MISSIONE 4
ISTRUZIONE
RICERCA

FORESEEN

Deliverable D1.3 - Report on attack scenarios and their impact on the sensory and actuation systems

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

MISSIONE 4
ISTRUZIONE
RICERCA

FORESEEN

FORmal m**E**thod**S** for attack d**E**t**E**ction in autonomous drivi**N**g systems

PRIN 2022 PNRR

Project number: P2022WYAEW
CUP: I53D23006130001

Deliverable D1.3: **Report on attack scenarios and their impact on the sensory and actuation systems**

Project Start Date: 30/11/2023 **Duration**: 24 months

Coordinator: *University of Pisa*

Deliverable No	D1.3
WP No:	WP1
WP Leader:	RU-PA
Tasks:	T1.4 - Leader: RU-PI
Due date:	M5-8
Delivery date:	July 31, 2024
Authors:	RU-MI, RU-PA, RU-PI

Dissemination Level:

PU	Public	X
PP	Restricted to other program participants (including the Commission Services)	
RE	Restricted to a group specified by the consortium (including the Commission Services)	
CO	Confidential, only for members of the consortium (including the Commission Services)	

Contents

List of Acronyms

CACC Cooperative Adaptive Cruise Control

CAN Controller Area Network

DSRC Dedicated Short-Range Communications

V2V Vehicle to Vehicle

V2N Vehicle to Network

1. Introduction

The objective of this deliverable is the selection of scenarios of attacks to be used in the future for the generation of the data set, which is the input to the attack detection activity based on formal methods.

While some attacks can be reasonably detected with rule-based intrusion detection systems, e.g., doubling the expected frequency of CAN bus messages, is easy to detect, other attacks, e.g. in the cases in which the same interarrival time of packets is maintained as in the absence of attacks, are more challenging to detect.

We assume data alteration cannot be easily detected by error detection tests, such as “reasonableness checks” or “rule-based” checks that state possible commands that can be issued in a current state.

Moreover, we do not consider attacks on the controller because, in this case, the attacker needs full access to the vehicle's software and has complete control of the vehicle.

The platooning system consists of two types of vehicles, the Leader and the Follower, plus the communication network, V2V or V2E communication paradigm.

The control law is distributed on single vehicles. The coordination algorithm (CACC protocol) can be distributed or centralized: in the V2V paradigm, each vehicle has its private view of the platoon; in the V2E paradigm, there is a centralized view of the platoon at the edge.

The following two classes of attacks are assumed in the project:

(1) Internal attack to a vehicle: an attacker impersonates a legitimate Sensor ECU and sends fake packets on the CAN-bus [Rajapaksha 2024] (attack to the leader and attack to a follower)
(2) External attack on the communication network: an attacker injects packets into the network in case of a low packet delivery rate (doubling the expected frequency of the CAN bus is easy to detect).

2. Attack internal to a vehicle

In this scenario, the attacker targets a single vehicle within a platoon, aiming to manipulate its sensory or control systems to disrupt the regular operation of the entire formation. The target vehicle can be any of the platoon's vehicles, whether a leader or a follower. The primary objective is to investigate the cascading effects of such a disruption on the whole platoon, focusing on the implications for system performance, stability, and passenger comfort.

This attack aims to explore vulnerabilities within the connected vehicle platoon system, where vehicles are interlinked through communication and control mechanisms. The attacker seeks to undermine vehicle coordination by attacking just one vehicle, as the control systems are interconnected. This can result in significant disturbances in driving behavior, vehicle spacing, and overall system stability, potentially compromising safety and efficiency.

The impact of the attack varies depending on the position of the targeted vehicle. If the vehicle under attack is the leader, the disruptions can propagate downstream, affecting all subsequent vehicles in the platoon. Conversely, if a non-leader or randomly selected vehicle is targeted, the disruption may be more localized but still influences the vehicles trailing behind. Understanding these dynamics is crucial for developing effective defenses against such attacks.

2.1 Sensor Attacks

In the context of sensor attacks, the attacker can alter sensor readings by injecting a spurious signal, which may consist of, for instance, N sinusoidal waves with precisely chosen frequencies and amplitudes. Once N is determined, the attacker's main objective is to identify the frequencies at which the spurious signal significantly impacts the control system. This can degrade the system's performance and create discomfort throughout the platoon of vehicles.

To address system uncertainties, including the inherent noise in sensor measurements, detecting such an attack would likely rely on preset thresholds. Consequently, another critical goal for the attacker is to minimize the amplitude of the injected signal, thereby reducing its power and making it less detectable. The attacker must decide whether to introduce low-frequency disturbances, such as a bias that subtly alters the system over time, or high-frequency disturbances that resemble random noise and are more difficult to distinguish from the natural sensor noise.

Even without specific information about the role of the targeted vehicle—whether it is a leader or a follower—the attacker can still analyze and evaluate the effects of their attack on vehicles based on their position in the platoon. By examining how disruptions affect vehicles at the front, middle, or rear, the attacker can optimize the overall impact of their strategy, creating widespread instability or discomfort within the platoon.

2.2 Actuator Attacks

In an actuator attack, the attacker can either alter the value of the actuator or introduce delays in the signal. When changing the actuator, the attack might involve adding sinusoidal components to the actuator's output or scaling the value.

For instance, adding sinusoidal components can introduce periodic fluctuations that disrupt the actuator's regular operation, potentially affecting the vehicle's behavior cyclically. Scaling the actuator's value, on the other hand, can systematically adjust the output to deviate from its intended performance, which might lead to more consistent and predictable changes in the vehicle's behavior.

Alternatively, introducing delays in the actuator signal can cause a lag in the vehicle's response, affecting the timing and coordination of its movements. This can create synchronization issues within the platoon, disrupting the overall flow and stability of the vehicle formation

3. External attack using the communication network

This section presents another attack scenario that can be conducted through the communication network. The attack consists of a sophisticated relaying of platoon messages by an external vehicle or entity, which allows the attacker to modify the message content or delay the forwarding to alternate the virtual representation of the platoon. This type of attack can be carried out regardless of whether the communication network is used to coordinate the platoon. The assumptions about the conditions under which the attack is successful strictly depend on the communication network type, but the effects on the platoon are the same. For example, in the case of DSRC (V2V) communication mode, the attacker must be within the radio communication range of the vehicles that are platoon members. On the contrary, if the platoon is coordinated through the cellular network (V2N), the attacker can perform the relaying attack by acting as men-in-the-middle between the vehicles and the edge-computing service.

Following the principle mentioned above of considering data alteration that error detection tests cannot easily detect, we do not consider attacks such as phantom car and radio jamming as they could be easily detected. In

particular, a phantom vehicle can be detected by correlating the onboard distance sensors (Radar/Lidar) and quickly discovering the mismatch. As for the jamming, radio receivers suddenly measure a higher noise level, making radio communication unfeasible.

As the FORESEEN project focuses on detecting data attacks, we assume the attacker has broken the security measures and can alter any data from/to platoon vehicles. In the following, we present the conditions under which this attack is possible and the potential side effects that could be caused to the platoon system. To better show the attack scenario, we describe the attack carried out using the V2V network and the one conducted using V2N separately.

3.1 V2V scenario

As described in Deliverable 1.1, the platooning system coordinated using a V2V communication network is distributed in which each vehicle is responsible for computing the control law using data received from other platoon vehicles. In this scenario, the only messages that could be relayed are those containing the vehicle's status. As mentioned before, the attacker vehicle must be close enough to the platoon vehicles, e.g., on other lanes or in front/on the back, so it is within the communication range of the platoon vehicles.

The attack is conducted as follows. The attacker's vehicle collects messages from the platoon members and performs a data alteration procedure like the one presented in Section 2. This attack exploits two aspects of the DSRC-based platooning:

1) V2V communications could be more reliable due to a noisy radio environment, limited transmission power and uncoordinated medium access, which lead to a high level of packet loss. This problem is considered in the DSRC-based platooning system's design by sending status updates at a higher rate than the one strictly necessary and tolerating high packet error/loss (even higher than 10^{-1}).
2) In many DSRC-based platooning, like the one proposed in [Won 2021], each platoon member relays other members' data to increase system reliability and radio coverage. The latter is significant in the case of long platoons where the messages sent by the platoon leader could fail to reach the last vehicles.

In this setting, the attacker vehicle can operate seamlessly with the other legitimate platoon member and perform subtle data alteration by adjusting the relay rate, i.e., the frequency at which tempered data is injected into the network. Moreover, the attacker can arbitrarily decide which data to alter to make the attack more effective. Finally, differently from the attack on CAN-bus (see Section 2), the legitimate messages cannot be blocked, so platoon members will receive both real and tempered messages, so the attacker strategy should be tailored to radio channel condition, e.g., noise level, packet error/loss, received signal power, and more.

The impact of this type of attack is the alteration of the virtual representation of the platoon, and the effects on the platooning system are analogous to the ones described in Section 2, with the opportunity to alter data of multiple vehicles.

3.2 V2N scenario

The cellular network's platooning system relies entirely on an external controller to obtain acceleration instructions. As mentioned, the attacker can perform the relaying attack by acting as a man-in-the-middle between the vehicles and the edge-computing service.

In this scenario, the attacker is not required to be close to the physical platoon, and in the V2V scenario, the attacker can also alter the instruction messages. As we can see, the characteristics of this attack are similar to those of a CAN-bus attack, with a substantial difference: the attacker can simultaneously modify messages of multiple platoon vehicles. For this reason, the impact on the platoon is analogous to the ones described in Section 2.

4. Roadmap for future work

This deliverable reports on identifying and defining the scenarios of internal attacks on a vehicle and network attacks on vehicles that will be analyzed and applied to the platooning use case in the project's next steps.

5. Bibliography

[Won 2021] Myounggyu Won, "L-Platooning: A Protocol for Managing a Long Platoon With DSRC," in IEEE Transactions on Intelligent Transportation Systems, vol. 23, no. 6, pp. 5777-5790, June 2022, doi: 10.1109/TITS.2021.3057956.

[Rajapaksha 2024] Sampath Rajapaksha, Garikayi Madzudzo, Harsha Kalutarage, Andrei Petrovski, M.Omar Al-Kadri, CAN-MIRGU: A Comprehensive CAN Bus Attack Dataset from Moving Vehicles for Intrusion Detection System Evaluation, In Proc. Symposium on Vehicles Security and Privacy (VehicleSec) 2024, San Diego, CA, USA, 2024, doi:10.14722/vehiclesec.2024.23043