Markov Chain Modelling of Probabilistic Real-Time Systems

Jasdeep Singh, Luca Santinelli, Guillaume Infantes, David Doose, Julien Brunel

ONERA
THE FRENCH AEROSPACE LAB

retour sur innovation

Real-Time System and Safety

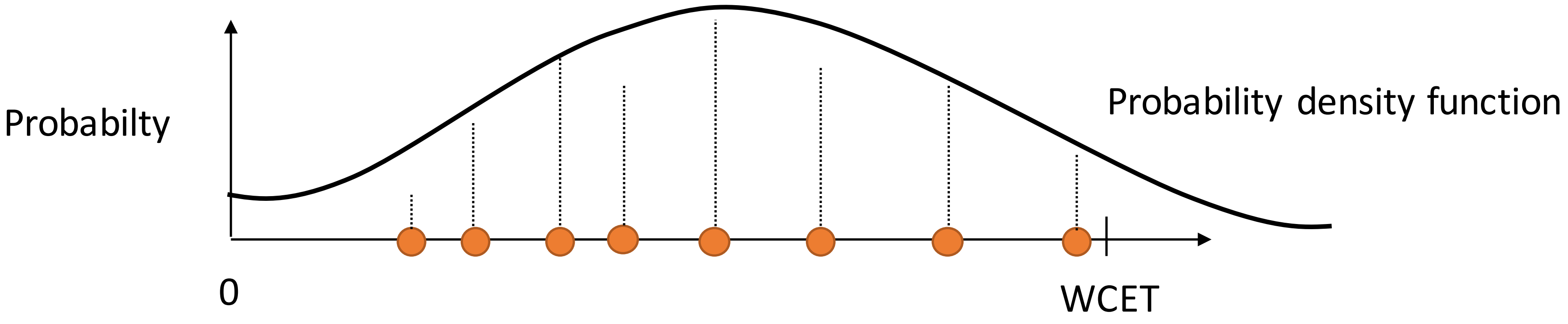
- Safety: ensure the correct working of R/T system; functional and non-functional aspects verified
- Modelling perspective: Ensure Task Deadlines are met
- R/T analysis required to verify this, in turn to ensure safety

Why Probabilities

- Task execution time: WCET, worst case
- Not all instances are worst case
- Over pessimistic analysis
- Each execution time (0,WCET] has a probability of occurrence
- Representation of many possible execution times by a random variable
- Probability can quantify the pessimism

Probabilistic Real-Time System (pRTS)

- R/T system with at least one probabilistic parameter
- WCET replaced by probabilistic WCET (pWCET)
- Each task has pWCET which is an upper bound probabilistic distribution of all possible execution times
- pWCET gives the probability that an execution $\in (0, WCET]$ occurs



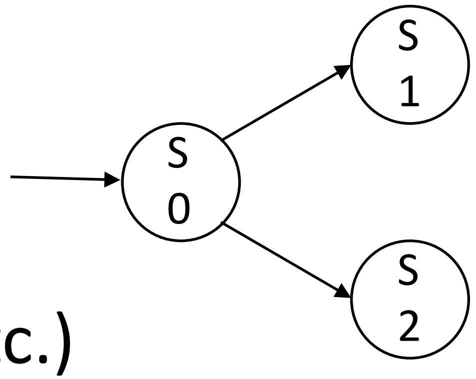
Objective

- To perform probabilistic Schedulability analysis of pRTS
- Task set is given with one or more probabilistic parameters (pWCET, Deadline, Period)
- Model stochastic occurrences and interactions (execution, delays, preemptions, etc.)
- Provide probabilistic guarantees
- Probabilistically answer the question of safety

[Diaz et el. 2002, Carnevali et al 2014, Maxim et al 2013, Manolache et al 2004]

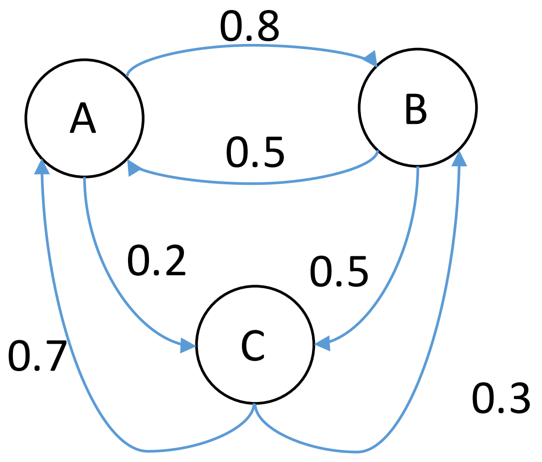
Formal methods for pRTS

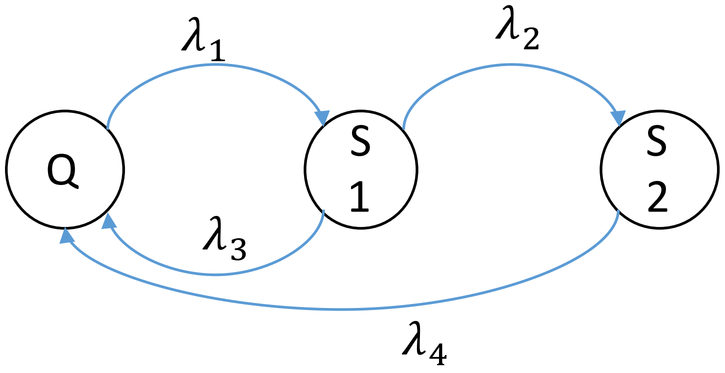
- Formal methods: mathematically proven techniques for specification and verification of a system
- Reliable: safe and accurate because of mathematical proofs available
- Model checking can be readily performed
- Model non-determinism and probability
- Handling continuous distribution (exponential, erlang, etc.)
- Feasible complexity



A model approach

- Markov Chain (MC): set of states and transitions, memoryless property
- Continuous Time MC: transitions labelled with rates, duration of transition is exponentially distributed (choice and probability)
- Other stochastic formal methods
  - Stochastic Petri Net: Problem too complex
  - Stochastic Timed Automata: inability to model probabilistic duration of execution

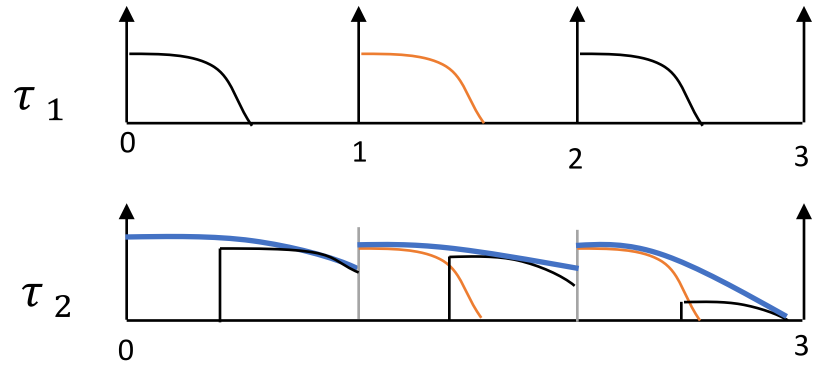


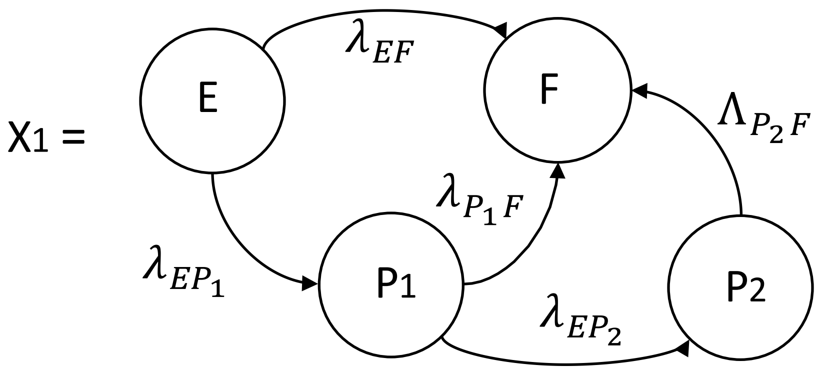


Current Status

- Task set at input, tasks can be probabilistic and/or deterministic; execution time, period and deadline
- Probabilistic task have pWCET for execution time
- Scheduling policy assigns each job a priority (EDF, FP)
- Number of preemptions are known, since dealing with distributions with base $(0, \infty)$

For τ_2:





Pr (time = 3; state = P2) = **Pr(DM)**

- Execution times and delays encoded in transition rates
- Deadlines checked as property

Limitations

- CTMC transitions are exponentially distributed
- Rigid time constraints like killing of job at deadline is not possible yet
- Convolutions are too heavy
- Hyperperiod delays not accounted for

Open Problems and Future Work

- Current methods is in the process of publishing
- Next steps: Imposing rigid timing constraints
- Avoid convolution by different interpretation of the requirement
- Integration with random variables as limits
- Hybrid stochastic model (Automata+ CTMC; CTMC+DTMC, CTMC+CTMC): to impose hard timing constraints (preemption, killing job, etc.)

Thank you
Questions