Gradient Descent Based Testing and Verification to Tune a Secure Cooperative Adaptive Cruise Control

Farahnaz Javidi-Niroumand[1], Somak Das [2,*], Ala' J. Alnaser[2], and Arman Sargolzaei[1]

[1]Department of Mechanical and Aerospace Engineering, University of South Florida, Tampa, FL
[2]Department of Applied Mathematics, Florida Polytechnic University, Lakeland, FL
[*]Corresponding author: sdas@floridapoly.edu

***Abstract*—Cooperative adaptive cruise control (CACC) is one of the main features of connected and autonomous vehicles (CAVs), improving safety and traffic efficiency by enabling vehicles to communicate and maintain optimal spacing. However, CACC systems are vulnerable to false data injection (FDI) attacks, which can disrupt vehicle behavior and compromise safety. To address this vulnerability, a Lyapunov-based controller, an observer, and an attack estimator are designed to improve system performance under FDI attacks. Unlike existing secure control designs, we provided a stability analysis showing that the estimated FDI attack error is semi-globally uniformly ultimately bounded. As tuning these controller parameters is challenging yet critical, we present a testing and verification framework for tuning CACC control parameters to mitigate the impact of FDI attacks. The framework employs gradient descent (GD) optimization to refine control parameters, minimizing tracking errors and improving FDI attack estimation. Simulation results demonstrate that the proposed approach significantly enhances safe following distances and attack estimation accuracy across diverse scenarios.**

***Index Terms*—Cooperative adaptive cruise control, Testing and verification, False data injection attack estimation, Parameter tuning, Gradient descent optimization.**

I. Introduction

Based on the National Highway Traffic Safety Administration (NHTSA) reports, human errors such as distracted driving, speeding, driving under the influence, and traffic law breaking are the leading contributors to approximately 94% of the crashes [1]. By Reducing the reliance on the human driver, autonomous vehicles (AVs) can significantly improve the safety [2]. Unlike human drivers, AVs are utilizing advanced sensors and control algorithms to enhance real-time decision-making and help traffic flow and fuel efficiency [3]. AVs continue to advance through the integration of artificial intelligence and robotics, with recent developments in deep and distributional reinforcement learning enabling more capable decision-making frameworks for complex tasks [4], [5]. By integrating communication technologies such as vehicle-to-vehicle (V2V) and vehicle-to-everything (V2X), connected and autonomous vehicles (CAVs) can leverage both autonomy and connectivity to enable seamless cooperation among vehicles. CAVs can promise smoother traffic flow, less congestion, and fewer delays by removing human error, strictly adhering to traffic laws, and improving traffic flow through communication with infrastructure and other vehicles [6], [7].

Corresponding author: sdas@floridapoly.edu

Cooperative adaptive cruise control (CACC) is a key feature in CAVs that enhances the efficiency of transportation networks. By enabling V2V communication and coordination, CACC improves traffic flow and mitigates road congestion [8]. Additionally, CACC leverages real-time data exchange to maintain safe following distances while ensuring smooth acceleration and deceleration, reducing unnecessary braking and acceleration cycles [9]. Consequently, CACC significantly enhances fuel efficiency and reduces emissions by promoting a more stable and optimized speed profile for all vehicles within a platoon [10]. Several CACC algorithms have been proposed in the literature to maintain safe and optimal following distances within a vehicle platoon. From a control perspective, these methods offer adaptive optimal solutions under uncertain dynamics [11], address both homogeneous and heterogeneous fleets [12], and ensure system stability in the presence of parameter uncertainties, sensor saturation, and deception attacks [13]. Moreover, robust control strategies have been developed to mitigate uncertain communication delays and preserve string stability in CACC systems [14].

Most CACC algorithms rely on the accurate sensor readings for safe and efficient cooperative driving and reliable communication for exchanging information. However, implementing CACC is challenging because the sensor information and the communication channels are not reliable due to existing cyberattacks such as false data injection (FDI) attacks [15]. Since these attacks can manipulate sensor data or disrupt V2V communication, they pose significant risks to vehicle coordination, potentially leading to unsafe behaviors such as sudden braking, incorrect acceleration, or even collisions [16]. To address these critical vulnerabilities, recent research has increasingly focused on developing CACC systems capable of detecting and mitigating cyber threats, ensuring safer and more reliable vehicle coordination.

Developments in CACC have concentrated on incorporating secure control algorithms that can identify and mitigate FDI attacks promptly. The secure control algorithms can successfully estimate the FDI attack and apply an adaptive control strategy to mitigate their effects. In [17], the authors present a secure resilient control algorithm based on Lyapunov stability, incorporating a neural network (NN)-based estimator to detect FDI attacks in real time. Similarly, [18] models FDI attacks

and introduces an observer designed to detect these attacks and pinpoint the injection location using a partial differential equation (PDE) model. Since delay in the communication channel can degrade the stability and performance of the CACC, leading it to safety risks, in [19] the authors have addressed FDI attack estimation for a CACC with communication delays by employing a Lyapunov-based nonlinear controller. Furthermore, [20] proposes a nonlinear controller for CACC to mitigate the impact of FDI attacks in the presence of time-varying input delays. However, the aforementioned CACC designs do not provide a formal stability guarantee for the FDI attack estimation error. In addition, they rely on several user-defined parameters without offering systematic guidance for their tuning. These parameters are critical for ensuring the safe operation of CACC systems under diverse scenarios. To address these limitations, this paper develops a novel CACC framework and establishes that the resulting FDI attack estimation error is semi-globally uniformly ultimately bounded. Furthermore, the proposed design reduces the number of user-defined parameters.

In addition, designing control algorithms, observers, and FDI attack estimators presents a challenge due to the numerous control parameters introduced into the system. If not optimally tuned, these parameters can degrade controller safety, security, and performance. The tuning process is often time-consuming and typically relies on trial-and-error methods. Therefore, a robust testing and verification framework is essential to evaluate different control parameters and ensure their proper selection.

Various testing and verification methods have been proposed in the literature to assess the performance of CAVs across different applications [21]. While some of these methods focused on evaluating CACC systems in terms of safety, security, and performance, only a few specifically address these aspects. In [22] , the authors discuss a comprehensive testing method to cover all possible situations that an AV may run into. The study proposes a mathematical framework for determining coverage in the context of employing pseudo-random simulations for testing, which is accomplished by introducing new equivalence relations between various system states known as scenes. However, these existing approaches do not explicitly quantify the security of CACC algorithms. In [23], the authors introduce a testing framework for generating scenarios and attacks to assess CACC safety under FDI attacks. However, the proposed cost function did not simultaneously evaluate both safety and security. In addition, the above frameworks are not used to tune control parameters to ensure safety and security.

Following a similar approach, [24] employed the particle swarm optimization (PSO) algorithm to tune the control parameters of a homogeneous CACC system under an FDI attack. While the algorithm effectively optimizes control performance, the resulting tracking error remains unsatisfactory due to the design of controller and nature of PSO algorithm. In [25], the authors proposed a testing framework for the parameter tuning problem of a CACC system under an FDI attack using reinforcement learning (RL). The results demonstrated safe speed and following distance tracking, along with a low-error FDI attack estimation. However, due to the complexity of the FDI attack estimation method, the number of tuning parameters increased, leading to a more complex tuning algorithm , making it harder to find optimized parameters. Therefore, this paper developed a secure CACC algorithm and a simple FDI attack estimator to address the complexity. In addition, a novel cost function is developed to simultaneously ensure the safety and security of CAVs under FDI attacks. We also develop a gradient descent (GD)-based optimization algorithm to tune the parameters of the developed CACC along with the observer and FDI attack estimator.

The contributions of this paper are as follows: (1) recognizing that existing secure CACC approaches contain numerous tunable parameters and lack a proof of convergence for all error signals, a secure controller, observer, and FDI attack estimator are developed using Lyapunov control theory, ensuring a reduced set of control parameters and providing a formal convergence guarantee for the FDI attack estimation error; (2) to enable systematic parameter tuning and ensure the safety of CACC under FDI attacks across diverse scenarios, a testing and verification framework along with a novel verification cost function is introduced to support structured parameter optimization; and (3) a gradient descent–based optimization approach is formulated to compute control parameters that ensure the safe and secure operation of CACC in the presence of FDI attacks.

This paper is organized as follows: Section II presents the modeling of the CACC system and the FDI attack, which serve as the foundation for control system design. Section III focuses on the development of the controller, observer, and FDI attack estimator using Lyapunov control theory. The mathematical formulation of the verification approach is detailed in Section IV. Section V outlines the optimization algorithm and numerical experiments used for parameter tuning. Simulation results under various FDI attack scenarios are presented and analyzed in Section VI. Finally, Section VII summarizes the findings and suggests directions for future research.

II. Dynamic Model of CACC under FDI Attack

A. Dynamic Model Representation

In this section, we describe a platoon of vehicles that are following each other using CACC. The follower vehicles in the platoon are identified as $i \in [2, n]$, and the leader is indicated as $i-1$. The control input is sent across the wireless communication channel to the follower vehicles as an acceleration command.

Onboard sensors are used to measure the leader's position and velocity. The follower vehicle dynamic model in CACC is defined as

$$\begin{cases} \dot{x}_i(t) = v_i(t), \\ \dot{v}_i(t) = -b_i v_i(t) + c_i u_i(t), \end{cases} \tag{1}$$

where $x_i(t) \in \mathbb{R}$, $v_i(t) \in \mathbb{R}$, and $u_i(t) \in \mathbb{R}$ represent the position, velocity, and control input of the follower vehicle, while $b_i \in \mathbb{R}_{>0}$ and $c_i \in \mathbb{R}_{>0}$ are constant parameters of the vehicle model.

The dynamic model of the leader vehicle is described as

$$\begin{cases} \dot{x}_{i-1}(t) = v_{i-1}(t), \\ \dot{v}_{i-1}(t) = -b_{i-1}v_{i-1}(t) + c_{i-1}u_{i-1}(t), \end{cases} \tag{2}$$

where $x_{i-1} \in \mathbb{R}$, $v_{i-1} \in \mathbb{R}$, and $u_{i-1} \in \mathbb{R}$ denote the position, velocity, and control input of the leader vehicle, respectively. The leader vehicle dynamics are defined as $b_{i-1} \in \mathbb{R}_{>0}$ and $c_{i-1} \in \mathbb{R}_{>0}$. The distance between the leader and the follower vehicles $d_i(t) \in \mathbb{R}$ is defined as

$$d_i(t) \triangleq x_{i-1}(t) - x_i(t) - L_i, \tag{3}$$

where $L_i \in \mathbb{R}$ is the length of the follower vehicle.

B. FDI Attack Representation

An FDI attack aims to compromise the communication link among vehicles while deliberately injecting false or altered data into the CACC system. Such an attack can manipulate the autonomous vehicle's decision-making by distorting its perception or hindering its ability to respond effectively. A general model of the FDI attack is presented as

$$\pi_f(u_{i-1}(t)) = u_{i-1}(t) + \beta_{i,i-1}(t), \tag{4}$$

where $\pi_f \in \mathbb{R}$ is the FDI attack function, and $\beta_{i,i-1}(t) \in \mathbb{R}$ is an unknown signal generated by the adversary to inject false data into the leader's control signal.

***Assumption** 1:* The FDI attack is assumed to be bounded, constant, and differentiable such that $\|\beta_{i,i-1}(t)\| \leq \bar{\beta}_{i,i-1}$ $\forall t \geq t_0$ where $\bar{\beta}_{i,i-1} \in \mathbb{R}$ is a positive constant value [26].

III. Control, Observer, and Attack Estimation Design

A. Error Signals

Platoon control, also referred to as string stability, aims to prevent disturbances from amplifying while ensuring consistent inter-vehicle spacing. Each vehicle, except the leader, must maintain a safe following distance from the preceding vehicle and adjust to dynamic traffic conditions. This approach can be formulated as

$$d_{d,i}(t) \triangleq h_i v_i(t) + d_0, \tag{5}$$

where $d_{d,i}(t) \in \mathbb{R}$ is the adaptive safe distance between the vehicles, $h_i \in \mathbb{R}$ is the time headway equals, set to 0.6, and $d_0 \in \mathbb{R}$ is the minimum safe standstill distance between the vehicles.

Furthermore, to quantify the performance of the designed controller, let $e_i : [t_0, \infty) \to \mathbb{R}$ be the tracking error between the leader and follower. Our main objective is to control the spacing error as

$$e_i(t) \triangleq d_{i,i-1,x}(t) - d_{d,i}(t), \tag{6}$$

where $d_{d,i} : [t_0, \infty) \to \mathbb{R}$ is the desired distance between leader and follower.

***Assumption** 2:* The desired distance, and its first and second derivatives are assumed to be bounded by positive known constants, $d_{d,i}, \dot{d}_{d,i}, \ddot{d}_{d,i} \in \mathcal{L}_\infty$ [27].

Additionally, to facilitate the design process and stability analysis, an auxiliary error signal $r_i \in \mathbb{R}$[1] is defined as

$$r_i(t) \triangleq \dot{e}_i(t) + \alpha_i e_i(t), \tag{7}$$

such that $\alpha_i \in \mathbb{R}_{>0}$, is a user-specified known gain.

Since the follower vehicle in the platoon lacks precise knowledge of the leader vehicle's location, it is essential to design an observer. To quantify the accuracy of the observer, a state estimation error $\tilde{x}_{i-1} : [t_0, \infty) \to \mathbb{R}$ is described as

$$\tilde{x}_{i-1}(t) \triangleq x_{i-1}(t) - \hat{x}_{i-1}(t), \tag{8}$$

where $\hat{x}_{i-1} \in \mathbb{R}$ denotes the estimated position of the lead vehicle.

The estimation of the auxiliary error signal $\tilde{r}_{i-1} : [t_0, \infty) \to \mathbb{R}$ is needed for stability analysis and can be defined as

$$\tilde{r}_{i-1}(t) \triangleq \dot{\tilde{x}}_{i-1}(t) + \alpha_{i-1}\tilde{x}_{i-1}(t), \tag{9}$$

where $\alpha_{i-1} \in \mathbb{R}_{>0}$ is a user-defined gain.

Additionally, it is necessary to assess the accuracy of the control signal using an estimation error value, $\tilde{u}_{i-1} : [t_0, \infty) \to \mathbb{R}$ defined as

$$\tilde{u}_{i-1}(t) \triangleq u_{i-1}(t) - \hat{u}_{i-1}(t), \tag{10}$$

where $\hat{u}_{i-1} \in \mathbb{R}$ is the estimated control signal of the leader. Defining $\bar{u}_{i-1}(t) \triangleq u_{i-1}(t) + \beta_{i,i-1}(t)$ and $\hat{u}_{i-1}(t) \triangleq \bar{u}_{i-1}(t) - \hat{\beta}_{i,i-1}(t)$ yields

$$\tilde{u}_{i-1}(t) = u_{i-1}(t) - \bar{u}_{i-1}(t) + \hat{\beta}_{i,i-1}(t), \tag{11}$$

where $\hat{\beta}_{i,i-1}(t) \in \mathbb{R}$ is the estimation of the actual attack $\beta_{i,i-1}(t)$. Furthermore, the accuracy of the FDI attack estimation is monitored using an estimation error signal, $\tilde{\beta}_{i,i-1} : [t_0, \infty) \to \mathbb{R}$, defined as

$$\tilde{\beta}_{1,i-1}(t) \triangleq \beta_{i,i-1} - \hat{\beta}_{i,i-1}(t). \tag{12}$$

Based on the definitions provided in this subsection, we design a controller, an observer and an FDI attack estimation in the next subsections.

B. Controller Design

The proposed control algorithm for the CACC system is developed using Lyapunov stability analysis, which is further discussed in Subsection III-E, and is formulated as

$$\begin{aligned} u_i(t) \triangleq & -\frac{b_{i-1}}{c_i}v_{i-1}(t) + \frac{c_{i-1}}{c_i}\bar{u}_{i-1}(t) + \frac{b_i}{c_i}v_i(t) \\ & - \frac{c_{i-1}}{c_i}\hat{\beta}_{i,i-1}(t) - \frac{1}{c_i}\ddot{d}_{d,i}(t) + \frac{1}{c_i}(\alpha_i + k_i)r_i(t) \\ & + \frac{1}{c_i}(1 - \alpha_i^2)e_i(t), \end{aligned} \tag{13}$$

where $k_i \in \mathbb{R}_{>0}$ is a gain specified for the controller that will be further optimized.

[1]It combines both the error and its rate of change yielding smooth and stable distance regulation. The aim is to provide a structured and stabilizing representation of the spacing error that enables controller design, simplifies the Lyapunov analysis, and guarantees convergence of the inter-vehicle distance to the desired safe spacing.

To enhance the stability analysis, we calculate the time derivative of (7), and substitute (6) as

$$\dot{r}_i(t) = \ddot{d}_i(t) - \ddot{d}_{d,i} + \alpha_i \dot{e}_i(t). \tag{14}$$

Since $\ddot{d}_i(t) = \ddot{x}_{i-1}(t) - \ddot{x}_i(t)$, replacing $\ddot{x}_i(t)$ and $\ddot{x}_{i-1}(t)$ from the model and substituting $\dot{e}_i(t)$ from (7) yields

$$\begin{aligned}\dot{r}_i(t) = &- b_{i-1}v_{i-1}(t) + c_{i-1}u_{i-1}(t) + b_i v_i(t) \\ &- c_i u_i(t) - \ddot{d}_{d,i}(t) + \alpha_i r_i(t) - \alpha_i^2 e_i(t).\end{aligned} \tag{15}$$

However, the actual leader acceleration command $u_{i-1}(t)$ is unknown for the follower vehicle. Considering the FDI attack in the communication channel, $u_{i-1}(t)$ will be substituted with $\bar{u}_{i-1}(t) - \beta_{i,i-1}(t)$ to insert the attack effect into the control design as

$$\begin{aligned}\dot{r}_i(t) = &- b_{i-1}v_{i-1}(t) + c_{i-1}\bar{u}_{i-1}(t) - c_{i-1}\beta_{i,i-1}(t) \\ &+ b_i v_i(t) - c_i u_i(t) - \ddot{d}_{d,i}(t) \\ &+ \alpha_i r_i(t) - \alpha_i^2 e_i(t),\end{aligned} \tag{16}$$

adding and subtracting $c_{i-1}\hat{\beta}_{i,i-1}$ to (16) and using (12) we have

$$\begin{aligned}\dot{r}_i(t) = &- b_{i-1}v_{i-1}(t) + c_{i-1}\bar{u}_{i-1}(t) - c_{i-1}\tilde{\beta}_{i,i-1}(t) \\ &- c_{i-1}\hat{\beta}_{i,i-1}(t) + b_i v_i(t) - c_i u_i(t) - \ddot{d}_{d,i}(t) \\ &+ \alpha_i r_i(t) - \alpha^2 e_i(t),\end{aligned} \tag{17}$$

finally, we insert the control law of $u_i(t)$ from (13) into the (17) to generate the tracking error as

$$\dot{r}_i(t) = -c_{i-1}\tilde{\beta}_{i,i-1}(t) - k_i r_i(t) - e_i(t). \tag{18}$$

C. Observer and FDI Attack Estimator Design

By employing a Lyapunov-based design approach, we define the observer as

$$\begin{aligned}\ddot{\hat{x}}_{i-1}(t) \triangleq &- b_{i-1}v_{i-1}(t) + c_{i-1}\bar{u}_{i-1}(t) - c_{i-1}\hat{\beta}_{i,i-1}(t) \\ &+ (l_i + \alpha_{i-1})\tilde{r}_{i-1}(t) + (1 - \alpha_{i-1}^2)\tilde{x}_{i-1}(t),\end{aligned} \tag{19}$$

such that $l_i \in \mathbb{R}$ denoted the observer gain, that will be tuned further. By calculating the time derivative of (9) for enhancing the stability analysis we have

$$\dot{\tilde{r}}_{i-1}(t) = \ddot{\tilde{x}}_{i-1}(t) + \alpha_{i-1}\dot{\tilde{x}}_{i-1}(t), \tag{20}$$

substituting $\tilde{x}_{i-1}(t)$ from (8), and u_{i-1} from (11) results in

$$\begin{aligned}\dot{\tilde{r}}_{i-1}(t) = &- b_{i-1}v_{i-1}(t) + c_{i-1}\bar{u}_{i-1}(t) - c_{i-1}\tilde{\beta}_{i,i-1}(t) \\ &- c_{i-1}\hat{\beta}_{i,i-1}(t) + \alpha_{i-1}\tilde{r}_{i-1}(t) - \alpha_{i-1}^2\tilde{x}_{i-1}(t) \\ &- \ddot{\tilde{x}}_{i-1}(t),\end{aligned} \tag{21}$$

substituting $\ddot{\tilde{x}}_{i-1}$ from (19) the tracking error estimation will be derived as

$$\dot{\tilde{r}}_{i-1}(t) = -c_{i-1}\tilde{\beta}_{i,i-1}(t) - \tilde{x}_{i-1}(t) - l_i\tilde{r}_{i-1}(t). \tag{22}$$

Additionally, based on the Lyapunov stability analysis provided in the next subsection, we determined the FDI attack estimation rate as

$$\dot{\hat{\beta}}_{i,i-1}(t) \triangleq -\Gamma_i\big(c_{i-1}r_i(t) + c_{i-1}\tilde{r}_{i-1}(t) + \gamma_i\hat{\beta}_{i,i-1}(t)\big). \tag{23}$$

where $\Gamma_i \in \mathbb{R}_{>0}$ and $\gamma_i \in \mathbb{R}_{>0}$ are user-defined gain.

D. Summary of Contribution

Given the dynamic models of the lead vehicle in (2) and the following vehicle in (1), the mathematical objective of the paper is to guarantee that the spacing error in (6) remains bounded so that a safe inter-vehicle distance is maintained. Unlike traditional CACC designs that rely on direct feedback of the lead vehicle's control signal, the present problem is complicated by the presence of an FDI attack on that signal, as described in (4). Consequently, the controller must be designed in parallel with an attack estimation mechanism. To achieve this, a nonlinear observer is developed in (19) to provide accurate state estimates, and its convergence properties are established through Lyapunov stability analysis. Building on this result, an FDI attack estimator is introduced in (23) to ensure uniform ultimate boundedness of the attack estimation error. Finally, the estimated attack signal is incorporated into the controller design in (13), while the remaining auxiliary signals are structured to ensure safe tracking performance and preservation of the desired inter-vehicle distance.

E. Stability Analysis

For simplicity in further analysis, the parameter t, which is time, is dropped from the equations. Let's define z_i as

$$z_i \triangleq [e_i^T \ r_i^T \ \tilde{x}_{i-1}^T \ \tilde{r}_{i-1}^T \ \tilde{\beta}_{i,i-1}^T]^T, \tag{24}$$

and, consider the following sufficient conditions as

$$k_i > 0, \ \alpha_i > 0, \ \alpha_{i-1} > 0, \ l_i > 0, \gamma_i > 0. \tag{25}$$

A stability method is required to ensure that all error signals in (24), including tracking errors, estimation errors, and FDI attack estimation errors ultimately guaranteeing semi-global uniform ultimate boundedness despite system uncertainties and adversarial disturbances.

Theorem 1: The controller given in (13), state estimator in (19), FDI attack estimator in (23), and Assumptions 1, and 2 and sufficient condition ensure semi-globally uniformly ultimately bounded tracking such that

$$\lim_{t\to\infty} \sup \|z_i(t)\| \leq \sqrt{\frac{1}{\eta_{i_1}}\left(\frac{\eta_{i_2}\phi_i}{\lambda_i}\right)}, \tag{26}$$

Proof 1: We first design a Lyapunov candidate function to assess the stability of the closed-loop error dynamics in (18) and (22). This function must be positive definite, radially unbounded, and continuously differentiable so that it provides a valid measure of the magnitude of the aggregated error vector in (24). For an ultimate boundedness result, its time derivative must be negative outside a compact set and bounded above within that set. This structure ensures that the error signals decrease whenever they are sufficiently large and remain confined to a bounded region determined by the design parameters. Therefore, we define a Lyapunov candidate function as

$$V_i \triangleq \frac{1}{2}e_i^2 + \frac{1}{2}r_i^2 + \frac{1}{2}\tilde{x}_{i-1}^2 + \frac{1}{2}\tilde{r}_{i-1}^2 + \frac{1}{2\Gamma_i}\tilde{\beta}_{i,i-1}^2, \tag{27}$$

where $V_i : \mathbb{R}^n \to \mathbb{R}$ is a continuous positive definite and continuously differentiable function, such that

$$\eta_{1_i} \|z_i\|^2 \leq V_i \leq \eta_{2_i} \|z_i\|^2, \tag{28}$$

Taking the time derivative of (27) results

$$\dot{V}_i = e_i\dot{e}_i + r_i\dot{r}_i + \tilde{x}_{i-1}\dot{\tilde{x}}_{i-1} + \tilde{r}_{i-1}\dot{\tilde{r}}_{i-1} + \frac{1}{\Gamma_i}\tilde{\beta}_{i,i-1}\dot{\tilde{\beta}}_{i,i-1}, \tag{29}$$

substituting $\dot{e}_i$, $\dot{r}_i$, $\dot{\tilde{x}}_{i-1}$, and $\dot{\tilde{r}}_{i-1}$ from (7), (18), (9), and (22), respectively and assuming that attack is constant for each cycle, yields

$$\begin{aligned}\dot{V}_i = {} & e_i(r_i - \alpha_i e_i) + r_i(-c_{i-1}\tilde{\beta}_{i,i-1} - k_i r_i - e_i) \\ & + \tilde{x}_{i-1}(\tilde{r}_{i-1} - \alpha_{i-1}\tilde{x}_{i-1}) \\ & + \tilde{r}_{i-1}(-c_{i-1}\tilde{\beta}_{i,i-1} - \tilde{x}_{i-1} - l_i\tilde{r}_{i-1}) \\ & - \frac{1}{\Gamma_i}\tilde{\beta}_{i,i-1}\dot{\tilde{\beta}}_{i,i-1}\end{aligned} \tag{30}$$

after some simplification, we have

$$\begin{aligned}\dot{V}_i = {} & -\alpha_i e_i^2 - k_i r_i^2 - \alpha_{i-1}\tilde{x}_{i-1}^2 - l_i\tilde{r}_{i-1}^2 \\ & - c_{i-1}\tilde{r}_{i-1}\tilde{\beta}_{i,i-1} - c_{i-1}r_i\tilde{\beta}_{i,i-1} \\ & - \frac{1}{\Gamma_i}\tilde{\beta}_{i,i-1}\dot{\tilde{\beta}}_{i,i-1},\end{aligned} \tag{31}$$

substituting $\dot{\tilde{\beta}}_{i,i-1}$ from (23) cancels the last two terms in (31).

$$\begin{aligned}\dot{V}_i = {} & -\alpha_i e_i^2 - k_i r_i^2 - \alpha_{i-1}\tilde{x}_{i-1}^2 - l_i\tilde{r}_{i-1}^2 \\ & - \gamma_i\tilde{\beta}_{i,i-1}^2 + \gamma_i\tilde{\beta}_{i,i-1}\beta_{i,i-1},\end{aligned} \tag{32}$$

as the FDI attack is assumed bounded based on Assumption 1, we can use Young's inequality to find the upper bounds for selected terms as

$$\tilde{\beta}_{i,i-1}\beta_{i,i-1} \leq \frac{1}{2\varepsilon_0}\left\|\tilde{\beta}_{i,i-1}\right\|^2 + \frac{\varepsilon_0}{2}\|\beta_{i,i-1}\|^2, \tag{33}$$

where $\varepsilon_0 \in \mathbb{R}$, denotes a positive known constants. Using the sufficient conditions in (25) and considering the upper bound of the FDI attack from Assumption 1 yields

$$\begin{aligned}\dot{V}_i \leq {} & -\alpha_i \|e_i\|^2 - k_i \|r_i\|^2 \\ & - \alpha_{i-1}\|\tilde{x}_{i-1}\|^2 - l_i\|\tilde{r}_{i-1}\|^2 \\ & - \gamma_i(1 - \frac{1}{2\varepsilon_0})\left\|\tilde{\beta}_{i,i-1}\right\|^2 \\ & + \frac{\varepsilon_0\gamma_i}{2}\bar{\beta}_{i,i-1}^2,\end{aligned} \tag{34}$$

summarizing the results we have

$$\dot{V}_i \leq -\lambda_i \|z_i\|^2 + \phi_i, \tag{35}$$

where ϕ_i is a positive constant value, and $\lambda_i \in \mathbb{R}$ is defined as

$$\lambda_i \triangleq \min\{\alpha_i, k_i,\ \alpha_{i-1},\ l_i, \gamma_i(1 - \frac{1}{2\varepsilon_0})\}. \tag{36}$$

The $\dot{V}_i$ inequality derived in (34) is a negative semi-definite function. According to the Lyapunov stability theorem, implies that there exist α_i, k_i, α_{i-1}, l_i, γ_i, and Γ_i gains such that $z_i \to 0$ as $t \to \infty$ in the presence of FDI attacks.

IV. The Mathematics of Verification

This section formalizes the testing-and-verification framework used to evaluate and tune the CACC system under FDI attacks. We first give the general mathematical objects (scene vector, assertion matrix, reference vector, residual, and scenario-level costs) based on the definitions in [28]–[30], next then specialize to the single-lead longitudinal scenario.

A. Terminology and Notation

Scene Vector: We use the term scene to denote the instantaneous and local traffic environment surrounding the Unit Under Test (UUT), that is, the vehicle whose safety and security performance is being evaluated. A **Scene vector** is defined as the vector representation of all measurable or estimated quantities relevant to a specific test requirement, such as the UUT's velocity, relative distances to surrounding actors, and the currently estimated fault/attack signal. The *Scene Vector* is defined as

$$\mathcal{C}(t) \triangleq \left[p_i,\ v_i,\ a_i,\ \{\,p_j,\ v_j,\ a_j,\ d_{i,j}\,\}_{j=i-1}^{i+q},\ \hat{\beta}_{i,j}\right]^T, \tag{37}$$

where the position, velocity and acceleration of the k^{th} actor in the scene are $p_k = [x_k, y_k]$, $v_k = [\dot{x}_k, \dot{y}_k]$, $a_k = [\ddot{x}_k, \ddot{y}_k]$ receptively, and $d_{i,j} = [d_{i,j,x}, d_{i,j,y}]$ is the longitudinal and latitudinal distances between the ith and jth actors in the scene. Finally, the term $\hat{\beta}_{i,j}$ is the current estimate of the FDI attack signal on link (i, j) as defined earlier.

Assertion Matrix and reference vector: Let $\mathcal{A}$ be the matrix with appropriate dimension that selects the specific quantities we must check, and let $\mathcal{C}_{ref}$ provide their required values/limits. We define the *Verification Cost Function* (or *Verification Residual*) as

$$\mathcal{V}(t) \triangleq \mathcal{A}\,\mathcal{C}(t) - \mathcal{C}_{ref}(t). \tag{38}$$

For multi-actor scenes (and optional lateral checks), $\mathcal{A}$ expands block-wise. One convenient layout is illustrated as

$$\mathcal{A} = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 & 0 & \cdots & & \\ & & \mathbf{0} & & 1 & 0 & & \cdots \\ & & & & 0 & 1 & & \\ & & \vdots & & \vdots & & & \ddots \\ & & & & & & 1 & 0 & 0 \\ & & \mathbf{0} & & \cdots & & 0 & 1 & 0 \\ & & & & & & 0 & 0 & \ddots \end{bmatrix}, \tag{39}$$

where the first row extracts $\dot{x}_i$, each 2×2 block extracts a pair $(d_{i,j,x}, d_{i,j,y})$, and the bottom-right identity isolates the estimates $\hat{\beta}_{i,j}$. (For brevity we keep this block form optional; it can be moved to an appendix without affecting the flow.)

In this paper, we check speed-limit compliance and minimum headway for longitudinal safety and we check attack-estimation accuracy for security. Accordingly

$$\mathcal{C}_{ref}(t) = \left[v_{x,\text{limit}}(t),\ d_{i,i-1,x}^{\min}(t),\ \beta_{i,i-1}(t)\right]^T, \tag{40}$$

and the corresponding measured/estimated quantities are

$$\mathcal{A}\mathcal{C}(t) = \left[\dot{x}_i(t),\ d_{i,i-1,x}(t),\ \hat{\beta}_{i,i-1}(t)\right]^T. \tag{41}$$

A test incorporates machine-verifiable assertions such as "longitudinal speed $\leq$ limit," "headway $\geq$ minimum safe distance," and "estimated attack $\approx$ true attack." These assertions are encoded as linear functionals of the scene vector through an assertion matrix. When multiplied by the scene vector, the assertion matrix extracts precisely those quantities that must be compared against their corresponding safety or security reference values, including but not limited to speed limits, minimum allowable distances, and ground-truth attack signals. **Penalizing only Violations:** We use the positive-part operator $[z]_+ = \max\{z, 0\}$ so that safety penalties accrue only for violations (overspeeding or headway safety distance deficits).

B. Scenario and scenario-level costs

Definition 1: **Sampling grid and scenario.** Fix $\Delta t > 0$ and set $t_\ell \triangleq \ell\,\Delta t$ for $\ell = 0, 1, \ldots, T$; denote $\mathcal{C}_\ell \triangleq \mathcal{C}(t_\ell)$. A *scenario* is the time-indexed sequence $\chi \triangleq [\,\mathcal{C}_0\ \mathcal{C}_1\ \cdots\ \mathcal{C}_T\,]$.

Definition 2: With $[z]_+ \triangleq \max\{z, 0\}$, the scenario-level safety and security costs can be defined as

$$\big(J_{\text{safe}}(\chi)\big)^2 \triangleq \frac{1}{T+1}\sum_{\ell=0}^{T}\Big([\dot{x}_i(t_\ell) - v_{x,\text{limit}}(t_\ell)]_+^2 + [d^{\min}_{i,i-1,x}(t_\ell) - d_{i,i-1,x}(t_\ell)]_+^2\Big), \tag{42}$$

$$\big(J_{\text{sec}}(\chi)\big)^2 \triangleq \frac{1}{T+1}\sum_{\ell=0}^{T}\Big(\hat{\beta}_{i,i-1}(t_\ell) - \beta_{i,i-1}(t_\ell)\Big)^2. \tag{43}$$

The scalar cost combines both safety and security costs and is defined as

$$J(\chi) = w_v\, J_{\text{safe}}(\chi) + w_\beta\, J_{\text{sec}}(\chi), \tag{44}$$

with weights $w_v, w_\beta \in \mathbb{R}_{>0}$. A test *passes* if $J_{\text{safe}}(\chi) \leq \varepsilon_{\text{safe}}$ and $J_{\text{sec}}(\chi) \leq \varepsilon_{\text{sec}}$.

C. Worked example: single-lead, longitudinal checks

For one lead vehicle $(i-1)$ and longitudinal-only checks, the three assertions (speed, headway, FDI accuracy) give the component-wise residual

$$\mathcal{V}(t) = \begin{bmatrix} \dot{x}_i(t) - v_{x,\text{limit}}(t) \\ d_{i,i-1,x}(t) - d^{\min}_{i,i-1,x}(t) \\ \hat{\beta}_{i,i-1}(t) - \beta_{i,i-1}(t) \end{bmatrix}. \tag{45}$$

In J_{safe}, we square $[\dot{x}_i - v_{x,\text{limit}}]_+$ (overspeed) and $[d^{\min}_{i,i-1,x} - d_{i,i-1,x}]_+$ (headway deficit); in J_{sec} we square the estimation error $(\hat{\beta}_{i,i-1} - \beta_{i,i-1})$.

V. Optimization using gradient descent approach

The controller in (13), the observer in (19), and the FDI attack estimator in (23) depend on several user-defined parameters. Although these parameters can be chosen through trial-and-error, such an approach typically yields configurations that perform adequately only for specific scenarios and provides no guarantee of safety or robustness under varying operating conditions. To address this limitation, we employ our testing and verification framework discussed in Section IV in conjunction with a gradient-descent–based optimization procedure to systematically tune these parameters. Accordingly, our objective is to tune the following vector of system gains, defined as

$$\boldsymbol{\theta}_i \triangleq \big[\alpha_i,\ \alpha_{i-1},\ k_i,\ l_i,\ \gamma_i,\ \Gamma_i\big]^T, \tag{46}$$

by *minimizing the scalar verification cost* in (44), setting the weights $\omega_\nu = \omega_\beta = 1$. We will denote the $\beth$-th entry of $\boldsymbol{\theta}_i$ as $\theta_{i,\beth}$ for $\beth \in \{1, 2, \cdots, 6\}$. We define a minimizer of the scalar cost as

$$\boldsymbol{\theta}_i^* \in \arg\min_{\boldsymbol{\theta}_i} J(\chi; \boldsymbol{\theta}_i). \tag{47}$$

where $\boldsymbol{\theta}_i^*$ is the (possibly non-unique) optimal gain vector. Since $J(\chi; \boldsymbol{\theta}_i)$ is simulation–defined without a closed form, we apply gradient descent (GD) with central finite differences to approximate partial derivatives. Starting from an initial guess $\boldsymbol{\theta}_i^{(0)}$. For clarity and computational purposes, we will use the following notation as

$$J(\chi; \boldsymbol{\theta}_i) \triangleq E(\boldsymbol{\theta}_i) = \frac{1}{2n}\sum_{i=0}^{n} f_i(\boldsymbol{\theta}_i), \tag{48}$$

where $f_i(\boldsymbol{\theta}_i) = (d_i - d_{d,i})^2 + (\beta_{i,i-1} - \hat{\beta}_{i,i-1})^2$, where $d_{d,i}$ is the desired position and $\hat{\beta}_{i,i-1}(t)$ is the estimated FDI attack.

The GD method starts with an initial guess $\boldsymbol{\theta}_i^{(0)}$ as the minimizer and repeatedly takes steps in the direction of steepest descent (opposite the gradient) of the function to update the minimizer. Due to the lack of a closed form for the optimization problem at hand, we will use a central finite difference method to estimate any partial derivative we need to evaluate to construct the gradient. However, prior to optimizing the cost function using the GD method, we will perform a sensitivity analysis to measure how the perturbation in the gains affect the output of the cost function.

A. Global sampling

We perform a global sampling to understand the overall influence of each of the gains and to find the best initial guess for the gains. We generate N uniformly distributed random samples of the gain vector with each gain within a reasonable bounds based on the knowledge of the domains and constraints for the gains. For each sampled gain vector, we compute the cost function E and then select the gain vector that produces the lowest cost as our best choice of initial guess. For the above sampling, we select the gain vector yielding the lowest cost as the initial guess $\boldsymbol{\theta}_i^{(0)}$.

B. Local sensitivity analysis

This section presents the procedure to compute the local sensitivity of the gains for the cost function in (48). The purpose of this analysis is to evaluate how the cost function is affected by small changes in each gain at the initial guess. To evaluate the sensitivity, we start with the initial guess obtained in subsection V-A. With respect to each gain $\theta_{i,\beth}$ in (46) we consider the relative perturbation of magnitude,

$$h_\beth = \rho\theta_{i,\beth}^{(0)}, \quad \beth \in \{1, 2, \cdots, 6\} \tag{49}$$

where $\rho = 0.005$ and $\theta_{i,\beth}^{(0)}$ is the $\beth$-th entry of initial guess $\boldsymbol{\theta}_i^{(0)}$. We then perturb each gain and approximate the partial derivative using the central finite difference formula. We use the notation for the approximate partial derivative of E with respect to each gain $\theta_{i,\beth}$ as,

$$\mathfrak{D}_{\theta_{i,\beth}} E = \frac{E(\boldsymbol{\theta}_i + h_\beth e_\beth) - E(\boldsymbol{\theta}_i - h_\beth e_\beth)}{2h_\beth} \tag{50}$$

where $h_\beth$ is the perturbation for the central finite difference given in (49) and $e_\beth$ is the standard basis vector in the direction of $\beth$. The absolute value of the approximate partial derivative serves as the local sensitivity of each gain. For any gain $\theta_{i,\beth}$, the $\beth$-th entry in $\boldsymbol{\theta}_i$, the local sensitivity is given by

$$\begin{aligned} s_{i,\beth} &= \left| \mathfrak{D}_{\theta_{i,\beth}} E\left(\boldsymbol{\theta}_i^{(0)}\right) \right| \\ &= \left| \frac{E(\boldsymbol{\theta}_i^{(0)} + h_\beth e_\beth) - E(\boldsymbol{\theta}_i^{(0)} - h_\beth e_\beth)}{2h_\beth} \right|. \end{aligned} \tag{51}$$

We denote the vector with the sensitivites in (51) as its entries by

$$\boldsymbol{s}_i \triangleq \left[s_{i,1}, s_{i,2}, \cdots, s_{i,6}\right]^T. \tag{52}$$

C. The Gradient Descent Algorithm

The iterative process in GD method updates the minimizer at every iteration by taking a step in the opposite direction of the gradient. The size of the step taken in each iteration is crucial and is called the step-size or learning rate of the GD algorithm. Applying a uniform step-size across all the gains can lead to undesirable results since highly sensitive gains can cause the method to be unstable by updating too fast, whereas gains with low sensitivity may update too slowly and may not converge. To improve stability and better convergence we employ a gradient descent optimization with a step-size scaling on account of the heterogeneous sensitivity of the gains in the sensitivity vector in (52). To ensure robustness against poorly scaled sensitivities, we introduce a cut-off for the median value of the sensitivities

$$s_{i,\min} = 0.1 \times median(\boldsymbol{s}_i). \tag{53}$$

Any sensitivity below this threshold is replaced by $s_{i,\min}$. We construct the diagonal matrix

$$D_i = diag(\delta_{i,1}, \delta_{i,2}, \cdots, \delta_{i,6}), \tag{54}$$

where $\delta_{i,\beth} = |\max(s_{i,\beth}, s_{i,\min})| > 0$. Using this diagonal matrix we construct the following iterative step for the GD algorithm with a positive constant η as

$$\begin{aligned} \boldsymbol{\theta}_i^{(\tau+1)} &= \boldsymbol{\theta}_i^{(\tau)} - \eta D_i^{-1} \nabla E\left(\boldsymbol{\theta}_i^{(\tau)}\right) \\ &= \boldsymbol{\theta}_i^{(\tau)} - \eta D_i^{-1} \left(\frac{1}{2n} \sum_{i=0}^{n} \nabla f_i \left(\boldsymbol{\theta}_i^{(\tau)}\right) \right), \end{aligned} \tag{55}$$

where $\tau \in \mathbb{Z}_{>0}$ denotes the iteration index for the algorithm, and $\boldsymbol{\theta}_i^{(\tau)}$ is the solution for the minimizer at the τ-th iteration. The gradient ∇E can be estimated by

$$\tilde{\nabla} E = \left[\mathfrak{D}_{\alpha_i} E, \mathfrak{D}_{\alpha_{i-1}} E, \mathfrak{D}_{k_i} E, \mathfrak{D}_{l_i} E, \mathfrak{D}_{\gamma_i} E, \mathfrak{D}_{\Gamma_i} E\right], \tag{56}$$

Algorithm 1: Gradient descent-based parameter tuning

```
Obtain θ_i^(0) (from section V-A)
Obtain matrix D_i (from section V-B)
Initialize τ ← 1
Initialize N, η
Initialize h_ב, ב ∈ {1, 2, ··· , 5}
out ← simulation result
while τ < N do
    ∇̃E(θ_i^(τ)) ←
      [D_{α_i}E, D_{α_{i−1}}E, D_{k_i}E, D_{l_i}E, D_{γ_i}E, D_{Γ_i}E]
    θ_i^(τ+1) ← θ_i^(τ) − ηD_i^{−1} ∇̃E(θ_i^(τ))
    out ← simulation result
    τ ← τ + 1
end
```

where the approximate partial derivative for each entry of $\tilde{\nabla} E$ is given by equation (50). We can rewrite the GD iteration step as

$$\boldsymbol{\theta}_i^{(\tau+1)} = \boldsymbol{\theta}_i^{(\tau)} - \eta D_i^{-1} \tilde{\nabla} E\left(\boldsymbol{\theta}_i^{(\tau)}\right). \tag{57}$$

Algorithm 1 demonstrates the application of the GD method.

D. Numerical Experiments

As a proof of concept, we show results of test runs. In this experiment we performed the three step process of global sampling, local sensitivity analysis and GD optimization to obtain the minimizer. We perform the global sampling with $N = 10000$ samples and with each gain in the interval of $[0.1, 65]$ in both cases. We obtain the initial value as

$$\boldsymbol{\theta}_i^{(0)} = [54.8247, 9.3123, 62.5106, 26.2762, 0.1399, 4.3500]. \tag{58}$$

On performing the local sensitivity analysis we obtain the sensitivity values for the gains at the initial value presented in Table. I, These values tell us that the cost function is mostly sensitive towards the gains k_i and γ_i and least sensitive towards the gain α_{i-1}. On applying the GD optimization in algorithm 1 for 60 iterations with the initial values of the gains in (58) the initial cost is around 5.265×10^{-3}. We observe that the cost drops to the lowest value of 4.493×10^{-3} for the 54 iteration. The optimal value for the gains are obtained as

$$\boldsymbol{\theta}_i^* = [52.4940, 6.8704, 62.4426, 25.8735, 0.0122, 6.4404]. \tag{59}$$

TABLE I
SENSITIVITY RESULTS FOR EACH CONTROL GAIN

Gain	Sensitivity
α_i	$6.3905e-06$
k_i	$1.4614e-04$
α_{i-1}	$-3.6973e-08$
l_i	$1.1892e-05$
γ_i	$3.0013e-03$
Γ_i	$-2.3561e-05$

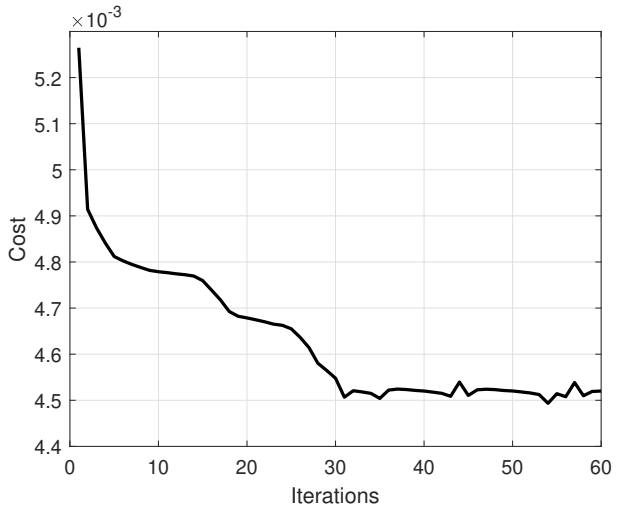

Fig. 1. Case studies for initial values of the gains $\theta_i^{(0)}$ showing the decrement of mean squared cost.

Fig. 1 shows the cost decreasing over 60 iterations and a schematic of the proposed CACC string of vehicles along with our proposed tuning approach is shown in Fig. 2.

VI. Results and Discussion

In this section, the Lyapunov-based controller, observer, and FDI attack estimator are simulated using MATLAB/Simulink. The optimized controller has been tested under two scenarios including Federal Test Procedure 75 (FTP-75) drive cycle which is a standardized test cycle for urban driving conditions, and (US06) which represents an aggressive high-speed/high-acceleration drive cycle. This scenario also includes randomly generated FDI attacks to challenge the safe operation of the CAV. In the CACC maneuver, each following vehicle must track the leader's speed profile while maintaining a safe following distance to prevent collisions. Two FDI attack scenarios have been designed to manipulate the leader's control signal as received by the follower vehicle.

In the simulation results, the "Baseline," which includes the controller in (13) and the observer in (19), is implemented with the initial gains that satisfy the conditions in (25). The baseline serves as a reference controller to evaluate the performance of the proposed gain optimization methods, representing the original design prior to any tuning or enhancements. Additionally, to assess the impact of the FDI attack, the baseline controller does not incorporate any attack estimation, as it is not designed for adversarial scenarios. The "Optimized Controller" incorporates optimally tuned control parameters, determined using the GD optimization technique to improve overall tracking performance and FDI attack estimation.

To assess the effectiveness of our optimization approach, we also compared its results with a secure CACC presented in [25]. The CACC designed in [25] employs a neural network–based FDI attack estimator and their parameters are tuned using a RL-based optimization approach. In contrast, our proposed CACC framework utilizes a Lyapunov-based method for FDI attack estimation with a proof of stability. In addition, the number of parameters/gains to be tuned are less than the one in the literature [2].

A. Scenario S_{11}

In this scenario, a CACC system is tested under the FTP-75 driving cycle, while the FDI attack is modeled as a random sequence of stair signals added to the leader vehicle's control signal received by the follower. To complicate detection via conventional methods, the random FDI attack is in the range of $[0, 1]$, mimicking a realistic pedal percentage ratio. Fig. 3 illustrates the simulation results for Scenario S_{11}. While the baseline controller fails to maintain a safe inter-vehicle

[2]We do not assert that GD–based tuning is superior to RL–based tuning. Rather, we compare the controller designs and demonstrate that the proposed controller outperforms recently developed CACC schemes reported in the literature.

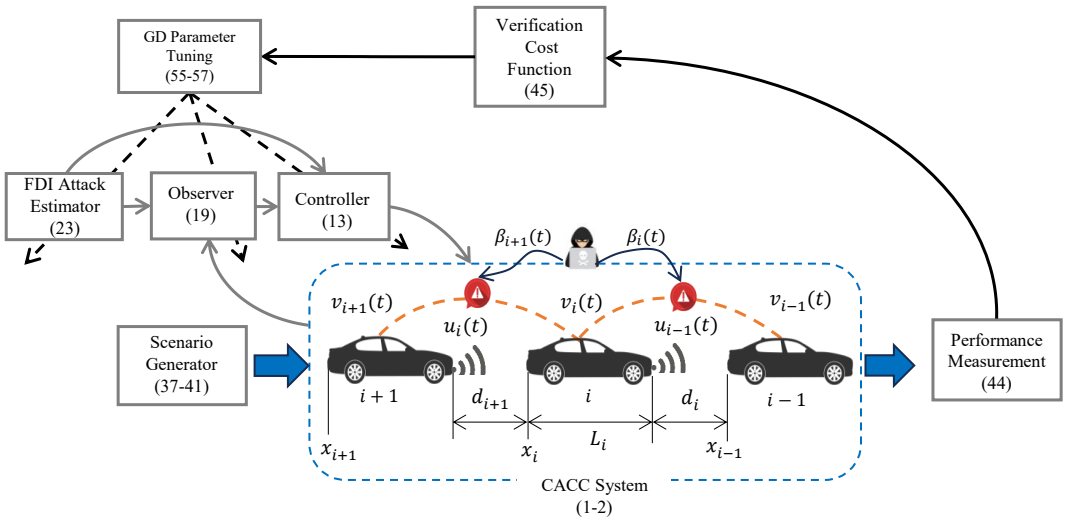

Fig. 2. The schematic of a string of vehicles affected by FDI attacks, alongside the proposed tuning framework.

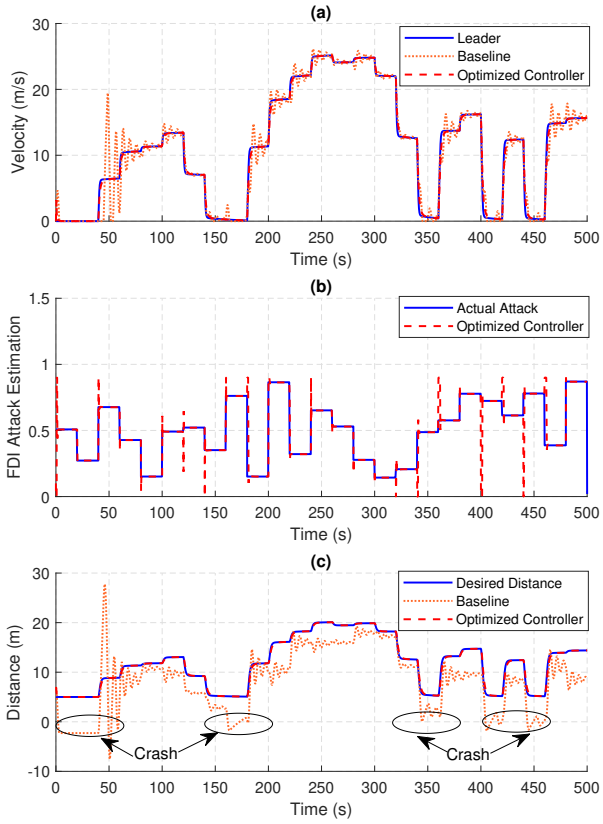

Fig. 3. Scenario S_{11} simulation results of (a) speed profile of the leader and follower vehicles, (b) FDI attack estimation results, (c) following distance between leader and follower vehicles for baseline and optimized controllers.

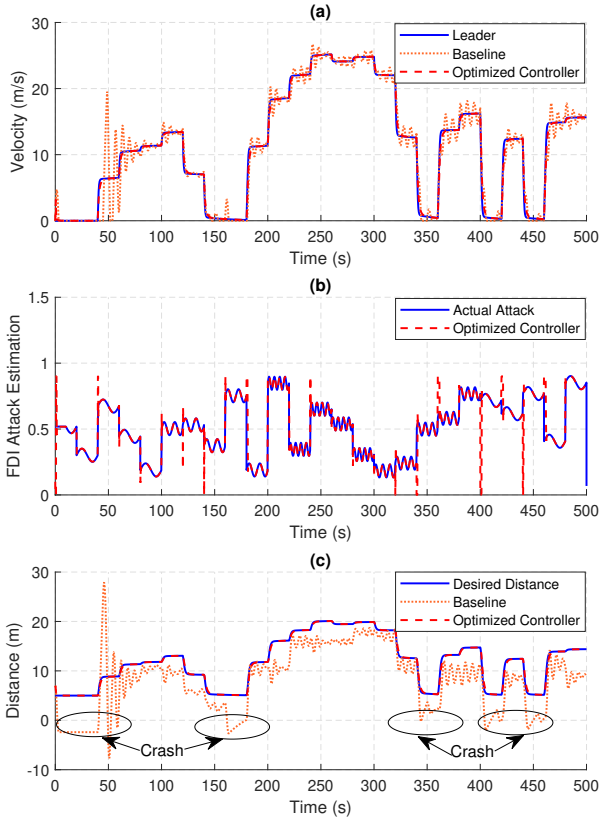

Fig. 4. Scenario S_{12} simulation results (a) Speed profile of the leader and follower vehicles, (b) FDI attack estimation results, (c) following distance between leader and follower vehicles for baseline, developed, and optimized controllers.

distance and resulting in several crashes, the optimized control system demonstrates satisfactory speed tracking and maintains a safe following distance. Furthermore, the optimized method successfully estimates the actual FDI attack profile.

B. Scenario S_{12}

In this scenario, the driving cycle is the FTP-75 and the FDI attack is designed as a variable-frequency sinusoidal signal with an amplitude of 0.1, added to the previously defined random FDI attack. As shown in Fig. 4, the baseline is unable to track the safe inter-vehicle distance and lead to several crashes while the optimized approach enhances speed tracking and safe following distance while minimizing the FDI attack estimation error.

C. Scenario S_{21}

To test the performance of the CACC system under more aggressive driving conditions, we used the US06 drive cycle,in presence of the random FDI attack similar to the S_{11}. The simulation results have been shown in Fig. 5. While the baseline results in multiple crashes during the stop-and-go segments of the drive cycle, the optimized method successfully maintains the safe following distance and accurately estimates the FDI attack.

D. Scenario S_{22}

This scenario applies the same combinatorial attack from S_{12} but aligns it with the US06 drive cycle. The simulation results of this test and verification scenario are presented in Fig. 6. While the baseline controller leads to multiple crashes during the test, the optimized controller achieves superior performance by maintaining a safe following speed and distance between the leader and follower vehicles, along with proper FDI attack estimation. Table II summarizes the RMS error in tracking the safe following distance for all scenarios, comparing the Baseline, our proposed optimization method, and the RL-based approach in [25]. The results indicate that the proposed method provides improved accuracy in maintaining the desired inter-vehicle distance.

Furthermore, to evaluate FDI attack estimation performance, Table III reports the RMS estimation error for the proposed GD-based optimization approach versus the RL method in [25]. As shown, the GD algorithm achieves a lower estimation error, demonstrating its superior performance.

Additionally, to evaluate the system performance in the presence of sensor noise, measurement noise was introduced into the follower vehicle's velocity readings. The results shown in Fig. 7 demonstrate that the optimized controller effectively attenuates the noise, maintaining accurate following-distance

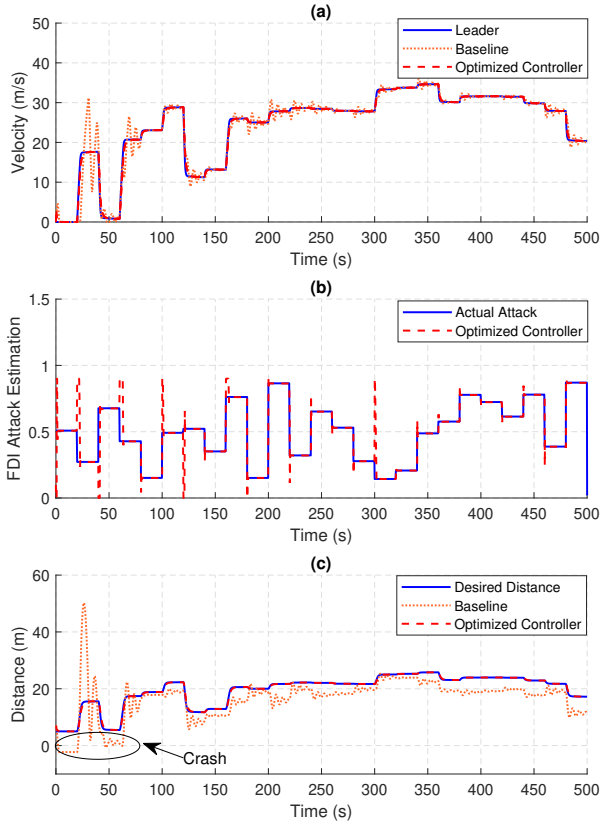

Fig. 5. Scenario S_{21} simulation results (a) Speed profile of the leader and follower vehicles, (b) FDI attack estimation results, (c) following distance between leader and follower vehicles for baseline, developed, and optimized controllers.

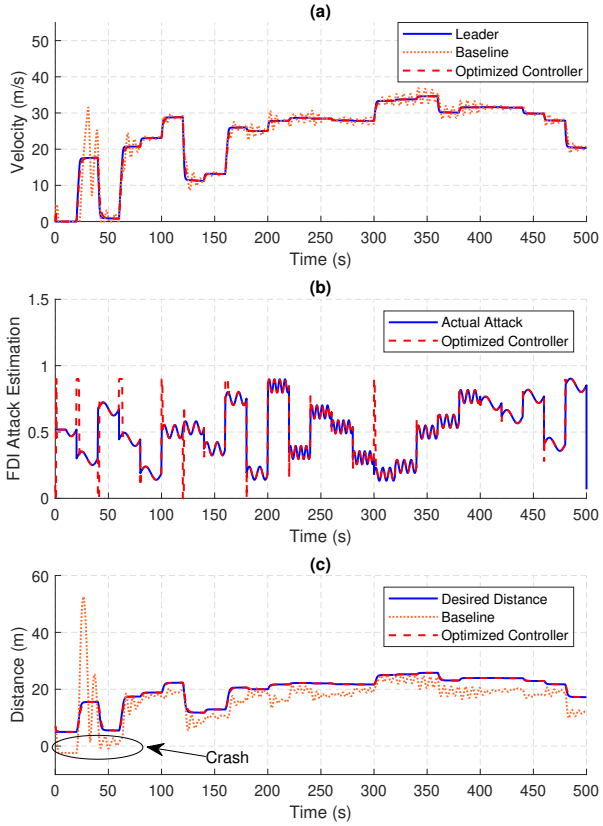

Fig. 6. Scenario S_{22} simulation results (a) Speed profile of the leader and follower vehicles, (b) FDI attack estimation results, (c) following distance between leader and follower vehicles for baseline, developed, and optimized controllers.

TABLE II
RMS ERROR IN THE SAFE FOLLOWING DISTANCE (m)

	S_{11}	S_{12}	S_{21}	S_{22}
Baseline	4.6064	4.6790	5.2991	5.5037
Optimized Controller	0.0526	0.0526	0.0527	0.0527
Approach in [25]	0.0647	0.0649	0.0705	0.0710

TABLE III
RMS ERROR IN FDI ATTACK ESTIMATION

	S_{11}	S_{12}	S_{21}	S_{22}
Optimized Controller	0.0781	0.0762	0.0848	0.0817
Approach in [25]	0.0781	0.0776	0.0868	0.0842

tracking while estimating the FDI attack with acceptable performance.

VII. Conclusion and Future Works

This work developed a secure Lyapunov-based CACC system capable of real-time FDI attack estimation and mitigation. We also conducted a systematic testing and tuning of the CACC algorithm to enhance its reliability using simulation-based analysis. Our approach leveraged approximate GD to minimize the mean square error with respect to the control gains, allowing us to iteratively refine their values for optimal performance. The results demonstrate that the GD approach effectively reduces the error, successfully converging to gain values that achieve the desired system behavior. This confirms the viability of our method for optimizing CACC algorithms across a wide range of scenarios, improving both accuracy and robustness. Future work could extend this methodology to incorporate additional real-world constraints, nonlinearity considerations, and adaptive learning techniques for even greater reliability in dynamic driving conditions.

This study has several limitations that warrant further investigation. First, the analysis assumes full knowledge of the lead vehicle's dynamic model, an assumption that may not hold in practical deployments. Future efforts could address this by developing CACC architectures that estimate unknown leader parameters or learning nonlinear leader dynamics using reinforcement learning or other machine learning–based techniques. Second, disturbances, model uncertainties, and communication delays—factors that frequently arise in real-world vehicle-to-vehicle networks—were not explicitly incorporated into the system model or the stability analysis. Extending the proposed framework to account for these effects would enhance its robustness and practical applicability. Third, the FDI attack was modeled as an additive malicious input. However, intelligent adversaries may employ more sophisticated and stealthy attack strategies, which would require advanced

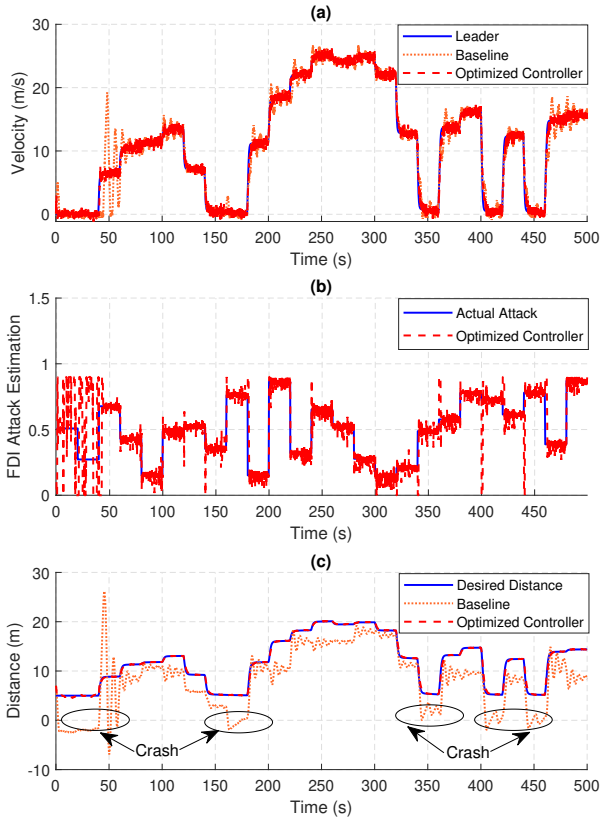

Fig. 7. Scenario S_{12} simulation results under sensor noise (a) Speed profile of the leader and follower vehicles, (b) FDI attack estimation results, (c) following distance between leader and follower vehicles for baseline, developed, and optimized controllers.

detection and estimation mechanisms beyond the scope of the current study. Finally, this work assumes that FDI attacks are continuous in time, whereas real-world attacks may occur intermittently or in a discrete-time manner. Addressing such scenarios would necessitate discrete-time stability analysis or event-triggered and hybrid control approaches, which remain important directions for future research.

Acknowledgment

Partial support of this research was provided by the National Science Foundation under Grant No. ECCS-EPCN-2241718. Any opinions, findings, and conclusions, or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the sponsoring agency.

Disclosure Statement

The authors declare no competing financial or non-financial interests.

References

[1] A. A. Hamid, N. S. Ishak, M. F. Roslan, and K. H. Abdullah, "Tackling human error in road crashes: An evidence-based review of causes and effective mitigation strategies," *Journal of Metrics Studies and Social Science*, vol. 2, no. 1, pp. 1–9, 2023.

[2] S. M. Hosseinian and H. Mirzahossein, "Efficiency and safety of traffic networks under the effect of autonomous vehicles," *Iranian Journal of Science and Technology, Transactions of Civil Engineering*, vol. 48, no. 4, pp. 1861–1885, 2024.

[3] B. Chen, Y. Chen, Y. Wu, Y. Xiu, X. Fu, and K. Zhang, "The effects of autonomous vehicles on traffic efficiency and energy consumption," *Systems*, vol. 11, no. 7, p. 347, 2023.

[4] A. Irshayyid, J. Chen, and G. Xiong, "A review on reinforcement learning-based highway autonomous vehicle control," *Green Energy and Intelligent Transportation*, vol. 3, no. 4, p. 100156, 2024.

[5] S. Xu, Q. Liu, Y. Hu, M. Xu, and J. Hao, "Decision-making models on perceptual uncertainty with distributional reinforcement learning," *Green Energy and Intelligent Transportation*, vol. 2, no. 2, p. 100062, 2023.

[6] H. Faghihian, J. Holland, and A. Sargolzaei, "Introduction to autonomous vehicles," in *Handbook of Power Electronics in Autonomous and Electric Vehicles*, pp. 1–16, Elsevier, 2024.

[7] J. Wang, L. Zhang, Y. Huang, J. Zhao, and F. Bella, "Safety of autonomous vehicles," *Journal of advanced transportation*, vol. 2020, pp. 1–13, 2020.

[8] J. Gorospe, S. Hasan, A. A. GÓMEZ, and E. Uhlemann, "Towards resilient cacc systems for automated vehicles," *IEEE Open Journal of Intelligent Transportation Systems*, 2025.

[9] H. Liu and R. Jiang, "Improving comfort level in traffic flow of cacc vehicles at lane drop on two-lane highways," *Physica A: Statistical Mechanics and its Applications*, vol. 575, p. 126055, 2021.

[10] H. Faghihian and A. Sargolzaei, "Energy efficiency of connected autonomous vehicles: A review," *Electronics*, vol. 12, no. 19, p. 4086, 2023.

[11] Y. Zhu, D. Zhao, and Z. Zhong, "Adaptive optimal control of heterogeneous cacc system with uncertain dynamics," *IEEE Transactions on Control Systems Technology*, vol. 27, no. 4, pp. 1772–1779, 2018.

[12] F. Navas, V. Milanés, C. Flores, and F. Nashashibi, "Multi-model adaptive control for cacc applications," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 2, pp. 1206–1216, 2020.

[13] C. Huang, S. Coskun, J. Wang, P. Mei, and Q. Shi, "Robust h_∞ dynamic output-feedback control for cacc with rosss subject to rodas," *IEEE Transactions on Vehicular Technology*, vol. 71, no. 1, pp. 137–147, 2021.

[14] H. Xing, J. Ploeg, and H. Nijmeijer, "Robust cacc in the presence of uncertain delays," *IEEE Transactions on Vehicular Technology*, vol. 71, no. 4, pp. 3507–3518, 2022.

[15] 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 Transactions on Intelligent Transportation Systems*, vol. 23, no. 4, pp. 3418–3429, 2020.

[16] J. Cunningham-Rush, J. Holland, S. Noei, and A. Sargolzaei, "Designing and testing a secure cooperative adaptive cruise control under false data injection attack," in *2023 IEEE Conference on Dependable and Secure Computing (DSC)*, pp. 1–8, IEEE, 2023.

[17] P. Ansari-Bonab, J. C. Holland, J. Cunningham-Rush, S. Noei, and A. Sargolzaei, "Secure control design for cooperative adaptive cruise control under false data injection attack," *IEEE Transactions on Intelligent Transportation Systems*, 2024.

[18] 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 transactions on intelligent transportation systems*, vol. 23, no. 7, pp. 8692–8703, 2021.

[19] P. A. Bonab and A. Sargolzaei, "A nonlinear control design for cooperative adaptive cruise control with time-varying communication delay," *Electronics*, vol. 13, no. 10, p. 1875, 2024.

[20] P. Ansari Bonab, F. Javidi-Niroumand, and A. Sargolzaei, "Secure control design for cooperative adaptive cruise control with a time-varying input delays under false data injection attacks," *International Journal of Systems Science*, vol. 56, no. 2, pp. 375–393, 2025.

[21] H. Alemayehu and A. Sargolzaei, "Testing and verification of connected and autonomous vehicles: A review," *Electronics*, vol. 14, no. 3, p. 600, 2025.

[22] A. Ala'J, A. Sargolzaei, and M. I. Akbaş, "Autonomous vehicles scenario testing framework and model of computation: On generation and coverage," *IEEE Access*, vol. 9, pp. 60617–60628, 2021.

[23] A. J. Alnaser, J. Holland, and A. Sargolzae, "Employing a model of computation for testing and verifying the security of connected and autonomous vehicles," *SAE International Journal of Connected and Automated Vehicles*, vol. 7, no. 12-07-03-0020, 2024.

[24] J. C. Holland, F. Javidi-Niroumand, A. Ala'J, and A. Sargolzaei, "A testing and verification approach to tune control parameters of coopera-

tive driving automation under false data injection attacks," *IEEE Access*, 2024.

[25] F. Javidi-Niroumand and A. Sargolzaei, "A reinforcement learning-based parameter tuning approach for a secure cooperative adaptive cruise control system," *SAE International Journal of Connected and Automated Vehicles*, vol. 8, no. 12-08-04-0033, 2025.

[26] A. Sargolzaei, B. C. Allen, C. D. Crane, and W. E. Dixon, "Lyapunov-based control of a nonlinear multiagent system with a time-varying input delay under false-data-injection attacks," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 4, pp. 2693–2703, 2021.

[27] P. M. Patre, W. MacKunis, K. Kaiser, and W. E. Dixon, "Asymptotic tracking for uncertain dynamic systems via a multilayer neural network feedforward and rise feedback control structure," *IEEE Transactions on Automatic Control*, vol. 53, no. 9, pp. 2180–2185, 2008.

[28] A. J. Alnaser, A. Sargolzaei, and M. I. Akbas, "Autonomous vehicles scenario testing framework and model of computation: On generation and coverage," *IEEE Access*, vol. 9, pp. 60617–60628, 2021.

[29] A. J. Alnaser, M. I. Akbas, A. Sargolzaei, and R. Rahul, "Autonomous vehicles scenario testing framework and model of computation," *SAE International Journal of Connected and Automated Vehicles*, 2019.

[30] A. J. Alnaser, J. Holland, and A. Sargolzae, "Employing a model of computation for testing and verifying the security of connected and autonomous vehicles," *SAE International Journal of Connected and Automated Vehicles*, 2024.