Reachability and Reward Checking for Stochastic Timed Automata

E. Moritz Hahn, Arnd Hartmanns, Holger Hermanns
Chinese Academy of Sciences, China / Saarland University, Germany
Talk Outline

1. Stochastic Timed Automata
   - Stochastic Timed Automata (STA)
   - Model Checking STA
   - Experimental Results

Reachability and Reward Checking for Stochastic Timed Automata

Arnd Hartmanns
Nondeterministic & Probabilistic

= unquantified = quantified
uncertainty uncertainty

[a, 1/2, 𝜏] {𝑐 \coloneqq 0} [b, 1/2, 𝜏] [𝑐 \geq 8, 𝜏]

MDP

LTS nondeterminism

DTMC discrete probabilities
Reachability and Reward Checking for Stochastic Timed Automata

Nondeterministic & Probabilistic & Timed
+ clocks
guards $c \geq 6$
invariants $c \leq 8$

P_{\text{max}}^\text{min?} (\Diamond \Box \land \text{time} < 8) = ?

Arnd Hartmanns  Reachability and Reward Checking for Stochastic Timed Automata
Stochastic Timed Automata

Nondeterministic & Probabilistic & Timed & Stochastic
+ sampling from arbitrary distributions

\[ P_{\text{max}}(\Diamond \Box \land \text{time} < 8) = ? \]
Stochastic Timed Automata

{c := 0}

wait for \( c = 8 \) when it causes most problems?

always wait until \( c = 8 \)?

\[ P_{\text{max}}(\Diamond \Box \land \text{time} < 8) = ? \]
Reachability and Reward Checking for Stochastic Timed Automata

\begin{align*}
\{ c := 0 \} & \quad + \quad c \geq 6 \quad + \quad [c \leq 8] \quad \Rightarrow \text{nondeterministic delay} \\
\{ c := 0, x := \text{UNI}(6,8) \} & \quad + \quad c \geq x \quad + \quad [c \leq x] \\
\Rightarrow \text{stochastic delay} & \quad = \text{specific resolution of the nondeterminism}
\end{align*}

\[
\begin{align*}
&\text{true} \\
a \quad &\frac{1}{2}, \{ c := 0, x := \text{EXP}(\lambda) \} \\
\frac{1}{2}, \{ c := 0 \} \quad &\frac{1}{2}, \{ c := 0 \} \\
&\text{true} \\
&\text{true}
\end{align*}
\]

\[ P_{\text{max}}(\diamond \Box \land \text{time} < 8) = ? \]
Nondeterministic & Probabilistic & Timed & Stochastic & Priced
+ rate and transition rewards

*: der(wait) = 1

**: {retries := retries + 1}

\[
\begin{align*}
E_{\text{max}}(\text{wait} \mid \square) &= ? \\
c \leq x & \xrightarrow{1/2,\{c := 0, x := \text{EXP(\lambda)}\}} c \geq x, b & \text{true} \\
c \geq 6, \tau & \xrightarrow{1/2,\{c := 0\}} c \leq 8 & \xrightarrow{1/2,\{c := 0\}} c \geq 8, \tau & \text{true}
\end{align*}
\]
Stochastic Hybrid Automata

+ complex continuous behaviour

\[ \text{der}(v) = a \land v \cdot v_{max} \]

"Markovian" models

= exponentially distributed delays

memoryless

Arnd Hartmanns  Reachability and Reward Checking for Stochastic Timed Automata
**STA:** nondeterministic probabilistic stochastic \( \times \) choices delays \( + \) rewards

\[
\begin{align*}
true & \xrightarrow{a} c \leq x \quad \frac{1}{2}, \{c := 0, x := \text{EXP}(\lambda)\} \\
& \quad \frac{1}{2}, \{c := 0\} \\
c \geq 6, \tau & \quad c \leq 8 \\
& \quad c \geq 8, \tau \quad true
\end{align*}
\]

Arnd Hartmanns  Reachability and Reward Checking for Stochastic Timed Automata
Where are we?

1. Stochastic Timed Automata

2. Model Checking STA

3. Experimental Results

Arnd Hartmanns
Reachability and Reward Checking for Stochastic Timed Automata
Model Checking STA

Adapt existing method for SHA implemented in the prohver tool:

SHA → PHA

Forge existing method for SHA

upper bound on maximum reachability probabilities

\[ P(\text{crash within 15 years}) \leq 10^{-5} \]

+ min probabilities

+ max/min rewards

Overapproximation of continuous distributions

\[ x := \text{Norm}(m, 1) \}\}

\[ \text{discrete pr. choice of interval + nondeterministic value} \]
Overapproximation of continuous distributions

\[
\begin{align*}
  &true \\
  a \quad &\frac{1}{2}, \{c := 0, x := \text{EXP}(\lambda)\} \\
  \quad &\frac{1}{2}, \{c := 0\} \\
  &c \leq 8 \quad c \geq 8, \tau \\
  &true
\end{align*}
\]
Overapproximation of continuous distributions
Reachability and Reward Checking for Stochastic Timed Automata

Model Checking STA

Specialised method for STA

STA \xrightarrow{\text{approx.}} PTA \xrightarrow{\text{digital clocks}} MDP \xrightarrow{\text{iteration}} \text{results}

\begin{itemize}
\item upper bounds on max. reachability & rewards
\item lower bounds on min. reachability & rewards
\end{itemize}

prohver for SHA:

SHA \xrightarrow{\text{approx.}} PHA \xrightarrow{\text{labels}} HA \xrightarrow{\text{mod. PHAVER}} LTS \xrightarrow{\text{value iteration}} MDP \xrightarrow{\text{results}}

\text{label mapping}
Where are we?

1. Stochastic Timed Automata
   - STA
   - \( * \leq x \), \( c \geq x, b \rightarrow \text{true} \)
   - \( \frac{1}{2} \{ c := 0, x := \text{Exp}(\lambda) \} \)
   - \( \frac{1}{2} \{ c := 0 \} \)
   - \( c \geq 6, \tau \rightarrow \text{true} \)
   - \( c \leq 8 \)

2. Model Checking STA
   - STA \rightarrow \text{PTA} \rightarrow \text{MDP} \rightarrow \text{results}
   - \text{over-approx. digital clocks} \\
   - \text{other PTA model checking techniques}

3. Experimental Results
   - mcsta
Experimental Results

Implementation: mcsta tool

1. Automatic overapproximation
   unit-width intervals, single parameter $\varrho$:
   "remaining probability" for unbounded distributions

2. On-the-fly digital clocks semantics

3. Explicit-state MDP model checking

⇒ part of the Modest Toolset

www.modestchecker.net
Experimental Results

Example: M/G/1/6 queueing system

✧ arrivals: exponentially distributed
✧ service time: normal distribution

\[ P(\text{queue full within time bound}) = ? \]
Experimental Results

Example: M/G/1/6 queueing system

✦ arrivals: exponentially distributed
✦ service time: normal distribution

P(queue full within time bound) = ?
Experimental Results

Example: M/G/1/6 queueing system

- arrivals: exponentially distributed
- service time: normal distribution

Time-bounded reachability probability

\[ P(\text{queue full within time bound}) = ? \]

Time-unbounded expected accumulated reward

\[ E(\text{time until queue full}) = ? \]
\[ [43.4, \infty) \text{ (actually } \approx 61) \]
\[ E(\#\text{customers until queue full}) = ? \]
\[ [3.52, \infty) \text{ (actually } \approx 6.2) \]

136K MDP states only
Experimental Results

Example: tandem queueing system

CTMC benchmark

も多い dilatation
to reduce error

Example: WLAN (CSMA/CA)

uniform instead of nondeterministic transmission time

<table>
<thead>
<tr>
<th>model</th>
<th>type</th>
<th>$P_{\text{max}}$</th>
<th>$[E_{\text{min}}, E_{\text{max}}]$</th>
<th>$[E_{\text{min}}, E_{\text{max}}]$</th>
<th>$[E_{\text{min}}, E_{\text{max}}]$</th>
<th>states</th>
<th>time</th>
</tr>
</thead>
<tbody>
<tr>
<td>wlan</td>
<td>PTA</td>
<td>0.18359</td>
<td>[1325, 6280] μs</td>
<td>[450, 4206] μs</td>
<td>[450, 5586] μs</td>
<td>104804</td>
<td>8 s</td>
</tr>
<tr>
<td>wlan-uni</td>
<td>STA</td>
<td>0.13659</td>
<td>[2325, 4607] μs</td>
<td>[950, 3018] μs</td>
<td>[950, 3880] μs</td>
<td>264240</td>
<td>15 s</td>
</tr>
</tbody>
</table>
Experimental Results

Example: file server with slow archival storage
= \textbf{exponentially} distributed interarrival times for requests
+ \textbf{uniformly} distributed file size (= time to send reply)
+ \textbf{2\% chance} for file to be in slow archival storage
+ time for archive retrieval \textbf{nondeterministic} in [30, 40] s
+ initial queue length follows \textbf{discrete uniform} distribution
Stochastic Timed Automata

Model Checking STA

Experimental Results
Reachability and Reward Checking for Stochastic Timed Automata

*Arnd Hartmanns*

**Summary**

**Stochastic Timed Automata**
- **nondeterministic**
- **probabilistic**
- **stochastic**

**Model checking with mcsta**
- **choices**
- **delays**
- **rewards**

¬ bounds for reachability probabilities & expected rewards

State space nuclear explosion

Over-/underapproximation

**www.modestchecker.net**

**www.modestchecker.net**