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

Cinzia Bernardeschi, Giuseppe Lettieri, Alessio Vivani,
Alessio Bechini, Alessio Vecchio, Federico Rossi
Department of Information Engineering
University of Pisa
Pisa, Italy

Christian Quadri, Alessia Galdeman
Department of Computer Science
University of Milano
Milano, Italy

Adriano Fagiolini, Salvatore Pedone
Department of Engineering
University of Palermo
Palermo, Italy

Antonella Santone, Vittoria Nardone, Francesco Mercaldo,
Simona Correra, Giulia Varriano
Department of Medicine and Health Sciences Vincenzo Tiberio
University of Molise
Campobasso, Italy

***Abstract*—This poster describes the methodology of the FORESEEN project for detecting cyber-attacks in autonomous vehicular networks. The methodology exploits co-simulation to generate the system's execution traces and formal methods to derive simple tests from traces that can be run for online monitoring services.**

***Index Terms*—Cyber-physical Systems, cybersecurity, digital-twin, formal methods**

I. Introduction

The proliferation of autonomous systems, particularly autonomous vehicles, represents one of the most transformative technological advancements of our era. These systems promise to revolutionize transportation, offering increased safety, efficiency, and convenience. However, the complexity and autonomy of these systems also pose significant challenges, especially concerning their robustness and security. Ensuring these systems can withstand and respond appropriately to various attacks and unexpected conditions is crucial for their safe deployment and operation.

II. The methodology

The FORESEEN project addresses the above challenges by implementing a comprehensive methodology that combines formal modelling, simulation, and verification techniques to analyze and detect robustness and security issues of autonomous vehicle systems under attack.

The schematic representation of the FORESSEN methodology, as depicted in Figure 1, comprises five systematic steps that collectively form a robust framework for simulating, analyzing, and verifying the behaviour of autonomous systems:

1) Simulation of an autonomous system of vehicles employing co-simulation and collection of simulation traces in the absence and presence of attacks
2) Generation of formal models for traces in terms of a process algebra language
3) Detection of attacks using model checking technique
4) Identification of trace segments characteristic of attacks that can be used for online monitoring
5) Using abstract interpretation techniques to quantify the robustness of the analysis

The process begins (1) with the modelling and simulation of an autonomous system of vehicles through co-simulation techniques. Co-simulation integrates various simulation tools to create a detailed and comprehensive system model, allowing for observing of its behaviour under different scenarios and conditions. The co-simulation tool chain developed by the INTO-CPS Association[1] is used. It is based on the FMI (Functional Mockup Interface) standard [1] for co-simulation. During this simulation phase, extensive traces of the system's behaviour are collected, which capture crucial data points and interactions within the system. In particular, the system model is instrumented to allow attack injection and the generation of the traces of the system behaviour under attack, following the approach in [2].

In the second step (2), the generation of formal models for each trace is performed using a process algebra language. Process algebra provides a rigorous and structured mathematical framework for describing concurrent systems, making it an ideal tool for modelling the interactions and behaviours observed in the simulation traces [3]. These formal models precisely represent the system's behaviour, facilitating detailed analysis and verification in subsequent steps.

The third (3) step involves the detection of attacks using model-checking techniques. Model checking is a formal verification method that systematically explores the states of a system model to check for the satisfaction of specific properties. By applying model checking to the formal models generated from the simulation traces, potential attacks and

This work 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.

[1]https://into-cps.org

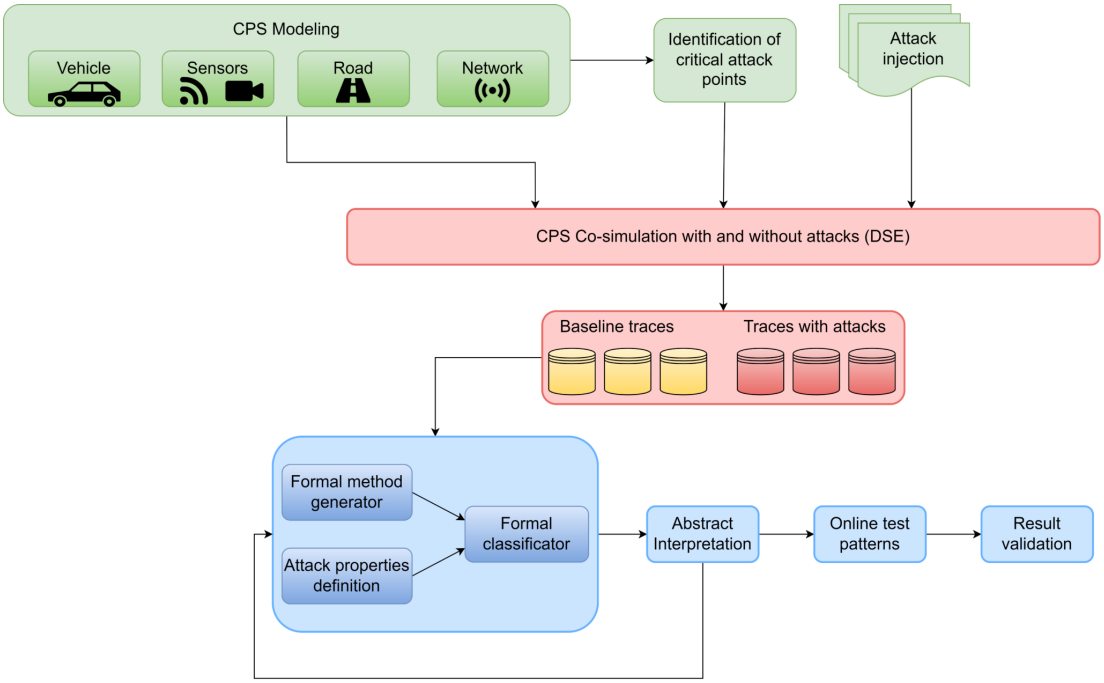

Fig. 1. FORESEEN Project methodology

vulnerabilities within the system can be identified. This step is crucial for ensuring the autonomous system can detect and respond to malicious activities effectively.

Once attacks have been detected, the fourth (4) step focuses on identifying trace segments characteristic of attacks. This involves the representation of traces as process algebra expressions and using temporal logic formulae to identify trace segments that can be used as online monitors.

The fifth (5) and final step of the methodology employs the Abstract Interpretation technique to generalise the results and guarantee the analysis's robustness.

The steps (2) to (5) form the core of the formal methods-based part of the FORESEEN methodology. These steps can be repeated iteratively, refining the models and analysis until the desired level of robustness is achieved.

The proposed framework is evaluated on a platoon of vehicles [4]. Two different communication paradigms, vehicle-to-vehicle (shown in Figure 2) and vehicle-to-edge, are considered. In our case study, each vehicle of the platoon is modeled in *Simulink*[2], with a couple of sub-models: (i) a kinematic model capturing the speed constraints of the car; (ii) a low-pass filter macroscopically modeling the dynamic response of the car. The control law of the platooning system and the network are modelled in C language and Python, respectively.

Different categories of attacks will be analysed:

- attacks exploiting network communications, e.g., attacks that cause communication delays and alteration of the cooperative perception
- attack on-board of a vehicle, e.g., attackers insert fraudulent messages into an automotive bus system.

Fig. 2. Vehicle to Vehicle communications (V2V)

III. Conclusions

By integrating simulation, formal modelling, and verification techniques, the FORESEEN project offers a comprehensive framework for detecting attacks in autonomous vehicle systems augmenting their robustness and security. Additional information can be found on the project website: https://foreseen.dii.unipi.it/

References

[1] T. Blochwitz, M. Otter, et al., "Functional Mockup Interface 2.0: The Standard for Tool independent Exchange of Simulation Models" Proc. of the 9th Intl. Modelica Conference. The Modelica Association, 2012, pp. 173–184, doi: 10.3384/ecp12076173.

[2] C. Bernardeschi, A. Domenici, M. Palmieri "Formalization and co-simulation of attacks on cyber-physical systems," Journal of Computer Virology and Hacking Techniques, 16, 2020, doi: 10.1007/s11416-019-00344-9

[3] C. Bernardeschi, A. Domenici, F. Mercaldo, A. Santone, "Identify Potential Attacks from Simulated Log Analysis," Int. Joint Conf. on Neural Networks, 2020, doi: 10.1109/IJCNN48605.2020.9206825.

[4] M. Palmieri, C. Quadri, A. Fagiolini, C. Bernardeschi. Co-simulated digital twin on the network edge: A vehicle platoon. Computer Communications, vol. 212, pp. 35-47, 2023, doi: 10.1016/j.comcom.2023.09.019

[2]https://it.mathworks.com/products/simulink.html