Available online at www.sciencedirect.com
ScienceDirect
Automatica 44 (2008) 875–881
automatica
www.elsevier.com/locate/automatica

Technical Communique

Robust supervisory control of timed discrete event systems under partial observation based on eligible time bounds: The existence conditions☆

Seong-Jin Park[a], Kwang-Hyun Cho[b,*]

[a]Department of Electrical and Computer Engineering, Ajou University, Suwon 443-749, Republic of Korea
[b]Department of Bio and Brain Engineering and KI for the BioCentury, Korea Advanced Institute of Science and Technology, 335 Gwahangno, Yuseong-gu, Daejeon 305-701, Republic of Korea

Received 15 May 2006; received in revised form 11 February 2007; accepted 26 July 2007
Available online 11 December 2007

Abstract

This paper addresses a supervisory control problem for uncertain timed discrete event systems (DESs) under partial observation. An uncertain timed DES to be controlled is represented by a set of possible timed models based on the framework of Brandin and Wonham [(1994). Supervisory control of timed discrete event systems. *IEEE Transactions on Automatic Control*, *39*(2), 329–342]. To avoid the state space explosion problem caused by *tick* events in the timed models, a notion of eligible time bounds is proposed for a single timed model obtained from the set of all possible timed models. Based on this notion, we present the necessary and sufficient conditions for the existence of a robust supervisor achieving a given language specification for the single timed model. Moreover, we show that the robust supervisor can also achieve the specification for any timed model in the set.

Keywords: Robust supervisors; Timed DESs; Partial observation; Eligible time bounds

1. Introduction

Since Brandin and Wonham (1994) proposed a supervisory control framework for timed discrete event systems (DESs) based on a *tick* event and a forcing mechanism, various studies on supervisory control of timed DESs have been accomplished within this framework (Lin & Wonham, 1995; Takai, 2000; Takai & Ushio, 2006). However, the introduction of the *tick* event often leads to the problem of state space explosion. To avoid such a state space explosion, Brandin (1998) has proposed to incorporate the timing information of states into timer variables under complete observation. On the other hand, Park and Cho (2006) have proposed the notion of eligible time bounds to investigate the supervisor existence problem under partial observation. However, the issue of partial observation and model uncertainty has not yet been properly addressed till this date in consideration of the state space explosion problem in spite of its practical importance in many real situations.

This paper addresses the supervisory control problem of satisfying a given language specification imposed on a timed DES under partial observation and model uncertainty. The timed model proposed by Brandin and Wonham (1994) is employed in this paper as a basic framework since the language-based supervisory control of Ramadge and Wonham can be easily adopted within this framework. In addition, we introduce the uncertainty modeling of Bourdon, Lawford, and Wonham (2005) to represent an uncertain timed DES by a set of possible timed models. In consideration of such a model uncertainty, Takai (2000) has also presented the robust supervisory control of timed DESs under partial observation. It was, however, based on the timed model of Brandin and Wonham (1994) and thereby the state space explosion problem still remains as a crucial issue. Hence, we investigate the robust supervisory control problem of uncertain timed DESs by introducing the notion of eligible time bounds to avoid such a state space explosion problem. The

☆ This paper was not presented at any IFAC meeting. This paper was recommended for publication in revised form by Associate Editor Karl Henrik Johansson under the direction of Editor André Tits.

* Corresponding author. Tel.: +82 42 869 4325; fax: +82 42 869 4310.
E-mail addresses: parksjin@ajou.ac.kr (S.-J. Park), ckh@kaist.edu (K.-H. Cho).

0005-1098/$ - see front matter © 2007 Elsevier Ltd. All rights reserved.
doi:10.1016/j.automatica.2007.07.019

primitive notion of eligible time bounds was introduced in Park and Cho (2006) under partial observation. We extend the notion of eligible time bounds to the case of partial observation and model uncertainty. To develop the main idea in a more concise way, we represent a given set of possible timed models by a single timed model, and investigate the controllability and observability properties of a language specification from the single timed model. Finally, we show that the resulting controllability and observability properties become the necessary and sufficient conditions for the existence of a robust supervisor that can achieve a given language specification for any model in the set of possible timed models.

2. Uncertain timed DESs

An uncertain timed DES $\mathscr{G}$ considered in this paper is assumed to be modeled by a set of possible timed models as follows: $\mathscr{G} := \{G_i | i \in I\}$ where $I = \{1, \ldots, n\}$. The timed models are based on the framework of Brandin and Wonham (1994). For each timed model G_i, an activity model describing its logical behavior is represented by a finite state automaton $G_{i,\mathrm{act}} = (A_i, \Sigma_{i,\mathrm{act}}, a_{i,0}, \delta_{i,\mathrm{act}})$ where A_i is the set of activity states, $\Sigma_{i,\mathrm{act}}$ is the set of activity events, $a_{i,0}$ is the initial activity state, and $\delta_{i,\mathrm{act}} : A_i \times \Sigma_{i,\mathrm{act}} \to A_i$ is the activity state transition (partial) function. Each event σ in $\Sigma_{i,\mathrm{act}}$ is assigned with a lower time bound $l(\sigma) \in N$ and an upper time bound $u(\sigma) \in N \cup \{\infty\}$ where N is the set of natural numbers. From the activity model and time bounds, the timed model can be represented by the following finite state automaton: $G_i = (Q_i, \Sigma_i, q_{i,0}, \delta_i)$ where Q_i is the set of states, Σ_i is the set of events, $q_{i,0}$ is the initial state, and $\delta_i : Q_i \times \Sigma_i \to Q_i$ is the state transition function (refer to Brandin & Wonham, 1994, for more detailed definitions of its transition structure). The set Σ_i is decomposed into $\Sigma_i = \Sigma_{i,\mathrm{act}} \cup \{tick\}$ in which the event *tick* represents the tick of the global clock. The set $\Sigma_{i,\mathrm{act}}$ is further classified as $\Sigma_{i,\mathrm{act}} = \Sigma_{i,\mathrm{c}} \dot\cup \Sigma_{i,\mathrm{uc}} = \Sigma_{i,\mathrm{o}} \dot\cup \Sigma_{i,\mathrm{uo}}$ ($\dot\cup$ means a disjoint union) where $\Sigma_{i,\mathrm{c}}$ is the set of controllable events, $\Sigma_{i,\mathrm{uc}}$ is the set of uncontrollable events, $\Sigma_{i,\mathrm{o}}$ is the set of observable events, and $\Sigma_{i,\mathrm{uo}}$ is the set of unobservable events. Furthermore, there is a set $\Sigma_{i,\mathrm{for}}$ ($\subseteq \Sigma_{i,\mathrm{act}}$) of forcible events which can preempt the *tick* event by forcing action of a supervisor.

To develop the main results in a more concise way, we consider a single timed model G with its activity model G_{act} as follows: $G_{\mathrm{act}} = (A, \Sigma_{\mathrm{act}}, a_0, \delta_{\mathrm{act}})$ where $A = (\cup_{i\in I} A_i) \cup \{a_0\}$, $\Sigma_{\mathrm{act}} = (\cup_{i\in I} \Sigma_{i,\mathrm{act}}) \cup \{\theta_1, \ldots, \theta_n\}$, a_0 is the initial state, and $\delta_{\mathrm{act}} : A \times \Sigma_{\mathrm{act}} \to A$ is the transition function ($\delta_{\mathrm{act}}(a_0, \theta_i) = a_{i,0}$ for all $i \in I$ and δ_{act} is the same as $\delta_{i,\mathrm{act}}$ for any other activity state $a \in \cup_{i\in I} A_i$). The hypothetical events θ_i's are adopted to discern $G_{i,\mathrm{act}}$'s in the single model G_{act}. The timed model G is then defined as follows: $G = (Q, \Sigma, q_0, \delta)$ where Q is the finite set of states, $\Sigma = (\cup_{i\in I} \Sigma_i) \cup \{\theta_1, \ldots, \theta_n\}$, q_0 is the initial state, and $\delta : Q \times \Sigma \to Q$ is the transition function as defined by Brandin and Wonham (1994). The hypothetical events θ_i's are assumed to be uncontrollable and unobservable with zero time bounds, i.e., $l(\theta_i) = u(\theta_i) = 0$ for all $i \in I$. In addition, we let $\Sigma_{\mathrm{c}} = \cup_{i\in I} \Sigma_{i,\mathrm{c}}$, $\Sigma_{\mathrm{uc}} = (\cup_{i\in I} \Sigma_{i,\mathrm{uc}}) \cup \{\theta_1, \ldots, \theta_n\}$, $\Sigma_{\mathrm{o}} = \cup_{i\in I} \Sigma_{i,\mathrm{o}}$, $\Sigma_{\mathrm{uo}} = (\cup_{i\in I} \Sigma_{i,\mathrm{uo}}) \cup \{\theta_1, \ldots, \theta_n\}$, and $\Sigma_{\mathrm{for}} = \cup_{i\in I} \Sigma_{i,\mathrm{for}}$.

Let Σ^*_{act} and Σ^* denote the set of all finite strings of elements in Σ_{act} and Σ, respectively, including the empty string ε. Then, we can define two projections P_{o} and P_{act} as follows: $P_{\mathrm{o}} : \Sigma^*_{\mathrm{act}} \to \Sigma^*_{\mathrm{o}}$ is defined as (i) $P_{\mathrm{o}}(\varepsilon) = \varepsilon$, (ii) for $s \in \Sigma^*_{\mathrm{act}}$ and $\sigma \in \Sigma_{\mathrm{act}}$, $P_{\mathrm{o}}(s\sigma) = P_{\mathrm{o}}(s)\sigma$ if $\sigma \in \Sigma_{\mathrm{o}}$, and $P_{\mathrm{o}}(s\sigma) = P_{\mathrm{o}}(s)$ otherwise, and $P_{\mathrm{act}} : \Sigma^* \to \Sigma^*_{\mathrm{act}}$ is defined as (i) $P_{\mathrm{act}}(\varepsilon) = \varepsilon$, (ii) for $s \in \Sigma^*$ and $\sigma \in \Sigma$, $P_{\mathrm{act}}(s\sigma) = P_{\mathrm{act}}(s)\sigma$ if $\sigma \neq tick$, and $P_{\mathrm{act}}(s\sigma) = P_{\mathrm{act}}(s)$ otherwise. Let $tick^i$ denote the string of *tick*s with length i. For instance, $tick^2 = tick\, tick$. The prefix closure of a language L ($\subset \Sigma^*$) is $pr(L) := \{t \in \Sigma^* | tu \in L \text{ for some } u \in \Sigma^*\}$, and L is said to be closed if $L = pr(L)$. For $s \in \Sigma^*$, let $\Sigma_L(s) := \{\sigma \in \Sigma | s\sigma \in pr(L)\}$. The closed behaviors of G_{act} and G are defined by $L(G_{\mathrm{act}}) := \{s \in \Sigma^*_{\mathrm{act}} | \delta_{\mathrm{act}}(a_0, s) \text{ is defined}\}$ and $L(G) := \{s \in \Sigma^* | \delta(q_0, s) \text{ is defined}\}$, respectively. We let $L(G_{\mathrm{act}}) = L_{\mathrm{act}}$ and $L(G) = L$ for short.

3. Eligible time bounds

We first define an eligible lower time bound (*el*) and an eligible upper time bound (*eu*) as follows:

Definition 1. Let $s \in \Sigma^*_{\mathrm{act}}$ and $\alpha \in \Sigma_{\mathrm{act}}$. Then $el(s, \alpha)$ and $eu(s, \alpha)$ are the minimum and maximum values, respectively, of k satisfying $\delta(q, tick^k \alpha) \in Q$ for any $v \in P^{-1}_{\mathrm{act}}(s) \cap L \cap \Sigma^* \Sigma_{\mathrm{act}}$ with $q = \delta(q_0, v)$.

After the occurrence of the last activity event of s, the event α can occur after at least $el(s, \alpha)$ and before at most $eu(s, \alpha)$ occurrences of a *tick*, respectively. The formula of computing the eligible time bounds is as follows: For $s, t \in L_{\mathrm{act}}$, $\lambda_0 \in \Sigma_{\mathrm{act}} \cup \{\varepsilon\}$, and $\lambda_1, \ldots, \lambda_n \in \Sigma_{\mathrm{act}}$, let $s = t\lambda_0\lambda_1 \ldots \lambda_n$. Then, an event $\alpha \in \Sigma_{\mathrm{act}}$ is called *impending* at s if the following conditions are all satisfied:

(i) $\lambda_k \neq \alpha$ for all $k = 1, \ldots, n$;
(ii) $\alpha \in \Sigma_{L_{\mathrm{act}}}(t\lambda_0\lambda_1 \ldots \lambda_k)$ for all $k = 0, 1, \ldots, n$;
(iii) $\alpha \notin \Sigma_{L_{\mathrm{act}}}(t) \backslash \{\lambda_0\}$ or $t = \lambda_0 = \varepsilon$.

For $s \in L_{\mathrm{act}}$ and an impending α at s, let

$$A_l(s, \alpha) := \sum_{k=0}^{n-1} el(t\lambda_0 \ldots \lambda_k, \lambda_{k+1}),$$

$$A_u(s, \alpha) := \sum_{k=0}^{n-1} eu(t\lambda_0 \ldots \lambda_k, \lambda_{k+1}).$$

For non-impending α at s, we define $A_l(s, \alpha) = A_u(s, \alpha) = 0$. The values $A_l(s, \alpha)$ and $A_u(s, \alpha)$ mean the minimum and maximum time elapses, respectively, from the first activation of α at $t\lambda_0$ until the occurrence of λ_n. Let

$$C(s) := \min_{\alpha \in \Sigma_{L_{\mathrm{act}}}(s)} (u(\alpha) - A_l(s, \alpha)).$$

Then, for all $\alpha \in \Sigma_{L_{\mathrm{act}}}(s)$, we can compute the eligible time bounds as follows:

$$el(s, \alpha) = \begin{cases} l(\alpha) - A_u(s, \alpha) & \text{if } l(\alpha) - A_u(s, \alpha) \leqslant C(s), \\ \text{undefined} & \text{otherwise,} \end{cases}$$

$$eu(s,\alpha)=\begin{cases} C(s) & \text{if } l(\alpha)-A_u(s,\alpha)\leqslant C(s),\\ \text{undefined} & \text{otherwise.}\end{cases}$$

We call an event α *feasible* at the string s if $el(s,\alpha)$ is defined.

We note that the computation of el and eu only requires searching over L_{act} and the time bounds of events. It does not require searching over L which can cause the problem of state space explosion. For any $s\in L_{\text{act}}$, the computation of el and eu for each event requires to check whether the event is impending. If so, A_l and A_u can be computed, and then el and eu can be computed by using the above formulae. Thus, the computational complexity of computing the eligible time bounds in G is $O(|A|\cdot 5|\Sigma_{\text{act}}|)$.

Since the eligible time bounds are not enough to properly describe the behavior of timed DESs under partial observation, it is necessary to extend those to the case of partial observation as follows.

Definition 2. For $s\in L_{\text{act}}$ and $\alpha\in\Sigma_{\text{act}}$, let $s=t\sigma_{\text{o}}\lambda_1\ldots\lambda_n$ and $\lambda_{n+1}=\alpha$ where $t\in\Sigma^*_{\text{act}}$, $\sigma_{\text{o}}\in\Sigma_{\text{o}}$, and $\lambda_1,\ldots,\lambda_n\in\Sigma_{\text{uo}}$. Then, an eligible lower time bound (elp) and an eligible upper time bound (eup) under partial observation are defined, respectively, as follows:

$$elp(s,\alpha):=el(t\sigma_{\text{o}},\lambda_1)+\sum_{k=1}^{n}el(t\sigma_{\text{o}}\lambda_1\ldots\lambda_k,\lambda_{k+1}),$$

$$eup(s,\alpha):=eu(t\sigma_{\text{o}},\lambda_1)+\sum_{k=1}^{n}eu(t\sigma_{\text{o}}\lambda_1\ldots\lambda_k,\lambda_{k+1}).$$

For $s\in L_{\text{act}}$ satisfying $P_{\text{o}}(s)=\varepsilon$, the string $t\sigma_{\text{o}}$ in the above definition is replaced with ε. The values of $elp(s,\alpha)$ and $eup(s,\alpha)$ imply that, after the occurrence of the last observable event σ_{o} of s, the event α should occur after at least $elp(s,\alpha)$ and before at most $eup(s,\alpha)$ occurrences of the *tick*, respectively.

4. Existence conditions of a robust supervisor

A supervisor $S=(V,I_{\text{e}},I_{\text{f}},\tau)$ is defined by $V:\Sigma^*_{\text{o}}\to 2^{\Sigma_{\text{act}}}$, $I_{\text{e}}:\Sigma^*_{\text{o}}\times\Sigma_{\text{act}}\to 2^N$, $I_{\text{f}}:\Sigma^*_{\text{o}}\times\Sigma_{\text{for}}\to 2^N$, and $\tau:\Sigma^*_{\text{o}}\to N$. For $s_{\text{o}}\in\Sigma^*_{\text{o}}$, $V(s_{\text{o}})$ is the set of events to be enabled or forced by the supervisor after the observation of s_{o}. Note that $V(s_{\text{o}})\supseteq\Sigma_{\text{uc}}$ since the uncontrollable events are permanently enabled. The supervisor enables an event $\alpha\in V(s_{\text{o}})$ if the value of a timer $\tau(s_{\text{o}})$ belongs to $I_{\text{e}}(s_{\text{o}},\alpha)$, otherwise the event is disabled. In addition, the supervisor forces an event $\alpha\in V(s_{\text{o}})$ if $\alpha\in\Sigma_{\text{for}}$ and the timer value $\tau(s_{\text{o}})$ belongs to $I_{\text{f}}(s_{\text{o}},\alpha)$.

A supervised system S/G denotes the timed DES G under control by the supervisor S. The closed behavior of S/G denoted by $L(S/G)$ is defined based on induction as follows: (i) $\varepsilon\in L(S/G)$ and $\tau(\varepsilon)=0$, (ii) for $s\in\Sigma^*$ and $\alpha\in\Sigma$, suppose that $s\in L(S/G)$ and $s\alpha\in L$ with $P_{\text{act}}(s)=s_{\text{a}}$ and $P_{\text{o}}(s_{\text{a}})=s_{\text{o}}$, then

(1) in case $\alpha\in V(s_{\text{o}})$ and $\tau(s_{\text{o}})\in I_{\text{e}}(s_{\text{o}},\alpha)\cup I_{\text{f}}(s_{\text{o}},\alpha)$, $s\alpha\in L(S/G)$ and $\tau(s_{\text{o}}\alpha)=0$ if $\alpha\in\Sigma_{\text{o}}$, otherwise $\tau(s_{\text{o}})$ is unchanged;

(2) in case $\alpha=tick$ and $k<eu(s_{\text{a}},\beta)$ for all $\beta\in\Sigma_{L_{\text{act}}}(s_{\text{a}})$ (where $s=s'\sigma tick^k$ and $\sigma\in\Sigma_{\text{act}}$), $s\alpha\in L(S/G)$ and $\tau(s_{\text{o}})$ is updated to $\tau(s_{\text{o}})+1$.

Given a closed language specification $\tilde{K}\subseteq\bigcap_{i\in I}L(G_{i,\text{act}})$ for an uncertain timed DES $\mathcal{G}:=\{G_i|i\in I\}$, we investigate the existence conditions of a robust supervisor S such that $P_{\text{act}}(L(S/G_i))=\tilde{K}$ for any $G_i\in\mathcal{G}$. For the single timed model G, it is evident that this problem is equivalent to finding the existence conditions of a robust supervisor S satisfying $P_{\text{act}}(L(S/G))=pr(\{\theta_1,\ldots,\theta_n\}\tilde{K})$. Let $K:=pr(\{\theta_1,\ldots,\theta_n\}\tilde{K})$ which denotes the closed language specification to be achieved in G. We assume that K is feasible with respect to (w.r.t.) G; i.e., for any $s\in K$, every event $\alpha\in\Sigma_K(s)$ is feasible at the string s.

To develop the existence conditions of a robust supervisor, it is necessary to introduce the following notions. First, for a string $s\in K$, let

$$B(K,s):=\begin{cases}\min\limits_{\gamma\in(\Sigma_{L_{\text{act}}}(s)\setminus\Sigma_K(s))\cap\Sigma_{\text{uc}}} elp(s,\gamma) & \text{if there exists a feasible } \gamma\in(\Sigma_{L_{\text{act}}}(s)\setminus\Sigma_K(s))\cap\Sigma_{\text{uc}},\\ \infty & \text{otherwise.}\end{cases}$$

Note that this is the minimum value of elp's for the uncontrollable events deviated from a path of K after s in G. For the language K to be achieved in G, there should exist a forcible event on the path of K after s with an elp value smaller than $B(K,s)$.

Let two strings $s_i,s_j\in K$ satisfy $P_{\text{o}}(s_i)=P_{\text{o}}(s_j)$. Then, a binary relation $\sqsubseteq_K$ is defined as $s_j\sqsubseteq_K s_i$ iff

(i) there is no feasible $\gamma\in(\Sigma_{L_{\text{act}}}(s_j)\setminus\Sigma_K(s_j))\cap\Sigma_{\text{uc}}$ with $elp(s_j,\gamma)<B(K,s_i)$, and
(ii) $\alpha\in\Sigma_{L_{\text{act}}}(s_j)$ and $elp(s_j,\alpha)<B(K,s_i)$ for at least one $\alpha\in\Sigma_K(s_i)\cap\Sigma_{\text{for}}$ satisfying $elp(s_i,\alpha)<B(K,s_i)$.

For the two different strings s_i and s_j with an identical observation, if the relation $s_j\sqsubseteq_K s_i$ holds then, after s_i in G, there always exist at least one uncontrollable event not belonging to $\Sigma_K(s_i)$ and at least one forcible event belonging to $\Sigma_K(s_i)$. Moreover, after s_j in G, there exists a forcible event belonging to $\Sigma_K(s_i)$ with its elp value smaller than $B(K,s_i)$. Thus, when a supervisor forces a forcible event before $B(K,s_i)$, the event *tick* is preempted by the forcible event after s_i and s_j.

For a string $s_{\text{o}}\in P_{\text{o}}(K)$, let $|s_{\text{o}}|_K:=\{s\in\Sigma^*_{\text{act}}|s\in K \text{ and } P_{\text{o}}(s)=s_{\text{o}}\}$ which can be partitioned into $|s_{\text{o}}|_K=g_1\dot{\cup}g_2\dot{\cup}\cdots\dot{\cup}g_m\dot{\cup}fl$, where

- g_k $(k=1,\ldots,m)$ is the set of elements satisfying $s_j\sqsubseteq_K s_i$ for some $s_i\in g_k$ and any $s_j\in g_k$ (such an s_i is defined as a master of g_k);
- fl is the set of elements satisfying $s_i\not\sqsubseteq_K s_j$, $s_k\not\sqsubseteq_K s_i$, and $s_i\not\sqsubseteq_K s_k$ for any $s_i,s_j\in fl$ $(s_i\neq s_j)$ and a master s_k of g_k;

- if s_i and s_j are the masters of g_i and g_j, respectively, then $s_i \not\sqsubseteq_K s_j$ and $s_j \not\sqsubseteq_K s_i$.

After a string s_j satisfying $s_j \in g_k$, at least one forcible event defined after s_i (s_i is the master of g_k) is enabled before the minimum value of *elp*'s for the uncontrollable events defined after s_i in G while not belonging to $\Sigma_K(s_i)$.

Based on the aforementioned notions, we consider the controllability and observability of a language specification as follows.

Definition 3. A closed language $K(\subset \Sigma^*_{\text{act}})$ is controllable w.r.t. an uncertain timed DES $\mathcal{G}$ if the following conditions hold for any $s \in K$:

(i) in case there exists a feasible $\gamma \in (\Sigma_{L_{\text{act}}}(s) \backslash \Sigma_K(s)) \cap \Sigma_{\text{uc}}$, there exists $\alpha \in \Sigma_K(s) \cap \Sigma_{\text{for}}$ with $elp(s, \alpha) < B(K, s)$,
(ii) in case $s \in g_k$ for some g_k with a master s_m, $\Sigma_K(s) = \{\alpha \in \Sigma_K(s) | elp(s, \alpha) < B(K, s_m)\}$.

The controllability condition implies that, when there are illegal uncontrollable events deviated from a path of K after a string s, there must be a legal forcible event α after s such that the value $elp(s, \alpha)$ is smaller than $B(K, s)$. Moreover, for any string after which the forcible event α is defined, the set of legal events after the string with their *elp*'s less than $B(K, s_m)$ must be identical with the set of legal events after the string.

For $s \in K$ and $\alpha \in \Sigma_{\text{act}}$, let

$$T(K, s, \alpha) := \begin{cases} \{l \in N | elp(s, \alpha) \leqslant l < B(K, s_m)\} & \text{if } s \in g_k \text{ for some} \\ & g_k \text{ with a master } s_m, \\ \{l \in N | elp(s, \alpha) \leqslant l \leqslant eup(s, \alpha)\} & \text{otherwise.} \end{cases}$$

Definition 4. A closed language K $(\subset \Sigma^*_{\text{act}})$ is observable w.r.t. an uncertain timed DES $\mathcal{G}$ if, for any $\alpha \in \Sigma_{\text{c}}$ and $s_1, s_2 \in K$ with $P_{\text{o}}(s_1) = P_{\text{o}}(s_2)$, $s_1\alpha \in K$, and $s_2\alpha \in L_{\text{act}}$, the following conditions hold: (i) $s_2\alpha \in K$; (ii) $T(K, s_1, \alpha) \cap T(K, s_2, \alpha) = \emptyset$ if $s_2\alpha \notin K$.

The observability condition states that, for the two different strings s_1 and s_2 with an identical observation, there should be no conflict by the event α in making a control decision, i.e., $s_1\alpha, s_2\alpha \in K$. If there is a conflict by the event, it requires that there should be no time instant at which the conflicted event is enabled either after s_1 or s_2. For the case of $s_2\alpha \notin K$, the conflict can be avoided by disabling the event α during the time interval $T(K, s_2, \alpha)$.

Let us discuss the computational complexity of verifying the presented controllability and observability conditions. First, we note that for each $s \in K$, $\alpha \in \Sigma_{\text{act}}$, the values such as $elp(s, \alpha)$, $eup(s, \alpha)$, $B(K, s)$, and $T(K, s, \alpha)$ can be computed separately in prior steps. For real implementations, these can be stored in a certain memory location associated with the pointer (s, α) as a data structure form. Hence, to check the conditions, only the values of the associated data structure for each (s, α) need to be compared, e.g., whether the value $elp(s, \alpha)$ is less than $B(K, s_i)$ (the condition (i) in Definition 3) or whether $T(K, s_1, \alpha) \cap T(K, s_2, \alpha)$ is an empty set or not (the condition (ii) in Definition 4). Therefore, the computational complexity of verifying the controllability condition becomes $O(m \cdot |A| \cdot |\Sigma_{\text{act}}|)$ and that of the observability condition becomes $O(m^2 \cdot |A| \cdot |\Sigma_{\text{act}}|)$ where m denotes the number of states of the automaton that recognizes the language K. Thus, checking the conditions does not require searching over the states set Q with *tick* transitions. On the other hand, the approach of Takai (2000), in a worst case, requires searching over $p|A_i|$ states of Q_i in each G_i where p is the finite maximum upper time bound of events, which therefore results in the computational complexity of $O(m \cdot p^2 \cdot |A| \cdot |\Sigma_{\text{act}}|)$ for controllability and $O(m^2 \cdot p^3 \cdot |A| \cdot |\Sigma_{\text{act}}|)$ for observability, respectively.

The following two theorems present the main results of this paper based on the foregoing developments.

Theorem 1. *For a closed language specification K $(\subseteq L_{\text{act}})$, there exists a robust supervisor S for an uncertain timed DES $\mathcal{G}$ such that $P_{\text{act}}(L(S/G)) = K$ if and only if K is controllable and observable w.r.t. $\mathcal{G}$.*

Proof. (If) Consider the following supervisor $S = (V, I_{\text{e}}, I_{\text{f}}, \tau)$: for any $s_{\text{o}} \in P_{\text{o}}(K)$,

$$V(s_{\text{o}}) = \{\alpha \in \Sigma_{\text{c}} | s_{\text{a}} \in |s_{\text{o}}|_K \text{ and } s_{\text{a}}\alpha \in K\} \cup \Sigma_{\text{uc}},$$

$$I_{\text{e}}(s_{\text{o}}, \alpha) = \bigcup_{s_{\text{a}} \in |s_{\text{o}}|_K} T(K, s_{\text{a}}, \alpha) \text{ for } \alpha \in V(s_{\text{o}}),$$

$$I_{\text{f}}(s_{\text{o}}, \alpha) = \{l \in N | l = B(K, s_m) - 1 \text{ for } s_m \in |s_{\text{o}}|_K, \alpha \in \Sigma_K(s_m) \text{ and a master } s_m \text{ of some } g_k\},$$

$$\tau(\varepsilon) = 0.$$

The proof can be done by induction on the length of strings. It holds that $\varepsilon \in P_{\text{act}}(L(S/G)) \cap K$. Let us assume that, for any string s_{a} with $|s_{\text{a}}| \leqslant n$, $s_{\text{a}} \in P_{\text{act}}(L(S/G))$ if and only if $s_{\text{a}} \in K$ where $|s_{\text{a}}|$ denotes the length of s_{a}. Let us prove the same for strings of $s_{\text{a}}\sigma$ where $|s_{\text{a}}| = n$ and $\sigma \in \Sigma_{\text{act}}$. Suppose $s \in L(S/G)$, $P_{\text{act}}(s) = s_{\text{a}}$, and $P_{\text{o}}(s_{\text{a}}) = s_{\text{o}}$. We first consider $s_{\text{a}}\sigma \in P_{\text{act}}(L(S/G))$ and assume that $s_{\text{a}}\sigma \notin K$. Then, we obtain $\sigma \in V(s_{\text{o}})$ by the definition of S. Let us consider the following two cases.

Case 1: $\sigma \in \Sigma_{\text{c}}$: The relations $s_{\text{a}}\sigma \in P_{\text{act}}(L(S/G))$, $\sigma \in V(s_{\text{o}})$, and $s_{\text{a}}\sigma \notin K$ imply that there exists $s' \in |s_{\text{o}}|_K$ such that $s'\sigma \in K$ and $T(K, s_{\text{a}}, \sigma) \cap T(K, s', \sigma) \neq \emptyset$. It contradicts the observability assumption of K.

Case 2: $\sigma \in \Sigma_{\text{uc}}$: Since K is controllable, there exists a feasible $\alpha \in \Sigma_K(s_{\text{a}}) \cap \Sigma_{\text{for}}$ satisfying $elp(s_{\text{a}}, \alpha) < B(K, s_m)$ for some master s_m. By the above definition of I_{f}, it follows that $B(K, s_m) - 1 \in I_{\text{f}}(s_{\text{o}}, \alpha)$. Then, the supervisor S forces the event α when $\tau(s_{\text{o}}) = B(K, s_m) - 1$, which results in $stick^j\sigma \notin L(S/G)$ for any j. Thus it holds that $s_{\text{a}}\sigma \notin P_{\text{act}}(L(S/G))$ which contradicts the assumption.

In the next, let $s_a\sigma \in K$. Then, if $s_a \in g_k$ for some g_k with a master s_m, the controllability of K implies $elp(s_a, \sigma) < B(K, s_m)$, otherwise it naturally holds that $elp(s_a, \sigma) \leqslant eup(s_a, \sigma)$. For both cases, it holds that $T(K, s_a, \sigma) \subseteq I_e(s_o, \sigma)$ by the above definition of I_e. Hence, when the timer $\tau(s_o)$ reaches a value in $I_e(s_o, \sigma)$, the event σ is enabled by the supervisor S and as a result $s\sigma \in L(S/G)$. It then follows that $s_a\sigma \in P_{act}(L(S/G))$. This completes the proof of the whole induction steps.

(Only if) Assume that a robust supervisor S satisfies $P_{act}(L(S/G)) = K$. First, let us prove that K is controllable w.r.t. $\mathcal{G}$ based on a contradiction principle. According to the definition of controllability, the following two cases can be considered.

Case 1: For some $s \in K$ satisfying $(\Sigma_{L_{act}}(s)\backslash\Sigma_K(s)) \cap \Sigma_{uc} \neq \emptyset$, assume that there does not exist any feasible $\alpha \in \Sigma_K(s) \cap \Sigma_{for}$ satisfying $elp(s, \alpha) < B(K, s)$. Then, according to the definition of $B(K, s)$, there exists $\gamma \in (\Sigma_{L_{act}}(s)\backslash\Sigma_K(s)) \cap \Sigma_{uc}$ satisfying $elp(s, \gamma) = B(K, s)$. In order to avoid the occurrence of γ after s, the supervisor should force a forcible event before its timer τ reaches the value $B(K, s)$. However, there is no feasible forcible event after s and therefore the occurrence of γ is not avoidable, i.e., $s\gamma \in P_{act}(L(S/G))$. Since $s\gamma \notin K$, it is a contradiction.

Case 2: For some $s \in K$, assume that $\Sigma_K(s) \neq \{\alpha \in \Sigma_K(s) | elp(s, \alpha) < B(K, s_m)\}$ where s_m is a master of some g_k with $s \in g_k$. Then, there exists $\alpha \in \Sigma_K(s)$ satisfying $elp(s, \alpha) \geqslant B(K, s_m)$. This means that there exists $\gamma \in (\Sigma_{L_{act}}(s)\backslash\Sigma_K(s)) \cap \Sigma_{uc}$ with $elp(s_m, \gamma) \leqslant elp(s, \alpha)$ by the definition of $B(K, s_m)$. Further, it follows from $s\alpha \in K$ and $P_{act}(L(S/G)) = K$ that $s\alpha \in P_{act}(L(S/G))$ implying $\alpha \in V(s_o)$ and $elp(s, \alpha) \in I_e(s_o, \alpha)$. Since $\gamma \in \Sigma_{uc}$, it is true that $\gamma \in V(s_o)$. Hence, in order to avoid the occurrence of γ after s_m, the supervisor S should force a forcible event before its timer value $\tau(s_o)$ reaches $B(K, s_m)$. However, since $elp(s_m, \gamma) \leqslant elp(s, \alpha)$, the forcing action prevents the occurrence of α after s, i.e., $s\alpha \notin P_{act}(L(S/G))$. This is a contradiction to the assumption of $P_{act}(L(S/G)) = K$.

From the above cases, we conclude that K is controllable w.r.t $\mathcal{G}$.

To verify the observability, let us assume that $s_2\sigma \notin K$ and $T(K, s_1, \sigma) \cap T(K, s_2, \sigma) \neq \emptyset$ for some $\sigma \in \Sigma_c$ and $s_1, s_2 \in K$ with $P_o(s_1) = P_o(s_2)$, $s_1\sigma \in K$, and $s_2\sigma \in L_{act}$. Then, $s_2, s_1\sigma \in P_{act}(L(S/G))$ from $P_{act}(L(S/G)) = K$. This implies that the supervisor S enables the event σ when its timer reaches a value in $T(K, s_1, \sigma)$. Since $T(K, s_1, \sigma) \cap T(K, s_2, \sigma) \neq \emptyset$, the supervisor also enables the event σ after the string s_2 when its timer reaches a value in $T(K, s_1, \sigma) \cap T(K, s_2, \sigma) \neq \emptyset$. Note that this is the time instant at which the event σ is simultaneously enabled after s_1 and s_2. Thus, it holds that $s_2\sigma \in P_{act}(L(S/G))$. However, since $s_2\sigma \notin K$, it is a contradiction to $P_{act}(L(S/G)) = K$. Therefore, we conclude that K is observable w.r.t. $\mathcal{G}$. □

Remark 1. Note that if the conditions of Theorem 1 are satisfied then a robust supervisor achieving K can be automatically designed from $P_o(K)$, $B(K, \cdot)$, and $T(K, \cdot, \cdot)$ as shown in the 'If' part of the proof. In this respect, the proof of Theorem 1 is constructive.

The following theorem shows that a robust supervisor achieving a language specification for a single model G also achieves the specification for any model G_i in $\mathcal{G}$.

Theorem 2. *Given a closed language specification* $\tilde{K} \subseteq \bigcap_{i\in I} L(G_{i,act})$ *for an uncertain timed DES* $\mathcal{G} := \{G_i | i \in I\}$ *and* $K := pr(\{\theta_1, \ldots, \theta_n\}\tilde{K})$, *if a robust supervisor S satisfies* $P_{act}(L(S/G)) = K$, *then* $P_{act}(L(S/G_i)) = \tilde{K}$ *for any* $G_i \in \mathcal{G}$.

Proof. From the definition of the single timed model G, it holds that

$$P_{act}(L(S/G)) = \{\varepsilon\} \cup \{\theta_1\}P_{act}(L(S/G_1)) \cup \{\theta_2\}P_{act}(L(S/G_2)) \cup \cdots \cup \{\theta_n\}P_{act}(L(S/G_n)).$$

In addition, it follows from $K := pr(\{\theta_1, \ldots, \theta_n\}\tilde{K})$ that

$$P_{act}(L(S/G)) = K = \{\varepsilon\} \cup \{\theta_1\}\tilde{K} \cup \{\theta_2\}\tilde{K} \cup \cdots \cup \{\theta_n\}\tilde{K}.$$

Hence, it follows that $P_{act}(L(S/G_i)) = \tilde{K}$ for any $G_i \in \mathcal{G}$. □

There have been various studies including Maler, Pnueli, and Sifakis (1995) and Tripakis and Altisen (1999) on the controller synthesis by using symbolic representations in the formal methods community. The studies were primarily based on dense-time models such as timed automata which can resolve the state space explosion problem of discrete-time models (e.g., timed transition models of Brandin & Wonham, 1994). However, most of the studies in the formal methods community focused on the state-based approach while this paper focuses on the language-based approach. For a language specification K, considering two different strings s_1, s_2 ($\in K$) reachable to one state q (i.e., $\delta_{act}(a_0, s_1) = \delta_{act}(a_0, s_2) = q$), the eligible time bounds for an event α defined at the reachable state can be different for the two strings, i.e., $el(s_1, \alpha) \neq el(s_2, \alpha)$ or $eu(s_1, \alpha) \neq eu(s_2, \alpha)$. This makes it difficult to specify eligible time bounds in terms of states. Although the language specification problem addressed in this paper can still be dealt with in timed automata models by using the formal methods such as on-the-fly algorithms and time-abstracting bisimulations (Tripakis & Altisen, 1999), the resulting presentation would be inevitably complicated as in this paper if we consider timed languages.

5. Example

To illustrate the main idea of this paper, we consider an uncertain timed DES $\mathcal{G}=\{G_1, G_2\}$ with the activity models $G_{1,act}$, $G_{2,act}$ and the single activity model G_{act} as shown in Fig. 1. The time bounds of the events are as follows: $(d_1, 1, 1)$, $(d_2, 1, 1)$, $(d_3, 1, 1)$, $(d_4, 1, 1)$, $(a, 1, \infty)$, $(b, 2, \infty)$, and $(c, 2, 3)$ where $(d_1, 1, 1)$ means $l(d_1) = 1$ and $u(d_1) = 1$. It is assumed that

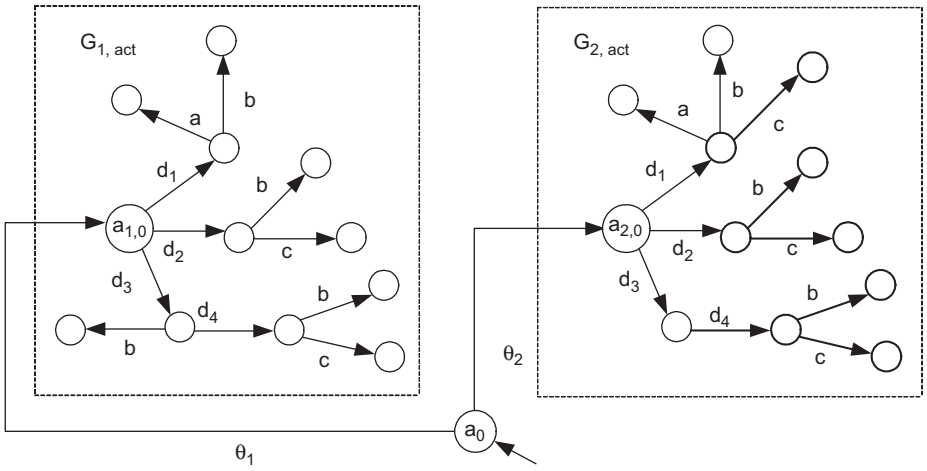

Fig. 1. The single activity model G_{act}.

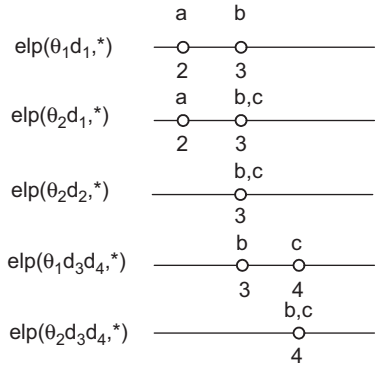

Fig. 2. The *elp* values.

$\Sigma_c = \{a, b\}$, $\Sigma_o = \{a, b, c\}$, and $\Sigma_{for} = \{a\}$. The *elp* values for some strings are shown in Fig. 2 where $elp(\theta_1 d_3 d_4, b) = 3$ is computed as follows: First, the event b is impending at $\theta_1 d_3 d_4$ since $b \in \Sigma_{L_{act}}(\theta_1 d_3) \cap \Sigma_{L_{act}}(\theta_1 d_3 d_4)$. We notice that there are no impending events except the event b at $\theta_1 d_3 d_4$. Then,

$$A_l(\theta_1 d_3 d_4, b) = el(\theta_1 d_3, d_4) = l(d_4) - A_u(\theta_1 d_3, d_4) = 1 - 0 = 1,$$

$$A_u(\theta_1 d_3 d_4, b) = eu(\theta_1 d_3, d_4) = C(\theta_1 d_3) = \min(u(b) - A_l(\theta_1 d_3, b), u(d_4) - A_l(\theta_1 d_3, d_4)) = \min(\infty - 0, 1 - 0) = 1,$$

$$C(\theta_1 d_3 d_4) = \min(u(b) - A_l(\theta_1 d_3 d_4, b), u(c) - A_l(\theta_1 d_3 d_4, c)) = \min(\infty - 1, 3 - 0) = 3,$$

$$el(\theta_1 d_3 d_4, b) = l(b) - A_u(\theta_1 d_3 d_4, b) = 2 - 1 = 1,$$

$$elp(\theta_1 d_3 d_4, b) = el(\varepsilon, \theta_1) + el(\theta_1, d_3) + el(\theta_1 d_3, d_4) + el(\theta_1 d_3 d_4, b) = 0 + 1 + 1 + 1 = 3.$$

We consider a language $\tilde{K}_1 = pr(\{d_1 a, d_1 b, d_2 b, d_3 d_4 c\})$ and then $K_1 = pr(\{\theta_1, \theta_2\}\tilde{K}_1) = pr(\{\theta_1 d_1 a, \theta_1 d_1 b, \theta_1 d_2 b, \theta_1 d_3 d_4 c, \theta_2 d_1 a, \theta_2 d_1 b, \theta_2 d_2 b, \theta_2 d_3 d_4 c\})$. For $s = \theta_2 d_1 \in K_1$, it follows that $c \in (\Sigma_{L_{act}}(s) \backslash \Sigma_{K_1}(s)) \cap \Sigma_{uc}$ and $B(K_1, s) = elp(s, c) = 3$. Through computations using this value, it turns out that $|\varepsilon|_{K_1} = g_1 \cup fl$ where $g_1 = \{\theta_1, \theta_2\}\{d_1, d_2\}$ ($s = \theta_2 d_1$ is a master of g_1). Then, it holds that $\Sigma_{K_1}(s) = \{a, b\}$, but $\{\alpha \in \Sigma_{K_1}(s) | elp(s, \alpha) < B(K_1, s)\} = \{a\}$ since $elp(s, a) = 2$ and $elp(s, b) = 3 = B(K_1, s)$. Thus, K_1 is not controllable w.r.t. $\mathcal{G}$. Moreover, for $s_1 = \theta_1 d_3 d_4$ and $s_2 = \theta_2 d_2$ satisfying $P_o(s_1) = P_o(s_2) = \varepsilon$, it holds that $s_1 c \in K_1$, $s_2 c \notin K_1$, but $T(K_1, s_1, c) \cap T(K_1, s_2, c) = \{4, 5\} \cap \{3, 4\} = \{4\} \neq \emptyset$. Hence, K_1 is not observable w.r.t. $\mathcal{G}$.

Throughout a similar procedure as in the above, we can show that for $\tilde{K}_2 = pr(\{d_1 a, d_2 c, d_3 d_4 c\})$, $K_2 = pr(\{\theta_1, \theta_2\}\tilde{K}_2)$ is controllable and observable w.r.t. $\mathcal{G}$. Then, according to Theorems 1 and 2, there exists a robust supervisor S satisfying $P_{act}(L(S/G_i)) = \tilde{K}_2$ for $i = 1, 2$. The supervisor can be designed following the definition presented in the 'if' part of the proof of Theorem 1. For instance, if there is no observed event at the initial state, $V(\varepsilon) = \{a\} \cup \Sigma_{uc}$, $I_e(\varepsilon, a) = T(K_2, \theta_1 d_1, a) \cup T(K_2, \theta_2 d_1, a) = \{2\} \cup \{2\} = \{2\}$, $I_e(\varepsilon, c) = T(K_2, \theta_1 d_2, c) \cup T(K_2, \theta_2 d_2, c) \cup T(K_2, \theta_1 d_3 d_4, c) \cup T(K_2, \theta_2 d_3 d_4, c) = \{3, 4\} \cup \{3, 4\} \cup \{4, 5\} \cup \{4, 5\} = \{3, 4, 5\}$, and $I_f(\varepsilon, a) = \{B(K_2, \theta_2 d_1) - 1\} = \{3 - 1\} = \{2\}$. If the timer $\tau(\varepsilon)$ reaches 2, the supervisor forces the event a to prevent the occurrence of the event c when d_1 has occurred. If d_2 has occurred, the forcing of the event a does not influence the occurrence of the event c since the forcible event a is not defined after d_2.

6. Conclusions

In this paper, we have shown that the controllability and observability are the existence conditions of a robust supervisor that can achieve a language specification for an uncertain timed DES. The results have been developed based on the notion of eligible time bounds in order to avoid the state space explosion problem of timed models.

Acknowledgments

This work was supported by the Korea Ministry of Science and Technology through the Korean Systems Biology Research Grant (M10503010001-07N030100112), the Nuclear Research Grant (M20708000001-07B0800-00110), and the 21C Frontier Microbial Genomics and Application Center Program (Grant MG05-0204-3-0), and in part from the Korea Ministry of Commerce, Industry and Energy through the Korea Bio-Hub Program (2005-B0000002). Also, this research was supported by the Ministry of Information and Communication (MIC), Korea, under the IT Foreign Specialist Inviting Program (ITFSIP) supervised by the Institute of Information Technology Advancement (IITA).

References

Bourdon, S. E., Lawford, M., & Wonham, W. M. (2005). Robust nonblocking supervisory control of discrete-event systems. *IEEE Transactions on Automatic Control*, *50*(12), 2015–2021.

Brandin, B. A. (1998). The modelling and supervisory control of timed DES. In *International workshop on discrete event systems WoDES'98* (pp. 8–14), Cagliari, Italy.

Brandin, B. A., & Wonham, W. M. (1994). Supervisory control of timed discrete event systems. *IEEE Transactions on Automatic Control*, *39*(2), 329–342.

Lin, F., & Wonham, W. M. (1995). Supervisory control of timed discrete event systems under partial observation. *IEEE Transactions on Automatic Control*, *40*(3), 558–562.

Maler, O., Pnueli, A., & Sifakis, J. (1995). On the synthesis of discrete controllers for timed systems. In *Proceedings of STACS'95. Lecture notes in Computer Science* (vol. 900, pp. 229–242).

Park, S.-J., & Cho, K.-H. (2006). Supervisory control of timed discrete event systems under partial observation based on activity models and eligible time bounds. *Systems and Control Letters*, *55*(5), 407–413.

Takai, S. (2000). Robust supervisory control of a class of timed discrete event systems under partial observation. *Systems and Control Letters*, *39*, 267–273.

Takai, S., & Ushio, T. (2006). A new class of supervisors for timed discrete event systems under partial observation. *Discrete Event Dynamic Systems: Theory and Applications*, *16*(2), 257–278.

Tripakis, S., & Altisen, K. (1999). On-the-fly controller synthesis for discrete and timed systems. In *World congress on formal methods*, *FM'99* (pp. 233–252).