Model checking process algebra of communicating resources for real-time systems
Boudjadar, Abdeldjalil; Kim, Jin Hyun; Larsen, Kim Guldstrand; Nyman, Ulrik Mathias

Publication date:
2014

Document Version
Accepted author manuscript, peer reviewed version

Link to publication from Aalborg University

Citation for published version (APA):
Model Checking Process Algebra of Communicating Resources for Real-time Systems

A.Jalil Boudjadar, Jin Hyun Kim, Kim G. Larsen, Ulrik Nyman
Institute of Computer Science, Aalborg University, Denmark
{jalil,jin,kgl,ulrik}@cs.aau.dk

Abstract—This paper presents a new process algebra, called PACoR, for real-time systems which deals with resource-constrained timed behavior as an improved version of the ACSR algebra. We define PACoR as a Process Algebra of Communicating Resources which allows to express preemtiveness, urgentness and resource usage over a dense-time model. The semantic interpretation of PACoR is defined in the form of a timed transition system expressing the timed behavior and dynamic creation of processes. We define a translation of PACoR systems to Parameterized Stopwatch Automata (PSA). The translation preserves the original semantics of PACoR and enables the verification of PACoR systems using symbolic model checking in UPPAAL and statistical model checking UPPAAL SMC. Finally we provide an example to illustrate system specification in PACoR, translation and verification.

I. INTRODUCTION

More and more complex systems are being used in a safety and mission critical setting. Such systems need to be specified in a rigorous and formal way and proved to be safe and correct in practice. As a complement to the many transition system based formal models, process algebras provide a means of compact and precise formal specification framework with a calculi for checking properties. This paper defines an improved dense time process algebra (PACoR) and provides a link to verification tools which makes it relevant for practical verification.

Algebra of Communicating Shared Resources (ACSR)[4],[14] is a process algebraic approach to specify resource-constrained real-time systems. It introduces the notion of prioritized transitions based on a preemption relation of concurrent real-time processes. Recently, ACSR has become more relevant as multi-core systems are increasingly being used for real-time systems. ACSR has inspired Process Algebra for Demand and Supply (PADS)[16] to specify hierarchical scheduling systems. ACSR has been defined over a dense real-time semantics, however the underlying verification tools, VERSA[7] and XVERSA[6], have only been able to deal with the discrete time version. Moreover, ACSR has some difficulties in describing real-time systems. In the continuous-time version of ACSR timed actions cannot be restored after they have been preempted [4], which is contrary to actual real-time system implementations. This notion of processes being restored can be described in the discrete time version of ACSR, but only with the granularity of one time unit.

Inspired by ACSR, this paper presents a new process algebra, called Process Algebra of Communicating Resources (PACoR), to address the above issues. PACoR supports more expressive descriptions for timed actions in terms of the urgentness and preemtiveness. Moreover, we present translation rules from PACoR to Parameterized Stopwatch Automata (PSA) models which can be analyzed using UPPAAL and UPPAAL SMC. The translation preserves the semantics of PACoR. The rest of this paper is organized as follows: Section II presents the related work. Section III presents the syntax and semantics of PACoR. Section IV provides the translation rules. Section B provides a train platform system example. Finally section VI concludes the paper.

II. RELATED WORK

Process algebras, like CCS[15] and CSP[12], have originally been introduced as a formal way to rigorously describe concurrent and communicating systems together with a calculi for the verification of their properties. Over the years, different algebras have been developed for the specification and analysis of domain-specific systems like ACSR [4],[14], mCRL2 [11] for resource sharing, Timed CSP [17] for time modeling, etc.
mCRL2 is a process algebra that includes data and time suitable for the specification and verification of real-time systems. It enables local communication, multi-actions and communication-independent parallelism that are key concepts of component-based and hierarchical systems. A toolset supporting the verification of mCRL2 models has been developed[8]. However the syntactic richness of mCRL2 makes the semantics and interaction between the different concepts hard to grasp, and leads to state space explosion that affects verification.

An alternative to algebra based formalisms are timed automata-based formalisms [2],[9], where systems are described as a set of concurrent automata modeling the concrete timed behavior of the systems. Such formalisms enable certain flexibility when describing systems but may suffer to deal with hierarchy. The PACoR language is relatively compact in terms of syntax comparing to other algebra, but provides sufficient expressiveness to model resource sharing in real-time systems in an elegant way, and also enables effective dense-time analysis thanks to its timed semantics and to the UPPAAL toolsuite.
III. PACoR: Process Algebra of Communicating Resources

Process Algebra of Communicating Resources (PACoR) is a revised and improved version of ACSR for requirement specification of real-time systems. It adopts the concept of timed actions and event actions of ACSR. The execution of a timed action requires a set of resources (potentially empty) that are requested with individual priorities. The execution time is given as an interval between best and worst cases. Event actions are instantaneous, and two events (e.g. e and \( e' \)) synchronize if they are compatible. An internal action, represented by the distinguished event \( \tau \), cannot synchronize with any other action. Unlike ACSR, we have chosen in PACoR not to associate priorities to the event actions. The reason for this being that event actions are not resource consuming, while our language framework is resource based. Moreover, PACoR changes the meaning of the ACSR operator "\{\}" so that timed actions can be non-urgent and preemptive. Instead of \{\}, we introduce () as a urgent non-preemptive operator by which the execution of timed actions is never allowed to stop once it starts. The urgency can be loosened or hardened when the operators () and {} are composed with the scope operator \( \Delta \).

A resource requirement is specified as a pair \((r, pri)\) representing a resource name \( r \) and a priority \( pri \). An action is a (potentially empty) sequence of resource requirements. A timed action without any resource requirement is called empty-set timed action and denoted by \( \emptyset \) or \{\}. An action \( a \) can be either preemptible \( (\{a\}) \) or non-preemptible \( (\langle a \rangle) \) signifying whether it can be preempted by an action having a higher priority. Higher priorities have numbers greater than that of lower priorities. In PACoR, all priorities should be greater than 0, which is reserved for the empty-set timed actions. A timed action \( a^\delta \) is defined as an action \( a \) specified with a timed interval \( \delta \) representing the best and worst case execution time. We use \( D_R \) as a set of resources and \( D_E \) a set of events. We also use \( x, y, z \) for clock variables; \( P, Q \) for processes; \( R \) for natural numbers; \( l, m, n, u \) for time values; and \( \alpha \) and \( \beta \) for events and actions.

A. Syntax of PACoR

The syntax of PACoR is defined by the following grammar:

\[
P ::= \text{NIL} | \text{DONE} | A : P | E.P | P_1 + P_2 \\
    | P_1 || P_2 | [P] | P\backslash F | \text{recX}.P
\]

\[
A ::= A^\Delta(n, P_1, P_2) \mid A^\delta
\]

\[
E ::= \text{E}\backslash(n, P_1, P_2) \mid E
\]

\[
\Delta ::= \{S\} | \langle S\rangle
\]

\[
\text{E} ::= e \mid \bar{e} \mid \tau
\]

\[
S ::= e \mid (r, pri), S
\]

\[
\delta ::= [l; u]
\]

\( \text{NIL} \) is a process that cannot progress, meaning that it is in deadlock. \( \text{DONE} \) is a regular termination statement. There are two prefix operators, corresponding to actions and events respectively. The timed action operator \( A : P \) executes a resource-consuming action \( A \). \( A^\Delta \) executes a specific time bound \( \delta = [l; u] \), and then proceeds to the process \( P \). The event action operator \( E.P \) executes an event action instantaneously. Basically, the event actions are urgent, but they can be delayed by the scope operator. The Choice construct \( P_1 + P_2 \) represents a non-deterministic choice between two processes \( P_1 \) and \( P_2 \). The construct \( P_1 || P_2 \) represents the parallel composition of two processes \( P_1 \) and \( P_2 \) where they may progress synchronously or independently. PACoR includes also two scope constructors to bind timed and event actions to timing requirements. \( A^\Delta(n, P_1, P_2) \) binds the timed action \( A \) to a temporal scope and incorporates time-out and exception handlers. For a given time bound \( n \in \mathbb{R}^+ \cup \{\infty\} \), the scope may be exited in 3 ways: 1) if \( A \) successfully terminates using resources for \( \delta \) time units before the deadline \( n \), then the system proceeds to the following process; 2) if \( A \) fails to execute and misses its deadline \( n \), then the system proceeds to a time-out handler \( P_1 \); 3) the scoped timed action can intervene by an exception handler \( P_2 \) at any time. Urgent and non-preemptive timed actions associated with the scope operator \( \Delta \) can be delayed until resources are available, but they cannot cease using resources once they start the execution. In contrast, non-urgent and preemptive timed actions are enforced to execute as soon as they start by setting the deadline as same as the execution time. The Scope constructor \( \text{E}\backslash(n, P_1, P_2) \) for event actions binds an event action \( E \) to a temporal scope, which requires an event to happen within the temporal scope \( n \). The process \( P_1 \) executes when the event \( E \) does not happen within the temporal scope \( n \). The waiting of event \( E \) can be interrupted by an exception process \( P_2 \). The Close operator \( \text{recX} \) associates a special resource \( r_0 \) to all simultaneously enabled timed actions, so that all enabled timed actions including the empty-set timed action (\( \emptyset \) or \{\}) become comparable according to the priority relation. Moreover, it enables to choose a process among a set of processes using the same priorities for the same resources. The Restriction operator, \( P\backslash F \), limits the behavior of \( P \) in a way that no event with labels in \( F \) is permitted to execute. The construct \( \text{recX} : P \) denotes a (infinite) recursive process.

| System  | def  | \( [[D_1 || D_2 || T_1 || T_2] \backslash \{s_1, s_2\}] \) |
|---------|------|--------------------------------------------------|
| \( D_1 \) | def  | \( \emptyset^5 : s_1, D_1 \) |
| \( D_2 \) | def  | \( \emptyset^{10} : s_2, D_2 \) |
| \( T_1 \) | def  | \( s_1\backslash(\infty, \text{NIL}, \text{NIL}) \cdot C_1 \) |
| \( T_2 \) | def  | \( s_2\backslash(\infty, \text{NIL}, \text{NIL}) \cdot C_2 \) |
| \( C_1 \) | def  | \( \{\text{cpu}, 3\}^{[2, 3]} \Delta(5, \text{NIL}, \text{NIL}) : T_1 \) |
| \( C_2 \) | def  | \( \{\text{cpu}, 2\}^{[3, 3]} \Delta(7, \text{NIL}, \text{NIL}) : T_2 \) |

Example 3.1: Table I shows a PACoR example of two periodic tasks having the following attributes:
- \( T_1 \): Period 5, Execution Time: 2, Deadline: 5
- \( T_2 \): Period 10, Execution Time: 3, Deadline: 7
$D_1$ and $D_2$ periodically dispatch $T_1$ and $T_2$, whereas $C_1$ and $C_2$ are timed actions that require the resource $cpu$.

**B. Comparison of PACoR and ACSR Algebra**

<table>
<thead>
<tr>
<th>Table II</th>
<th>Expressiveness Comparison of ACSR and PACoR</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Attribute</strong></td>
<td><strong>ACSR</strong></td>
</tr>
<tr>
<td><strong>Timed Action</strong></td>
<td>Non-urgent &amp; Preemptive</td>
</tr>
<tr>
<td></td>
<td>Urgent &amp; Non-preemptive</td>
</tr>
<tr>
<td></td>
<td>Non-urgent &amp; Non-preemptive</td>
</tr>
<tr>
<td><strong>Process Creation &amp; Termination</strong></td>
<td>Static</td>
</tr>
<tr>
<td><strong>Verification Tools</strong></td>
<td>No</td>
</tr>
</tbody>
</table>

Table II compares ACSR Dense-Time and PACoR in terms of expressiveness for timed actions, processes creation, and verification tools. Notice that PACoR allows the preemption of timed actions. In ACSR, a process in which a timed action using a resource is preempted cannot restore the execution of such an action. For instance, the following is a typical way where process $P$ waits to use the resource $cpu$ in dense-time ACSR:

$$P \triangleq (cpu_1, 3)^5 : P'$$

In this ACSR specification, the process $P$ is idling until the resource $cpu$ is available. If $cpu$ is free, the timed action $(cpu_1, 3)^5$ starts its execution. However, it will be in a deadlock if the timed action can be preempted again. In contrast, PACoR specifies the non-urgent and preemptive timed actions in the following way:

$$P \triangleq (cpu_1, 3)^5 : P'$$

In this PACoR specification, $P$ can either execute the timed action $(cpu_1, 3)$ or wait for $cpu$. PACoR allows $P$ to restore and execute using the resource even if it is earlier preempted.

In addition to the static creation of processes, PACoR provides dynamic creation and termination of processes, adopting the new features of UPPAUΛ. In ACSR, a process never dies or terminates once it starts. In contrast, PACoR supports process termination, such a termination does not influence any process execution. In our framework, the static process creation can be supported by both UPPAUΛ and UPPAUΛ SMC verification techniques, but the dynamic process creation can be supported only by UPPAUΛ SMC.

**C. Timed Operational Semantics**

In the following, we define the semantics of PACoR in terms of a timed transition system (TTS). Such a semantics allows expressing both the discrete behavior of the process terms and the timed progress. Given a timed action $A$, the function $\rho(A)$ returns the set of resources required by $A$. The function $lp(A)$ states 1) the lowest priority of requests of action $A$ if $A$ has shared resources, 2) $lp(A) = 0$ if $\rho(A) = \emptyset$, otherwise 3) $lp(A) = 1$ if $A$ has no shared resources and $\rho(A) \neq \emptyset$. Moreover, we generalize the timed action priority relation in order to consider event actions, making then all action types comparable. This priority relation also functions as a preemption relation between timed actions, and thus specifies in which cases a timed action can preempt another timed action.

**Definition 3.1: (Priority Relation)** Given two actions $\alpha$ and $\beta$, we say that $\beta$ has priority over $\alpha$, denoted by $(\alpha < \beta)$, if one of the following cases holds:

1) $\alpha \in D_R$ and $\beta \in D_E$

2) Both $\alpha$ and $\beta$ are actions in $D_R$, where

$$\forall r \in \rho(\beta) \cap \rho(\alpha), \quad (r, p) \in \alpha \land (r, p') \in \beta \Rightarrow p < p'$$

According to the first condition, all instantaneous events have priority over timed actions. Besides, timed actions sharing a resource are arbitrated according to the second condition: if there exist resources shared by two timed actions $\alpha$ and $\beta$, then $\beta$ preempts $\alpha$ if and only if all the priorities of $\alpha$ over the shared resources are lower than the priorities of $\beta$ over the same resources. Our preemption relation is more strict than the ACSR preemption relation but helps to solve non-deterministic relations between tasks. Such a fact makes the system more deterministic.

**Example 3.2:** some relations between two timed actions can be as follows:

1) $\{(r_1, 2), (r_2, 5)\} \prec \{(r_1, 7), (r_2, 5)\}$

2) $\{(r_1, 2), (r_2, 5)\} \prec \{(r_2, 7), (r_3, 5)\}$

3) $\{(r_1, 2), (r_2, 5)\} \neq \{(r_1, 7), (r_2, 3)\}$

4) $\{(r_1, 2), (r_2, 0)\} \prec \{(r_1, 7)\}$

5) $\{(r_1, 2), (r_2, 1)\} \prec \{(r_1, 7)\}$

6) $\{(r_1, 3), (r_2, 3), (r_3, 1)\} \neq \{(r_1, 1), (r_2, 1), (r_3, 1)\}$

In ACSR, cases 2 and 4 are incomparable, no one has priority over the other, but in case 6 actions are comparable.

Let us first recall timed transition systems and their bisimulation relation. Timed Transition Systems (TTS) [13] represent an elegant model to define the semantics of real-time formalisms. Basically, a TTS is a labeled transition system where labels can be events or durations.

**Definition 3.2 (Timed transition System):** a timed transition system over an alphabet $\Sigma$ is a tuple $\langle S, S_0, \rightarrow \rangle$ where $S$ is a set of states, $S_0 \subseteq S$ is the set of initial states and $\rightarrow \subseteq S \times \Sigma \cup \{\tau\} \cup \mathbb{R}_{\geq 0} \times S$ is the transition relation.

Here and elsewhere, we write $s \triangleleft s'$ for any transition $(s, \lambda, s) \in \rightarrow$. Moreover, a transition is continuous if it is labeled by a real value from $\mathbb{R}_{\geq 0}$, otherwise the transition is discrete. TTSs are comparable via simulation and bisimulation relations. The simulation relation of TTSs establishes a mapping between their timed traces [1] where, from a common state, we check whether for each outgoing transition of the simulating system, a corresponding transition can be triggered in the simulated system.

We introduce the transition relation $\rightarrow_{\pi'} = \langle \pi' \rangle^*$ as a sequence of internal transitions such that for any event $\lambda$, $s \triangleleft_{\pi'} s' = s \triangledown_{\pi'} s_1 \triangledown_{\pi'} s_2 \triangledown_{\pi'} s'$. Such a transition relation enables to check the weak-bisimulation relation of TTS.

**Definition 3.3 (TTS simulation):** Given 2 TTSs $T_1 = \langle S_1, S_0^1, \rightarrow_1 \rangle$ and $T_2 = \langle S_2, S_0^2, \rightarrow_2 \rangle$ defined on the same alphabet $\Sigma$, $T_1$ simulates $T_2$ through a relation $\mathcal{R} \subseteq S_1 \times S_2$, denoted by $T_1 \sqsubseteq_{\mathcal{R}} T_2$, if $\forall s \in S_0^1 \exists s' \in S_0^2 ((s, s') \in \mathcal{R}$

3
We introduce \textit{ID} according to the following theorem, the TTS restriction \( T \). Accordingly, (\textit{The transition relation} \( \rightarrow \) \textit{denotes the execution of a regular timed action with respect to its execution of an} to know at any instant the owner process of a statement. The \textit{rules of Table III.} \textit{rules state a preemption of either an urgent or a non-urgent preemptive timed action.} \textit{E-success} rule is the same as A-success, for urgent (\( E \)) and non-urgent (\( E \{ n, P_1, P_2 \} \)) events execution, where no time elapses because events execution is instantaneous. Rule E-failure corresponds to the triggering of a timeout handler process when the execution of a non-urgent event misses its deadline. Rule Exception corresponds to the triggering of an exception handler process \( P_e \) when a non-urgent event or timed action is waiting to be triggered. Rule E-delay expresses a delay of a non-urgent event while the corresponding deadline \( n \) is respected. Rules E-ChoiceL and A-ChoiceL specify a non-deterministic choice between 2 executions, where the left hand statement is taken. A synchronization of 2 compatible events is described by rule E-sync. The resulting transition will be considered as an internal event (\( r \)) of the composition. E-AsyncL describes an asynchronous event of parallel composition. In rule A-sync, 2 concurrent timed actions progress together if they do not require the same resources. The execution time of such a synchronization will be the maximum of the execution time of both actions. \( A_1 \cup A_2 \) is the union of resource requests of both actions \( A_1 \) and \( A_2 \). The priority relation is not considered because actions \( A_1 \) and \( A_2 \) do not compete the same resources, so they are incomparable. Rule A-async corresponds to the execution of a timed action \( A_1 \) having priority over the concurrent timed action \( A_2 \). Rule Event-Action states that event actions have priority over timed actions. Rule NIL states a system deadlock if one of the concurrent processes reaches a \( NIL \) statement. In the rules explained above, the set of activated process identifiers \( ID \) is not updated when executing any transition because no process is created or killed on the execution of these transitions. Rule P-destroy states an on-the-fly destruction of a process once it reaches a \( DONE \) statement. The identifier of the corresponding process (\( Ident(DONE) \)) will be so removed from the set of active process identifiers \( ID \). For this reason, we propagated the process identifiers throughout transition rules in order to recognize the identifier of the owner process of each statement. Rule P-create expresses a dynamic creation of processes where the number of active processes in a system may differ from a state to another. The on-the-fly creation of a process [3] can be interpreted by the extension of the current system state by a new instance of such a process, where a fresh identifier is picked from the set of identifiers \( ID \) and assigned to such a process instance. Such a feature is recently integrated in the UPPaal tool suite [10].
TABLE III

<table>
<thead>
<tr>
<th>A-success</th>
<th>$m \in \mathbb{R}_{\geq 0}, l \leq m \leq u, \text{Ident}(P) := \text{Ident}(A^{[[l,u]]}; P)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>A-failure</td>
<td>$\langle A^{[[l,u]]} \Delta(n, P_l, P_e), x, ID \rangle \xrightarrow{m = n = 0} \langle P_l, x, ID \rangle$</td>
</tr>
<tr>
<td>Close</td>
<td>$m \in \mathbb{R}_{\geq 0}, \text{Ident}(P) := \text{Ident}(A^{[[l,u]]}; P)$</td>
</tr>
<tr>
<td>Preemption</td>
<td>$0 \leq m &lt; l, l' = l - m, u' = u - m$ $\langle {a}^{[[l,u]]}: P, x, ID \rangle \xrightarrow{m = n = 0} \langle {a}^{[[l',u']]}, P, x, ID \rangle$</td>
</tr>
<tr>
<td>E-success</td>
<td>$\text{Ident}(P) := \text{Ident}(E, P)$</td>
</tr>
<tr>
<td>E-failure</td>
<td>$m \in \mathbb{R}_{\geq 0}, m &lt; n, n' = n - m$ $\langle \mathcal{E}, P, x, ID \rangle \xrightarrow{(E,P), x, ID} \langle P_l, x, ID \rangle$</td>
</tr>
<tr>
<td>E-Delay</td>
<td>$m \in \mathbb{R}_{\geq 0}, m &lt; n, n' = n - m$ $\langle \mathcal{E}, P, x, ID \rangle \xrightarrow{(E,P), x, ID} \langle P_l, x, ID \rangle$</td>
</tr>
<tr>
<td>E-ChoiceL</td>
<td>$n &gt; 0, \text{Ident}(P) := \text{Ident}(E, P)$</td>
</tr>
<tr>
<td>E-Asyncl</td>
<td>$n &gt; 0, \text{Ident}(P) := \text{Ident}(E, P)$</td>
</tr>
<tr>
<td>A-sync</td>
<td>$\rho(A_1) \cap \rho(A_2) = \emptyset, m = \max_{i \in {A_1, A_2}}(A_i \cup A_2)$ $\langle A_1: P_l</td>
</tr>
<tr>
<td>Event-Action</td>
<td>$\rho(A_1) \cap \rho(A_2) = \emptyset, \langle A_1: P_l</td>
</tr>
<tr>
<td>P-destroy</td>
<td>$\langle \text{DONE}: P, x, ID \rangle \xrightarrow{m \in \mathbb{R}_{\geq 0}} \langle P, x, ID \setminus \text{Ident(DONE)} \rangle$</td>
</tr>
<tr>
<td>P-create</td>
<td>$\langle P, x, ID \rangle \xrightarrow{\text{fresh}(ID)} \langle P</td>
</tr>
</tbody>
</table>

IV. TRANSITION RELATION OF PACOR SEMANTICS

In order to analyze PACOR models automatically, we define a transition rewriting any PACOR description in terms of UPPAAL time automata, while UPPAAL and UPPAAL SMC tools can be applied to simulate the system execution and check the underlying properties. To this end, we consider timed automata using stopwatches [5], often called Prioritized Stopwatch Automata (PSA). Roughly speaking, stopwatches are clocks that can be stopped and resumed at any time, without reinitialization, during the system execution.

A. Parametrized Stopwatch Automata

The stopwatch concept [5] provides a sophisticated clock mechanism to measure the execution time of preemptive tasks. Such a mechanism enables to accumulate time when the action is running, and once the action is preempted the stopwatch clock makes a pause and resumes when the corresponding action resumes its execution. Given a set variables $\text{Var}$, by $C(\text{Var}) = \{x \times v | x \in \text{Var}, v \in \mathbb{R}\}$ we define the set of variable constraints of $\text{Var}$ where $\preceq \in \{<, \leq, >, \geq, =\}$.

Definition 4.1 (Parameterized Stopwatch Automaton): A stopwatch automaton over a set of channels $\Omega$ is given by a tuple $(Q, q^0, \text{Com}, C, \mathcal{V}, \mathcal{V}^0, \rightarrow, \text{Act}, \text{Inv})$ where $Q$ is a set of locations, $q^0 \in Q$ is the initial location, function $\text{Com} : Q \rightarrow \mathbb{B}$ states whether a location is committed or not, $C$ is a set of stopwatch clocks, $\mathcal{V}$ is a set of discrete variables initialized according to the valuation $\mathcal{V}^0$, $\rightarrow \subseteq Q \times C(\mathcal{C} \cup \mathcal{V}) \times \Omega! \cup \Omega? \cup \{\tau\} \times C \times Q$ is the transition relation where $\Delta : \{C \rightarrow \{0\}\} \cup \{\mathcal{V} \rightarrow \mathbb{R}\}$ is a set of actions that reset some clocks and update some discrete variables, $\text{Act} : Q \times C \rightarrow \mathbb{N}$ defines the set of actions that can be performed on stopwatch clocks at each location, and $\text{Inv} : Q \rightarrow C(\mathcal{C})$ associates to each location clock invariants.

We write $q_1 \xrightarrow{g/\lambda/\alpha} q_2$ for a transition $(q_1, g, \lambda, \alpha, q_2) \xrightarrow{d}$ outgoing from $q_1$ to $q_2$ guarded by $g$, labeled with $\lambda$ and performing the action $\alpha$ on clocks and discrete variables. In fact, we have used a long right-arrow $\rightarrow$ in order to distinguish the transition relation of PSA from that of TTS $\rightarrow$. $\text{Act}(q)(c) = v$ means that the first derivative of $c$ at location $q$ has value $v$, which represents the rate of progress each one time unit. So, for any duration $d$ the clock $c$ progresses
with \( v \times d \).

Therefore, a network of PSA is a set of concurrent PSA instances (processes) that can be created on the fly when needed. These processes are defined on the same set of channels where some clocks and variables can be shared. The dynamic creation of processes is the subject of a recent extension implemented in UPPAAL. Thus, the semantics is based on a dynamically evolving set of processes where at least one process (main) is immediately created when the system starts. For this reason, we associate to each process (template instance) an identifier \( Id \) enabling us to distinguish between the different instances of the same template. Moreover, we associate to each process a fresh variable \( loc \) stating the current location of the process. We also introduce \( f \triangleq g \) as the right overriding function where function \( g \) overrides function \( f \) for all elements in the intersection of their domains.

For all \( z \in \text{domain}(f \triangleq g) \),

\[
(f \triangleq g)(z) \triangleq \begin{cases} g(z) & \text{if } z \in \text{domain}(g) \\ f(z) & \text{if } z \in \text{domain}(f) \setminus \text{domain}(g) \end{cases}
\]

**Definition 4.2 (Semantics of a network of PSA):** Given a network of PSA \( \langle T_0, \ldots, T_n \rangle \) defined on the same set of channels \( \Omega \) where some discrete variables and clocks can be shared (global). Assuming that \( T_0 \) is the main (root) template of our network. We associate the identifier \( Id_0 \) and variable \( loc \) to the first instance of \( T_0 \). The semantics of network \( \langle T_0, \ldots, T_n \rangle \) is given by the TTS \( \langle S, S_0, \rightarrow \rangle \) where \( S = \{s \in \text{val}(W) | \forall i s \models \text{Inv}_i(loc_i) \} \) is a set of valuations, each one satisfies the local invariants of the involved locations \( loc \), of the corresponding active processes. \( S_0 = \bigcup_i \{V_i^0 \cup \{C_i \mapsto \{0\}\} \} \cup \{Id_0.loc \mapsto q_0^0\} \). \( W = \bigcup_i \{Id_i.C\} \cup \bigcup_i \{Id_i.V \cup \{loc\}\} \) is the set of discrete and continuous variables of the instances that can be created together with the newly introduced variables \( loc \). The transition relation is given by the rules of table IV.

The TTS states of the semantics are partial functions where only variables of created channels are valued. The condition \( \text{comit}(s, Id) = \forall Id' \in s \text{ comit}_l(s(Id'.loc)) \Rightarrow \text{comit}_l(s(Id.loc)) \) states that if \( s \) contains a committed location, the current location of process \( Id \) should also be committed [3]. Rule **Action** of table IV states that if there exists a process \( Id \) such that its current location \( Id.loc \) corresponds to the current reached location \( q \), and the current system state \( s \) satisfies the guard \( q \) of the PSA outgoing edge from \( q \) so the system moves to another state obtained by applying action \( a \) on state \( s \) where the current location of process \( Id \) is updated to \( q' \). Rule **Sync** describes a synchronization of 2 edges having compatible labels when the source locations match with the current system state \( s \), and both guards are satisfied. The resulting transition is labeled with internal event \( r \), where the receiver action \( a_j \) is applied after taking into account the update made by the sender action \( a_i \). Rule **Create** expresses the on-the-fly creation of processes. Such a feature is newly implemented in UPPAAL via statement \( \text{spawn} \). \([T]_s \) defines an instance of template \( T \) where the template parameters are evaluated according to state \( s \). The rule associates to the newly created process a fresh identifier \( Id' := \text{fresh}(s) \) thanks to the function \( \text{Ident} \). The new instance will be immediately initialized through function \( f\text{Init} \) given by:

\[
\text{fInit}(Id', T) = \{Id'.loc \mapsto T_0, \|c \in T.V \{Id'.v \mapsto T.V_0(v)\}, \|c \in T.C \{Id'.c \mapsto 0\}\}
\]

Such a function consists of initializing variables and initial location according to the instantiated template declaration, whereas clocks are initialized to 0. Over the syntactic function \( \text{exit} \) of rule **Destroy**, stating that the process execution is done, UPPIAL removes such a process from the system.

Rule **Delay** states that a delay \( d \) is allowed if the invariants of the current locations \( s(Id.loc) \) of all processes \( Id \in s \) are still satisfied, and no one of the current locations is committed. The time progress function \( s \triangleq d \) updates the stopwatch clocks at state \( s \) by \( d \). In fact, \( d \) is the real amount of time units elapsed whereas the update of each clock depends on its rate, defined by function \( \text{Act} \). Formally, \( s \triangleq d = \forall Id \in s, \forall c \in Id.C \ c := s(Id.c) + \text{Act}(Id.loc)(c) \times d \).

### B. Graphical Notations of PACoR

The translation of PACoR to timed automata is carried out in two steps: translation of a PACoR system to a graphical PACoR (gpACoR) model, and then translation of the gpACoR model into the corresponding timed automata model.

<table>
<thead>
<tr>
<th>Rule</th>
<th>PACoR</th>
<th>gPACoR</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>( p \triangleq p' )</td>
<td>( p ) [ p' ]</td>
</tr>
<tr>
<td>2</td>
<td>( p \triangleq A[l,u] : p' )</td>
<td>( p ) [ \frac{A}{z} \leq \frac{l}{z} \leq \frac{u}{z} ] [ p' ]</td>
</tr>
<tr>
<td>3</td>
<td>( p \triangleq \varepsilon ) [ p' ]</td>
<td>( p ) [ \varepsilon ] [ p' ]</td>
</tr>
<tr>
<td>4</td>
<td>( p \triangleq p_1 \parallel p_2 )</td>
<td>( p ) [ p_1 ] [ p_2 ]</td>
</tr>
<tr>
<td>5</td>
<td>( p \triangleq p_1 \parallel p_2 )</td>
<td>( p ) [ p_1 ] [ p_2 ]</td>
</tr>
<tr>
<td>6</td>
<td>( p \triangleq A[l,u] \Delta(n, p_r, p_s) : p' )</td>
<td>( p ) [ \frac{A}{z} \leq \frac{l}{z} \leq \frac{u}{z} ] [ s_{n} \leq z \leq s_{s} ] [ p_r ] [ p_s ] [ p' ]</td>
</tr>
<tr>
<td>7</td>
<td>( p \triangleq \varepsilon \nabla(n, p_r, p_s) : p' )</td>
<td>( p ) [ \varepsilon \leq \frac{n}{z} ] [ p_r ] [ p_s ]</td>
</tr>
<tr>
<td>8</td>
<td>( p \triangleq A[l,u] : p' )</td>
<td>( p ) [ \frac{A}{z} \leq \frac{l}{z} \leq \frac{u}{z} ] [ p' ]</td>
</tr>
</tbody>
</table>

Table V shows PACoR syntax and the corresponding notations in gpACoR. As shown in Rule 1, a process is represented by a box with a name and a transition arrow to the definition of the process. Timed actions are depicted as a circle, called timed action node, with resource requirements \( A \), as shown in Rule 2. For timed action statements, a clock \( x \) is introduced to specify timing requirements. Using this clock, the upper bound of the execution time is represented by an invariant.
associated to the node (oval state in Rule 2) representing the timed action, and the lower bound is a guard on the outgoing transition from that node. Event actions are represented by edges from the box \( P \), as shown in Rule 3. Rule 4 and 5 show that gPACoR processes can be composed using Choice and Parallel operators. The Choice operator is represented by a choice connector \( \oplus \) and arrows leading to possible processes, whereas the parallel composition is represented by a dashed box. The scoped timed action node, with resource requirements \( A \), is shown in Rule 6. It has 3 outgoing transitions leading to a normal process \( (P_1) \), a time-out handler \( (P_2) \), and an exception handler \( (P_e) \), respectively. A new clock \( y \) is introduced for the scoped timed action to measure the time elapsed (for deadline) since the scoped action is reached. Rule 7 shows the scoped event action node. It is almost the same as the scope timed action node. The event action node triggers an event \( E \) on the normal termination outgoing transition, and does not contain any resource-consuming requirements. Rule 8 shows a timed action node which is applied with the Close operator.

![gPACoR model of Example 3.1](image)

Fig. 2. gPACoR model of Example 3.1

Fig. 2 shows the gPACoR model of task \( T_1 \) and its dispatcher \( D_1 \) of Example 3.1. Based on a gPACoR model, a model of PSA can be built using the realizations of the priority relations.

C. Translation of Process Models

The PSA model of a PACoR specification is graphically similar to the gPACoR description, and simply obtained by making PSA stopwatch clocks run depending on the availability of resources that the process timed actions would use. Timed actions of gPACoR including resources and timing requirements are represented in locations of PSA using stopwatch clock variables. Event actions are executed on transitions of PSA. The stopwatch clocks associated with resources can run and stop according to the availability of resources. For the convenience, we use \( R \) for a set of resources, \( A_1, A_2, \ldots \) for resource requirements, and \( A_1, A_2, \ldots \) for timed action nodes. For resource operations, we define the following functions:

- \( S(A) \) is a resource requirement that a timed action node \( A \) requires,
- \( \rho(A) \subseteq R \) is the set of resources that a timed action node \( A \) requires.
- \( \text{Request}(A) \) is a resource request according to the resource requirement \( A \),
- \( \text{Release}(2^R) \) is a function that releases a set of resources \( (2^R) \),
- \( \text{Available}(2^R) \) is a function stating whether a set of resources \( (2^R) \) is available,
- \( \text{LockPreemp}(pid) \) sets a process \( pid \) to non preemptive process.

Table VI shows how each basic structure (transition) of gPACoR is implemented in PSA. The boxes in gPACoR represent process names and correspond to the circles in PSA. Such circles are the starting locations of the PSA model. The hexagons in both sides represent definition of actions. For a given \( P_{gPACoR} \), every PSA automaton, as shown Table VI, is given with a starting location \( P_{PSA} \). In later, all starting locations will be interpreted by the commit connector of UPPAAL because the outgoing transitions linked to the starting location of PSA should always be urgently taken. For gPACoR actions, the corresponding actions in PSA are defined according to translation rules given in this section. In fact, we only focus on the translation and implementation of gPACoR transition relation.

Rule 2-1 and 2-2 show how to translate a timed action node of gPACoR to a PSA automaton. Every single timed action node of gPACoR and its clocks is transformed to a PSA with a set of clocks. In principle, a PSA process requires a set of resources using the function \( \text{Request}(A) \) according to a resource requirement \( A \) before entering the timed action location. The PSA process should release resources, using the function \( \text{Release}(2^R) \), when it exits from the timed action location. Inside a timed action node, the stopwatch \( x \) runs depending on the resource availability which is checked using \( \text{Available}(2^R) \). If a process wants an exclusive (non-preemptive) use of resources, it sets itself to “non-preemptive” using \( \text{LockPreemp}(pid) \).
Rule 3 shows how gPACOR events are translated to a set of transitions into the corresponding PSA model. As shown in Rule 4, the Choice operator \( \oplus \) is replaced by the commit connector \( \odot \) of UPPAAL. The Choice operator has alternatives of possible actions. In case of timed actions, the availability of resources should be known before the selection of an outgoing transition. Thus, as shown in Rule 4-1, all resources that the alternative timed actions require are requested, e.g. \( \text{Request}(S(A_1)) \), before making a choice and checked to be usable (transitions are enabled) when making the choice, e.g. \( \text{Available}(\rho(A_1)) \). The Parallel operator is realized by instantiating parallel composed processes, as shown in Rule 5. In our translation, the processes instantiation can be static or on-the-fly. The static creation is implemented by a special event, \( \text{Spawn}[\text{pid}]! \), whereas the dynamic instantiation is supported by the UPPAAL statement \( \text{Spawn} \) together with a template name. Rule 6 shows the translation of a scoped timed action of gPACOR. According to whether the action is preemptive (\( \{S\} \)) or not (\( \langle S \rangle \)), the entering transition into the timed action location executes the function \( \text{LockPreemp}(\text{pid}) \). Notice that the resource requirement \( S(A_e) \) of the exception handler \( P_e \) is required on the transition going to the timed action node,
because the exception handler can have the same possibility to execute as the scoped timed action if it is enabled. Thus the resources requests for \( P_e \) are performed before the execution of the scoped timed actions. Similarly, in case that \( P_e \) is a composition of processes using the Choice operator, all alternative transitions are directly linked to the timed action location in order to make them possibly enabled when the timed action executes.

Rule 7-1 and 7-2 show the translation of the scoped event action. In Rule 7-1, the resources request of the exception handler \( P_e \) is performed in the same way as in the scoped timed action. Rule 7-2 describes the case where the exception handler \( P_e \) carries out an event action \( \varepsilon_e \). Rule 8 shows how to apply the Close operator to PSA. According to the semantics of PACoR, if a process extended with the Close operator, it adds a special resource requirement \((r, lp(A))\) to its resource requirements for the execution of its timed actions. Rule 9 and 10 show how to realize \( \textit{NIL} \) and \( \textit{DONE} \) actions. The \( \textit{NIL} \) action is interpreted by a deadline. For the \( \textit{DONE} \) action, the final location can be one of two types: 1) Rule 10-1 shows the execution of \textit{DONE} action, using the statement \textit{exit()} of UPPAAL, in the case of dynamic process creation; 2) Rule 10-2 shows a final location for the static process creation, which has an outgoing transition labeled with the process instantiation event \( \text{Spawn}[\text{pid}] \).

**D. Composition and Instantiation of Process Models**

Individual PSA automata are composed into a networked PSA system in the following way. First, every starting location for individual PSAs is replaced by a commit connector. Second, every edge leading to a final location is redirected to the starting location of the same name. PSA templates are instantiated either by static or dynamic process creation. If dynamic process creation is used, every PSA template has an initial location as shown in Fig. 3(a). Initially, only the top level process is instantiated, and other processes are instantly created when needed. If using static process creation, all processes are created at the same time and every PSA template has an initial location as shown in Fig. 3(b), except for the top level process which follows Fig. 3(a). The actual execution of a process, in case of static instantiation, begins by the instantiation event \( \text{Spawn}[\text{pid}] \) according to the Rule 5-1. Rule 8 shows how to apply the Close operator to PSA. According to the semantics of PACoR, if a process extended with the Close operator, it adds a special resource requirement \((r, lp(A))\) to its resource requirements for the execution of its timed actions. Rule 9 and 10 show how to realize \( \textit{NIL} \) and \( \textit{DONE} \) actions. The \( \textit{NIL} \) action is interpreted by a deadline. For the \( \textit{DONE} \) action, the final location can be one of two types: 1) Rule 10-1 shows the execution of \textit{DONE} action, using the statement \textit{exit()} of UPPAAL, in the case of dynamic process creation; 2) Rule 10-2 shows a final location for the static process creation, which has an outgoing transition labeled with the process instantiation event \( \text{Spawn}[\text{pid}] \).

**Theorem 4.1:** The TTS semantics restricted to \( \tau \) and time-transitions of a PACoR system is bisimilar to the TTS associated to the PACoR translation into a network of PSA.  

**Proof concept.** The proof is direct and consists in checking that each TTS transition, except event transitions restricted by restriction, generated by one of the rules given in Definition. 3.5 can also be generated using the rules given in Definition. 4.2 after applying the translation of PACoR transitions according to tables VI and VII, and vice versa. A sketch of this proof is given in the Appendix.

**V. EXAMPLE: PLATFORM CONTROL SYSTEM**

In order to illustrate our framework, we present an example of a train platform system in Fig. 5. In this system, the trains enter from five incoming tracks and stop in one of two segments \((\text{seg}_1, \text{seg}_2)\) on each side of the platform. Individual tracks have priorities for a train to occupy the segments, and the priorities increase every specified time interval \((\text{wt})\) unless the train can enter the platform. The train can stay at the platform for \( st \) time units. Each track has the minimum inter-arrival time \((\text{mt})\) to serve a train. Variable \( j \) and \( i \) are used to index segment number and train identity, respectively. In the second line of Table VIII we use a timed action with an infinite execution time but with a deadline of \( \text{wt} \). If a segment becomes available the train can occupy that segment, otherwise the train becomes a new \( \text{TrnReqP} \) process waiting for a segment, but with a priority increased by \( k \). In the experiment shown in Table IX, we have 5 tracks and 2 or 3 segments. Over this example, we show 1) how to specify the system using PACoR, 2) how to translate the PACoR model into PSA, and 3) how to apply UPPAAL and UPPAAL SMC to reason about various characteristics of the system. Table VIII describes the platform system using PACoR. The PSA model which is translated from the same PACoR model is given in the Appendix.

**A. Analysis using UPPAAL and UPPAAL SMC**

The analysis of the train platform system has been done using two verification methods, symbolic and statistical model checking. We use UPPAAL to check with symbolic model checking that there is no deadlock in the system. With UPPAAL SMC we generate the probability distribution for the waiting time of each train.
from PACoR to PSA which preserves the semantics. The translation is not implemented yet, but it is designed to utilize new features of UPAPAAL, such as on-the-fly process creation. Finally we have provided an example illustrating the complete process from systems specification in PACoR, translation to gPACoR, further translation to PSA and verification of system properties using UPAPAAL and UPAPAAL SMC.

### References


APPENDIX A

REALIZATION OF RESOURCE OPERATIONS IN UPPAAL

In order to realize the priority relation in UPPAAL, we implemented the prioritizing functions and resource availability functions using the user-defined functions of UPPAAL.

Listing 1. Data structures for PACOR process and resource

typedef struct 
{ 
    pid_t pid;
    ppri_t pri;
    bool preemptive;
} proc_t;

typedef struct 
{ 
    pid_t rid;
    len_t len;
    pid_t elem[pid_t];
} rq_t;

Listing 2. Prioritizing functions

void insert_at(rq_t *rq, pid_t pid, place_t place, pid_t pid) { 
    pid_t i = rq->len;
    for(i = rq->len; i > place; i--){
        rq->elem[i] = rq->elem[i-1];
    }
    rq->elem[place] = pid;
    rq->len++;
}

void request(rq_t *rq, pid_t pid, ppri_t pri) { 
    pid_t place = 0;
    test[pid] = pri;
    proc[pid] = pri;
    if ( (rq->len > 0) && ((proc[rq->rid].len > 0) && (proc[rq->rid].elem[0].elem[pid].prior < proc[pid].pri) ) )
        place++;
    insert_at(rq, place, pid);
}

void release(rq_t *rq, pid_t pid) { 
    pid_t i = 0;
    while( i < rq->len && rq->elem[i].prior < pid )
        i++;
    while( i < rq->len - 1 )
        rq->elem[i] = rq->elem[i+1];
    rq->len--;
    return;
}

The function request() calculates the order of a process in the present resource queue status according to its priority. The function insert_at() inserts a new process into the queue. The function release() deletes a process from a resource queue. It searches and removes a given process id in resource queue, deletes it, and re-orders all the elements of processes.

Listing 3. Resource availability function

int [0..1] isSched(rq_t *rq, pid_t pid) { 
    return (rq->elem[0].elem[0].prior < pid) ? 1:0;
}

int [0..1] isNotSched(rq_t *rq, pid_t pid) { 
    return (rq->elem[0].elem[0].prior == pid) ? 1:0;
}

The functions isSched(pid,pri) and isNotSched(pid,pri) are used to check if a resource represented by a resource queue (rid) is available to a process pid. The function isSched() returns 1 when pid is the first element in the resource queue of rid, and otherwise, it returns 0. The function isNotSched() is opposite to isSched(), returning 1 if the process is not scheduled.

APPENDIX B

PSA MODEL FOR TRAIN PLATFORM SYSTEMS

Fig. 7 shows the gPACOR and the corresponding PSA model of the train platform systems translated from the PACOR model given in Section . As shown Fig. 7, the PSA model has almost same structure as the gPACOR model, except for NIL process and the Choice connector. The NIL process has the incoming transition which is never taken because the clock x cannot ever hold. The Choice connector is removed since all alternative transitions have the same possibility to be taken as the timed action execution, thus they directly linked to the time action location. All the same name of gPACOR can be found in the PSA model. The clock variable waitTime[pid] is added to the PSA model after the translation in order to analyze the waiting time of a train before entering a platform. The urgent event dummy is also added in order for transitions depending on conditions to be taken urgently.

APPENDIX C

PROOF OF THEOREM 4.1

The proof consists in showing that each TTS semantics (direct, translation-based) of PACOR simulates the other. Because of space limitation, we only focus on one simulation, from direct semantics to the translation-based one, of the transition relations where we provide the minimum elements making our theorem clearly satisfied. In fact, the proof relies on the fact that:

- The semantics of each PACOR event is represented by either an event transition (rule E-success) or a delay (rule Delay) followed by the event transition if the PACOR event is not urgent. Similarly, in the translation from PACOR to PSA, each event corresponds to an edge performing such an event (Rule 3) where the PSA template may have a wait if the event is not urgent. Such a waiting time corresponds to a delay transition (rule Delay), in the TTS semantics of PSA, depending on the PSA location invariant that depends in turn to the urgentness of the PACOR event. In both cases, the target states of the
event-transitions match each other in terms of simulation relation.

A PACoR timed action semantics corresponds to a TTS transition performing such an action (rule A-success) when resources are available. Such a PACoR transition corresponds to a sequence of 2 PSA edges $t_1$ and $t_2$ (Rule 2-1, 2-2, 6-1, 6-2, 6-3). The first edge $t_1$ requests resources whereas the second edge $t_2$ performs such an action and release resources. In fact, the use of resources is implemented by a stay at the source location of $t_2$. One can remark that the TTS state corresponding to the source location of $t_2$ matches perfectly with the (direct semantics) TTS states of the event transition in terms of the simulation relation. Such an extra internal transition, corresponding to the PSA edge $t_1$ for resource request, can be ignored according to the weak bisimulation relation we considered. Moreover, the target state of the action transition (direct semantics) matches with the target state of the semantics of edge $t_2$. Thus, our simulation relation is satisfied in the case of timed action transitions.

The proof of the simulation relation from translation-based semantics and direct semantics is similar to the proof sketch given above.