Partial stochastic characterization
of timed runs over DBM domains

Laura Carnevali  Lorenzo Ridi  Enrico Vicario

Dipartimento di Sistemi e Informatica
Università di Firenze

PMCCS-9
September 18, 2009 - Eger, Hungary
Outline

1 Introduction
   - The addressed problem: an intuition
   - Contribution
   - Related work

2 partially stochastic Time Petri Nets

3 Characterization of symbolic runs
   - Domain of timings along a symbolic run
   - Timing boundaries enlargement
   - Partial stochastic characterization of timings
The addressed problem: an intuition

- Continuous-Time Discrete-Events Model
  - non-deterministic timings;
  - **controllable** timings are bounded within continuous intervals;
  - **non-controllable** timings are chosen by the system within a predictable range, following a given probability distribution.
  - (input/output transitions, actions/endogenous events)
The addressed problem: an intuition

- The system can execute along different firing sequences (symbolic runs);
  - the actual sequence is determined by values assumed by timers.

![Diagram of Time Petri Nets](image)

**Controllable events**
- $t_1$ with intervals $[3, 20]$ and $[10, 25]$
- $t_2$ with intervals $[0, 10]$ and $[5, 25]$
- $t_3$ and $t_4$

**Non-controllable environment**
- $t_1$
- $t_2$
- $t_3$
- $t_4$

Timeline:
- $0$ to $25$

Network:
- $t_1$, $t_4$, $t_3$, $t_2$
The addressed problem: an intuition

- **Problem**: force the system to run along a selected sequence.
  - controllable timers can be assigned arbitrary values;
  - success still depends upon values of non-controllable timers.

- The problem has a qualitative and a quantitative aspect:
  - identification of the range of valuations for controllable timers that can let the system run along the selected sequence (**qualitative** problem);
  - evaluation of the success probability for every choice of controllable timers (**quantitative** problem).
An introductory example

- 4 concurrent transitions;
- $t_1,t_2$: controllable transitions;
- $t_3,t_4$: non-controllable transitions;

**Problem:** select values for $t_1$ and $t_4$ so as to make possible/maximize the probability to execute the sequence $\rho = t_3, t_1, t_2, t_4$. 

[Diagram of Time Petri Nets with timed transitions and intervals]
Contribution

- **partially** stochastic Time Petri Nets
  - combines non-deterministic selection of controllable timers and stochastic sampling of non-controllable timers.

- evaluation of the **execution probability** of any firing sequence:
  - **support**: set of controllable choices that can let the system execute along the sequence;
  - **function**: distribution of the success probability as a function of values given to controllable timers.
Related work

- **Real-Time test case sensitization**
  - L. Carnevali, L. Sassoli, E. Vicario: ETFA ’07
  - qualitative approach: all timers are non-deterministic.
  - application in testing of real-time software (Linux RTAI).

- **stochastic Time Petri Nets**
  - G. Bucci, R. Piovosi, L. Sassoli, E. Vicario: QEST ’05
  - quantitative evaluation: all timers are stochastic.

- **Test case execution optimization on Timed Automata**
  - M. Jurdiński, D. Peled, H. Qu: FATES ’05
  - N. Wolowick, P. D’Argenio, H. Qu: ICST ’09
  - non-controllable timers are uniformly distributed.
partially stochastic Time Petri Nets: Syntax

\[ psTPN = \langle P; T^c; T^{nc}; A^+; A^-; m_0; EFT; LFT; \tau_0; C; F \rangle \]

- \( T \) partitioned: \( T^c \) controllable, \( T^{nc} \) non-controllable;
- \( F : T^{nc} \rightarrow \mathbb{F} \) associates each non-controllable transition with a static probability distribution \( F_t() \) supported in \([EFT(t), LFT(t)]\):

\[
F_t(x) = \int_0^x f_t(y) \, dy
\]
Tokens move as in Petri Nets (logical locations);
each transition $t$ has an Earliest and a Latest Firing Time ($EFT(t)$ and $LFT(t)$), and an initial time to fire $\tau_0(t)$.

- $t$ cannot fire before it has been enabled with continuity for $EFT(t)$;
- neither it can let time advance without firing after it has been enabled with continuity for $LFT(t)$;
- firings occur in zero-time.
**partially stochastic Time Petri Nets: Analysis**

- **state** \( s = \text{marking} + \text{valuation} \) of transitions times-to-fire
- **state class** \( S = \text{marking} + \) continuous set of times-to-fire
  - timers within the same state class range in a **Difference Bound Matrix (DBM)** zone.
  
  \[ \tau_i - \tau_j \leq b_{ij} \]

- **Remark**: every state (class) may jointly enable controllable and non-controllable transitions, thus combining **stochastic** and **non-deterministic** behavior.
**State class graph enumeration**

- **AE reachability relation** between state classes:

**Definition: AE reachability relation**

Given two state classes $S$ and $S'$ we say that $S'$ is a successor of $S$ through $t_0$ iff $S'$ contains all and only the states that are reachable from some state collected in $S$ through some feasible firing of $t_0$.

- Enumeration $\rightarrow$ Timed Transition System (state class graph);
- DBM form is closed wrt successor evaluation;
- **symbolic runs** are paths in the state class graph.
Consider a symbolic run $\rho$ starting from class $S^0$, terminating in $S^N$;

- $t^n_i$ is the instance of transition $t_i$ enabled along $\rho$ in class $S^n$;
  - associated to an **absolute virtual** firing time $\tau^n_i$;

absolute firing times feasible for $\rho$ satisfy three kinds of constraints:

1. model constraints;
2. disabling constraints;
3. sequence constraints.
1 Model constraints

- time elapsed between enabling and firing of each transition $t_i^n$ fired along $\rho$ must range within its static firing interval:

$$EFT(t_i) \leq \tau^n_i - \tau^\nu(n) \leq LFT(t_i)$$

where $t^\nu(n)$ enables $t^n_i$
2 Disabling constraints

- if transition $t^n_x$ is enabled but not fired along $\rho$, its absolute firing time must be greater than the one of its disabling transition $t^\delta(x,n)$:

$$\tau^n_x \geq \tau^\delta(x,n) \text{ where } t^\delta(x,n) \text{ disables } t^n_x$$

$t^n_x$ is enabled

$t^\delta(x,n)$ fires $(t^n_x$ is disabled)
3 Sequence constraints

- transitions must fire in the expected sequence:

$$\tau_{\nu(n+1)} \geq \tau_{\nu(n)} \forall n \in [0, N - 1]$$

$$\tau_{\nu(n)} - \tau_{\nu(n-1)}$$

$$\tau_{\nu(n)}$$ fires
(class $$S_{n}$$ is entered)

$$\tau_{\nu(n-1)}$$ fires
(class $$S_{n-1}$$ is entered)
Domain of timings along a symbolic run

- timers of transitions enabled along $\rho$ are encoded in two vectors $\tau^c$ and $\tau^{nc}$;
- the set of valuations $(x, y)$ of timers $(\tau^c, \tau^{nc})$ that are feasible for $\rho$ is a DBM domain $D_\tau$:

```
LFT^s(t_{nc})
EFT^s(t_{nc})
```

```
EFT^s(t_c)
LFT^s(t_c)
```
The problem of domain enlargement

- Non-controllable timers can take values outside $D_{\tau}$; must be taken into account to evaluate the probability of successful execution;
- **enlarged** domain $D_{\tau}$ includes divergent behaviors:
  - controllable timers conform to $D_{\tau}$;
  - non-controllable timers satisfy model constraints.
Main result:
distribution of the probability of successful execution

- **family of functions** $f_{\tilde{\tau}^{nc}}(\tau^{nc})(x)$:
  - for each selection $x$ of controllable timers, probability density function of non-controllable timers.
  - for a valuation $x = x_1$ of controllable timers, the integral of function $f_{\tilde{\tau}^{nc}}(\tau^{c})(x_1)$ over domain $D_{\tau^{nc}}(x_1)$ represents the probability to execute $\rho$ under the assumption of the choice $x_1$ on controllable timers.

\[
f_{\tilde{\tau}^{nc}}(\tau^{nc})(x) = \prod_{t^n_i \in A^{nc}} f_{t_i}(y^n_i - y^{v(n)}_{t_i(n)}) \cdot \prod_{t^n_i \in A^{nc}} f_{t_i}(y^n_i - x^{v(n)}_{t_i(n)})
\]
The integral of the whole family of function over $D_{\tau^{nc}}(x)$ defines a new function $p(x)$;

- $p(x)$ associates each valuation of controllable timers with the execution probability of $\rho$:

$$p(x) = \int_{D_{\tau^{nc}}(x)} f_{\tilde{\tau}^{nc}}(\tau^{nc})(x) \quad d(\tau^{nc}) = \text{Prob}\{(x, y) \in D_{\tau} \mid \tau^c = x\}$$
we considered a **probabilistic extension** of Time Petri Nets;
we introduced a partial stochastic characterization of timed runs based on the definition of **controllable** and **non-controllable** timers;
we identified a measure of probability of successful execution of a run as a function of non-deterministic (controllable) variables.

**Ongoing work**

- **optimization** of $p(x)$ to maximize the execution probability;
- bring to application in (real) **real-time testing** (test case sensitization).