Secure Control Design for Cooperative Adaptive Cruise Control Under False Data Injection Attack

Parisa Ansari-Bonab, James C. Holland, *Graduate Student Member, IEEE*, Jonas Cunningham-Rush, Shirin Noei, and Arman Sargolzaei, *Senior Member, IEEE*

***Abstract*— Cooperative adaptive cruise control (CACC) is one of the many advanced driver assistance systems (ADAS) that leverage communication between nearby vehicles to maintain speed while ensuring safe following distances. The current CACC algorithms are designed with the assumption that the communication channel is secure. However, the use of communication channels makes CACC susceptible to attacks, such as False data injection (FDI). This paper develops a novel secure nonlinear controller and a nonlinear observer which can estimate FDI attacks in real-time. Furthermore, this paper shows that the developed controller and FDI attack estimation techniques ensure semi-globally uniformly bounded tracking under FDI attacks, noise, and disturbances. The efficaciousness of the proposed CACC algorithm was demonstrated in simulation and through experimental implementation. During testing using both methodologies, the controller was able to maintain a safe following distance and estimate FDI attacks and noise in real-time.**

***Index Terms*— Secure control design, nonlinear observer, attack estimation, false data injection attack, Lyapunov stability, cooperative adaptive cruise control.**

I. Introduction

IT IS estimated that an average of 6 million car collisions occur every year in the United States [1]. The National Highway and Traffic Safety Administration (NHTSA) also estimated that human error contributes to 94%-96% of all automobile accidents in the United States [2].

In recent years, technology has advanced in leaps and bounds. Due to this, advanced driver assistance systems (ADAS) have rapidly pervaded the automotive industry. Automated vehicles (AVs) use sensors to perceive the world around them and support the driver to reduce the likelihood of a crash. Further improvement of AVs can be achieved by adding connectivity between vehicles, creating connected automated vehicles (CAVs). CAVs are capable of communicating with each other and infrastructure to maximize efficiency in terms of traffic, energy, and safety [3], [4], [5]. Furthermore, CAVs possess the ability to identify roadway threats and hazards and disseminate that information to other vehicles.

CAVs provide numerous benefits, the most prominent being improved transportation that eases the driver's task load. With vehicles being able to send and receive information about the environment ahead of it, they can better prepare themselves for adjusting to the flow of traffic and possible obstructions. CAVs reduce the energy consumption of vehicles by eliminating excessive acceleration, deceleration, and aerodynamic drag [6]. Vehicle platoons have been proven to decrease the aerodynamic drag of the entire convoy [7]. Another benefit of vehicle strings is increasing the number of vehicles that a given highway can safely accommodate, improving the entire efficiency of the roadway. Vehicles following at a closer distance reduce the time delay between vehicles and maximizes the vehicle capacity of the road. The final, and most important, benefit of CAVs is the potential to drastically reduce crashes and traffic fatalities [8]. A study by Papadoulis et. al [9] demonstrates that as CAVs adoption rate increases, traffic conflicts could decrease by as much as 94%, at full CAVs adoption.

Adaptive cruise control (ACC) is an ADAS that adjusts the speed of a vehicle to maintain a safe following distance from a lead vehicle on the roadway. This process is reliant strictly upon onboard sensors, such as radar, lidar, and cameras. One of the major drawbacks of ACC is its inability to form vehicle strings, effectively; because of the transmission delay for CAVs, which averages 1.5 seconds per vehicle length [10]. The reason is the lengthy perception and decision-making pipeline through the onboard sensors, processors, control, and actuators. To address this issue, cooperative adaptive cruise control (CACC) was designed [11].

CACC builds upon the foundation of ACC by enabling vehicle-to-everything (V2X) communication between vehicles and intelligent transportation systems, allowing for advanced traffic management [12]. This information is broadcast continuously to provide other vehicles in the loop with real-time data in order to improve performance [13]. Other benefits of CACC include shorter following distances, time gaps, and improved stability against oscillations in the flow of traffic [14]. ACC is susceptible to oscillations in traffic flows that are compounded further along the vehicle string. CACC mitigates the majority of this problem as the vehicles resemble the leading vehicle more closely [15]. In a favorable environment, CACC-equipped vehicles will acquire information sent from the

Manuscript received 21 December 2022; revised 1 January 2024 and 7 March 2024; accepted 19 April 2024. Date of publication 13 May 2024; date of current version 1 August 2024. This work was supported in part by the National Science Foundation under Grant CNS-1919855 and Grant ECCS-EPCN-2241718. The Associate Editor for this article was S. Kumari. *(Corresponding author: James C. Holland.)*

Parisa Ansari-Bonab, James C. Holland, and Arman Sargolzaei are with the Department of Mechanical Engineering, University of South Florida, Tampa, FL 33620 USA (e-mail: holland33@usf.edu; a.sargolzaei@gmail.com).

Jonas Cunningham-Rush is with the Department of Mechanical Engineering, Tennessee Technological University, Cookeville, TN 38505 USA.

Shirin Noei is with the Department of Civil and Coastal Engineering, University of Florida, Gainesville, FL 32611 USA.

Digital Object Identifier 10.1109/TITS.2024.3395208

leading vehicle and adjust accordingly, which greatly reduces the delay between vehicles, resulting in improved energy efficiency, reduced travel time, and reduced collisions [16].

Despite all the benefits of CACC, since it uses communication channels to transmit data, it is vulnerable to different types of attacks, such as false data injection (FDI), time delay switch (TDS), and denial of service (DoS) [17]. In FDI attack, an adversary can gain access to the communication channels and inject FDI attacks into the transmitted information [18].

Each attack challenges the system in a different manner depending on where the attack has been injected. This is evident in [19] where the origin of the attack is at the application-layer of the CACC system. They effectively mitigated DoS and FDI attacks through the use of a bi-objective proportional-integral-derivative (PID) controller and a fuzzy detector, to take specific actions against the attacks.

Further efforts into mitigating DoS attacks are shown in [20], [21], and [22]. Research in [20] designed a system that can identify the malicious vehicle in the loop and isolate it by comparing the behaviors of a normal vehicle versus ones with abnormal behavior, using fuzzy Petri nets to detect packet drops. The detection of DoS attacks was also outlined in [21], which used a scheme that logs the node at which a packet drop occurred. The repetitive nature of packet drops indicated an attack at that node. It is then isolated from the network, rerouting information to its neighbors. This problem was also solved similarly in [22], using a packet detection algorithm that incorporated bandwidth and entropy and isolated the malicious nodes, improving the network's efficiency. Due to the nature of TDS attacks, the above-mentioned techniques are unable to detect and mitigate this form of attack. In the case of TDS attacks, the research in [23], [24], and [25] has shown effectiveness at detecting and mitigating TDS attacks. In [23], a time delay estimator was used to detect the maximum allowable delay to a system for it to remain stable. For a delay beyond the allowed threshold, an emergency controller is used until the attack subsides or stability is reached. In [24] they devised an adaptive channel technique and a state estimator to quickly stabilize the system under TDS attacks. Authors in [25] devised a robust feedback controller that was not affected by the distribution of out-of-order information, a variation of the TDS attack.

Several studies focus on FDI attacks on a CACC system during the past several years in [26], [27], [28], [29], [30], [31], [32], and [33]. In [26], they designed a partial differential equation (PDE) to detect the FDI attack on a platoon of vehicles. An attack was determined by comparing its signature in a no-attack and attack scenario. Differing strategies for mitigating FDI attacks are studied in [27]. They compared different approaches and determined that an attack-resilient controller provided the best potential for mitigation. They did not, however, develop a control or detection algorithm for a CACC system. Additionally, in [28] they concluded that a detection algorithm alone does not perform well enough against FDI attacks, instead, showing that the combination of a resilient controller and effective detection algorithm performs the best at attack mitigation. In [29], only a detection algorithm was developed. The algorithm is a cloud-based method that accurately detects an FDI attack in order to isolate the attacker. This approach also did not create a resilient controller to overcome the FDI attack once detected.

Another idea to mitigate FDI attacks that propagate through communication channels is to disable the connectivity of CACC and operate as purely ACC. However, in [32], their approach was able to maintain CACC capabilities. This was achieved by implementing a consensus-based control system that checks each vehicle at every time step for anomalies to identify and exclude a malicious vehicle from the loop upon detection. This paper focused on designing a secure controller and did not include a detection algorithm. In [33], they used a neural network (NN) approach to detect and estimate the FDI attack. The NN approach with their designed control strategy proved effective against the injected attack. However, the stability of the proposed method has not been investigated.

Unlike other papers in the literature, this paper aims to develop a novel secure Lyapunov-based controller. Our study introduces a control and estimation technique that integrates both model-based and learning-based approaches. The goal is to improve accuracy and processing time. Unlike traditional methods that exclusively employ either learning-based or model-based techniques, our proposed method strikes a balance between processing time and accuracy.[1] The designed novel controller and observer are able to maintain the real-time tracking of the lead vehicle while the communication channel is under FDI attacks and measurement noise. Additionally, this paper, unlike others, will also validate its controller and estimation accuracy in real-world. The contributions of this paper are summarized as follows: (i) a novel control strategy is developed which is resilient under FDI attacks and measurement noise, (ii) FDI attacks and measurement noise estimation technique is developed which is able to estimate FDI attacks and measurement noise in real-time and with high accuracy, and (iii) the stability of the developed nonlinear controller, nonlinear observer, and FDI attacks and measurement noise estimator is illustrated using Lyapunov stability, and finally (iv) the effectiveness of the proposed resilient controller is shown both in simulation and experimental setup.

The rest of the paper is organized as follows: mathematical model of CACC under FDI attacks and measurement noise is formulated in Section II, section III describes the problem statement of the paper, section IV illustrates the proposed solution including controller design, FDI attacks and measurement noise estimator, and observer design. The stability analysis of the designed observer and controller, and FDI attacks and measurement noise estimation is explained in section V. Section VI shows the results. Finally, section VII explains the conclusion of the paper.

II. Mathematical Model of CACC Under FDI Attacks and Measurement Noise

CACC-equipped string of vehicles are shown in Figure 1. It is assumed that the control command, velocity, and position

[1] There is a trade off between accuracy and processing time. Learning-based method has computational time problem and model-based methods needs highly accurate model of system. Using an integration of these two methods could improve the accuracy and processing time.

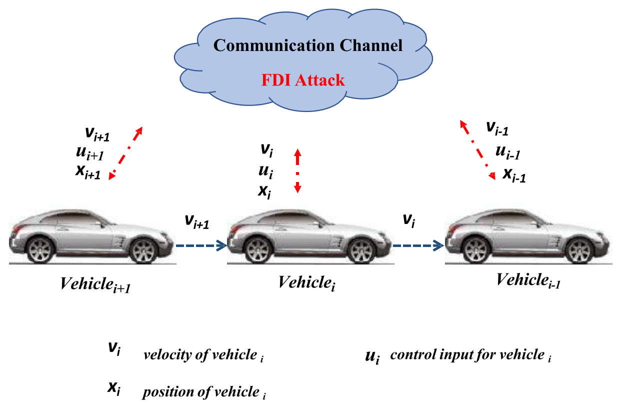

Communication Channel
FDI Attack
v_{i+1} u_{i+1} x_{i+1}
v_i u_i x_i
v_{i-1} u_{i-1} x_{i-1}
v_{i+1}
v_i
Vehicle$_{i+1}$
Vehicle$_i$
Vehicle$_{i-1}$
v_i velocity of vehicle $_i$
u_i control input for vehicle $_i$
x_i position of vehicle $_i$

Fig. 1. CACC-equipped string of vehicles.

from the lead vehicle are relayed to the following vehicle. For a string of homogeneous vehicles with the same models and CACC capabilities, the dynamics model of the vehicles is described as below which is the dynamic model of a real vehicle and was derived through an experimental setup

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

where $i \in \{2, \cdots n\}$ denotes the follower vehicle, n is the number of vehicles, and $i-1$ indicates the lead vehicle. It means that each vehicle follows its own leader. The equations are for follower i with the leader $i-1$. In Equation (1), $a_i \in \mathbb{R}$ and $b_i \in \mathbb{R}$ are the constant parameters which were obtained from experimental analysis in VI. Also $x_i \in \mathbb{R}$, $v_i \in \mathbb{R}$, $u_i \in \mathbb{R}$, and $d_i \in \mathbb{R}$ represent the position, velocity, control input, and external disturbance, respectively.

Assumption 1: It is assumed that the vehicles' movement is in one dimension and they are moving along x axis [14], [26], [34], [35].[2]

Assumption 2: The disturbance is assumed to be continuous and bounded by a known constant such that $\|d_i(t)\| < \bar{d}_i$ for $t \geq t_0$, where $\bar{d}_i \in \mathbb{R}_{>0}$ [36].

A. FDI Attacks and Measurement Noise Representation

FDI attacks and noise are injected into the communication network of connected vehicles such that vehicles that access that information are obtaining corrupted data. This causes instability in a platoon of vehicles, resulting in possible collisions. For this paper, we assume that control command is the only parameter affected by the attack, interpreted as equation (3). The attack and noise affect the output, which transforms it into the observed output as

$$\pi_i(u_{i-1}(t)) \triangleq u_{i-1}(t) + \beta_i(t), \tag{2}$$

where $\pi_i \in \mathbb{R}$ is the attack function, u_{i-1} is the leader control command, and β_i is defined as

$$\beta_i(t) \triangleq \omega_i(t) + \theta_i(t), \tag{3}$$

where $\omega_i \in \mathbb{R}$ is the bounded, unknown, continuous, and time-varying FDI attack, and θ_i denotes a bounded Gaussian measurement noise.

Assumption 3: $\beta_i(t)$ is assumed to be bounded and differentiable such that $|\beta_i(t)| \leq \bar{\beta}_i$, where $t \geq t_0$ and $\bar{\beta}_i$ is a positive constant.

III. Problem Statement

The main objective of this paper is to design a secure controller that guarantees a safe distance between vehicles is maintained, even while under FDI attacks, measurement noise, and disturbances. The CACC algorithm requires a control signal from the lead vehicle in real-time. However, adversarial manipulation challenges this process, which potentially leads to collisions. Therefore, our second objective is to design a nonlinear observer and FDI attacks and noise estimation mechanism to estimate the FDI attacks and noise in real-time and mitigate their effects on the controller. To quantify these objectives we defined some error signals as distance error, state estimation error, and FDI attacks and noise estimation error. The distance error, $e_i : [t_0, \infty) \to \mathbb{R}$ is defined as

$$e_i(t) \triangleq x_i(t) - x_{i-1}(t) + D_i + x_{d_i}(t), \tag{4}$$

where $D_i \in \mathbb{R}$ is the length of vehicle$_i$, and $x_{d_i} \in \mathbb{R}$ is the desired distance between vehicles.

Assumption 4: The desired distance as well as its first and second derivatives are assumed to be bounded by positive known constants, $x_{d_i}, \dot{x}_{d_i}, \ddot{x}_{d_i} \in \mathcal{L}_\infty$ [37].

To facilitate the design process and stability analysis, an auxiliary error equation is proposed as

$$r_i(t) \triangleq \dot{e}_i(t) + \alpha_i e_i(t), \tag{5}$$

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

The follower vehicle are relayed false information from the leader during FDI attacks and noise. Therefore, the accuracy of the observer needs to be measured and maintained. A state estimate error $\tilde{x}_{i-1} : [t_0, \infty) \to \mathbb{R}$, is described as

$$\tilde{x}_{i-1}(t) \triangleq x_{i-1}(t) - \hat{x}_{i-1}(t), \tag{6}$$

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

To facilitate the stability analysis for the state estimation, another auxiliary error signal $\tilde{r}_{i-1} : [t_0, \infty) \to \mathbb{R}$ can be defined as

$$\tilde{r}_{i-1}(t) \triangleq \dot{\tilde{x}}_{i-1}(t) + \alpha_{i-1}\tilde{x}_{i-1}(t), \tag{7}$$

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

For determining the accuracy of the control signal estimation, an estimation error for the control signal, $\tilde{u}_{i-1} : [t_0, \infty) \to \mathbb{R}^{n_i}$, is defined as

$$\tilde{u}_{i-1} \triangleq u_{i-1} - \hat{u}_{i-1}, \tag{8}$$

where $\hat{u}_{i-1} \in \mathbb{R}$ and $u_{i-1} \in \mathbb{R}$ are the estimated and actual control signal of the leader, respectively.

Defining $\bar{u}_{i-1} \triangleq u_{i-1} + \beta_i$ and $\hat{u}_{i-1} \triangleq \bar{u}_{i-1} - \hat{\beta}_i$ yields

$$\tilde{u}_{i-1} = u_{i-1} - \bar{u}_{i-1} + \hat{\beta}_i, \tag{9}$$

[2] Considering the close proximity in which vehicles operate under CACC, it is reasonable to assume their movement along a singular dimension, particularly the x-axis.

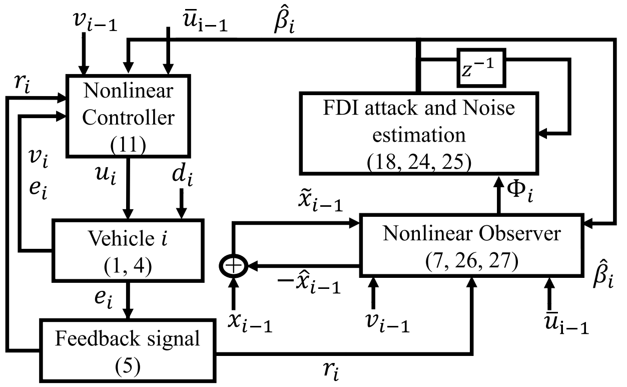


Fig. 2. Proposed solution diagram.

where $\hat{\beta}_i \in \mathbb{R}$ is the estimated FDI attack and noise.

To measure the accuracy of the FDI attack and noise estimation, the estimation error for the FDI attack and noise, $\tilde{\beta}_i : [t_0, \infty) \to \mathbb{R}^{n_i}$, is defined as

$$\tilde{\beta}_i(t) \triangleq \beta_i(t) - \hat{\beta}_i(t). \tag{10}$$

IV. Proposed Solution

In order to address problem statement, we proposed a nonlinear Lyapunov based controller, a FDI attack and noise estimator, and a nonlinear observer which will be discussed in detail in the following subsections. Also, Figure 2 shows the proposed solution diagram which is an integration of nonlinear controller, observer, and FDI attack and noise estimator.

A. Controller Design

The control signal was designed using the Lyapunov stability analysis in section V as

$$\begin{aligned} u_i(t) \triangleq\ & \frac{a_i}{b_i} v_i(t) - \frac{a_{i-1}}{b_{i-1}} v_{i-1}(t) + \bar{u}_{i-1} - \hat{\beta}_i(t) - \frac{1}{b_i}\ddot{x}_{d_i}(t) \\ & - \frac{\alpha_i}{b_i} r_i(t) + \frac{\alpha_i^2}{b_i} e_i(t) - \frac{1}{b_i} e_i(t) - \frac{K_{1_i}}{b_i} r_i(t), \end{aligned} \tag{11}$$

where $K_{1_i} \in \mathbb{R}_{>0}$ is a gain specified by the user.

Time derivative of the error signals should be obtained to be used in stability analysis section. Taking the derivative of equation (5) and substituting (4) yields the closed loop form of the system as

$$\dot{r}_i(t) = \ddot{x}_i(t) - \ddot{x}_{i-1}(t) + \ddot{x}_{d_i}(t) + \alpha_i \dot{e}_i(t). \tag{12}$$

Replacing $\ddot{x}_i$ and $\ddot{x}_{i-1}$ and (9) into (12) produces

$$\begin{aligned} \dot{r}_i(t) = & -a_i v_i(t) + b_i u_i(t) + d_i(t) + a_{i-1} v_{i-1}(t) \\ & - b_i \bar{u}_{i-1}(t) + b_i \hat{\beta}_i - d_{i-1} + \ddot{x}_{d_i}(t) + \alpha_i \dot{e}_i(t). \end{aligned} \tag{13}$$

Substituting (5) and (11) into (13) results in

$$\dot{r}_i = b_i \tilde{\beta}_i - K_{1_i} r_i - e_i + d_i - d_{i-1}. \tag{14}$$

B. FDI Attack and Measurement Noise Estimation

The detailed observer design in the subsequent subsection includes a neural network-based FDI attack and noise estimation algorithm and state estimator. The FDI attack and noise, β_i, occurs over a non-compact domain, so a nonlinear mapping, $M_{\beta_i} : [t_0, \infty) \to [0, 1]$ is required to map time to a compact spatial domain given as

$$M_{\beta_i} \triangleq \frac{c_{\beta_i}(t - t_0)}{c_{\beta_i}(t - t_0) + 1}, \quad \zeta \in [0, 1], \ t \in [t_0, \infty), \tag{15}$$

where $c_{\beta_i} \in \mathbb{R}_{>0}$ describes a user-specified gain [38]. Consequently the FDI attack and noise, $\beta_i(t)$, is mapped into the compact domain ζ as

$$\beta_i(t) = \beta_i(M_{\beta_i}^{-1}(\zeta)) \triangleq \beta_{M_{\beta_i}}(\zeta), \tag{16}$$

where $\beta_{M_{\beta_i}} : [0, 1] \to \mathbb{R}^{n_i}$ is now defined.

Our developed neural network relies on real-time input data to update its weights is used to estimate the FDI attacks which is described as

$$\beta_{M_{\beta_i}}(\zeta) = W_i^T \sigma(V_i^T \delta_i) + \gamma_i, \tag{17}$$

where $\delta_i \in \mathbb{R}^{(n_i+1)\times 1}$ signifies the inputs, vectors $W_i \in \mathbb{R}^{(n_i+1)\times n_i}$ and $V_i \in \mathbb{R}^{(n_i+1)\times n_n}$ indicate the unknown ideal weights, and n_n represents the number of neurons in the hidden layer. Additionally, $\sigma(\cdot) \in \mathbb{R}^{(n_n+1)}$ denotes an activation function vector and $\gamma_i \in \mathbb{R}^{n_i}$ signifies a bounded signal.

Considering respect to the spatial domain, the NN output which is the estimation of the FDI attack and noise can be described as

$$\hat{\beta}_i \triangleq \hat{W}_i^T \sigma(\hat{V}_i^T \delta_i), \tag{18}$$

where $\hat{W}_i \in \mathbb{R}^{(n_i+1)\times n_i}$, $\hat{V}_i \in \mathbb{R}^{(n_i+1)\times n_n}$ represent the estimated ideals weights, and δ_i is given as

$$\delta_i \triangleq [1, \phi_i^T]^T. \tag{19}$$

where ϕ_i is defined as

$$\phi_i \triangleq b_i(r_i - \tilde{r}_{i-1}). \tag{20}$$

Substituting (16), (17), and (18) into (10) yields

$$\tilde{\beta}_i = W_i^T \sigma(V_i^T \delta_i) - \hat{W}_i^T \sigma(\hat{V}_i^T \delta_i) + \gamma_i. \tag{21}$$

A Taylor's series approximation is applied resulting

$$\tilde{\beta}_i = \tilde{W}_i^T \sigma(\hat{V}_i^T \delta_i) + \hat{W}_i^T \sigma'(\hat{V}_i^T \delta_i)\tilde{V}_i^T \delta_i + N_{n_i}, \tag{22}$$

given

$$N_{n_i} \triangleq \tilde{W}_i^T \sigma'(\hat{V}_i^T \delta_i)\tilde{V}_i^T \delta_i + W_i^T \vartheta(\tilde{V}_i^T \delta_i) + \gamma_i, \tag{23}$$

where $\tilde{V}_i = V_i - \hat{V}_i$ is the inner NN weight error, $\tilde{W}_i = W_i - \hat{W}_i$ is the outer NN weight error, ϑ denotes higher order terms, and N_{n_i} is bounded such that $\|N_{n_i}\| \leq \bar{n}_{n_i}$, where $\bar{n}_{n_i} \in \mathbb{R}_{>0}$.

Resulting from the upcoming stability analysis, the updating laws for the NN weights are described as

$$\dot{\hat{W}}_i = proj(\Gamma_{1_i} \sigma(\hat{V}_i^T \delta_i)|\phi_i|), \tag{24}$$

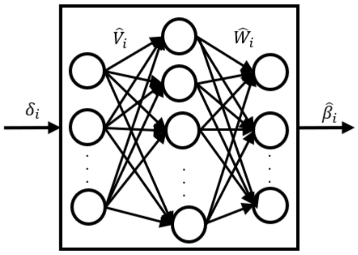


Fig. 3. Neural network diagram.

and

$$\dot{\hat{V}}_i = proj(\Gamma_{2_i}^T |\phi_i| \hat{W}_i^T \sigma(\hat{V}_i^T \delta_i)), \tag{25}$$

where the function proj denotes a Lipschitz continuous projection operator defined in [39], and $\Gamma_{1_i}, \Gamma_{2_i} \in \mathbb{R}^{n_i \times n_i}$ are definite positive matrices.

Figure 3 which shows the diagram of NN is a clear demonstration of input, output, layers, and weights of layers.

C. Observer Design

Based on the stability analysis in Section V, the nonlinear observer for vehicle i is designed as

$$\ddot{\hat{x}}_{i-1}(t) = -a_{i-1}v_{i-1}(t) + b_{i-1}\bar{u}_{i-1}(t) - b_{i-1}\hat{\beta}_i + L_{1_i}\tilde{r}_{i-1} + \alpha_{i-1}\tilde{r}_{i-1} - \alpha_{i-1}^2\tilde{x}_{i-1} + \tilde{x}_{i-1}, \tag{26}$$

where L_{1_i} represents a user-defined gain

Taking the derivative of (7) with respect to time yields

$$\dot{\tilde{r}}_{i-1}(t) = \ddot{\tilde{x}}_{i-1}(t) + \alpha_{i-1}\dot{\tilde{x}}_{i-1}(t). \tag{27}$$

After substituting (27) and (7) with simplification, the equation becomes

$$\dot{\tilde{r}}_{i-1}(t) = \ddot{x}_{i-1}(t) - \ddot{\hat{x}}_{i-1}(t) + \alpha_{i-1}\tilde{r}_{i-1}(t) - \alpha_{i-1}^2\tilde{x}_{i-1}(t). \tag{28}$$

Further simplification and variable substitution yields

$$\dot{\tilde{r}}_{i-1}(t) = -a_{i-1}v_{i-1}(t) + b_{i-1}u_{i-1}(t) + d_{i-1}(t) - \ddot{\hat{x}}_{i-1} + \alpha_{i-1}\tilde{r}_{i-1}(t) - \alpha_{i-1}^2\tilde{x}_{i-1}(t). \tag{29}$$

Substituting (26), the final error equation can be further simplified into

$$\dot{\tilde{r}}_{i-1}(t) = -b_{i-1}\tilde{\beta}_i - L_{1_i}\tilde{r}_{i-1}(t) - \tilde{x}_{i-1}(t) + d_{i-1}(t), \tag{30}$$

which will be used in stability analysis section.

V. Stability Analysis

For the sake of simplicity (t) was dropped in further calculations. Consider $V_{L_i} : \mathbb{R}^5 \times [0, \infty) \to \mathbb{R}_{\geq 0}$, a radially unbounded, positive definite, continuously differentiable Lyapunov function displayed as

$$V_{L_i} = \frac{1}{2}e_i^2 + \frac{1}{2}r_i^2 + \frac{1}{2}\tilde{x}_{i-1}^2 + \frac{1}{2}\tilde{r}_{i-1}^2 + H_i, \tag{31}$$

where $H_i : [t_0, \infty) \to \mathbb{R}_{\geq 0}$ is defined as

$$H_i \triangleq \frac{1}{2}tr(\tilde{W}_i^T \Gamma_{1_i}^{-1} \tilde{W}_i) + \frac{1}{2}tr(\tilde{V}_i^T \Gamma_{2_i}^{-1} \tilde{V}_i). \tag{32}$$

Since $\tilde{W}_i$ and $\tilde{V}_i$ are bounded, H_i is bounded by $|H_i| \leq H_{i,max}$ where $H_{i,max} \in \mathbb{R}_{>0}$. Furthermore, let $p_i \in \mathbb{R}^{4ni}$ be defined as

$$p_i \triangleq [e_i^T, r_i^T, \tilde{r}_{i-1}^T, \tilde{x}_{i-1}^T]^T, \tag{33}$$

and let ψ_{1_i} and ψ_{2_i} be defined as

$$\psi_{1_i} \triangleq \frac{1}{2}\|p_i\|^2, \tag{34}$$

and

$$\psi_{2_i} \triangleq \|p_i\|^2. \tag{35}$$

Let the following be the sufficient conditions that are obtained from (51) to

$$\begin{aligned} \alpha_{i-1} &> 0, \\ \alpha_i &> 0, \\ L_{1_i} &> \frac{1}{2\varepsilon_1} + \frac{1}{2\varepsilon_4}, \\ K_{1_i} &> \frac{1}{2\varepsilon_2} + \frac{1}{2\varepsilon_0}, \end{aligned} \tag{36}$$

where ε_0, ε_1, ε_2, ε_3, and ε_4 denote positive known constants.

Based on the sufficient conditions in (36), positive constants, α_{1_i} and α_{2_i} can be written as

$$\alpha_{1_i} \triangleq L_{1_i} - \frac{1}{2\varepsilon_1} - \frac{1}{2\varepsilon_4}, \tag{37}$$

$$\alpha_{2_i} \triangleq K_{1_i} - \frac{1}{2\varepsilon_2} - \frac{1}{2\varepsilon_0}, \tag{38}$$

where α_{3_i} is defined under (52).

Consequently φ_i is defined as

$$\varphi_i \triangleq \frac{\varepsilon_0}{2}\bar{n}_{n_i}^2 + \frac{\varepsilon_1}{2}\bar{n}_{n_i}^2 + \frac{\varepsilon_2}{2}\bar{d}_i^2 + \frac{\varepsilon_3}{2}\bar{d}_{i-1}^2 + \frac{\varepsilon_4}{2}\bar{d}_{i-1}^2. \tag{39}$$

Theorem 1: For the nonlinear controller given in (11), nonlinear observer in (26), FDI attack and noise estimator in (18), dynamics in (1) ensure semi-globally uniformly bounded tracking such that

$$\limsup_{t \to \infty} \|p_i(t)\| \leq \sqrt{\frac{1}{\psi_{1_i}}(H_{i,max} + \frac{\psi_{2_i}\varphi_i}{\alpha_{3_i}})}, \tag{40}$$

given that assumptions 2-4 are satisfied and the sufficient conditions in (36) are satisfied.

Proof: Taking the derivative of (31) yields

$$\dot{V}_{L_i} = e_i\dot{e}_i + r_i\dot{r}_i + \tilde{x}_{i-1}\dot{\tilde{x}}_{i-1} + \tilde{r}_{i-1}\dot{\tilde{r}}_{i-1} - tr(\tilde{W}_i\Gamma_{1i}^{-1}\dot{\hat{W}}_i) - tr(\tilde{V}_i\Gamma_{2i}^{-1}\dot{\hat{V}}_i). \tag{41}$$

The Lyapunov function satisfies the following inequality

$$\psi_{1_i} \leq V_{L_i} \leq \psi_{2_i} + H_{i,max}. \tag{42}$$

Substituting (5) and (14) into (41) yields

$$\begin{aligned} \dot{V}_{L_i} = &\, e_i(r_i - \alpha_i e_i) + r_i(b_i\tilde{\beta}_i - K_{1_i}r_i - e_i + d_i - d_{i-1}) \\ &+ \tilde{x}_{i-1}\dot{\tilde{x}}_{i-1} + \tilde{r}_{i-1}\dot{\tilde{r}}_{i-1} - tr(\tilde{W}_i\Gamma_{1i}^{-1}\dot{\hat{W}}_i) \\ &- tr(\tilde{V}_i\Gamma_{2i}^{-1}\dot{\hat{V}}_i). \end{aligned} \tag{43}$$

Further simplification by distributing variable e_i is given as

$$\begin{aligned}\dot{V}_{L_i} &= -\alpha_i e_i^2 + r_i(b_i\tilde{\beta}_i - K_{1_i} r_i + d_i - d_{i-1}) + \tilde{x}_{i-1}\dot{\tilde{x}}_{i-1}\\ &\quad + \tilde{r}_{i-1}\dot{\tilde{r}}_{i-1} - tr(\tilde{W}_i\Gamma_{1i}^{-1}\dot{\hat{W}}_i) - tr(\tilde{V}_i\Gamma_{2i}^{-1}\dot{\hat{V}}_i). \quad (44)\end{aligned}$$

Plugging in (7) and (30) into (44) yields

$$\begin{aligned}\dot{V}_{L_i} &= -\alpha_i e_i^2 + r_i(b_i\tilde{\beta}_i - K_{1_i} r_i + d_i - d_{i-1}) + \tilde{x}_{i-1}(\tilde{r}_{i-1}\\ &\quad - \alpha_i\tilde{x}_{i-1}) + \tilde{r}_{i-1}(-b_{i-1}\tilde{\beta}_i - L_{1_i}\tilde{r}_{i-1} - \tilde{x}_{i-1} + d_{i-1})\\ &\quad - tr(\tilde{W}_i\Gamma_{1i}^{-1}\dot{\hat{W}}_i) - tr(\tilde{V}_i\Gamma_{2i}^{-1}\dot{\hat{V}}_i). \qquad (45)\end{aligned}$$

Simplification results in

$$\begin{aligned}\dot{V}_{L_i} &= -\alpha_i e_i^2 + r_i(b_i\tilde{\beta}_i - K_{1_i} r_i + d_i - d_{i-1}) - \alpha_i\tilde{x}_{i-1}^2\\ &\quad - L_{1_i}\tilde{r}_{i-1}^2 - b_{i-1}\tilde{r}_{i-1}\tilde{\beta}_i + \tilde{r}_{i-1}d_{i-1} - tr(\tilde{W}_i\Gamma_{1i}^{-1}\dot{\hat{W}}_i)\\ &\quad - tr(\tilde{V}_i\Gamma_{2i}^{-1}\dot{\hat{V}}_i). \qquad (46)\end{aligned}$$

Substituting in ϕ_i from (20) yields

$$\begin{aligned}\dot{V}_{L_i} &= -\alpha_i e_i^2 + \tilde{\beta}_i\phi_i + r_i(-K_{1_i} r_i + d_i - d_{i-1}) - \alpha_i\tilde{x}_{i-1}^2\\ &\quad - L_{1_i}\tilde{r}_{i-1}^2 + \tilde{r}_{i-1}d_{i-1} - tr(\tilde{W}_i\Gamma_{1i}^{-1}\dot{\hat{W}}_i) - tr(\tilde{V}_i\Gamma_{2i}^{-1}\dot{\hat{V}}_i). \qquad (47)\end{aligned}$$

Further substitution of (22) in (47) results in

$$\begin{aligned}\dot{V}_{L_i} &= -\alpha_i e_i^2 + (\tilde{W}_i^T\sigma(\hat{V}_i^T\delta_i) + \hat{W}_i^T\sigma'(\hat{V}_i^T\delta_i)\tilde{V}_i^T\delta_i)\phi_i\\ &\quad + r_i N_{n_i} - \tilde{r}_{i-1}N_{n_i} + r_i(-K_{1_i} r_i + d_i - d_{i-1})\\ &\quad - \alpha_i\tilde{x}_{i-1}^2 - L_{1_i}\tilde{r}_{i-1}^2 + \tilde{r}_{i-1}d_{i-1}\\ &\quad - tr(\tilde{W}_i\Gamma_{1i}^{-1}\dot{\hat{W}}_i) - tr(\tilde{V}_i\Gamma_{2i}^{-1}\dot{\hat{V}}_i). \qquad (48)\end{aligned}$$

Young's Inequality is applied to select terms in (48) and given as

$$\begin{aligned} r_i N_{n_i} &\le \frac{1}{2\varepsilon_0}\|r_i\|^2 + \frac{\varepsilon_0}{2}\left\|N_{n_i}\right\|^2,\\ \tilde{r}_{i-1}N_{n_i} &\le \frac{1}{2\varepsilon_1}\|\tilde{r}_{i-1}\|^2 + \frac{\varepsilon_1}{2}\left\|N_{n_i}\right\|^2,\\ r_i d_i &\le \frac{1}{2\varepsilon_2}\|r_i\|^2 + \frac{\varepsilon_2}{2}\|d_i\|^2,\\ r_i d_{i-1} &\le \frac{1}{2\varepsilon_3}\|r_i\|^2 + \frac{\varepsilon_3}{2}\|d_{i-1}\|^2\\ \tilde{r}_{i-1}d_{i-1} &\le \frac{1}{2\varepsilon_4}\|\tilde{r}_{i-1}\|^2 + \frac{\varepsilon_4}{2}\|d_{i-1}\|^2. \qquad (49)\end{aligned}$$

Weights of NN, $\dot{\hat{W}}_i$, $\dot{\hat{V}}_i$ in (48) could be designed in the way that last two terms of (48) could remove the $(\tilde{W}_i^T\sigma(\hat{V}_i^T\delta_i) + \hat{W}_i^T\sigma'(\hat{V}_i^T\delta_i)\tilde{V}_i^T\delta_i)\phi_i$. Then by designing the weights as (24) and (25), and applying Young's Inequality the equation (48) becomes

$$\begin{aligned}\dot{V}_{L_i} &\le -\alpha_i\|e_i\|^2 + \frac{1}{2\varepsilon_0}\|r_i\|^2 + \varphi_i + \frac{1}{2\varepsilon_1}\|\tilde{r}_{i-1}\|^2\\ &\quad - K_{1_i}\|r_i\|^2 + \frac{1}{2\varepsilon_2}\|r_i\|^2 + \frac{1}{2\varepsilon_3}\|r_i\|^2\\ &\quad - \alpha_{i-1}\|\tilde{x}_{i-1}\|^2 - L_{1_i}\|\tilde{r}_{i-1}\|^2 + \frac{1}{2\varepsilon_4}\|\tilde{r}_{i-1}\|^2. \qquad (50)\end{aligned}$$

TABLE I

Specific Parameters

Controller Gains	Observer Gains	FDI Estimation Parameters
$\alpha_i = 1$	$\alpha_{i-1} = 0.01$	Activation Function: Sigmoid
$K_{1_i} = 2$	$L_{1_i} = 1$	$n_i = 1$, $n_n = 1$

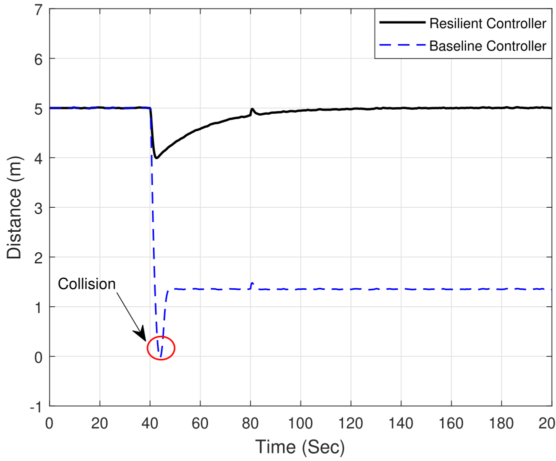


Fig. 4. Distance between Follower and Lead Vehicles.

Combining similar terms results in

$$\begin{aligned}\dot{V}_{L_i} &\le -(\alpha_{i-1})\|\tilde{x}_{i-1}\|^2 - (\alpha_i)\|e_i\|^2\\ &\quad - (L_{1_i} - \frac{1}{2\varepsilon_1} - \frac{1}{2\varepsilon_4})\|\tilde{r}_{i-1}\|^2\\ &\quad - (K_{1_i} - \frac{1}{2\varepsilon_2} - \frac{1}{2\varepsilon_0})\|r_i\|^2 + \varphi_i. \qquad (51)\end{aligned}$$

Knowing that the Lyapunov function is bounded, (51) can be written as

$$\dot{V}_{L_i} \le -\frac{\alpha_{3_i}}{\psi_{2_i}}V_{L_i} + \frac{\alpha_{3_i}}{\psi_{2_i}}H_{i,max} + \varphi_i, \qquad (52)$$

where $\alpha_{3_i} \triangleq \min\{\alpha_{i-1}, \alpha_i, \alpha_{1_i}, \alpha_{2_i}\}$.

Stability is assured given the sufficient equations provided in (36) are satisfied. ■

VI. Results

This section presents and discusses the results of testing the proposed resilient nonlinear controller, nonlinear observer, and FDI attack and noise estimator using MATLAB Simulink and Experimental setup. The following subsections explain the tests in details.

A. Simulink Results

In this section, MATLAB Simulink was employed to validate the effectiveness of the proposed control method. The results encompass representations of critical parameters, including the distance between vehicles, the speed of both the lead and follower vehicles, and plot depicting the estimation of FDI attack and measurement noise. Design specific parameters including controller and observer gains, activation function and neurons numbers used in the neural network section are added to the table I.

As depicted in Figure 4, the distance in resilient controller reflects the distance between the follower and lead vehicles when utilizing the proposed resilient controller. This controller

TABLE II
ROOT MEAN SQUARE ERROR OF DISTANCE

FDI Attack and Noise Injected	Resilient Controller	Baseline Controller
0.5	0.2386	4.0288
0.6	0.2874	4.4739
0.75	0.3611	5.1212
0.9	0.4381	5.5581

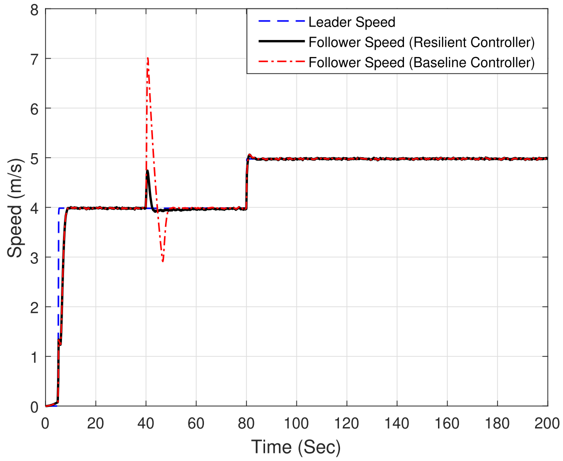


Fig. 5. Follower and lead vehicles' speed profile.

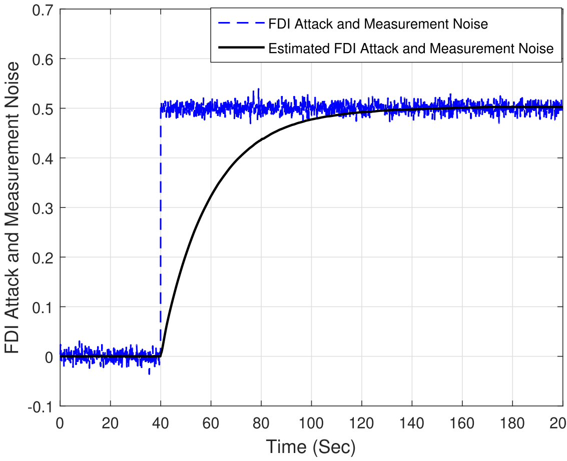


Fig. 6. FDI attack and measurement noise estimation ($\hat{\beta}_i$).

TABLE III
ROOT MEAN SQUARE ERROR OF FDI ATTACK AND NOISE ESTIMATION

FDI Attack and Noise Injected	Root Mean Square Error
0.5	0.1091
0.6	0.1310
0.75	0.1632
0.9	0.1940

ensures the consistent maintenance of a safe distance, 5 meters–the predefined desired distance between the vehicles. Notably, the singular undershoot observed in the resilient distance, occurring during the presence of the FDI attack and noise, remains well within safe parameters, eliminating the possibility of a collision. However, the distance in baseline controller, representing the distance between vehicles in the absence of FDI attack and noise estimation and compensation in the controller, reveals a critical scenario where a crash and accident occur as the distance between the vehicles converges to zero. To be more specific, table II provides the Root Mean Square Error (RMSE) values between the actual distance and the desired distance (5 meters). The first column presents the values of the defined FDI attack and noise, with the second and last columns displaying the RMSE for distance and desired distance under the proposed resilient controller and baseline controller, respectively. It is clear that there is a significant difference between values in second and third columns. Errors are smaller in resilient RMSE and it shows that distance is converging to desired distance using proposed controller.

Figure 5 depicts the velocity profiles of both the lead and follower vehicles. In the resilient scenario, the follower's speed follows the leader's velocity, showcasing adherence to the safety even in the presence of FDI attack and noise. Contrastingly, the follower speed in baseline controller diverges from the leader's velocity. During the occurrence of an FDI attack and noise, the follower accelerates, surpassing the leader's speed and resulting in a collision.

Finally, Figure 6 presents the estimation of the FDI attack utilizing the proposed method detailed in IV-B. Also, table III provides the Root Mean Square Error (RMSE) values associated with FDI attack estimation. The value of the error shows the effectiveness of the estimator method as they are small values. Notably, the table highlights a proportional increase in the estimation error corresponding to the magnitude of the step FDI attack. Also, the injected disturbance in dynamic models of vehicles in Simulink is defined as $d_i(t) = d_{i-1}(t) = 0.01sin(t/8)$.

To verify our assertion that the integration of learning-based and model-based methodologies enhances both accuracy and processing time, we conducted a precise evaluation of the computational time in Simulink across two distinct scenarios: our proposed method and the other relying solely on a model-based strategy. The results showed that our hybrid method took 43.4720 seconds to complete, compared to the model-based (baseline) approach, which required only 30.7659 seconds. The additional time observed in our approach is attributed to the integration of the learning-based component (NN), which inherently adds to the processing time due to its complexity. In a broader comparison encompassing learning-based, model-based, and hybrid methodologies, the learning-based method takes the longest time to compute, followed by our hybrid method. The model-based strategy is the most efficient, exhibiting the shortest computational time. Despite the longer computational time, our analysis supports the use of the hybrid approach that integrates both learning-based and model-based techniques. Considering RMSE values in table II, the proposed method strikes an optimal balance between improved accuracy and a reasonable increase in processing time.

B. Vehicle Model Through Experimental Analysis

The dynamic model of the vehicle, as elucidated in section II, was derived from an experimental setup featuring a 2017 Ford Fusion Hybrid, research vehicle, Figure 7. In this practical test, the first-order transfer function of the i^{th} vehicle

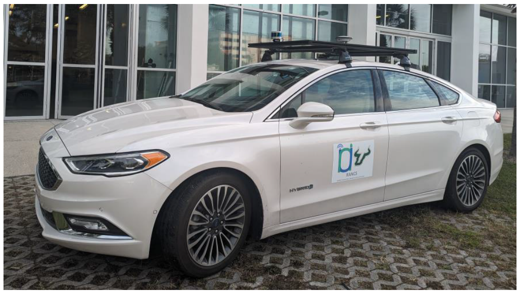


Fig. 7. Experimental setup.

is as

$$T_i(s) = \frac{V_i(s)}{U_i(s)}, \tag{53}$$

where $T_i(s)$ is the first order transfer function of the vehicle in the Laplace domain, s is the variable of Laplace domain, $V_i(s)$ is the Laplace form of the actual velocity, and $U_i(s)$ is the Laplace form of control command which is the provided pedal percentage which transmitted to the vehicle as an input. To derive the transfer function of the vehicle, a series of real-world tests were conducted, varying the pedal percentage, and subsequently measuring the average actual velocity. The calculation of the time constant (c_i) from the averaged velocity enabled the determination of the transfer function as

$$T_i(s) = \frac{b_i}{s + a_i}, \tag{54}$$

where $a_i \in \mathbb{R}$ is a constant value obtained as below

$$a_i \triangleq \frac{1}{c_i}, \tag{55}$$

and $b_i \in \mathbb{R}$ is obtained from below equation

$$\frac{b_i}{a_i} = \frac{v_{i_{ss}}}{u_{i_{ss}}}, \tag{56}$$

where $v_{i_{ss}} \in \mathbb{R}$ is the steady state value of the actual velocity in the time domain, and $u_{i_{ss}} \in \mathbb{R}$ is the steady state value of the provided input. Using Laplace inverse transform, dynamic model of the i^{th} vehicle is obtained from (53) and (54) which has been explained in section II. The values of parameters in (1) were obtained as $b_i = 6.6870$ and $a_i = 0.1413$.

C. Experimental Setup Test

The obtained real model of the Ford Fusion was used in both Simulink test and experimental setup test. Experimental setup test was employed to validate the results obtained from MATLAB Simulink. The test configuration involves the integration of the lead vehicle, the designed controller, observer, and FDI attack estimator within MATLAB Simulink, and a real-world passenger vehicle, specifically a 2017 Ford Fusion Hybrid research vehicle as follower. During the test, the resilient control signal is designed in MATLAB Simulink. Through specific blocks within Simulink, the designed signal is converted into a Controller Area Network (CAN) message. This message is then transmitted to the real vehicle via CAN communication. The interface within the vehicle that both receives and sends CAN messages is known as the CAN bus interface. To establish a connection between the Simulink environment on the computer and the CAN bus interface in the vehicle, we utilized Kvaser USB interfaces. After transmitting the control signal to the vehicle, we obtained the vehicle's velocity as CAN messages. These messages are then sent

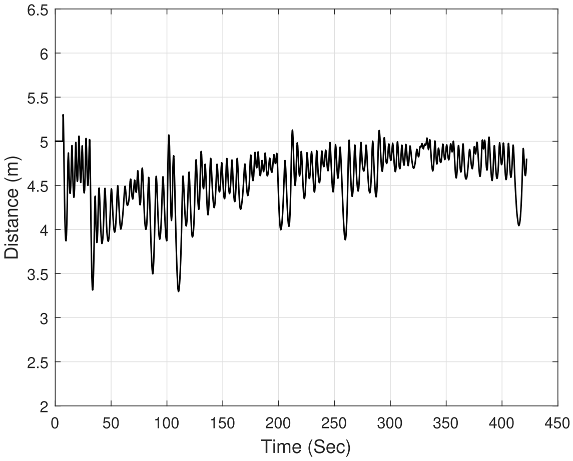


Fig. 8. Distance between follower and lead vehicles.

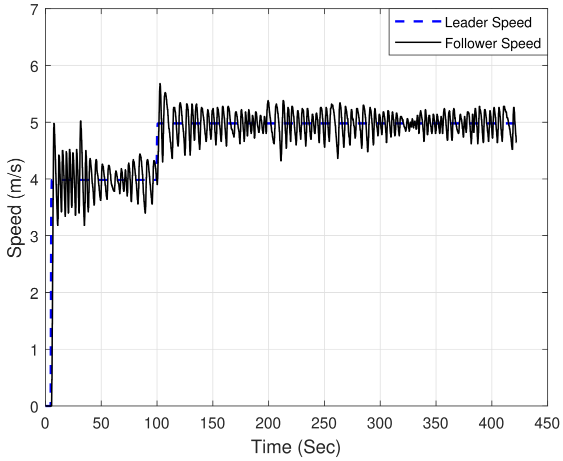


Fig. 9. Follower and lead vehicles speed profile.

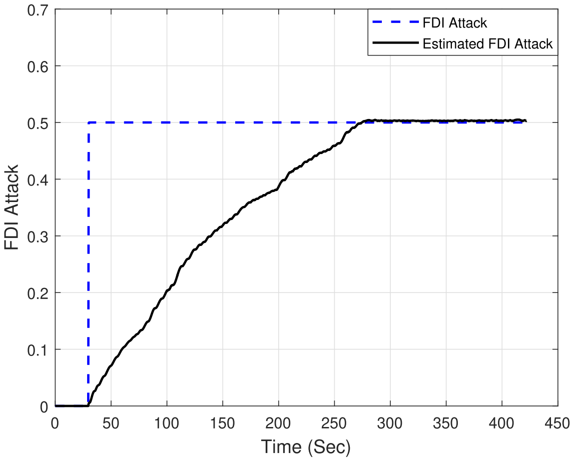


Fig. 10. FDI attack estimation.

back to MATLAB Simulink, enabling real-time monitoring and adjustments as needed.

The results of the experimental setup test are depicted in the following figures. Figure 8 showcases the distance between the lead and follower vehicles, maintaining a safe distance even during periods when a FDI attack is injected to the communication channel. Despite the attack, the distance is only momentarily reduced to 3.5 meters, still within the predefined safe distance. Furthermore, Figure 9 illustrates the velocity profiles of both the lead and follower vehicles, demonstrating the follower's synchronization with the leader's speed. Follower's velocity obtained using proposed resilient controller. This emphasizes the robust performance of the control system in adapting to dynamic scenarios and mitigating the effect of FDI attack. Finally, Figure 10 provides the estimation of the injected FDI attack. Together, these figures affirm the effectiveness of the proposed control method in maintaining safety and resilience in the face of real-world experimental conditions.

VII. Conclusion

A. Conclusion

CACC is an ADAS that collects data from a leading car, along with its own onboard sensor data to adjust the vehicle's speed in order to maintain a safe distance between both vehicles. An FDI attack and noise occur when incorrect data is injected into the transmitted data, with the goal of causing instability and collisions. In order to negate the effects of an FDI attack and noise on a CACC system, both a secure and resilient controller and estimation algorithm were designed. The proposed designs accurately estimated the FDI attack and noise and negated their effects on the vehicle, causing it to maintain a safe distance throughout the entire tests. The simulation was run through MATLAB/Simulink, and a passenger vehicle was utilized in experimental setup test. In this paper, we assumed that the lead and follower vehicles have the same dynamic models, which are the real vehicle model and obtained through experimental setup.

B. Future Work

Additional research could be focused on designing a secure controller with an unknown leader dynamic model. Further research into this area could outline the effects that an FDI attack has on other communication signals, primarily velocity and position. Also, another research could be considered as using optimization algorithms to select optimal values for controller and observer parameters. Additional research focusing on negating the effects of different types of attacks, TDS, and DoS, would prove beneficial because they are the most common adversarial attacks on CAVs.

Acknowledgment

The authors would like to thank Dr. Stephen Canfield of Tennessee Tech for supporting and reviewing this article. 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.

References

[1] *Crash Report Sampling*, National Highway Traffic Safety Administration, Washington, DC, USA, 2017.

[2] *2016 Fatal Motor Vehicle Crashes: Overview*, National Highway Traffic Safety Administration, Washington, DC, USA, Oct. 2017.

[3] H. B. Almobayedh, "Simulation of the impact of connected and automated vehicles at a signalized intersection," Ph.D. thesis, School Eng., Univ. Dayton, Dayton, OH, USA, 2019.

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

[5] H. Faghihian, M. Sarkar, and A. Sargolzaei, "A novel energy-efficient regenerative braking system for electric vehicles," in *Proc. SoutheastCon*, Mar. 2024, pp. 1300–1305.

[6] *Smart Mobility Connected and Automated Vehicles Capstone Report*, O. of Energy Efficiency & Renewable Energy, Washington, DC, USA, Jul. 2020.

[7] J. J. Cerutti, G. Cafiero, and G. Iuso, "Aerodynamic drag reduction by means of platooning configurations of light commercial vehicles: A flow field analysis," *Int. J. Heat Fluid Flow*, vol. 90, Aug. 2021, Art. no. 108823.

[8] M. Campbell, M. Egerstedt, J. P. How, and R. M. Murray, "Autonomous driving in urban environments: Approaches, lessons and challenges," *Phil. Trans. Roy. Soc. A, Math., Phys. Eng. Sci.*, vol. 368, no. 1928, pp. 4649–4672, Oct. 2010.

[9] A. Papadoulis, M. Quddus, and M. Imprialou, "Evaluating the safety impact of connected and autonomous vehicles on motorways," *Accident Anal. Prevention*, vol. 124, pp. 12–22, Mar. 2019.

[10] T. Guo, "Cooperatie adaptive cruise control (CACC) in the context of vehicle to vehicle communications: An overview," Tech. Rep., UC Davis, 2017.

[11] S. Noei, M. Parvizimosaed, and M. Noei, "Longitudinal control for connected and automated vehicles in contested environments," *Electronics*, vol. 10, no. 16, p. 1994, Aug. 2021.

[12] *Vehicle-to-Infrastructure Program, Cooperative Adaptive Cruise Control*, document FHWA-JPO-16-257, F. H. A. NU.S. Department of Transportation, 2015.

[13] S. E. Shladover, C. Nowakowski, X.-Y. Lu, and R. Ferlis, "Cooperative adaptive cruise control: Definitions and operating concepts," *Transp. Res. Rec.*, vol. 2489, no. 1, pp. 145–152, Jan. 2015.

[14] K. C. Dey et al., "A review of communication, driver characteristics, and controls aspects of cooperative adaptive cruise control (CACC)," *IEEE Trans. Intell. Transp. Syst.*, vol. 17, no. 2, pp. 491–509, Feb. 2016.

[15] V. Milanés and S. E. Shladover, "Modeling cooperative and autonomous adaptive cruise control dynamic responses using experimental data," *Transp. Res. C, Emerg. Technol.*, vol. 48, pp. 285–300, Nov. 2014.

[16] E. Semsar-Kazerooni, J. Verhaegh, J. Ploeg, and M. Alirezaei, "Cooperative adaptive cruise control: An artificial potential field approach," in *Proc. IEEE Intell. Vehicles Symp. (IV)*, Jun. 2016, pp. 361–367.

[17] F. J. Niroumand, P. A. Bonab, and A. Sargolzaei, "Security of connected and autonomous vehicles: A review of attacks and mitigation strategies," in *Proc. SoutheastCon*, Mar. 2024, pp. 1197–1204.

[18] P. A. Bonab, J. Holland, and A. Sargolzaei, "An observer-based control for a networked control of permanent magnet linear motors under a false-data-injection attack," in *Proc. IEEE Conf. Dependable Secure Comput. (DSC)*, Nov. 2023, pp. 1–8.

[19] S. Noei, A. Sargolzaei, A. Abbaspour, and K. Yen, "A decision support system for improving resiliency of cooperative adaptive cruise control systems," *Proc. Comput. Sci.*, vol. 95, pp. 489–496, Jan. 2016.

[20] K. M. A. Alheeti, A. Gruebler, K. D. McDonald-Maier, and A. Fernando, "Prediction of DoS attacks in external communication for self-driving vehicles using a fuzzy Petri net model," in *Proc. IEEE Int. Conf. Consum. Electron. (ICCE)*, Jan. 2016, pp. 502–503.

[21] P. S. Waraich and N. Batra, "Prevention of denial of service attack over vehicle ad hoc networks using quick response table," in *Proc. 4th Int. Conf. Signal Process., Comput. Control (ISPCC)*, Sep. 2017, pp. 586–591.

[22] S. Kumar and K. S. Mann, "Detection of multiple malicious nodes using entropy for mitigating the effect of denial of service attack in VANETs," in *Proc. 4th Int. Conf. Comput. Sci. (ICCS)*, Aug. 2018, pp. 72–79.

[23] A. Sargolzaei, K. K. Yen, M. N. Abdelghani, A. Mehbodniya, and S. Sargolzaei, "A novel technique for detection of time delay switch attack on load frequency control," *Intell. Control Autom.*, vol. 6, no. 4, pp. 205–214, 2015.

[24] A. Sargolzaei, K. K. Yen, M. N. Abdelghani, S. Sargolzaei, and B. Carbunar, "Resilient design of networked control systems under time delay switch attacks, application in smart grid," *IEEE Access*, vol. 5, pp. 15901–15912, 2017.

[25] Y. Shoukry, J. Araujo, P. Tabuada, M. Srivastava, and K. H. Johansson, "Minimax control for cyber-physical systems under network packet scheduling attacks," in *Proc. 2nd ACM Int. Conf. High Confidence Netw. Syst.*, Apr. 2013, pp. 93–100.

[26] R. A. Biroon, Z. A. Biron, and P. Pisu, "False data injection attack in a platoon of CACC: Real-time detection and isolation with a PDE approach," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 7, pp. 8692–8703, Jul. 2022.

[27] M. Wolf et al., "Securing CACC: Strategies for mitigating data injection attacks," in *Proc. IEEE Veh. Netw. Conf. (VNC)*, Dec. 2020, pp. 1–7.

[28] R. van der Heijden, T. Lukaseder, and F. Kargl, "Analyzing attacks on cooperative adaptive cruise control (CACC)," in *Proc. IEEE Veh. Netw. Conf. (VNC)*, Nov. 2017, pp. 45–52.

[29] C. Zhao, J. S. Gill, P. Pisu, and G. Comert, "Detection of false data injection attack in connected and automated vehicles via cloud-based sandboxing," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 7, pp. 9078–9088, Jul. 2022.

[30] M. Amoozadeh et al., "Security vulnerabilities of connected vehicle streams and their impact on cooperative driving," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 126–132, Jun. 2015.

[31] A. Bezemskij, G. Loukas, D. Gan, and R. J. Anthony, "Detecting cyber-physical threats in an autonomous robotic vehicle using Bayesian networks," in *Proc. IEEE Int. Conf. Internet Things (iThings) IEEE Green Comput. Commun. (GreenCom) IEEE Cyber, Phys. Social Comput. (CPSCom) IEEE Smart Data (SmartData)*, Jun. 2017, pp. 98–103.

[32] A. Petrillo, A. Pescapé, and S. Santini, "A collaborative control strategy for platoons of autonomous vehicles in the presence of message falsification attacks," in *Proc. 5th IEEE Int. Conf. Models Technol. Intell. Transp. Syst. (MT-ITS)*, Jun. 2017, pp. 110–115.

[33] A. Sargolzaei, C. D. Crane, A. Abbaspour, and S. Noei, "A machine learning approach for fault detection in vehicular cyber-physical systems," in *Proc. 15th IEEE Int. Conf. Mach. Learn. Appl. (ICMLA)*, Dec. 2016, pp. 636–640.

[34] V. Milanés, S. E. Shladover, J. Spring, C. Nowakowski, H. Kawazoe, and M. Nakamura, "Cooperative adaptive cruise control in real traffic situations," *IEEE Trans. Intell. Transp. Syst.*, vol. 15, no. 1, pp. 296–305, Feb. 2014.

[35] J. Ploeg, B. T. M. Scheepers, E. van Nunen, N. van de Wouw, and H. Nijmeijer, "Design and experimental evaluation of cooperative adaptive cruise control," in *Proc. 14th Int. IEEE Conf. Intell. Transp. Syst. (ITSC)*, Oct. 2011, pp. 260–265.

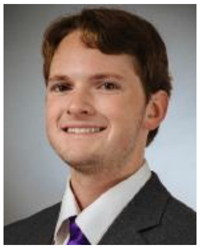
[36] A. Sargolzaei, "A secure control design for networked control system with nonlinear dynamics under false-data-injection attacks," in *Proc. Amer. Control Conf.*, May 2021, pp. 2693–2699.

[37] 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 Trans. Autom. Control*, vol. 53, no. 9, pp. 2180–2185, Oct. 2008.

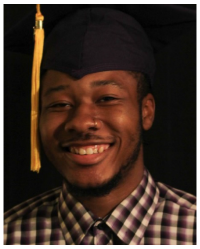
[38] I. Chakraborty, S. S. Mehta, E. Doucette, and W. E. Dixon, "Control of an input delayed uncertain nonlinear system with adaptive delay estimation," in *Proc. Amer. Control Conf. (ACC)*, May 2017, pp. 1779–1784.

[39] A. Sargolzaei, F. M. Zegers, A. Abbaspour, C. D. Crane, and W. E. Dixon, "Secure control design for networked control systems with nonlinear dynamics under time-delay-switch attacks," *IEEE Trans. Autom. Control*, vol. 68, no. 2, pp. 798–811, Feb. 2023.

Parisa Ansari-Bonab received the bachelor's degree in electrical engineering-control from the University of Tabriz and the master's degree in electrical engineering from the Shahrood University of Technology. She is currently pursuing the Ph.D. degree in mechanical engineering with the University of South Florida. Her research interests are control systems, fault detection, robust control, and security of systems.

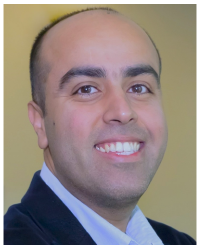


James C. Holland (Graduate Student Member, IEEE) received the Bachelor of Science degree in computer science and the master's degree in mechanical engineering from Tennessee Technological University. He is currently pursuing the Ph.D. degree in computer science and engineering with the University of South Florida. His research interests include hardware and software is of no surprise to those who know him, machine learning, cybersecurity, and testing and verification of connected and autonomous vehicles. He joined the RANCS research group as an undergraduate during his freshman year. For as long as, he can remember, he has been an Avid Tinkerer, exploring the intricacies of technology whether it be an old motherboard or an antique car.



Jonas Cunningham-Rush received the Bachelor of Science and Master of Science degrees in mechanical engineering from Tennessee Technological University. He is currently an Alum with Tennessee Technological University. He has always been fascinated by cars and in his free time, you can always find him working on his own. This fascination has grown as vehicle technology has expanded.

Shirin Noei received the master's degree in transportation engineering and in construction management from Florida International University, and the Ph.D. degree in transportation engineering from the University of Florida. She was a Research Assistant Professor at a multi-disciplinary center engaged in smart grid, resilient infrastructure, and wireless power. She has been awarded multiple USDOT projects as a Principal Investigator and has been involved in multiple Florida DOT projects as a Research Assistant. She is currently affiliated with Resilient, Autonomous, Networked Control Systems Research Laboratory as a Co-Advisor, Women's Transportation Seminar at Middle Tennessee Chapter as a Mentor, and Women in Engineering and Computing with Tennessee Technological University as a Faculty Mentor. She has published more than 20 journals and conference papers with high-impact factors.



Arman Sargolzaei (Senior Member, IEEE) received the M.S. and Ph.D. degrees in electrical and computer engineering from Florida International University, Miami, FL, USA, in 2012 and 2015, respectively, and the master's degree in aerospace engineering and the Ph.D. degree in mechanical engineering from the University of Florida, Gainesville, FL, USA, in 2019 and 2020, respectively. He is currently an Assistant Professor with the Department of Mechanical Engineering, University of South Florida. He was honored with the "2017 Faculty Research Excellence" and "2018 Faculty Research Excellence" Awards. In addition, he received the NSF CAREER Award in 2022. Prior to joining USF, he held positions as an Assistant Professor in mechanical engineering with Tennessee Technological University and as an Assistant Professor in electrical engineering and the Director of the Advanced Mobility Institute, Florida Polytechnic University. His mission is to enhance the quality of life for people by addressing security and privacy concerns through extensive collaboration across multidisciplinary fields.