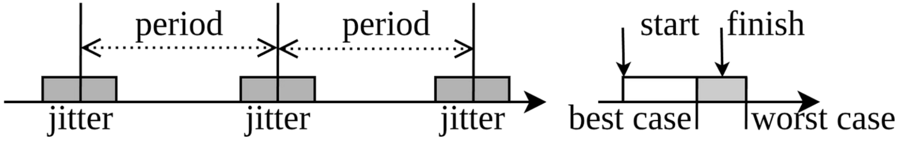
Deductive State-Space Construction and Verification of Discrete-Time Stochastic Timed Automata (WiP)

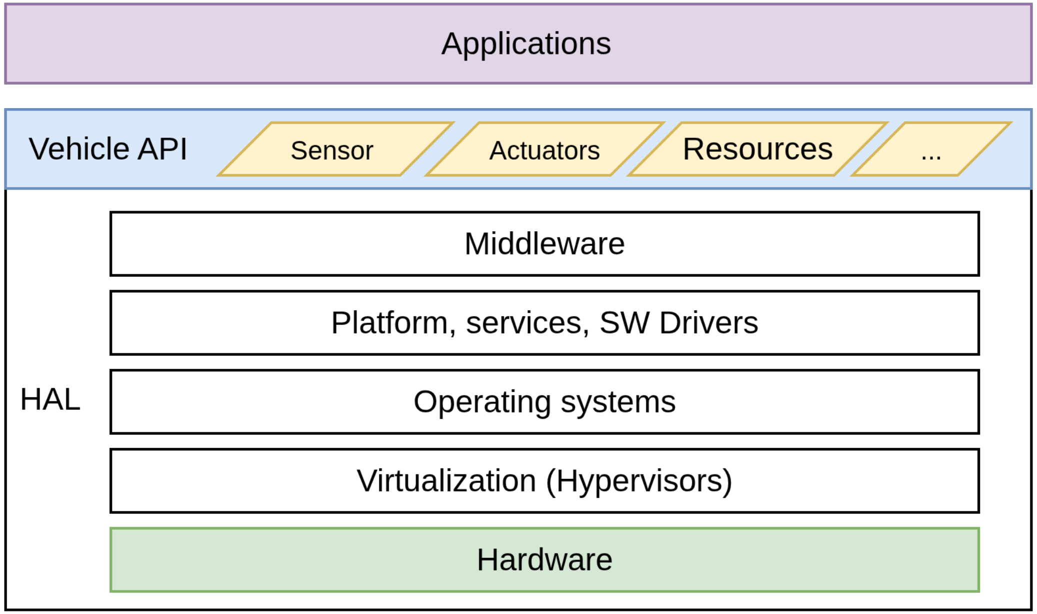
Irman Faqrizal

32th International Open Workshop on Synchronous Programming,
Centre CNRS Paul Langevin, Aussois,
November 24-28 2025

Systems with timing uncertainties

- Real-time systems often posses **timing uncertainties**
  - E.g., applications on **hardware abstraction layer** of a **software defined vehicles**




Applications

Vehicle API
Sensor
Actuators
Resources
...

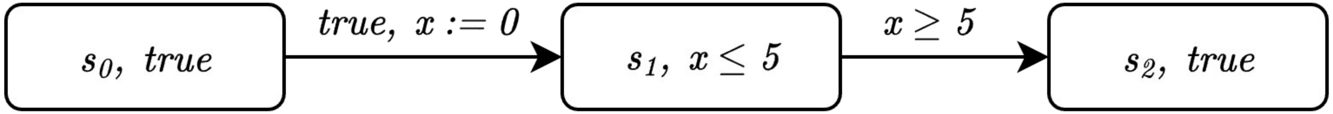
HAL
Middleware
Platform, services, SW Drivers
Operating systems
Virtualization (Hypervisors)
Hardware

- Sensors and actuators have **jitters** on their periodic activations
- Software components (e.g., controller) execute for some specified **time bounds**
- The timing uncertainties are characterized by **probabilistic distribution**

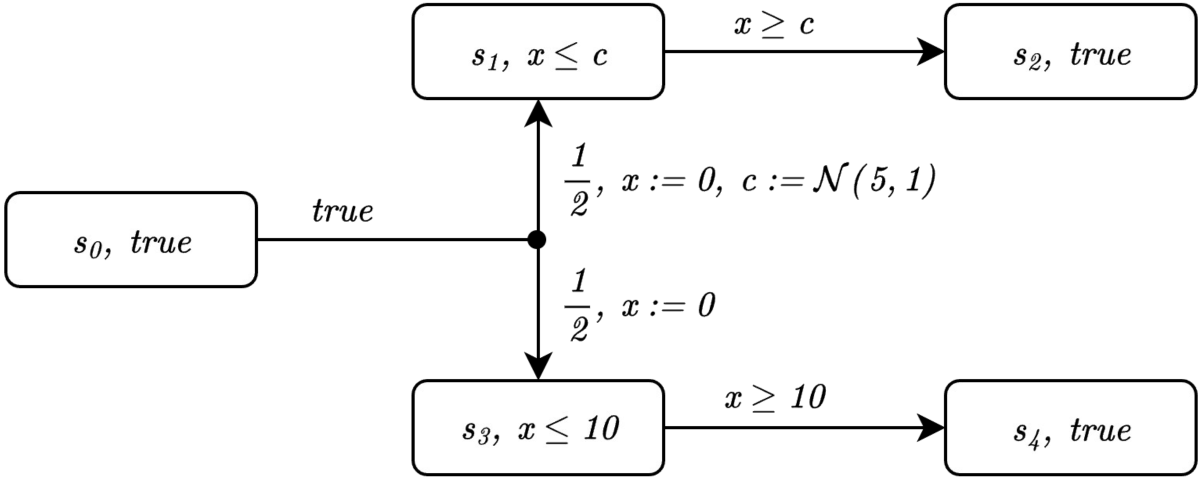
Stochastic timed automata

- Stochastic Timed Automata (STA) are Timed Automata (TA) extended with (i) **probabilities** on the **transitions** and (ii) **probabilistic distribution** on the **delay** of the transition

Timed automata



Stochastic timed automata



STA modeling and verification methods

- MCSTA in the Modest toolset [1]
  - **Explicit-state** model checker
  - Translation from STA to Probabilistic Timed Automata (PTA)
- UPPAAL SMC [2]
  - Analysis using **statistical** model checking
- Almost-sure model checking [3]

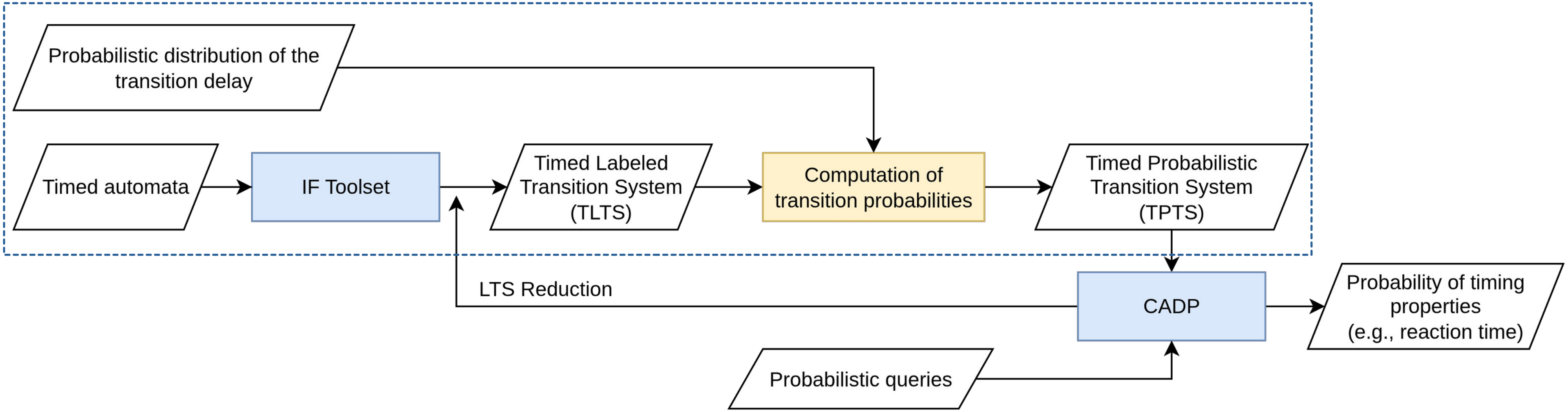
[1] Hahn, E. M., Hartmanns, A., & Hermanns, H. (2014). Reachability and Reward Checking for Stochastic Timed Automata. ECEASST, 70.

[2] David, A., Larsen, K.G., Legay, A., Mikučionis, M., Wang, Z. (2011). Time for Statistical Model Checking of Real-Time Systems. CAV 2011.

[3] N. Bertrand, P. Bouyer, T. Brihaye, Q. Menet, C. Baier, M. Größer, and M. Jurdzinski (2014). Stochastic timed automata. Logical Methods in Computer Science, 10(4).

State-space construction and verification of discrete-time STA

- We consider **discrete-time STA** and (for now) include **only** the **stochastic** part


Probabilistic distribution of the transition delay
Timed automata
IF Toolset
Timed Labeled Transition System (TLTS)
Computation of transition probabilities
Timed Probabilistic Transition System (TPTS)
LTS Reduction
CADP
Probability of timing properties (e.g., reaction time)
Probabilistic queries

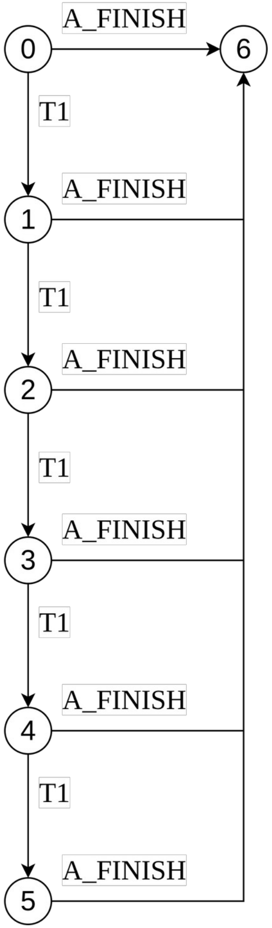
- The result can be used when comparing the analysis results of **simulation** and **execution** of the real system

From discrete-time STA to TPTS

```
process A(1);
  var x clock;
  state start #start;
    set x := 0;
    nextstate end;
  endstate;
  state end;
    deadline delayable;
    when x <= 5;   (uniform)
      informal "A_FINISH";
      reset x;
      stop;
  endstate;
endprocess;
```

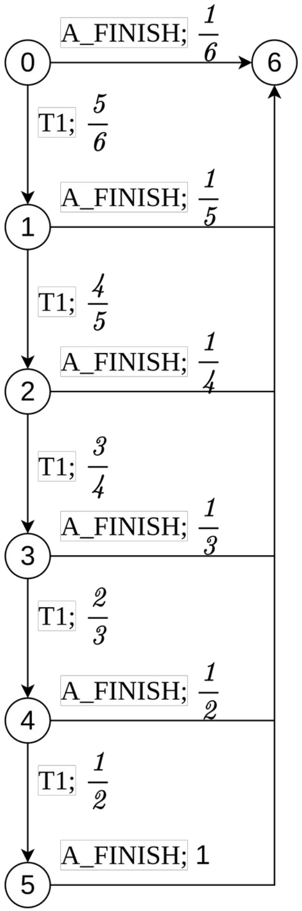
TA in IF

(IF) TA to LTS,
(CADP) reductor



TLTS

Compute probabilities
According to distribution

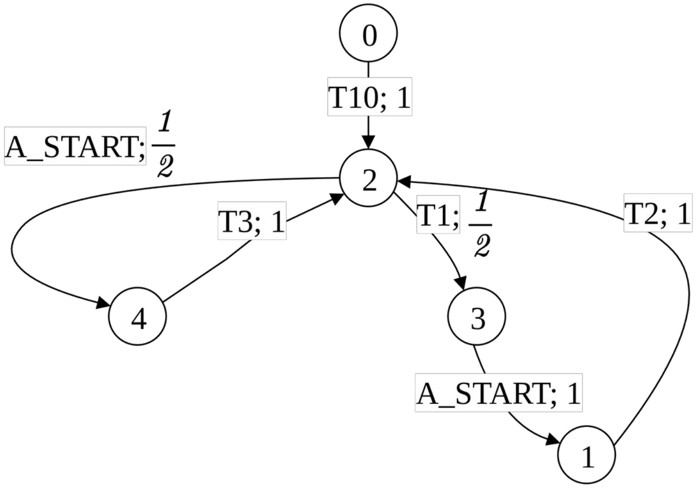


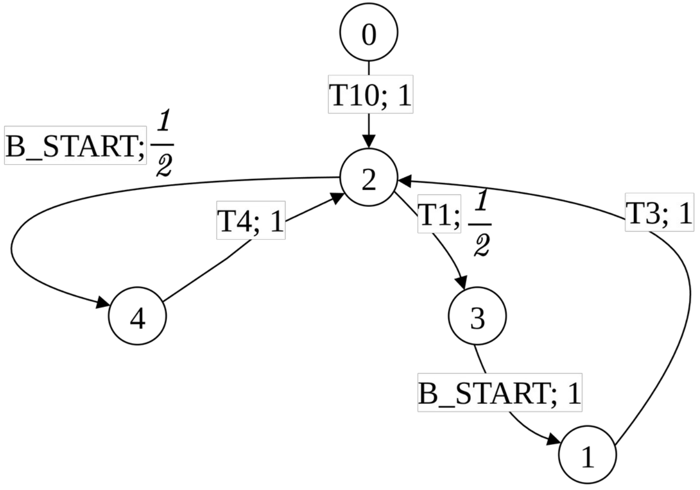
TPTS

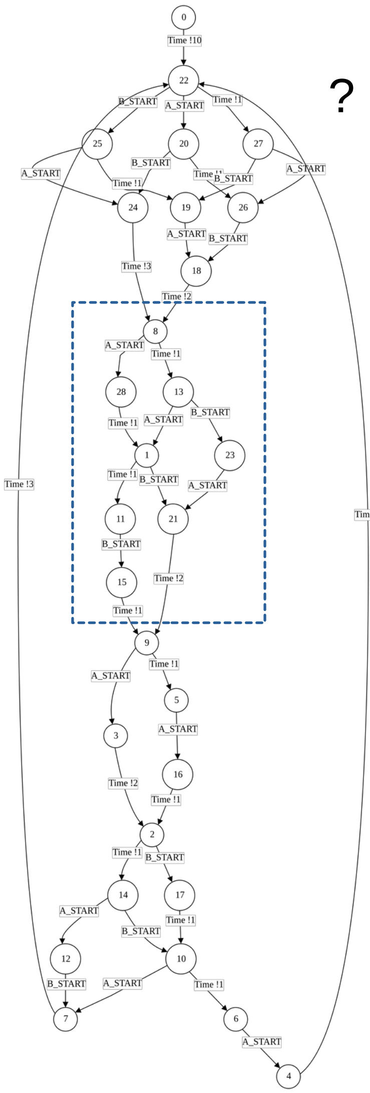
TPTS computation for network of STA

```
process A(1);
   var x clock;
   state start #start ;
      set x := 0;
      nextstate first;
   endstate;
   state first;
      when x = 10;
         set x:= 0;
         nextstate jitter;
   endstate;
   state jitter;
      deadline delayable;
      when x <= 1;
         informal "A_START";
         nextstate wait;
   endstate;
   state wait;
      when x = 3;
         set x:= 0;
         nextstate jitter;
   endstate;
endprocess;
```

```
process B(1);
   var x clock;
   state start #start ;
      set x := 0;
      nextstate first;
   endstate;
   state first;
      when x = 10;
         set x:= 0;
         nextstate jitter;
   endstate;
   state jitter;
      deadline delayable;
      when x <= 1;
         informal "B_START";
         nextstate wait;
   endstate;
   state wait;
      when x = 4;
         set x:= 0;
         nextstate jitter;
   endstate;
endprocess;
```

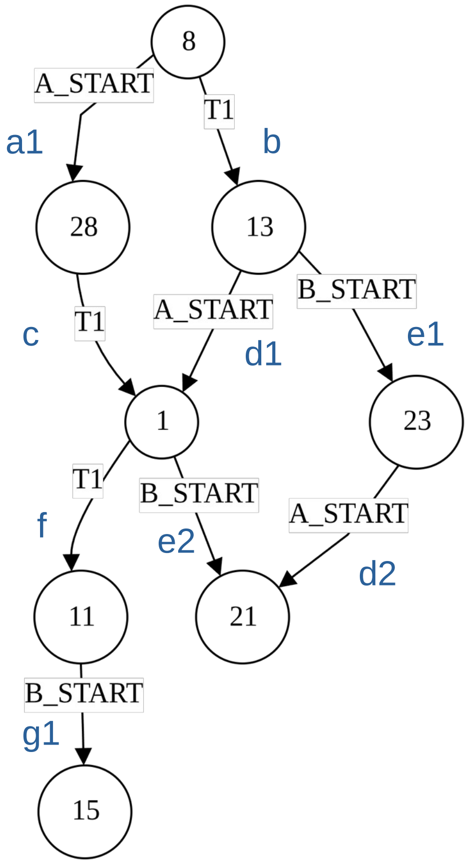


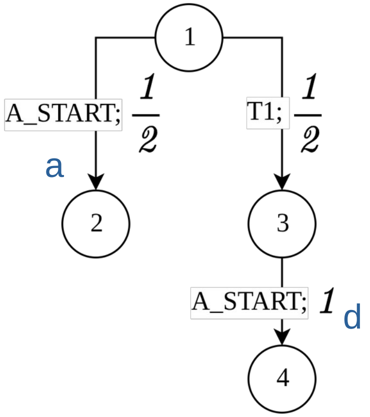


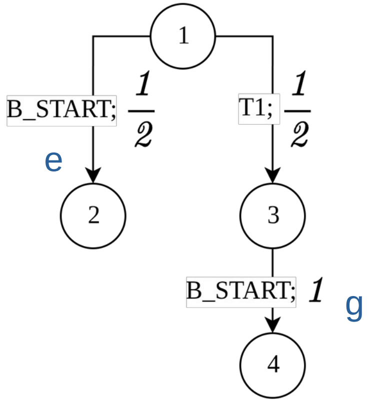


?

TPTS computation for network of STA







System of equations:

b (d1 + e1*d2) = ½

a1 = ½

b (e1 + d1*e2) + a1*c*e2 = ½

f*g1 (a1*c + b*d1) = ½

b*d1 = b*e1*d2

b*e1 = e2 (b*d1 + a1*c)

a1+b = 1

c = 1

d1 + e1 = 1

f + e2 = 1

d2 = 1

g1 = 1

Solution:

A1 = 1/2, b = 1/2, c = 1, d1 = 1/2,
e1 = 1/2, f = 2/3, e2 = 1/3, d2 = 1, g1 = 1

Concluding remarks

- An idea to analyze **timing uncertainties**
  - Express the system as a network of **discrete-time stochastic timed automata**
  - Compute a **probabilistic behavioural model (TPTS)** according to the **distributions** of the **transition delays**
- Possible next steps
  - Take into account
    - Transition probabilities
    - Varying probabilistic distributions
    - Multiple clocks
  - Investigate scalability