Statistical Model Checking

Axel Legay
INRIA Rennes and Aalborg University
and
Alexandre David
Aalborg University

February 28, 2012
Today’s objectives

- A brief introduction to priced timed stochastic automata
- A presentation of Uppaal-SMC
- Handling case studies in Uppaal-SMC
- Stochastic Abstraction (if time permits)
- The future of SMC
The Context

Previous lecture
SMC for pure stochastic systems
The Context

Previous lecture
SMC for pure stochastic systems

However ...
- Many systems highly depend on timed features
- Many systems are the composition of small independent sub-systems.
The Context

Previous lecture
SMC for pure stochastic systems

However ...
- Many systems highly depend on timed features
- Many systems are the composition of small independent sub-systems.

This lecture
SMC for component-based design of timed stochastic systems
The Objective

- Verifying properties of networks of automata mixing both continuous time and stochastic aspects
- Is the probability of reaching $q$ in less than $c$ unit of time greater than $\theta$?
- Clock rates should be general (energy problems, ...)
- Observation: Most of these questions are undecidable
The challenges

- How to combine stochastic and timed aspects?
- Which semantic shall we give to the model?
- How to overcome undecidability?

Solution

Statistical Model Checking for Networks of Priced Timed Stochastic Automata
The Priced Timed Automata Model (1)

Formal definition

A Priced Timed Automaton (PTA) is a tuple $A = (L, \ell_0, X, \Sigma, E, R, I)$ where: (i) $L$ is a finite set of locations, (ii) $\ell_0 \in L$ is the initial location, (iii) $X$ is a finite set of clocks, (iv) $\Sigma = \Sigma_i \cup \Sigma_o$ is a finite set of actions partitioned into inputs ($\Sigma_i$) and outputs ($\Sigma_o$), (v) $E \subseteq L \times \mathcal{L}(X) \times \Sigma \times 2^X \times L$ is a finite set of edges, (vi) $R : L \rightarrow \mathbb{N}^X$ assigns a rate vector to each location, and (viii) $I : L \rightarrow \mathcal{U}(X)$ assigns an invariant to each location.

As a summary, Timed Automata with:

- General clock constraints
- Input and output actions on discrete transitions
Example of three PTA

A0
x<=1

B0
y<=2

T0
C’==4

A1

B1

T1
C’==2

T3

A

B

T

A B T
Axel Legay INRIA Rennes and Aalborg University

Statistical Model Checking

And Alexandre D
The Priced Timed Automata Model (2)

**Definition**

The semantics of NPTAs is a timed labeled transition system whose states are pairs $(\ell, \nu) \in L \times \mathbb{R}^X_{\geq 0}$ with $\nu \models I(\ell)$, and whose transitions are either delay $(\ell, \nu) \xrightarrow{d} (\ell, \nu')$ with $d \in \mathbb{R}_{\geq 0}$ and $\nu' = \nu + R(\ell) \cdot d$, or discrete $(\ell, \nu) \xrightarrow{a} (\ell', \nu')$ if there is an edge $(\ell, g, a, Y, \ell')$ such that $\nu \models g$ and $\nu' = \nu[Y]$. We write $(\ell, \nu) \rightsquigarrow (\ell', \nu')$ if there is a finite sequence of delay and discrete transitions from $(\ell, \nu)$ to $(\ell', \nu')$.

**As a summary:**

Classical infinite-state transition semantic from timed automata
Networks of Priced Timed Automata (1)

- Compose Priced Timed Automata (component-based design of complex systems)
- Input-enabled, deterministic, non-zeno
- Disjoint sets of clocks
- Disjoint sets of outputs
- Inputs synchronize with Outputs
Networks of Priced Timed Automata (2)

Formal Definition

Let $\mathcal{A}^j = (L^j, X^j, \Sigma, E^j, R^j, I^j)$ (with $j = 1, \ldots, n$) be composable NPTAs. Their composition $(\mathcal{A}_1 | \ldots | \mathcal{A}_n)$ is the NPTA $\mathcal{A} = (L, X, \Sigma, E, R, L)$ where (i) $L = \times_j L^j$, (ii) $X = \bigcup_j X^j$, (iii) $R(\ell)(x) = R^j(\ell^j)(x)$ when $x \in X^j$, (iv) $I(\ell) = \bigcap_j I(\ell^j)$, and (v) $(\ell, \bigcap_j g_j, a, \bigcup_j r_j, \ell') \in E$ whenever $(\ell_j, g_j, a, r_j, \ell'_j) \in E^j$ for $j = 1, \ldots, n$. 
Example of NPTA

Observation: composite systems \((A|B|T)\) and \((AB|T)\) are timed (and priced) bisimilar.
Stochastic Semantic

- Independence between components
- Race: all the components propose a delay and an output
- Smallest delay is chosen
- Uniform delays for bounded intervals
- Exponential delays otherwise
- Composition may lead to complex distributions
Properties in PWCTL

Cost-based Logic

\[ \psi ::= P(\Diamond c \leq c \varphi) \sim p \mid P(\Box c \leq c \varphi) \sim p \]

Conceptually:

Classical PLTL with cost-measure on executions.
Back to Example (1)

Illustration

\[(A|B|T) \models P(\Diamond_{t \leq 2} T_3) = 0.75 \quad (A|B|T) \models P(\Diamond_{c \leq 6} T_3) = 0.75,\]
\[(AB|T) \models P(\Diamond_{t \leq 2} T_3) = 0.50 \quad \text{and} \quad (AB|T) \models P(\Diamond_{c \leq 6} T_3) = 0.50.\]
<table>
<thead>
<tr>
<th>Time</th>
<th>A</th>
<th>B</th>
<th>C</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0.15</td>
<td>0.30</td>
<td>0.15</td>
</tr>
<tr>
<td>0.7</td>
<td>0</td>
<td>0.30</td>
<td>0.45</td>
</tr>
<tr>
<td>1.4</td>
<td>0.30</td>
<td>0.60</td>
<td>0.75</td>
</tr>
<tr>
<td>2.1</td>
<td>0.45</td>
<td>0.75</td>
<td>0</td>
</tr>
</tbody>
</table>

### Diagrams

(a) Graph showing probability over time for different events.

(b) Graph showing probability with a different variable on the x-axis.
SMC for NPTA

- First, provide monitors and an engine to generate simulations
- Second, implement SMC algorithms
- Third, find a tool for timed systems in where you can implement all that easily!

Our Solution

UPPAAL-SMC
What is UPPAAL-SMC?
The first toolset for Statistical Model Checking of complex networks of timed stochastic automata
What is UPPAAL-SMC?

The first toolset for Statistical Model Checking of complex networks of timed stochastic automata.

Features:
- Friendly-user interface
- Feedback procedures
- Implements NPTAs
- Implements Various monitoring algorithms for complex logics
The Future of SMC

- Rare event systems
- Handling non-determinism
- Stochastic abstraction
- Distributing single simulations
- Bayesian Model Checking
- Nested Probabilities
- Runtime procedures
- More statistics, learning, stochastic abstraction, ...
  
- 

....