Evaluating regulation policies for subways with model checking

Benjamin Bordais[1], Thomas Mari[1], Julie Parreaux[1]
supervised by
Nathalie Bertrand[2], Loïc Hélouët[2], Ocan Sankur[2]

[1]ENS Rennes

[2]Inria Rennes, Team SUMO

May 29, 2018

Introduction

Every day, millions of people take the subway !

Challenges:

- Prove the safety of subway networks
- Ensure the efficiency of subways regarding delays with a **regulation policy**

glasgow-metro.jpg

Introduction: related work

Safety

Model checking is used to prove the security of critical sections[1](e.g. signaling system)

Efficiency

Simulation of the physic reality of subways from a very specific situation[2]

---

[1] Automated verification and validation of signaling systems in PTC and CBTC environements, Smith et al., 2012

[2] Railroad simulation using opentrack. A. Nash and D. Huerlimann, 2004

Introduction: our approach

Hypothesis

The safety of the subway networks we study is ensured.

- Model checking offers formal guarantees
- It can be used to evaluate efficiency of subways
- That is : evaluating regulation policies
- Use the model checker PRISM[3]

[3] PRISM 4.0: Verification of Probabilistic Real-time Systems, Kwiatkowska et al., 2011

Outline

Outline

Required features in the model

We need a formal model to represent subway networks.

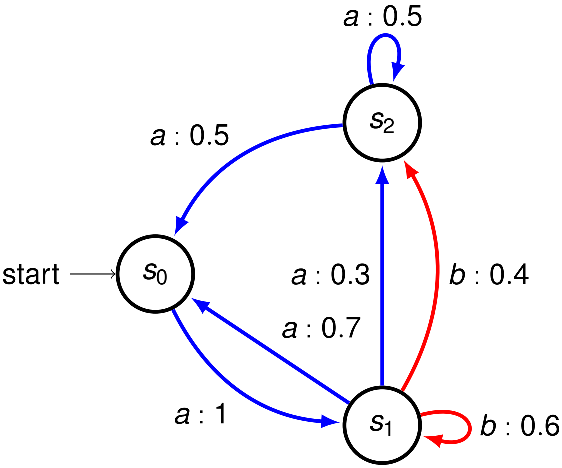
Need for randomness

Delays are unpredictable and conveniently represented through probabilities.

Need for nondeterminism

Regulation policies can increase or decrease the dwell time of subways in station. This can be seen as nondeterminism.

Model: Markov Decision Process (MDP)



An example of an MDP

Regulation policy

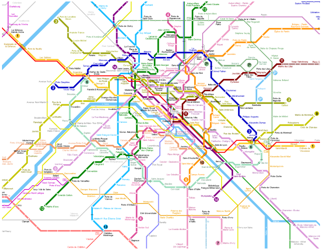
- Chooses the behavior of trains according to the state of the system
- Resolves the nondeterminism of the MDP

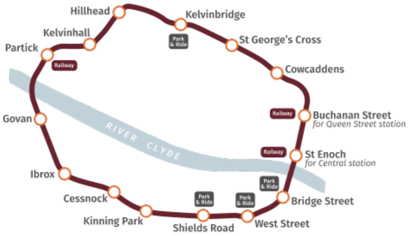
Our Goal

Design regulation policies and evaluate their efficiency at recovering from a delay

Glasgow: a simple topology

- Real systems are often too complex for formalization
- Simpler the system, simpler the model !
- First, we study a ring system

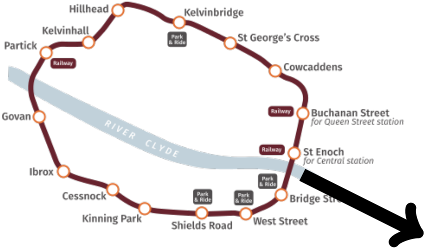




Outline

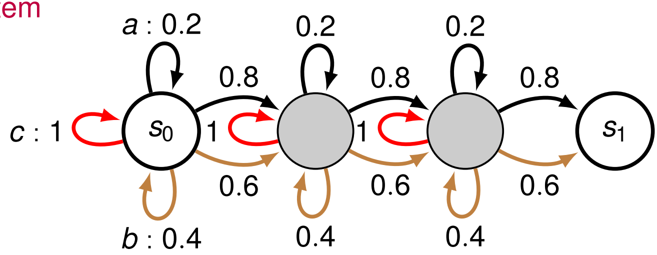
Space and Time Discretization

- Action a : usual speed
- Action b : lower speed
- Action c : dwell



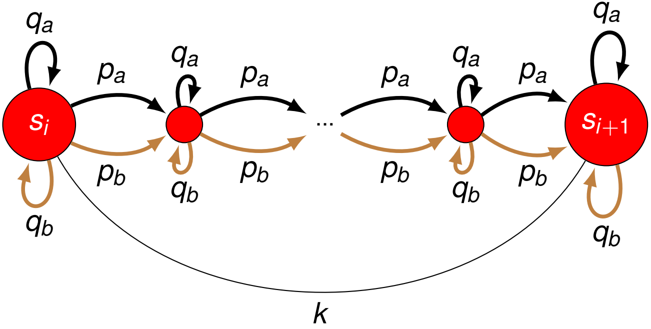
Continuous system

Discrete model

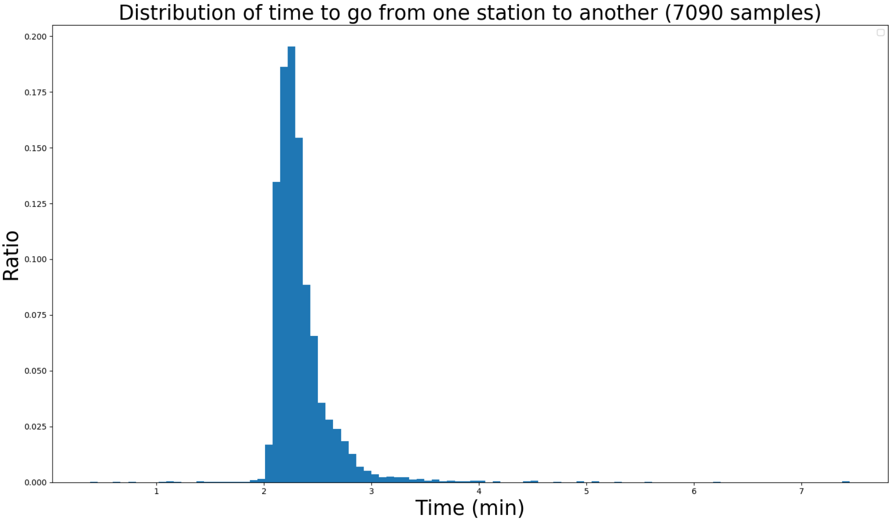


Parameters of interest

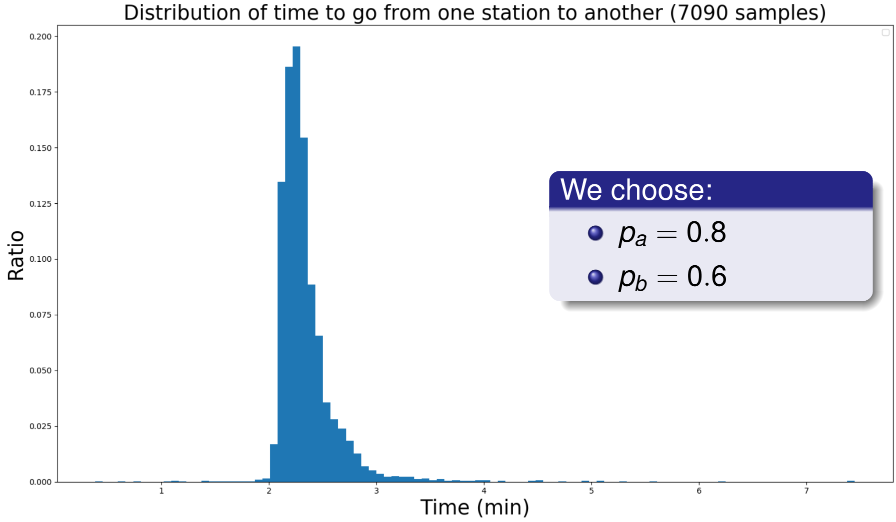
- Time discretization step: Δt
- Space discretization step: Δd
- Probabilities: p_a, p_b (also $q_a = 1 - p_a$ and $q_b = 1 - p_b$)
- Number of intermediate steps: k
- Number of trains: nb_{train}



Choosing the probabilities: data from Santiago



Choosing the probabilities: data from Santiago



We choose:

- $p_a = 0.8$
- $p_b = 0.6$

Choosing the parameters: from the Glasgow subway

Choosing nb_{train}:

- Peak time: $nb_{train} = 6$
- Off-peak time: $nb_{train} = 4$

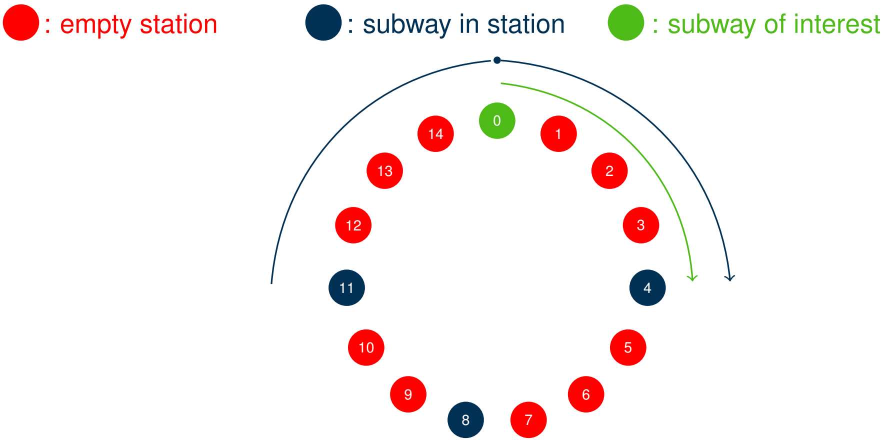
We have the following relation between k, Δt and p_a:

$$k \times \Delta t = p_a \times 66s$$

- $k = 5$
- $\Delta t \simeq 10s$
- $\Delta d = 140m$

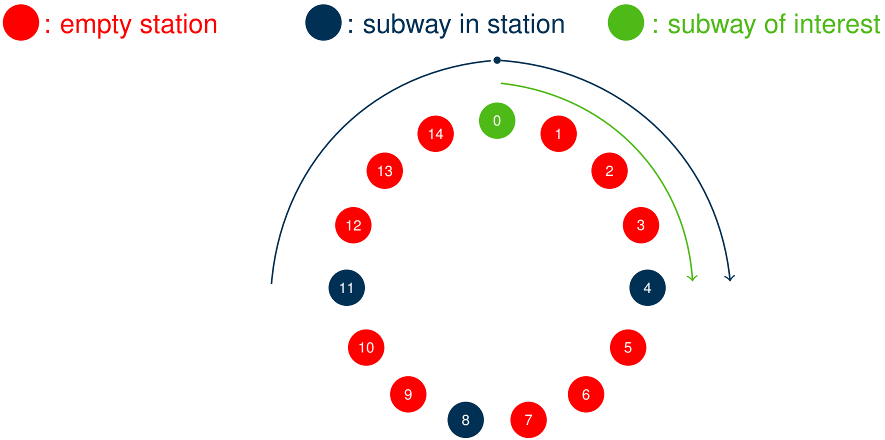
- $k = 10$
- $\Delta t \simeq 5s$
- $\Delta d = 70m$

How to estimate delay?



$$\alpha = \frac{d(current, next)}{d(previous, current) + d(current, next)} \in [0, 1]$$

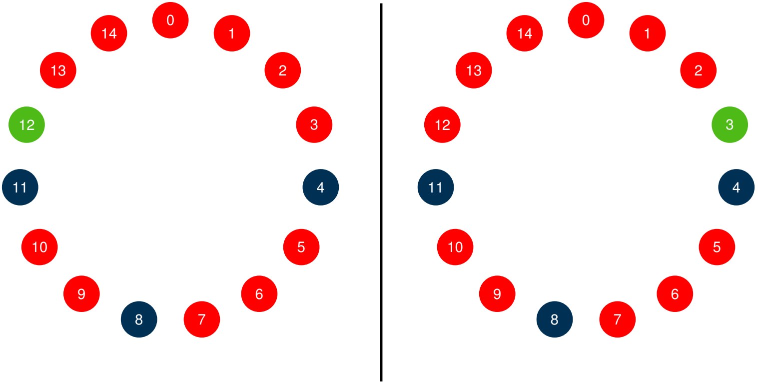
How to estimate delay?



Delay: $\alpha \notin [0.4, 0.6]$

Extreme cases

: empty station   : subway in station   : subway of interest

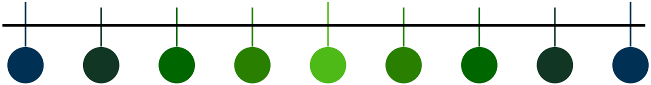


$\alpha \simeq 1$ $\alpha \simeq 0$

A simple regulation policy

Chooses the dwell time in station as a function of α:

					Nominal time					
$t_{station} =$	20	22.5	25	27.5	30	32.5	35	37.5	40	s
$\alpha =$	1.0	0.88	0.75	0.63	0.5	0.38	0.25	0.13	0.0	



Properties to be checked

Safety property

Two trains must not collide: $P_{max=0}(G \neg \text{"} collision \text{"})$

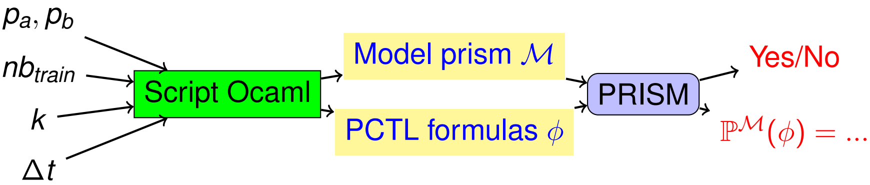
Efficiency of the regulation policy given an initial configuration

- Recovering time from an unbalanced configuration: $P_{min=?}(F_{\leq n} \neg \text{"} delay \text{"})$
- Avoiding delays from a balanced configuration: $P_{max=?}(F_{\leq n} \text{"} delay \text{"})$

Outline

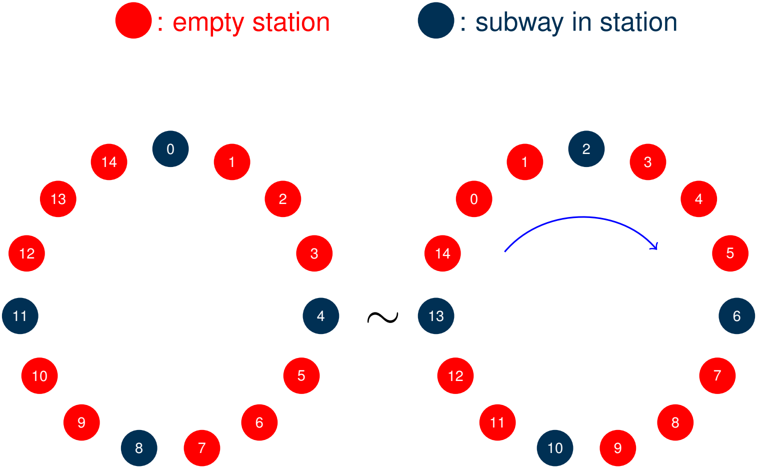
First attempt

- Automated generation of prism models and properties on which prism may work



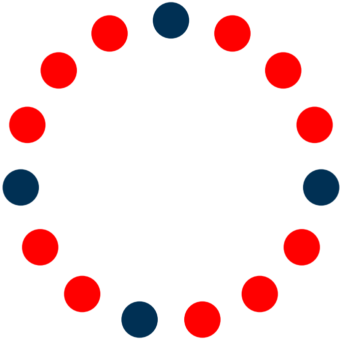
- Prism : unable to build the state space for $nb_{train} = 4, k = 5$ (smaller model of interest), the properties cannot be verified

Abstraction: reduce the size of the model

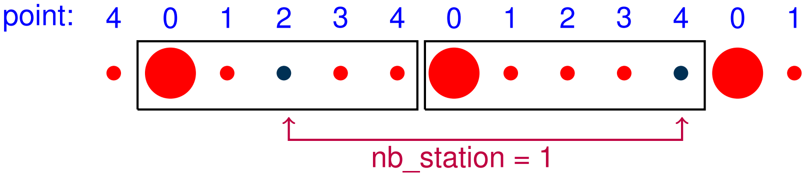


Abstraction: station ids are irrelevant

: empty station   : subway in station



Abstraction of our model: description



- point: distance between a train and its previous station
- nb_station: number of stations between a train and its successor

Abstraction of our model: some results

Model / Number of trains	Before abstraction	After abstraction
3 trains	2.1×10^8 states 3.4×10^9 transitions	3.5×10^5 states 8.3×10^5 transitions
4 trains	Not built in PRISM	2.0×10^7 states 5.7×10^7 transitions

Table: Size of the model in terms of number of states and transitions

Soundness of the model

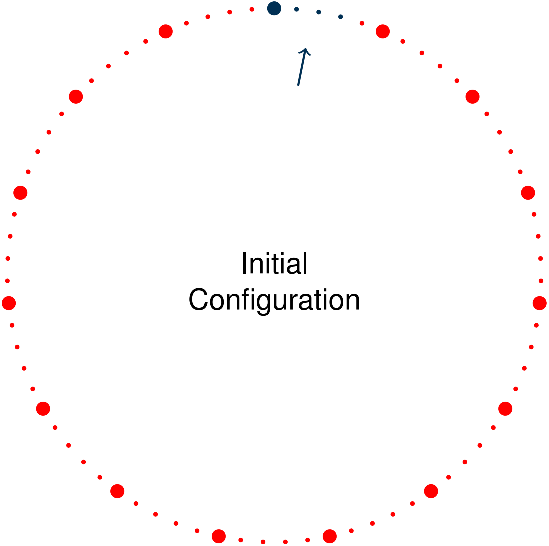
The model must satisfy the safety property!

- Provable in Prism with four trains
- Prism cannot build the model with six trains

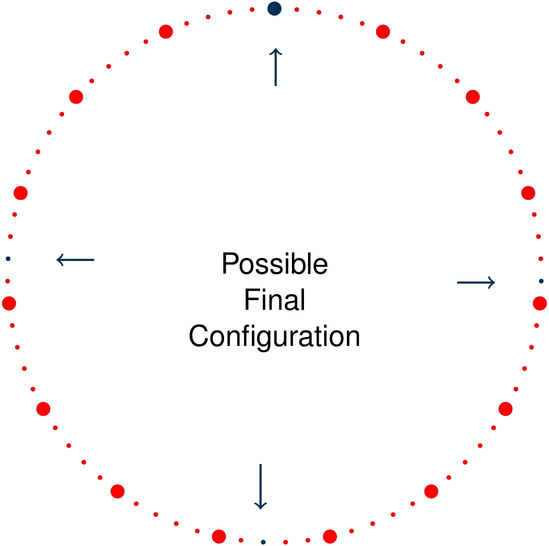
A new abstraction:

- A simpler model: encompasses the previous one
- Every transition becomes nondeterministic
- Safety property was proven with 6 trains

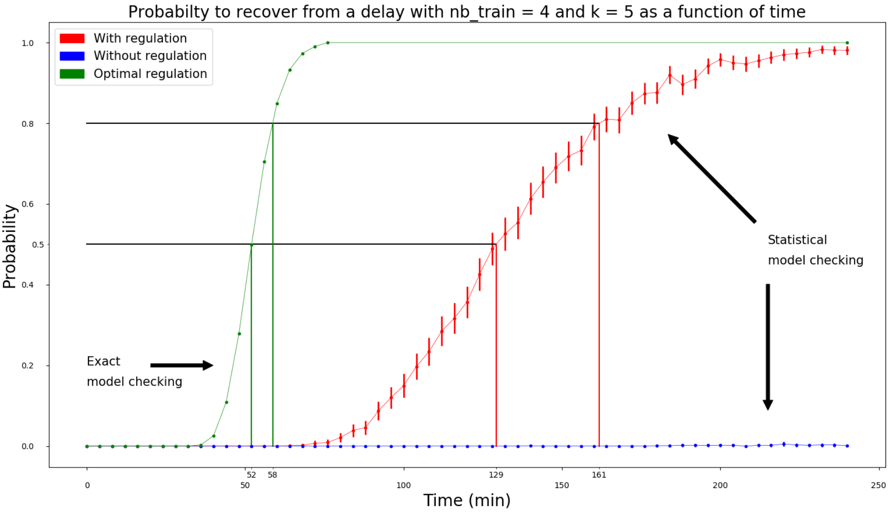
Evaluating efficiency: $nb_{train} = 4$, k = 5



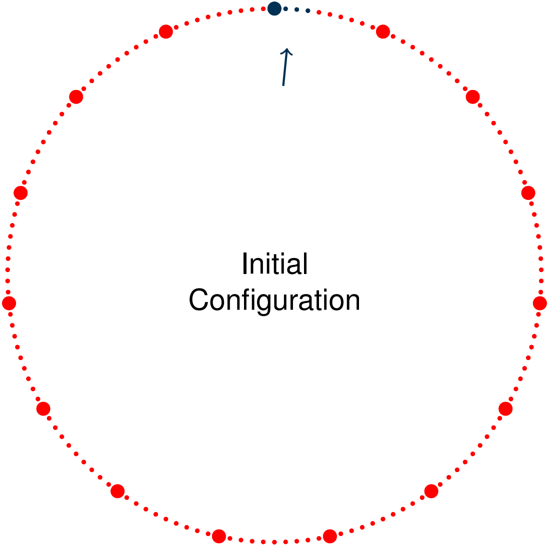
Evaluating efficiency: $nb_{train} = 4$, k = 5



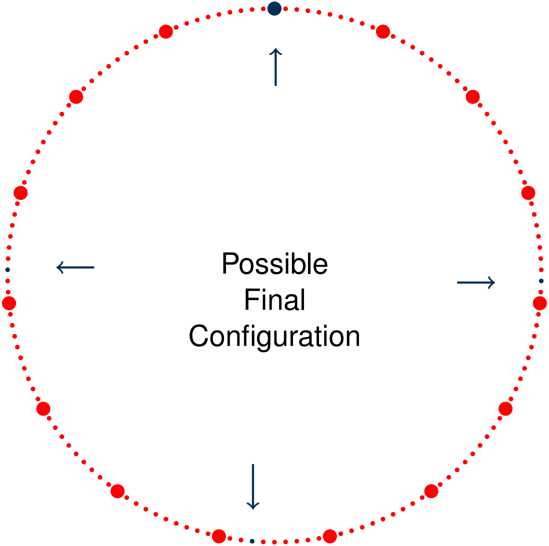
Evaluating efficiency: $nb_{train} = 4$, k = 5



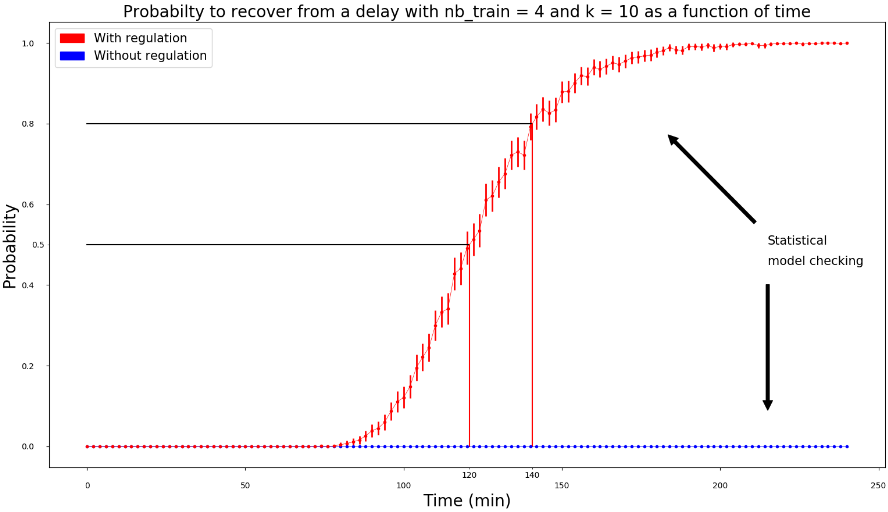
Evaluating efficiency: nb_{train} = 4, k = 10



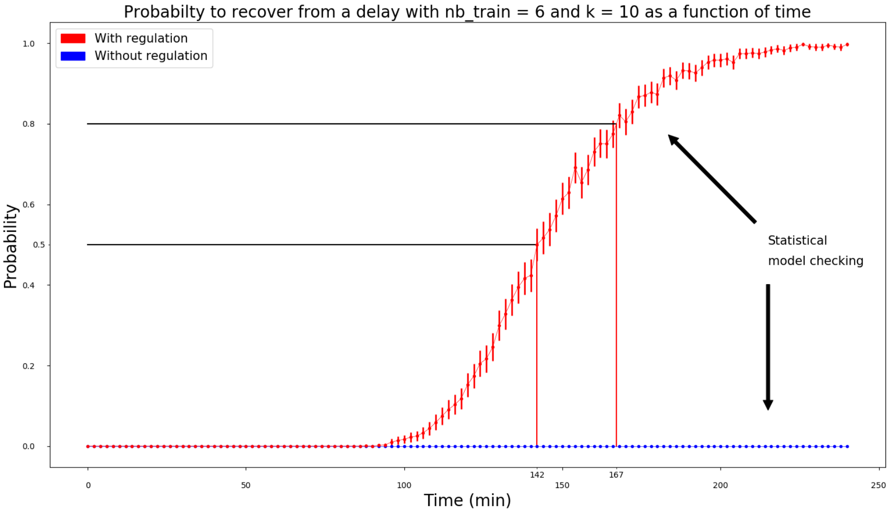
Evaluating efficiency: $nb_{train} = 4$, k = 10



Evaluating efficiency: $nb_{train} = 4$, k = 10



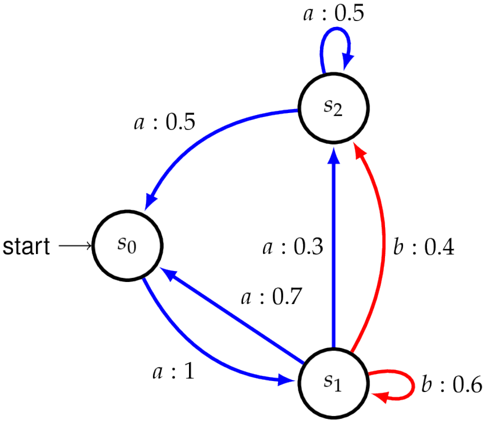
Evaluating efficiency: $nb_{train} = 6$, k = 10

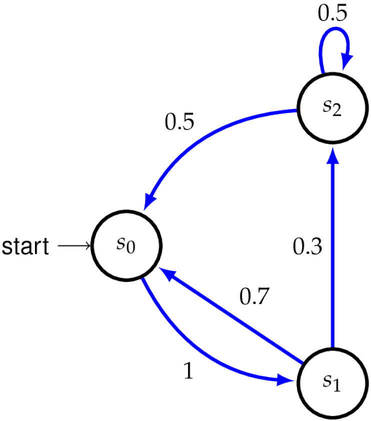


Future Work

- Assess more accurately the efficiency of the regulation policy
- Refine the abstraction of the model
- Study another modelisation of the speed of subways
- What about a new definition of delay ?

Discrete Time Markov Chain (DTMC)





MDP
+ regulation policy
(e. g. always choose a)

=

DTMC

PCTL logic

The PCTL[4][5] logic uses sevral connectors :

- The usual connectors of propositional logic
- Temporal connectors :
  - Next : $X\ \phi$
  - Eventually : $F\ \phi$
  - Bounded eventually : $F^{\leq n}\ \phi$
- A probabilistic connector : $P_{\alpha\ p}$ with $\alpha \in \{\leq, <, \geq, >\}$ and $p \in [0, 1]$

[4] A logic for reasoning about time and reliability, Hanson et al., 1994

[5] Automatic Verification of Finite-state Concurrent Systems Using Temporal Logic Specifications, Clarke et al., 1986

PCTL logic

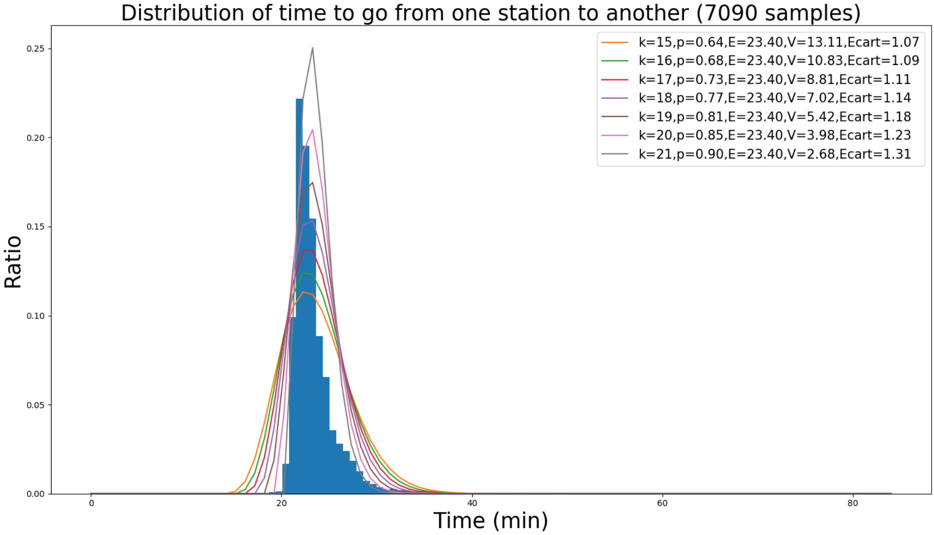
- Two trains never collide :

$$\phi = P_{\leq 0}(F\ \phi_{collision})$$

- If a train has some delays it will catch it up within 10 steps with a high probability:

$$\phi = \phi_{delay} \Rightarrow P_{\geq 0.9}(F^{\leq 10}\ \neg\phi_{delay})$$

Choosing the probabilities: data from Santiago



Parameters 2

Data collected from actual subway rail system:

- Total duration of the course in Glasgow : $t_{tot} = 24min$
- Length of a complete circuit in Glasgow : $d = 10.5km$
- Usual speed of subways : v between 30 and 40 $km.h^{-1}$
- Restriction on the probability : $p \geq 0.8$