École Temps-Réel 2017

Mardi 29 août 2017
Paris, France

IMITATOR dans une coquille de noix

Étienne André
LIPN, Université Paris 13, CNRS, France
Context: Verifying complex timed systems

- Need for early bug detection
  - Bugs discovered when final testing: expensive
- Need for a thorough specification and verification phase
Outline

1. Parametric timed automata in a nutshell
2. IMITATOR in a nutshell
3. A case study: Verifying a real-time system under uncertainty
4. What are we going to do in the TP?
Outline: Parametric timed automata in a nutshell

1. Parametric timed automata in a nutshell

2. IMITATOR in a nutshell

3. A case study: Verifying a real-time system under uncertainty

4. What are we going to do in the TP?
Beyond timed model checking: parameter synthesis

- Verification for **one** set of constants does not usually guarantee the correctness for other values

- Challenges
  - **Numerous verifications**: is the system correct for any value within [40; 60]?
  - **Optimization**: until what value can we increase 10?
  - **Robustness** [Markey, 2011]: What happens if 50 is implemented with 49.99?
  - **System incompletely specified**: Can I verify my system even if I don’t know the period value with full certainty?
Beyond timed model checking: parameter synthesis

- Verification for **one** set of constants does not usually guarantee the correctness for other values

- Challenges
  - **Numerous verifications**: is the system correct for any value within \([40; 60]\)?
  - **Optimization**: until what value can we increase 10?
  - **Robustness [Markey, 2011]**: What happens if 50 is implemented with 49.99?
  - **System incompletely specified**: Can I verify my system even if I don’t know the period value with full certainty?

- **Parameter synthesis**
  - Consider that timing constants are unknown constants (**parameters**)

É. André (Université Paris 13)
Parametric timed automata in a nutshell

**timed model checking**

A model of the system

A property to be satisfied

Question: does the model of the system satisfy the property?

Yes

No

Counterexample
Parametric timed model checking

A model of the system

A property to be satisfied

Question: for what values of the parameters does the model of the system satisfy the property?

Yes if...

\[ 2 \text{delay} > \text{period} \]
\[ \land \text{period} < 20.46 \]
Parametric Timed Automaton (PTA)

- Timed automaton (sets of locations, actions and clocks)

```plaintext
\begin{align*}
x &:= 0 \\
y &:= 0 \\
y &\leq 5; \\
x &\geq 1 \\
y &\leq 8;
\end{align*}
```

```plaintext
coffee!
press?
```

```plaintext
x &:= 0 \\
y &:= 8 \\
press?
```

```plaintext
cup!
```

É. André (Université Paris 13)
Parametric Timed Automaton (PTA)

- Timed automaton (sets of locations, actions and clocks) augmented with a set $P$ of parameters [Alur et al., 1993]
  - Unknown constants compared to a clock in guards and invariants

$$y = p_3$$
coffee!

$$x := 0$$
$$y := 0$$

$$x \geq p_1$$
cup!

$$x := 0$$
press?

$$y \leq p_2$$

$$y = p_2$$

$$y \leq 8$$
Outline

1. Parametric timed automata in a nutshell

2. IMITATOR in a nutshell

3. A case study: Verifying a real-time system under uncertainty

4. What are we going to do in the TP?
IMITATOR in a nutshell

IMITATOR

- A tool for modeling and verifying real-time systems with unknown constants

- Input language: parametric timed automata extended with
  - Communication through (strong) broadcast synchronization
  - Rational-valued shared discrete variables
  - Stopwatches, to model schedulability problems with preemption
Features of IMITATOR

- **Algorithms implemented in IMITATOR**
  - Computation of the symbolic state space
  - (non-Zeno) parametric model checking (using a subset of TCTL)
  - Language and trace preservation, and robustness analysis
  - Parametric deadlock-freeness checking
  - Behavioral cartography

- **Graphical output**
Inside IMITATOR

- Entirely programmed in OCaml

- Polyhedral operations computed using the Parma Polyhedra Library [Bagnara et al., 2008]

- Free and open source software: Available under the GNU-GPL license
IMITATOR: download and benchmarks

Under continuous development since 2008

[André et al., 2012]

A library of benchmarks

- Communication protocols
- Schedulability problems
- Asynchronous circuits
- ...and more
IMITATOR: download and benchmarks

Under continuous development since 2008 [André et al., 2012]

A library of benchmarks

- Communication protocols
- Schedulability problems
- Asynchronous circuits
- ...and more

Try it!

www.imitator.fr
Some success stories using IMITATOR

- Modeled and verified an asynchronous memory circuit by ST-Microelectronics
  - Project ANR Valmem

- Parametric schedulability analysis of a prospective architecture for the flight control system of the next generation of spacecrafts designed at ASTRIUM Space Transportation [Fribourg et al., 2012]

- Formal timing analysis of music scores [Fanchon and Jacquemard, 2013]

- Solution to a challenge related to a distributed video processing system by Thales
Outline

1. Parametric timed automata in a nutshell
2. IMITATOR in a nutshell
3. A case study: Verifying a real-time system under uncertainty
4. What are we going to do in the TP?
The FMTV 2015 Challenge (1/2)

Challenge by Thales proposed during the WATERS 2014 workshop
Solutions presented at WATERS 2015

System: an unmanned aerial video system with uncertain periods
- Period constant but with a small uncertainty (typically 0.01 %)
- Not a jitter!
The FMTV 2015 Challenge (2/2)

Goal

Compute the end-to-end BCET and WCET times for a buffer size of $n = 1$ and $n = 3$
The FMTV 2015 Challenge (2/2)

Goal

Compute the end-to-end BCET and WCET times for a buffer size of \(n = 1\) and \(n = 3\)

🤔 Not a typical parameter synthesis problem?
- No parameters in the specification
The FMTV 2015 Challenge (2/2)

Goal

Compute the end-to-end BCET and WCET times for a buffer size of \( n = 1 \) and \( n = 3 \)

😊 Not a typical parameter synthesis problem?
- No parameters in the specification

😊 A typical parameter synthesis problem
- The end-to-end time can be set as a parameter... to be synthesized
- The uncertain period is typically a parameter (with some constraint, e.g., \( P1 \in [40 - 0.004, 40 + 0.004] \))
Propose a PTA model with parameters for uncertain periods and the end-to-end time
Methodology

1. Propose a PTA model with parameters for uncertain periods and the end-to-end time
2. Add a specific location corresponding to the correct transmission of the frame
Methodology

1. Propose a PTA model with parameters for uncertain periods and the end-to-end time
2. Add a specific location corresponding to the correct transmission of the frame
3. Run the reachability synthesis algorithm EFsynth (implemented in IMITATOR) w.r.t. that location
Methodology

1. Propose a PTA model with parameters for uncertain periods and the end-to-end time
2. Add a specific location corresponding to the correct transmission of the frame
3. Run the reachability synthesis algorithm EFsynth (implemented in IMITATOR) w.r.t. that location
4. Gather all constraints (in as many dimensions as uncertain periods + the end-to-end time)
Methodology

1. Propose a PTA model with parameters for uncertain periods and the end-to-end time
2. Add a specific location corresponding to the correct transmission of the frame
3. Run the reachability synthesis algorithm EFsynth (implemented in IMITATOR) w.r.t. that location
4. Gather all constraints (in as many dimensions as uncertain periods + the end-to-end time)
5. Eliminate all parameters but the end-to-end time

Note: not eliminating parameters allows one to know for which values of the periods the best / worst case execution times are obtained.
Methodology

1. Propose a PTA model with parameters for uncertain periods and the end-to-end time
2. Add a specific location corresponding to the correct transmission of the frame
3. Run the reachability synthesis algorithm EFsynth (implemented in IMITATOR) w.r.t. that location
4. Gather all constraints (in as many dimensions as uncertain periods + the end-to-end time)
5. Eliminate all parameters but the end-to-end time
6. Exhibit the minimum and the maximum

Note: not eliminating parameters allows one to know for which values of the periods the best / worst case execution times are obtained.
To build the PTA model

- Uncertainties in the system:
  - P1 ∈ [40 − 0.004, 40 + 0.004]
  - P3 ∈ [\frac{40}{3} − \frac{1}{150}, \frac{40}{3} + \frac{1}{150}]
  - P4 ∈ [40 − 0.004, 40 + 0.004]
To build the PTA model

- Uncertainties in the system:
  - $P1 \in [40 - 0.004, 40 + 0.004]$
  - $P3 \in \left[\frac{40}{3} - \frac{1}{150}, \frac{40}{3} + \frac{1}{150}\right]$
  - $P4 \in [40 - 0.004, 40 + 0.004]$

- Parameters:
  - $P1_{\text{uncertain}}$
  - $P3_{\text{uncertain}}$
  - $P4_{\text{uncertain}}$
To build the PTA model

- **Uncertainties in the system:**
  - \( P_1 \in [40 - 0.004, 40 + 0.004] \)
  - \( P_3 \in \left[ \frac{40}{3} - \frac{1}{150}, \frac{40}{3} + \frac{1}{150} \right] \)
  - \( P_4 \in [40 - 0.004, 40 + 0.004] \)

- **Parameters:**
  - \( P_{1\text{-uncertain}} \)
  - \( P_{3\text{-uncertain}} \)
  - \( P_{4\text{-uncertain}} \)

- The end-to-end latency (another parameter): \( E2E \)
To build the PTA model

- Uncertainties in the system:
  - $P_1 \in [40 - 0.004, 40 + 0.004]$  
  - $P_3 \in \left[\frac{40}{3} - \frac{1}{150}, \frac{40}{3} + \frac{1}{150}\right]$  
  - $P_4 \in [40 - 0.004, 40 + 0.004]$  

- Parameters:
  - $P_1_{\text{uncertain}}$  
  - $P_3_{\text{uncertain}}$  
  - $P_4_{\text{uncertain}}$  

- The end-to-end latency (another parameter): $E2E$  

- Others:
  - the register between task 2 and task 3: discrete variable $\text{reg}_{2,3}$  
  - the buffer between task 3 and task 4: $n = 1$ or $n = 3$
Simplification

- T1 and T2 are synchronised; T1, T3 and T4 are asynchronous
  - (exact modeling of the system behaviour is too heavy)
Simplification

- T1 and T2 are synchronised; T1, T3 and T4 are asynchronised
  - (exact modeling of the system behaviour is too heavy)

- We choose a single arbitrary frame, called the target one

- We assume the system is initially in an arbitrary status
  - This is our only uncertain assumption (in other words, can the periods deviate from each other so as to yield any arbitrary deviation?)
The initialization automaton

\[ ckT_1T_2 = WCET_1 \]
The initialization automaton

\[
\text{camera0} \xrightarrow{\text{ckT1T2} = \text{WCET}_1} \text{camera1}
\]

\[
\begin{align*}
\text{buffer}_{3,4} &:= 0 \\
\text{highest}_{3,4} &:= 0
\end{align*}
\]

\[
\begin{align*}
\text{buffer}_{3,4} &:= 1 \\
\text{highest}_{3,4} &:= 1
\end{align*}
\]
The initialization automaton

\[ \text{camera0} \quad \text{ckT1T2} = \text{WCET}_1 \quad \text{buffer}_{3,4} := 0 \quad \text{highest}_{3,4} := 0 \]

\[ \text{camera1} \quad \text{ckT1T2} = \text{WCET}_1 \quad \text{buffer}_{3,4} := 1 \quad \text{highest}_{3,4} := 1 \]

\[ \text{camera2} \quad \text{ckT1T2} = \text{WCET}_1 \quad \text{frame}_{in \_3} := 0 \]

\[ \text{camera3} \quad \text{ckT1T2} = \text{WCET}_1 \quad \text{frame}_{in \_3} := 2 \]
The initialization automaton

\[
\begin{align*}
\text{camera}0 & \quad \text{buffer}_{3,4} := 0 \\
& \quad \text{highest}_{3,4} := 0 \\
\text{camera}1 & \quad \text{buffer}_{3,4} := 1 \\
& \quad \text{highest}_{3,4} := 1 \\
& \quad \text{frame}_{in \_ 3} := 0 \\
& \quad \text{frame}_{in \_ 3} := 2 \\
\text{camera}2 & \quad \text{reg}_{2,3} := 0 \\
& \quad \text{reg}_{2,3} := 3 \\
\end{align*}
\]
The initialization automaton

\[
\text{camera0: } \quad \text{buffer}_{3,4} := 0, \quad \text{highest}_{3,4} := 0
\]

\[
\text{camera1: } \quad \text{buffer}_{3,4} := 1, \quad \text{highest}_{3,4} := 1
\]

\[
\text{camera2: } \quad \text{frame}_{in\_3} := 0, \quad \text{frame}_{in\_3} := 2
\]

\[
\text{camera3: } \quad \text{reg}_{2,3} := 0, \quad \text{reg}_{2,3} := 3
\]

\[
\text{T1T2: } \quad \text{WCET}_1 + \text{WCL}_2 \geq \text{ckT1T2}
\]
The initialization automaton

\[ c_{kT_1T_2} = W\text{CET}_1 \]

\begin{align*}
\text{camera0} & : 
\begin{aligned}
\text{buffer}_{3,4} & := 0 \\
\text{highest}_{3,4} & := 0
\end{aligned} \\
\text{camera1} & : 
\begin{aligned}
\text{buffer}_{3,4} & := 1 \\
\text{highest}_{3,4} & := 1
\end{aligned} \\
\text{camera2} & : 
\begin{aligned}
\text{frame}_\text{in}_3 & := 0 \\
\text{frame}_\text{in}_3 & := 2
\end{aligned} \\
\text{camera3} & : 
\begin{aligned}
\text{reg}_{2,3} & := 0 \\
\text{reg}_{2,3} & := 3
\end{aligned} \\
\text{T1T2done} & : 
\begin{aligned}
\text{ckT1T2} & \geq W\text{CET}_1 + B\text{CL}_2 \\
\text{T2done} & \\
\text{reg}_{2,3} & := \text{target}
\end{aligned} \\
\text{T1T2} & : 
\begin{aligned}
\text{WCET}_1 + W\text{CL}_2 & \geq \text{ckT1T2}
\end{aligned}
\end{align*}
Task T3
Task T3

\[ WCET_T3 \geq ckT3 \]

\[ start \]

\[ WCET_T3 \geq ckT3 \]

\[ frame_in_3 = \text{reg} \]

\[ wcet_T3 = ckT3 \wedge búer_{3,4} = 0 \wedge \text{highest}_{3,4} \geq frame_in_3 \]

\[ T3_{\text{wait}} \]

\[ P3_{\text{uncertain}} = ckT3 \]

\[ T3_{\text{start}} = 0 \]

\[ wcet_T3 = ckT3 \wedge búer_{3,4} > 0 \]

\[ T3_{\text{done}} \]

\[ wcet_T3 = ckT3 \wedge búer_{3,4} = 0 \wedge \text{highest}_{3,4} \geq frame_in_3 \]

\[ T3_{\text{process}} \]

\[ T3_{\text{preinit}} \]
Verifying a real-time system under uncertainty

The PTA model for $n = 1$

Task T3

$\text{T3preinit}$

$\text{WCET}_3 \geq \text{ckT}_3$

$\text{start}$

$\text{T3process}$

$\text{WCET}_3 \geq \text{ckT}_3$

$\text{T3wait}$

$\text{P3\_uncertain} \geq \text{ckT}_3$

$\text{start}$
Task T3

\[ \text{WCET}_3 \geq \text{ckT}_3 \]

\[ \text{P}_3_{\text{uncertain}} = \text{ckT}_3 \]
\[ \text{T}_3 \text{ start} \]
\[ \text{ckT}_3 := 0 \]
\[ \text{frame in 3} := \text{reg}_{2,3} \]

\[ \text{WCET}_3 \geq \text{ckT}_3 \]

\[ \text{T}_3_{\text{wait}} \]

\[ \text{P}_3_{\text{uncertain}} \geq \text{ckT}_3 \]
Task T3

\[ P_{3\text{-}uncertain} = \begin{cases} 
    \text{ckT3} & \text{T3 \ start} \\
    0 & \text{ckT3} := 0 \\
    \text{frame\_in\_3} := \text{reg}_{2,3} 
\end{cases} \]

\[ \text{WCET}_3 \geq \text{ckT3} \geq \text{ckT3} \]

\[ \text{frame\_in\_3} > \text{highest}_{3,4} \]

\[ \text{T3\_done} \]

\[ \text{write\_by\_T3()} \]
Task T3

Verifying a real-time system under uncertainty

The PTA model for \( n = 1 \)

\[ \text{WCET}_3 \geq \text{ckT}_3 \]

\[ \text{P3\_uncertain} = \text{ckT}_3 \]
\[ \text{T3\_start} \]
\[ \text{ckT}_3 := 0 \]
\[ \text{frame\_in\_3} := \text{reg}_{2,3} \]

\[ \text{WCET}_3 = \text{ckT}_3 \]
\[ \land \text{buffer}_{3,4} = 0 \]
\[ \land \text{frame\_in\_3} > \text{highest}_{3,4} \]
\[ \text{T3\_done} \]
\[ \text{write\_by\_T3}() \]

\[ \text{WCET}_3 = \text{ckT}_3 \]
\[ \land \text{buffer}_{3,4} > 0 \]
\[ \text{T3\_done} \]

\[ \text{P3\_uncertain} \geq \text{ckT}_3 \]
Task T3

\[ WCET_T3 \geq ckT3 \]

\[ P3_{\text{uncertain}} = ckT3 \cap buffer_{3,4} = 0 \cap \text{highest}_{3,4} \geq \text{frame}_{in}_{3} \cap T3_{\text{done}} \]

\[ WCET_T3 = ckT3 \cap buffer_{3,4} = 0 \cap \text{frame}_{in}_{3} \cap \text{highest}_{3,4} \cap T3_{done} \cap write_{by}_{T3}() \]

\[ WCET_T3 = ckT3 \cap buffer_{3,4} = 0 \cap \text{highest}_{3,4} \geq \text{frame}_{in}_{3} \cap T3_{done} \]

\[ T3_{\text{preinit}} \]

\[ T3_{\text{process}} \]

\[ T3_{\text{wait}} \]

\[ T3_{\text{start}} \]

É. André (Université Paris 13)
Task T4

\[ \text{T4wait} \]

\[ P_{4\_\text{uncertain}} \geq ckT4 \]
Task T4

\[ P_{4\text{-}\text{uncertain}} = ckT_4 \land buffer_{3,4} > 0 \]
\[ ckT_4 := 0 \]
\[ \text{read\_by\_T4()} \]

\[ P_{4\text{-}\text{uncertain}} \geq ckT_4 \]
\[ 10 \geq ckT_4 \]
Task T4

\[
\begin{align*}
P_4\text{\_uncertain} &= \text{ckT4} \\
\text{buffer}_{3,4} &= 0 \\
\text{ckT4} &:= 0
\end{align*}
\]

\[
\begin{align*}
P_4\text{\_uncertain} &= \text{ckT4} \\
\text{buffer}_{3,4} &> 0 \\
\text{ckT4} &:= 0 \\
\text{read\_by\_T4()}
\end{align*}
\]

\[
\begin{align*}
P_4\text{\_uncertain} &\geq \text{ckT4} \\
10 &\geq \text{ckT4}
\end{align*}
\]
Task T4

\[ P_{4\_uncertain} = \text{ckT4} \]
\[ \land \quad \text{buffer}_{3,4} = 0 \]
\[ \text{ckT4} := 0 \]

\[ P_{4\_uncertain} = \text{ckT4} \]
\[ \land \quad \text{buffer}_{3,4} > 0 \]
\[ \text{ckT4} := 0 \]
\[ \text{read\_by\_T4()} \]

\[ P_{4\_uncertain} \geq \text{ckT4} \]

\[ 10 = \text{ckT4} \]
\[ \land \]
\[ \text{frame\_in\_4} \neq \text{target} \]

\[ 10 \geq \text{ckT4} \]
Task T4

\[ P_{4\_uncertain} = \text{ck}T_4 \]
\[ \land \quad \text{buffer}_{3,4} = 0 \]
\[ \text{ck}T_4 := 0 \]
\[ \text{T4wait} \]

\[ P_{4\_uncertain} = \text{ck}T_4 \]
\[ \land \quad \text{buffer}_{3,4} > 0 \]
\[ \text{ck}T_4 := 0 \]
\[ \text{read\_by\_T4()} \]
\[ \text{T4process\_nonempty} \]

\[ P_{4\_uncertain} \geq \text{ck}T_4 \]
\[ \land \quad \text{frame\_in\_4} \neq \text{target} \]

\[ 10 = \text{ck}T_4 \]
\[ \land \quad \text{frame\_in\_4} = \text{target} \]
\[ \text{ck}T_1T_2 = \text{E2E} \]
\[ \text{ck}T_4 := 0 \]
\[ \text{T4end\_ok} \]
Results

E2E latency results for $n = 1$ and $n = 3$

<table>
<thead>
<tr>
<th></th>
<th>$n = 1$</th>
<th>$n = 3$</th>
</tr>
</thead>
<tbody>
<tr>
<td>min E2E</td>
<td>63 ms</td>
<td>63 ms</td>
</tr>
<tr>
<td>max E2E</td>
<td>145.008 ms</td>
<td>225.016 ms</td>
</tr>
</tbody>
</table>

Results obtained using IMITATOR in a few seconds
Outline

1. Parametric timed automata in a nutshell
2. IMITATOR in a nutshell
3. A case study: Verifying a real-time system under uncertainty
4. What are we going to do in the TP?
Outline of the practical session

1. Perform parameter synthesis for a railway crossing system
Outline of the practical session

1. Perform parameter synthesis for a railway crossing system

2. Specify and verify the coffee machine
What are we going to do in the TP?

Outline of the practical session

1. Perform parameter synthesis for a railway crossing system

2. Specify and verify the coffee machine

3. ...and if you are fast: a free bonus exercise!
Bibliography
References I

Parametric real-time reasoning.
In *STOC*, pages 592–601. ACM.

IMITATOR 2.5: A tool for analyzing robustness in scheduling problems.

The Parma Polyhedra Library: Toward a complete set of numerical abstractions for
the analysis and verification of hardware and software systems.

Formal timing analysis of mixed music scores.
In *ICMC (International Computer Music Conference)*.

Robustness analysis for scheduling problems using the inverse method.
Robustness in real-time systems.
Additional explanation
Explanation for the 4 pictures in the beginning

Allusion to the Northeast blackout (USA, 2003)
Computer bug
Consequences: 11 fatalities, huge cost
(Picture actually from the Sandy Hurricane, 2012)

Error screen on the earliest versions of Macintosh

Allusion to the sinking of the Sleipner A offshore platform (Norway, 1991)
No fatalities
Computer bug: inaccurate finite element analysis modeling
(Picture actually from the Deepwater Horizon Offshore Drilling Platform)

Allusion to the MIM-104 Patriot Missile Failure (Iraq, 1991)
28 fatalities, hundreds of injured
Computer bug: software error (clock drift)
(Picture of an actual MIM-104 Patriot Missile, though not the one of 1991)
Licensing
Source of the graphics used I

Title: Hurricane Sandy Blackout New York Skyline
Author: David Shankbone
Source: https://commons.wikimedia.org/wiki/File:Hurricane_Sandy_Blackout_New_York_Skyline.JPG
License: CC BY 3.0

Title: Sad mac
Author: Przemub
Source: https://commons.wikimedia.org/wiki/File:Sad_mac.png
License: Public domain

Title: Deepwater Horizon Offshore Drilling Platform on Fire
Author: ideum
Source: https://secure.flickr.com/photos/ideum/4711481781/
License: CC BY-SA 2.0

Title: DA-SC-88-01663
Author: imcomkorea
Source: https://secure.flickr.com/photos/imcomkorea/3017886760/
License: CC BY-NC-ND 2.0
Source of the graphics used II

Title: Smiley green alien big eyes (aaah)
Author: LadyofHats
Source: https://commons.wikimedia.org/wiki/File:Smiley_green_alien_big_eyes.svg
License: public domain

Title: Smiley green alien big eyes (cry)
Author: LadyofHats
Source: https://commons.wikimedia.org/wiki/File:Smiley_green_alien_big_eyes.svg
License: public domain

Title: Krups Vivo F880 home espresso maker
Author: Mike1024
Source: https://commons.wikimedia.org/wiki/File:Krups_Vivo_F880_home_espresso_maker.jpg
License: public domain

Title: Skizze eines offenen Bahnüberganges
Author: MichaelFrey
Source: https://commons.wikimedia.org/wiki/File:Schranke_fast_oben.svg
License: CC BY-SA 3.0
Source of the graphics used III
License of this document

This presentation can be published, reused and modified under the terms of the license Creative Commons Attribution-ShareAlike 4.0 Unported (CC BY-SA 4.0)

(LaTeX source available on demand)

Author: Étienne André

https://creativecommons.org/licenses/by-sa/4.0/