2024 IEEE 63rd Conference on Decision and Control (CDC)
December 16-19, 2024. MiCo, Milan, Italy

Optimal Controller Realizations against False Data Injections in Cooperative Driving

Mischa Huisman, Carlos Murguia, Erjen Lefeber, and Nathan van de Wouw

Abstract— **To enhance the robustness of cooperative driving to cyberattacks, we study a controller-oriented approach to mitigate the effect of a class of False-Data Injection (FDI) attacks. By reformulating a given dynamic Cooperative Adaptive Cruise Control scheme (the base controller), we show that a class of new but equivalent controllers (base controller realizations) can represent the base controller. This controller class exhibits the same platooning behavior in the absence of attacks, but in the presence of attacks, their robustness varies with the realization. We propose a prescriptive synthesis framework where the base controller and the system dynamics are written in new coordinates via an invertible coordinate transformation on the controller state. Because the input-output behavior is invariant under coordinate transformations, the input-output behavior is unaffected (so controller realizations do not change the system's closed-loop performance). However, each controller realization may require a different combination of sensors. Subsequently, we obtain the optimal combination of sensors that minimizes the effect of FDI attacks by solving a linear matrix inequality while quantifying the FDI's attack impact through reachability analysis. Through simulation studies, we demonstrate that this approach enhances the robustness of cooperative driving without relying on a detection scheme and maintaining all system properties.**

I. INTRODUCTION

Cooperative Adaptive Cruise Control (CACC) is a well-explored technology within Connected and Automated Vehicles (CAVs) that allows groups of vehicles to form tightly-coupled platoons by exchanging inter-vehicle data through Vehicle-to-Vehicle (V2V) wireless communication networks [1]-[3]. However, as CACC requires communication networks, network access points are exposed that adversaries can exploit for cyberattacks [4]-[7]. To counter these attacks, technologies are being developed to prevent and detect cyberattacks, increasing system security [6]-[9]. However, the effectiveness of current mitigation technology is limited by: (i) unknown process or measurement disturbances [10], [11], (ii) limited operating resources (e.g., computing power, budget) [12], and (iii) adversaries exploiting model knowledge [12], [13]. Therefore, technology is needed to enhance the robustness of cooperative driving to attacks on system elements such as sensors, actuators, networks, and software.

To address these challenges, the literature offers two control-theoretic approaches: (i) active methods that leverage attack detection to switch controllers and (ii) passive attack-resilient methods that seek to withstand the effect of attacks. The former relies on a detection scheme to notify the controller to switch towards a fallback mechanism (e.g., from CACC to adaptive cruise control [14]), while the latter often compromises the nominal performance (e.g., string stability [15]).

In this paper, we introduce a third controller-oriented approach to implement a given dynamic CACC scheme without affecting the input-output behavior of the closed-loop system, thereby preserving nominal performance. By reformulating the dynamic CACC scheme (the base controller), we show that the base controller can be represented by a class of equivalent realizations (base controller realizations). These realizations have equivalent nominal behavior with varying robustness in the presence of attacks. This approach enhances the robustness of cooperative driving without relying on a detection scheme and maintains system properties such as string stability.

We demonstrate that a different controller realization may require a different combination of sensors from a set of sensors, which could be subject to a resource-limited False Data Injection (FDI) attack. The effect of such an FDI attack can be quantified using reachability analysis to obtain the adversarial reachable set, which provides insight into the size of the state space portion that the FDI attack can induce [16]. Moreover, the reachable set provides insight into the potential damage an FDI attack can do to a platoon, e.g., cause a collision. To this end, we formulate a Semi-Definite Program (SDP) to obtain the optimal controller realization that minimizes the size of the adversarial reachable set. Moreover, the corresponding synthesis problem results in a Linear Matrix Inequality (LMI). A simulation study is conducted to support our claims, where the original CACC realization, an alternative formulation, and the optimal realization are compared. Our findings reveal that the optimal realization has the smallest size of the reachable set within the considered class of controllers.

The structure of the paper is as follows. Section II introduces preliminary results. Section III describes the general problem setting, including the platooning dynamics, the dynamic CACC scheme, and the available measurements. Section IV presents the class of controllers that can be derived from the given problem setting, after which the optimization problem is introduced. Section V presents the optimal realization, and a simulation study is conducted to demonstrate its performance. Finally, Section VI provides the concluding remarks.

The research leading to these results has received funding from the European Union's Horizon Europe programme under grant agreement No 101069748 – SELFY project.

M. Huisman, C. Murguia, E. Lefeber, and N. van de Wouw are with the Department of Mechanical Engineering, Eindhoven University of Technology, The Netherlands. [m.r.huisman, C.G.Murguia, A.A.J.Lefeber, N.v.d.Wouw]@tue.nl

II. Mathematical Preliminaries

A. Notation

The symbol $\mathbb{R}$ stands for the real numbers, $\mathbb{R}_{>0}$ ($\mathbb{R}_{\geq 0}$) denotes the set of positive (non-negative) real numbers. The symbol $\mathbb{N}$ denotes the set of natural numbers, including zero. The $n \times m$ matrix composed of only zeros is denoted by $\mathbf{0}_{n\times m}$, or $\mathbf{0}$ when its dimension is clear. Consider a finite index set $\mathcal{L} \coloneqq \{l_1, \ldots, l_\rho\} \subset \mathbb{N}$, then $\mathrm{diag}[B_j]$ and $(B_j), j \in \mathcal{L}$, stand for the diagonal block matrix $\mathrm{diag}[B_{l_1}, \ldots, B_{l_\rho}]$ and stacked block matrix $(B_{l_1}, \ldots, B_{l_\rho})$, respectively. The notation $A \geq 0$ (resp., $A \leq 0$) indicates that the matrix A is positive (resp., negative) semidefinite, i.e., all the eigenvalues of the symmetric matrix A are positive (resp. negative) or equal to zero, whereas $A > 0$ (resp., $(A < 0)$) indicates the positive (resp., negative) definiteness, i.e., all the eigenvalues are strictly positive (resp. negative). Time dependencies of signals are often omitted for simplicity of notation.

B. Definitions and Preliminary Results

Definition 1 (Reachable Set) [16] *Consider the perturbed Linear Time-Invariant (LTI) system:*

$$\zeta(k+1) = \mathcal{A}\zeta(k) + \sum_{i=1}^{N} \mathcal{B}_i \omega_i(k), \ \zeta(0) = \zeta_0, \tag{1}$$

with $k \in \mathbb{N}$, state $\zeta(k) \in \mathbb{R}^{n_\zeta}$, perturbation $\omega_i \in \mathbb{R}^{p_i}$ satisfying $\omega_i(k)^\top W_i \omega_i(k) \leq 1$ for some positive definite matrix $W_i \in \mathbb{R}^{p_i \times p_i}, i = \{1, ..., N\}, N \in \mathbb{N}$, and matrices $\mathcal{A} \in \mathbb{R}^{n_\zeta \times n_\zeta}$ and $\mathcal{B}_i \in \mathbb{R}^{n_\zeta \times p_i}$. The reachable set $\mathcal{R}^{\zeta_0}(k)$ at time $k \geq 0$ from the initial condition $\zeta_0 \in \mathbb{R}^{n_\zeta}$ is the set of states reachable in k steps by system (1) through all possible disturbances satisfying $\omega_i^\top(k) W_i \omega_i(k) \leq 1$, i.e.,

$$\mathcal{R}^{\zeta_0}(k) \coloneqq \left\{ \zeta \in \mathbb{R}^{n_\zeta} \;\middle|\; \begin{array}{c} \zeta = \zeta(k), \zeta(k) \text{ solution to (1),} \\ \text{and } \omega_i(k)^\top W_i \omega_i(k) \leq 1. \end{array} \right\}. \tag{2}$$

Lemma 1 (Ellipsoidal Approximation) [16] *Consider the perturbed LTI system (1) and the reachable set $\mathcal{R}^{\zeta_0}(k)$ in Definition 1. For a given $a \in (0,1)$, if there exist constants $a_1, \ldots, a_N$ and matrix P that is the solution of the convex program:*

$$\begin{cases} \min\limits_{P, a_1, \ldots, a_N} -\log\det[P], \\ \text{s.t. } a_1, \ldots, a_N \in (0,1),\ a_1 + \ldots + a_N \geq a, \\ P > 0, \begin{bmatrix} aP & \mathcal{A}^\top P & \mathbf{0} \\ P\mathcal{A} & P & P\mathcal{B} \\ \mathbf{0} & \mathcal{B}^\top P & W_a \end{bmatrix} \geq 0 \end{cases} \tag{3}$$

with matrices $W_a \coloneqq \mathrm{diag}[(1-a_1)W_1, \ldots, (1-a_N)W_N] \in \mathbb{R}^{\bar{p}\times\bar{p}}$, $\mathcal{B} \coloneqq (\mathcal{B}_1, \ldots, \mathcal{B}_N) \in \mathbb{R}^{n_{\zeta_0} \times \bar{p}}$, and $\bar{p} = \sum_{i=1}^{N} p_i$, then for all $k \in \mathbb{N}$, $\mathcal{R}^{\zeta_0}(k) \subseteq \mathcal{E}^{\zeta_0}(k)$ with $\mathcal{E}^{\zeta_0}(k) \coloneqq \{\zeta^\top(k) P^{\zeta_0} \zeta(k) \leq \alpha^{\zeta_0}(k)\}$, with convergent scalar sequence $\alpha^{\zeta_0}(k) \coloneqq a^{k-1}\zeta(k)^\top P^{\zeta_0}\zeta(k) + ((N-a)(1-a^{k-1}))/(1-a)$. Ellipsoid $\mathcal{E}^{\zeta_0}(k)$ has the minimum asymptotic volume among all outer ellipsoidal approximations of $\mathcal{R}^{\zeta_0}(k)$.

Lemma 2 (Projection) [16] *Consider the ellipsoid:*

$$\mathcal{E} \coloneqq \left\{ x \in \mathbb{R}^n, y \in \mathbb{R}^m \;\middle|\; \begin{bmatrix} x \\ y \end{bmatrix}^\top \begin{bmatrix} Q_1 & Q_2 \\ Q_2^\top & Q_3 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \alpha \right\}, \tag{4}$$

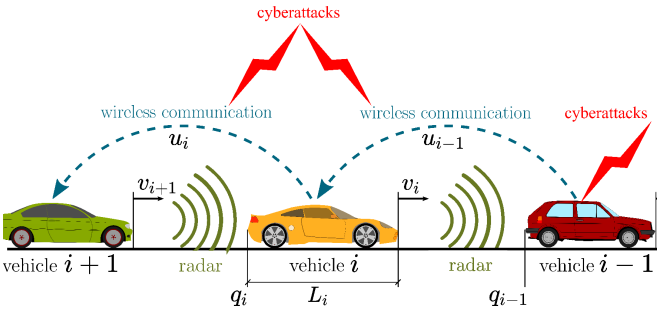

Fig. 1. CACC-equipped vehicle platoon. Each vehicle has onboard sensors (e.g., radars/LiDARs, cameras, and velocity/acceleration sensors). Vehicles may be subject to FDI attacks.

for some positive definite matrix $Q \in \mathbb{R}^{(n+m)\times(n+m)}$ and constant $\alpha \in \mathbb{R}_{>0}$. The projection $\mathcal{E}'$ of $\mathcal{E}$ onto the x-hyperplane is given by the ellipsoid:

$$\mathcal{E}' \coloneqq \left\{ x \in \mathbb{R}^n \;\middle|\; x^\top \left[Q_1 - Q_2 Q_3^{-1} Q_2^\top \right] x = \alpha \right\}. \tag{5}$$

III. Problem Setting

Consider a homogeneous platoon of m vehicles, schematically depicted in Fig. 1, where the vehicles are enumerated with index $i = 1, ..., m$, with $i = 1$ indicating the lead vehicle. To model such a platoon, we adopt the longitudinal vehicle model from [2]:

$$\begin{bmatrix} \dot{d}_i \\ \dot{v}_i \\ \dot{a}_i \end{bmatrix} = \begin{bmatrix} v_{i-1} - v_i \\ a_i \\ -\frac{1}{\tau} a_i + \frac{1}{\tau} u_i \end{bmatrix}, \ i \in S_m \backslash \{1\}, \tag{6}$$

where $d_i = q_{i-1} - q_i - L_i$ (q_i reflects the position of the rear bumper of vehicle i and L_i its length) being the distance between vehicle i and its preceding vehicle $i-1$, v_i, and a_i denoting the velocity, and acceleration of vehicle i, respectively, and $S_m \coloneqq \{i \in \mathbb{N} \mid 1 \leq i \leq m\}$ (i.e., the set of all vehicles in a platoon of length $m \in \mathbb{N}$). The desired acceleration u_i represents the control input, and $\tau > 0$ is a time constant modeling driveline dynamics.

The objective of each follower vehicle is to keep a desired distance $d_{r,i}$ (the so-called constant time-gap policy) with its preceding vehicle:

$$d_{r,i} = r + h v_i, \ i \in S_m \backslash \{1\} \tag{7}$$

with the time gap $h > 0$, and standstill distance $r > 0$. The spacing error is then defined as

$$e_i \coloneqq d_i - d_{r,i}. \tag{8}$$

To obtain the desired error dynamics, in [1] a CACC controller is introduced to achieve string-stable vehicle-following behavior at small inter-vehicle distances for a homogeneous platoon. This CACC controller is a dynamic controller of the following form:

$$\mathcal{C} \coloneqq \begin{cases} u_i = \rho_i, \\ \dot{\rho}_i = -\frac{1}{h}\rho_i + \frac{1}{h}(k_p e_i + k_d \dot{e}_i) + \frac{1}{h} u_{i-1}, \end{cases} \tag{9}$$

which stabilizes the resulting error dynamics in (8). The constants $k_p > 0$ and $k_d > 0$ are control gains to be designed. An alternative to (9) is the CACC controller introduced in [3], which results in the same control signal u_i at the vehicle

but is now also applicable for heterogeneous platoons. This CACC controller is also dynamic and of the following form:

$$\hat{\mathcal{C}} \coloneqq \begin{cases} \hat{u}_i = -\frac{\tau}{h}\hat{\rho}_i + (1-\frac{\tau}{h})a_i + \frac{\tau}{h}a_{i-1}, \\ \dot{\hat{\rho}}_i = -\frac{1}{\tau}\hat{\rho}_i - \frac{1}{\tau_i}(k_p e_i + k_d \dot{e}_i). \end{cases} \tag{10}$$

Note that the real-time realization of any control scheme depends on the available sensors $y_{i,j}$ (sensor number j of vehicle i). Considering a combination of sensor data coming from onboard sensors (e.g., LiDAR, radar, cameras, and velocity/acceleration sensors) and wirelessly received data from adjacent vehicles, we assume to have the following sensors to realize controllers $\mathcal{C}$ and $\hat{\mathcal{C}}$:

$$\begin{aligned} y_{i,1} &\coloneqq d_i + \delta_{i,1}, & y_{i,2} &\coloneqq v_i + \delta_{i,2}, \\ y_{i,3} &\coloneqq a_i + \delta_{i,3}, & y_{i,4} &\coloneqq v_{i-1} - v_i + \delta_{i,4}, \\ y_{i,5} &\coloneqq a_{i-1} + \delta_{i,5}, & y_{i,6} &\coloneqq u_{i-1} + \delta_{i,6}. \end{aligned} \tag{11}$$

Herein, $\delta_{i,j}$ models potential FDI attacks. Sensors $y_{i,1}$ and $y_{i,4}$ provide relative distance and velocity information, $y_{i,2}$ and $y_{i,3}$ denote the onboard measured velocity and acceleration, while $y_{i,5}$ and $y_{i,6}$ model data received from the preceding vehicle via V2V communication. Using (11), it can be observed that a difference in realization between $\mathcal{C}$ and $\hat{\mathcal{C}}$ is the use of sensors $y_{i,6}$ and $y_{i,5}$, respectively. The findings in [17] show that both controller realizations yield the same control input u_i when $\delta_{i,j} = 0$; however, this equivalence is not guaranteed when $\delta_{i,j} \neq 0$.

By applying a linear coordinate transformation to the internal state of the dynamic controller (9), also known as a similarity transformation, infinitely many real-time realizations of (9) exist using sensors from (11) ($\hat{\mathcal{C}}$ is just one of these realizations). Therefore, the problem we address in this paper is determining the optimal controller realization for (9), which minimizes the impact of resource-limited adversaries. The effect of a resource-limited FDI attack can be quantified using the size of the reachable set induced by such an attack. By minimizing the size of the adversarial reachable set, we select an optimal combination of sensors and the corresponding controller realizations to mitigate the effect of a potential FDI attack on the closed-loop dynamics.

IV. Approach for Optimal Controller Realization

A. Controller Realization

One could interpret the difference between the CACC controllers in (9) and (10) as a coordinate transformation on the internal control variable ρ_i. Therefore, we propose to find the class of controllers that yields the same control signal u_i while using the system output y_i by applying the following coordinate transformation

$$\bar{\rho}_i = \alpha_i \rho_i + \underbrace{\begin{bmatrix}\beta_{i,1} & \beta_{i,2} & \beta_{i,3} & \beta_{i,4} & \beta_{i,5} & 0\end{bmatrix}}_{\beta_i} y_i \tag{12}$$

with new controller state $\bar{\rho}_i$. The goal is to determine the optimal values for both $\alpha_i \in \mathbb{R}$ and $\beta_i \in \mathbb{R}^{n_y}$ (n_y number of measurements) to reduce the impact of FDI attacks. Note that in the proposed change of coordinates $\beta_{i,6} = 0$ (excluding $y_{i,6}$), as this would require information about $\dot{u}_{i-1}$, and thus also knowledge about the control structure of vehicle $i-1$ (and possibly sensor data from vehicle $i-2$).

The closed-loop system formulation is adopted from [3], where it was observed that the resulting closed-loop dynamics, with output e_i and input u_i, has the relative degree two. Therefore, we differentiate the output e_i twice and then investigate the resulting internal dynamics. To this end, we define the stacked state vector $x = [e_i \ \dot{e}_i \ z_i \ v_{i-1} \ a_{i-1}]^\top$, where $z_i \coloneqq v_{i-1} - v_i$ is the internal dynamic state. Using (6) and (8) we obtain the platooning dynamics of the form:

$$\dot{x} = Ax + B_1 u_i + B_2 u_{i-1}, \tag{13}$$

where

$$A = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & \frac{1}{h} - \frac{1}{\tau} & \frac{1}{\tau} - \frac{1}{h} & 0 & 1 \\ 0 & \frac{1}{h} & -\frac{1}{h} & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & -\frac{1}{\tau} \end{bmatrix}, B_1 = \begin{bmatrix} 0 \\ -\frac{h}{\tau} \\ 0 \\ 0 \\ 0 \end{bmatrix}, B_2 = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ \frac{1}{\tau} \end{bmatrix}, \tag{14}$$

and by substituting the base controller from (9) we obtain:

$$\begin{bmatrix} \dot{x} \\ \dot{\rho}_i \end{bmatrix} = \underbrace{\begin{bmatrix} A & B_1 \\ K & -\frac{1}{h} \end{bmatrix}}_{\mathcal{A}} \begin{bmatrix} x \\ \rho_i \end{bmatrix} + \underbrace{\begin{bmatrix} B_2 \\ \frac{1}{h} \end{bmatrix}}_{\mathcal{B}_{u_{i-1}}} u_{i-1}, \tag{15}$$

as the closed-loop dynamics, where $K = [\frac{k_p}{h} \ \ \frac{k_d}{h} \ \ 0 \ \ 0 \ \ 0]$.

The sensor measurements in (11) can be expressed in terms of the closed-loop coordinates and disturbance u_{i-1}, as the coordinate transformation from $[d_i \ v_i \ a_i \ v_{i-1} \ a_{i-1}]^\top$ to $[e_i \ \dot{e}_i \ z_i \ v_{i-1} \ a_{i-1}]^\top$ is invertible. For $\delta_i = 0$, we obtain:

$$y_i = \underbrace{\begin{bmatrix} 1 & 0 & -h & h & 0 \\ 0 & 0 & -1 & 1 & 0 \\ 0 & -\frac{1}{h} & \frac{1}{h} & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}}_{C} \begin{bmatrix} e_i \\ \dot{e}_i \\ z_i \\ v_{i-1} \\ a_{i-1} \end{bmatrix} + \underbrace{\begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}}_{D} u_{i-1}. \tag{16}$$

Given that $(C, \ D)$ is full rank, (16) can be rewritten as:

$$\begin{bmatrix} x \\ u_{i-1} \end{bmatrix} = [C \ \ D]^{-1} y_i. \tag{17}$$

To derive the class of base controller realizations, $\dot{\rho}_i$ in (9) is first reformulated using the proposed change of coordinates in (12) and subtituting (17), resulting in

$$\dot{\rho}_i = -\tfrac{1}{\alpha_i h}\bar{\rho}_i + \left([K \ \ \tfrac{1}{h}][C \ \ D]^{-1} + \tfrac{1}{\alpha_i h}\beta_i\right) y_i. \tag{18}$$

The dynamics of $\bar{\rho}_i$ are then obtained by differentiating (12),

$$\begin{aligned} \dot{\bar{\rho}}_i &= \alpha_i \dot{\rho}_i + \beta_i \dot{y}_i \\ &= \alpha_i \dot{\rho}_i + \beta_i (C\dot{x} + D\dot{u}_{i-1}), \end{aligned} \tag{19}$$

where due to the structure of β_i and D we have that $\beta_i D = 0$. Substitution of (13) and (17) provides that:

$$\dot{\bar{\rho}}_i = \alpha_i \dot{\rho}_i + \beta_i C[A \ \ B_2][C \ \ D]^{-1} y_i + \beta_i C B_1 u_i. \tag{20}$$

The new formulation of the control input u_i is obtained by applying the change of coordinates to (9), resulting in

$$u_i = \tfrac{1}{\alpha_i}\bar{\rho}_i - \tfrac{1}{\alpha_i}\beta_i y_i. \tag{21a}$$

Substitution of (18) and (21a) into (20) yields:

$$\begin{aligned}\dot{\bar{\rho}}_i = &(\tfrac{1}{\alpha_i}\beta_i CB_1 - \tfrac{1}{h})\bar{\rho}_i + \Big(\big(\alpha_i[K \quad \tfrac{1}{h}]+\\ &\beta_i C[A \quad B_2]\big)[C \quad D]^{-1}+\tfrac{1}{h}\beta_i-\tfrac{1}{\alpha_i}\beta_i CB_1\beta_i\Big)\, y_i.\end{aligned} \tag{21b}$$

Consequently, (21) represents the class of controller realizations of (9), which exhibit equivalent closed-loop behavior without an FDI attack. Notice that for $\alpha_i = 1, \beta_i = 0$, or for $\alpha_i = -\frac{\tau}{h}, \beta_i = [0 \quad 0 \quad (1-\frac{\tau}{h}) \quad 0 \quad \frac{\tau}{h} \quad 0]$, the controller realizations $\mathcal{C}$ or $\hat{\mathcal{C}}$ are obtained, respectively. Note that, (21) is derived for $\delta_i = 0$ to find all equivalent controller realizations that exhibit equivalent closed-loop behavior.

However, the change of coordinates affects the combinations of sensors being used and, therefore, also influences the effect of an FDI on the closed-loop behavior. To model the effect of FDI attacks, we now derive (21) for $\delta_i \neq 0$ by reformulating (16) by including FDI attack signals δ_i:

$$y_i = [C \quad D]\begin{bmatrix} x \\ u_{i-1}\end{bmatrix} + \delta_i. \tag{22}$$

Substitution of (22) into (21) yields the realized controller in presence of FDI attacks,

$$u_i = \tfrac{1}{\alpha_i}\bar{\rho}_i - \tfrac{1}{\alpha_i}\beta_i[C \quad D]\begin{bmatrix} x \\ u_{i-1}\end{bmatrix} - \tfrac{1}{\alpha_i}\beta_i\delta_i, \tag{23a}$$

$$\begin{aligned}\dot{\bar{\rho}}_i = &(\tfrac{1}{\alpha_i}\beta_i CB_1 - \tfrac{1}{h})\bar{\rho}_i + \big(\alpha_i[K \quad \tfrac{1}{h}] + \beta_i C[A \quad B_2]\\ &+(\tfrac{1}{h}\beta_i - \tfrac{1}{\alpha_i}\beta_i CB_1\beta_i)[C \quad D]\big)\begin{bmatrix} x \\ u_{i-1}\end{bmatrix}\\ &+ \big(\big(\alpha_i[K \quad \tfrac{1}{h}] + \beta_i C[A \quad B_2]\big)[C \quad D]^{-1}\\ &+\tfrac{1}{h}\beta_i - \tfrac{1}{\alpha_i}\beta_i CB_1\beta_i\big)\delta_i.\end{aligned} \tag{23b}$$

When deriving the closed-loop system using (13) and (23), the system matrices $\bar{\mathcal{A}}(\alpha_i, \beta_i)$ and $\bar{\mathcal{B}}_{u_{i-1}}(\alpha_i, \beta_i)$ are dependent on the choice of α_i and β_i. Although different sensors are used, the realization does not affect the nominal closed-loop behavior. This is because the input-output behavior of the closed-loop system is invariant under a linear coordinate transformation, commonly referred to as a similarity transformation. Therefore, after selecting the required combination of sensors (including δ_i), the closed-loop system is transformed back to its original coordinates $[x \quad \rho_i]^\top$ as in (15). As we show below: (i) a fair comparative analysis is made between different realizations, as $\mathcal{A}$ and $\mathcal{B}_{u_{i-1}}$ in (15) are independent of α_i and β_i, and therefore only $\mathcal{B}_{\delta_i}$ is dependent on α_i and β_i, and (ii) the resulting dynamics are affine in $\frac{1}{\alpha_i}\beta_i$, allowing for linear and convex optimization techniques, whereas solving it in the new coordinates requires nonlinear optimization techniques. To prove the latter, note that the change of coordinates in (12) is invertible for $\alpha_i \neq 0$:

$$\begin{bmatrix} x \\ \bar{\rho}_i\end{bmatrix} = \begin{bmatrix} I & 0 \\ \beta_i C & \alpha_i\end{bmatrix}\begin{bmatrix} x \\ \rho_i\end{bmatrix}. \tag{24}$$

By applying the inverse coordinate transformation to the closed-loop system of (13) using (23), the original closed-loop system (15) is obtained. However, now the closed-loop dynamics include a matrix that represents the effect of an FDI attack on the closed-loop system dynamics (depending on the realization of the controller):

$$\begin{bmatrix} \dot{x} \\ \dot{\rho}_i\end{bmatrix} = \mathcal{A}\begin{bmatrix} x \\ \rho_i\end{bmatrix} + \mathcal{B}_{u_{i-1}}u_{i-1} + \mathcal{B}_{\delta_i}\delta_i, \tag{25a}$$

where

$$\mathcal{B}_{\delta_i} = \begin{bmatrix} -\frac{1}{\alpha_i}B_1\beta_i \\ \Big([K \quad \frac{1}{h}]+\frac{1}{\alpha_i}\beta_i C[A \quad B_2]\Big)[C \quad D]^{-1}+\frac{1}{h\alpha_i}\beta_i\end{bmatrix}. \tag{25b}$$

Note that when converting the system back to its original coordinates, only the attack matrix $\mathcal{B}_{\delta_i}$ is affected by the choice of α_i and β_i. The following section introduces an optimization scheme to find the optimal realization of the base controller within the suggested class of realized controllers.

B. Optimization Problem

In search of the optimal controller realization, we aim to minimize the reachable set induced by resource-limited FDI attacks on the closed-loop dynamics. FDI attacks manipulate sensing, actuation, and networked data while constrained by physical limitations, computing power, and attack strategy [11]. We use the volume of these reachable sets as a security metric, whereas minimizing the volume directly reduces the size of the state space portion that can be induced by a series of attacks [16]. Computing the exact reachable set is generally not tractable and time-dependent. Instead, we seek to minimize the volume of the outer ellipsoidal approximation of the reachable set.

Computing the reachable set for (25a) is not possible, due to v_{i-1} and a_{i-1} being uncontrollable states, introducing zero-eigenvalues in $\mathcal{A}$. However, note that v_{i-1} and a_{i-1} are fully decoupled from the other states (see (14), (15)). Moreover, the choice of α_i and β_i does not affect v_{i-1} and a_{i-1}, as the attack only affects the dynamics of $\dot{e}_i$ and ρ_i. Therefore, (25a) is reformulated

$$\begin{bmatrix} \dot{x}_i \\ \dot{\rho}_i\end{bmatrix} = \mathcal{A}_i\begin{bmatrix} x_i \\ \rho_i\end{bmatrix} + \mathcal{B}_{i,i-1}\begin{bmatrix} x_{i-1} \\ u_{i-1}\end{bmatrix} + \mathcal{B}_{i,\delta_i}\delta_i, \tag{26}$$

where $x_i = [e_i \ \dot{e}_i \ z_i]^\top$, $x_{i-1} = [v_{i-1} \ a_{i-1}]^\top$, $\mathcal{A}_i$ and $\mathcal{B}_{i,i-1}$ derived from (15), and $\mathcal{B}_{i,\delta_i}$ as $\mathcal{B}_{\delta_i}$ in (25b) but excluding the zero entries for $\dot{v}_{i-1}$ and $\dot{a}_{i-1}$.

In (26), x_{i-1} and u_{i-1} act as input on the platooning dynamics. Assuming boundedness of x_{i-1} and u_{i-1}, which is reasonable considering vehicle physical constraints, a reachable set can be found for $\delta_i = 0$ due to the additional disturbances entering through $\mathcal{B}_{i,i-1}$. However, the ellipsoidal approximation of the reachable set for (26) with $\delta_i \neq 0$ can be obtained by the Minkowski sum of two independent ellipsoidal approximations of the reachable sets induced by the inputs associated to $\mathcal{B}_{i,i-1}$ and $\mathcal{B}_{i,\delta_i}$ separately [18]. Therefore, we discard the effect of $\mathcal{B}_{i,i-1}$, as the optimal α_i and β_i do not affect this reachable set. Moreover, we are only interested in minimizing the reachable set induced by $\mathcal{B}_{i,\delta_i}$ to enhance robustness against FDI attacks. To this end, for the synthesis of the optimal realization, (26) is modeled as if it is only perturbed by δ_i:

$$\begin{bmatrix} \dot{\tilde{x}}_i \\ \dot{\tilde{\rho}}_i\end{bmatrix} = \mathcal{A}_i\begin{bmatrix} \tilde{x}_i \\ \tilde{\rho}_i\end{bmatrix} + \mathcal{B}_{i,\delta_i}\delta_i, \tag{27}$$

where $\tilde{x}_i$ is used to distinguish the platooning dynamics in (26) and (27), as these represent different dynamical systems.

Given the fact that the realized controller operates in discrete time, and attacks operate on sampled signals, a discrete-time equivalent model of (27) is obtained via exact discretization at the sampling time instant, $t = T_s k$, $k \in \mathbb{N}$, where $T_s > 0$ is the sampling interval. We assume a zero-order hold on control input $u(t)$ and sampling on the FDI attack $\delta_i(t)$. The resulting discrete-time model yields:

$$\tilde{x}_i(k+1) = \mathcal{A}_i^d \tilde{x}_i(k) + \mathcal{B}_{i,\delta_i}^d \delta_i(k), \ \tilde{x}_i(0) = \tilde{x}_{i,0} \quad (28a)$$

with

$$\mathcal{A}_i^d = e^{\mathcal{A}_i T_s}, \quad \mathcal{B}_{i,\delta_i}^d = \left(\int_0^{T_s} e^{\mathcal{A}_i (T_s - s)} ds \right) \mathcal{B}_{i,\delta_i}. \quad (28b)$$

On $\delta_i(k)$ we impose the constraints of the form

$$\delta_{i,j}(k) \in \{\delta_{i,j} \mid \delta_{i,j}^2 \leq W_{i,j}^2\}, \forall k \in \mathbb{N}, \quad (29)$$

for some known constants $W_{i,j} \in \mathbb{R}_{>0}, j \in \{1, 2, .., 6\}$. Associated with these constraints, the adversarial reachable set (Definition 1) is introduced

$$\mathcal{R}^{\tilde{x}_{i,0}}(k) := \left\{ \tilde{x}_i \in \mathbb{R}^4 \middle| \begin{array}{l} \tilde{x}_{i,0} = \tilde{x}_i(0), \\ \tilde{x}_i(k) \text{ solution to (28a)}, \\ \delta_i(k) \text{ satisfies (29)}. \end{array} \right\} \quad (30)$$

We seek to obtain the outer ellipsoidal approximation $\mathcal{E}^{\tilde{x}_i}(k)$ of $\mathcal{R}^{\tilde{x}_{i,0}}(k)$ via Lemma 1. Moreover, we have that $\mathcal{E}^{\tilde{x}_i}(k) \approx \mathcal{E}^{\tilde{x}_i}(\infty) := \{\tilde{x}_i \mid \tilde{x}_i^\top \mathcal{P}^{\tilde{x}_i} \tilde{x}_i \leq (N-a)/(1-a)\}$, for some positive definite matrix $\mathcal{P}^{\tilde{x}_i} \in \mathbb{R}^{4\times 4}$. Considering the reachable set at infinity, the ellipsoidal approximation is independent of the initial condition, given that $\mathcal{A}_i^d$ is Schur.

By applying Lemma 1, $\mathcal{P}^{\tilde{x}_i}$ can be found, where $\mathcal{A} = \mathcal{A}_i^d$, $\mathcal{B} = \mathcal{B}_{i,\delta_i}^d$, with $\mathcal{A}_i^d$ and $\mathcal{B}_{i,\delta_i}^d$ as formulated in (28b). However, the goal is to solve (3) by minimizing $-\log\det[\mathcal{P}^{\tilde{x}_i}]$, while also optimizing α_i and β_i, leading to a non-linear optimization problem. To this end, the SDP problem in Lemma 1 is converted to a problem formulation that is affine in both $\mathcal{P}^{\tilde{x}_i}$ and $\mathcal{B}_{i,\delta_i}^d(\alpha_i, \beta_i)$. A congruence transformation of the form $QWQ^\top \geq 0$ is applied, with $W \geq 0$ and $Q = Q^\top = \text{diag}[(\mathcal{P}^{\tilde{x}_i})^{-1}, (\mathcal{P}^{\tilde{x}_i})^{-1}, I] > 0$, which preserves the definiteness of the matrix inequality [19]. Applying this congruence transformation to Lemma 1 yields

$$\begin{bmatrix} a(\mathcal{P}^{\tilde{x}_i})^{-1} & (\mathcal{P}^{\tilde{x}_i})^{-1}(\mathcal{A}_i^d)^\top & \mathbf{0} \\ \mathcal{A}_i^d(\mathcal{P}^{\tilde{x}_i})^{-1} & (\mathcal{P}^{\tilde{x}_i})^{-1} & \mathcal{B}_{i,\delta_i}^d(\alpha_i, \beta_i) \\ \mathbf{0} & (\mathcal{B}_{i,\delta_i}^d(\alpha_i, \beta_i))^\top & W_a \end{bmatrix} \geq 0, \quad (31)$$

which is now linear in both $\mathcal{P}^{\tilde{x}_i}$ and $\mathcal{B}_{i,\delta_i}^d$. Moreover, the resulting SDP is now an LMI.

However, when applying the congruence transformation, the resulting objective function $\min -\log\det[(\mathcal{P}^{\tilde{x}_i})^{-1}]$ becomes concave. Therefore, we alternatively seek to minimize a convex upper bound on $\sqrt{\det[(\mathcal{P}^{\tilde{x}_i})^{-1}]}$, which is proportional to the volume of the ellipsoid, from which also the original objective $\log\det[\mathcal{P}^{\tilde{x}_i}]$ is derived. To this end, we minimize $\text{tr}[Y]$, where $Y = (\mathcal{P}^{\tilde{x}_i})^{-1}$ [16]. Additionally, $\mathcal{B}_{i,\delta_i}^d(\alpha_i, \beta_i)$ is affine in $\frac{1}{\alpha_i}\beta_i$, where α_i only scales β_i and hence does not affect the reachable set. Therefore, w.l.o.g., the SDP is solved for $\alpha_i = 1 \ \forall i \in S_m \backslash \{1\}$, resulting in the following optimization problem:

$$\begin{cases} \underset{Y, \beta_i, a_1, \ldots, a_N}{\text{minimize}} \ \text{tr}[Y], \\ \textit{s.t. } a_1, \ldots, a_N \in (0,1), \ a_1 + \ldots + a_N \geq a, \\ Y > 0, \begin{bmatrix} aY & Y(\mathcal{A}_i^d)^\top & \mathbf{0} \\ \mathcal{A}_i^d Y & Y & \mathcal{B}_{i,\delta_i}^d(\beta_i) \\ \mathbf{0} & (\mathcal{B}_{i,\delta_i}^d(\beta_i))^\top & W_a \end{bmatrix} \geq 0. \end{cases} \quad (32)$$

This minimization problem is solved in the following section to optimize the realization of $\mathcal{C}$.

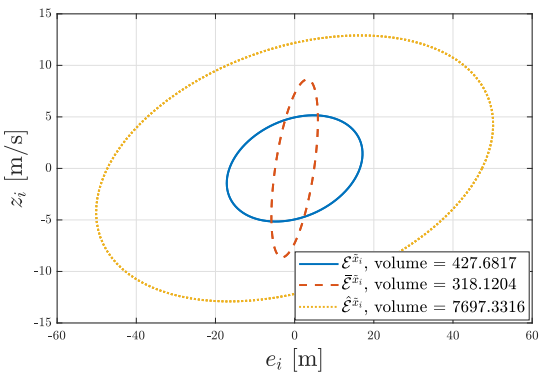

Fig. 2. Projection of the outer ellipsoidal approximation of the reachable set in (28a) for the different controller realizations $\mathcal{C}$, $\bar{\mathcal{C}}$, and $\hat{\mathcal{C}}$. Results are projected onto the z_i-e_i plane, given that $\delta_i \neq 0$, and $W_i = I$.

V. Results

In this section, the optimization problem introduced in (32) is solved to determine the optimal realization of the base controller in (9). We adopt the controller settings from [1], with a desired inter-vehicle distance of $r = 3\,\text{m}$, with driveline dynamics constant $\tau = 0.1\,\text{s}$, time headway constant $h = 0.5\,\text{s}$, and controller gains of $(k_p, k_d) = (0.2, 0.7)$. The sampling rate is $T_s = 0.01\,\text{s}$. For the resource-limited FDI attacks $\delta_{i,j}(k)$, we assume adherence to the bound specified in (29) with $W_i = I$, thereby considering FDI attacks on all sensors. The bound W_i is arbitrarily chosen to illustrate the results. The resulting LMI is solved using YALMIP [20], with SDP solver SDPT3 [21], providing the optimal realization $\bar{\mathcal{C}}$:

$$\bar{\mathcal{C}} := \begin{cases} \bar{u}_i = \bar{\rho}_i + 0.771 y_{i,1} - 0.33 y_{i,2} \\ \quad - 0.135 y_{i,3} + 1.672 y_{i,4} + 0.187 y_{i,5}, \\ \dot{\bar{\rho}}_i = -0.65 \bar{\rho}_i - 1.142 y_{i,1} + 0.46 y_{i,2} \\ \quad + 0.222 y_{i,3} - 2.715 y_{i,4} - 0.176 y_{i,5} + 0.13 y_{i,6}. \end{cases} \quad (33)$$

Notably, the optimal realization $\bar{\mathcal{C}}$ maximizes robustness against δ_i by utilizing all available sensors in (16).

In Fig. 2, the outer ellipsoidal approximation of the state of (28a) (using Lemma 1) is projected on the e_i-z_i plane (using Lemma 2). Among the three controllers, despite being derived from minimizing the upper bound on the volume, $\bar{\mathcal{C}}$ has the smallest ellipsoidal approximation ($\bar{\mathcal{E}}^{\tilde{x}_i}$) in terms of volume, therefore being the most robust realization. However, the projections in Fig. 2 indicate there exists some attack where $\mathcal{C}$ is more robust than $\bar{\mathcal{C}}$, as $\bar{\mathcal{E}}^{\tilde{x}_i} \not\subseteq \mathcal{E}^{\tilde{x}_i}$.

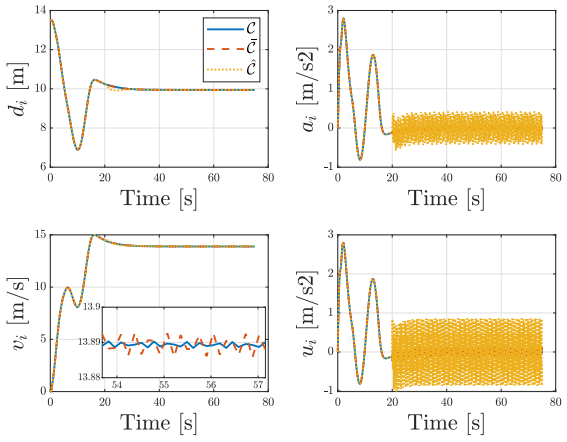

Fig. 3. Vehicle and controller response for the different controller realizations $\mathcal{C}$, $\bar{\mathcal{C}}$, and $\hat{\mathcal{C}}$, given an FDI attack on $y_{i,3}$, where $\delta_{i,3} = \sin(3t)\ \forall t \in [20, 75]$ s.

As a case study, all three controllers are implemented in a MATLAB Simulink simulation. The vehicles are modeled via the platooning dynamics in (6), where the controllers in (9), (10), and (33) are used to control three different platoons. Each platoon consists of a follower (vehicle i), controlled via one of the realized controllers, and a leader vehicle (vehicle $i-1$), controlled via a cruise controller. The leader aims to drive a steady-state velocity of 50 km/h while accelerating and braking in the initial stage, resulting in some transient platooning behavior. In the simulation vehicle i is subject to a FDI attack on $y_{i,3}$, representing the onboard acceleration measurement, where $\delta_{i,3} = \sin(3t)\ \forall t \in [20, 75]$s.

The results in Fig. 3 show that in the initial stage the different controller realizations exhibit equivalent platooning behavior, as the platooning behavior is invariant under the coordinate transformation. During the FDI, controller $\mathcal{C}$ shows the least magnitude amplification of $\delta_{i,3}$, which corresponds with the results obtained in Fig. 2, where $\bar{\mathcal{E}}^{\tilde{x}_i} \not\subseteq \mathcal{E}^{\tilde{x}_i}$, indicating $\bar{\mathcal{C}}$ is less robust that $\mathcal{C}$ for some FDI.

VI. CONCLUSIONS AND FUTURE WORKS

Cooperative driving must ensure safety and reliability in adversarial environments. To this end, we introduce the choice for a dynamic controller realization as a third controller-oriented approach to enhance the robustness of cooperative driving to cyberattacks. By reformulating a given dynamic CACC scheme, a class of equivalent controller realizations exists, having equivalent nominal behavior with varying robustness in the presence of attacks.

Furthermore, a framework is introduced to find the optimal subset of sensors to realize the controller by minimizing the effect of FDI attacks, quantified using reachability analysis. To show our findings, three different CACC realizations are compared, one of which is the optimal realization. The optimal realization is shown to have the smallest reachable set; however, real-time simulations show that attacks still exist where different realizations are more robust. Hence, a direction of further research would be to investigate different optimization strategies to find the best realization. Another line of research concerns controller realization, considering a detection scheme that provides a more accurate bound on the FDI attacks.

REFERENCES

[1] J. Ploeg, B. T. M. Scheepers, van Nunen, N. van de Wouw, and H. Nijmeijer, "Design and Experimental Evaluation of Cooperative Adaptive Cruise Control", in *IEEE Conference on Intelligent Transportation Systems (ITSC)*, p. 260–265, 2011.

[2] J. Ploeg, E. Semsar-Kazerooni, G. Lijster, N. van de Wouw, and H. Nijmeijer, "Graceful Degradation of CACC Performance Subject to Unreliable Wireless Communication", in *IEEE Conference on Intelligent Transportation Systems (ITSC)*, p. 1210–1216, 2013.

[3] E. Lefeber, J. Ploeg, and H. Nijmeijer, "Cooperative Adaptive Cruise Control of Heterogeneous Vehicle Platoons", in *IFAC-PapersOnLine*, vol. 53, no. 2, p. 15217–15222, 2020.

[4] M. Amoozadeh, A. Raghuramu, C. Chuah, D. Ghosal, M. Zhang, J. Rowe, and K. Levitt, "Security Vulnerabilities of Connected Vehicle Streams and Their Impact on Cooperative Driving", in *IEEE Communications Magazine*, vol. 53, p. 126–132, 2015.

[5] Z. El-Rewini, K. Sadatsharan, D. F. Selvaraj, S. J. Plathottam, and P. Ranganathan, "Cybersecurity Challenges in Vehicular Communications", in *Vehicular Communications*, vol. 23, p. 100214, 2020.

[6] Z. Ju, H. Zhang, X. Li, X. Chen, J. Han, and M. Yang, "A Survey on Attack Detection and Resilience for Connected and Automated Vehicles: From Vehicle Dynamics and Control Perspective," in *IEEE Transactions on Intelligent Vehicles*, vol. 7, p. 815–837, 2022.

[7] X. Sun, F. R. Yu, and Z. Zhang, "A Survey on Cyber-Security of Connected and Autonomous Vehicles (CAVs)", in *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 7, p. 6240–6259, 2022.

[8] A. Teixeira, I. Shames, H. Sandberg, and K. H. Johansson, "A Secure Control Framework for Resource-Limited Adversaries, in *Automatica*, vol. 51, p. 135–148, 2015.

[9] A. Chowdhury, G. Karmakar, J. Kamruzzaman, A. Jolfaei, and R. Das, "Attacks on Self-Driving Cars and Their Countermeasures: A Survey", in *IEEE Access*, vol. 8, p. 207308–207342, 2020.

[10] A. Teixeira, D. Pérez, H. Sandberg, and K. H. Johansson, "Attack models and scenarios for networked control systems", in *Proceedings of the 1st international conference on High Confidence Networked Systems*, p. 55-64, 2012.

[11] X.-M. Zhang, Q.-L Han, X. Ge et al., "Networked Control Systems: A Survey of Trends and Techniques", in *IEEE/CAA Journal of Automotica Sinica*, p. 1-17, 2019.

[12] S. C. Anand, A. M. H. Teixeira, and A. Ahlen, "Risk assessment and optimal allocation of security measures under stealthy false data injection attacks", in *2022 IEEE Conference on Control Technology and Applications (CCTA)*, p. 1347—1353, 2022.

[13] A. Teixeira, H. Sandberg and K. H. Johansson, "Strategic stealthy attacks: The output-to- output L2-gain", in *2015 54th IEEE Conference on Decision and Control (CDC)*, p. 2582—2587, 2015.

[14] R. van der Heijden, T. Lukaseder, and F. Kargl, "Analyzing Attacks on Cooperative Adaptive Cruise Control (CACC)", in *IEEE Vehicular Networking Conference (VNC)*, p. 45–52, 2017.

[15] M. Wolf, A. Willecke, J.-C. Muller et al., "Securing CACC: Strategies for Mitigating Data Injection Attacks", in *2020 IEEE Vehicular Networking Conference (VNC)*, p. 1–7, 2020.

[16] C. Murguia, I. Shames, J. Ruths, and D. Nešić, "Security metrics and synthesis of secure control systems," in *Automatica*, vol. 115, p. 108757, 2020.

[17] M. Huisman, C. Murguia, E. Lefeber, and N. van de Wouw, "Impact Sensitivity Analysis of Cooperative Adaptive Cruise Control Against Resource-Limited Adversaries", in *62nd IEEE Conference on Decision and Control (CDC)*, p. 5105–5110, 2023.

[18] A. Halder, "On the Parameterized Computation of Minimum Volume Outer Ellipsoid of Minkowski Sum of Ellipsoids", in *IEEE Conference on Decision and Control (CDC)*, p. 4040–4045, 2018.

[19] S. Boyd, L. El Ghaoi, E. Feron, and V. Balakrishnan, "Linear Matrix Inequalities in System and Control Theory", *SIAM*, 1994.

[20] J. Lofberg, YALMIP: A Toolbox for Modeling and Optimization in MATLAB, In Proceedings of the CACSD Conference, 2004.

[21] K.C. Toh, M.J. Todd, and R.H. Tutuncu, SDPT3 — a Matlab software package for semidefinite programming, version 1.3, Optimization Methods and Software, 11 (1999), pp. 545–581.