. We observe that $\omega m_2\leq k$ and $Dis(m_{pc2})=\{t\in T|\omega m_2+\varpi(t)>k\}$. Since $\rho(t_1t_2)=Dis(m_{pc2}*)$, any firable transition t at m_2 satisfies the condition: $\omega m_2+\varpi(t)\leq k$, i.e., any marking reachable from m_1 by firing a transition is legal.

By repeating the above reasoning, every time we observe a transition, the computed disabled set guarantees that the reachable markings in the next step are all legal. As a result, $R(N, m_0)|_\rho \subseteq \mathcal{L}_{(\omega, k)}$, i.e., the policy ρ is acceptable.

III. Proof of Theorem 4

Let ρ_3 and ρ_2 be the policies computed by Methods 3 and 2, respectively. We prove that ρ_3 is as permissive as ρ_2, i.e., $L(N, m_0)|_{\rho_3}=L(N, m_0)|_{\rho_2}$.

We preliminarily introduce a new notation. Given a policy ρ and $\delta\in L_o(N, m_0)$, we denote $Next_\rho(\delta)=\{t\in T \;|\sigma t\in L(N, m_0)|_\rho$, where $\sigma\in A^{-1}(\delta)\}$, i.e., the set of transitions that are firable in the next step under the control policy ρ after observing δ.

First, consider $\delta=\varepsilon$. It is clear that $\rho_2(\varepsilon)=\Psi(m_0^c)=Dis(m_{pc0})\cap En(m_0)$, while $\rho_3(\varepsilon)=Dis(m_{pc0})$, where m_{pc0} is the marking of monitor p_c s.t. $m_0^c=[m_0 \;\; m_{pc0}]^T$. Note that $Next_{\rho 2}(\varepsilon)=En(m_0)\backslash\rho_2(\varepsilon)$ and $Next_{\rho 3}(\varepsilon)=En(m_0)\backslash\rho_3(\varepsilon)$. Hence, it obviously holds that $Next_{\rho 2}(\varepsilon)=Next_{\rho 3}(\varepsilon)$.

Next, let t_1 be the first observed transition, i.e., $\delta=t_1$. Consider Method 2. Let $\mathcal{M}^c$ be the set of possible reached markings of (N^c, m_0^c) consistent with t_1 under control policy ρ_2. We observe that, $\forall m^c\in\mathcal{M}^c$, $m_{pc}=m_{pc0}-\varpi(t_1')$, where $t_1'\in A^{-1}(t_1)$. Since $\varpi(t_{11})=\varpi(t_{12})=\ldots=\varpi(t_{1n})$, where $\{t_{11}, t_{12}, \ldots, t_{1n}\}=A^{-1}(t_1)$, all the markings in $\mathcal{M}^c$ have the identical token-count in monitor p_c. Let a be such a number. It holds that $\Psi(\mathcal{M}^c)=\bigcup_{m^c\in\mathcal{M}^c}\Psi(m^c)=\bigcup_{m^c\in\mathcal{M}^c}(Dis(m_{pc})\cap En(m))$. As a result, $\rho_2(t_1)=\Psi(\mathcal{M}^c)=En(\mathcal{M})\cap Dis(a)$, where $\mathcal{M}$ is the set of markings by restricting markings in $\mathcal{M}^c$ to the net N, which is exactly the set of possible reached markings of (N, m_0) consistent with t_1 under control policy ρ_2. Hence, $Next_{\rho 2}(t_1)=En(\mathcal{M})\backslash\rho_2(t_1)=En(\mathcal{M})\backslash Dis(a)$. Consider Method 3. $\rho_3(t_1)=Dis(m_{pc}*)$, where $m_{pc}*=m_{pc0}+\min_{t'\in T_{real}}(-\varpi(t'))$ and $T_{real}\subseteq A^{-1}(t_1)$. Hence, $m_{pc}*=a$. Since $Next_{\rho 2}(\varepsilon)=Next_{\rho 3}(\varepsilon)$, the set of possible reached markings of (N, m_0) consistent with t_1 under the control of ρ_3 is also $\mathcal{M}$. Hence, $Next_{\rho 3}(t_1)=En(\mathcal{M})\backslash\rho_3(t_1)=En(\mathcal{M})\backslash Dis(a)$. Clearly, $Next_{\rho 2}(t_1)=Next_{\rho 3}(t_1)$.

By repeating the same procedure, we can see $Next_{\rho 2}(\delta)=Next_{\rho 3}(\delta)$, $\forall\delta\in L_o(N, m_0)$. This implies that $L(N, m_0)|_{\rho 3}=L(N, m_0)|_{\rho 2}$. Thus we conclude that, since ρ_2 is optimal, ρ_3 is also optimal.

IV. Case Study

We consider a tourist attraction consisting of four areas A-D, as shown in Fig. 1. The entrance and exit of the tourist attraction are located in area A and there are several one-way gates between areas. A PN system modelling the flow of visitors in the tourist attraction is depicted in Fig. 2. In more detail, places p_1-p_4 model areas A-D, respectively. Each transition models the transit of one visitor in the corresponding gate, which is physically detected by a sensor installed on the gates. Moreover, each token models one visitor. Initially, the PN system is in a state where each area contains one visitor.

Suppose that there is a restriction on the number of visitors in area C (modeled by place p_3) due to safety constraints. Assume that a malicious attacker wants to interfere with the control system with the goal of compromising its safety. Here, we consider a practical scenario in which the control center communicates with sensors/actuators related to all the gates via a communication network. In terms of PNs, this means that a control policy to be designed works by observing the firing of transitions and controlling transitions according to the current observation. Now, suppose that the controller knows that the communication channel related to sensors installed with gate g_{BC} is vulnerable to attacks and its sensor signals are prone to be disguised as the sensor signals produced by gate g_{BD}. In this case, when designing a control policy, we need to take into account the replacement attack $\mathcal{A}=\{(t_3, t_4)\}$.

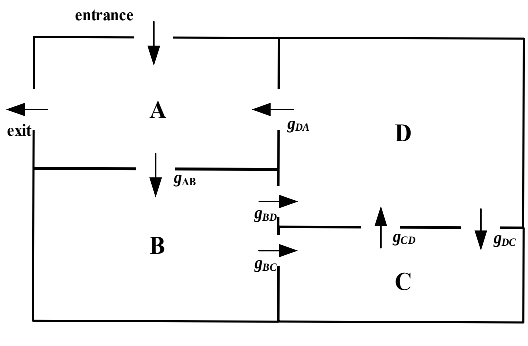

Fig. 1 Sketch map of a tourist attraction

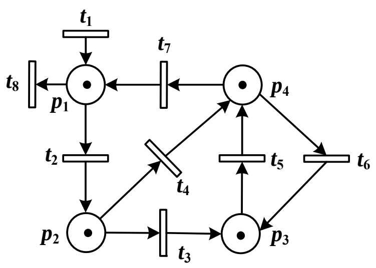

Fig. 2 PN model of the tourist attraction in Fig. 1 vulnerable to the replacement attack $\mathcal{A}=\{(t_3, t_4)\}$

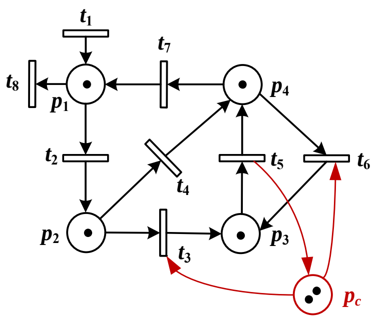

Fig. 3 Monitor-controlled PN system relative to the PN system in Fig. 2 and the GMEC (ω, k): $m(p_3)\leq 3$

In what follows, we apply Methods 1-3 in the paper to control the system. We assume that the number of visitors in area C cannot be more than three, i.e., we enforce the GMEC (ω, k): $m(p_3)\leq 3$. The monitor-controlled PN system relative to the GMEC (ω, k): $m(p_3)\leq 3$ is shown in Fig. 3. Table 1 illustrates the application of Methods 1-3 for a possible system evolution. In more detail, the first column shows the observed transitions, the second column records the set $\mathcal{M}$ of markings consistent with the current observation, which is computed in Method 1, the third column records the set $\mathcal{M}^c$ of markings of the monitor-controlled system consistent with the current observation, which is computed in Method 2, and the forth column provides the disabled set computed by Methods 1 and 2. The last three columns refer to Method 3 and contain the marking, Flag, and the disabled set computed in Method 3, respectively. Note that, for sake of clarity, the number of tokens in the monitor place p_c are highlighted in bold in the table. Besides, we write "×" to indicate that we do not record the token count in the corresponding place.

For this example, it can be verified that the condition of Theorem 4 is not satisfied. In more detail, we observe that $A^{-1}(t_4)=\{t_3, t_4\}$ but $\varpi(t_3)\neq\varpi(t_4)$ since $\varpi(t_3)=1$ and $\varpi(t_4)=0$. Thus, the policy computed by Method 3 is not guaranteed to be optimal. Indeed, from TABLE 1, we can see that the policy computed by Method 3 is more restrictive than those computed by Methods 1 and 2. Nevertheless, we note that Method 3 records one marking only while Methods 1 and 2 both record multiple markings.

TABLE 1 Application of Methods 1-3

	Method 1&2			Method 3		
t_i	$\mathcal{M}$	$\mathcal{M}^c$	$\rho(\delta)$	m^c	Flag	$\rho(\delta)$
ε	$[1, 1, 1, 1]^T$	$[1, 1, 1, 1, \mathbf{2}]^T$	∅	$[1, 1, 1, 1, \mathbf{2}]^T$	True	∅
t_1	$[2, 1, 1, 1]^T$	$[2, 1, 1, 1, \mathbf{2}]^T$	∅	$[2, 1, 1, 1, \mathbf{2}]^T$	True	∅
t_1	$[3, 1, 1, 1]^T$	$[3, 1, 1, 1, \mathbf{2}]^T$	∅	$[3, 1, 1, 1, \mathbf{2}]^T$	True	∅
t_2	$[2, 2, 1, 1]^T$	$[2, 2, 1, 1, \mathbf{2}]^T$	∅	$[2, 2, 1, 1, \mathbf{2}]^T$	True	∅
t_4	$[2, 1, 2, 1]^T$; $[2, 1, 1, 2]^T$	$[2, 1, 2, 1, \mathbf{1}]^T$; $[2, 1, 1, 2, \mathbf{2}]^T$	∅	$[\times,\times,\times,\times, \mathbf{1}]^T$	False	∅
t_7	$[3, 1, 2, 0]^T$; $[3, 1, 1, 1]^T$	$[3, 1, 2, 0, \mathbf{1}]^T$; $[3, 1, 1, 1, \mathbf{2}]^T$	∅	$[\times,\times,\times,\times, \mathbf{1}]^T$	False	∅
t_2	$[2, 2, 2, 0]^T$; $[2, 2, 1, 1]^T$	$[2, 2, 2, 0, \mathbf{1}]^T$; $[2, 2, 1, 1, \mathbf{2}]^T$	∅	$[\times,\times,\times,\times, \mathbf{1}]^T$	False	∅
t_4	$[2, 1, 3, 0]^T$; $[2, 1, 2, 1]^T$; $[2, 1, 1, 2]^T$	$[2, 1, 3, 0, \mathbf{0}]^T$; $[2, 1, 2, 1, \mathbf{1}]^T$; $[2, 1, 1, 2, \mathbf{2}]^T$	$\{t_3\}$	$[\times,\times,\times,\times, \mathbf{0}]^T$	False	$\{t_3, t_6\}$
t_4	$[2, 0, 3, 1]^T$; $[2, 0, 2, 2]^T$; $[2, 0, 1, 3]^T$	$[2, 0, 3, 1, \mathbf{0}]^T$; $[2, 0, 2, 2, \mathbf{1}]^T$; $[2, 0, 1, 3, \mathbf{2}]^T$	$\{t_6\}$	$[\times,\times,\times,\times, \mathbf{0}]^T$	False	$\{t_3, t_6\}$
t_2	$[1, 1, 3, 1]^T$; $[1, 1, 2, 2]^T$; $[1, 1, 1, 3]^T$	$[1, 1, 3, 1, \mathbf{0}]^T$; $[1, 1, 2, 2, \mathbf{1}]^T$; $[1, 1, 1, 3, \mathbf{2}]^T$	$\{t_3, t_6\}$	$[\times,\times,\times,\times, \mathbf{0}]^T$	False	$\{t_3, t_6\}$
t_5	$[1, 1, 2, 2]^T$; $[1, 1, 1, 3]^T$; $[1, 1, 0, 4]^T$	$[1, 1, 2, 2, \mathbf{1}]^T$; $[1, 1, 1, 3, \mathbf{2}]^T$; $[1, 1, 0, 4, \mathbf{3}]^T$	∅	$[\times,\times,\times,\times, \mathbf{1}]^T$	False	∅

t_2	$[0, 2, 2, 2]^T$; $[0, 2, 1, 3]^T$; $[0, 2, 0, 4]^T$	$[0, 2, 2, 2, \mathbf{1}]^T$; $[0, 2, 1, 3, \mathbf{2}]^T$; $[0, 2, 0, 4, \mathbf{3}]^T$	$\varnothing$	$[\times,\times,\times,\times, \mathbf{1}]^T$	False	$\varnothing$
t_7	$[1, 2, 2, 1]^T$; $[1, 2, 1, 2]^T$; $[1, 2, 0, 3]^T$	$[1, 2, 2, 1, \mathbf{1}]^T$; $[1, 2, 1, 2, \mathbf{2}]^T$; $[1, 2, 0, 3, \mathbf{3}]^T$	$\varnothing$	$[\times,\times,\times,\times, \mathbf{1}]^T$	False	$\varnothing$
t_6	$[1, 2, 3, 0]^T$; $[1, 2, 2, 1]^T$; $[1, 2, 1, 2]^T$	$[1, 2, 3, 0, \mathbf{0}]^T$; $[1, 2, 2, 1, \mathbf{1}]^T$; $[1, 2, 1, 2, \mathbf{2}]^T$	$\{t_3\}$	$[\times,\times,\times,\times, \mathbf{0}]^T$	False	$\{t_3, t_6\}$
t_5	$[1, 2, 2, 1]^T$; $[1, 2, 1, 2]^T$; $[1, 2, 0, 3]^T$	$[1, 2, 2, 1, \mathbf{1}]^T$; $[1, 2, 1, 2, \mathbf{2}]^T$; $[1, 2, 0, 3, \mathbf{3]}^T$	$\varnothing$	$[\times,\times,\times,\times, \mathbf{1}]^T$	False	$\varnothing$
…	…	…	…	…	…	…