An Exact Schedulability Test for Non-Preemptive Self-Suspending Real-Time Tasks

Yalcinkaya, Beyazit; Nasri, Mitra; Brandenburg, Björn B.

DOI
10.23919/DATE.2019.8715111

Publication date
2019

Document Version
Accepted author manuscript

Published in
2019 Design, Automation & Test in Europe Conference & Exhibition (DATE)

Citation (APA)

Important note
To cite this publication, please use the final published version (if applicable). Please check the document version above.

Copyright
Other than for strictly personal use, it is not permitted to download, forward or distribute the text or part of it, without the consent of the author(s) and/or copyright holder(s), unless the work is under an open content license such as Creative Commons.

Takedown policy
Please contact us and provide details if you believe this document breaches copyrights. We will remove access to the work immediately and investigate your claim.
An Exact Schedulability Test for Non-Preemptive Self-Suspending Real-Time Tasks
— Extended Version —

Beyazit Yalcinkaya\textsuperscript{1,2}, Mitra Nasri\textsuperscript{1,3}, Björn B. Brandenburg\textsuperscript{1},
\textsuperscript{1} Max Planck Institute for Software Systems (MPI-SWS), Germany \textsuperscript{2} Middle East Technical University, Turkey \textsuperscript{3} Delft University of Technology, Netherlands

Abstract—Exact schedulability analysis of limited-preemptive (or non-preemptive) real-time workloads with variable execution costs and release jitter is a notoriously difficult challenge due to the inherent predictability advantages [1]. To counteract these inherent difficulties, one common practice is to insert fixed preemption points to break jobs into a sequence of segments, where each such segment is executed non-preemptively. However, it is well-understood to add tremendous complications to an already difficult problem. By mapping the scheduling to the Reachability Problem in timed automata (TA), this paper presents an exact schedulability test for this challenging model. Specifically, using TA extensions available in UPPAAL, this paper presents an exact schedulability test for sets of periodic and sporadic self-suspending tasks with fixed preemption points that are scheduled under a global fixed-priority scheduling policy. To the best of our knowledge, this is the first exact schedulability test for non- and limited-preemptive self-suspending tasks (for both uniprocessor and multiprocessor systems), and also the first exact schedulability test for the special case of global non-preemptive fixed-priority scheduling (for either periodic or sporadic tasks). Additionally, the paper highlights some subtle pitfalls and limitations in existing TA-based schedulability tests for non-preemptive workloads.

I. INTRODUCTION

The current state of the art in worst-case execution time analysis (WCET) favors non-preemptive execution due to its inherent predictability advantages [1]. To counteract these inherent difficulties, one common practice is to insert fixed preemption points to break jobs into a sequence of segments, where each such segment is executed non-preemptively. However, it is well-understood to add tremendous complications to an already difficult problem. By mapping the scheduling to the Reachability Problem in timed automata (TA), this paper presents an exact schedulability test for this challenging model. Specifically, using TA extensions available in UPPAAL, this paper presents an exact schedulability test for sets of periodic and sporadic self-suspending tasks with fixed preemption points that are scheduled under a global fixed-priority scheduling policy. To the best of our knowledge, this is the first exact schedulability test for non- and limited-preemptive self-suspending tasks (for both uniprocessor and multiprocessor systems), and also the first exact schedulability test for the special case of global non-preemptive fixed-priority scheduling (for either periodic or sporadic tasks). Additionally, the paper highlights some subtle pitfalls and limitations in existing TA-based schedulability tests for non-preemptive workloads.

Prior work. To the best of our knowledge, no exact schedulability test for non-preemptive (or limited-preemptive) self-suspending tasks has been proposed to date (for either uniprocessor or multiprocessor platforms).

Several exact schedulability tests have been introduced for preemptively scheduled uni- and multiprocessor platforms (i.e., for global fixed priority scheduling) [5]–[8] and for non-preemptive scheduling upon uniprocessor platforms for both sporadic [9,10] and periodic tasks [11]. None of these tests support self-suspending tasks. Further, even for the special case of non-preemptive global scheduling without self-susensions or preemption points, no exact test has been proposed to date.
The TA formalism has been previously leveraged in a number of schedulability tests for preemptive tasks scheduled by a global scheduling policy upon a multiprocessor platform [12–18]. These tests, however, are not designed for self-suspending tasks, cannot handle blocking times caused by non-preemptive execution, and some use stopwatches (e.g., [14,17,18]) that render the TA reachability problem undecidable [19]. As we discuss in Sec. III, the use of stopwatches significantly limits the practical applicability of the tests. There are further a few TA-based schedulability tests for non-preemptive tasks [14,20,21]. These tests, however, are limited to uniprocessors and do not support self-suspensions or preemption points.

Finally, prior work has yielded several sufficient schedulability tests for global non-preemptive scheduling that target either sporadic [22–25] or periodic tasks [26], but these tests do not support self-suspending or limited-preemptive tasks.

II. SYSTEM MODEL AND BACKGROUND

We consider a multiprocessor system with $m$ identical processors and a set of $n$ independent, self-suspending tasks $\tau = \{\tau_1, \tau_2, \ldots, \tau_n\}$. Each task $\tau_i$ is represented by a tuple $(T_i, D_i, O_i, P_i, k_i, S_i)$, where $T_i$ is the period (or equivalently, the minimum inter-arrival time), $D_i \leq T_i$ is the relative deadline, $O_i$ is the initial offset, $P_i$ is the priority, $k_i$ is the number of segments, and $S_i$ is the vector of segments of the task. Smaller values of $P_i$ indicate higher priorities. We assume global fixed-priority scheduling and that $P_1 < \ldots < P_n$.

The $j$th segment of a task $\tau_i$ is denoted by a tuple $S_{i,j} = ([s_{i,j}^{\min}, s_{i,j}^{\max}], [C_{i,j}^{\min}, C_{i,j}^{\max}])$, where $s_{i,j}^{\min}$ and $s_{i,j}^{\max}$ are the best-case suspension time (BCST) and worst-case suspension time (WCST), and $C_{i,j}^{\min}$ and $C_{i,j}^{\max}$ are the best-case execution time (BCET) and the worst-case execution time (WCET) of the segment, respectively. Our model implicitly supports release jitter, i.e., the first suspension prior to the first execution segment represents the release jitter of the task. Both the BCST and WCST can be zero for any or all of the segments, which turns such a segment boundary into a fixed preemption time (i.e., for a limited-preemptive task, $s_{i,j}^{\min} = s_{i,j}^{\max} = 0$ for $1 < j \leq k_i$). Once a segment starts execution it is not preempted until it finishes. If $k_i = 1$ for every $\tau_i \in \tau$, then the problem reduces to non-preemptive global scheduling.

We assume $C_i + X_i \leq D_i$, where $C_i = \sum_{j=1}^{k_i} C_{i,j}^{\max}$ is the total execution time and $X_i = \sum_{j=1}^{k_i} s_{i,j}^{\max}$ is the total suspension time of task $\tau_i$. The system utilization by $U = \sum_{i=1}^{n} U_i$, where $U_i = C_i/T_i$ is the utilization of task $\tau_i$. The execution time ratio of $\tau_i$ is given by $\beta_i = C_i/(C_i + X_i)$.

Timed automata. A timed automaton is a finite-state machine extended with a finite set of real-valued clocks that progress monotonically at the same rate and measure the time spent after their latest resets [4].\(^2\) UPPAAL\(^3\) extends the formal definition of timed automata with integer variables, structured data types, C-like programming constructs, specialized locations, and synchronization channels for modeling, simulating, and verifying real-time systems by defining them as networks of timed automata. In UPPAAL, the state of a system, i.e., a network of timed automata, is defined by the present locations of all timed automata, the values of all clocks, and the values of any discrete variables. Hence, the number of locations, clocks, and discrete variables has a significant effect on the size of the state space as well as the verification time.

Our schedulability test uses three special features of UPPAAL: committed locations, urgent channels, and broadcast channels. Whenever a state includes a committed location, the next transition must be one of the outgoing transitions of (one of) the committed location(s). Whenever a transition with an urgent channel is enabled, it must be taken without any time delay. Finally, a broadcast channel is used for synchronizing more than two timed automata: whenever a transition with a broadcast channel is taken, all other enabled transitions that use the same channel must be taken, too. When one location has multiple enabled transitions that use the same broadcast channel, UPPAAL selects one of them non-deterministically.

III. MOTIVATION AND PITFALLS

In this section, we discuss a few potential pitfalls and challenges related to the design of TA-based schedulability tests and the analysis of non-preemptive self-suspending tasks.

Stopwatch limitations. Since UPPAAL introduced stopwatch in version 4.1, several TA-based schedulability tests have used stopwatches for the analysis of preemptive and non-preemptive tasks [14,17,18]. However, in our experiments (Sec. V), we found that stopwatch-based tests are unable to provide any concrete schedulability answer even for very simple task sets. That is, due to the underlying undecidability result [19], instead of concluding that a task set is “schedulable” or “not schedulable,” the evaluated stopwatch-based tests yield “may not be schedulable” as the analysis result for almost all task sets, unless the task set has only two tasks and the total sum of WCETs is less than the shortest period. To the best of our knowledge, this is a new observation; prior work on stopwatch-based tests [14,17,18] did not report on empirical evaluations of the tests in the context of non-preemptive workloads.

Impossible event ordering. The ordering of the start times of jobs plays a crucial role in the analysis of non-preemptive tasks since it determines the amount of blocking incurred by high-priority tasks. To be exact, a schedulability test must hence discount any impossible orderings. However, some previous studies (e.g., [14,21]) have modeled tasks as independent TAs without synchronizing transitions related to their respective job releases. Consequently, tasks with the same release time could be scheduled in any order, including in orders contrary to their assigned priorities, which is actually impossible when a deterministic scheduling algorithm such as fixed-priority scheduling is used. As a concrete example, consider the following periodic task set, which is schedulable on a uniprocessor under non-preemptive fixed-priority scheduling.

---

1 For example, if a task $\tau_i$ has a minimum and maximum release jitter equal to $[s_{i,j}^{\min}, s_{i,j}^{\max}]$, then $s_{i,j}^{\min} = s_{i,j}^{\max} = s_{i,j}^{\max}$

2 This paper assumes the reader to be familiar with the timed automata formalism; an overview and tutorial may be found in [19,27].

3 http://www.uppaal.com
which is however deemed not schedulable by David et al.’s analysis [21] due to the inclusion of impossible event orderings.

**Counterexample 1.** When applying David et al.’s test [21] to the periodic task set $T_1 = (3, 3, 0, 1, 1, \{(0, 0), [1, 1]\})$ and $T_2 = (6, 6, 0, 2, 1, \{(0, 0), [3, 3]\})$, UPPAAL reports the following scenario to result in a deadline miss: at time 0, $T_2$ enters its ready location before $T_1$. Next, UPPAAL activates the scheduler, which dispatches the only job in the ready queue, i.e., $T_2$ (at time 0). This is allowed as the scheduler and task automata are independent of each other [21], i.e., UPPAAL is allowed to non-deterministically pick any enabled transition, including the scheduler transition. Finally, $T_1$ also moves to its ready location (still at time 0). However, the processor has already been allocated, so $T_2$ blocks $T_1$ for three time units. Consequently, $T_1$ is reported to miss its deadline at time 3. This, however, is actually impossible, since actual priority scheduling will always select the higher-priority task $T_1$ if both $T_1$ and $T_2$ release a job at exactly the same time (note the absence of release jitter). The problem can be avoided if, at time 0, both tasks are forced to synchronously move to their ready locations before the scheduler can be called.

UPPAAL’s scheduling framework [14], which uses stopwatches, reports “may not be schedulable” for this example.

**Suspension-oblivious analysis is unsound.** The following example shows that, given a self-suspending task set (either periodic or sporadic), if suspension segments are analyzed as if they were execution segments (i.e., using a suspension-oblivious approach [2]), then the resulting task set may be deemed schedulable while the original task set is in fact not schedulable. Hence, naïvely accounting for suspensions as execution time is not safe for limited-preemptive self-suspending tasks.

**Counterexample 2.** Consider three tasks $T_1 = (20, 6, 1, 1, 2, \{(0, 0), [1, 1]\}, ([1, 1], [1, 1]))$, $T_2 = (20, 20, 2, 2, 1, \{(0, 0), [3, 3]\})$, and $T_3 = (20, 20, 0, 3, 1, \{(0, 0), [3, 3]\})$. Fig. 1(a) shows that the task set is schedulable if suspension time is treated as execution time since $T_1$ can only suffer from one low-priority blocking, while in reality it can suffer from two such blockings and hence is not schedulable as shown in Fig. 1(b). This counterexample holds also for sporadic tasks.

**IV. PROPOSED SCHEDULABILITY TEST**

Our solution includes three TA templates for tasks (Task), the scheduler (SCHED), and an event synchronizer (SYNC), as shown in Figs. 2(a)–(c).\(^3\) Fig. 2(d) provides details of the functions used in the timed automata. A system with $n$ tasks requires $n$ Task instances, and one SCHED and one SYNC instance each. The SYNC automaton uses a broadcast channel synch, defined in Fig. 2(d), whose receivers are the Task automata. The SCHED automaton uses $n$ high-priority urgent channels called run to send signals to the Task automata. The system is schedulable if, in any reachable state, no TASK automaton resides in its Missed location.

**TASK.** This automaton models a periodic, segmented, self-suspending task with initial offset and release jitter. Each TASK automaton uses two clocks: $t$ keeps track of the arrival time (and deadline) of the task, while $x$ keeps track of the execution and suspension time of each segment. The initial offset of the task is enacted in the Start location, in which the automaton is forced to stay for offset time units. Next, the automaton enters the Suspended location, which realizes both release jitter and suspensions. A task stays Suspended nondeterministically for $x$ units of time, where $s_{\text{min}}(x) \leq s \leq s_{\text{max}}(x)$. The functions $s_{\text{min}}(x)$ and $s_{\text{max}}(x)$ return the minimum and maximum suspension duration of the current segment of the task (indicated by seg_idx), respectively.

When the suspension time (or initial jitter delay) has passed, the task enters the Ready location, where it waits until it receives a run signal from the scheduler to start its execution and enter the Running location. During this transition, it decreases the number of available processors by one as it starts executing on one of the processors. The task remains in the Running location until some time within the minimum and maximum execution time of the current segment, denoted by $c_{\text{min}}(x)$ and $c_{\text{max}}(x)$, respectively. When the task completes the execution of its current segment, it either enters the Completed location (if seg_idx indicates the last segment of the task), or goes back to the Suspended location to model the next suspension. Whenever the task leaves the Running location, it increments the current segment index as well as the number of available processors. If a task is not completed before its deadline, i.e., it is still in the Suspended, Ready, or Running location when $t$ exceeds deadline, then it enters the Missed location. A task enters the Completed location when it completes the execution of its last segment, and stays there until the next arrival time (i.e., the end of its period, as is indicated by $t == \text{period}()$).

The TASK automaton can be easily modified to realize a sporadic task by (i) adding a self-loop to the Completed location with guard “synch?” and removing the location invariant “$t <= \text{period}()$”, and (ii) replacing “$t == \text{period}$” with “$t >\text{period}$” on the transition from Completed to Suspended. The resulting automaton is discussed in the Appendix.

**SCHED.** This automaton is similar to the scheduler model used by David et al. [14,21] and realizes a global work-conserving

\(^3\)Fig. 2 differs in a minor way from the conference version. Specifically, the SYNC automaton first sends a first_synch signal followed by two synch signals (in the conference version, it simply sends three synch signals in a row). This modification is required to address a corner case in the analysis of limited-preemptive (non-suspending) tasks.
fixed-priority scheduler using a priority queue that stores a sorted list of tasks whose current segment is ready for execution. The first task in the list has the highest priority among all ready tasks. This automaton schedules a task as soon as there is a ready task in the queue and at least one processor available, in which case it sends a run signal to the highest-priority task.

**SYNCH.** The purpose of SYNCH is to synchronize the TASK automata such that all tasks that release a segment at a given time \( t' \) enter their Ready location at the same time before the scheduler is triggered. This construct serves to avoid the impossible event ordering problem mentioned in Sec. III.

Specifically, the SYNCH automaton uses a broadcast channel to synchronize the TASK automata. In UPPAAL, any receiver of a broadcast channel is forced to activate the transition that has the highest priority among all ready tasks, as indicated by an inner circle. The declarations of front(), enqueue(), and dequeue() have been omitted as they implement a standard priority queue.

Another important detail of the SYNCH automaton is that it always sends a sequence of three synchronization signals (one first_synch followed by two synch signals) due to the two committed locations that follow the Init location in the SYNCH automaton. This design covers corner cases in which a task finishes its execution exactly at the end of its current period and hence must be able to reach the Ready location from the Running location in the same instant (i.e., at the period boundary). This requires a forced multi-step transition from Running to Ready via Completed and Suspended without any passage of time, which in turn requires first a first_synch signal, as indicated in the transitions out of the Running location, and two subsequent synch signals to move from Completed to Suspended and then to Ready.

The reason for distinguishing between the first_synch and synch signals, and for using the first_synch signal to leave the Running location, is to align the SYNCH automaton’s sequence of three committed transitions with the TASK automaton’s multi-step transition. Specifically, this construction ensures that whenever a task leaves the Running location, it will receive a sufficient number of follow-up synch signals (i.e., two) to let the task automaton reach the Ready location if needed, which is required to ensure an exact analysis of limited-preemptive tasks that do not suspend in between segments.
This section answers the following questions: (i) How is the proposed test’s runtime affected by various system parameters, such as the number of cores, tasks, etc., and (ii) to what extent does it improve schedulability gain w.r.t. the state of the art?

We compared the proposed test against existing schedulability tests for global non-preemptive (G-NP) and global limited-preemptive (G-LP) scheduling in terms of average runtime and schedulability ratio (i.e., the fraction of task sets deemed schedulable for a particular set of parameters). We considered the following baselines: Guan et al.’s test [24] for any work-conserving G-NP policy (Guan-G-NP-WC), three tests for fixed-priority G-NP scheduling by Guan et al. [24], Lee et al. [25], and Nasri et al. [26] (denoted Guan-G-NP-FP, Lee-G-NP, and Nasri-G-NP, respectively), and Serrano et al.’s test for limited-preemptive scheduling [28] (Serrano-G-LP).

It should be noted that, with the exception of Nasri-G-NP [26], all baseline tests were designed specifically for sporadic tasks. We hence expect them to exhibit some degree of inherent pessimism when applied to periodic workloads (i.e., some feasible periodic workloads become infeasible if tasks exhibit sporadic arrivals). We focus on periodic tasks in the following and report on experiments involving sporadic tasks in the Appendix.

We generated periodic task sets following the guidelines of the Autosar benchmark introduced by Kramer et al. [29]. Specifically, for a given number of tasks $n$, we sampled the (non-uniform) distribution of common periods ($\{1, 2, 5, 10, 20, 50, 100, 200, 1000\}$)ms reported by Kramer et al. [29] to randomly draw a realistic period for each task. Due to UPPAAL’s restricted support for integer variables and parameters, we multiplied each period by ten to obtain integer values, respectively. Finally, for each segment, we assigned rate-monotonic priorities. Moreover, we performed four experiments by varying the number of cores (for $m \in \{1, 2, 4, 8\}$), $U=0.3 \cdot m$, one segment per task, and no suspensions).

We generated periodic task sets following the guidelines of the Autosar benchmark introduced by Kramer et al. [29]. Specifically, for a given number of tasks $n$, we sampled the (non-uniform) distribution of common periods ($\{1, 2, 5, 10, 20, 50, 100, 200, 1000\}$)ms reported by Kramer et al. [29] to randomly draw a realistic period for each task. Due to UPPAAL’s restricted support for integer variables and parameters, we multiplied each period by ten to obtain integer values, respectively. Finally, for each segment, we assigned rate-monotonic priorities. Moreover, we performed four experiments by varying the number of cores (for $m \in \{1, 2, 4, 8\}$), $U=0.3 \cdot m$, one segment per task, and no suspensions).

We performed four experiments by varying (Exp1) the number of cores and total utilization $U$ (for $U \in \{0.5m, 0.5m, 0.7m\}$, $n = 10$, one segment per task, and no suspensions); (Exp2) the number of tasks $n$ (for $m \in \{1, 2, 4, 8\}$, $U=0.3 \cdot m$, one segment per task, and no suspensions); (Exp3) the maximum execution time ratio $\beta$ (for $m \in \{1, 2\}$,
While our test confirms that schedulability improves with increasing $m$ and $n$ than by joint increases in $m$ and $U$.

**Discussion.** While the proposed test suffers from the typical scalability limitations expected from TA-based analyses, we nonetheless found it to be able to scale to periodic workloads of nontrivial size: up to 60 tasks on 2 cores, 30 tasks on 4 cores, and 15 tasks on 8 cores. The test performs worse when the number of possible execution scenarios increases, e.g., when there are more segments or longer suspension times (see Fig. 3(g)). Similarly, its runtime grows very quickly in the presence of sporadic tasks (as reported in the Appendix).

Nonetheless, our exact test provides a useful baseline for evaluating the accuracy of other, only sufficient tests. For instance, in the special case of G-NP scheduling (i.e., no preemption points, no suspensions), Nasri-G-NP is as accurate as the exact test while scaling much better: Figs. 3(e) and (f) show the Nasri-G-NP test to be three orders of magnitude faster.

**VI. CONCLUSION**

We have proposed the first exact schedulability test for limited-preemptive (and non-preemptive) self-suspending real-time tasks scheduled upon a uniprocessor or multiprocessor platform (under a global fixed-priority scheduling policy). We mapped the schedulability problem to the TA reachability problem, discussed some subtle pitfalls and limitations of prior TA-based schedulability tests, and proposed task, scheduler, and event synchronizer automata to realize an exact test. In addition to scaling to nontrivial workload sizes before succumbing to the state-space explosion problem, our work also provides the first exact baseline against which sufficient schedulability tests can be compared and thus enables future research into self-suspending and limited-preemptive models.

**REFERENCES**


Fig. 4. The TASK automaton for sporadic tasks.

There are only few differences between the periodic and sporadic task automata. First, in the sporadic TASK automaton, the Completed location has a self-loop with guard “synch?” to implement sporadic release behavior (i.e., a task does not necessarily release its next job after exactly $T_i$ time units).

Second, the invariant on the Completed location (i.e., ”$t <= period()$”) is removed so that the task can stay in this location even after its minimum inter-arrival time has been exceeded. Finally, we have replaced ”$t == period$” with ”$t >= period$” on the transition from Completed to Suspended so that this transition can be activated any time after the minimum inter-arrival time of the task has passed.

APPENDIX

Timed Automaton Model for Sporadic Tasks

Fig. 4 shows the TASK automaton for sporadic tasks. There are only few differences between the periodic and sporadic task automata. First, in the sporadic TASK automaton, the Completed location has a self-loop with guard “synch?” to implement sporadic release behavior (i.e., a task does not necessarily release its next job after exactly $T_i$ time units). Second, the invariant on the Completed location (i.e., “$t <= period()$”) is removed so that the task can stay in this location even after its minimum inter-arrival time has been exceeded. Finally, we have replaced “$t == period$” with “$t >= period$” on the transition from Completed to Suspended so that this transition can be activated any time after the minimum inter-arrival time of the task has passed.
Extended Experiments on Sporadic Task Sets

We conducted additional experiments on sporadic task sets to assess the scalability of the model shown in Fig. 4. Unfortunately, sporadic task behavior induces a much larger state space, which translates into substantially worse runtimes.

We used the same task set parameters that were generated for Exp2 in Sec. V (varying number of tasks for $n = \{2, 3, 4\}$) and assumed that every task is sporadic. Fig. 5 shows the observed runtime of the analysis for $m = 1$ and $m = 2$ cores and a varying number of tasks.

Fig. 5 shows that the runtime of the analysis increases exponentially with the increase in the number of sporadic tasks. This is due to the large number of possible release scenarios in sporadic task sets. Unfortunately, for $m = 1, n > 4$ and $m = 2, n > 3$, the analysis did not finish within the configured one-hour time budget. In conclusion, an exact yet scalable analysis of sporadic workloads remains a challenge for future work.