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

Project FORESEEN

Kickoff meeting

University of Pisa

December 18, 2023

FORESEEN

FORMAL METHODS FOR ATTACK DETECTION IN AUTONOMOUS DRIVING SYSTEMS

Agenda

- Project proposal
- For each research unit, proposed research activity
- Brainstorming on the project objective
- Next steps

PROJECT FORESEEN

Duration:
24 months (30/11/2023 – 30/11/2025,

Project type:
PRIN PNRR
Funding body:
MINISTERO (MUR)
Project identification number:
P2022WYAEW

Research units:
- Università di PISA (RU-PI)
- Università degli Studi del MOLISE (RU-MOL)
- Università degli Studi di MILANO (RU-MI)
- Università degli Studi di PALERMO (RU-PA)

The main objective of the project is the development of a ***formal-method based methodology*** with *supported tools* for the detection of sensor and actuator attacks in autonomous driving systems.
Autonomous driving systems are complex cyber-physical systems (CPS) that rely on connectivity and advanced driver-assistance technologies (Connected Autonomous Vehicles CAV). CAV systems perceive surrounding environment via sensors and actuators.

***The innovative aspect of the project is in the choice of providing a further line of defense in addition to the mechanisms currently adopted in practice or discussed in the literature*.**

While formal methods usually involve expensive computations, our methodology consists in using formal methods to generate simple tests that can be run online on limited resources available in a CAV.

The results of FORESEEN will therefore enable ***on-line monitoring services development***.

The methodology is based on the following steps:

(i) simulation of an autonomous system of vehicles by means of co-simulation and collection of simulation traces;
(ii) generation of formal models for each trace in terms of a process algebra language;
(iii) detection of attacks by means of model checking technique;
(iv) identification of trace segments characteristic of attacks, and of their formal model (as process algebra expressions or temporal logic formulae); and
(v) using Abstract Interpretation techniques to quantify the robustness of the analysis.

To achieve these objectives, a strong cooperation between information technology research units, automation engineering and networking research areas is essential.

The proposed ***framework is evaluated on a platoon of CAVs***. To show the efficacy of the proposed method, two different **communication paradigms, vehicle-to-vehicle and vehicle to edge, is considered with different road surface conditions.**

Technological innovation

Security technologies in the automotive field are mostly aimed at shielding vehicles from external intrusions by providing defensive mechanisms such as message encryption.

The FORESEEN projects will deliver results that could enable a runtime monitor to deploy a “last ditch” defense against intrusions that have penetrated the other mechanisms.

Community reinforcement and dissemination

FORESEEN will produce a platoon simulation case study, **based on well-known modeling tools**, provided with **a clear interactive user interface** that can be used by different users to gain insights on the CAV.
All the FMUs will be openly available on a well-documented **FORESEEN Github** repository, publicly released at the end of the project.

Furthermore, in order to improve the visibility of the **FORESEEN project, a website** will be created to help the scientific community accessing the results of the project.

Moreover, we plan to **organize a workshop, associated to a conference in related fields**, for the dissemination of the results of the project.

Mailing list : Foreseen.dii@listgateway.unipi.it

Website link: FORESEEN.dii.unipi.it
Github link on the website

Hardware resources: Virtual machine for simulation and mode checking tools (FoReLab, dii.unipi.it)

Website development

INTO-CPS co-simulation framework

Bando per assegno ricerca (previsto per gennaio 2024): 30.000 Euro all'anno, rinnovabile

Atto d'obbligo
il Coordinatore scientifico e i Responsabili di Unità di ricerca si impegnano a rispettare i termini, le condizioni, le modalità di attuazione nonché gli obblighi di rendicontazione previsti dal bando e dai suoi allegati, ……

DELIVERABLES and MILESTONES

***Milestone 1**: CPS modelling, identification of critical attack points and attack scenarios*
- *Deliverable D1.1*: Report on the component and system definition of the CPS
- *Deliverable D1.2*: Report on threats analysis and identification of critical physical devices
- *Deliverable D1.3*: Report on attack scenarios and their impact on the sensory and actuation systems

***Milestone 2**: Data set generation without attacks*
- *Deliverable D2.1*: Report on co-simulation framework features and configurable parameters to generate trace dataset

***Milestone 3**: Data set generation with injected attacks*
- *Deliverable D3.1*: Report on how to include and configure attacks in co-simulation architectures

DELIVERABLES and MILESTONES

***Milestone 4**: Formal models generation and robustness analysis*

- *Deliverable D4.1*: Report on the process to build a formal model for vehicular behavior traces and on-line tests generation
- *Deliverable D4.2*: Report on the use of Abstract Interpretation for Robustness assessment

***Milestone 5**: Validation of results*

- *Deliverable D5.1*: Report on the use case and requirement definitions
- *Deliverable D5.2*: Final report on the application of the FORESEEN to the use case

WP0: Project Management and coordination [M: 1-24]
WP leader: RU-PI

WP1: CPS modelling, identification of critical attack points [M: 1-8] *(Milestone 1)*
WP leader: RU-PA

Deliverables

T1.2 CPS modelling [M: 1-6] RU-PI T1.2 will produce D1.1

T1.3 Threats analysis and identification of critical physical devices [M: 3-6] RU-MI T1.3 will produce D1.2

T1.4 Definition of attack scenarios [M: 5-8] RU-PI
T1.4 will produce D1.3

WP2: CPS co-simulation and traces generation [M: 7-12] *(Milestone 2 , Milestone 3)*
WP leader: RU-MI

T2.1 Implementation and testing of CPS model (FMUs) [M: 7-10] RU-MI T2.1 will produce D2.1

T2.3 Implementation and testing of attacks (FMUs) [M: 9-12] RU-MI T2.3 will produce D3.1

Deliverables

WP3: Formal methods for threat identification [M: 9-24] *(Milestone 4, Milestone 5)*
WP leader: RU-MOL

T3.1 Formal model generation [M: 9-20] RU-MOL
T3.1 will produce D4.1

T3.4 Abstract interpretation for robustness analysis [M: 15-20] RU-PI
T3.4 will produce D4.2

T3.7 Validation through co-simulation on use case [M: 21-24] RU-MI
T3.7 will produce D5.1, D5.2

- For each research unit, proposed research activity
- Brainstorming on the project objective
- Next steps