Finanziato dall'Unione europea
NextGenerationEU

Ministero dell'Università e della Ricerca

Italiadomani
PIANO NAZIONALE DI RIPRESA E RESILIENZA

Università di Pisa

FORESEEN Project

PRIN 2022 PNRR

FORmal mEthodS for attack dEtEction in autonomous driviNg systems

https://forseen.dii.unipi.it

Severity of attacks in a vehicle platoon by model-based simulation

Cinzia Bernadeschi, Giuseppe Lettieri, **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

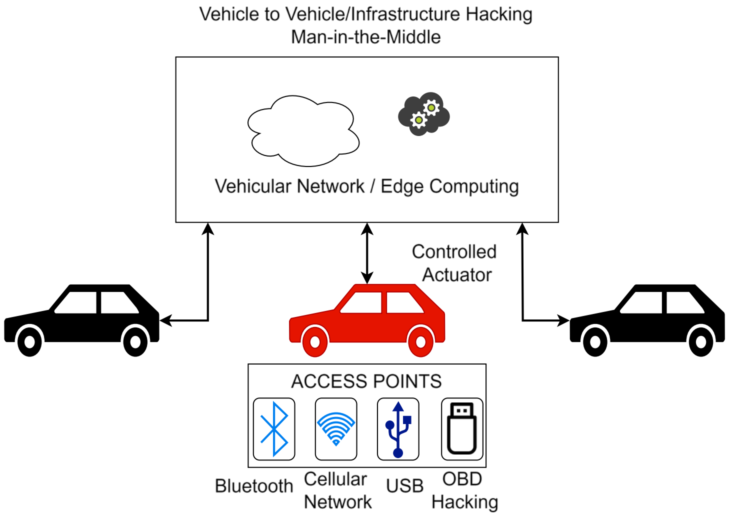
Antonella Santone, Vittoria Nardone
Dep. of Medicine and Health Sciences Vincenzo Tiberio, University of Molise

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

Introduction

The goals of our work:

1. Enhancing security of *connected autonomous vehicles* (CAV) by developing run-time local monitors for attack detection: the case of vehicle platoon
2. Model-based design security analysis
3. Traces analyses for anomaly detection
4. Model checking & abstract interpretation to identify patterns suggesting the possibility of an impending attack

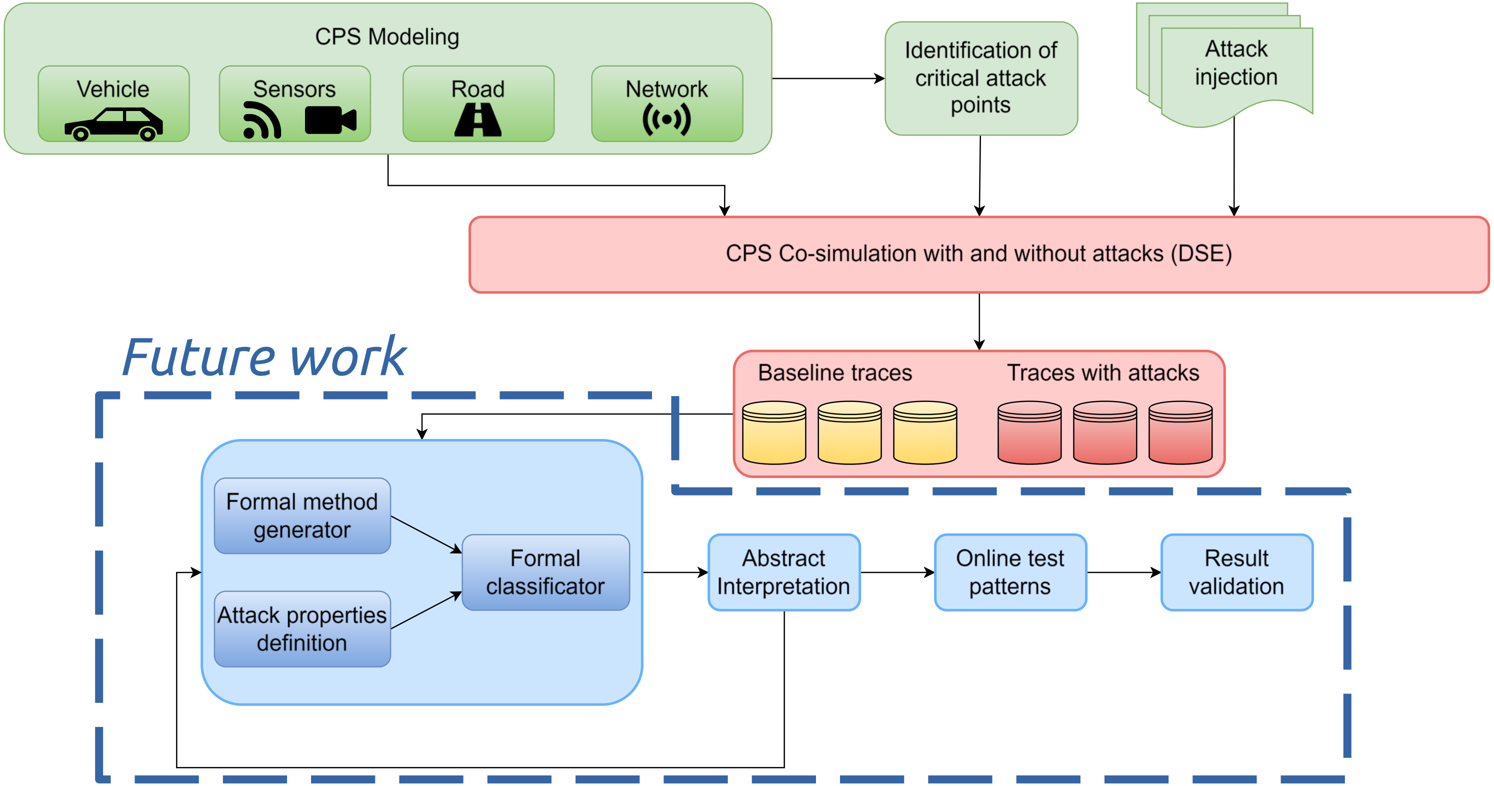


Motivations:

Vulnerability in vehicle ecosystems

GPS, OBD, CAN etc… etc…

Introduction – Project's goal



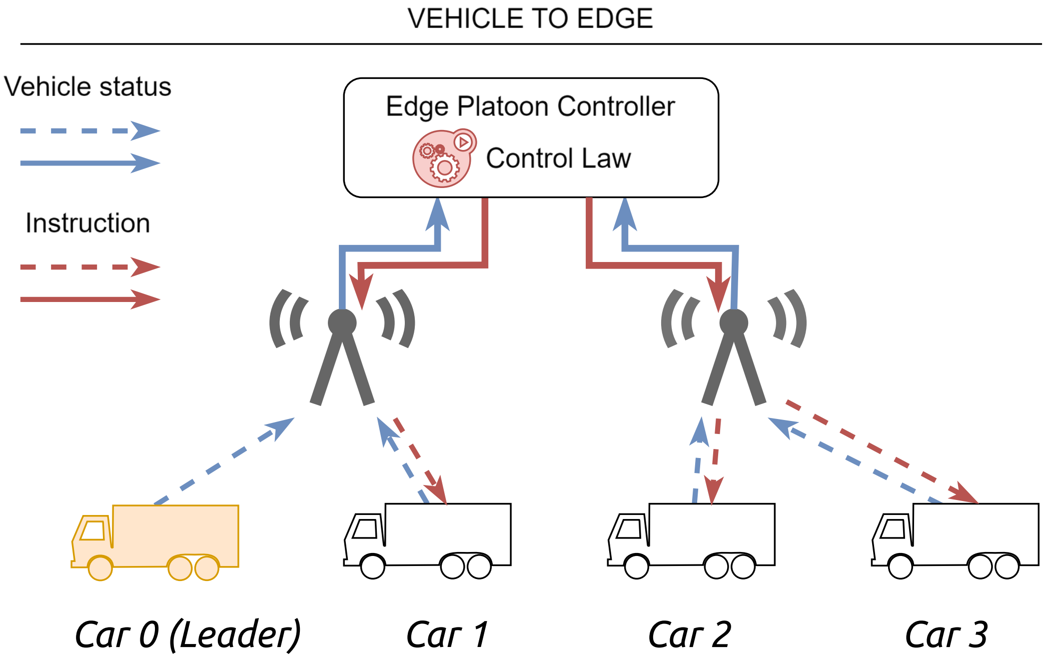
Vehicle platoon

The platoon's main objective is to keep an inter-vehicular distance D=11 meters between each pair of cars.

We study two kind of configurations:

1. Vehicle-to-edge
2. Vehicle-to-vehicle

The *Cooperative Adaptive Cruise Control* (CACC) is used to control the platoon

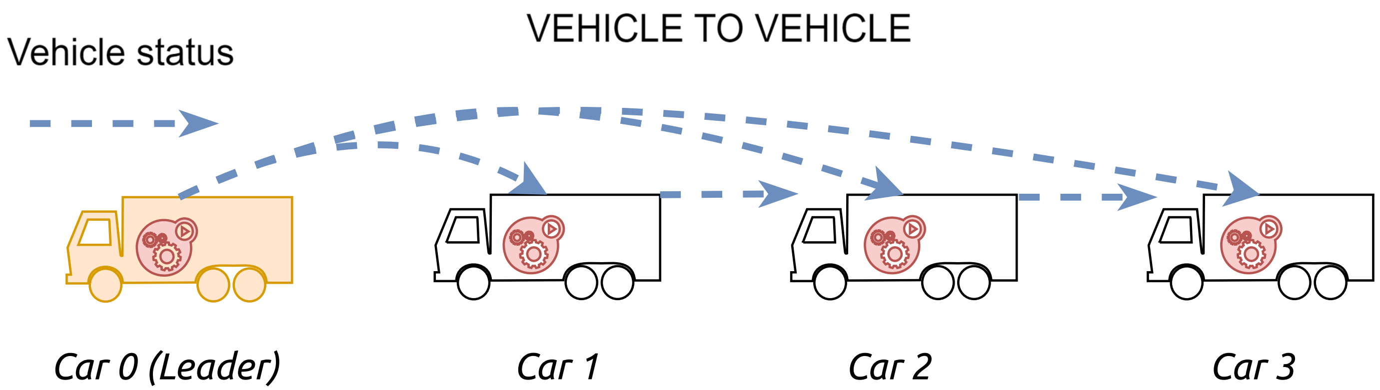


Vehicle platoon – V2V

The V2V counterpart is similar but there's a pair of edge of each pair of cars (i, i - 1) and (i, 0).

The IEEE 802.11p protocol is implemented as the network medium.

[1] was used to simulate the rate of packet drops in function of distance, vehicle distance and network traffic



[1] M. Sepulcre, M. Gonzalez-Martín, J. Gozalvez, R. Molina-Masegosa and B. Coll-Perales, "Analytical Models of the Performance of IEEE 802.11p Vehicle to Vehicle Communications," in *IEEE Transactions on Vehicular Technology*, vol. 71, no. 1, pp. 713-724, Jan. 2022

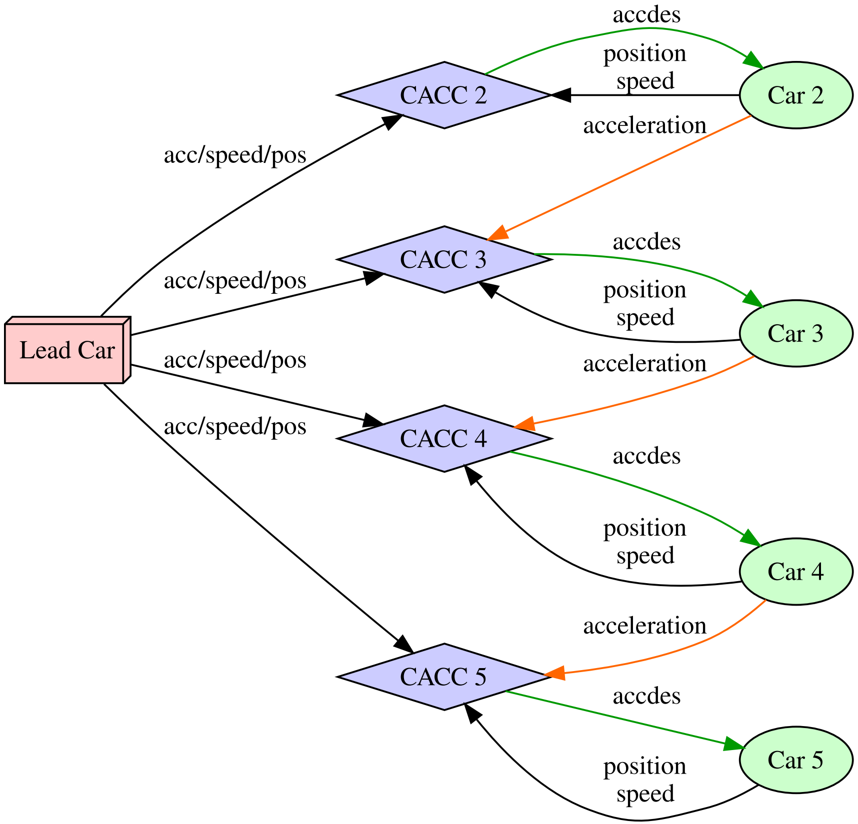
Co-simulation

We have the following FMUs:

Name	Language
Car's physics	MATLAB
[V2E] Network medium + CACC Controller	Python
[V2V] Network Medium	C++
[V2V] CACC Controller	C

INTO-CPS is used as the COE

http://into-cps.org



How the FMUs are connected in the V2V scenario

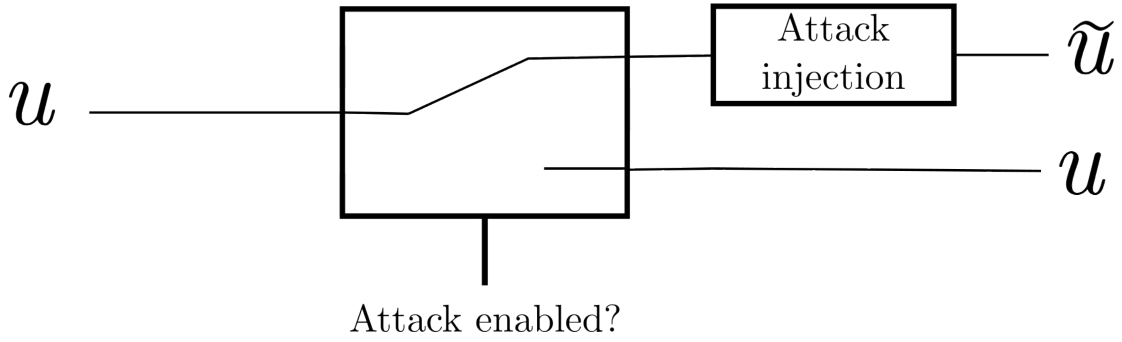
Attack injection

We study two kinds of *data alteration* attacks:

1) **Actuator alternation** (i.e. on the value of desired acceleratoin u sent by the CACC to the car's physics)

2) **Physical values alteration** (i.e. on the x,v,a values sent by vehicle to the edge/other vehicles)

They're implemented by **adding a switch** in the car's physics' FMU



Attack injection for the 1st case

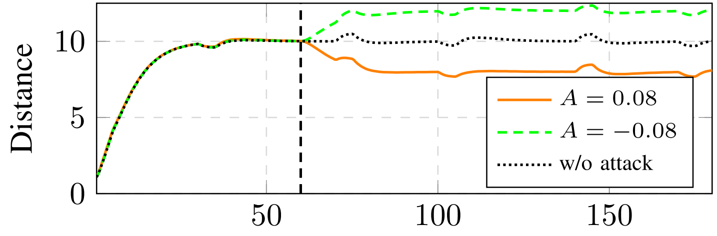
For the 2nd attack is analogous

Actuator alteration

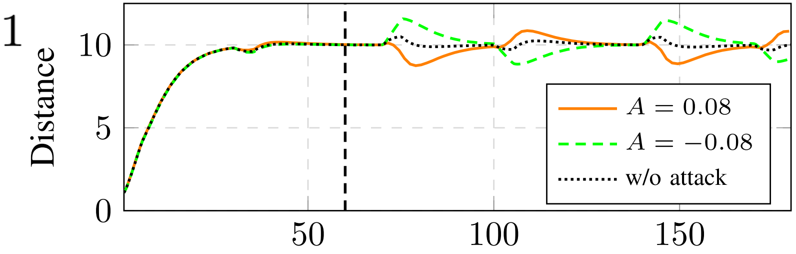
Attack on the actuator with a certain parameter A

$$\tilde{u}_1 = u_1 + A$$

$$\tilde{u}_1 = (1 + A) \cdot u_1$$



(a) d_1, gap between car 1 and the leader



Physical values alteration

$$\tilde{a}(t) = a(t) + A \sin(2\pi f t)$$

$$\tilde{v}(t) = v(t_0) + \int_{t_0}^{t} \tilde{a}(\tau) d\tau$$

$$\tilde{x}(t) = x(t_0) + \int_{t_0}^{t} \tilde{v}(\tau) d\tau$$

Ranges under study

Examples of possible values of A:

±0.08, ±0.04, ±0.5, etc…

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

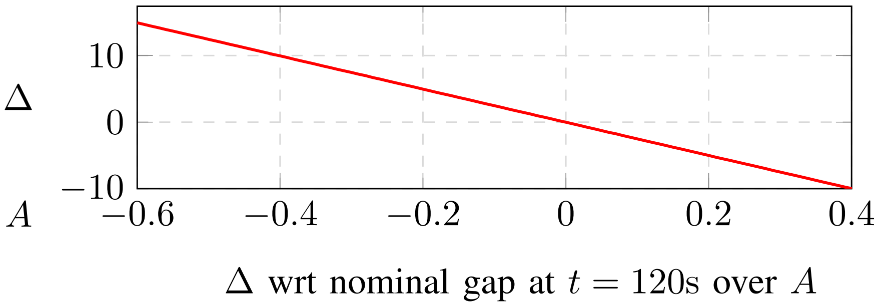
Assumptions

- The CACC control law is assumed to be the same between the two scenario
- Packet latency are drawn from an exponential distribution
- V2V
  - Simulation of highly congested radio channel
- V2E
  - Reliable link (no packet loss)
  - RTT within 30 ms

Some results & Conclusions

We tested many parameter combinations.

- Attacks **data-alteration** are most dangerous
- Attacks on **actuators** mainly result in a reduced inter-vehicular distance.



Example of possible data aggregation

These figures are relative to V2E. (similar to V2V)

***P1**: Physical values alteration attacks*

***P2**: actuator alteration attacks*

Label class	*No attack*	*Attack leader P1*	*Attack on car 1 - P1*	*Attack on car 1 - P2*	*Attack on car 4 - P1*	*Attack on car 4 - P2*
OK	100.00%	33.33%	33.33%	50.00%	33.33%	75.00%
TOO CLOSE	0.00%	0.00%	0.00%	50.00%	0.00%	25.00%
COLLISION	0.00%	66.67%	66.67%	0.00%	66.67%	0.00%
# TRACES	*96*	*576*	*288*	*384*	*288*	*384*

Further work

- More attacks
- Extract models of the cars' behaviors from the traces
- Extract properties from the traces
- Generate online tests to check against attacks on the vehicle

FIN
Thank you for the attention

This work is part of the FORSEEN project

https://forseen.dii.unipi.it

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