# Formal methods for attack detection in autonomous driving systems: the FORESEEN project

Cinzia Bernardeshi, Giuseppe Lettieri , Alessio Vivani , Alessio Bechini , Alessio Vecchio , Federico Rossi - University of Pisa, Italy
Christian Quadri , Alessia Galdeman - University of Milan, Italy
Adriano Fagiolini, Salvatore Pedone - University of Palermo, Italy
Antonella Santone, Vittoria Nardone, Francesco Mercaldo, Simona Correra, Giulia Varriano - University of Molise, Italy

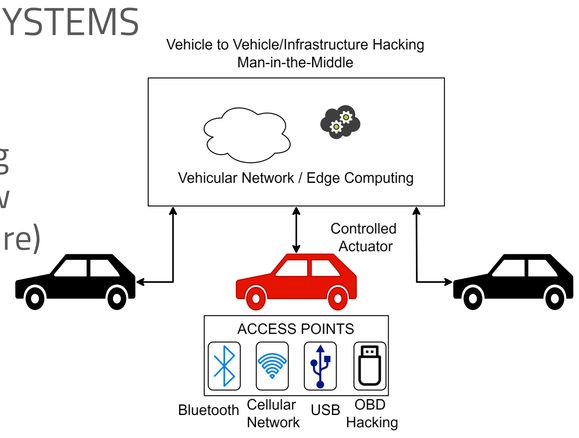
PURPOSE AND GOALS

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

## MOTIVATIONS

VULNERABILITY IN VEHICLE ECOSYSTEMS

- GPS spoofing attack
- On-Board Diagnostic (OBD) hacking
- Actuator controlled by malicious sw
- Attack on CAN bus (Injection/Capture)
- V2I hacking
- V2V hacking
- Man-in-the-Middle attack
- .....



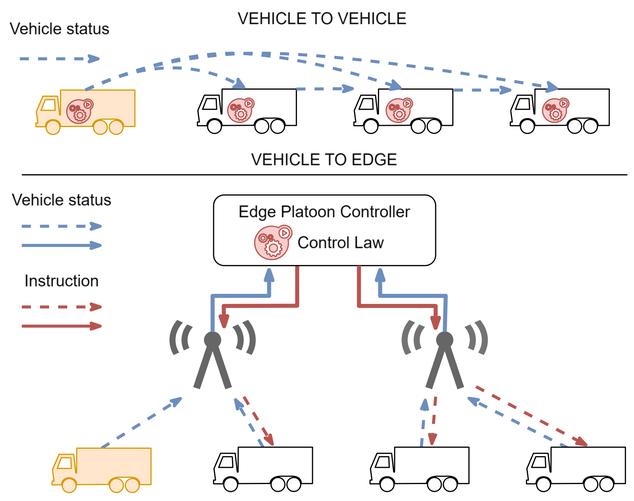

## PLATOONING APPLICATION

❑ VEHICLE TO VEHICLE

Vehicle to vehicle broadcast communication
Cooperative Adaptive Cruise Control (CACC) law on-board of the vehicle

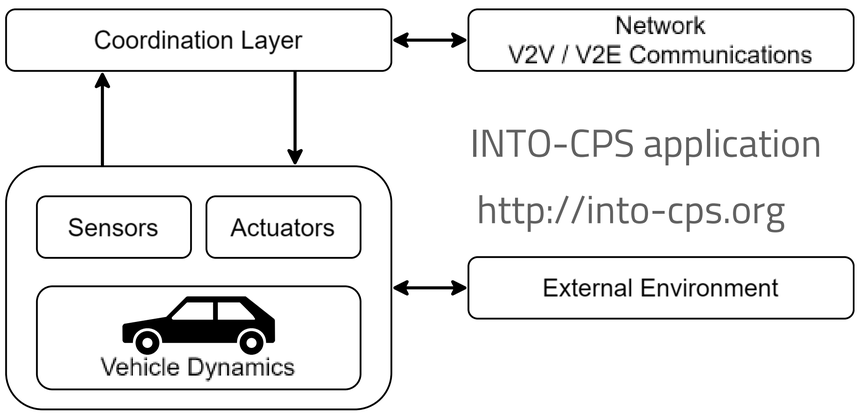
❑ VEHICLE TO EDGE

Vehicle communications through mobile network
Cooperative Adaptive Cruise Control (CACC) law on the edge node




## BACKGROUND

❑ CO-SIMULATION




INTO-CPS application

http://into-cps.org

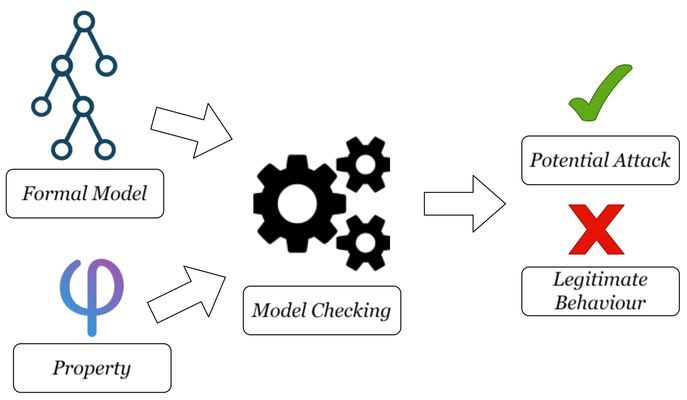
Co-simulate heterogeneous subsystems: vehicle dynamics, control and communication network

Maurizio Palmieri, Christian Quadri, Adriano Fagiolini, Cinzia Bernardeschi. *Co-simulated digital twin on the network edge: A vehicle platoon*. Computer Communications, vol. 212, pp. 35-47, 2023

❑ Model-based attack injection and security analysis

Cinzia Bernardeschi, Andrea Domenici, Maurizio Palmieri. *Formalization and co-simulation of attacks on cyber-physical systems*. Journal of Computer Virology and Hacking Techniques, vol. 16, pp. 63-77, 2020

❑ FORMAL METHODS



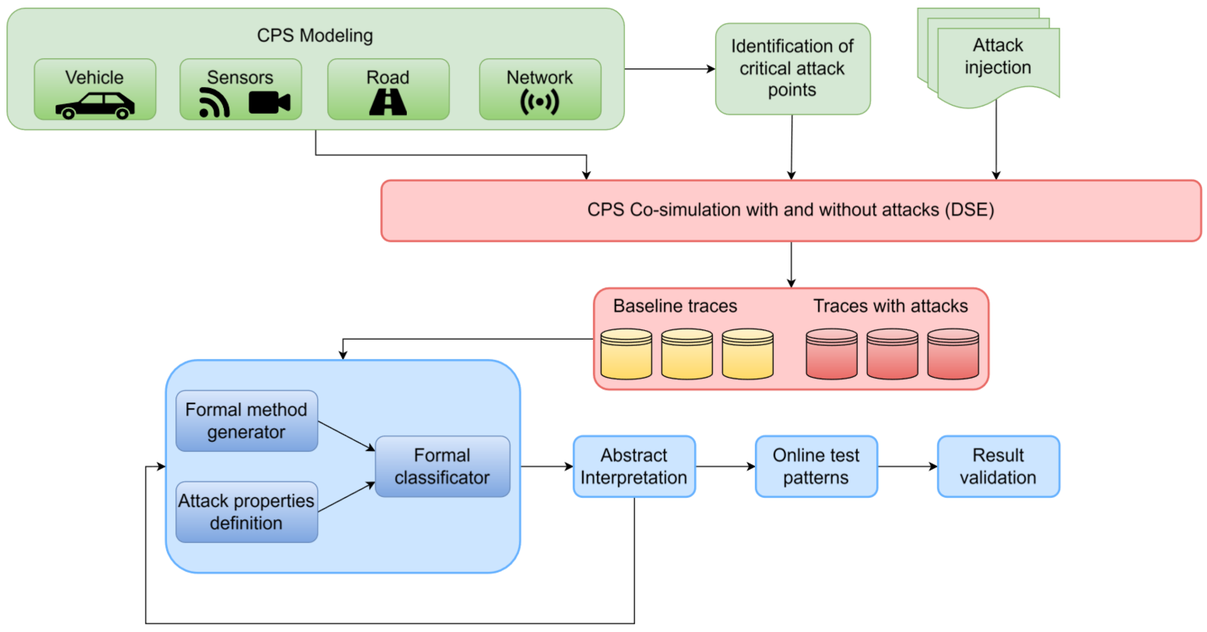

Model checking

Automated verification of temporal logic formulae on system's model expressed as an automaton

Cinzia Bernardeschi, Andrea Domenici, Francesco Mercaldo, Antonella Santone. *Identify Potential Attacks from Simulated Log Analysis*. Proceedings of the International Joint Conference on Neural Networks, IJCNN 2020: pp. 1-6, 2020

## CONTRIBUTION

The methodology




1. Simulation of an autonomous system of vehicles employing co-simulation and collection of simulation traces in the absence and presence of attacks. The **Design Exploration Tool** for generation of multiple simulations is exploited ("CPS Co-simulation with and without attacks (DSE)" activity)

2. Generation of formal models for traces, in terms of a process algebra language ("Formal Method generator" activity)

3. Detection of attacks using model checking technique ("Attack properties definition" activity)

4. Identification of trace segments characteristic of attacks that can be used for on-line monitoring ("Formal classificator" activity)

5. Using abstract interpretation techniques to quantify the robustness of the analysis ("Abstract Interpetation" and "Results validation" activities)

**This project received funding from the European Union – Next-GenerationEU – National Recovery and Resilience Plan (NRRP) – MISSION 4 COMPONENT 2, INVESTMENT N. 1.1, CALL PRIN 2022 PNRR D.D. 1409 14-09-2022 – FORESEEN: FORmal mEthodS for attack dEtEction in autonomous driviNg systems, CUP N.I53D23006130001.**

Funded by the European Union NextGenerationEU | Ministero dell'Università e della Ricerca | Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA | Università di Pisa