Verification of Two Real-Time Systems Using Parametric Timed Automata
Youcheng Sun, Giuseppe Lipari, Étienne André

To cite this version:

HAL Id: hal-01240583
https://hal.archives-ouvertes.fr/hal-01240583
Submitted on 9 Dec 2015

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L’archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d’enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.
Verification of Two Real-Time Systems Using Parametric Timed Automata

Youcheng Sun  
Scuola Superiore Sant’Anna  
Pisa, Italy

Étienne André  
LIPN, Université Paris 13,  
Sorbonne Paris Cité, France

Giuseppe Lipari  
CRIStAL - UMR 9189  
University of Lille, France

Abstract—In this paper we propose solutions to the FMTV challenge of a distributed video processing system using the formalism of Parametric Timed Automata (PTA). The first challenge is harder because of the very large number of states to be analysed, so we only provide upper bounds. The second challenge consists of a real-time scheduling problem for which we provide exact solutions by using a scheduling analysis based on the critical instant, and a PTA model.

I. INTRODUCTION

With the increasing size and complexity of concurrent systems, the need for formal verification techniques has become higher and higher in the past decades. Systems mixing time and concurrency are especially subject to undesired behaviours (deadlocks, race conditions, etc.); often, their complexity makes the use of formal methods very challenging.

In this paper, we address the Formal Methods for Timing Verification Challenge (FMTV 2015) proposed by Thales (http://waters2015.inria.fr/challenge) by using the formalism of parametric timed automata (PTA). Timed automata (TA) [AD94] are a well-known formalism for specifying and verifying concurrent real-time systems. TA extend finite-state automata with a set of clocks (real-time variables growing linearly) that can be compared with integer constants. TA are used in several powerful tools such as UPPAAL [LPY97] or PAT [SLDP09]. However, the binary answer (“yes” or “no”) output by model checking is not always satisfactory; indeed, it does not allow to change or optimize some values of the system constants, nor (in general) to evaluate the system robustness, i.e., the infinitesimal variation of timing constants while preserving the reachability. PTA [AHV93] extend TA with rational-valued parameters allowed in place of constants. PTA are particularly well suited to verify systems where timing delays are known with uncertainty. The natural drawback of PTA is the infamous state space explosion, that may prevent the verification to be truly scalable. We will use the tool IMITATOR [AFKS12] that takes PTA as an input formalism.

Outline: We briefly review PTA and IMITATOR (Section II). Then, we recall the challenge (Section III). We derive solutions to Challenge 1A empirically (Section IV), and formally by using IMITATOR (Section V). We provide a different PTA model for the much harder Challenge 1B (Section VI) for which we derive an upper bound. Finally we analyse the problem in Challenge 2 and provide a solution based on schedulability analysis (Section VII-A) and a solution based on a PTA model (Section VII-B). Finally, we conclude in Section VIII.

II. PARAMETRIC TIMED AUTOMATA

Timed automata are finite-state automata augmented with clocks, i.e., real-valued variables increasing uniformly, that are compared within guards and invariants with timing delays [AD94]. Parametric timed automata (PTA) [AHV93] extend timed automata with parameters, i.e., unknown constants, that can be used in guards and invariants.

Given a set $X$ of clocks (real-valued variables) and a set $P$ of parameters (unknown rational-valued constants), a constraint $C$ over $X$ and $P$ is a conjunction of linear inequalities on $X$ and $P$. Given a parameter valuation (or point) $v$, we write $v \models C$ when the constraint where all parameters within $C$ have been replaced by their value as in $v$ is satisfied by a non-empty set of clock valuations.

Definition 1: A parametric timed automaton (PTA) $A$ is $(\Sigma, L, l_0, X, P, I, E)$ with $\Sigma$ a finite set of actions, $L$ a finite set of locations, $l_0 \in L$ the initial location, $X$ a set of clocks, $P$ a set of parameters, $I$ the invariant assigning to every $l \in L$ a constraint over $X$ and $P$, and $E$ a step relation consisting of elements $(l, g, a, R, l')$, where $l, l' \in L$, $a \in \Sigma$, $R \subseteq X$ is the set of clocks to be reset, and the guard $g$ is a constraint over $X$ and $P$.

The semantics of a PTA $A$ can be found in, e.g., [AHV93], [AS13].

Most problems related to PTA (e.g., the parametric reachability of a location) are undecidable [AHV93], [JLR15], with some decidable syntactic subclasses related to the use of the parameters [HRSV02], [BL09], [JLR15] or on the number of clocks [AHV93], [BO14], [BBLS15]. We do not consider it as drawback, as we use semi-algorithms that “often” terminate in practice; we will see this is also the case for solving challenge 1A.

IMITATOR [AFKS12] is a tool for modeling and verifying systems modeled using parametric timed automata. In its latest

1Note that this is a more general form than the strict original definition of PTA [AHV93]; since most problems for PTA are undecidable anyway, this has no practical incidence, and increases the expressiveness of the formalism.
version (2.7-beta2). IMITATOR implements several algorithms, among which:

- parametric reachability analysis: “find all parameter val-
  uations such that some state is reachable“
- parametric robustness analysis: “given a parameter val-
  uation ν, find other valuations for which the discrete
  (untimed) behavior is the same as ν”
- behavioral cartography: “find all parametric subspaces in
  which the discrete behavior is uniform”.

IMITATOR extends PTA with some useful constructions, such as constants, global discrete integer variables, strong broadcast synchronization between components, and stop-

The input syntax of IMITATOR is a text file, which makes
it possible to write models either manually or using scripts
(e.g., for large models derived from another formalism). For
example, in the past several parametric schedulability analy-

The task T1 periodically receives frames from the camera
and pre-processes them. Task T2 embeds further tracking

There are four tasks T1, T2, T3 and T4, distributed in differ-
ent processing units and performing respective functionalities.

Tasks T1, T3 and T4 are periodic, but their triggering clocks
are subject to drift. That is, their periods

Tasks T2 and T5 have access to a shared mutually exclusive
resource protected by the priority ceiling protocol. The access
to the shared resource takes 2ms for both tasks. 1) Compute the
best-case and worst-case end-to-end latencies from activation of
T6 to termination of T7 when \( J_6 = 0 \). 2) Compute the best and worst-case end-to-end latencies when \( J_6 = 20\)ms.

\[
\begin{align*}
\text{Challenge 1B:} & \quad \text{Given the different clock drifts, all frames with a same index may be discarded at the entrance of the buffer at the input of the task T4. Compute the minimum time distance between two frames produced by the camera that will not reach the display, for a buffer size } n = 3 \text{ (challenge 1B.3).} \\
\end{align*}
\]

\[
\begin{align*}
\text{Challenge 2B:} & \quad \text{Tasks T2 and T5 have access to a shared mutually exclusive resource protected by the priority ceiling protocol. The access to the shared resource takes 2ms for both tasks. 1) Compute the best-case and worst-case end-to-end latencies from activation of T6 to termination of T7 for a jitter value } J_6 = 0 \text{ms 2) compute the best-case and worst-case end-to-end latencies from activation of T6 to termination of T7 for a jitter value } J_6 = 20\text{ms. 3) The optimum priority assignment minimizing the worst-case latency for a jitter value } J_6 = 0 \text{ms and } J_6 = 20\text{ms.} \\
\end{align*}
\]

\[
\begin{align*}
\text{IV. SOLVING CHALLENGE 1A EMPIRICALLY} & \quad \text{First, we can try to find the latency using a manual es-
imation. We claim that the minimum latency occurs in the fol-
lowing scenario (times are given in ms):} \\
& \quad \text{1) The frame is output by the camera at } t = 0 \\
& \quad \text{2) The frame is processed immediately by Task T1 } t = 28 \\
& \quad \text{3) The frame is processed immediately by Task T2, which takes a minimal time (BCL}_2=17) \\
& \quad \text{4) The frame is processed immediately read task 3 } t = 45 \\
\end{align*}
\]

\[
\begin{align*}
\text{http://www-soc.lip6.fr/~bara/valmem/vhdl2ta/rapports/vhdl2ta-web/ vhdll2ta.html} \quad & \quad \text{2}
\end{align*}
\]
5) After task 3’s execution, the frame is inserted into an empty buffer \( t = 53 \)

6) Immediately, the frame is got by task 4 \( t = 53 \)

7) Task T4 processes the frame and sends it to display \( t = 63 \)

In fact nothing prevents this scenario to happen: with tasks appropriately synchronised with each other, this scenario can indeed happen. That is, 63ms is the exact minimum latency. Even with \( n = 3 \), the fastest scenario built above still holds. And the minimum latency is still 63 ms.

Then, we claim that an upper bound on the maximum latency occurs in the following scenario (times are given in ms):

1) The frame is output by the camera \( t = 0 \)

2) The frame is processed immediately by task 1 \( t = 28 \)

3) The frame is sent to task 2, which takes a maximal time \( \text{WCL}_{2}=19 \)\( t = 47 \)

4) The frame can stay within \text{Register23} for at most \( P_1 \) ms before it is overwritten by the successive frame \( t \leq 87.004 \)

5) Task T3 processes the frame and puts it in \text{Buffer34} \( t \leq 95.004 \)

6) \text{Buffer34} can host the frame for at most \( P_4 \) ms \( t \leq 135.008 \)

7) Task T4 takes 10ms to execute the frame \( t \leq 145.008 \)

Thus, an upper bound to the maximal latency is 145.008ms. For the maximum latency with \( n = 3 \), based on the result with \( n = 1 \) we can derive a safe upper bound immediately. This upper bound is \( \leq 145.008 + 2 \times P_4 \leq 225.016 \) ms.

V. SOLVING CHALLENGE 1A USING IMITATOR

In this part, we formally solve the challenge using PTA. At first, we will solve the case with \( n = 1 \) for \text{Buffer34}. The corresponding PTA model is shown in Figure Fig. 1b. Later, we show how to adapt this model to a larger buffer.

Experimental environment: We used the latest version of IMITATOR (v2.7-beta2, build 1073) with no specific modification of the tool. We just used a small Python script to parse the long list of intervals that IMITATOR produces, and outputs to produce a single minimum and maximum. Sources, binary and models are available at [XP].

A. Camera, Task T1, Task T2

In order to reduce the state space, we model the camera, Task T1 and Task T2 into a single PTA (Fig. 1a). We also use this PTA to non-deterministically initialize the buffer and the frame currently processed by Task T4.

We choose an arbitrary frame with index \text{target} for end-to-end latency estimation and we start from the exact point such that the target frame is handled from Task T1 to task T2. A clock \text{ckT1T2} is initialised to be \text{WCET}_1 and measures the end-to-end latency of target frame. Discrete variables \text{frame_in_3} and \text{frame_in_4} represent the index of frames in Task 3 and Task 4 respectively. The value 0 is used to denote that there is no frame in a task. \text{reg}_{2,3} and \text{buffer}_{3,4} are for frames within \text{Register23} and \text{Buffer34}. While we assume frame index in the system is monotonically increased, \text{highest}_{3,4} denotes the highest frame index among frames having been stored inside the buffer. For the register, buffer and Task 3, they may or may not initially contain a frame.

We do not model the period of the camera (or task 1), since we are only interested in a single frame. Let us now model the buffer. IMITATOR does not support other kinds of global variables than discrete integer variables. For a buffer with one slot (\( n = 1 \)), its status can be modeled by using two discrete variables \text{buffer}_{3,4} and \text{highest}_{3,4}.

- \text{buffer}_{3,4} denotes the index of current frame inside \text{Buffer34};
- \text{highest}_{3,4} is the highest index recorded so far.

B. Task T3

The period of Task T3 is a parameter \text{P3_uncertain}, that is initialised as follows:

\[
\text{P3_uncertain} \in [40 - \text{P3_delta}, 40 + \text{P3_delta}]
\]

where \( \text{P3_delta} = 0.05 \% \times 40 = \frac{1}{200} \). Recall that parameters in PTA are unknown constants, i.e., the value of which cannot evolve during the execution; this is exactly what we need to model \text{P3_uncertain}.

Task T3 is modeled by a periodic PTA in Fig. 1b. \text{ckT3} is a clock variable for recording task 3’s activation and execution. At the initial point, the PTA T3 is non-deterministically waiting for a new activation or executing. When T3 finishes execution, it writes into \text{Buffer34} if the buffer is empty and its current frame has not been put into the buffer. We define a function call for this writing operation \text{write_by_T3}():

\[
\text{buffer}_{3,4} := \text{highest}_{3,4} := \text{frame_in_3}
\]

IMITATOR does not support function call in a model; here we still utilise the notation of function call for simplicity. Otherwise, task 3’s writing fails. As shown in PTA T3, we utilise the operator \( \text{"||"} \) ("or") in the edge representing writing failure. Again, this is for saving some space.

C. Task T4

We use here a modeling mechanism similar to Task T3. The period of Task T4 is a parameter \text{P4_uncertain}, that is initialised as follows:

\[
\text{P4_uncertain} \in [40 - \text{P4_delta}, 40 + \text{P4_delta}]
\]

where \( \text{P4_delta} = 0.01 \% \times 40 = 0.004 \).

Task T4 is modeled by a periodic PTA as in Fig. 1c. A clock variable \text{ckT4} is used for task 4’s periodic activation and execution. When T4 activates, If the buffer is empty, T4 goes directly back to another waiting cycle. According to the system specification, there should an empty processing session for task 4. However, such an empty processing does not affect the end-to-end latency of any frame, and we omit it in PTA T4. If the buffer is not empty, task 4 reads a frame from the buffer by the function call \text{read_by_T4}():

\[
\text{frame_in_4} := \text{buffer}_{3,4}, \text{buffer}_{3,4} := 0
\]
Task T4 takes 10ms to process a frame, after the processing, if its current frame is the target one, ckt4 is reset and T4 moves to an ending location. E2E ≥ 0 is the parameter for representing all possible end-to-end latencies of the target frame.

**D. Deriving the Latency for n = 1**

As we have seen, in order to avoid exploring the exact configurations in the system, we target a single frame (which explains the non-cyclic behavior of the PTA modeling the camera, tasks 1 and 2) that is output from the task 1 at \( t = \text{WCET}_1 \). The main idea is that, at \( t = \text{WCET}_1 \), the initial state must be arbitrary, i.e., encode all possible configurations that could happen in the system. However, such a model may be pessimistic for containing behaviors that cannot really happen in the system. Again, we aim to derive upper and lower bounds on end-to-end latency of an arbitrary frame.

After developing the model, we use IMITATOR to perform parametric reachability analysis of location T4end_ok, that is we ask IMITATOR to return all parameter valuations such that T4end_ok is reachable. Then, IMITATOR hides (using existential quantification) all parameters except E2E, and then returns a list of intervals for E2E. After some post-processing to unify intervals, we get

\[ E2E \in [63, 145.008] \]

This result is compatible with our empirical estimation. The maximum end-to-end latency is empirically bounded by explicitly considering the time a successive frame arrives; while the PTA model does not consider frames after the target one, the result by IMITATOR still matches the empirical reasoning.

**E. Deriving the Latency for n = 3**

For the case of \( n = 3 \) for Buffer34, we can keep the same IMITATOR model, with the exception of the buffer modeling.
We assume that access to elements in the buffer follows a FIFO manner.

Let us model Buffer34 for \( n = 3 \): besides the variable \( \text{highest}_{3,4} \), we need 3 more discrete variables for frames within each slot in the buffer: \( \text{buffer}_{1,3,4}^{1} \), \( \text{buffer}_{2,3,4}^{2} \), and \( \text{buffer}_{3,4}^{3} \). When non-deterministically initializing the buffer, we need to take into account all possible scenarios of frame occupation within it. When T3 writes into the buffer, it needs to find the first free position (say \( x \); thus the writing call becomes write_by_T3():

\[
\text{buffer}_{3,4}^{x} := \text{highest}_{3,4} := \text{frame in } 3.
\]

Similarly, for T4 to read from the buffer, we call the adapted function read_by_T4():

\[
\text{frame in } 4 := \text{buffer}_{3,4}^{x+1}, \quad \forall x \in \{1, 2\} \quad \text{buffer}_{3,4}^{x} := \text{buffer}_{3,4}^{x+1}, \quad \text{buffer}_{3,4}^{1} := 0.
\]

Note that the buffer status is also updated by the reading operation such that the first slot always contains the oldest frame.

Then, we can apply parametric analysis on the model for \( n = 3 \) using \textsc{imitator}. A projection of all possible values to parameter E2E gives the following result:

\[
\text{E2E} \in [63, 225.016] .
\]

Again, this matches our empirical estimation. Finally, we conclude results for Challenge 1A in Table I.

<table>
<thead>
<tr>
<th>Buffer34 size</th>
<th>min E2E</th>
<th>max E2E</th>
</tr>
</thead>
<tbody>
<tr>
<td>( n = 1 )</td>
<td>63 ms</td>
<td>63 ms</td>
</tr>
<tr>
<td>( n = 3 )</td>
<td>145.008 ms</td>
<td>225.016 ms</td>
</tr>
</tbody>
</table>

\text{TABLE I: E2E latency results for Challenge 1A}

VI. SOLUTION TO CHALLENGE 1B

This challenge is the most difficult to solve with a formal model. The first problem we encountered is that the analysis must keep track of many frames to measure the distance between two frame losses, and the number of frames to analyze can be very large.

In the long term the average rate of dropped frames depends on the rate between the period of the producer task (T1) and the period of the consumer task (T4). In particular, the average frame loss rate can be computed as \( (n_1-n_4)/\text{lcm}(P_{2\text{min}}, P_{4\text{max}}) \approx 0.005 \), where \( n_1 \) and \( n_4 \) are the number of instances of T1 and T4 in the hyperperiod between T1 and T4, respectively (and lcm the least common multiple). By computing the formula, the average distance between 2 frame losses is \( \approx 200 \) sec., i.e., one loss every 5000.5 frames. Therefore the minimum distance between two frame loss is \( \leq 200 \) seconds.

Unfortunately, computing the actual minimum distance is a very difficult task. First of all, due to clock drift, periods are fixed but they can vary in a small interval, so the hyperperiod can become very large. Also, Task T3 contributes to add a substantial amount of complexity: in fact, the period P3 is approximately one third of P2. Therefore, T3 will read the same frame more than once. However, the exact number of times that a frame is read (which we call frame repetition) depends on the periods and on the relative initial offset of T2 and T3. Also it depends on the actual latency of T2. Consider the situation depicted in Fig. 2. Here T2 writes the frame \( i \) in the register terminating at its worst-case latency, just a little bit after Task T3 has read frame \( i-1 \). Then T3 reads frame \( i \) twice. Finally the response time of the second instance of T3 is equal to its best case, so frame \( i+1 \) is written just before task T3 can read the register. This means that Frame \( i \) is only read twice. By inverting the sequence of response times of T2, it is possible to show that one frame can be read 4 times. Finally, obviously a frame can be read 3 times.

If T3 has a period that is exactly equal to the period of T1 divided by 3, it is possible to construct periodic sequences of repetitions. We denote these periodic sequences as \( \langle f_1, f_2, \ldots, f_{j-1} \rangle \), where \( f_1 \) denoted the repetitions of frames \( 0, j, 2j, \ldots \), \( f_2 \) denotes the repetitions of frames \( 1, j+1, 2j+1, \ldots \), and so on.

Of course, repetitions can obey any pattern, even non-periodic ones. Assume that \( P_3 = P_{1/3} \) and the offsets are as shown in Fig. 2. Then every possible sequence can be generated by the automaton in Fig. 3, that we call \textit{Sequence Automaton}. Depending on whether the response time of T2 is equal to the best case or to the worst-case (non deterministic choice), we generate the next repetition.

Therefore, our strategy for reducing the complexity of the model to something analysable is the following:

- We fix periods \( P_1 = P_2 = P_{1\text{min}}, \ P_3 = P_{2/3}, \ P_4 = P_{4\text{max}} \);  
- We model the sequence of frames generated by T2 with the Sequence Automaton;  
- The frame index is an integer number that varies in
\{0, 1, 2\}. In fact, it is easy to see that it is impossible to have 2 consecutive frame losses, and in the case of Buffer34 having only one position, there is no risk of conflicting indexes.

- Buffer34 is modeled by a discrete variable last and a counter with the number of frames in the buffer. Variable last maintains the index of the last frame successfully written in the buffer.
- Task T2 is modeled by a timed automaton that periodically tries to write the current frame in the buffer. The write is successful if the buffer is not full and if the frame index is different from last, in this case both variables are updated accordingly. Otherwise the frame is dropped. Every frame is repeated the number of times specified by the Sequence Automaton. After that, the frame index is increased (modulo 3) and a new repetition is generated. If the old frame index is not different from last, then the frame was not successfully written, and we signal the occurrence of a frame drop.
- The distance between two frame drops is measured by an automaton Observer that uses an appropriate clock from measuring this distance.

We do not report here the full model for space constraints: the interested reader can find it at [XP].

Even fixing the periods, the model is still non-deterministic due to the Sequence Automaton, and unfortunately after 18 hours of running time MITATOR had explored only 10 seconds of executions, generating a large number of states and never encountering two frame losses. Therefore we decided to further simplify the model by substituting the Sequence Automaton with a deterministic automaton that generates only periodic sequences. In this way the model becomes fully deterministic and can be analyzed in a relatively small time. Unfortunately we could not try all possible periodic sequences, nor we could try different values of the periods, therefore the computed values may not correspond to the minimal distance. The results are shown in Table II.

### Table II: Results of deterministic model for problem 1B

<table>
<thead>
<tr>
<th>Buffer</th>
<th>Sequence</th>
<th>limit</th>
<th>runtime</th>
<th>Dist.</th>
<th>Frames</th>
</tr>
</thead>
<tbody>
<tr>
<td>full</td>
<td>&lt; 2343 &gt;</td>
<td>60000</td>
<td>680</td>
<td>66.7133</td>
<td>1668</td>
</tr>
<tr>
<td>full</td>
<td>&lt; 24 &gt;</td>
<td>100000</td>
<td>2.005</td>
<td>66.7133</td>
<td>1668</td>
</tr>
<tr>
<td>empty</td>
<td>&lt; 2343 &gt;</td>
<td>60000</td>
<td>639.54</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>empty</td>
<td>&lt; 24 &gt;</td>
<td>150000</td>
<td>26880.23</td>
<td>199980</td>
<td>5000</td>
</tr>
</tbody>
</table>

We modeled the system following the scheduling framework for PTA proposed in [LSAF14]. We do not report here the full model for lack of space, it can be found at [XP]. We just summarize the main points:
The scheduler is modeled as a separate automaton, generated automatically from the priority ordering, and it interacts with the task automata using synchronization.

Variable execution times are modeled by non-deterministic choices.

Also, initial task offsets are modeled as non-deterministic choices: the period of T6 is $p_6 \in [0, P_6 - 32]$, whereas the period of T2 is $p_2 \in [0, P_2 - 17]$.

An observer automaton measures the end-to-end latency with a clock. Maximum and minimum latencies are modeled as parameters, exactly in the same way as the model developed for Challenge 1A.

Due to lack of time, we modeled only Challenge 2A, however an extension of the model to Challenge 2B is straightforward.

The model converges after 2 seconds to the same values as the ones computed by the schedulability analysis. This confirms the results and confirms the fact that this second challenge is much easier to solve than Challenge 1.

One potential benefit of using IMITATOR is that we can easily investigate the robustness of the solution with respect to variations in task worst-case execution times or periods by choosing them as parameters in the PTA model.

In the end, we report the results for Challenge 2 in Table III. As we discussed, the existence of a shared resource between T5 and T6 does not affect the latency for the chain T5-T7.

<table>
<thead>
<tr>
<th></th>
<th>min latency</th>
<th>max latency</th>
</tr>
</thead>
<tbody>
<tr>
<td>$J_6 = 0$ ms</td>
<td>49 ms</td>
<td>74 ms</td>
</tr>
<tr>
<td>$J_6 = 20$ ms</td>
<td>49 ms</td>
<td>94 ms</td>
</tr>
</tbody>
</table>

(a) The min/max latency

<table>
<thead>
<tr>
<th>T2&gt;T5&gt;T7&gt;T6</th>
<th>max latency</th>
</tr>
</thead>
<tbody>
<tr>
<td>$J_6 = 0$ ms</td>
<td>69 ms</td>
</tr>
<tr>
<td>$J_6 = 20$ ms</td>
<td>89 ms</td>
</tr>
</tbody>
</table>

(b) The optimal priority assignment

TABLE III: Results for Challenge 2

VIII. CONCLUSION

We proposed solutions to the FMTV challenge both using empirical analysis and formal methods based on PTA. Thanks to their expressiveness, PTA are especially convenient for modeling systems that contain some unknown but constant configurations. Challenges 1A and 1B were the most difficult, so we only provided upper bounds on results for them. The high complexity is mainly due to the large hyperperiods, therefore a complete model is intractable. We spent about one week for studying the problem and provide a model that could converge in a decent time.

Conversely, Challenge 2 is a scheduling problem, whose solution can be obtained quickly using schedulability analysis methods. The solution has been validated by a formal model based on PTA that took half a day to be built using the framework developed in [LSAF14], and only a few seconds to converge.

An advantage of using parametric model checking for challenge 1A is that we do not get only a min/max value for the end-to-end latency, but a list of all possible values according to our model. Furthermore, we also get the exact values of the periods that lead to the smallest and largest end-to-end latency, which can be of interest to better understand the model.

IMITATOR is the software tool we rely on for performing parametric analysis. IMITATOR turned out to be particularly well-suited for the analysis of such systems with period constants but with some (unknown) imprecision. We also note that we used the current version of IMITATOR, with no dedicated improvement for this challenge (with the exception of a small Python script to parse the result). Hence, this leaves space for improvements dedicated to these case studies, i.e., specific heuristics or simulation relations for ad-hoc reductions of the state space.

REFERENCES


