Finanziato dall'Unione europea
NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani
PIANO NAZIONALE DI RIPRESA E RESILIENZA
UNIVERSITÀ DI PISA

FORESEEN Project

PRIN PNRR 2022

FORmal mEthodS for attack dEtEction in autonomous driviNg systems

Statistical Model Checking for the Analysis of Attacks in Connected Autonomous Vehicles

Cinzia Bernadeschi, **Dario Pagani**
Dep. of Information Engineering, University of Pisa

Adriano Fagiolini
Dep. of Engineering, University of Palermo

Christian Quadri
Computer Science Dep., University of Milan

Summary

1. Introduction
   - Related works
2. Background
   - Uppaal and Uppaal SMC
   - Statistical model checking for CPS
   - The [longitudinal] platoon
3. Modeling the platoon
   - The network
   - The car
   - Attacks on the platoon
   - Centralized controller and temporization
   - The leader's driver
   - Simulation
4. Analysis of properties
5. Conclusions & Further work

1. Introduction

- **Cyber-Physical Systems** (CPSs) are characterized by cooperating hardware and software components, connected with the external world. (Smart Grids, Transportation Systems, Manufacturing, Energy Systems, IoTs etc…)
- **Cybersecurity** is a relevant activity in CPSs. Examples of attacks on CPSs could be on sensors, actuators or controllers, or even on the communication or computing components.
- Modern **autonomous vehicles** are highly computerized CPSs, thus providing a wide range of access points for a potential attacker, who could gain full control over the vehicle and turn off all safety measures installed on it.

Finanziato dall'Unione europea
NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani
PIANO NAZIONALE DI RIPRESA E RESILIENZA
Università di Pisa

Introduction

In this work, we show

- The use of statistical model checking for the analysis of attacks in connected autonomous vehicles
- The use of timed automata to model physics, system behavior and cyber-attacks
- The framework can be used to model uncertainties and stochastic behaviors

Related works

Examples of SMC in CPS:

- To gauge the performance of electrical converters [1]
- To validate the safety properties of autonomous lanes switching on a motorway [2]
- To validate a Bayesian perception framework used to detect potential collision at crossroads [3]

On platooning:

- Platooning is a driving strategy where multiple vehicles travel closely together in a coordinated group [4]
- The advent of 5G has enabled centralized approaches for vehicle coordination [5]

[1] M. Novak, U. M. Nyman, T. Dragicevic, and F. Blaabjerg, “Statistical model checking for finite-set model predictive control converters: A tutorial on modeling and performance verification,” IEEE Industrial Electronics Magazine, vol. 13, no. 3, pp. 6–15, 2019
[2] M. Barbier et al, “Validation of perception and decision-making systems for autonomous driving via statistical model checking,” in 2019 IEEE Intelligent Vehicles Symposium (IV), p. 252–259, June 2019.
[3] B. Barbot, B. Bérard, Y. Duplouy, and S. Haddad, “Statistical model-checking for autonomous vehicle safety validation,” in Conference SIA Simulation Numérique, (France), Société des Ingénieurs de l’Automobile, Mar. 2017.
[4] C. Bergenhem, S. Shladover, E. Coelingh, C. Englund, and S. Tsugawa, “Overview of platooning systems,” in Proceedings of the 19th ITS World Congress, (Vienna, Austria), pp. 22–26, Oct. 2012.
[5] C. Quadri, V. Mancuso, M. A. Marsan, and G. P. Rossi, “Edge-based platoon control,” Computer Communications, vol. 181, pp. 17–31, 2022.

2. Background – UPPAAL and UPPAAL SMC

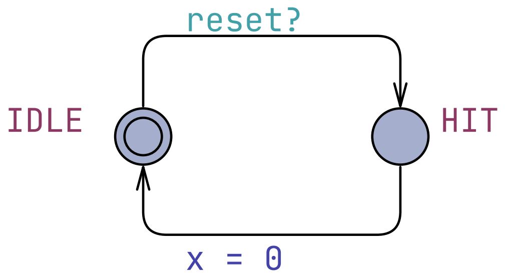
- UPPAAL is a model checker
- It's used to *formally verify* properties on a **network of timed automata**
- A timed automaton is a *finite state machine* with **clocks** and **variables**
- Time is *continuous* and clocks measure time progress
- Automata can synchronize with each other with synchronization primitives
- **UPPAAL SMC** is an extension that allows *statistical verification* of complex and/or stochastic networks of timed automata

Finanziato dall'Unione europea
NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani
PIANO NAZIONALE DI RIPRESA E RESILIENZA
UNIVERSITÀ DI PISA

UPPAAL and UPPAAL SMC

Location

The initial location of the automaton is marked with 2 conc. circles



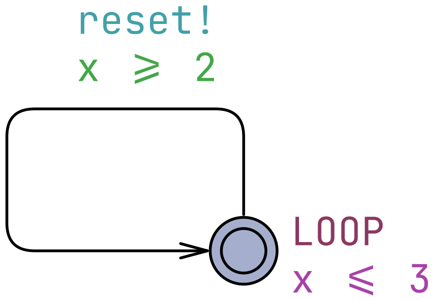
Synchronization

- Within a location, an edge is traversed if a sync with ? is received
- When traversing an edge the syncs with ! are emitted

Assignments to clocks and variables

Transition guard

An expression that must be true for the process to transition through that edge



Invariant

A logical conjunction of simple conditions on clocks that holds true when the process is in the location

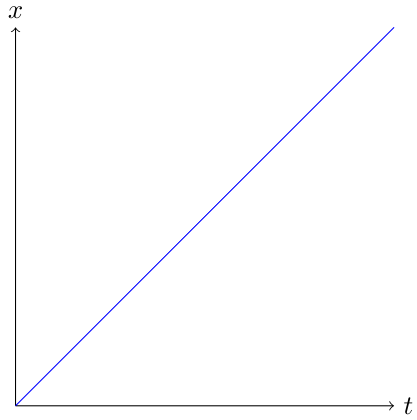
UPPAAL SMC

- Some systems may be too large to be evaluated with classical model checking
- It allows to implement stochastic behaviors
- UPPAAL SMC allows custom clocks' rates
- The custom rates are put in logical AND in the *invariant expression* of a location e.g. `x' == 0.5 and x <= 10`

This is normally omitted for time clocks

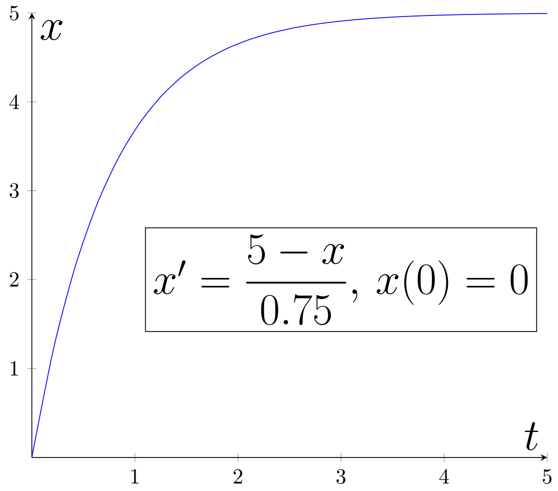
`x'==1`

Default behavior

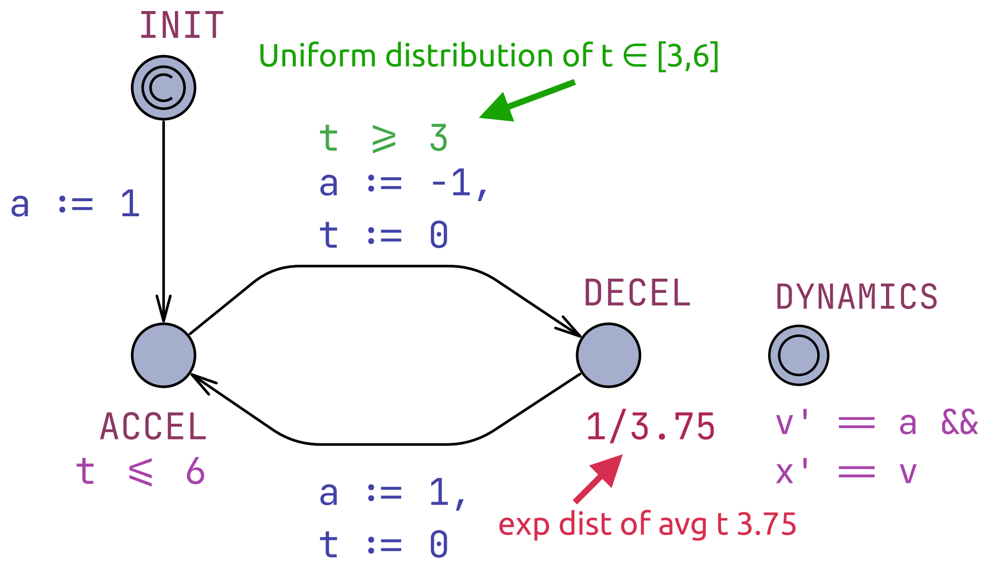


`x'==`$expr$

Custom rate



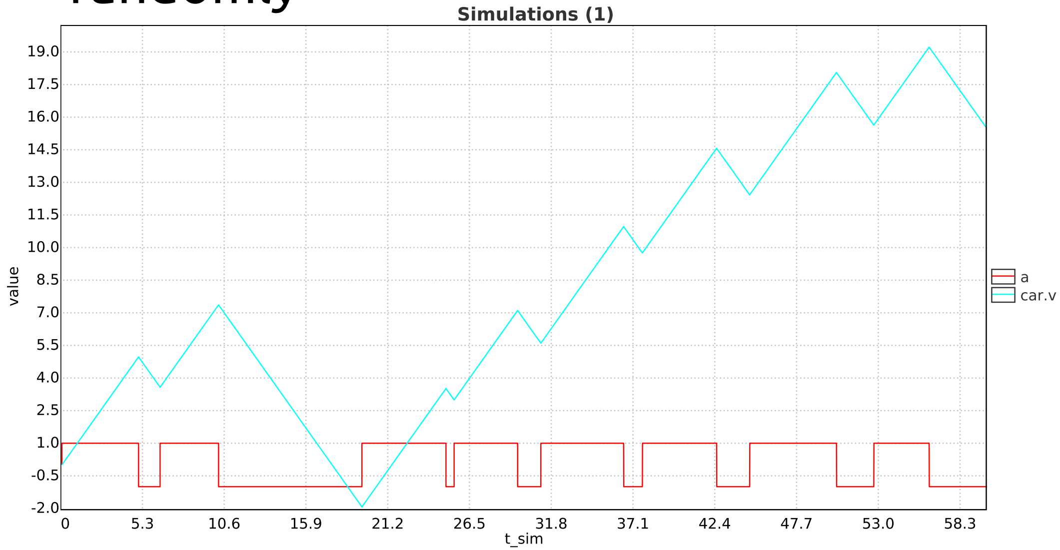
UPPAAL SMC – Simple Car



Driver

Car

- Custom clocks can be used to **model physics**
- Example: a **driver** and a **car**
- The driver accelerates and brakes randomly



UPPAAL SMC

Queries are used to estimate the probability of an expression being true

```
Pr[t_sim ≤ 60] (<> t_sim ≥ 55 && car.v > 10)          0.771707 ± 0.0472945 (95% CI)
Pr[t_sim ≤ 60] ([] t_sim ≥ 55 imply car.v > 10)                ≤ 0.0499441 (95% CI)
```

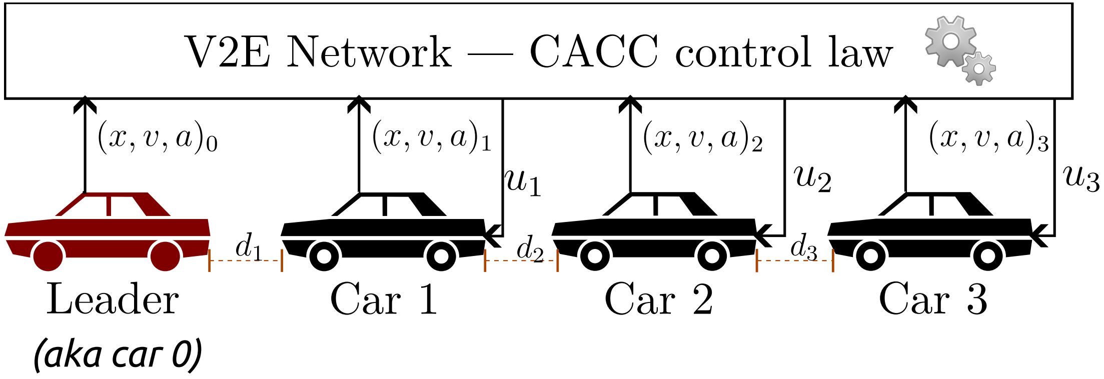
- The operator <> checks if the condition holds for at least an instant
- The operator [ ] checks if the condition holds from start to finish
- The engine will continue to accumulate traces to estimate the probability until the set *confidence interval* is satisfied

Statistical model checking for CPS

- It can model stochastic behaviors
- It can model physics with the derivative notation
- It can mix time-continuous an time-discrete components
- Given a confidence interval, the tool will automatically gather enough traces to estimate a probability of a certain event

Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA
Università di Pisa

The [*longitudinal*] platoon



$$d_i = x_{i-1} - x_i - 4$$

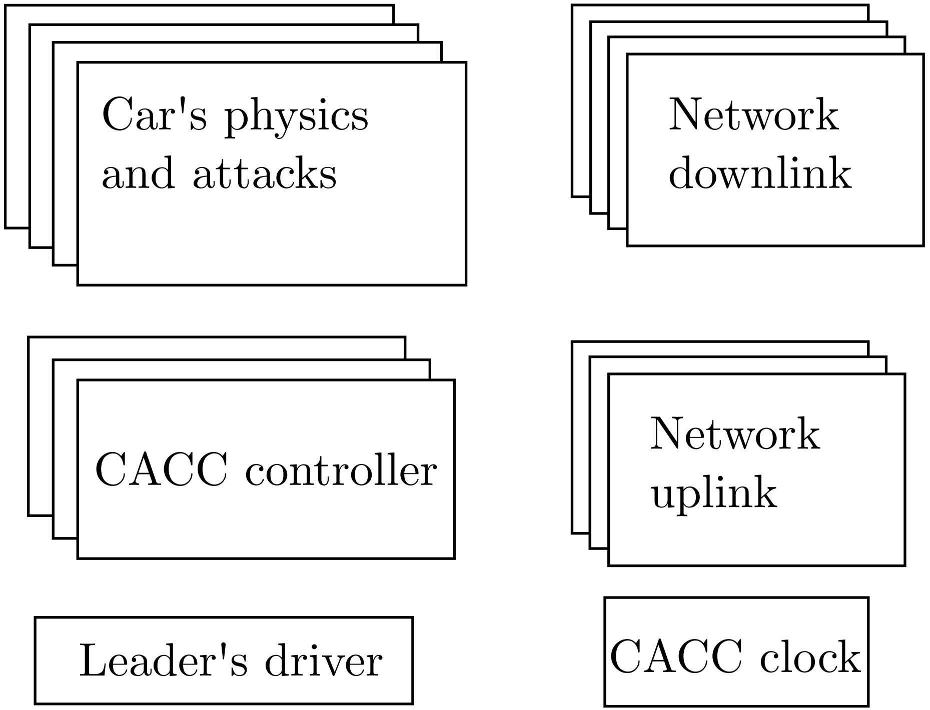
- The follower cars follow the leader
- They try to maintain a safety distance D from the car in front
- The **Cooperative Adaptive Cruise Control** (CACC) [1] control law is used

$$u_i = \alpha_1 a_{i-1} + \alpha_2 a_0 + \alpha_3 (v_i - v_{i-1}) + \alpha_4 (v_i - v_0) + \alpha_5 (D - d_i)$$

[1] Rajamani, R. and Han-Shue Tan and Boon Kait Law and Wei-Bin Zhang "Demonstration of integrated longitudinal and lateral control for the operation of automated vehicles in platoons" 2000

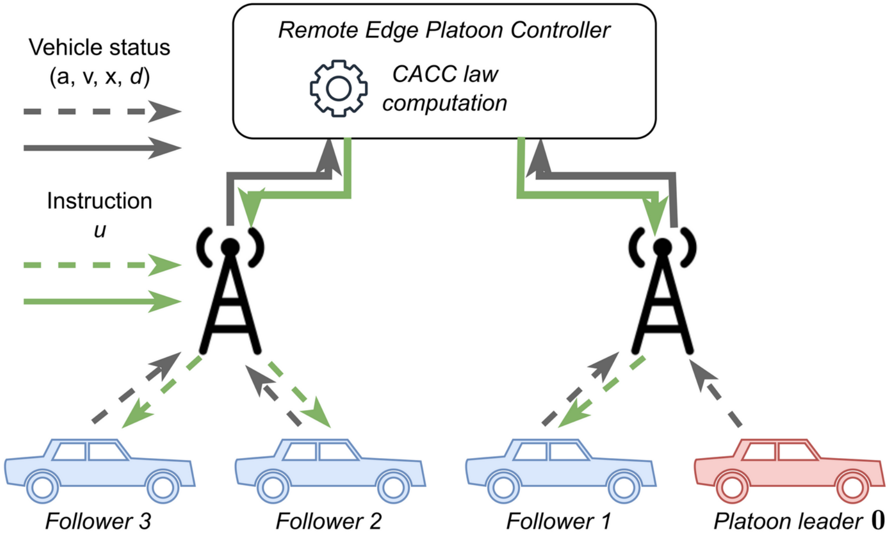
Modeling the platoon

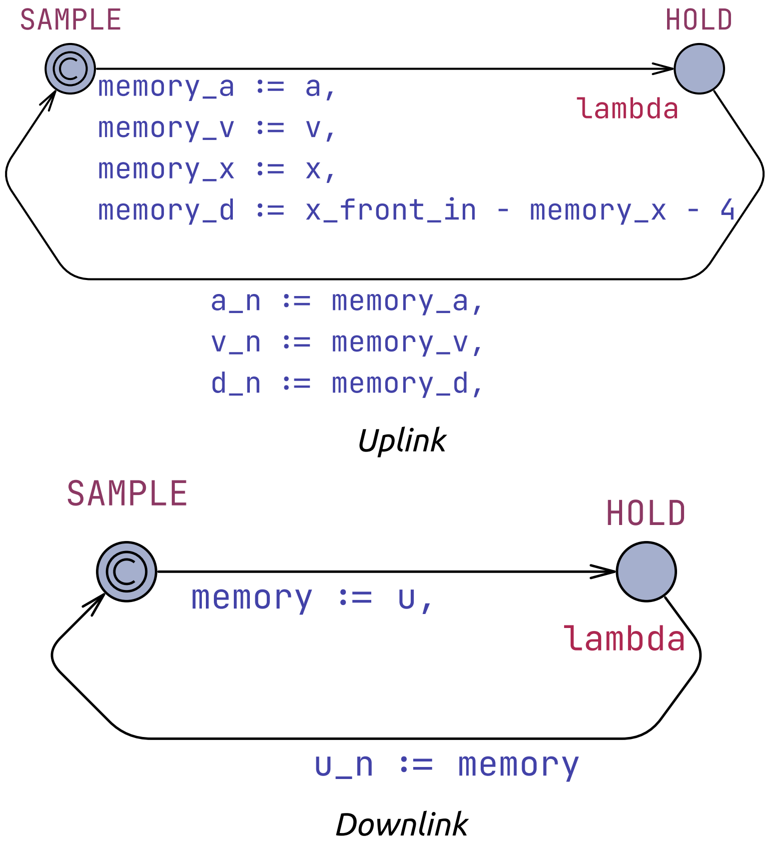
- We modeled the platoon using six timed automata



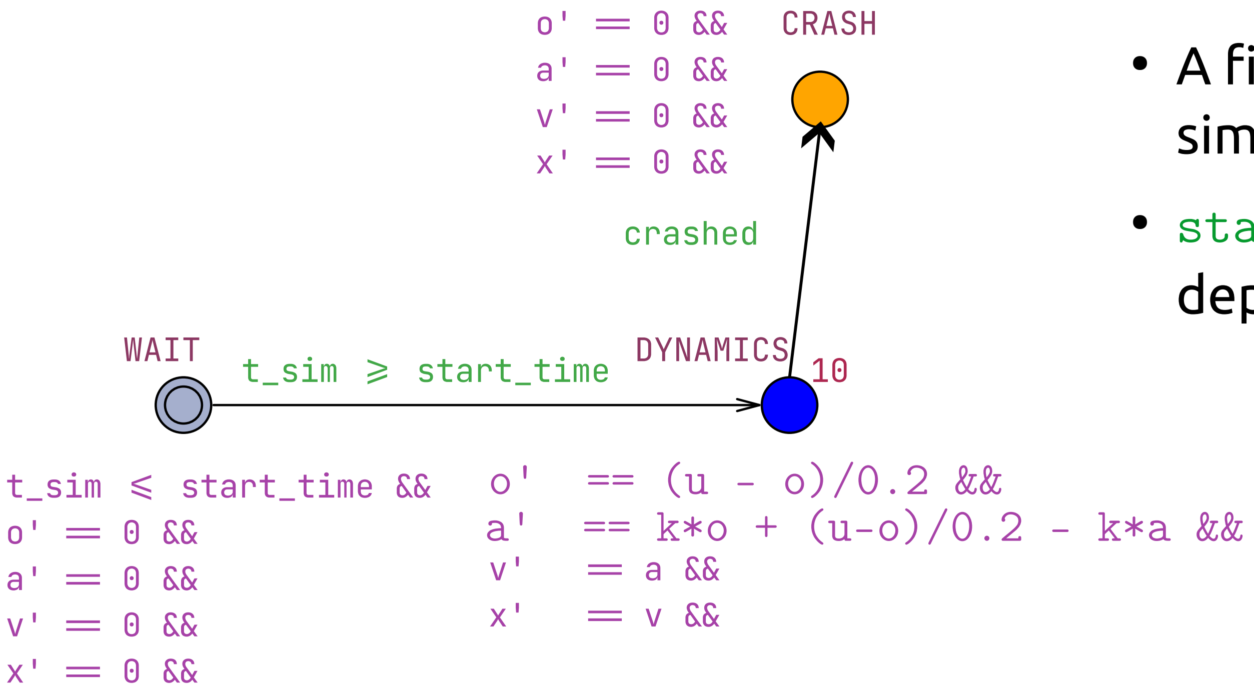
The network

- Data are delayed by 1/lambda seconds, on average





The car



Car's physics

- u is the reference acceleration computed by CACC
- A first-order filter (a, o) is used to simulate the *actuation delay*
- start_time is used to delay the departure of the car

Attacks on the platoon

- We consider the case of **data alteration** of one of the car's state variable (we'll consider car 1 under attack)
- We alter the value of *position*, *speed* and *acceleration* reported back to the centralized controller at the network edge from car 1
- The attack starts at a certain time $t_{\mathrm{A}} = 30\mathrm{s}$
- We add a **spurious signal** with parameter A

Simulation time

$$a(t) = \hat{a}(t) + A \sin\left(\frac{2\pi}{10} t\right)$$

Modified accel — *Unaltered accel* — *Frequency of 0.1Hz*

Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA
Università di Pisa

Attacks on the platoon

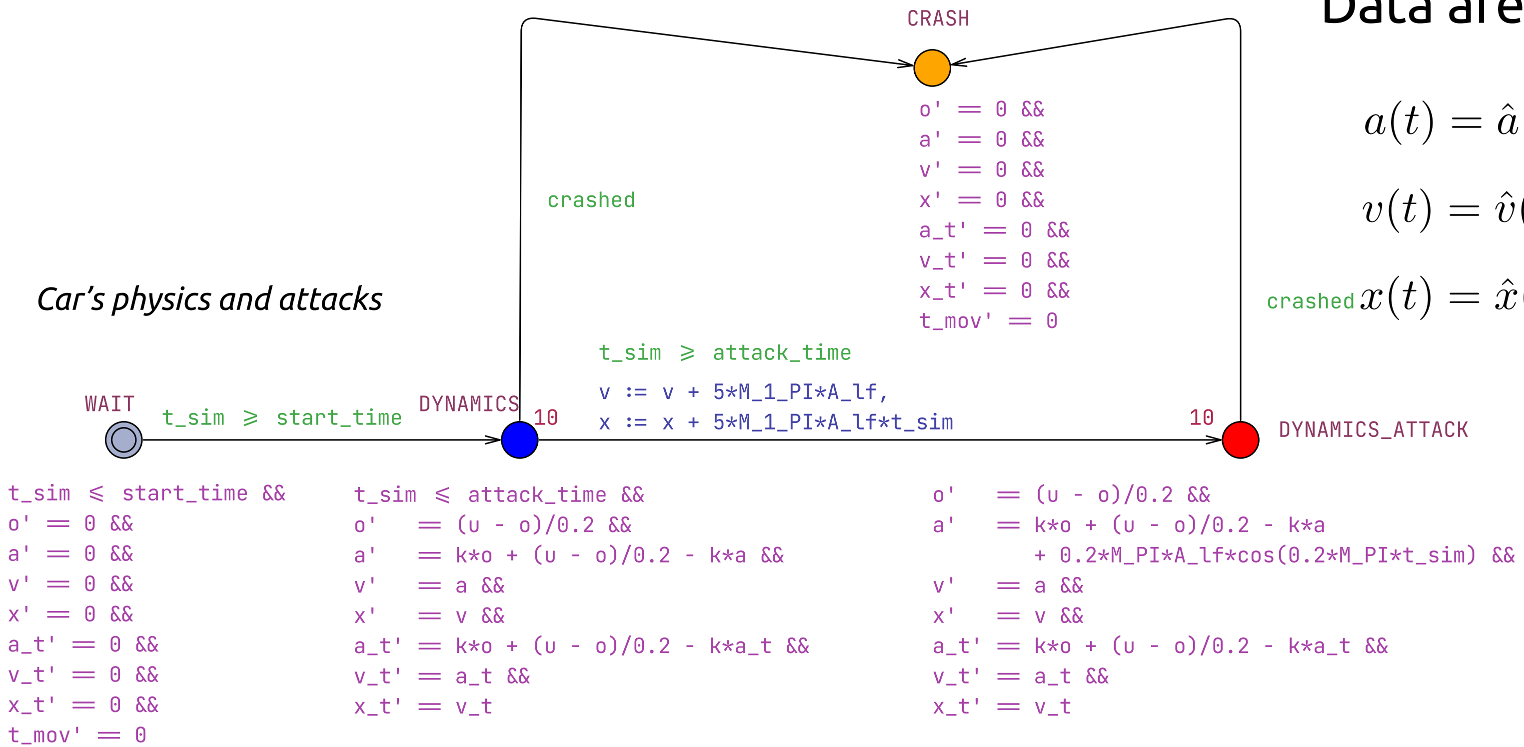
Data are altered **consistently**

$$a(t) = \hat{a}(t) + A\sin\left(\frac{2\pi}{10}t\right)$$

$$v(t) = \hat{v}(t) - \frac{5}{\pi}A\cos\left(\frac{2\pi}{10}t\right) + \frac{5}{\pi}A$$

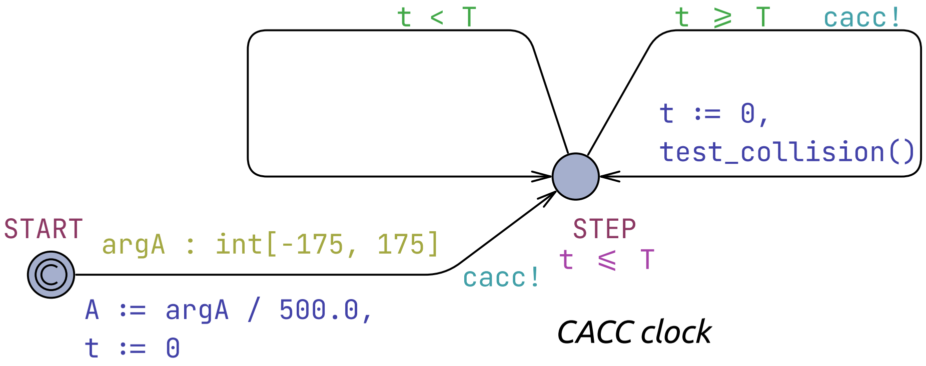
$$x(t) = \hat{x}(t) - \frac{25}{\pi^2}A\sin\left(\frac{2\pi}{10}t\right) + \frac{5}{\pi}At$$

Car's physics and attacks

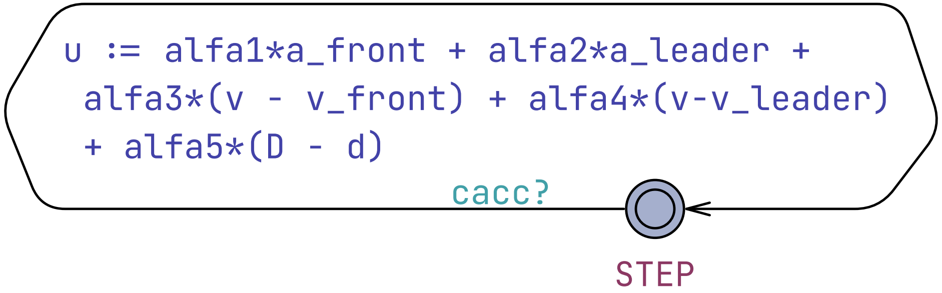


These addenda are the initial conditions on x and v

Centralized controller and temporization



CACC clock



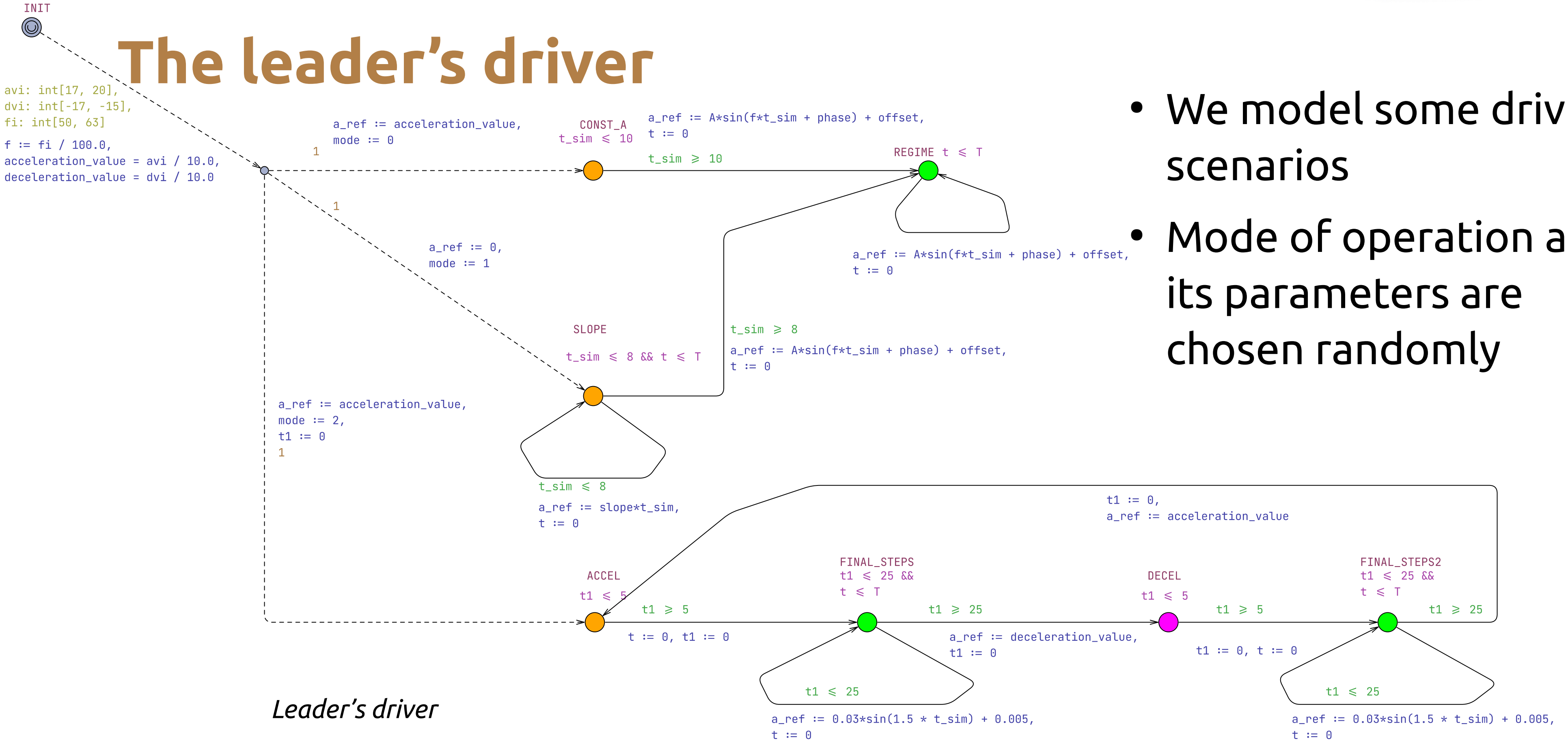
CACC controller

- Using T = 10 ms
- Every T a `cacc!` sync is fired, causing the update of the control law
- The `test_collision()` procedure checks if cars have crashed

Finanziato dall'Unione europea
NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani
PIANO NAZIONALE DI RIPRESA E RESILIENZA
UNIVERSITÀ DI PISA

The leader's driver

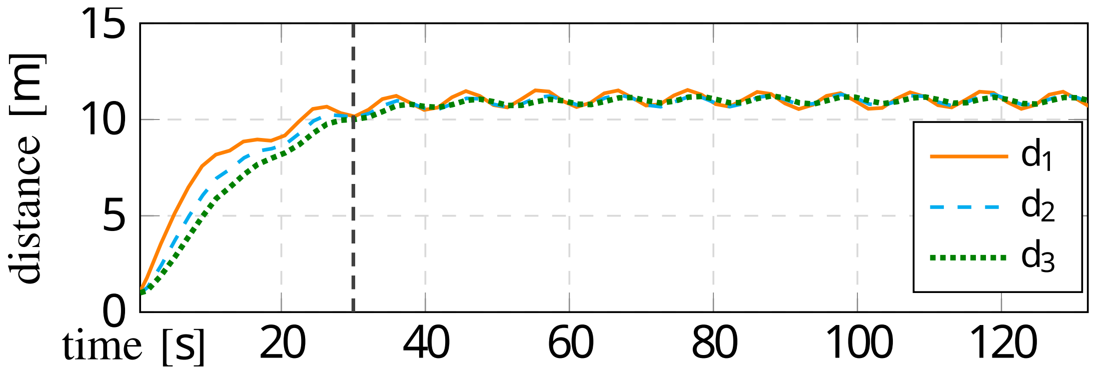
- We model some driving scenarios
- Mode of operation and its parameters are chosen randomly



Leader's driver

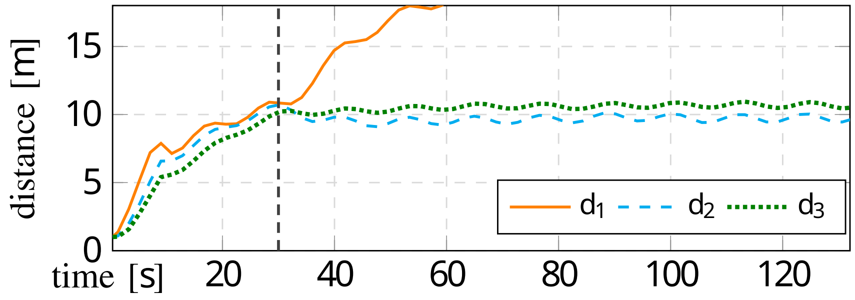
Simulation

- Let us consider some example of simulation traces
- Simulation are performed via the `simulate` query
- The attack takes place on car 1 after 30 seconds



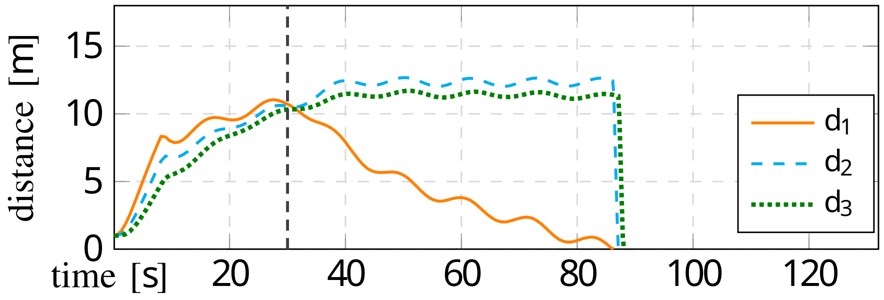
- With no attack the system behaves as expected.
- Distances converge to 11 meters

Simulation



Attack with A > 0

No crash but the car 1 distances itself from the leader



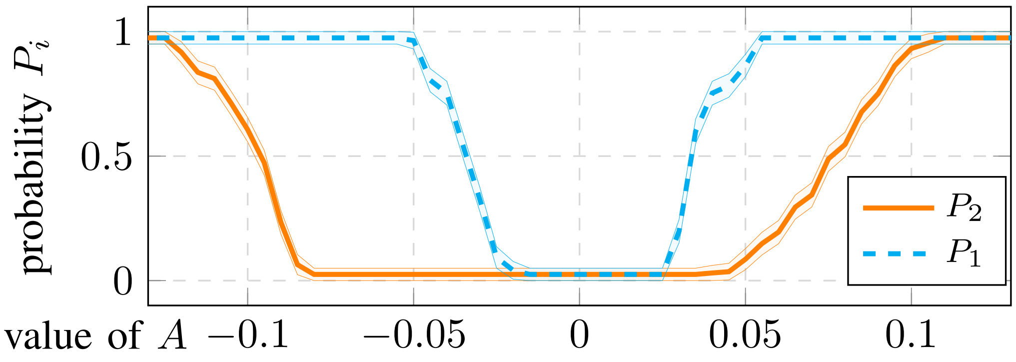
Attack with A < 0

Car 1 gets closer to the leader until they crash and cause a pile-up

Analysis of properties

Given A, let us consider the probability of having a *relative error* on the following distance of car i greater than 15%

$$\varepsilon_i = \frac{|\hat{d}_i - D|}{D} \qquad P_i = P(\varepsilon_i \geq 0.15 \,|\, 30 \leq t \leq 40)$$

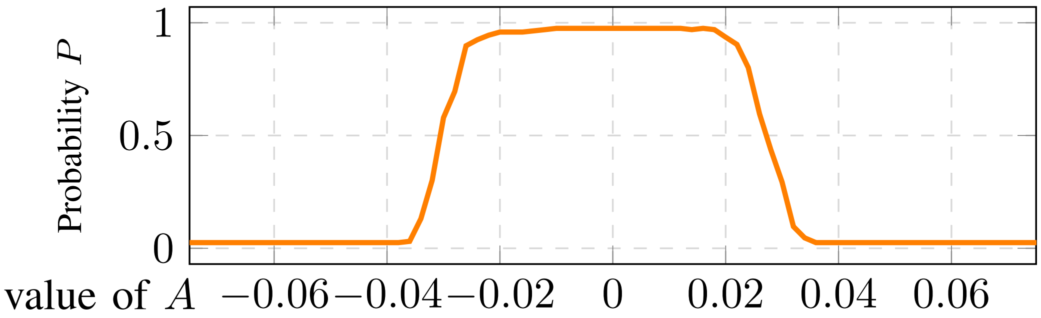


- `Pr[t_sim <= 40] (<> t_sim >= 30 && fabs((x_p[0] - x_p[1] - 4)/11 - 1) > 0.15)`
- `Pr[t_sim <= 40] (<> t_sim >= 30 && fabs((x_p[1] - x_p[2] - 4)/11 - 1) > 0.15)`
- The *confidence interval* was set to 95
- Intuitively, this metrics tells us how easy it is to do attack detection in a small window of time

Finanziato dall'Unione europea NextGenerationEU | Ministero dell'Università e della Ricerca | Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA | UNIVERSITÀ DI PISA

Analysis of properties

$$P(\forall t \leq 40\text{s}, \quad t \geq 30\text{s} \implies \forall i \quad \varepsilon_i < 0.15)$$




- ```
  Pr[t_sim <= 40] ([] t_sim >= 30 imply
          forall (I : int[1, 3]) fabs((x_p[i-1] - x_p[i] - 4)/11 - 1) < 0.15)
  ```
- The *confidence interval* was set to 95
- Intuitively, this tells us how the platoon overall is safe to a certain attack in a certain of window of time
  ```

Conclusions

- We've shown how SMC can be used to study the safety and resilience of CPSs to cyber-attacks
- Risk assessment of cyber-attacks can be performed
- It can be used to find properties to evaluate at runtime to check for attacks

Further work

- Increase the fidelity of the model, i.e. adding packet drops, aerodynamic draft, latitudinal movements etc…
- Study more types of attacks

Finanziato dall'Unione europea
NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani
PIANO NAZIONALE DI RIPRESA E RESILIENZA
Università di Pisa

FIN
Thank you for the attention

This work is part of the FORESEEN project

https://foreseen.dii.unipi.it

P2022WYAEW – *FORESEEN: FORmal mEthodS for attack dEtEction in autonomous driviNg systems*