

Optimal-Coupling-Observer AV Motion Control Securing Comfort in the Presence of Cyber Attacks

Tajdari, Farzam; Papaioannou, Georgios; Happee, Riender

DOI

[10.1109/TITS.2025.3629989](https://doi.org/10.1109/TITS.2025.3629989)

Publication date

2026

Document Version

Final published version

Published in

IEEE Transactions on Intelligent Transportation Systems

Citation (APA)

Tajdari, F., Papaioannou, G., & Happee, R. (2026). Optimal-Coupling-Observer AV Motion Control Securing Comfort in the Presence of Cyber Attacks. *IEEE Transactions on Intelligent Transportation Systems*, 27(1), 1426-1441. <https://doi.org/10.1109/TITS.2025.3629989>

Important note

To cite this publication, please use the final published version (if applicable). Please check the document version above.

Copyright

Other than for strictly personal use, it is not permitted to download, forward or distribute the text or part of it, without the consent of the author(s) and/or copyright holder(s), unless the work is under an open content license such as Creative Commons.

Takedown policy

Please contact us and provide details if you believe this document breaches copyrights. We will remove access to the work immediately and investigate your claim.

**Green Open Access added to [TU Delft Institutional Repository](#)
as part of the Taverne amendment.**

More information about this copyright law amendment
can be found at <https://www.openaccess.nl>.

Otherwise as indicated in the copyright section:
the publisher is the copyright holder of this work and the
author uses the Dutch legislation to make this work public.

Optimal-Coupling-Observer AV Motion Control Securing Comfort in the Presence of Cyber Attacks

Farzam Tajdari¹, Georgios Papaioannou², and Riender Happee¹

Abstract—The security of Automated Vehicles (AVs) is an important emerging area of research in traffic safety. Methods have been published and evaluated in experimental vehicles to secure safe AV control in the presence of attacks, but human motion comfort is rarely investigated in such studies. In this paper, we present an innovative optimal-coupling-observer-based framework that rejects the impact of bounded sensor attacks in a network of connected and automated vehicles from safety and comfort point of view. We demonstrate its performance in car following with cooperative adaptive cruise control for platoons with redundant distance and velocity sensors. The error dynamics are formulated as a Linear Time Variant (LTV) system, resulting in complex stability conditions that are investigated using a Linear Matrix Inequality (LMI) approach guaranteeing global asymptotic stability. We prove the capability of the framework to secure occupants' safety and comfort in the presence of bounded attacks. In the onset of attack, the framework rapidly detects attacked sensors and switches to the most reliable observer eliminating attacked sensors, even with modest attack magnitudes. Without our proposed method, severe (but bounded) attacks result in collisions and major discomfort. With our method, attacks had negligible effects on motion comfort evaluated using ISO-2631 Ride Comfort and Motion Sickness indexes. The results pave the path to bring comfort to the forefront of AVs security.

Index Terms—Security of automated vehicle, human motion comfort, platooning vehicles, optimal-coupling-observer, linear matrix inequality.

I. INTRODUCTION

A. Background

IN THE realm of contemporary automotive technology, the advent of Connected and Automated Vehicles (CAVs) has become increasingly pronounced [1], [2], [3]. The distinguishing feature of these CAVs lies in their capacity to accurately sense position and velocity of other vehicles, and exchange information seamlessly, facilitating the formation of platoons

[4], [5], [6], [7]. This collaborative approach enhances their efficiency in traversing distances, potentially elevating road capacity, smoothing traffic flow, curbing fuel consumption, and reducing collision rates. However, there are still great challenges to overcome regarding the two main components of the CAVs before they are part of our daily life. On one hand, methods to design CAV perception and motion control struggle with securing and proving safety. On the other hand, these methods also have to ensure motion comfort, through “smooth” driving styles preventing motion sickness [8], [9]. Securing safety refers to guaranteeing stability of the vehicles facing external factors and avoiding collisions with other vehicles, while motion comfort refers to the experience of occupants and is directly affected by acceleration and deceleration of the vehicle [10] and motion relative to other road users [11], [12].

CAV platoons harness information exchanged through Vehicle-to-Vehicle (V2V) communication and onboard sensors to establish informed decisions and strategically adjust the collective behavior of vehicles. This approach ensures the stable lateral and longitudinal control of the platoon during operation. Lateral formation control [13] pertains to the lateral movement of the vehicles within the platoon, guided by the topological structure, potentially altering the platoon's overall topology. On the other hand, longitudinal formation control [14], [15] focuses on maintaining a safe following distance and velocity between vehicles, swiftly achieving internal and string stability within the platoon. Due to the inherent instability of V2V communication networks, the longitudinal control of CAV platoons encounters numerous challenges from securing safety point of view, since potential cyber attacks can hamper vehicle stability and occupant's perceived safety and motion comfort [16], [17], [18], [19], [20], [21]. Effective cyber-attacks encompass Denial of Service (DoS) [22], [23], False Data Injection (FDI) [24], replay attacks [25], and hybrid cyber-attacks [13], [26]. Among these, FDI attacks, investigated in this paper, are of particular concern to researchers in the context of vehicle platoon systems [24], [27], [28], [29]. FDI attacks represent a prevalent and harmful form of network intrusion, disrupting the decision-making processes of communicated vehicle controllers within the platoon by intercepting and injecting misleading information into the wireless communication channel, often circumventing existing firewalls [30], [31], [32].

Received 30 September 2024; revised 19 April 2025 and 28 July 2025; accepted 19 October 2025. Date of publication 26 November 2025; date of current version 26 December 2025. This work was supported in part by the HiDrive Project under Grant 91561. The Associate Editor for this article was S. Kumari. (Corresponding author: Farzam Tajdari.)

Farzam Tajdari is with the Faculty of Mechanical Engineering, Cognitive Robotics (CoR) Group, Delft University of Technology, 2628 CD Delft, The Netherlands, and also with the Department of Mechanical Engineering, Dynamics and Control (D&C) Group, Eindhoven University of Technology, 5612 AZ Eindhoven, The Netherlands (e-mail: f.tajdari@tudelft.nl).

Georgios Papaioannou and Riender Happee are with the Faculty of Mechanical Engineering, Cognitive Robotics (CoR) Group, Delft University of Technology, 2628 CD Delft, The Netherlands.

Digital Object Identifier 10.1109/TITS.2025.3629989

B. Motivation

In the field of AVs, motion discomfort and in particular Motion Sickness (MS) are considered, together with cybersecurity, as the main inhibitors of AVs adoption and acceptance. In vehicle design, road induced vertical vibrations, also referred to as “ride comfort” have received ample attention leading to advanced suspension systems. However, with the advent of AVs, the interest has shifted towards horizontal accelerations, and more specifically longitudinal acceleration which occurs during accelerating and braking. The reason is that the longitudinal movement of automated vehicles can be influenced by motion planning, allowing the engineers to design controllers that could enhance occupants’ comfort and mitigate motion sickness, as highlighted by Elbanhawi et al. [33]. Thus, longitudinal movement in AVs and platooning vehicles draws substantial attention to potential challenges in securing safety and securing comfort.

Based on the literature, there are multiple research works focusing on platooning or motion planning of AVs focusing on vehicle stability, or occupants’ safety and motion comfort [34], [35], while others propose methods to sort motion planner alternatives based on multiple criteria [36]. However, to the authors’ knowledge, there is no literature exploring AV control under security attacks with consideration of occupant’s motion comfort. In this direction, this paper will explore the nuanced challenges associated with longitudinal formation control in CAV platoons under security attacks by developing a framework that is capable of enhancing occupants’ motion comfort.

Due to the two main components of CAVs, only considering vehicles’ safety requirements, is not sufficient [37] unless occupants’ motion comfort is secured. The traditional approaches that utilized Adaptive Cruise Control (ACC) encounter amplified shock-wave effects due to delay in sensor and actuator systems [38] and therefore, might be likely to cause discomfort. Similarly, any type of attack e.g., replay/delay attack [39], [40] that results in acceleration and deceleration can cause discomfort [41]. In the absence of attack, the safety, namely collision avoidance [42], and comfort, namely jerk control [43] issues in particular in longer platoons have been resolved by communication within platoons through so-called “Cooperative Adaptive Cruise Control (CACC)” [44]. However, the impact of security attacks on occupants’ motion comfort and the ability of the various cybersecurity methods to mitigate it have not yet been studied according to the authors’ knowledge. In the occurrence of significant attacks, vehicle safety is the primary concern, namely from car crashes, but the occupants’ comfort is also at risk [39], [45]. Meanwhile, even if a security method successfully reduces the impacts of the attacks, occupants’ discomfort and motion sickness may be still significantly affected.

Fundamentally, there are two main categories based on the performance of existing cybersecurity methods for platooning vehicles [46]. In the first category, methods target to minimize the impact of attacks to ensure the boundedness of the closed-loop error system [29], [47], [48], [49] rather than completely eliminating the impact. Although safety is secured, there is no guarantee that the remaining minimised attack also ensures occupants’ motion comfort. In the second category, existing

approaches [5], [50], [51], [52], [53] identify the most reliable sensors and only use these for the CAV control, resulting in a switching system. However, the switching between different sensor sets usually excites the dynamic system states, which can also negatively affect the occupants’ comfort.

C. Contributions

Accordingly, there is a lack of methods that secure robustness and safety and can guarantee the stability of the closed-loop system in the presence of bounded FDI attacks, meanwhile rejecting the impact of the attacked sensors to secure the occupants’ comfort. Therefore, we aim to design an optimal-coupling-observer-based framework (synchronizing the observers with the most reliable observer), capable of robustly rejecting the impact of multiple sensor attacks. Our primary focus in this paper centers on securing longitudinal string stability and comfort for a connected homogeneous vehicles platoon in the face of bounded sensor attacks.

The main contributions of our work are:

- Presenting a novel nonlinear observer method detecting and rejecting attacked sensors, enhancing the observability of the dynamic system.
- Analytically deriving the observer parameters using a Linear Matrix Inequality (LMI) approach to achieve global asymptotic stability of the overall estimation error guaranteeing marginal excitation from attacks.
- Assessing the framework’s ability to mitigate occupants’ motion discomfort using ISO-2631 Ride Comfort and Motion sickness indexes, while ensuring safety in car following and platooning for different types of bounded sensor FDI attacks, such as white noise, repeatedly on-off switching white noise, stepwise attacks, and repeatedly on-off switching stepwise attacks.
- Benchmarking the framework against three State-Of-The-Art (SOTA) cybersecurity methods, our method detects and rejects attacks more quickly and more effectively minimises effects of attacks by excluding the attacked sensors resulting in superior safety and comfort.

We present a generic optimal-coupling-observer framework with guaranteed global stability (Section II-C), to secure any linear time-invariant system from sensor attacks. The system can include any finite number of components, e.g., any number of vehicles in platooning. The method includes only constant parameters designed off-line using an LMI approach, allowing real-time implementations. In Section III, we assess our security method for two-vehicle platooning and later for 10-vehicle platooning under various sensor attacks, controlled by an established distributed CACC scheme [54], which fulfills vehicle-following and string stability requirements in the absence of attacks. The CACC scheme is designed for a pair of platooning vehicles with guaranteed stability using the same CACC for any number of vehicles in the platoon. Performance and stability were proven experimentally in a platoon of 6 vehicles in Section VI of [54]. In this paper, we demonstrate string stability, safety and comfort of this CACC under bounded attacks using our attack detection framework.

II. METHODOLOGY

A. Notations

Let the real numbers be denoted by \mathbb{R} ($\mathbb{R}_{>0} = (0, \infty)$), the natural numbers be denoted by \mathbb{N} , the integer numbers be denoted by \mathbb{Z} ($\mathbb{Z}_{\geq 0} = [0, \infty)$), and $\mathbb{R}^{n \times m}$ the set of $n \times m$ matrices with real entries for any $m, n \in \mathbb{N}$. For any vector $v \in \mathbb{R}^n$, we denote $|v| = \sqrt{v^T v}$. For $v(k) \in \mathbb{R}^n$, time interval $k \in \mathbb{Z}_{\geq 0}$, $\|v\|_{\infty} := \sup_{k \geq 0} |v(k)|$. We say that $v(k)$ belongs to l_{∞} , $v(k) \in l_{\infty}$, if $\|v\|_{\infty} < \infty$. Similarly, $\|v(k)\|_p$ is the p -norm of signal $v(k)$.

For a set \mathcal{N} let us denote by $\text{card}[\mathcal{N}]$ the cardinality of the set. $\binom{n}{m}$ denotes the binomial coefficient ‘ n choose m ’. $\exp(\cdot)$ denotes the exponential of its argument. An identity matrix with dimension $n \times n$, is defined as $I_n \in \mathbb{R}^{n \times n}$. $\lambda_A = [\lambda_{A,1}, \dots, \lambda_{A,n}]^T$ is a vector including all the eigenvalues of square matrix $A \in \mathbb{R}^{n \times n}$. The function $\text{floor}[\cdot]$ takes a real number as input and gives the greatest integer less than or equal to the number as output.

B. System Dynamics

In this paper, we focus on platoons of AVs, with longitudinal movement, in which the system dynamics of the platoons of AVs have been studied extensively by other scholars [55], [56], [57], [58]. Accordingly, the majority of the previous studies considered the platooning formation as a Linear Time-Invariant (LTI) system [59], [60], [61], [62]. This system may include two vehicles up to any finite number of vehicles. Thus, to explain our problem, we investigate a generic discrete-time LTI system with a time step T_s , indexed by $k \in \mathbb{Z}_{\geq 0}$, where the time is $t = T_s k$, with p sensors of the form:

$$\begin{cases} x(k+1) = Ax(k) + Bu(k) + w(k), \\ y_i(k) = C_i x(k) + \gamma_i(k) + \delta_i(k), \quad i = 1, \dots, p, \end{cases} \quad (1)$$

with state $x(k) = [x_1(k), \dots, x_n(k)]^T \in \mathbb{R}^n$, known input $u(k) \in \mathbb{R}^m$, system noise $w(k) \in \mathbb{R}^n$ with $\|w(k)\| \leq \mathcal{B}_w$, i -th sensor measurement $y_i(k) \in \mathbb{R}$, sensor noise $\gamma_i(k) \in \mathbb{R}$ with $\|\gamma_i(k)\| \leq \mathcal{B}_{\gamma}$, unknown attack signal $\delta_i(k) \in \mathbb{R}$, and known system matrices of appropriate dimensions (A, B, C_i), $i = 1, \dots, p$. Noise signals, $w(k)$ and $\gamma_i(k)$, are uniformly bounded. If $\delta_i(k) = 0$ then the i -th sensor is attack-free; otherwise, sensor i is under attack, and $\delta_i(k)$ is arbitrary. We assume that there are $q \in \mathbb{N}$ attacks, where $q < p$. The unknown set of attacked sensors is denoted as $\Psi \subset \{1, \dots, p\}$, where $\text{card}[\Psi] = q$.

Problem 1: Consider the system dynamics (1) with state $x(k)$, known system matrices (A, B, C_i), measured input-output trajectories ($u(k), y(k)$), and q sensor attacks $\delta_i(k)$, $i \in G$, $k \in \mathbb{Z}_{\geq 0}$. Design a state estimator $\hat{x}(k)$ of $x(k)$ in which in the presence of bounded attack ($\delta_i, i \in \{1, \dots, p\}$), the estimation error ($e(k) = x(k) - \hat{x}(k)$) becomes globally asymptotically stable for $\gamma_i(k) = 0$, $w(k) = \mathbf{0}$, and uniformly bounded for nonzero $\gamma_i(k)$ and $w(k)$.

C. Generic Optimal-Coupling-Observer Framework

Based on the construction of the sensor measurements (y_i), we design a framework including $N \in \mathbb{N}$ number of coupled

nonlinear observers for the system in (1) as

$$\begin{cases} \hat{x}_{J_j}(k+1) = A\hat{x}_{J_j}(k) + Bu(k) + L_{J_j}(y_{J_j}(k) - C_{J_j}\hat{x}_{J_j}(k)) \\ \quad + (1 - \beta_{J_j}(k))D(\hat{x}(k) - \hat{x}_{J_j}(k)), \\ r_{J_j}(k) = y_{J_j}(k) - C_{J_j}\hat{x}_{J_j}(k), \end{cases} \quad (2)$$

where $J_j \in J$, $\text{card}[J] = N$, and J denotes the set that contains designed subsets of sensors. $y_{J_j}(k) \in \mathbb{R}^{\text{card}[J_j]}$, $\hat{x}_{J_j}(k) \in \mathbb{R}^n$ is the observer state, and $r_{J_j}(k) \in \mathbb{R}^{\text{card}[J_j]}$ is a vector including the residuals of the observer. Diagonal matrix $D \in \mathbb{R}^{n \times n}$ is a weighting matrix instructed based on the eigenvalues of A . Nonlinear time-varying parameter $\beta_{J_j}(k) \in \mathbb{R}_{>0}$ is the classification ratio capturing the performance of each observer based on $r_{J_j}(k)$. The term $(1 - \beta_{J_j}(k))D(\hat{x}(k) - \hat{x}_{J_j}(k))$ couples the observer J_j with the most reliable output ($\hat{x} \in \mathbb{R}^n$) belonging to the observer with the maximum classification ratio. The matrix $L_{J_j} \in \mathbb{R}^{n \times \text{card}[J_j]}$ is the observer gain, and $C_{J_j} \in \mathbb{R}^{\text{card}[J_j] \times n}$ depends on the construction of sensors subsets.

Remark 1: The logic behind formulating the observer with the nonlinear time-varying term $(1 - \beta_{J_j}(k))D(\hat{x}(k) - \hat{x}_{J_j}(k))$ in (2) is to smoothly increase the excitability of the system in the presence of attack(s). To show the importance of embedding the term, we assume (2) without the nonlinear term, define the observer error as $e_{J_j}(k) = x(k) - \hat{x}_{J_j}(k)$, and introduce a perturbed version of the error dynamics, following from (1), (2), as

$$\begin{aligned} e_{J_j}(k+1) &= (A - L_{J_j}C_{J_j})e_{J_j}(k) \\ &\quad - L_{J_j}(\gamma_{J_j}(k) + \delta_{J_j}(k)) + w(k), \end{aligned} \quad (3)$$

in which $(A - L_{J_j}C_{J_j})$ is stable (Schur stable), $\gamma_{J_j}(k) \in \mathbb{R}^{\text{card}[J_j]}$ includes all γ_i , $i \in J_j$, and $\delta_{J_j}(k) \in \mathbb{R}^{\text{card}[J_j]}$ includes all δ_i , $i \in J_j$. For simplification let $\gamma_i(k) = 0$, $w(k) = \mathbf{0}$, for any $\delta_{J_j}(k)$ that results in error convergence, namely $e_{J_j}(k+1) = e_{J_j}(k)$, from (3), we have

$$e_{J_j}(k) = (A - I_n - L_{J_j}C_{J_j})^{-1}L_{J_j}\delta_{J_j}(k). \quad (4)$$

From (2), (4) and knowing $y_{J_j}(k) = C_{J_j}x(k) + \delta_{J_j}(k)$, the residual of the observer would be

$$\begin{aligned} r_{J_j}(k) &= C_{J_j}x(k) + \delta_{J_j}(k) - C_{J_j}\hat{x}_{J_j}(k), \\ &= C_{J_j}e_{J_j}(k) + \delta_{J_j}(k), \\ &= (C_{J_j}(A - I_n - L_{J_j}C_{J_j})^{-1}L_{J_j} + I_{\text{card}[J_j]})\delta_{J_j}(k). \end{aligned} \quad (5)$$

We assume $A_{r_{J_j}} = C_{J_j}(A - L_{J_j}C_{J_j} - I_n)^{-1}L_{J_j} + I_{\text{card}[J_j]}$. For any eigenvalues of A equal to one ($\lambda_{A,g} = 1$ corresponding to $x_g(k) \in x(k)$) and the y_i that is measuring fully or partly the x_g , the columns of $A_{r_{J_j}}$ have only zero entries corresponding to $i \in J_j$. This is because the I_n in $A - I_n$ bans the excitation of r_{J_j} by the attacks on the sensors measure the states corresponding to $\lambda_{A,g} = 1$, known as Excitability Problem (EP). This means that the residual r_{J_j} is independent of the sensor measurements y_i , and will not change if y_i is under attack. To this end, we design the diagonal matrix $D = \text{diag}(D_1, \dots, D_n)$ in (2) such that only the entries corresponded to $\lambda_{A,g} = 1$ are equal to 1 and the rest of entries on the diagonal of D are zero, i.e.,

$$D_z = \begin{cases} 1 & \text{if } \lambda_{A,g} = 1, \text{ and } z = g, \\ 0 & \text{otherwise,} \end{cases} \quad , z \in \{1, \dots, n\}. \quad (6)$$

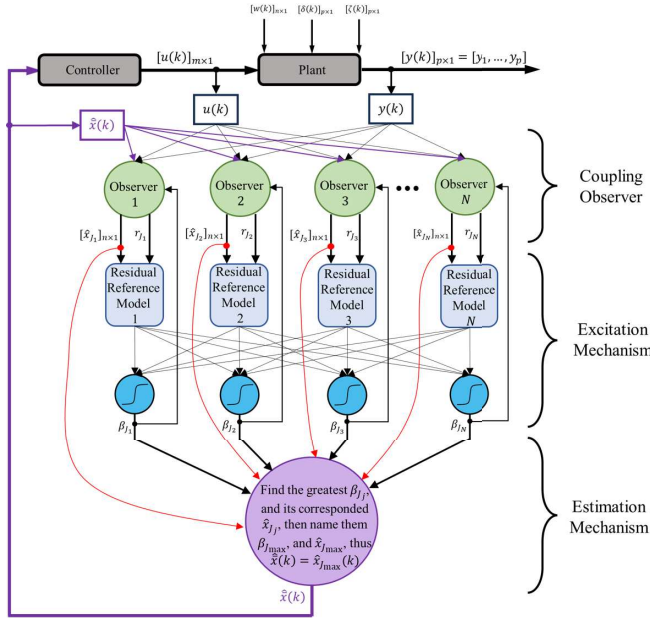


Fig. 1. The optimal-coupling-observer network scheme.

Thus, embedding a nonzero $\beta_{J_j} \in (0, 1)$, and the matrix D in (6) guarantees the excitability of r_{J_j} by any type of bounded attacks where D shifts those $\lambda_{A,g} = 1$ from 1 towards zero to solve the excitability problem.

Example 1: To illustrate Remark 1, we assume a simple system with no extended-term where $A = 1$, thus $n = 1$, $\text{card}[J_j] = 1$, $L_{J_j} \in \mathbb{R}_{\neq 0}$, and $C_{J_j} = 1$. From (5), the residual of the observer under error convergence would be

$$\begin{aligned} r_{J_j}(k) &= (C_{J_j}(1 - L_{J_j}C_{J_j} - 1)^{-1}L_{J_j} + 1)\delta_{J_j}(k), \\ &= (-L_{J_j}^{-1}L_{J_j} + 1)\delta_{J_j}(k), \\ &= 0. \end{aligned} \quad (7)$$

From (7) it is shown that when the error of the observer is converging, the residuals of some observers have the EP, are converging to zero and independent of the attacks (δ_{J_j}) and the observer gains L_{J_j} , which means that the r_{J_j} is not excitable. However, if there exist the term $(1 - \beta_{J_j}(k))D(\hat{x}(k) - \hat{x}_{J_j}(k))$ in (2) with $\beta_{J_j} \neq 1$ for the compromised observers, the impact of I_n in $A - I_n$ will be degraded and thus $r_{J_j} \neq 0$ for any $\delta_{J_j} \neq 0$.

To practically use the suggested observer, the framework relies on designing three major components: 1) Sensor set design, 2) Excitation mechanism, and 3) Estimation mechanism. As shown in Fig. 1, all these components together form the framework that secures the system from sensor attacks. We describe each component in the sequel.

1) *Sensor Set Design:* let J , $\text{card}[J] = N$, $N \in \mathbb{N}$, contain all the detectable subsets of sensors where for any $J_\rho, J_j \in J$, $\rho, j \in \{1, \dots, N\}$, $j \neq \rho$, and $\text{card}[J_\rho] \leq \text{card}[J_j]$, we have $J_\rho \not\subseteq J_j$. Then we call J_ρ and J_j independent. As stated in [63], chapter 5, the reason to skip all the dependent subsets is that any impact on the independent subset appears in the dependent subset, thus considering them only makes the computations expensive. In addition, by minimizing the $\text{card}[J_j]$ we increase the freedom for the variation of the number of tolerable attacks

(q), as we know from [63] that,

$$\text{card}[J_j] \leq q < \frac{p}{2}. \quad (8)$$

Apparently, for any subset of sensors $J_j \in J$, the $C_{J_j} \in \mathbb{R}^{\text{card}[J_j] \times n}$ that results from stacking the rows of C corresponding to y_i , $i \in J_j$, leads to a detectable pair (A, C_{J_j}) .

Example 2: Assume having a system as follows:

$$\begin{aligned} x_1(k+1) &= x_2(k) + u_1(k), \\ x_2(k+1) &= x_1(k) - x_2(k), \end{aligned} \quad (9)$$

with $p = 4$ sensors

$$\begin{aligned} y_i &= x_1 + \delta_i, \text{ and } C_i = [1 \ 0], \text{ for } i \in \{1, 2\}, \\ y_i &= x_2 + \delta_i, \text{ and } C_i = [0 \ 1], \text{ for } i \in \{3, 4\}. \end{aligned} \quad (10)$$

First, note that this system is observable in the usual sense considering $A = \begin{bmatrix} 0 & 1 \\ 1 & -1 \end{bmatrix}$. Accordingly, the number of all

possible sensor combinations is $\sum_{s=1}^4 \binom{4}{s} = 15$. By checking Hautus lemma [64] for detectability check for each subset, we find out that all 15 subsets are detectable. Considering the detectable set $\Phi = \{\Phi_1, \dots, \Phi_{15}\}$, where $\Phi_1 = \{1\}$, $\Phi_2 = \{2\}$, $\Phi_3 = \{3\}$, $\Phi_4 = \{4\}$, $\Phi_5 = \{1, 2\}$, $\Phi_6 = \{1, 3\}$, $\Phi_7 = \{1, 4\}$, $\Phi_8 = \{2, 3\}$, $\Phi_9 = \{2, 4\}$, $\Phi_{10} = \{3, 4\}$, $\Phi_{11} = \{1, 2, 3\}$, $\Phi_{12} = \{1, 2, 4\}$, $\Phi_{13} = \{1, 3, 4\}$, $\Phi_{14} = \{2, 3, 4\}$, and $\Phi_{15} = \{1, 2, 3, 4\}$. As, J should contain the independent subsets of Φ , thus $J = \{\Phi_1, \Phi_2, \Phi_3, \Phi_4\}$, $\text{card}[J] = 4$. Accordingly, $J_1 = \Phi_1$, $J_2 = \Phi_2$, $J_3 = \Phi_3$, and $J_4 = \Phi_4$, and $\text{card}[J_j] = 1$, $j \in \{1, \dots, 4\}$, thus from (8), the system is one attack tolerable ($q = 1$).

2) *Excitation Mechanism:* Using the N observers, our purpose is to classify the observers based on their degree of vulnerability against accrued attacks. In the best-case scenario, the criterion used to evaluate the performance of each observer would depend on the observer error $e_{J_j}(k) = x(k) - \hat{x}_{J_j}(k)$ for $J_j \in J$. However, the state $x(k)$ is unknown which makes $e_{J_j}(k)$ become unknown, and any performance criterion involving $e_{J_j}(k)$ would not be implementable. As a result and similarly to other works e.g., [65], [66], [67], we use the knowledge from the sensors sets $y_{J_j}(k)$, and the corresponding observer states $\hat{x}_{J_j}(k)$ with $j \in \{1, \dots, N\}$. The excitation mechanism includes the following components:

a) *Residual Reference Model:* we introduce a residual reference model (η_{J_j}) excited by the residual of each observer employing the well-known mass-spring-damper model [68] with mass value 1, which is a two-state system with globally asymptotically stable dynamics around $|r_{J_j}|$ as follows.

$$x_{r_{J_j}}(k+1) = A_r x_{r_{J_j}}(k) + B_r |r_{J_j}(k)|, \quad (11)$$

where

$$\begin{cases} A_r = \exp(A_r^c T_s), B_r = \int_0^{T_s} \exp(A_r^c(T_s - s)) B_r^c ds, \\ A_r^c = \begin{bmatrix} 0 & 1 \\ -K_r & -C_r \end{bmatrix}, B_r^c = \begin{bmatrix} 0 \\ K_r \end{bmatrix}, \end{cases} \quad (12)$$

$x_{r_{J_j}} := [x_{r_{J_j}}^{1,1} \ x_{r_{J_j}}^{2,1}]^\top$ and $\eta_{J_j}(k) = x_{r_{J_j}}^{1,1}(k)$. The system is globally asymptotically stable if all the eigenvalues of A_r^c are negative and the pair (A_r^c, B_r^c) is stabilisable (see, e.g., [69]).

b) *Classification Ratio*: To give a logical comparison between the observers, we design a classifier term $\beta_{J_j}^n(k) \in \mathbb{R}$, $\beta_{J_j}^n(k) \in (0, 1)$ with $J_j \in J$ for each of the observers which is dependant to all the $\eta_{J_j}(k) J_j \in J$, that contains higher values for reliable sets comparing to the compromised sets (see Remark 2). To this end, we design the classifier term for the j^{th} observer as below:

$$\beta_{J_j}^n(k) = 1 - \frac{\eta_{J_j}(k) + \mathcal{B}_w + \mathcal{B}_\gamma}{\sum_{s=1}^N (\eta_{J_s}(k) + \mathcal{B}_w + \mathcal{B}_\gamma)}, \quad \beta_{J_j}(0) \in (0, 1). \quad (13)$$

According to (13), we define $\bar{\beta}^n = 1 - \frac{1}{N}$ as the classifier term value for the safe condition where $q = 0$ and thus η_{J_j} converges to zero for any $J_j \in J$.

Remark 2: If $J_j \cap \Psi = \emptyset$, and $\Psi \neq \emptyset$, subset $J_j \in J$ is a reliable set and the corresponding η_{J_j} convergence to 0, and β_{J_j} converges to 1; otherwise, J_j is a compromised subset and consequently $\eta_{J_j} \leq \bar{\eta}_{J_j}$ for some non-negative constant $\bar{\eta}_{J_j}$.

Although the introduced classifier term in (13) offers a higher value close to 1 for the reliable set(s), the term is least likely to offer a value close to 0, especially when $q \geq 2$. To make the mechanism more sensitive to reliable and compromised sets, we use the following activation function to design the classification ratio.

$$\beta_{J_j}(k) = \frac{1}{\pi} \arctan \left((\beta_{J_j}^n(k) - \bar{\beta}^n) a_\beta \right) + 0.5, \quad (14)$$

where, $\beta_{J_j}(k) \in \mathbb{R}$, $\beta_{J_j}(k) \in (0, 1)$ is the classification ratio, and a_β is the magnifier parameter which regulates the sensitivity of the classification ratio to attacks. Accordingly, if $q = 0$ ($\Psi = \emptyset$), then $\beta_{J_j}^n(k) = \bar{\beta}^n$, and thus $\beta_{J_j}(k) = 0.5$.

3) *Estimation Mechanism*: Given the N observers' outputs, and the N classification ratios, we present an estimation mechanism that estimates the unknown state $x(k)$, such that

$$\hat{x}(k) = \hat{x}_{J_j}(k), \quad \beta_{J_j}(k) = \beta_{J_{\max}}(k), \quad (15)$$

where the estimated state $\hat{x}(k) \in \mathbb{R}^n$, $\beta_{J_{\max}}(k)$ is the maximum of all the $\beta_{J_j}(k)$, and $\hat{x}_{J_j}(k)$ belongs to the observer with the classification ratios value equal to the best achievable $\beta_{J_{\max}}(k)$ which is supposed to be the most reliable observer. In the case that there are several observers with reliable sets, i.e., several $\beta_{J_j}(k)$ are equal to $\beta_{J_{\max}}(k)$, we determine $\hat{x}(k)$ equal to the reliable observer that has the lowest j .

D. Stability Discussion

1) *Error Dynamics System*: We define the estimation error using (1), and (15) as follows

$$e(k) = x(k) - \hat{x}(k), \quad (16)$$

$$e(k+1) = (A - L_{J_{\max}}(k)C_{J_{\max}}(k))e(k) - L_{J_{\max}}(k)(\gamma_{J_{\max}}(k) + \delta_{J_{\max}}(k)) + w(k). \quad (17)$$

We also define the observer error dynamics following from (1) and (2), and knowing $-(1 - \beta_{J_j}(k))D(\hat{x}(k) - \hat{x}_{J_j}(k)) = (1 - \beta_{J_j}(k))De(k) - (1 - \beta_{J_j}(k))De_{J_j}(k)$, as

$$e_{J_j}(k+1) = (A - (1 - \beta_{J_j}(k))D - L_{J_j}C_{J_j})e_{J_j}(k) - L_{J_j}(\gamma_{J_j}(k) + \delta_{J_j}(k)) + w(k) + (1 - \beta_{J_j}(k))De(k). \quad (18)$$

Considering (17) and (18), the overall error system dynamics for the observers J_j and the estimation error is derived as follows

$$\begin{aligned} E_{J_j}(k+1) &= \mathbb{A}_{J_j}(k)E_{J_j}(k) - \mathbb{L}_{J_j}(\Gamma_{J_j}(k) + \Delta_{J_j}(k)) + W(k), \\ E_{J_j}(k) &= \begin{bmatrix} e_{J_j}(k) \\ e(k) \end{bmatrix}, \Gamma_{J_j}(k) = \begin{bmatrix} \gamma_{J_j}(k) \\ \gamma_{J_{\max}}(k) \end{bmatrix}, \Delta_{J_j}(k) = \begin{bmatrix} \delta_{J_j}(k) \\ \delta_{J_{\max}}(k) \end{bmatrix}, \\ \mathbb{A}_{J_j}(k) &= \begin{bmatrix} A - (1 - \beta_{J_j}(k))D - L_{J_j}C_{J_j} & (1 - \beta_{J_j}(k))D \\ 0 & A - L_{J_{\max}}(k)C_{J_{\max}}(k) \end{bmatrix}, \\ \mathbb{L}_{J_j}(k) &= \begin{bmatrix} L_{J_j} & 0 \\ 0 & L_{J_{\max}}(k) \end{bmatrix}, W(k) = \begin{bmatrix} w(k) \\ w(k) \end{bmatrix}, \end{aligned} \quad (19)$$

where $E_{J_j}(k) \in \mathbb{R}^{2n}$, $\Gamma_{J_j}(k) \in \mathbb{R}^{\text{card}[J_j] + \text{card}[J_{\max}]}$, $\Delta_{J_j}(k) \in \mathbb{R}^{\text{card}[J_j] + \text{card}[J_{\max}]}$, $W(k) \in \mathbb{R}^{2n}$, and $\mathbb{L}_{J_j} \in \mathbb{R}^{2n \times (\text{card}[J_j] + \text{card}[J_{\max}])}$.

2) *Stability Discussion and Parameters Design*: Regarding the error dynamics system explained in (19), here, the purpose is to design matrices L_{J_j} such that the complete error dynamic system (19) becomes asymptotically stable in the absence of attack and noise. Due to the construction of matrix \mathbb{A}_{J_j} which is an upper triangle matrix in (19), complete error dynamic after k time intervals in the absence of attack, and noise ($\Gamma_{J_j} = \mathbf{0}$, $\Delta_{J_j} = \mathbf{0}$, $W = \mathbf{0}$) is

$$E_{J_j}(k+1) = \left(\prod_{\iota=0}^k \mathbb{A}_{J_j}(\iota) \right) E_{J_j}(0), \quad (20)$$

where

$$\begin{aligned} \prod_{\iota=0}^k \mathbb{A}_{J_j}(\iota) &= \begin{bmatrix} \mathbb{A}_{1,1}^\Pi(k) & \star \\ \mathbf{0} & \mathbb{A}_{2,2}^\Pi(k) \end{bmatrix}, \\ \mathbb{A}_{1,1}^\Pi(k) &= \prod_{\iota=0}^k A - (1 - \beta_{J_j}(\iota))D - L_{J_j}C_{J_j}, \\ \mathbb{A}_{2,2}^\Pi(k) &= \prod_{\iota=0}^k A - L_{J_{\max}}(\iota)C_{J_{\max}}(\iota). \end{aligned} \quad (21)$$

As $\prod_{\iota=0}^k \mathbb{A}_{J_j}(\iota)$ is an upper triangle matrix, the complete error system is asymptotically stable if and only if the matrices on the diagonal of $\prod_{\iota=0}^k \mathbb{A}_{J_j}(\iota)$ converges to 0 when $k \rightarrow \infty$. To satisfy this condition, we will design L_{J_j} by using the LMI method.

Remark 3: In (21), there are two time-varying matrices on the diagonal of $\prod_{\iota=0}^k \mathbb{A}_{J_j}(\iota)$ as $\mathbb{A}_{1,1}^\Pi(k)$ and $\mathbb{A}_{2,2}^\Pi(k)$. Note that $\mathbb{A}_{1,1}^\Pi(k)$ is a stronger time-varying matrix than $\mathbb{A}_{2,2}^\Pi(k)$ as it includes a time-varying component of β_{J_j} , and asymptotic stability of $\mathbb{A}_{1,1}^\Pi(k)$ results in the asymptotic stability of $\mathbb{A}_{2,2}^\Pi(k)$ as $\mathbb{A}_{2,2}^\Pi(k)$ is equal to $\mathbb{A}_{1,1}^\Pi(k)$ when $\beta_{J_j}(k) = 1$. Thus, designing L_{J_j} for asymptotic stability of $\mathbb{A}_{1,1}^\Pi(k)$ for the extreme conditions of β_{J_j} (0 and 1) is enough to guarantee the asymptotic stability of the complete error system in (20).

First, we explain the inequalities in the form of discrete Lyapunov functions that can be reformulated as an LMI problem using the Schur complement approach [70]. Regarding Remark 3, the equivalent inequality to be solved by the LMI method for the condition that $\beta_{J_j} = 1$ is:

$$(A - L_{J_j}C_{J_j})^\top P(A - L_{J_j}C_{J_j}) - P < 0, \quad J_j \in J, \quad (22)$$

where $P \in \mathbb{R}_{>0}^{n \times n}$ is a positive definite matrix. Similarly, the equivalent inequality to be solved by the LMI method for the condition that $\beta_{J_j} = 0$ is:

$$(A - D - L_{J_j} C_{J_j})^\top P (A - D - L_{J_j} C_{J_j}) - P < 0, \quad J_j \in J. \quad (23)$$

Accordingly, the LMI problem includes $2N$ inequalities in (22)–(23), and one inequality for $P > 0$ that should be satisfied by designing a unique P and proper L_{J_j} with $j \in \{1, \dots, N\}$.

Using the Schur complement method [70], the N inequalities in (22) can be turned into an equivalent LMI problem as

$$\begin{bmatrix} -P & P^\top A - Z_{J_j}^\top C_{J_j} \\ A^\top P - C_{J_j}^\top Z_{J_j} & -P \end{bmatrix} < 0, \quad (24)$$

the extra N inequalities in (23) can be turned into an equivalent LMI problem as

$$\begin{bmatrix} -P & P^\top (A - D) - Z_{J_j}^\top C_{J_j} \\ (A - D)^\top P - C_{J_j}^\top Z_{J_j} & -P \end{bmatrix} < 0, \quad (25)$$

while,

$$P > 0. \quad (26)$$

We solved all the $2N + 1$ inequalities in (24)–(26) to find P , and Z_{J_j} , $J_j \in J$, where

$$L_{J_j} = (Z_{J_j} P^{-1})^\top. \quad (27)$$

Remark 4: The LMI problem including the $2N + 1$ inequalities in (24)–(26) is solved off-line, and thus the value of N and solving time have no impact on the real-time implementation of the method in practice.

Remark 5: The LMI problem including the $2N + 1$ inequalities in (24)–(26) should have a unique solution as long as each pair (A, C_{J_j}) , and $(A - D, C_{J_j})$ is detectable. The reason is that the detectability of each pair (A, C_{J_j}) defines the feasibility of (24), and the detectability of each pair $(A - D, C_{J_j})$ defines the feasibility of (25). Due to the instruction of D in (6), pair $(A - D, C_{J_j})$ gives equal detectability to pair (A, C_{J_j}) (if none of the eigenvalues of A is equal to 1) or stronger detectability than (A, C_{J_j}) (if at least one of the eigenvalues of A is equal to 1). And as C_{J_j} is designed to guarantee detectability of pair (A, C_{J_j}) , thus $(A - D, C_{J_j})$ should be detectable in general sense. Note that matrix D does not make the matrix $A - D$ Schur stable, and it only improves the detectability of pair $(A - D, C_{J_j})$ compared to pair (A, C_{J_j}) .

III. SIMULATION SETUP

A. Vehicle Platooning Model

Similar to [71], we consider a string of $M \in \mathbb{N}$ platooning vehicles, schematically depicted in Fig. 2, with d_l being the distance between vehicle l and its preceding vehicle $l - 1$, and v_l the velocity of vehicle l .

The main objective of each vehicle is to follow its preceding (lead) vehicle at a desired distance $d_{r,l}$. Here, a constant time headway spacing policy is adopted, formulated as

$$d_{r,l}(t) = s_l + h v_l(t), \quad l \in S_M, \quad (28)$$

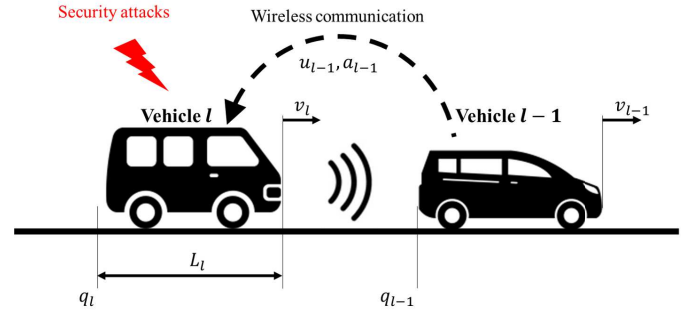


Fig. 2. CACC-equipped vehicles.

where $h > 0$ is the so-called time headway, s_l is the standstill distance, and $S_M := \{l \in \mathbb{N} | l \leq M\}$. This spacing policy is known to improve string stability [38], [72], [73]. A homogeneous string is assumed, which is why the time headway h is taken independently of l . The spacing error $e_l(t)$ is thus defined as

$$\begin{aligned} e_l(t) &= d_l(t) - d_{r,l}(t), \\ &= (q_{l-1}(t) - q_l(t) - \mathcal{L}_l) - (s_l + h v_l(t)), \end{aligned} \quad (29)$$

with $q_l(t)$ is the position of vehicle l and \mathcal{L}_l is its length, and $d_l(t) = q_{l-1}(t) - q_l(t) - \mathcal{L}_l$ is the distance between the vehicle l and its preceding vehicle $l - 1$. As a basis for control design, the following vehicle model is adopted from [54]

$$\begin{bmatrix} \dot{d}_l(t) \\ \dot{v}_l(t) \\ \dot{a}_l(t) \end{bmatrix} = \begin{bmatrix} v_{l-1}(t) - v_l(t) \\ a_l(t) \\ -\frac{1}{\tau} a_l(t) + \frac{1}{\tau} u_l(t) \end{bmatrix}, \quad l \in S_M, \quad (30)$$

where τ is a time constant modelling driveline dynamics (namely, $\tau = 0.1$ s in [54]), a_l denotes the acceleration of vehicle l , and $u_l(t)$ is its desired acceleration (the control input).

B. Vehicle Platooning Control

To enforce the platooning behavior (by designing controller u_l in (30)), we exactly adopt the distributed CACC scheme introduced in [54], which fulfills the vehicle-following objective and string stability requirement in the absence of attacks [54]. This controller $u_l(t)$ is dynamic and can be written as follows:

$$\begin{cases} \dot{\xi}_l(t) = k_p e_l(t) + k_d \dot{e}_l(t) + k_{dd} \ddot{e}_l(t) + u_{l-1}(t), \\ \dot{u}_l(t) = -\frac{1}{h} u_l(t) + \frac{1}{h} \xi_l(t), \end{cases} \quad (31)$$

where $l \in S_m$, $\xi_l \in \mathbb{R}$ is the controller state and constants $k_p \in \mathbb{R}$, $k_d \in \mathbb{R}$, and $k_{dd} \in \mathbb{R}$ are the control gains, i.e., to have asymptotic stability according to [54] it is sufficient if $k_p, k_d > 0$, $k_{dd} > -1$ and $(1 + k_{dd})k_d > \tau k_p$. The feedforward term u_{l-1} is the desired acceleration of the preceding vehicle obtained through wireless communication.

C. Communication and Sensing Topology

We adopt a decentralized communication topology, where vehicles are interconnected by a set of wireless communication

links that allow each vehicle $l-1$ (lead vehicle) to send its acceleration to vehicle l (following vehicle). For control and monitoring purposes, we further use sensor data coming from onboard sensors (e.g., radar, LiDAR, cameras, sensing distance and relative velocity to the lead vehicle). Please note that, as indicated in (32), when measuring the same variables with different sensors, we utilize three sensors for the distance ($d_l(t)$), specifically $y_1(t)$, $y_6(t)$, and $y_8(t)$, as well as three sensors for velocity, namely $y_2(t)$, $y_7(t)$, and $y_9(t)$. Without loss of generality, we assume that available sensors for vehicle l are:

Variable	Related sensor measures the variable
$d_l(t)$	$y_1(t) = q_{l-1}(t) - q_l(t) - \mathcal{L}_l + \gamma_1(t) + \delta_1(t)$, (32a)
$v_l(t)$	$y_2(t) = v_l(t) + \gamma_2(t) + \delta_2(t)$, (32b)
$a_l(t)$	$y_3(t) = a_l(t) + \gamma_3(t) + \delta_3(t)$, (32c)
$\Delta v_l(t)$	$y_4(t) = v_{l-1}(t) - v_l(t) + \gamma_4(t) + \delta_4(t)$, (32d)
$a_{l-1}(t)$	$y_5(t) = a_{l-1}(t) + \gamma_5(t) + \delta_5(t)$, (32e)
$d_l(t)$	$y_6(t) = q_{l-1}(t) - q_l(t) - \mathcal{L}_l + \gamma_6(t) + \delta_6(t)$, (32f)
$v_l(t)$	$y_7(t) = v_l(t) + \gamma_7(t) + \delta_7(t)$, (32g)
$d_l(t)$	$y_8(t) = q_{l-1}(t) - q_l(t) - \mathcal{L}_l + \gamma_8(t) + \delta_8(t)$, (32h)
$v_l(t)$	$y_9(t) = v_l(t) + \gamma_9(t) + \delta_9(t)$, (32i)

where $y_s(t)$ denotes sensor measurements, $\delta_s(t)$ models potential FDI attacks that tamper with hardware, networks, and computers, and $\gamma_s(t)$ denotes reliable (normal) sensor noise with $s \in \{1, \dots, 9\}$. In addition, Δv_l defines the relative velocity between vehicle l and its preceding vehicle (vehicle $l-1$). Note that sensors $y_1(t)$, $y_6(t)$, $y_8(t)$ and $y_4(t)$ provide relative tracking and relative velocity information, and sensors $y_2(t)$, $y_7(t)$, $y_9(t)$ and $y_3(t)$ model onboard measured velocity and acceleration. In addition, $y_5(t)$ models acceleration data received wirelessly from the lead vehicle. Moreover, we know from (32) that $\dot{e}(t) = v_{l-1}(t) - v_l(t) - h a_l(t)$ measurable by y_4 and y_3 . Similarly, $\ddot{e}(t) = a_{l-1}(t) - a_l(t) - h \dot{a}_l(t) = a_{l-1}(t) + \left(\frac{h}{\tau} - 1\right) a_l(t) - \frac{h}{\tau} u_l(t)$ measurable by y_3 and y_5 . Thus, y_1, \dots, y_9 in (32) are the sensor inputs to our framework, resulting in \hat{x} in the estimation mechanism (15) which will be used to define the control signal (31) as follows.

D. Continuous-Time Closed-Loop Dynamics

Next, consider controller (31) and let $y \in \mathbb{R}^9$ denote the vector of stacked sensor, i.e., $y := \text{col}[y_1, \dots, y_9]^\top$, $\delta \in \mathbb{R}^9$ denote the vector of stacked sensor attacks, i.e., $\delta := \text{col}[\delta_1, \dots, \delta_9]^\top$, and $\gamma \in \mathbb{R}^9$ denote the vector of stacked sensor noise, i.e., $\gamma := \text{col}[\gamma_1, \dots, \gamma_9]^\top$. Define the stacked state vector $x_l := \text{col}[e_l, v_l, a_l, \Delta v_l, a_{l-1}]^\top$, where $\Delta v_l := v_{l-1} - v_l$ is the relative velocity between vehicle l and its preceding vehicle (vehicle $l-1$), carries information from u_{l-1} as $\Delta v_l = a_{l-1} - a_l$. In addition, similar to (30), $\dot{a}_{l-1} = -\frac{1}{\tau} a_{l-1}(t) + \frac{1}{\tau} u_{l-1}(t)$, where $u_{l-1}(t)$ is assumed to be securely available. Using this notation and considering that the $\hat{x} := \text{col}[\hat{x}_1, \hat{x}_2, \hat{x}_3, \hat{x}_4, \hat{x}_5]^\top$ in (15) from our framework is the estimation of x_l , the closed-loop

dynamics (30)–(31) can be written as follows:

$$\begin{cases} \dot{x}_l(t) = A^c x_l(t) + B_1^c u_{l-1}(t) + B_2^c u_l(t), \\ \xi_l(t) = k_p \hat{x}_1(t) + k_d (\hat{x}_4(t) - h \hat{x}_3(t)) \\ \quad + k_{dd} \left(\hat{x}_5(t) + \left(\frac{h}{\tau} - 1 \right) \hat{x}_3(t) - \frac{h}{\tau} u_l(t) \right) + u_{l-1}(t), \\ \dot{u}_l(t) = -\frac{1}{h} u_l(t) + \frac{1}{h} \xi_l(t), \\ y(t) = C x_l(t) + \gamma(t) + \delta(t), \end{cases} \quad (33)$$

where

$$\begin{cases} A^c = \begin{bmatrix} 0 & 0 & -h & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & -\frac{1}{\tau} & 0 & 0 \\ 0 & 0 & -1 & 0 & 1 \\ 0 & 0 & 0 & 0 & -\frac{1}{\tau} \end{bmatrix}, B_1^c = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ \frac{1}{\tau} \end{bmatrix}, \\ B_2^c = \begin{bmatrix} 0 \\ 0 \\ \frac{1}{\tau} \\ 0 \\ 0 \end{bmatrix}, C = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \end{bmatrix}. \end{cases} \quad (34)$$

E. Discrete-Time Closed-Loop Dynamic

Due to the fact that the controller implementation in practice is feasible in discrete time, we exactly discretized (33) at the sampling time instants, $t = T_s k$, $k \in \mathbb{Z}_{\geq 0}$, assuming a zero-order hold to implement control actions and model discrete-time uncertainties and obtain the equivalent discrete-time systems:

$$\begin{cases} x_l(k+1) = A x_l(k) + B_1 u_{l-1}(k) + B_2 u_l(k), \\ \xi_l(k) = k_p \hat{x}_1(k) + k_d (\hat{x}_4(k) - h \hat{x}_3(k)) \\ \quad + k_{dd} \left(\hat{x}_5(k) + \left(\frac{h}{\tau} - 1 \right) \hat{x}_3(k) - \frac{h}{\tau} u_l(k) \right) + u_{l-1}(k), \\ u_l(k+1) = \exp\left(-\frac{T_s}{h}\right) u_l(k) + \left(1 - \exp\left(-\frac{T_s}{h}\right)\right) \xi_l(k), \\ y(k) = C x_l(k) + \delta(k) + \gamma(k), \end{cases} \quad (35)$$

with $x_l(k) := x_l(T_s k)$, $u_{l-1}(k) := u_{l-1}(T_s k)$, $u_l(k) := u_l(T_s k)$, $\xi_l(k) := \xi_l(T_s k)$, $\hat{x}(k) := \hat{x}(T_s k)$, $y(k) := y(T_s k)$, $\delta(k) := \delta(T_s k)$, $\gamma(k) := \gamma(T_s k)$, and matrices

$$\begin{cases} A = \exp(A^c T_s), B_1 = \int_0^{T_s} \exp(A^c(T_s - s)) B_1^c ds, \\ B_2 = \int_0^{T_s} \exp(A^c(T_s - s)) B_2^c ds. \end{cases} \quad (36)$$

The discrete-time platooning system described in (35) constitutes a specific instance of the general linear time-invariant (LTI) system structure given in (1). In both formulations, the system matrix A retains an identical mathematical form. The input matrix B and the input vector u in (1) correspond,

respectively, to $[B_1 \ B_2]$ and $[u_{l-1} \ u_l]^\top$, as derived from the structure of (35).

F. Sensor Set (J) Configuration

For the system in (33)–(34), we only design 9 sets of disturbed sensors (equal to the number of observers) based on our method. In more detail, according to Section II-C1, and (33)–(34), the number of all possible subsets of disturbed sensors for $q = 9$ (number of sensors) is

$$\sum_{i=1}^q \binom{q}{i} = 511. \quad (37)$$

However, we are only interested in the “independent” subsets that have detectable pair (A, C_{J_j}) according to Section II-C which are 9 subsets as $J_1 = \{1, 2\}$, $J_2 = \{1, 7\}$, $J_3 = \{1, 9\}$, $J_4 = \{2, 6\}$, $J_5 = \{2, 8\}$, $J_6 = \{6, 7\}$, $J_7 = \{6, 9\}$, $J_8 = \{7, 8\}$, and $J_9 = \{8, 9\}$. Thus $j \in \{1, \dots, N\}$, $N = 9$ from the 511 subsets in (37), and the system can guarantee security up to two sensors under attack according to (8).

G. Motion Comfort Assessment

ISO-2631:1997 [74] provides guidelines for objectively measuring and evaluating human exposure to whole-body mechanical vibration and repeated shock. The guidelines suggest the consideration of two metrics: (1) Ride Comfort (RC) emphasizing the higher frequencies (mainly above 1 Hz); (2) MS emphasizing the lower frequencies (mainly below 1 Hz). The first metric (RC) reflects the immediate perception of motion discomfort through perceivable accelerations which are normally road induced but in this paper will result from forwards/rearward accelerations induced by sensor attacks and by acceleration and deceleration of the lead vehicle. The second metric (MS) reflects low frequency components which will induce motion sickness in particular in passengers and AV users taking the eyes off the road over longer periods.

The metrics are evaluated by combining the Root Mean Square (RMS) values of weighted accelerations (a_{w_o}), translational and rotational, measured at the vehicle’s center of gravity. More specifically, the RMS value of each acceleration is calculated as follows:

$$RC_o = \left(\frac{1}{t} \int_0^t a_{w_o}^2(s) ds \right)^{\frac{1}{2}}, \quad (38)$$

where o is the acceleration type, either translational or rotational, while a_{w_o} stands for the frequency weighted accelerations in the time domain. The overall RC is calculated as:

$$RC = \left(\sum k_o^2 RC_o^2 \right)^{\frac{1}{2}}, \quad (39)$$

where k_o is a weighting factor for each term which can be found in the literature [74]. This work addresses car following and hence only longitudinal accelerations ($o = X$) are considered both for comfort and motion sickness [75]. For MS, the weighting filter for longitudinal WP_{f_x} is used [75], which is similar to ISO and Motion Sickness Dose Value (MSDV).

H. Assumed Experimental Parameters

Consider two homogeneous vehicles in a platoon i.e., $l = 2$ in Fig. 2. We obtain the discrete-time system (35) with sampling interval $T_s = 0.1$ seconds. The discrete-time system corresponds to the exact discretization of the continuous-time LTI system in (33). Based on [54] we select the following CACC parameters and conditions. We select $h = 0.5$ seconds representing a relatively short following distance which can be string stable with CACC [54]. We select $\tau = 0.1$, $k_p = 0.2$, $k_d = 0.7$, $k_{dd} = 0.5$, $a_\beta = 1000$, $s_2 = 1$ m in (28), and $K_r = 2$ and $C_r = 3$ (see Section IV-B). We assumed that the system noise w is i.i.d. uniformly distributed random vector normalized to satisfy noise bound $\mathcal{B}_w = 0$. We simulate CACC where at each interval k , the desired acceleration of vehicle 1, i.e., $u_1(k)$ is transmitted from vehicle 1 to vehicle 2 via the communication network. Let $u_1(k) = 2 e^{-0.01 k}$, the initial relative velocity between vehicles 1 and 2 be 0.5 m/s, the initial spacing error be 0.1 m, and the initial velocity of vehicle 2 be 30 m/s. Therefore, $x_2(0) = [0.1, 30, 0, 0, 0.5, 0]^\top$. The initial condition for each observer set of $\hat{x}_{J_j}(0)$, $j \in \{1, \dots, N\}$, $N = 9$ (see Section III-F) is randomly chosen. Furthermore, we considered the initial condition of $\eta_{J_j}(0) = 0$, and $\beta_{J_j}(0) = 0.5$, $j \in \{1, \dots, N\}$.

I. Benchmark Method

We compare the performance of our work with that of Zhao et al. [23], Ko and Son [76], and Karmakar et al. [77].

In [23], the authors presented a recovery mechanism to confine the duration and frequency of adverse effects caused by attacks on platoon control. Meanwhile, a resilient platoon control protocol was proposed to achieve the internal stability of the Vehicular Cyber Physical Systems (VCPSs) under attacks. Although their methods successfully secure the system against attacks, as with most cybersecurity schemes, the dynamic systems experience significant excitation when the attacks begin, resulting in reduced comfort. For comparison, we use the same scheme as that used in Section V.B. Example 2 in [23].

In [76], an LSTM-based detection framework is proposed to identify malicious information attacks within connected adaptive cruise control (CACC) systems. The model captures temporal dependencies in vehicular data to detect anomalies effectively. Meanwhile, Karmakar et al. [77] present a deep learning-based approach that evaluates the trustworthiness of autonomous vehicles operating under cyberattack scenarios. While both methods demonstrate competent attack detection and mitigation capabilities, their reliability under diverse operating conditions remains insufficiently validated, which may hinder robust deployment in safety-critical environments.

IV. SIMULATION RESULTS

A. Observer Gain (L_{J_j}) Design Using LMI

Having $N = 9$, we solved all the $2N + 1 = 19$ inequalities in (24)–(26) to find P , and Z_{J_j} , $j \in \{1, \dots, 9\}$, using `gevp` (Generalized eigenvalue minimization under LMI constraints) function in MATLAB [78], which leads us to define all the observer gains L_{J_j} , $j \in \{1, \dots, 9\}$ according to (27).

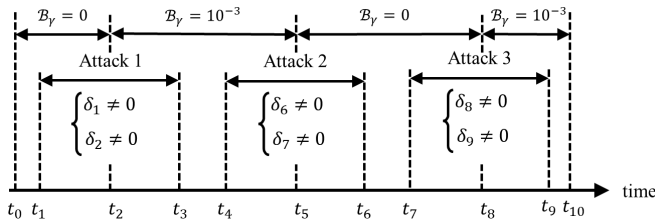


Fig. 3. Designed simulation scenario.

B. Reference Model Parameters (K_r , C_r) Design

According to A_r^c in (12), and assuming that the eigenvalues of the reference model system are $\lambda_{r,1}$ and $\lambda_{r,2}$, the parameters of A_r^c should be

$$\begin{aligned} C_r &= -(\lambda_{r,1} + \lambda_{r,2}), \\ K_r &= \lambda_{r,1} \lambda_{r,2}. \end{aligned} \quad (40)$$

The system is asymptotically stable (A_r^c is Hurwitz) if $\lambda_{r,1} < 0$ and $\lambda_{r,2} < 0$. For our simulation, we consider $\lambda_{r,1} = -1$, and $\lambda_{r,2} = -2$ which results in $K_r = 2$ and $C_r = 3$. Note that the eigenvalues are selected customary while they are holding distinct negative real values [79].

C. Simulation Scenario

Here, we study bounded attacks with three attack severities (magnitudes), ordered from high to low as 1) Critical, 2) Very Uncomfortable, and 3) Uncomfortable. The Critical Safety attacks are designed as intense attacks that result in collisions when no countermeasures are taken, the Very Uncomfortable attacks are designed such that they lead to considerable discomfort, and the Uncomfortable attacks' design achieves considerably more power than common sensor noise while it does not result in collisions or major discomfort. To generate Critical Safety Attacks, the attack amplitude was increased to ensure that at least one collision occurred in each attack. Very Uncomfortable Attacks were then derived by gradually reducing the attack amplitude from the Critical Safety Attack level until no collisions were observed. Finally, Uncomfortable Attacks were formulated by adjusting the attack amplitude such that the overall MSDV_x and RC values fell within the predefined uncomfortable range [80].

Within each attack magnitude case, three different attacks are simulated. In each of the attacks, two of the sensors are hacked at the same time where the hacked sensors are different from one attack to the other attack. According to Fig. 3, for two parts of the simulation (from t_2 to t_5 and from t_8 to t_{10}), normal sensor noise γ_i is nonzero as a realistic condition and is i.i.d. uniformly distributed random vectors normalized to satisfy noise bounds $\mathcal{B}_\gamma = 10^{-3}$. For the rest of the simulation, we set $\mathcal{B}_\gamma = 0$. In addition, in Attack 1, sensors y_1 and y_2 are under FDI attack between t_1 and t_3 . Similarly, in Attack 2 which is between t_4 and t_6 , sensors y_6 and y_7 are under FDI attack. Furthermore, in Attack 3, sensors y_8 and y_9 are under FDI attack between t_7 and t_9 .

Both Attack 1 and Attack 2 are white noise, and Attack 3 is a repeatedly on-off switching white noise where the RMS value of each of attack per each scenario is reported in

TABLE I
RMS VALUE OF DESIGNED ATTACKS PERSEVERITY LEVEL

Severity level	Attack 1		Attack 2		Attack 3	
	δ_1 (m)	δ_2 ($\frac{m}{s}$)	δ_6 (m)	δ_7 ($\frac{m}{s}$)	δ_8 (m)	δ_9 ($\frac{m}{s}$)
Critical Safety	300	300	300	300	300	300
Very Uncomfortable	150	150	150	150	150	150
Uncomfortable	15	15	15	15	15	15

TABLE I. Attack 3 is repeatedly (de)activated by an activation logic as follows.

$$\begin{cases} \delta_8(k) = 0, \delta_9(k) = 0, & \text{if } \{\text{floor}[kT_s] = 2l \mid l \in \mathbb{Z}\}, \\ \delta_8(k) \neq 0, \delta_9(k) \neq 0 & \text{otherwise.} \end{cases} \quad (41)$$

By setting $\mathcal{B}_\gamma = 0$ between t_5 and t_8 , we investigate the asymptotical stability of the framework in the presence of attack and absence of normal sensor noise. We performed a 30 minutes simulation where $t_0 = 0s$, $t_1 = 60s$, $t_2 = 300s$, $t_3 = 540s$, $t_4 = 660s$, $t_5 = 900s$, $t_6 = 1140s$, $t_7 = 1260s$, $t_8 = 1500s$, $t_9 = 1740s$, and $t_{10} = 1800s$.

D. Results: Steady State Platooning

To evaluate our method comprehensively, we evaluate the scenario of steady state platooning with the three sequential attacks defined in Section IV-C. We compare four conditions as follows from securing safety and securing comfort points of view:

- **Condition 1 (Insecure controller [54] without attack):** Depicts the performance of the controller in (31) in the absence of attack ($\delta_i = 0, i \in \{1, \dots, 9\}$). Note that, here, for the variables measured with multiple sensors we use the average of the measured values for a variable to design the control signal in (31).
- **Condition 2 (Insecure controller [54] with attack):** Depicts the performance of the controller in (31) but not using any cyber attack security approach along with the three designed attacks in Section IV-C. Same as Condition 1, for the variables measured with multiple sensors we use the average of the measured values for a variable to design the control signal in (31).
- **Condition 3 (Zhao's method [23] with attack):** Depicts the performance of the security method in [23] (explained in Section III-I) along with the designed attacks in Section IV-C.
- **Condition 4 (Our method with attack):** Depicts the performance of our security method explained in Section II-C using controller (35), along with the designed attacks in Section IV-C. The controller in (35) is the secure version of the controller in (31) using our method to reject attacked sensors.

1) *Securing Safety:* Fig. 4 shows the followed distance (d_2) in Condition 2 (Insecure controller [54] with attack) where $d_2 < 0$ defines the collisions. The designed Critical Safety attacks result in five collisions, the Very Uncomfortable attacks lead to 30 m oscillations of the d_2 and no collision, and the Uncomfortable attacks lead to 5 m oscillations of the d_2 and no collision. TABLE II summarizes the main results, namely

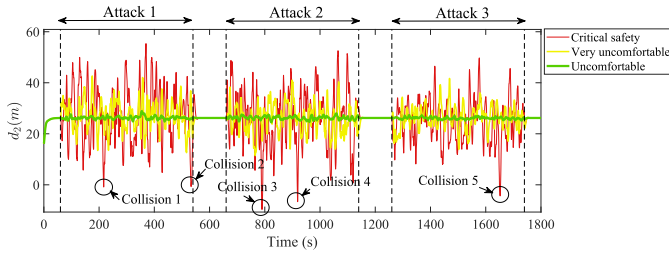


Fig. 4. Following distance (d_2) between the Vehicle 2 and its preceding Vehicle 1 per each attack severity level by the insecure platooning controller in (31) (Condition 2).

TABLE II

OBJECTIVE ASSESSMENT OF SAFETY FOR STEADY STATE MANEUVER (ATTACK 1-3) BASED ON NUMBER OF COLLISIONS (NC) AND RMS OF THE SPACING ERROR IN METERS (RMS_{e_2})

Condition	Severity level					
	Critical Safety		Very Uncomfortable		Uncomfortable	
	NC	RMS_{e_2}	NC	RMS_{e_2}	NC	RMS_{e_2}
1 (Insecure controller [54] without attack)	0	0.028	0	0.028	0	0.028
2 (Insecure controller [54] with attack)	5	9.516	0	4.912	0	0.547
3 (Zhao's method [23] with attack)	0	0.774	0	0.579	0	0.079
4 (Our method with attack)	0	0.029	0	0.029	0	0.029

the Number of Collisions (NC) and RMS of the spacing error (RMS_{e_2}) per severity level. Apparently both Zhao's method [23] (Condition 3) and our method (Condition 4) avoid all collisions but our method achieves a much lower spacing error which is almost as low as in the case without attack.

Fig. 5 illustrates the attack detection dynamics as function of time for the continuous Attacks 1 and 2 and the rapidly switching Attack 3. Obviously, the CACC without any security approach (Condition 2) has the highest vulnerability to sensor attacks compared to Conditions 3 and 4. In Fig. 5, Zhao's method [23] (Condition 3) presents asymptotic stability of the estimation error against Attack 1 and Attack 2, while at the beginning of the attacks, namely at t_1 for Attack 1 and t_4 for Attack 2, the system states are excited for a while. This is more evident in the zoomed-in area at time t_1 in Fig. 5(a), where it takes approximately 20 seconds for Condition 3 to reject the attack impact on the system states. In Attack 3, Zhao's method [23] (Condition 3) fails to secure the system, and Attack 3 successfully disturbs the system states due to the states' excitations in every two seconds defined in (41). The failure can be addressed more clearly in TABLE II where the resulting $RMS_{e_2} = 0.58$ (m), which defines a considerable error safe distance ($d_{r,2}$). However, based on Fig. 5, our method (Condition 4) could successfully secure the safety of vehicle platooning control by almost completely rejecting the impact of all three attacks. For instance, Condition 4 rejects the attack impact almost immediately, in contrast to Zhao's method [23], as illustrated in the zoomed-in area at time t_1 in Fig. 5(a). In terms of safety, our method (Condition 4) resulted in $RMS_{e_2} = 0.03$ (m) similar to the best performance, i.e.

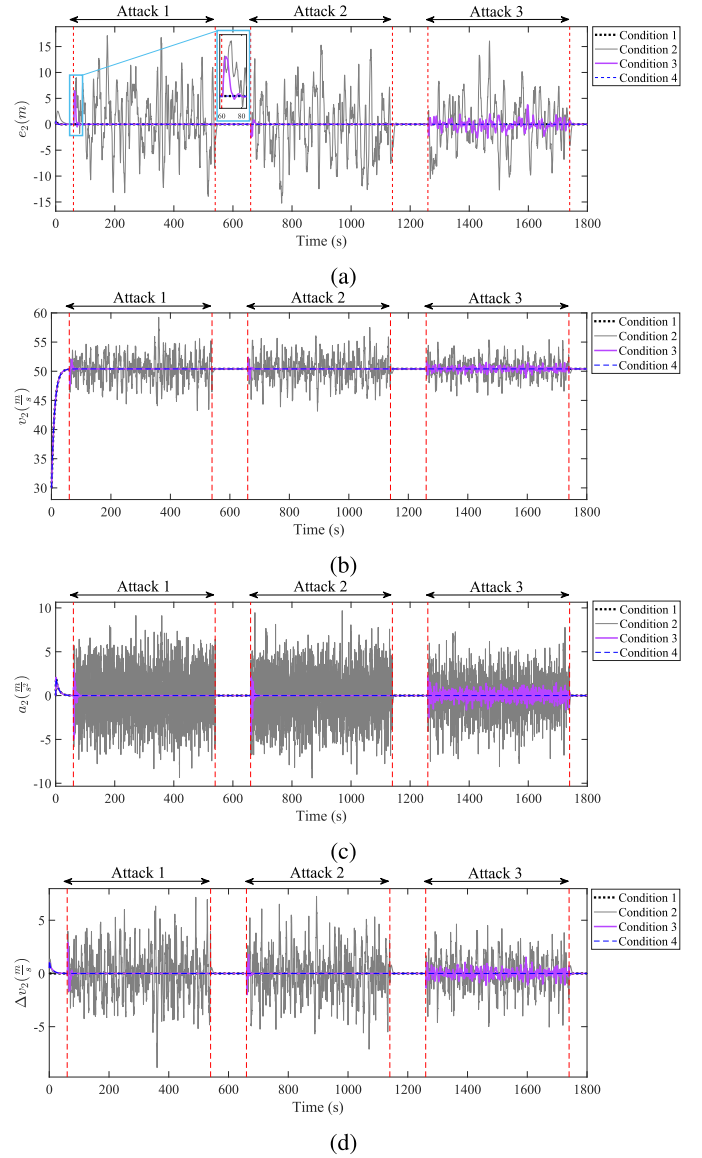


Fig. 5. Control performance for the Very Uncomfortable attack severity: a) Spacing error (e_2), b) Velocity (v_2), c) Acceleration (a_2), d) Relative velocity (Δv_2).

Condition 1 without any attacks, and about 94% less than the RMS_{e_2} of Zhao's method [23] (Condition 3).

The asymptotic stability with no states' excitation can be investigated more precisely in Fig. 6(a), where the estimation error in (17) is depicted. Between t_2 and t_5 and between t_8 and t_{10} , the error is only affected by the normal sensor noise which is inevitable and cannot be rejected by any existing methods due to the best of our knowledge. Furthermore, between t_0 and t_2 and between t_5 and t_8 , the estimation error in Condition 4 (contrary to Condition 3) not only rejects the impact of attacks with no states' excitation but also is asymptotically stable and converges to zero which reflects the strong stability of the framework. Fig. 6 (b) and (c) draw the performance of each framework component. In Fig. 6(b) the classification ratio's (14) performance to the noise and the attacks is depicted. The classification ratio could classify each observer based on the degree of affectedness to the attack. In each attack, the

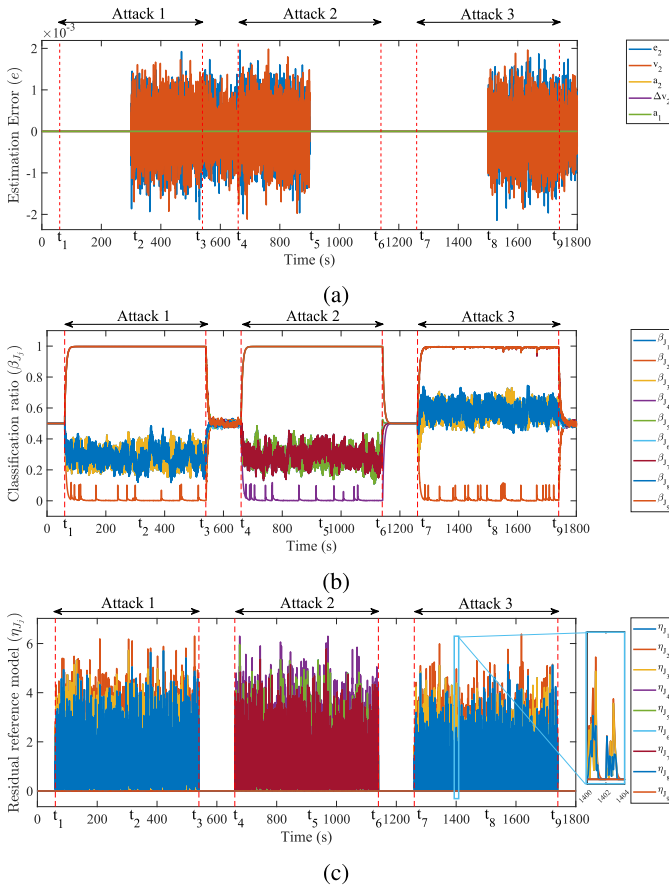


Fig. 6. The optimal-coupling-observer framework's components' performance (Condition 4): a) Estimation error, b) classification ratio, c) residual reference model.

classification ratio includes three regions around 1, 0.6, 0.3, and 0. Apparently, the framework is using the observer with the greatest value for classification ratio (ideally equal to 1) to estimate the system states.

Fig. 6(c) shows that the residual reference model in (12) is asymptotically stable in the usual sense in the absence of noise and attack, namely between t_6 and t_7 , and also can be correctly excited in the presence of three of the attacks. In the rapidly switching Attack 3, which was a bottleneck for Zhao's method [23] (Condition 3), it is clear that the residual reference model is correctly excited every two seconds, namely at $t = 1400s$, and $t = 1402s$ which are the start of the on-mode of the Attack 3 in (41).

Regarding the Critical Safety and Uncomfortable severity levels in TABLE II, the same conclusion as Very Uncomfortable severity level emerges. Condition 2 is the most vulnerable to attacks, Condition 3 is considerably affected by Attack 3, and Condition 4 (our method) performs similar to Condition 1. However, Condition 2 under Critical Safety attacks results in instability of the Vehicle 2 states with five collisions shown in Fig. 4 (while they are bounded during all of the Attacks) which strongly threatens safety.

2) *Securing Comfort*: To assess the occupants' comfort, the longitudinal accelerations of Vehicle 2 in the platoon with Very Uncomfortable severity level are compared in the frequency domain in Fig. 7(a). In addition, the objective comfort scores

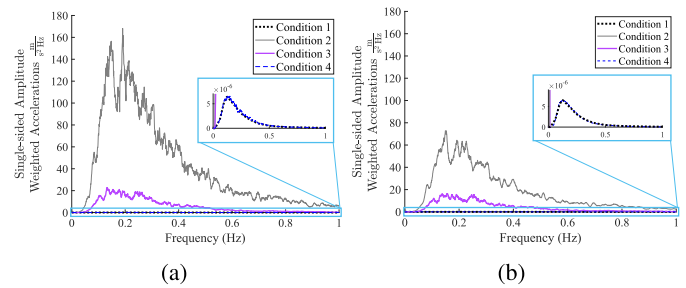


Fig. 7. Frequency analysis for the Very Uncomfortable attack severity: (a) Vehicle 2, (b) Vehicle 10 in platooning.

TABLE III
OBJECTIVE ASSESSMENT OF COMFORT FOR STEADY STATE MANEUVER (ATTACK 1-3) BASED ON MOTION SICKNESS (MSDV_x) AND RIDE COMFORT (RC) INDEXES

Condition	Severity level					
	Critical Safety		Very Uncomfortable		Uncomfortable	
	MSDV _x	RC	MSDV _x	RC	MSDV _x	RC
1 (Insecure controller [54] without attack)	0.0028	4e-5	0.0028	4e-5	0.0028	4e-5
2 (Insecure controller [54] with attack)	94.69	3.08	47.38	1.59	4.65	0.15
3 (Zhao's method [23] with attack)	10.41	0.29	6.57	0.16	1.01	0.02
4 (Our method with attack)	0.0029	5e-5	0.0029	5e-5	0.0029	5e-5

(MSDV_x reflecting motion sickness and RC reflecting ride comfort, Section III-G) based on the vehicle's longitudinal acceleration are reported in TABLE III per each severity level.

In condition 2 without security method the most severe "Critical Safety" attack with $RC = 3.08 \frac{m}{s^2}$ is indeed classified as extremely uncomfortable ($RC > 2 \frac{m}{s^2}$ according to ISO2361) whereas the "Very Uncomfortable" attack with $RC = 1.59 \frac{m}{s^2}$ is indeed classified as very uncomfortable ($1.25 < RC < 2.5 \frac{m}{s^2}$ according to ISO2631).

Fig. 7 illustrates the longitudinal accelerations as filtered with regards to motion sickness (Section III-G). According to Fig. 7(a), the highest of the longitudinal accelerations is identified in Condition 2. This is consistent across the whole frequency range, relevant for motion sickness i.e., 0 to 1 Hz. This shows that the system with insecure controller is sensitive to attacks in the frequency range which affects the occupants' sickness drastically (i.e., around 0.2 Hz). Meanwhile, the lowest power is identified in Conditions 1 and 4. The performance of Condition 3 shows that although the compared method in Section III-I could reduce the maximum power for about 87% compared to the insecure controller in Condition 2, it is considerably greater than the almost zero power ($0.01 (\frac{m}{s^2 Hz})$) in Condition 4 as well as no attack scenario in Condition 1. Furthermore, our method in Condition 4 has an almost identical response to no attack scenario in Condition 1, illustrating that the impact of the attack was almost completely zeroed out. As a result, no additional sickness would occur to the occupants.

According to TABLE III for Critical Safety severity level, the generated $MSDV_x = 10.41$ and $RC = 0.29 \frac{m}{s^2}$ in Con-

dition 3 are reduced about 89% and 91% compared to the insecure controller in Condition 2, respectively, while they are considerably higher than $\text{MSDV}_x = 0.0028$ and $\text{RC} = 4e-5 \frac{m}{s^2}$ for Condition 4 as well as no attack scenario in Condition 1. In addition, for Very Uncomfortable severity level, the $\text{MSDV}_x = 6.57$ and $\text{RC} = 0.16 \frac{m}{s^2}$ in Condition 3 decreased about 86% and 89% compared to Condition 2, respectively, however, they are higher than $\text{MSDV}_x = 0.0028$ and $\text{RC} = 4e-5 \frac{m}{s^2}$ for Condition 4 as well as no attack scenario in Condition 1. Finally, for Uncomfortable severity level, the generated $\text{MSDV}_x = 1.01$ and $\text{RC} = 0.02 \frac{m}{s^2}$ in Condition 3 dropped about 78% and 84% compared to the insecure controller in Condition 2, and increased drastically compared to Condition 1 with $\text{MSDV}_x = 0.0028$ and $\text{RC} = 4e-5 \frac{m}{s^2}$, respectively. As a result, Zhao's method [23] could generally reduce MS and RC at all severity levels while it could not completely secure the occupant's comfort.

On the contrary and for all severity levels, our method (Condition 4) illustrated almost zero MS metric by canceling out the impact of the attack providing similar comfort with no attack scenario in Condition 1. There was a small increase ($\sim 4\%$) for MSDV_x compared to Condition 1, which was negligible due to the insignificant amplitude of the metric.

E. Platooning With 10 Vehicles

To further evaluate the scalability and robustness of the proposed method, we simulated a platoon of 10 vehicles, where Vehicle 1 is the lead vehicle and Vehicle 10 is the tail vehicle. As above, an attack was launched on Vehicle 2, following the scenario illustrated in Fig. 3. Now 8 additional vehicles were simulated to demonstrate attack attenuation in the platoon. A comparison of the single-sided amplitude-weighted acceleration spectra for Vehicle 2 and Vehicle 10, shown in Fig. 7(a) and Fig. 7(b), respectively, reveals notable differences in system response across control strategies. Zhao's method [23] (Condition 3) reduced the peak amplitude by approximately 22%, while the insecure controller in Condition 2 achieved a more substantial reduction of about 56%. Remarkably, our proposed method (Condition 4) maintained performance nearly identical to the no-attack baseline (Condition 1), demonstrating high resilience to the injected disturbance.

These results highlight the string stability of the controller defined in (35) used for Condition 1,2, and 4, which effectively suppresses disturbance propagation along the platoon. In contrast, Zhao's method exhibited limitations under the repeatedly on-off switching attack scenario, where spacing errors were neither amplified nor sufficiently damped, thereby affecting downstream vehicle performance. Our method preserved the ride comfort of the tail vehicle at a level comparable to that of the second vehicle, underscoring its effectiveness in maintaining platoon stability and passenger comfort under adversarial conditions.

F. State-of-Art Reliability Comparison

To further compare the reliability of Zhao's method [23] (Condition 3) with our method (Condition 4), we study variation of two metrics of False positive (FP) and F1-Score by

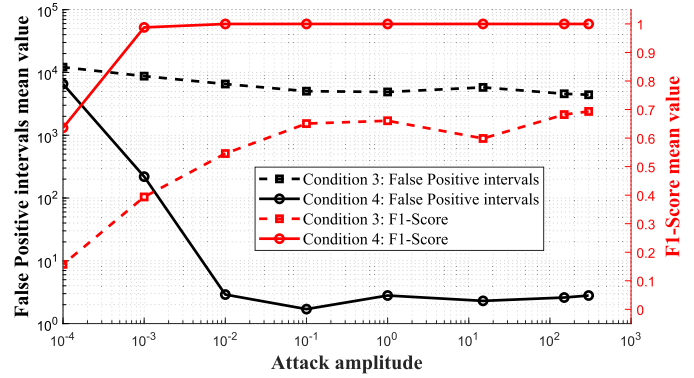


Fig. 8. Reliability of attack detection mechanisms.

running the scenario in Section IV-D for 100 times and with different attack amplitudes from 0.0001 to 300. FP defines the number of intervals that the method mistakenly did not use the most reliable observer, and F1-Score estimates the quality of resiliency under attacks.

Since our method does not explicitly classify an observer as reliable or compromised but instead selects the most reliable observer at each time step, a FP occurs when the method selects a compromised observer. In such cases, the other, more reliable observers are incorrectly ignored, leading to a False Negative (FN). Consequently, the number of time intervals with FP is equal to those with FN. By the same reasoning, the number of time intervals for True Negative (TN) and True Positive (TP) are also equal. Since $\text{TP} = \text{TN}$ and $\text{FP} = \text{FN}$, the evaluation metrics—F1-score, Precision, and Recall—yield the same value.

The reliability measures as function of attack amplitude are depicted in Fig. 8. From Fig. 8(left axis) both methods have high FP mean values for attack amplitudes below or equal to 0.001. The reason is that the attack amplitude is below the noise amplitude and thus both methods are practically disabled. For attack amplitudes above 0.001, the FP mean value for our method (Condition 4) is around 2, while this is around 7000 for Zhao's method [23] (Condition 3). This is because Zhao's method [23] (Condition 3) fails to secure the system in presence of the on-off Attack 3 as discussed in Section IV-D. In practice, the FP around 2 means that attacks of relevant magnitude are recognised in around two time steps after the start of the attack (0.2 seconds) and that the end of the attack is detected similarly, while during the attack the detection remains correct. This shows that the attack detection with our method is considerably quicker than Zhao's method [23]. Fig. 8(right axis) gives the same conclusion for the attacks above noise amplitude (0.001), where our method (Condition 4) with mean F1-Score of 0.999 is about 53% more reliable than Zhao's method [23] (Condition 3) with mean F1-Score of 0.65. The main reason for the reliability drop by Zhao's method [23] (Condition 3) results from the vulnerability of the method to on-off Attack 3.

Remark 6: For a broader comparison with SOTA cybersecurity frameworks, we evaluate the performance of our method (Condition 4) alongside Zhao's method [23] (Condition 3), as well as the approaches by Ko and Son [76] and Karmakar

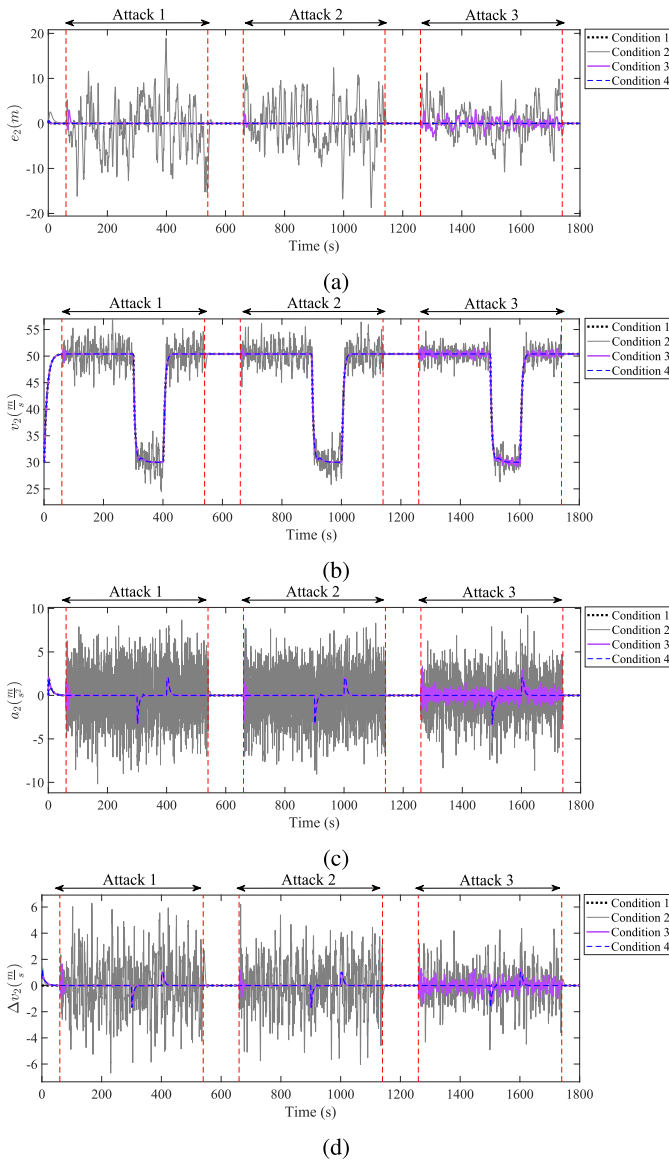


Fig. 9. The platooning vehicles control performance under the designed scenario including braking: a) Spacing error (e_2), b) Velocity (v_2), c) Acceleration (a_2), d) Relative velocity (Δv_2).

et al. [77], in terms of F1-score for Attack 1 and Attack 2. Attack 3 is not addressed by the methods of Ko and Son [76] and Karmakar et al. [77] and therefore excluded for this comparison. Considering only Attack 1 and 2, our method (Condition 4) achieves an F1-score of 0.999, outperforming Condition 3 (F1-score = 0.97), as well as the methods by Ko and Son [76] and Karmakar et al. [77] (both with F1-score = 0.96).

G. Results: Braking Maneuver

For steady state platooning as investigated in Section IV-D, our method (Condition 4) performed excellently. Here we explore attacks in the more critical condition where the lead vehicle is suddenly decelerating by adding three extreme braking events to the scenario in Section IV-C at t_2 , t_5 , and t_8 to reach and stay on the speed of $30 \frac{m}{s}$ for 100 s, and then accelerate to reach the speed of $50.4 \frac{m}{s}$. As shown in

TABLE IV
OBJECTIVE ASSESSMENT OF SAFETY FOR BRAKING MANEUVER BASED ON NUMBER OF COLLISIONS (NC) AND RMS OF THE SPACING ERROR IN METERS (RMS_{e_2})

Condition	Severity level					
	Critical Safety		Very Uncomfortable		Uncomfortable	
	NC	RMS_{e_2}	NC	RMS_{e_2}	NC	RMS_{e_2}
1 (Insecure controller [54] without attack)	0	0.03	0	0.03	0	0.03
2 (Insecure controller [54] with attack)	10	9.76	1	4.54	0	0.77
3 (Zhao's method [23] with attack)	0	1.15	0	0.53	0	0.10
4 (Our method with attack)	0	0.05	0	0.03	0	0.03

TABLE V
OBJECTIVE ASSESSMENT OF COMFORT FOR BRAKING MANEUVER BASED ON MOTION SICKNESS ($MSDV_x$) AND RIDE COMFORT (RC) INDEXES

Condition	Severity level					
	Critical Safety		Very Uncomfortable		Uncomfortable	
	$MSDV_x$	RC	$MSDV_x$	RC	$MSDV_x$	RC
1 (Insecure controller [54] without attack)	3.81	0.03	3.81	0.03	3.81	0.03
2 (Insecure controller [54] with attack)	97.41	3.17	48.21	1.59	5.63	0.16
3 (Zhao's method [23] with attack)	13.13	0.27	7.09	0.15	3.94	0.04
4 (Our method with attack)	3.81	0.03	3.81	0.03	3.81	0.03

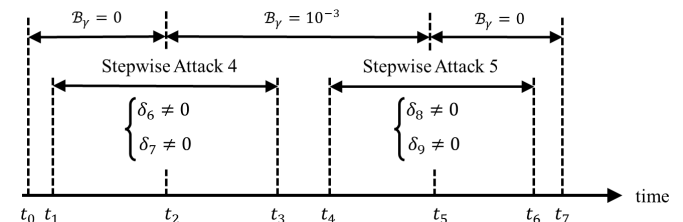


Fig. 10. Designed scenario for stepwise FDI attacks.

TABLE IV, the braking maneuver drastically affected safety in Condition 2 as NC increased from 5 to 10 for Critical Safety attack and from 0 to 1 for Very Uncomfortable attack. From Fig. 9, we have the same conclusion as Fig. 5 which shows that Condition 4 could successfully reject the impact of attacks with no attack-related state excitation. However, Fig. 9(c) shows high excitation of the acceleration due to braking, which considerably affects comfort. From TABLE V and TABLE IV, one can see that $MSDV_x$, RC, and RMS_{e_2} for Conditions 1 and 4 are similar across all severity levels, demonstrating the effectiveness of our method in rejecting the attacks' impact without any loss of comfort and security also during extreme braking.

H. Results: Stepwise FDI Attack

Referring to Remark 1, any attack resulting in error convergence during attack occurrence may degrade the excitability

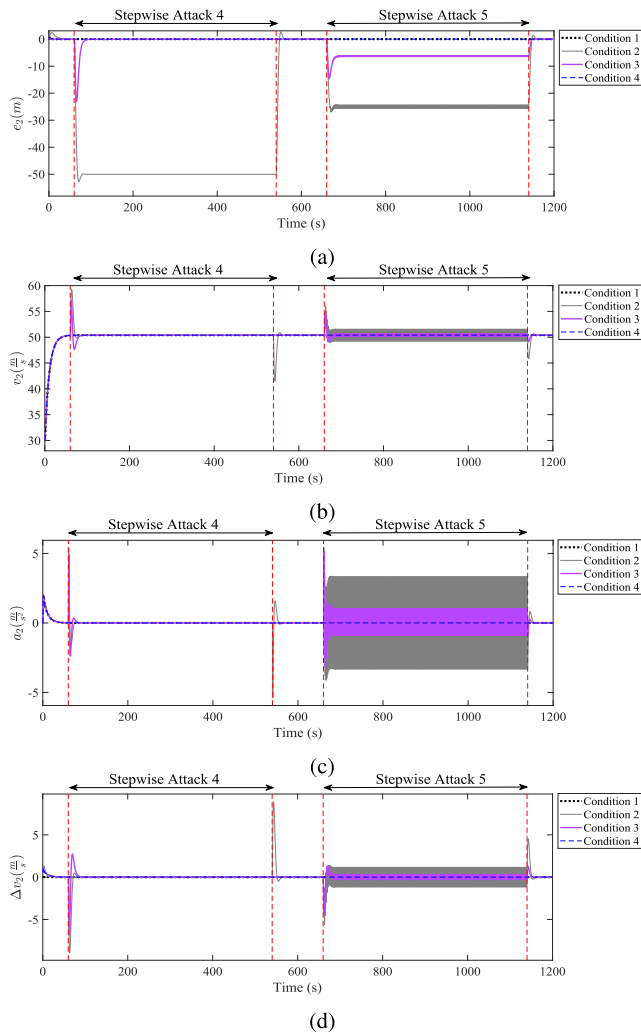


Fig. 11. Control performance under stepwise FDI attack: a) Spacing error (e_2), b) Velocity (v_2), c) Acceleration (a_2), d) Relative velocity (Δv_2).

of the residuals of the observer or the classification ratio. To investigate the excitability impact, we study steady state platooning using a continuous stepwise FDI attack, and a repeatedly on-off switching stepwise FDI attack [81] with the Very Uncomfortable magnitude. In each of the attacks, two of the sensors are hacked at the same time, where the hacked sensors are different from one attack to the other. According to Fig. 10, for one part of the simulation (from t_2 to t_5), sensor noise γ_i is nonzero as a realistic condition and is i.i.d. uniformly distributed random vectors normalized to satisfy noise bounds $\mathcal{B}_\gamma = 10^{-3}$. For the rest of the simulation, we set $\mathcal{B}_\gamma = 0$. In addition, in Attack 4, sensors y_6 and y_7 are under continuous stepwise FDI attack between t_1 and t_3 . In Attack 5 which is between t_4 and t_6 , sensors y_8 and y_9 are under a repeatedly on-off switching stepwise FDI attack, which is activated by the activation logic in (41).

We performed a 20 minutes simulation where $t_0 = 0s$, $t_1 = 60s$, $t_2 = 300s$, $t_3 = 540s$, $t_4 = 660s$, $t_5 = 900s$, $t_6 = 1140s$, and $t_7 = 1200s$.

As above, we compare four conditions in the presence of stepwise FDI attacks. The states of Vehicle 2 in the platoon are depicted in Fig. 11. Based on these states, the distributed CACC scheme without any security approach (Condition 2)

shows the highest vulnerability to sensor attacks compared to Condition 3 and Condition 4. On the other hand, in Fig. 11, Zhao's method [23] (Condition 3) presents asymptotic stability of the estimation error against Attack 4, while at the beginning of the attack, namely at t_1 , the system states are excited for a short time. Continuously in Attack 5, Zhao's method [23] (Condition 3) fails to secure the system, and Attack 5 successfully disturbs the system states due to the states' excitations in every two seconds defined in (41). However, based on Fig. 11, our method (Condition 4) could successfully secure the safety of vehicle platooning control by completely rejecting the impact of the two attacks.

V. CONCLUSION AND FUTURE WORK

This article presents a novel optimal-coupling-observer-based framework for a homogeneous CAV platoon under bounded attacks. The framework includes three main components: 1) sensor set design, 2) excitation mechanism, and 3) estimation mechanism, in which all components work simultaneously together to gradually zero out the estimation error by identifying and using the most reliable observer to estimate the system states. Due to the coupling of each observer with the most reliable observer in the framework and the nonlinearity of the observer, the overall error system results in an LTV system with a complicated problem of designing the observer parameters, in which we used an LMI approach to design the parameters with guaranteed global asymptotic stability. The results show that the framework guarantees the string stability of platoons in the presence of bounded attacks.

Further developments include integrating the lateral behaviour, besides the longitudinal behaviour of platooning vehicles, testing in more complex scenarios such as mixed traffic flows or highly dynamic environments. From a methodology point of view, the observer structure may be regulated with a new design to achieve maximum detectability for maximum attack tolerability with minimum needed observers. In addition, to validate the secured comfort, experiments including human participants should be considered to confirm motion comfort and perceived safety with our framework in a real environment.

REFERENCES

- [1] N. Lu, N. Cheng, N. Zhang, X. Shen, and J. W. Mark, "Connected vehicles: Solutions and challenges," *IEEE Internet Things J.*, vol. 1, no. 4, pp. 289–299, Aug. 2014.
- [2] J. A. Guerrero-Ibanez, S. Zeadally, and J. Contreras-Castillo, "Integration challenges of intelligent transportation systems with connected vehicle, cloud computing, and Internet of Things technologies," *IEEE Wireless Commun.*, vol. 22, no. 6, pp. 122–128, Dec. 2015.
- [3] A. Khalil, K. F. Aljanaideh, and M. A. Janaideh, "On connected autonomous vehicles with unknown human driven vehicles effects using transmissibility operators," *IEEE Trans. Autom. Sci. Eng.*, vol. 20, no. 3, pp. 1876–1889, Jul. 2023.
- [4] S. E. Li et al., "Dynamical modeling and distributed control of connected and automated vehicles: Challenges and opportunities," *IEEE Intell. Transp. Syst. Mag.*, vol. 9, no. 3, pp. 46–58, Fall. 2017.
- [5] Y. Zheng, S. E. Li, K. Li, and W. Ren, "Platooning of connected vehicles with undirected topologies: Robustness analysis and distributed H-infinity controller synthesis," *IEEE Trans. Intell. Transp. Syst.*, vol. 19, no. 5, pp. 1353–1364, May 2018.
- [6] J. Zhou et al., "Robust min-max model predictive vehicle platooning with causal disturbance feedback," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 9, pp. 15878–15897, Sep. 2022.

- [7] Y. Li, Y. Zhao, and S. Tong, "Adaptive fuzzy control for heterogeneous vehicular platoon systems with collision avoidance and connectivity preservation," *IEEE Trans. Fuzzy Syst.*, vol. 31, no. 11, pp. 3934–3943, Nov. 2023.
- [8] C. Diels and J. E. Bos, "Self-driving carsickness," *Appl. Ergonom.*, vol. 53, pp. 374–382, Mar. 2016.
- [9] G. Papaioannou, C. Shen, M. Rothhämel, and R. Happee, "Occupants' comfort: What about human body dynamics in road and rail vehicles?," *Vehicle Syst. Dyn.*, vol. 63, no. 7, pp. 1–59, Jul. 2025.
- [10] M. Aledhari, M. Rahouti, J. Qadir, B. Qolomany, M. Guizani, and A. Al-Fuqaha, "Motion comfort optimization for autonomous vehicles: Concepts, methods, and techniques," *IEEE Internet Things J.*, vol. 11, no. 1, pp. 378–402, Jan. 2024.
- [11] X. He, R. Happee, and M. Wang, "A new computational perceived risk model for automated vehicles based on potential collision avoidance difficulty (PCAD)," *Transp. Res. C, Emerg. Technol.*, vol. 166, Sep. 2024, Art. no. 104751.
- [12] X. He, J. Stapel, M. Wang, and R. Happee, "Modelling perceived risk and trust in driving automation reacting to merging and braking vehicles," *Transp. Res. F, Traffic Psychol. Behav.*, vol. 86, pp. 178–195, Apr. 2022.
- [13] Z. Lian, P. Shi, C.-C. Lim, and X. Yuan, "Fuzzy-model-based lateral control for networked autonomous vehicle systems under hybrid cyber-attacks," *IEEE Trans. Cybern.*, vol. 53, no. 4, pp. 2600–2609, Apr. 2023.
- [14] Y. Bian, C. Du, M. Hu, S. E. Li, H. Liu, and C. Li, "Fuel economy optimization for platooning vehicle swarms via distributed economic model predictive control," *IEEE Trans. Autom. Sci. Eng. (from July 2004)*, vol. 19, no. 4, pp. 2711–2723, Oct. 2022.
- [15] Y. Li, Y. Zhao, W. Liu, and J. Hu, "Adaptive fuzzy predefined-time control for third-order heterogeneous vehicular platoon systems with dead zone," *IEEE Trans. Ind. Informat.*, vol. 19, no. 9, pp. 9525–9534, Sep. 2023.
- [16] J. Petit and S. E. Shladover, "Potential cyberattacks on automated vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 2, pp. 546–556, Apr. 2015.
- [17] Y. Deng, T. Zhang, G. Lou, X. Zheng, J. Jin, and Q.-L. Han, "Deep learning-based autonomous driving systems: A survey of attacks and defenses," *IEEE Trans. Ind. Informat.*, vol. 17, no. 12, pp. 7897–7912, Dec. 2021.
- [18] M. Adhikari, A. Munusamy, A. Hazra, V. G. Menon, V. Anavangot, and D. Puthal, "Security in edge-centric intelligent Internet of Vehicles: Issues and remedies," *IEEE Consum. Electron. Mag.*, vol. 11, no. 6, pp. 24–31, Nov. 2022.
- [19] A. Nikitas, S. Parkinson, and M. Vallati, "The deceitful connected and autonomous vehicle: Defining the concept, contextualising its dimensions and proposing mitigation policies," *Transp. Policy*, vol. 122, pp. 1–10, Jun. 2022.
- [20] S. Nordhoff, J. Stapel, X. He, A. Gentner, and R. Happee, "Do driver's characteristics, system performance, perceived safety, and trust influence how drivers use partial automation? A structural equation modelling analysis," *Frontiers Psychol.*, vol. 14, Apr. 2023, Art. no. 1125031.
- [21] S. Nordhoff et al., "Using the UTAUT2 model to explain public acceptance of conditionally automated (L3) cars: A questionnaire study among 9,118 car drivers from eight European countries," *Transp. Res. F, Traffic Psychol. Behav.*, vol. 74, pp. 280–297, Oct. 2020.
- [22] Y. Li and S. Tong, "Bumpless transfer distributed adaptive backstepping control of nonlinear multi-agent systems with circular filtering under DoS attacks," *Automatica*, vol. 157, Nov. 2023, Art. no. 111250.
- [23] Y. Zhao, Z. Liu, and W. S. Wong, "Resilient platoon control of vehicular cyber physical systems under DoS attacks and multiple disturbances," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 8, pp. 10945–10956, Aug. 2022.
- [24] R. A. Biroon, Z. A. Biron, and P. Pisu, "False data injection attack in a platoon of CACC: Real-time detection and isolation with a PDE approach," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 7, pp. 8692–8703, Jul. 2022.
- [25] M. Xie, D. Ding, X. Ge, Q.-L. Han, H. Dong, and Y. Song, "Distributed platooning control of automated vehicles subject to replay attacks based on proportional integral observers," *IEEE/CAA J. Autom. Sinica*, vol. 11, no. 9, pp. 1954–1966, Sep. 2024.
- [26] Z. Ju, H. Zhang, and Y. Tan, "Deception attack detection and estimation for a local vehicle in vehicle platooning based on a modified UFIR estimator," *IEEE Internet Things J.*, vol. 7, no. 5, pp. 3693–3705, May 2020.
- [27] F. Yang, Z. Gu, L. Hua, and S. Yan, "A resource-aware control approach to vehicle platoons under false data injection attacks," *ISA Trans.*, vol. 131, pp. 367–376, Dec. 2022.
- [28] Z. Zhou, F. Zhu, D. Xu, S. Guo, and Y. Zhao, "Attack resilient control for vehicle platoon system with full states constraint under actuator faulty scenario," *Appl. Math. Comput.*, vol. 419, Apr. 2022, Art. no. 126874.
- [29] M. S. Chong, M. Wakaiki, and J. P. Hespanha, "Observability of linear systems under adversarial attacks," in *Proc. Amer. Control Conf. (ACC)*, Jul. 2015, pp. 2439–2444.
- [30] H. Fawzi, P. Tabuada, and S. Diggavi, "Secure estimation and control for cyber-physical systems under adversarial attacks," *IEEE Trans. Autom. Control*, vol. 59, no. 6, pp. 1454–1467, Jun. 2014.
- [31] Y. Shoukry and P. Tabuada, "Event-triggered projected Luenberger observer for linear systems under sparse sensor attacks," in *Proc. 53rd IEEE Conf. Decis. Control*, Dec. 2014, pp. 3548–3553.
- [32] V. Hassani, A. P. Aguiar, M. Athans, and A. M. Pascoal, "Multiple model adaptive estimation and model identification using a minimum energy criterion," in *Proc. Amer. Control Conf.*, Jun. 2009, pp. 518–523.
- [33] M. Elbanhawi, M. Simic, and R. Jazar, "In the passenger seat: Investigating ride comfort measures in autonomous cars," *IEEE Intell. Transp. Syst. Mag.*, vol. 7, no. 3, pp. 4–17, Fall. 2015.
- [34] Z. Htike, G. Papaioannou, E. Siampis, E. Velenis, and S. Longo, "Fundamentals of motion planning for mitigating motion sickness in automated vehicles," *IEEE Trans. Veh. Technol.*, vol. 71, no. 3, pp. 2375–2384, Mar. 2022.
- [35] V. Jain, S. S. Kumar, G. Papaioannou, R. Happee, and B. Shyrokau, "Optimal trajectory planning for mitigated motion sickness: Simulator study assessment," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 10, pp. 10653–10664, Oct. 2023.
- [36] G. Papaioannou, Z. Htike, C. Lin, E. Siampis, S. Longo, and E. Velenis, "Multi-criteria evaluation for sorting motion planner alternatives," *Sensors*, vol. 22, no. 14, p. 5177, Jul. 2022.
- [37] T. Limbasiya, K. Z. Teng, S. Chattopadhyay, and J. Zhou, "A systematic survey of attack detection and prevention in connected and autonomous vehicles," *Veh. Commun.*, vol. 37, Oct. 2022, Art. no. 100515.
- [38] R. Rajamani and C. Zhu, "Semi-autonomous adaptive cruise control systems," *IEEE Trans. Veh. Technol.*, vol. 51, no. 5, pp. 1186–1192, Sep. 2002.
- [39] V. Linkov, P. Zámečník, D. Havlíčková, and C.-W. Pai, "Human factors in the cybersecurity of autonomous vehicles: Trends in current research," *Frontiers Psychol.*, vol. 10, p. 995, May 2019.
- [40] P. Wang, X. Wu, and X. He, "Modeling and analyzing cyberattack effects on connected automated vehicular platoons," *Transp. Res. C, Emerg. Technol.*, vol. 115, Jun. 2020, Art. no. 102625.
- [41] R. A. Shet and F. Schewe, "Performance evaluation of cruise controls and their impact on passenger comfort in autonomous vehicle platoons," in *Proc. IEEE 89th Veh. Technol. Conf. (VTC-Spring)*, Apr. 2019, pp. 1–7.
- [42] J. Kuang, G. Tan, X. Guo, X. Pei, and D. Peng, "Research of obstacle vehicles avoidance for automated heavy vehicle platoon by switching the formation," *IET Intell. Transp. Syst.*, vol. 18, no. 4, pp. 630–644, Apr. 2024.
- [43] J. Liu, Z. Wang, and L. Zhang, "Efficient eco-driving control for EV platoons in mixed urban traffic scenarios considering regenerative braking," *IEEE Trans. Transport. Electrific.*, vol. 10, no. 2, pp. 2988–3001, Jun. 2024.
- [44] S. Öncü, J. Ploeg, N. van de Wouw, and H. Nijmeijer, "Cooperative adaptive cruise control: Network-aware analysis of string stability," *IEEE Trans. Intell. Transp. Syst.*, vol. 15, no. 4, pp. 1527–1537, Aug. 2014.
- [45] M. Wolf, A. Weimerskirch, and C. Paar, "Security in automotive bus systems," in *Proc. Workshop Embedded Security Cars*, Apr. 2004, pp. 1–13.
- [46] A. Zhou, J. Wang, and S. Peeta, "Robust control strategy for platoon of connected and autonomous vehicles considering falsified information injected through communication links," *J. Intell. Transp. Syst.*, vol. 27, no. 6, pp. 735–751, Nov. 2023.
- [47] X. Jin, W. M. Haddad, Z.-P. Jiang, A. Kanellopoulos, and K. G. Vamvoudakis, "An adaptive learning and control architecture for mitigating sensor and actuator attacks in connected autonomous vehicle platoons," *Int. J. Adapt. Control Signal Process.*, vol. 33, no. 12, pp. 1788–1802, Dec. 2019.
- [48] M. Yadegar, N. Meskin, and W. M. Haddad, "An output-feedback adaptive control architecture for mitigating actuator attacks in cyber-physical systems," *Int. J. Adapt. Control Signal Process.*, vol. 33, no. 6, pp. 943–955, Jun. 2019.

- [49] N. Jahanshahi and R. M. G. Ferrari, "Attack detection and estimation in cooperative vehicles platoons: A sliding mode observer approach," *IFAC-PapersOnLine*, vol. 51, no. 23, pp. 212–217, 2018.
- [50] Z. Li, M. U. B. Niazi, C. Liu, Y. Mo, and K. H. Johansson, "Secure state estimation against sparse attacks on a time-varying set of sensors," *IFAC-PapersOnLine*, vol. 56, no. 2, pp. 270–275, 2023.
- [51] A. Petrillo, A. Pescapé, and S. Santini, "A collaborative control strategy for platoons of autonomous vehicles in the presence of message falsification attacks," in *Proc. 5th IEEE Int. Conf. Models Technol. Intell. Transp. Syst. (MT-ITS)*, Jun. 2017, pp. 110–115.
- [52] P. Kremer, I. Koley, S. Dey, and S. Park, "State estimation for attack detection in vehicle platoon using VANET and controller model," in *Proc. IEEE 23rd Int. Conf. Intell. Transp. Syst. (ITSC)*, Sep. 2020, pp. 1–8.
- [53] R. Merco, Z. A. Biron, and P. Pisu, "Replay attack detection in a platoon of connected vehicles with cooperative adaptive cruise control," in *Proc. Annu. Amer. Control Conf. (ACC)*, Jun. 2018, pp. 5582–5587.
- [54] J. Ploeg, N. van de Wouw, and H. Nijmeijer, "Lp string stability of cascaded systems: Application to vehicle platooning," *IEEE Trans. Control Syst. Technol.*, vol. 22, no. 2, pp. 786–793, Mar. 2014.
- [55] Z. Shen, Y. Liu, Z. Li, and M. H. Nabin, "Cooperative spacing sampled control of vehicle platoon considering undirected topology and analog fading networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 10, pp. 18478–18491, Oct. 2022.
- [56] V. Vegamoor, S. Rathinam, and S. Darbha, "String stability of connected vehicle platoons under lossy V2V communication," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 7, pp. 8834–8845, Jul. 2022.
- [57] K. Li, J. Wang, and Y. Zheng, "Cooperative formation of autonomous vehicles in mixed traffic flow: Beyond platooning," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 9, pp. 15951–15966, Sep. 2022.
- [58] S. Baldi, D. Liu, V. Jain, and W. Yu, "Establishing platoons of bidirectional cooperative vehicles with engine limits and uncertain dynamics," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 5, pp. 2679–2691, May 2021.
- [59] W. Yu, D. Ngoduy, X. Hua, and W. Wang, "On the stability of a heterogeneous platoon-based traffic system with multiple anticipations in the presence of connected and automated vehicles," *Transp. Res. C, Emerg. Technol.*, vol. 157, Dec. 2023, Art. no. 104389.
- [60] C. Zhao, X. Duan, L. Cai, and P. Cheng, "Vehicle platooning with non-ideal communication networks," *IEEE Trans. Veh. Technol.*, vol. 70, no. 1, pp. 18–32, Jan. 2021.
- [61] K. Halder, L. Gillam, S. Dixit, A. Mouzakitis, and S. Fallah, "Stability analysis with LMI based distributed H_∞ controller for vehicle platooning under random multiple packet drops," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 12, pp. 23517–23532, Dec. 2022.
- [62] R. G. Dutta, Y. Hu, F. Yu, T. Zhang, and Y. Jin, "Design and analysis of secure distributed estimator for vehicular platooning in adversarial environment," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 4, pp. 3418–3429, Apr. 2022.
- [63] T. Yang, "Multi-observer approach for estimation and control under adversarial attacks," Ph.D. dissertation, Dept. Elect. Electron. Eng., Univ. Melbourne, Melbourne, VIC, Australia, 2019.
- [64] E. D. Sontag, *Mathematical Control Theory: Deterministic Finite Dimensional Systems*, vol. 6. Cham, Switzerland: Springer, 2013.
- [65] J. C. Willems, "Deterministic least squares filtering," *J. Econometrics*, vol. 118, nos. 1–2, pp. 341–373, Jan. 2004.
- [66] J. Na, G. Herrmann, and K. G. Vamvoudakis, "Adaptive optimal observer design via approximate dynamic programming," in *Proc. Amer. Control Conf. (ACC)*, May 2017, pp. 3288–3293.
- [67] M. S. Chong, D. Nešić, R. Postoyan, and L. Kuhlmann, "Parameter and state estimation of nonlinear systems using a multi-observer under the supervisory framework," *IEEE Trans. Autom. Control*, vol. 60, no. 9, pp. 2336–2349, Sep. 2015.
- [68] S. Armaghan, A. Moridi, and A. K. Sedigh, "Design of a switching PID controller for a magnetically actuated mass spring damper," in *Proc. World Congr. Eng.*, 2020, pp. 6–8.
- [69] R. L. Williams and D. A. Lawrence, *Linear State-Space Control Systems*. Hoboken, NJ, USA: Wiley, 2007.
- [70] L. Li and F. Liao, "Design of a preview controller for discrete-time systems based on LMI," *Math. Problems Eng.*, vol. 2015, pp. 1–12, Apr. 2015.
- [71] T. Yang and C. Lv, "A secure sensor fusion framework for connected and automated vehicles under sensor attacks," *IEEE Internet Things J.*, vol. 9, no. 22, pp. 22357–22365, Nov. 2022.
- [72] G. J. L. Naus, R. P. A. Vugts, J. Ploeg, M. J. G. van de Molengraft, and M. Steinbuch, "String-stable CACC design and experimental validation: A frequency-domain approach," *IEEE Trans. Veh. Technol.*, vol. 59, no. 9, pp. 4268–4279, Nov. 2010.
- [73] S. Klinge and R. H. Middleton, "String stability analysis of homogeneous linear unidirectionally connected systems with nonzero initial conditions," in *Proc. IET Irish Signals Syst. Conf.*, May 2009, pp. 1–17.
- [74] N. An and S. Si, "Mechanical vibration and shock-evaluation of human exposure to whole-body vibration—Part 1: General requirements," Acoust. Soc. Amer. (Standards Secretariat), Melville, NY, USA, Tech. Rep. ANSI S2.72-2002, 1997.
- [75] G. Papaioannou, R. Desai, and R. Happee, "The impact of body and head dynamics on motion comfort assessment," 2023, *arXiv:2307.03608*.
- [76] B. Ko and S. H. Son, "An approach to detecting malicious information attacks for platoon safety," *IEEE Access*, vol. 9, pp. 101289–101299, 2021.
- [77] G. Karmakar, A. Chowdhury, R. Das, J. Kamruzzaman, and S. Islam, "Assessing trust level of a driverless car using deep learning," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 7, pp. 4457–4466, Jul. 2021.
- [78] Y. Nesterov and A. Nemirovskii, *Interior-Point Polynomial Algorithms in Convex Programming*. Philadelphia, PA, USA: SIAM, 1994.
- [79] H. Khalil, *Nonlinear Systems*. Upper Saddle River, NJ, USA: Prentice-Hall, 2002. [Online]. Available: https://books.google.nl/books?id=t_d1QgAACAAJ
- [80] Mechanical Vibration and Shock-Evaluation of Human Exposure to Whole Body Vibration. Part 1: General Requirements, Standard ISO2631, 1997.
- [81] S. J. Taylor, F. Ahmad, H. N. Nguyen, S. A. Shaikh, and D. Evans, "Safety, stability and environmental impact of FDI attacks on vehicular platoons," in *Proc. NOMS-IEEE/IFIP Netw. Oper. Manage. Symp.*, Apr. 2022, pp. 1–6.



Farzam Tajdari received the first Ph.D. degree from the School of Engineering, Aalto University, in 2023, and the second Ph.D. degree in mechatronic design engineering from Delft University of Technology in 2023. In 2023, he was a Post-Doctoral Researcher with the Mechanical Engineering Department at Eindhoven University of Technology, where he is currently a Guest Post-Doctoral Researcher. Since 2024, he has been a Post-Doctoral Researcher with the Faculty of Mechanical Engineering, Delft University of Technology. His research interests include control, non-linear systems, addressing challenges in the fields of ITS, privacy of dynamic systems, and geometry processing.



Georgios Papaioannou received the Ph.D. degree from the National Technical University of Athens (NTUA), Greece, in 2019, which received an award regarding its innovation and impact. He is currently an Assistant Professor of AVs at TU Delft, with a focus on motion comfort, after conducting post-doctoral research at the KTH Royal Institute of Technology, Sweden, and Cranfield University, U.K. His research interests include motion comfort, seat comfort, postural stability, human body modeling, automated vehicles, motion planning, and optimization and control.



Riender Happee received the Ph.D. degree from Delft University of Technology (TU Delft), The Netherlands, in 1992. He investigated road safety and introduced biomechanical human models for impact and comfort at TNO Automotive from 1992 to 2007. Currently, he investigates the human interaction with automated vehicles, focusing on motion comfort, perceived safety, and acceptance at TU Delft, where he is a Full Professor.