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

Cinzia Bernardeschi, Giuseppe Lettieri, Dario Pagani
Department of Information Engineering
University of Pisa
Pisa, Italy

Christian Quadri
Computer Science Department
University of Milano
Milano, Italy

Adriano Fagiolini
Department of Engineering
University of Palermo
Palermo, Italy

Antonella Santone, Vittoria Nardone
Department of Medicine and Health Sciences Vincenzo Tiberio
University of Molise
Campobasso, Italy

***Abstract*—This work explores model-based attack injection technique to analyse the severity of attacks to a vehicle platoon. Once the model of the cyber-physical system has been generated, we proceed to the identification of the damage scenarios and the threats that can be used to explore vulnerability to affect the vehicle control. Then we design attack scenarios, and run the simulation in case of attacks by exploring different attack parameters. The analysis of collected traces improves our knowledge on the resilience of the system to the attacks and their severity, and allows us to explore countermeasures to improve safety.**

***Index Terms*—Cyber-phisical systems, model-based design, cyber-attacks, co-simulation**

I. Introduction

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. In last years, several researches investigated about the safety and security in automotive networks, for instance, the paper [1] shows that remote exploitation is feasible through a broad range of attack vectors (i.e., mechanical tools, CD players, Bluetooth and cellular radio). Simulation is one of the techniques that are usually applied together with testing in the analysis of systems behaviors. In the case of cyber-physical systems, simulation often takes place in the form of co-simulation, which allows sub-systems, each modeled with its most appropriate languages and tools, to be composed together. The main advantage of co-simulation is modeling flexibility, because it does not require a single modeling language for all system parts (e.g., discrete and continuous parts). The Functional Mockup Interface (FMI) is an emerging standard for co-simulation of cyber-physical systems. Many modeling and simulation tools can export their models as Function Mock-up Units (FMU) that can be run under the supervision of an FMI-based orchestration engine — such as INTO-CPS [2]. This work reports on our research activity aimed to analyze the behavior of a vehicle platoon under attack by employing the open-loop *Design Space Exploration (DSE)* feature of INTO-CPS co-simulation framework. Once the CPS model has been generated, we proceed to the identification of the safety-critical physical devices, namely sensors and actuators, which are directly responsible for the vehicle control. Then we design attack scenarios, and run the co-simulation in case of attacks. The DSE tool is used to vary the attack parameter within a certain domain and to generate and collect simulation traces.

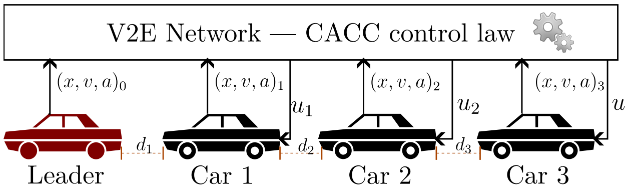


Figure 1: Platoon

II. Simulation and Components

In this work we consider a vehicle platoon, controlled by the Cooperative adaptive cruise control (CACC) [3], running at edge of the network, see Fig. 1. CACC allows cars to react to the car in front of them in their lane by using a mix of sensors and inter-vehicular communication.

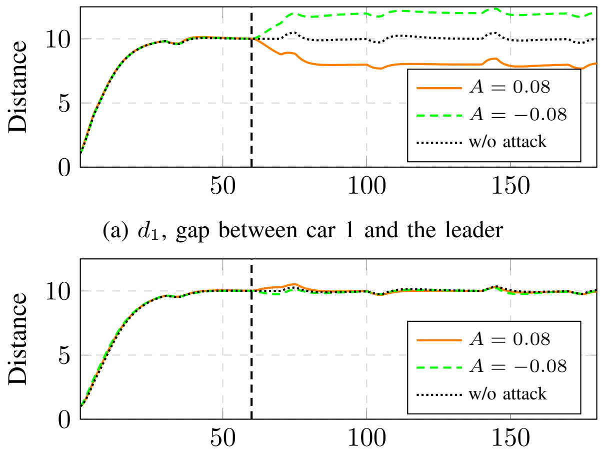
The centralized CACC FMU is implemented in Python [4], it also implements the transmission delays. There's one instance of said FMU, reading data from all the cars and sending back the desired acceleration u_i to the follower cars. The delay is drawn from an exponential distribution with average delay $33\,\mathrm{ms}$.

The vehicle dynamics and attack models are implemented in MATLAB Simulink. Two versions of said FMU are used: one for the leader and one for the followers. The leader FMU generates its own acceleration signal u_0, whereas the follower FMU receives a desired acceleration signal u_i as an input connection, which is then linked to its respective CACC's output during co-simulation.

The simulation is set to run for $180\,\mathrm{s}$, the attack — described in the following section — starts after $60\,\mathrm{s}$ of simulation. All vehicles start from a standstill, spaced $1\,\mathrm{m}$ from each other. The CACC is set to maintain a saftey distance of d_{safe}=10m.

III. Attacks

Two specific attack scenarios are shown in this section. In the first scenario, the **Shift attack**, a constant acceleration term



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

(b) d_2, gap between car 2 and 1

Figure 2: Shift attack, gaps d_1 and d_2 plotted over time

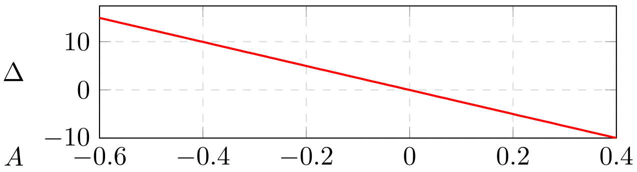


Figure 3: Δ wrt nominal gap at $t = 120$s over A

A is added to the desired acceleration u_1 of vehicle 1, thereby modifying the input applied to the vehicle as

$$\tilde{u}_1 = u_1 + A. \tag{1}$$

In the second scenario, the **Scale attack**, the desired acceleration u_1 of vehicle 1 is scaled by a factor A, resulting in a modified control input given by

$$\tilde{u}_1 = Au_1. \tag{2}$$

IV. Results and Discussion

Let us consider the gap between car 1 and the leader, and the gap between car 2 and car 1; noted as d_1 and d_2 respectively and computed as $d_i = x_{i-1} - x_1 - 4\text{m}$, assuming a vehicle length of 4m.

A. Shift attack

In Fig. 2 we plot the value of the gaps in the nominal case and in case of attack given by (1), considering the case of a positive and a negative value of A. We didn't report the value of d_3 as it follows a similar behavior as d_2.

We can observe how such an attack does not affect the cars behind but only the attacked car. In particular, a value of $A = 0.08$ reduces the gap to the vehicle in front by around two meters; whereas a value of $A = -0.08$ increase the gap by around two meter.

Let us now, given a certain A, consider the error $\Delta = d_1 - d_{\text{safe}}$ made when car 1 is attacked as in (1). The results are shown in Fig. 3. We initially run the simulation within the domain $A \in [-0.6, 0.6]$ discretized with step 0.01. We exclude from further analysis the interval $(0.4, 0.6]$ as car 1 ends up rear-ending the leader. Overall, we can see how negative values of A are non fatal, as the gap between vehicles increases, thus causing an efficiency loss.

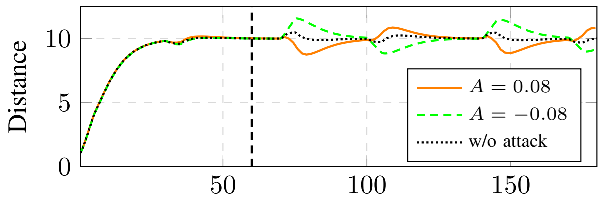


Figure 4: Scale attack, gaps d_1 plotted over time

There is a linear relation between A and Δ. After a linear regression, we can show that for the considered domain the relation between A and Δ is, with $R^2 = 0.996$,

$$\Delta \simeq -25.41 \cdot A - 0.06. \tag{3}$$

B. Scale factor attack

In Fig. 4 we plot d_1 with the attack described by (2). The figure shows that the gap between car 1 and the leader only *scale* by a certain factor without impact on the platoon's safety. For brevity's sake, we omitted d_2, d_3 as they don't show any differences compared to the baseline.

V. Conclusions

This study reports on our research activity on analysis of effects of attacks in cyber-physical systems. Two examples of attacks to a vehicle platoon are shown to demonstrate the effectiveness of model-based co-simulation and statistical analysis in evaluating the resilience of vehicle platoons to actuator-focused cyber-attacks.

Acknowledgment

This study 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) CUP N.P2022WYAEW and from the Italian Ministry of University and Research (MUR) in the framework of the Crosslab and FoReLab projects (Departments of Excellence).

References

[1] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, and T. Kohno, "Comprehensive experimental analyses of automotive attack surfaces," in *SEC'11: Proc. of the 20th USENIX conference on Security*, USENIX Association, 2011.

[2] P. G. Larsen, J. Fitzgerald, J. Woodcock, P. Fritzson, J. Brauer, C. Kleijn, T. Lecomte, M. Pfeil, O. Green, S. Basagiannis, and A. Sadovykh, "Integrated tool chain for model-based design of cyber-physical systems: The into-cps project," in *2nd International Workshop on Modelling, Analysis, and Control of Complex CPS (CPS Data)*, pp. 1–6, 2016.

[3] R. Rajamani, H.-S. Tan, B. K. Law, and W.-B. Zhang, "Demonstration of integrated longitudinal and lateral control for the operation of automated vehicles in platoons," *IEEE Transactions on Control Systems Technology*, vol. 8, no. 4, pp. 695–708, 2000.

[4] M. Palmieri, C. Quadri, A. Fagiolini, and C. Bernardeschi, "Co-simulated digital twin on the network edge: A vehicle platoon," *Computer Communications*, vol. 212, p. 35–47, 2023.