attacks. Cyber-attacks targeting CAVs present significant risks, including breaches of privacy and potentially life-threatening alterations to control systems. Due to the high level of interconnectivity in CAVs, an adversarial attack on a single vehicle can have far-reaching implications, affecting other CAVs and associated infrastructures (Niroumand et al., 2024; Sun et al., 2022). One significant category of cyber-physical attacks is FDI attacks. In this scenario, adversaries exploit vulnerabilities in the system configuration to inject falsified data into the system (Bonab et al., 2023; Sargolzaei, 2021; Sargolzaei et al., 2020; Zideh et al., 2023). Consequently, there is an urgent need to develop a secure CACC algorithm to mitigate these threats.

A significant amount of research has focused on designing CACC system. For instance a reinforcement learning approach is applied to design a CACC in Desjardins and Chaib-draa (2011). The primary goal of this research is to maintain a safe distance between vehicles. The study incorporates function approximation techniques and gradient-descent learning algorithms to optimise the performance of their proposed controller. In designing this CACC, the delay in communication channel has been considered. In Emirler et al. (2018), a robust parameter space approach is used to design the CACC system. D-stability is selected as the performance objective, and a feedback PD controller is designed within the controller parameter space to achieve D-stability across various longitudinal dynamics time constants and time gap values.

Also, in Sybis et al. (2019), a modified CACC is designed to support the high-density car platooning. In the designed CACC, impact of actuation lag, message periodicity, and communication delay are analysed and considered. In addition, the development of CACC is investigated in Liu et al. (2020). This study develops a CACC algorithm that accounts for constant time delays in the communication channel.

All the previously mentioned studies have developed the CACC system with a primary emphasis on mitigating delays within the communication channel. Nonetheless, these approaches fail to guarantee safety in the presence of FDI attacks, input delays and disturbances.

Another relevant study on the design of a CACC algorithm is presented in Milanés et al. (2014). This research validates the effectiveness of the proposed CACC through comprehensive experimental setups. The development of the CACC algorithm considers critical factors such as input delay, communication delay and disturbances. The system incorporates two controllers: one dedicated to managing the approach manoeuver towards the leading vehicle, and the other responsible for regulating the car-following behaviour once the vehicle becomes part of the platoon.

Also, in Ploeg et al. (2011), a CACC is presented to guarantee string stability in the presence of communication delay, vehicle's input delay and disturbance. Another research considers the communication structure within the CACC and validates the CACC system, particularly in scenarios where the follower vehicle experiences input delay (Lunze, 2020). While the mentioned algorithms demonstrate effective performance in the presence of disturbance, communication delay and input delay, these methods are not able to mitigate the negative effects of FDI attacks.

In Biroon et al. (2020, 2022), researchers introduce a continuous model for a platoon of connected vehicles equipped with the CACC algorithm, utilising partial differential equation (PDE) approximations. Their design also considers FDI attacks within the platoon. Unlike typical approaches, the FDI attack in their study is not applied to transmitted data. Instead, they model an intelligent FDI attack within the Dedicated Short-Range Communication (DSRC) network by simulating the injection of fake vehicles. Another example of detecting cyber-attacks in the communication channel of CACC is presented in Keijzer and Ferrari (2019). This paper introduces a robust method, specifically a sliding mode observer, to detect and estimate cyber-attacks, taking communication delay into account as part of the analysis. Additional study has utilised a fault detection technique based on neural network (NN) to detect and track FDI attacks on the CACC layer of a platoon of connected vehicles in real time (Sargolzaei et al., 2016). In Sargolzaei et al. (2016), a decision support system was developed to reduce the probability and severity of any consequent accident. The referenced papers are not able to mitigate FDI attacks while the system is under input delay and disturbances. Additionally, some of these papers lack comprehensive stability analyses, and their designs rely solely on linear control methods.

Unlike other studies in the literature, this paper aims to develop a novel secure Lyapunov-based nonlinear controller. Our study introduces a control and estimation technique that integrates both

model-based and learning-based approaches. The goal is to enhance both accuracy and processing time. Unlike conventional methods that solely rely on either learning-based or model-based techniques, our proposed method strikes a balance between processing time and accuracy. The designed novel controller is able to maintain the real-time tracking of the lead vehicle while the communication channel is under FDI attacks and measurement noise, and the follower vehicle is under input delay and disturbance.

The contributions of our paper are as follows: (i) A novel control strategy that integrates both model-based and learning-based approaches is developed. This strategy is resilient against FDI attacks, measurement noise, input time delays and external disturbances. (ii) We propose a nonlinear observer and a neural network (NN)-based FDI attack estimator capable of estimating FDI attacks in real time. (iii) Lyapunov–Krasovskii (LK) functionals are utilised to provide the stability analysis of our proposed nonlinear controller, nonlinear observer and NN-based FDI attack estimator. (iv) We obtain a real-world vehicle model through an experimental setup.

The outline of the rest of the paper is as follows: Section 2 describes the mathematical model of CACC. The problem statement is explained in Section 3. Section 4 overviews the proposed solution including controller design, FDI attacks and measurement noise estimator, and observer design. The stability analysis of the designed controller, observer and FDI attacks estimator is explained in Section 5. Section 6 shows the results. Finally, Section 7 explains the conclusion of the paper.

2. Mathematical model of CACC

CACC-equipped strings of vehicles in the presence of FDI attacks and input time delay are demonstrated in Figure 1. It is assumed that the control command of lead vehicle is transmitted to the following vehicle through communication channel. Also, velocity and position of the lead vehicle are estimated by radar sensor. This paper assumes a string of homogeneous vehicles with the same models and CACC capabilities. The dynamics model of the vehicles are derived through an experimental setup, as detailed in Section 6. The dynamic model of the ith vehicle is defined as follows :

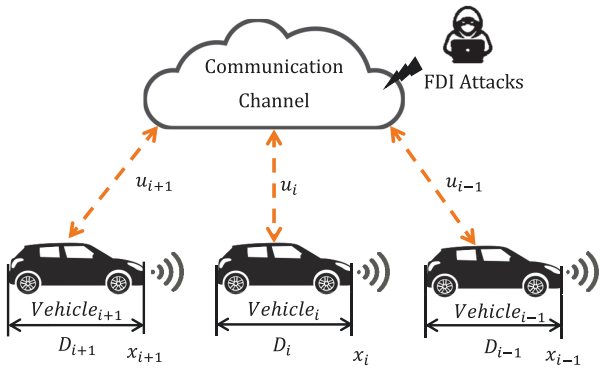

Figure 1. CACC-equipped string of vehicles in the presence of FDI attacks and input time delay.

$$\begin{cases} \dot{x}_i(t) = v_i(t), \\ \dot{v}_i(t) = -\gamma_i v_i(t) + \beta_i u_{\tau_i}(t) + d_i(t), \end{cases} \tag{1}$$

where $i \in \{2, \ldots, n\}$ 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), $x_i(t) \in \mathbb{R}$, $v_i(t) \in \mathbb{R}$, $u_{\tau_i}(t) \in \mathbb{R}$ and $d_i(t) \in \mathbb{R}$ represent the position, velocity, generalised delayed control input, and external disturbance, respectively. $\tau_i(t) \in \mathbb{R}$ represents a known time-varying delay, and γ_i and β_i are constant parameters. The dynamic model of the leader vehicle is described as

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

where $x_{i-1}(t) \in \mathbb{R}$, $v_{i-1}(t) \in \mathbb{R}$, $u_{i-1}(t) \in \mathbb{R}$ and $d_{i-1}(t) \in \mathbb{R}$ represent the position, velocity, control input and external disturbance, respectively. Since vehicles are homogeneous then $\gamma_{i-1} = \gamma_i$ and $\beta_{i-1} = \beta_i$.

Assumption 2.1: The disturbances are assumed to be continuous and bounded by known constants such that $\|d_i(t)\| < \bar{d}_{1_i}$ and $\|d_{i-1}(t)\| < \bar{d}_{2_i}$ for $t \geq t_0$, and $\bar{d}_{1_i}, \bar{d}_{2_i} \in \mathbb{R}_{>0}$ (Sargolzaei, 2021).

Assumption 2.2: The time-varying input delay is bounded and differentiable such that $0 \leq \tau_i(t) \leq \overline{\tau_i}$, $\forall\, t \in \mathbb{R}_{>0}$ where $\overline{\tau_i}$ is a positive known constant. The rate of change for the delay is bounded such that $|\dot{\tau}_i(t)| < \dot{\tau}_{\max} < 1, \forall\, t \in \mathbb{R}_{>0}$, where $\dot{\tau}_{\max}$ is a positive known constant.

2.1. FDI attack and measurement noise representation

The communication network of connected vehicles is being subjected to both FDI attacks and measurement noise. Therefore, vehicles receive corrupted data. This causes instability in a platoon of vehicles, resulting in possible collisions. In the context of this paper, we make the assumption that the control command is the only parameter affected by the attack, as expressed in Equation (3). This attack impacts the output, ultimately transforming it into the observed output as

$$\pi_i(u_{i-1}(t)) \triangleq u_{i-1}(t) + \nu_{i-1}(t), \tag{3}$$

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

$$\nu_{i-1}(t) \triangleq \Lambda_{i-1}(t) + \theta_i(t), \tag{4}$$

where $\Lambda_{i-1}(t) \in \mathbb{R}$ is the bounded, unknown, continuous, and time-varying FDI attack, and θ_i denotes a bounded Gaussian measurement noise.

Assumption 2.3: $\nu_{i-1}(t)$ is assumed to be bounded and differentiable such that $\|\nu_{i-1}(t)\| \leq \overline{\nu}_{i-1}$, where $t \geq t_0$ and $\overline{\nu}_{i-1}$ is a positive known constant (Sargolzaei, 2021).

3. Problem statement

The primary objective of this paper is to develop a robust controller for CACC to mitigate FDI attacks and noise effects and to compensate for the input time delay and disturbance to ensure the maintenance of a safe following distance between the leader and follower vehicles. The CACC algorithm requires a control signal from the lead vehicle in real-time. However, adversary manipulation challenges this process, which potentially leads to collisions. Therefore, our second objective is to design an observer and an FDI attacks estimation mechanism to estimate the FDI attacks in real-time. To quantify these objectives, we define some error signals as distance error ($e_i(t)$), an auxiliary error to obtain a delay-free control signal ($e_{u_i}(t)$), state estimation error ($\tilde{x}_{i-1}(t)$), and FDI attacks estimation error ($\tilde{\nu}_{i-1}(t)$).

The error signals are in detail as following, $e_i(t) : [t_0, \infty) \to \mathbb{R}$ as

$$e_i(t) \triangleq x_i(t) - x_{i-1}(t) + D_{i-1} + x_{d_i}(t), \tag{5}$$

where $D_{i-1} \in \mathbb{R}$ is the length of lead vehicle and is a constant, and $x_{d_i}(t) \in \mathbb{R}$ is the desired distance between vehicles. Achieving and maintaining this desired distance is our objective.

Assumption 3.1: The desired distance, its first, and second derivatives are assumed to be bounded by positive known constants, $x_{d_i}, \dot{x}_{d_i}, \ddot{x}_{d_i} \in \mathcal{L}_\infty$ (Patre et al., 2008).

Another challenge is the known time-varying delay in the control signal of follower vehicles. To achieve a delay-free control signal in the closed-loop system, an auxiliary signal, $e_{u_i}(t) : [t_0, \infty) \to \mathbb{R}$, is defined as

$$e_{u_i}(t) \triangleq \int_{t-\tau_i}^{t} u_i(s)\, \mathrm{d}s. \tag{6}$$

Time derivative of $e_{u_i}(t)$ is obtained as

$$\dot{e}_{u_i}(t) = u_i(t) - (1 - \dot{\tau}_i(t))u_{\tau_i}(t). \tag{7}$$

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

$$r_i(t) \triangleq \dot{e}_i(t) + \alpha_i e_i(t) + \beta_i e_{u_i}(t), \tag{8}$$

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

The follower vehicles 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 $\tilde{x}_{i-1}(t) : [t_0, \infty) \to \mathbb{R}$, is described as

$$\tilde{x}_{i-1}(t) \triangleq x_{i-1}(t) - \hat{x}_{i-1}(t), \tag{9}$$

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

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

$$\tilde{r}_{i-1}(t) \triangleq \dot{\tilde{x}}_{i-1}(t) + \alpha_{i-1}\tilde{x}_{i-1}(t), \tag{10}$$

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

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

$$\tilde{u}_{i-1}(t) \triangleq u_{i-1}(t) - \hat{u}_{i-1}(t), \tag{11}$$

where $\hat{u}_{i-1}(t) \in \mathbb{R}$ is the estimated control signal of the leader.

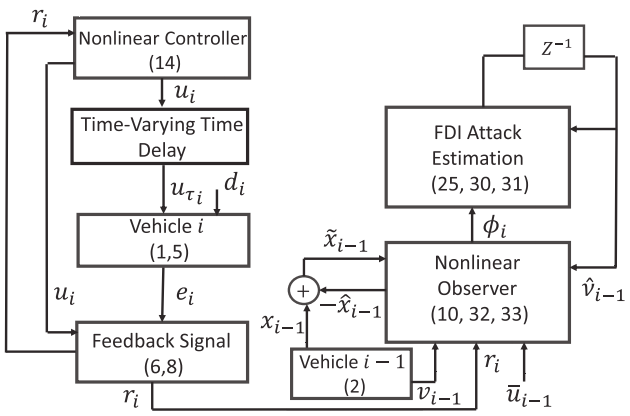

Figure 2. Proposed solution diagram.

Defining $\overline{u}_{i-1}(t) \triangleq u_{i-1}(t) + v_{i-1}(t)$ and $\hat{u}_{i-1}(t) \triangleq \overline{u}_{i-1}(t) - \hat{v}_{i-1}(t)$ yields

$$\tilde{u}_{i-1}(t) = u_{i-1}(t) - \overline{u}_{i-1}(t) + \hat{v}_{i-1}(t), \tag{12}$$

where $\hat{v}_{i-1}(t) \in \mathbb{R}$ is the estimated FDI attacks.

Assumption 3.2: $\overline{u}_{i-1}(t)$ is bounded such that $\|\overline{u}_{i-1}(t)\| \leq \overline{U}_{i-1}$ where $\overline{U}_{i-1} \in \mathbb{R}_{>0}$.[1]

To measure the accuracy of the FDI attacks estimation, the estimation error, $\tilde{v}_{i-1}(t) : [t_0, \infty) \to \mathbb{R}$ is defined as

$$\tilde{v}_{i-1}(t) \triangleq v_{i-1}(t) - \hat{v}_{i-1}(t). \tag{13}$$

4. Proposed solution

In order to address problem statement, we proposed a nonlinear Lyapunov based controller, an FDI attack estimator, and a nonlinear observer which will be discussed in detail in the following subsections. Also, Algorithm 1 and the diagram in Figure 2 are a summary of the procedure.

4.1. Controller design

The control signal was designed using the Lyapunov stability analysis in Section 5 as

$$u_i(t) \triangleq -k_i r_i(t), \tag{14}$$

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

Taking the derivative of Equation (8) and substituting (5) yields the closed loop form of the system as

$$\dot{r}_i(t) = \ddot{x}_i(t) - \ddot{x}_{i-1}(t) + \ddot{x}_{d_i}(t) + \alpha_i \dot{e}_i(t) + \beta_i \dot{e}_{u_i}(t). \tag{15}$$

Replacing $\ddot{x}_i, \ddot{x}_{i-1}, \dot{e}_{u_i}, u_{i-1}$ from definition before (12), and (14) into (15) produces

$$\begin{aligned}\dot{r}_i(t) = &-\gamma_i v_i(t) + d_i(t) + \gamma_i v_{i-1}(t) - \beta_i \overline{u}_{i-1}(t) \\ &+ \beta_i v_{i-1}(t) - d_{i-1}(t) + \ddot{x}_{d_i}(t) + \alpha_i \dot{e}_i(t) \\ &- \beta_i k_i r_i(t) - \beta_i k_i \dot{\tau}_i r_{\tau_i}(t).\end{aligned} \tag{16}$$

Closed-loop error system is obtained by adding and subtracting $\gamma_i \dot{x}_{d_i}(t)$ and $\beta_i \hat{v}_{i-1}(t)$ to (16) to yield

$$\begin{aligned}\dot{r}_i(t) = &-\gamma_i (v_i(t) - v_{i-1}(t) + \dot{x}_{d_i}(t)) \\ &+ \beta_i (v_{i-1}(t) - \hat{v}_{i-1}(t)) \\ &- \beta_i \overline{u}_{i-1}(t) + d_i(t) - d_{i-1}(t) \\ &+ \ddot{x}_{d_i}(t) + \gamma_i \dot{x}_{d_i}(t) \\ &+ \beta_i \hat{v}_{i-1}(t) + \alpha_i \dot{e}_i(t) - \beta_i k_i r_i(t) \\ &- \beta_i k_i \dot{\tau}_i(t) r_{\tau_i}(t),\end{aligned} \tag{17}$$

using (13), time derivative of (5), and further simplification, (17) changes to

$$\begin{aligned}\dot{r}_i(t) = &(\alpha_i - \gamma_i)\dot{e}_i(t) + \beta_i \tilde{v}_{i-1}(t) - \beta_i \overline{u}_{i-1}(t) + d_i(t) \\ &- d_{i-1}(t) + \ddot{x}_{d_i}(t) + \gamma_i \dot{x}_{d_i}(t) + \beta_i \hat{v}_{i-1}(t) \\ &- \beta_i k_i r_i(t) - \beta_i k_i \dot{\tau}_i(t) r_{\tau_i}(t).\end{aligned} \tag{18}$$

Substituting (8) in (18) and defining $\alpha_i - \gamma_i \triangleq \iota_i, \alpha_i^2 - \gamma_i \alpha_i \triangleq \eta_i$, and $\beta_i(\alpha_i - \gamma_i) \triangleq \Upsilon_i$ results in

$$\begin{aligned}\dot{r}_i(t) = &\iota_i r_i(t) - \eta_i e_i(t) - \Upsilon_i e_{u_i}(t) + \beta_i \tilde{v}_{i-1}(t) \\ &- \beta_i \overline{u}_{i-1}(t) + d_i(t) - d_{i-1}(t) + \ddot{x}_{d_i}(t) \\ &+ \gamma_i \dot{x}_{d_i}(t) + \beta_i \hat{v}_{i-1}(t) \\ &- \beta_i k_i r_i(t) - \beta_i k_i \dot{\tau}_i(t) r_{\tau_i}(t),\end{aligned} \tag{19}$$

finally

$$\begin{aligned}\dot{r}_i(t) = &\iota_i r_i(t) - \eta_i e_i(t) - \Upsilon_i e_{u_i}(t) + \beta_i \tilde{v}_{i-1}(t) + N_i(t) \\ &- \beta_i k_i r_i(t) - \beta_i k_i \dot{\tau}_i(t) r_{\tau_i}(t),\end{aligned} \tag{20}$$

where $N_i \in \mathbb{R}$ is an auxiliary term which is defined as

$$\begin{aligned}N_i(t) \triangleq &d_i(t) - d_{i-1}(t) + \ddot{x}_{d_i}(t) + \gamma_i \dot{x}_{d_i}(t) - \beta_i \overline{u}_{i-1}(t) \\ &+ \beta_i \hat{v}_{i-1}(t).\end{aligned} \tag{21}$$

4.2. FDI attack estimation

The detailed observer design in the subsequent subsection includes a neural network-based FDI attacks estimation algorithm and state estimator. The FDI attacks

occur over a non-compact domain, so a nonlinear mapping, $M_{v_{i-1}} : [t_0, \infty) \to [0, 1]$ is required to map time to a compact spatial domain given as

$$M_{v_{i-1}} \triangleq \frac{c_{v_{i-1}}(t - t_0)}{c_{v_{i-1}}(t - t_0) + 1}, \zeta \in [0, 1], t \in [t_0, \infty), \tag{22}$$

where $c_{v_{i-1}} \in \mathbb{R}_{>0}$ describes a user-specified gain (Chakraborty et al., 2017). Consequently, $v_{i-1}(t)$ is mapped into the compact domain ζ as

$$v_{i-1}(t) = v_{i-1}(M^{-1}_{v_{i-1}}(\zeta)) \triangleq v_{M_{v_{i-1}}}(\zeta), \tag{23}$$

where $v_{M_{v_{i-1}}} : [0, 1] \to \mathbb{R}$ is now defined.

The FDI attack can now be estimated using a neural-network (NN) described as

$$v_{M_{v_{i-1}}}(\zeta) = W_i^T \sigma(V_i^T \delta_i) + \mu_i, \tag{24}$$

where $\delta_i \in \mathbb{R}^{2\times 1}$ signifies the inputs, vectors $W_i \in \mathbb{R}^{(n_n+1)\times 1}$ and $V_i \in \mathbb{R}^{2\times n_n}$ indicate the unknown ideal weights, n_n represents the neurones number in the hidden layer. Additionally, $\sigma(\cdot) \in \mathbb{R}^{(n_n+1)}$ denotes an activation functions vector and $\mu_i \in \mathbb{R}$ signifies a bounded signal. Considering respect to the spatial domain, the NN estimation of FDI attack can be described as

$$\hat{v}_{i-1}(t) \triangleq \hat{W}_i^T \sigma(\hat{V}_i^T \delta_i), \tag{25}$$

where $\hat{W}_i \in \mathbb{R}^{(n_n+1)\times 1}$ and $\hat{V}_i \in \mathbb{R}^{2\times n_n}$ represent the estimated ideals weights, and δ_i is given as

$$\delta_i \triangleq [1, \phi_i^T]^T, \tag{26}$$

where $\phi_i \triangleq \beta_i(r_i(t) - \tilde{r}_{i-1}(t))$.

Substituting (23)–(25) into (13) yields

$$\tilde{v}_{i-1}(t) = W_i^T \sigma(V_i^T \delta_i) - \hat{W}_i^T \sigma(\hat{V}_i^T \delta_i) + \mu_i. \tag{27}$$

A Taylor's series approximation is applied resulting

$$\tilde{v}_{i-1}(t) = \tilde{W}_i^T \sigma(\hat{V}_i^T \delta_i) + \hat{W}_i^T \sigma'(\hat{V}_i^T \delta_i) \tilde{V}_i^T \delta_i + N_{n_i}, \tag{28}$$

given

$$N_{n_i} \triangleq \tilde{W}_i^T \sigma'(\hat{V}_i^T \delta_i) \tilde{V}_i^T \delta_i + W_i^T \vartheta(\tilde{V}_i^T \delta_i) + \mu_i, \tag{29}$$

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

$$\dot{\hat{W}}_i = proj(\Gamma_{1_i} \sigma(\hat{V}_i^T \delta_i) \phi_i), \tag{30}$$

and

$$\dot{\hat{V}}_i = proj(\Gamma_{2_i} \phi_i \delta_i \hat{W}_i^T \sigma'(\hat{V}_i^T \delta_i)), \tag{31}$$

where $\Gamma_{1_i} \in \mathbb{R}^{(n_n+1)\times(n_n+1)}$ and $\Gamma_{2_i} \in \mathbb{R}$ are definite positive matrices, and the function proj denotes a Lipschitz continuous projection operator defined in Cai et al. (2006).

Remark 4.1: Recall that v_{i-1} is bounded by Assumption 2.3. In addition, observe that $\hat{W}_i$ and $\sigma(\hat{V}_i^T \delta_i)$ are bounded by construction. Therefore, (25) implies that there exist a $\hat{v}_{i-1,\max} \in \mathbb{R}_{>0}$ such that $\|\hat{v}_{i-1}(t)\| \leq \hat{v}_{i-1,\max}$. Therefore, (13) implies that there exists a $\tilde{v}_{i-1,\max} \in \mathbb{R}_{>0}$ such that $\|\tilde{v}_{i-1}(t)\| \leq \tilde{v}_{i-1,\max}$.

Remark 4.2: Assumptions 2.1, 3.1, 3.2 and Remark 4.1 are used to show that $N_i(t)$ in (21) is bounded such that $\|N_i(t)\| \leq \overline{N}_i$ where $\overline{N}_i \in \mathbb{R}_{>0}$.

4.3. Observer design

Based on the stability analysis in Section 5, the observer for vehicle i is designed as

$$\begin{aligned}\ddot{\hat{x}}_{i-1}(t) = &-\gamma_i v_{i-1}(t) + \beta_i \overline{u}_{i-1}(t) \\ &- \beta_i \hat{v}_{i-1}(t) + L_{1_i} \tilde{r}_{i-1}(t) \\ &+ \alpha_{i-1} \tilde{r}_{i-1}(t) - \alpha_{i-1}^2 \tilde{x}_{i-1}(t) + \tilde{x}_{i-1}(t),\end{aligned} \tag{32}$$

where L_{1_i} represents a user-defined gain. Taking the derivative of (10) with respect to time yields

$$\dot{\tilde{r}}_{i-1}(t) = \ddot{\tilde{x}}_{i-1}(t) + \alpha_{i-1} \dot{\tilde{x}}_{i-1}(t). \tag{33}$$

After substituting (9) and (10) and simplification, the equation becomes

$$\begin{aligned}\dot{\tilde{r}}_{i-1}(t) = &\ddot{x}_{i-1}(t) - \ddot{\hat{x}}_{i-1}(t) + \alpha_{i-1} \tilde{r}_{i-1}(t) \\ &- \alpha_{i-1}^2 \tilde{x}_{i-1}(t),\end{aligned} \tag{34}$$

variable substitution from (2) yields

$$\begin{aligned}\dot{\tilde{r}}_{i-1}(t) = &-\gamma_i v_{i-1}(t) + \beta_i \overline{u}_{i-1}(t) \\ &- \beta_i v_{i-1}(t) + d_{i-1}(t)\end{aligned}$$

$$-\ddot{\tilde{x}}_{i-1}(t)+\alpha_{i-1}\tilde{r}_{i-1}(t)-\alpha_{i-1}^2\tilde{x}_{i-1}(t), \quad (35)$$

substituting $\bar{u}_{i-1}(t)$ from the definition before (12) and (32) in (35) results in

$$\begin{aligned}\dot{\tilde{r}}_{i-1}(t) = &-\gamma_i v_{i-1}(t)+\beta_i\bar{u}_{i-1}(t)\\ &-\beta_i v_{i-1}(t)+d_{i-1}(t)\\ &+\gamma_i v_{i-1}(t)-\beta_i\bar{u}_{i-1}(t)\\ &+\beta_i\hat{v}_{i-1}(t)-L_{1_i}\tilde{r}_{i-1}(t)\\ &-\alpha_{i-1}\tilde{r}_{i-1}(t)+\alpha_{i-1}^2\tilde{x}_{i-1}(t)-\tilde{x}_{i-1}(t)\\ &+\alpha_{i-1}\tilde{r}_{i-1}(t)-\alpha_{i-1}^2\tilde{x}_{i-1}(t), \end{aligned} \quad (36)$$

further simplification in (36) yields

$$\begin{aligned}\dot{\tilde{r}}_{i-1}(t) = &-\beta_i\tilde{v}_{i-1}(t)+d_{i-1}(t)\\ &-L_{1_i}\tilde{r}_{i-1}(t)-\tilde{x}_{i-1}(t).\end{aligned} \quad (37)$$

The Algorithm 1 illustrates the summarised steps followed in this paper to design a secure controller, in presence of variable time delay and FDI attacks and noise. Additionally, Figure 2 depicts the proposed solution diagram, which integrates a nonlinear controller, an observer and an estimator for FDI attacks.

Algorithm 1: Proposed secure controller and estimation approach

Begin
Initialize parameters
Vehicles' model parameters: β_i, γ_i.
Selected controller gains: α_i and k_i.
Selected observer gains: α_{i-1}, L_{1_i}. **for** t **do**
  Compute the distance error signal from (5);
  Compute the auxiliary error signal using (6), (8),
  α_i, and β_i;
  Calculate the control signal from (14) and user-defined gain k_i;
  Compute the state estimation error from (9);
  Compute the auxiliary estimation error signal using (10) and α_{i-1};
  Use (30) & (31) to compute the update laws of NN;
  Estimate the FDI attacks using (25);
  Compute the observer signal using (32);

5. Stability analysis

For the sake of simplicity (t) was dropped in further calculations. Let z_i and $\Pi_i \in \mathbb{R}^{4ni+3}$ be defined as

$$z_i \triangleq [e_i^T, r_i^T, \tilde{r}_{i-1}^T, \tilde{x}_{i-1}^T]^T, \quad (38)$$

and

$$\Pi_i \triangleq [z_i^T, \sqrt{P_{LK_i}}, \sqrt{Q_{LK_i}}, \sqrt{R_{LK_i}}]^T, \quad (39)$$

where P_{LK_i}, Q_{LK_i}, $R_{LK_i} : [t_0, \infty) \to \mathbb{R}_{\geq 0}$ are LK functionals defined as[2]

$$P_{LK_i} \triangleq \omega_{1_i}\int_{t-\tau_i}^{t}\left(\int_{\theta}^{t}\|u_i(s)\|^2\,\mathrm{d}s\right)\mathrm{d}\theta, \quad (40)$$

$$Q_{LK_i} \triangleq \omega_{2_i}\int_{t-\tau_i}^{t}\|r_i(s)\|^2\,\mathrm{d}s, \quad (41)$$

$$R_{LK_i} \triangleq \omega_{3_i}\int_{t-\tau_i}^{t}\left(\int_{\theta}^{t}\|r_i(s)\|^2\,\mathrm{d}s\right)\mathrm{d}\theta, \quad (42)$$

and $\omega_{1_i}, \omega_{2_i}, \omega_{3_i} \in \mathbb{R}_{\geq 0}$ are user-defined constants.

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

$$H_i \triangleq \frac{1}{2}\mathrm{tr}(\tilde{W}_i^T\Gamma_{1_i}^{-1}\tilde{W}_i)+\frac{1}{2}\mathrm{tr}(\tilde{V}_i^T\Gamma_{2_i}^{-1}\tilde{V}_i). \quad (43)$$

where tr is the trace of a matrix which is defined as the sum of the elements on the main diagonal of a square matrix.

Since $\tilde{W}_i$ and $\tilde{V}_i$ are bounded, H_i is bounded by $|H_i| \leq H_{i,\max}$ where $H_{i,\max} \in \mathbb{R}_{>0}$.

Let the following be the sufficient conditions

$$\begin{aligned}\alpha_i &> \frac{(1-\eta_i)\varepsilon_{1_i}}{2}+\frac{\beta_i}{2\varepsilon_{2_i}},\\ k_i &> \frac{(1-\eta_i)}{2\beta_i\varepsilon_{1_i}}+\frac{\iota_i}{\beta_i}+\frac{\Upsilon_i}{2\beta_i\varepsilon_{3_i}}+\frac{1}{2\varepsilon_{4_i}}+\frac{1}{2\beta_i\varepsilon_{6_i}}\\ &\quad+\frac{k_i\dot{\tau}_{\max}}{2\varepsilon_{7_i}}+\frac{\tau_i\omega_{1_i}k_i^2+\omega_{2_i}}{,}\beta_i+\frac{\tau_i\omega_{3_i}}{\beta_i},\\ \omega_{1_i} &> \frac{\beta_i\tau_i\varepsilon_{2_i}}{K_{1_i}}+\frac{\Upsilon_i\varepsilon_{3_i}\tau_i}{K_{1_i}},\\ \omega_{2_i} &> \frac{\beta_i k_i\dot{\tau}_{\max}\varepsilon_{7_i}}{2K_{1_i}},\\ \alpha_{i-1} &> 0,\\ L_{i-1} &> \frac{\beta_i}{2\varepsilon_{5_i}}+\frac{1}{2\varepsilon_{8_i}},\end{aligned} \quad (44)$$

where $K_{1_i} = 1-\dot{\tau}_i$ and $\varepsilon_{p_i} \in \mathbb{R}_{>0}, p \in \{1,\ldots,8\}$ denote positive known constants.

Let χ_{1_i} and χ_{2_i} be defined as

$$\chi_{1_i} \triangleq \min\left\{\frac{1}{2}, \frac{\omega_{1_i}}{2}\right\},$$
$$\chi_{2_i} \triangleq \max\left\{1, \frac{\omega_{1_i}}{2}\right\}. \tag{45}$$

Based on the sufficient conditions presented in (44), we define the positive constants α_{p_i} for $p \in \{1, \ldots, 6\}$ as

$$\begin{aligned}
\alpha_{1_i} &\triangleq \alpha_i - \frac{(1-\eta_i)\varepsilon_{1_i}}{2} - \frac{\beta_i}{2\varepsilon_{2_i}},\\
\alpha_{2_i} &\triangleq \beta_i k_i - \frac{(1-\eta_i)}{2\varepsilon_{1_i}} - \iota_i - \frac{\Upsilon_i}{2\varepsilon_{3_i}} - \frac{\beta_i}{2\varepsilon_{4_i}} - \frac{1}{2\varepsilon_{6_i}},\\
&\quad - \frac{\beta_i k_i \dot{\tau}_{\max}}{2\varepsilon_{7_i}} - \tau_i\omega_{1_i}k_i^2 - \omega_{2_i} - \tau_i\omega_{3_i},\\
\alpha_{3_i} &\triangleq \frac{K_{1_i}\omega_{1_i}}{2\tau_i} - \frac{\varepsilon_{2_i}\beta_i}{2} - \frac{\Upsilon_i\varepsilon_{3_i}}{2},\\
\alpha_{4_i} &\triangleq K_{1_i}\omega_{2_i} - \frac{\beta_i k_i \dot{\tau}_{\max}\varepsilon_{7_i}}{2},\\
\alpha_{5_i} &\triangleq \alpha_{i-1},\\
\alpha_{6_i} &\triangleq L_{1_i} - \frac{\beta_i}{2\varepsilon_{5_i}} - \frac{1}{2\varepsilon_{8_i}}.
\end{aligned} \tag{46}$$

Furthermore, let $\alpha_{7_i} \triangleq \min\left\{\alpha_{1_i}, \alpha_{2_i}, \alpha_{5_i}, \alpha_{6_i}\right\}$ and $\alpha_{8_i} \triangleq \min\left\{\alpha_{7_i}, \frac{K_{1_i}}{2\bar{\tau}_i}, \frac{K_{1_i}\omega_{3_i}}{2\omega_{2_i}}\right\}$.

Theorem 5.1: *For the dynamics in* (1) *and* (2)*, controller given in* (14)*, FDI attack estimator in* (25)*, and observer in* (32) *ensure semi-globally uniformly ultimately bounded tracking such that*

$$\limsup_{t\to\infty} \|\Pi_i(t)\| \leq \sqrt{\frac{1}{\chi_{1_i}}\left(H_{i,\max} + \frac{\chi_{2_i}\varphi_i}{\alpha_{8_i}}\right)}, \tag{47}$$

given that Assumptions 2.1–3.2 *are satisfied and the sufficient conditions in* (44) *are satisfied.*

Proof: Let $V_{L_i} : D_i \to \mathbb{R}_{\geq 0}$, denotes a radially unbounded, positive definite, continuously differentiable Lyapunov function displayed as

$$\begin{aligned}
V_{L_i} &= \frac{1}{2}e_i^2 + \frac{1}{2}r_i^2 + \frac{1}{2}\tilde{x}_{i-1}^2 + \frac{1}{2}\tilde{r}_{i-1}^2 + P_{LK_i} + Q_{LK_i}\\
&\quad + R_{LK_i} + H_i.
\end{aligned} \tag{48}$$

The Lyapunov candidate function, V_{L_i}, can be bounded as

$$\chi_{1_i}\|\Pi_i\|^2 \leq V_{L_i} \leq \chi_{2_i}\|\Pi_i\|^2 + H_{i,\max}, \tag{49}$$

taking the derivative of (48) and applying Leibniz Rule to (40)–(42) results in

$$\begin{aligned}
\dot{V}_{L_i} &= e_i\dot{e}_i + r_i\dot{r}_i + \tilde{x}_{i-1}\dot{\tilde{x}}_{i-1} + \tilde{r}_{i-1}\dot{\tilde{r}}_{i-1}\\
&\quad + \left(\tau_i\omega_{1_i}k_i^2\|r_i\|^2 - K_{1_i}\omega_{1_i}\int_{t-\tau_i}^{t}\|u_i(s)\|^2\,\mathrm{d}s\right)\\
&\quad + (\omega_{2_i}\|r_i\|^2 - K_{1_i}\omega_{2_i}\|r_{\tau_i}\|^2) + \left(\tau_i\omega_{3_i}\|r_i\|^2\right.\\
&\quad \left. - K_{1_i}\omega_{3_i}\int_{t-\tau_i}^{t}\|r_i(s)\|^2\,\mathrm{d}s\right) - \mathrm{tr}(\tilde{W}_i^T\Gamma_{1i}^{-1}\dot{\hat{W}}_i)\\
&\quad - \mathrm{tr}(\tilde{V}_i^T\Gamma_{2i}^{-1}\dot{\hat{V}}_i).
\end{aligned} \tag{50}$$

Substituting (8), (10), (20), and (37) into (50) yields

$$\begin{aligned}
\dot{V}_{L_i} &= e_i(r_i - \alpha_i e_i - \beta_i e_{u_i})\\
&\quad + r_i(\iota_i r_i - \eta_i e_i - \Upsilon_i e_{u_i} + \beta_i\tilde{\nu}_{i-1}\\
&\quad + N_i - \beta_i k_i r_i - \beta_i k_i\dot{\tau}_i r_{\tau_i})\\
&\quad + \tilde{x}_{i-1}(\tilde{r}_{i-1} - \alpha_{i-1}\tilde{x}_{i-1})\\
&\quad + \tilde{r}_{i-1}(-\beta_i\tilde{\nu}_{i-1} - L_{1_i}\tilde{r}_{i-1} + d_{i-1} - \tilde{x}_{i-1})\\
&\quad + \left(\tau_i\omega_{1_i}k_i^2\|r_i\|^2 - K_{1_i}\omega_{1_i}\int_{t-\tau_i}^{t}\|u_i(s)\|^2\,\mathrm{d}s\right)\\
&\quad + (\omega_{2_i}\|r_i\|^2 - K_{1_i}\omega_{2_i}\|r_{\tau_i}\|^2) + \left(\tau_i\omega_{3_i}\|r_i\|^2\right.\\
&\quad \left. - K_{1_i}\omega_{3_i}\int_{t-\tau_i}^{t}\|r_i(s)\|^2\,\mathrm{d}s\right) - \mathrm{tr}(\tilde{W}_i^T\Gamma_{1i}^{-1}\dot{\hat{W}}_i)\\
&\quad - \mathrm{tr}(\tilde{V}_i^T\Gamma_{2i}^{-1}\dot{\hat{V}}_i),
\end{aligned} \tag{51}$$

further simplification by distributing variables $e_i, r_i, \tilde{x}_{i-1}, \tilde{r}_{i-1}$, and substituting in ϕ_i from (26) yields

$$\begin{aligned}
\dot{V}_{L_i} &= -\alpha_i e_i^2 + (1-\eta_i)r_i e_i - \beta_i e_i e_{u_i} + \iota_i r_i^2 - \Upsilon_i r_i e_{u_i}\\
&\quad + \phi_i\tilde{\nu}_{i-1} + r_i N_i - \beta_i k_i r_i^2\\
&\quad - \beta_i k_i\dot{\tau}_i r_i r_{\tau_i} - \alpha_{i-1}\tilde{x}_{i-1}^2\\
&\quad - L_{1_i}\tilde{r}_{i-1}^2 + d_{i-1}\tilde{r}_{i-1} + \tau_i\omega_{1_i}k_i^2\|r_i\|^2\\
&\quad - K_{1_i}\omega_{1_i}\int_{t-\tau_i}^{t}\|u_i(s)\|^2\,\mathrm{d}s + \omega_{2_i}\|r_i\|^2\\
&\quad - K_{1_i}\omega_{2_i}\|r_{\tau_i}\|^2 + \tau_i\omega_{3_i}\|r_i\|^2\\
&\quad - K_{1_i}\omega_{3_i}\int_{t-\tau_i}^{t}\|r_i(s)\|^2\,\mathrm{d}s - \mathrm{tr}(\tilde{W}_i^T\Gamma_{1i}^{-1}\dot{\hat{W}}_i)\\
&\quad - \mathrm{tr}(\tilde{V}_i^T\Gamma_{2i}^{-1}\dot{\hat{V}}_i),
\end{aligned} \tag{52}$$

further substitution of (28) in (52) results in

$$\dot{V}_{L_i} = -\alpha_i e_i^2 + (1-\eta_i)r_i e_i - \beta_i e_i e_{u_i} + \iota_i r_i^2 - \Upsilon_i r_i e_{u_i}$$

$$
\begin{aligned}
&+ (\tilde{W}_i^T \sigma(\hat{V}_i^T \delta_i) + \hat{W}_i^T \sigma'(\hat{V}_i^T \delta_i) \tilde{V}_i^T \delta_i) \phi_i \\
&+ \beta_i r_i N_{n_i} - \beta_i \tilde{r}_{i-1} N_{n_i} + r_i N_i \\
&- \beta_i k_i r_i^2 - \beta_i k_i \dot{\tau}_i r_i r_{\tau_i} - \alpha_{i-1} \tilde{x}_{i-1}^2 \\
&- L_{1_i} \tilde{r}_{i-1}^2 + d_{i-1} \tilde{r}_{i-1} + \tau_i \omega_{1_i} k_i^2 \|r_i\|^2 \\
&- K_{1_i} \omega_{1_i} \int_{t-\tau_i}^{t} \|u_i(s)\|^2 \, ds + \omega_{2_i} \|r_i\|^2 \\
&- K_{1_i} \omega_{2_i} \left\|r_{\tau_i}\right\|^2 + \tau_i \omega_{3_i} \|r_i\|^2 \\
&- K_{1_i} \omega_{3_i} \int_{t-\tau_i}^{t} \|r_i(s)\|^2 \, ds - \mathrm{tr}(\tilde{W}_i^T \Gamma_{1i}^{-1} \dot{\hat{W}}_i) \\
&- tr(\tilde{V}_i^T \Gamma_{2i}^{-1} \dot{\hat{V}}_i), \qquad (53)
\end{aligned}
$$

below inequality can be concluded from (53)

$$
\begin{aligned}
\dot{V}_{L_i} \leq\ & -\alpha_i \|e_i\|^2 + (1-\eta_i) \|r_i\| \|e_i\| - \beta_i \|e_i\| \left\|e_{u_i}\right\| \\
&+ \iota_i \|r_i\|^2 - \Upsilon_i \|r_i\| \left\|e_{u_i}\right\| + (\tilde{W}_i^T \sigma(\hat{V}_i^T \delta_i) \\
&+ \hat{W}_i^T \sigma'(\hat{V}_i^T \delta_i) \tilde{V}_i^T \delta_i) \phi_i + \beta_i \|r_i\| \left\|N_{n_i}\right\| \\
&- \beta_i \left\|\tilde{r}_{i-1}\right\| \left\|N_{n_i}\right\| + \|r_i\| \|N_i\| - \beta_i k_i \|r_i\|^2 \\
&- \beta_i k_i \dot{\tau}_i \|r_i\| \left\|r_{\tau_i}\right\| - \alpha_{i-1} \left\|\tilde{x}_{i-1}\right\|^2 \\
&- L_{1_i} \left\|\tilde{r}_{i-1}\right\|^2 + \|d_{i-1}\| \left\|\tilde{r}_{i-1}\right\| + \tau_i \omega_{1_i} k_i^2 \|r_i\|^2 \\
&- K_{1_i} \omega_{1_i} \int_{t-\tau_i}^{t} \|u_i(s)\|^2 \, ds + \omega_{2_i} \|r_i\|^2 \\
&- K_{1_i} \omega_{2_i} \left\|r_{\tau_i}\right\|^2 + \tau_i \omega_{3_i} \|r_i\|^2 \\
&- K_{1_i} \omega_{3_i} \int_{t-\tau_i}^{t} \|r_i(s)\|^2 \, ds \\
&- \mathrm{tr}(\tilde{W}_i^T \Gamma_{1i}^{-1} \dot{\hat{W}}_i) - \mathrm{tr}(\tilde{V}_i^T \Gamma_{2i}^{-1} \dot{\hat{V}}_i), \qquad (54)
\end{aligned}
$$

applying updated laws from (30) and (31) into the inequality (54) cancels the term $(\tilde{W}_i^T \sigma(\hat{V}_i^T \delta_i) + \hat{W}_i^T \sigma'(\hat{V}_i^T \delta_i) \tilde{V}_i^T \delta_i) \phi_i$ as below

$$
\begin{aligned}
\dot{V}_{L_i} \leq\ & -\alpha_i \|e_i\|^2 + (1-\eta_i) \|r_i\| \|e_i\| - \beta_i \|e_i\| \left\|e_{u_i}\right\| \\
&+ \iota_i \|r_i\|^2 - \Upsilon_i \|r_i\| \left\|e_{u_i}\right\| + \beta_i \|r_i\| \left\|N_{n_i}\right\| \\
&- \beta_i \left\|\tilde{r}_{i-1}\right\| \left\|N_{n_i}\right\| + \|r_i\| \|N_i\| - \beta_i k_i \|r_i\|^2 \\
&- \beta_i k_i \dot{\tau}_i \|r_i\| \left\|r_{\tau_i}\right\| - \alpha_{i-1} \left\|\tilde{x}_{i-1}\right\|^2 \\
&- L_{1_i} \left\|\tilde{r}_{i-1}\right\|^2 + \|d_{i-1}\| \left\|\tilde{r}_{i-1}\right\| + \tau_i \omega_{1_i} k_i^2 \|r_i\|^2 \\
&- K_{1_i} \omega_{1_i} \int_{t-\tau_i}^{t} \|u_i(s)\|^2 \, ds + \omega_{2_i} \|r_i\|^2 \\
&- K_{1_i} \omega_{2_i} \left\|r_{\tau_i}\right\|^2 + \tau_i \omega_{3_i} \|r_i\|^2 \\
&- K_{1_i} \omega_{3_i} \int_{t-\tau_i}^{t} \|r_i(s)\|^2 \, ds. \qquad (55)
\end{aligned}
$$

Applying Young's Inequality to the inequality (55) yields

$$
\begin{aligned}
\dot{V}_{L_i} \leq\ & -\alpha_i \|e_i\|^2 + \frac{(1-\eta_i)}{2\varepsilon_{1_i}} \|r_i\|^2 \\
&+ \frac{(1-\eta_i)\varepsilon_{1_i}}{2} \|e_i\|^2 + \frac{\beta_i}{2\varepsilon_{2_i}} \|e_i\|^2 \\
&+ \frac{\beta_i \varepsilon_{2_i}}{2} \left\|e_{u_i}\right\|^2 + \iota_i \|r_i\|^2 + \frac{\Upsilon_i}{2\varepsilon_{3_i}} \|r_i\|^2 \\
&+ \frac{\Upsilon_i \varepsilon_{3_i}}{2} \left\|e_{u_i}\right\|^2 + \frac{\beta_i}{2\varepsilon_{4_i}} \|r_i\|^2 + \frac{\beta_i \varepsilon_{4_i}}{2} \left\|N_{n_i}\right\|^2 \\
&+ \frac{\beta_i}{2\varepsilon_{5_i}} \left\|\tilde{r}_{i-1}\right\|^2 + \frac{\beta_i \varepsilon_{5_i}}{2} \left\|N_{n_i}\right\|^2 \\
&+ \frac{1}{2\varepsilon_{6_i}} \|r_i\|^2 + \frac{\varepsilon_{6_i}}{2} \|N_i\|^2 - \beta_i k_i \|r_i\|^2 \\
&+ \frac{\beta_i k_i \dot{\tau}_{\max}}{2\varepsilon_{7_i}} \|r_i\|^2 + \frac{\beta_i k_i \dot{\tau}_{\max} \varepsilon_{7_i}}{2} \left\|r_{\tau_i}\right\|^2 \\
&- \alpha_{i-1} \left\|\tilde{x}_{i-1}\right\|^2 - L_{1_i} \left\|\tilde{r}_{i-1}\right\|^2 + \frac{1}{2\varepsilon_{8_i}} \left\|\tilde{r}_{i-1}\right\|^2 \\
&+ \frac{\varepsilon_{8_i}}{2} \|d_{i-1}\|^2 + \tau_i \omega_{1_i} k_i^2 \|r_i\|^2 \\
&- K_{1_i} \omega_{1_i} \int_{t-\tau_i}^{t} \|u_i(s)\|^2 \, ds \\
&+ \omega_{2_i} \|r_i\|^2 - K_{1_i} \omega_{2_i} \left\|r_{\tau_i}\right\|^2 \\
&+ \tau_i \omega_{3_i} \|r_i\|^2 - K_{1_i} \omega_{3_i} \int_{t-\tau_i}^{t} \|r_i(s)\|^2 \, ds, \qquad (56)
\end{aligned}
$$

using Assumption 2.1, upper bound of N_i from Remark 4.2, and upper bound of N_{n_i} from (29), φ_i is defined as

$$
\varphi_i \triangleq \frac{\beta_i \varepsilon_{4_i}}{2} \bar{N}_{n_i}^2 + \frac{\beta_i \varepsilon_{5_i}}{2} \bar{N}_{n_i}^2 + \frac{\varepsilon_{6_i}}{2} \overline{N}_i^2 + \frac{\varepsilon_{8_i}}{2} \overline{d}_{2_i}^2. \qquad (57)
$$

Using Cauchy–Schwarz inequality and Mean Value Theorem, the integral terms in (56) can be replaced with an upper bound, also applying (57) into (56) change (56) to

$$
\begin{aligned}
\dot{V}_{L_i} \leq\ & -\alpha_i \|e_i\|^2 + \frac{(1-\eta_i)}{2\varepsilon_{1_i}} \|r_i\|^2 + \frac{(1-\eta_i)\varepsilon_{1_i}}{2} \|e_i\|^2 \\
&+ \frac{\beta_i}{2\varepsilon_{2_i}} \|e_i\|^2 + \frac{\beta_i \varepsilon_{2_i}}{2} \left\|e_{u_i}\right\|^2 + \iota_i \|r_i\|^2 \\
&+ \frac{\Upsilon_i}{2\varepsilon_{3_i}} \|r_i\|^2 + \frac{\Upsilon_i \varepsilon_{3_i}}{2} \left\|e_{u_i}\right\|^2 + \frac{\beta_i}{2\varepsilon_{4_i}} \|r_i\|^2
\end{aligned}
$$

$$
\begin{aligned}
&+\frac{\beta_i}{2\varepsilon_{5_i}}\left\|\tilde{r}_{i-1}\right\|^2+\frac{1}{2\varepsilon_{6_i}}\left\|r_i\right\|^2-\beta_i k_i\left\|r_i\right\|^2\\
&+\frac{\beta_i k_i\dot{\tau}_{\max}}{2\varepsilon_{7_i}}\left\|r_i\right\|^2+\frac{\beta_i k_i\dot{\tau}_{\max}\varepsilon_{7_i}}{2}\left\|r_{\tau_i}\right\|^2\\
&-\alpha_{i-1}\left\|\tilde{x}_{i-1}\right\|^2-L_{1_i}\left\|\tilde{r}_{i-1}\right\|^2+\frac{1}{2\varepsilon_{8_i}}\left\|\tilde{r}_{i-1}\right\|^2\\
&+\tau_i\omega_{1_i}k_i^2\left\|r_i\right\|^2-\frac{K_{1_i}\omega_{1_i}}{2\tau_i}\left\|e_{u_i}\right\|^2\\
&-\frac{K_{1_i}\omega_{1_i}}{2\tau_i}\left(\int_{t-\tau_i}^{t}\left(\int_{\theta}^{t}\left\|u_i(s)\right\|^2\,\mathrm{d}s\right)\mathrm{d}\theta\right)\\
&+\omega_{2_i}\left\|r_i\right\|^2-K_{1_i}\omega_{2_i}\left\|r_{\tau_i}\right\|^2+\tau_i\omega_{3_i}\left\|r_i\right\|^2\\
&-\frac{K_{1_i}\omega_{3_i}}{2}\int_{t-\tau_i}^{t}\left\|r_i(s)\right\|^2\,\mathrm{d}s\\
&-\frac{K_{1_i}\omega_{3_i}}{2\tau_i}\int_{t-\tau_i}^{t}\left(\int_{\theta}^{t}\left\|r_i(s)\right\|^2\,\mathrm{d}s\right)\mathrm{d}\theta+\varphi_i,
\end{aligned}
\tag{58}
$$

using the LK functionals definition in (40)–(42), in (58) results in

$$
\begin{aligned}
\dot{V}_{L_i}\le&\left(-\alpha_i+\frac{(1-\eta_i)\varepsilon_{1_i}}{2}+\frac{\beta_i}{2\varepsilon_{2_i}}\right)\left\|e_i\right\|^2\\
&+\left(\frac{(1-\eta_i)}{2\varepsilon_{1_i}}+\iota_i+\frac{\Upsilon_i}{2\varepsilon_{3_i}}+\frac{\beta_i}{2\varepsilon_{4_i}}+\frac{1}{2\varepsilon_{6_i}}-\beta_i k_i\right.\\
&\left.+\frac{\beta_i k_i\dot{\tau}_{\max}}{2\varepsilon_{7_i}}+\tau_i\omega_{1_i}k_i^2+\omega_{2_i}+\tau_i\omega_{3_i}\right)\left\|r_i\right\|^2\\
&+\left(\frac{\beta_i\varepsilon_{2_i}}{2}+\frac{\Upsilon_i\varepsilon_{3_i}}{2}-\frac{K_{1_i}\omega_{1_i}}{2\tau_i}\right)\left\|e_{u_i}\right\|^2\\
&+\left(\frac{\beta_i k_i\dot{\tau}_{\max}\varepsilon_{7_i}}{2}-K_{1_i}\omega_{2_i}\right)\left\|r_{\tau_i}\right\|^2\\
&-\alpha_{i-1}\left\|\tilde{x}_{i-1}\right\|^2+\left(\frac{\beta_i}{2\varepsilon_{5_i}}-L_{1_i}+\frac{1}{2\varepsilon_{8_i}}\right)\left\|\tilde{r}_{i-1}\right\|^2\\
&-\frac{K_{1_i}}{2\tau_i}P_{LK_i}-\frac{K_{1_i}\omega_{3_i}}{2\omega_{2_i}}Q_{LK_i}-\frac{K_{1_i}}{2\tau_i}R_{LK_i}+\varphi_i.
\end{aligned}
\tag{59}
$$

substituting the gains defined in (46) in (59) changes it to

$$
\begin{aligned}
\dot{V}_{L_i}\le&-\alpha_{1_i}\left\|e_i\right\|^2-\alpha_{2_i}\left\|r_i\right\|^2-\alpha_{3_i}\left\|e_{u_i}\right\|^2\\
&-\alpha_{4_i}\left\|r_{\tau_i}\right\|^2-\alpha_{5_i}\left\|\tilde{x}_{i-1}\right\|^2-\alpha_{6_i}\left\|\tilde{r}_{i-1}\right\|^2\\
&-\frac{K_{1_i}}{2\tau_i}P_{LK_i}-\frac{K_{1_i}\omega_{3_i}}{2\omega_{2_i}}Q_{LK_i}\\
&-\frac{K_{1_i}}{2\tau_i}R_{LK_i}+\varphi_i.
\end{aligned}
\tag{60}
$$

The effects of e_{u_i} and r_{τ_i}, could be cancelled by designing α_{3_i} and α_{4_i} gains, then we can write (60) as

$$
\begin{aligned}
\dot{V}_{L_i}\le&-\alpha_{1_i}\left\|e_i\right\|^2-\alpha_{2_i}\left\|r_i\right\|^2-\alpha_{5_i}\left\|\tilde{x}_{i-1}\right\|^2\\
&-\alpha_{6_i}\left\|\tilde{r}_{i-1}\right\|^2-\frac{K_{1_i}}{2\bar{\tau}_i}P_{LK_i}-\frac{K_{1_i}\omega_{3_i}}{2\omega_{2_i}}Q_{LK_i}\\
&-\frac{K_{1_i}}{2\bar{\tau}_i}R_{LK_i}+\varphi_i,
\end{aligned}
\tag{61}
$$

based on the definition (39), (61) can be summarised a

$$
\dot{V}_{L_i}\le-\alpha_{8_i}\left\|\Pi_i\right\|^2+\varphi_i,
\tag{62}
$$

by substituting the upper bound for Lyapunov function denoted in (49), we can summarise (62) as

$$
\dot{V}_{L_i}\le-\frac{\alpha_{8_i}}{\chi_{2_i}}V_{L_i}+\frac{\alpha_{8_i}}{\chi_{2_i}}H_{i,\max}+\varphi_i.
\tag{63}
$$

Solving (63) results in the sufficient condition in (44). According to the provided ultimate upper bound for Π_i, it is proven that $z_i\in\mathcal{L}_\infty$, thus the semi-globally uniformly boundedness tracking is assured. ■

6. Results

This section presents and discusses the experimental setup for obtaining the vehicle model and the simulation results of testing the proposed resilient nonlinear controller, nonlinear observer and FDI attack estimator using MATLAB Simulink. The subsequent subsections provide a comprehensive elaboration on the conducted tests.

6.1. Vehicle model through experimental analysis

The dynamic model of the vehicle, as introduced in Section 2, was derived through an experimental setup using a 2017 Ford Fusion Hybrid (the research vehicle is shown in Figure 3). During this test, the system's input is represented by the pedal percentage, while the measurable output is the velocity of the vehicle. Suppose that the first-order transfer function of the ith vehicle is as

$$
T_i(s)=\frac{V_i(s)}{U_i(s)},
\tag{64}
$$

where $T_i(s)$ is the first-order transfer function of the vehicle in the Laplace domain, s is the variable of the Laplace domain, $V_i(s)$ is the Laplace form of the actual velocity and $U_i(s)$ is the Laplace form of the

Figure 3. Experimental setup.

control command, which is the provided pedal percentage. In obtaining the transfer function of the vehicle, we conducted experimental tests with varied pedal percentage values. Subsequently, we determined the average actual velocity resulting from these tests. By computing the time constant (c_i) associated with the average output, we were able to ascertain the transfer function as

$$T_i(s) = \frac{\beta_i}{s + \gamma_i}, \tag{65}$$

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

$$\gamma_i \triangleq \frac{1}{c_i}, \tag{66}$$

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

$$\frac{\beta_i}{\gamma_i} = \frac{v_{i_{ss}}}{u_{i_{ss}}}, \tag{67}$$

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 ith vehicle is obtained from (64) and (65) which has been explained in section 2. The values of parameters in (1) are $\beta_i = 6.6870$ and $\gamma_i = 0.1413$.

6.2. Simulation results

In this subsection, we employed MATLAB Simulink to validate the effectiveness of the proposed method. The results include visual representations of critical parameters, such as the distance between vehicles, the velocities of both lead and follower vehicles, and the estimation of the FDI attack. Additionally, to enhance clarity, we present the root mean square error (RMSE) for distance, as well as the RMSE for FDI attack estimation. To provide a comprehensive analysis of the Simulink results, which consider all factors affecting vehicle velocity and, consequently, the distance between vehicles, we examine two scenarios. The first scenario presents results with a single FDI attack and varying input delays. The second scenario includes results with a single input delay and different FDI attacks, as detailed below.

6.2.1. Scenario 1 (single FDI attack and varying input delays)

Here, we present the results with a single FDI attack modelled as a step function with a step time of 50 s, an initial value of 0, and a final value of 0.4. The desired distance is defined as $x_{d_i} = 5m$. Additionally, one measurement noise source is considered in Simulink. The time delay injected into the input is defined as $\tau_i(t) = \rho\,(2\sin(t/2) + 3)$ where ρ is a coefficient varied in the results. In the dynamic models of the follower and leader vehicles, as described in (1) and (2), the injected disturbance is defined as $d_i(t) = d_{i-1}(t) = 0.01\sin(t/8)$. In this scenario, we compare our proposed resilient controller, which compensates for both FDI attacks and input delays, with two baseline controllers. The first baseline controller, as described in Ansari-Bonab et al. (2024), lacks input delay compensation but compensates for FDI attacks. The second baseline controller lacks compensation for both input delays and FDI attacks.

Figure 4 illustrates the distance between follower and lead vehicles. The proposed resilient controller aims to maintain the desired distance, indicating that an excessive gap between vehicles is also undesirable. CACC is designed not only to ensure safety but also to enhance traffic flow by optimising space for additional vehicles. As shown in sub-figure (a), the resilient controller maintains the desired distance of 5 m, despite some overshoots and undershoots, which do not compromise safety. Even during undershoots, the distance between the two vehicles remains safe. In the baseline 1 controller, which lacks input delay compensation but compensates for FDI attacks, there are numerous overshoots and undershoots. In one instance, the undershoot results in a shorter distance between the vehicles compared to the resilient controller. The baseline 2 controller, which does not compensate for either input delays or FDI attacks, exhibits frequent overshoots

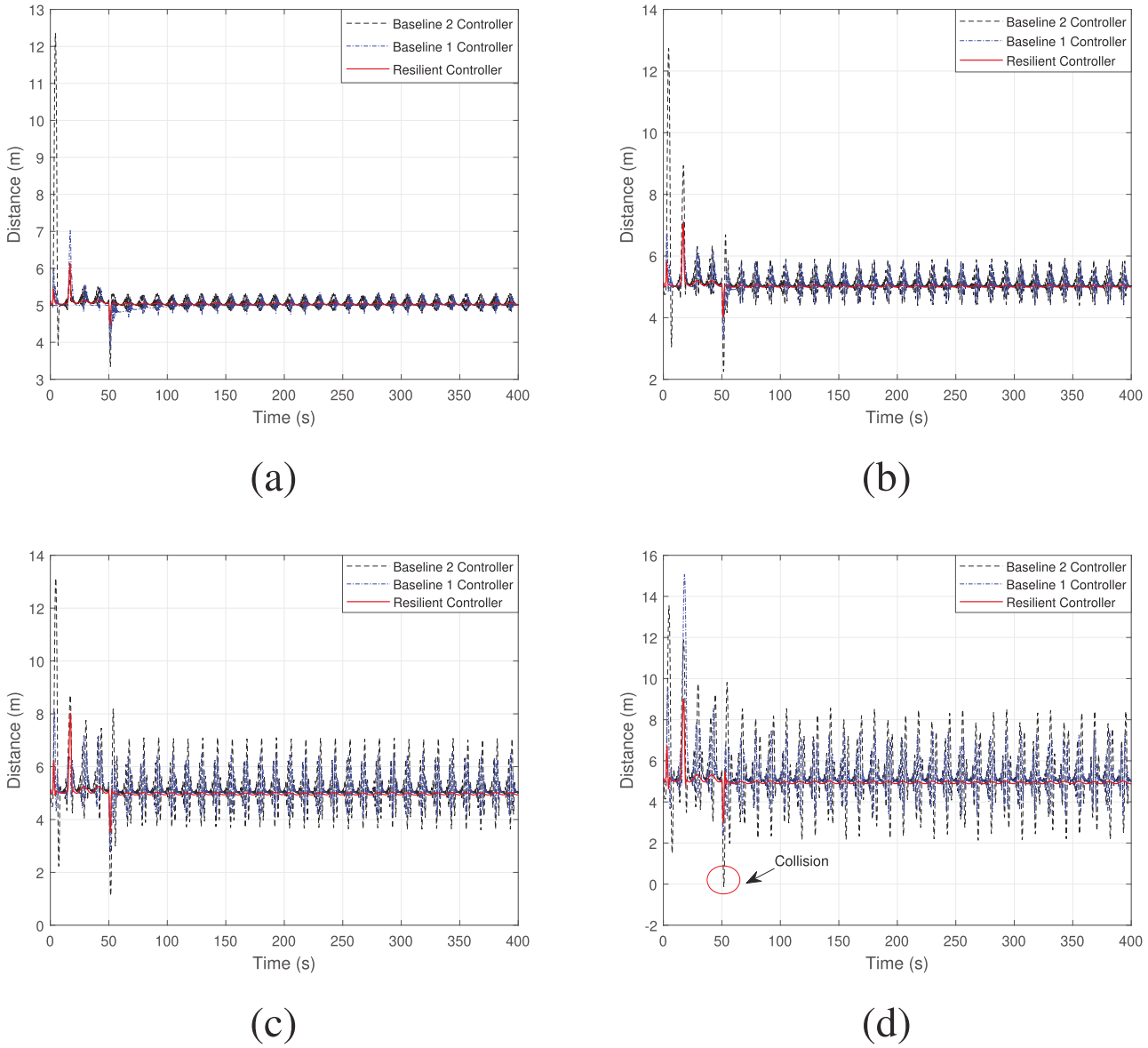

Figure 4. Scenario 1: (a) Distance between vehicles ($\rho = 0.02$). (b) Distance between vehicles ($\rho = 0.04$). (c) Distance between vehicles ($\rho = 0.06$). (d) Distance between vehicles ($\rho = 0.08$).

and undershoots, leading to vehicles being either too closely packed or excessively spaced apart. Additional sub-figures showing the resilient controller and baseline controllers with higher ρ values exhibit similar outcomes to sub-figure (a). However, as the input delay value increases, the baseline controllers yield worse results, causing vehicles to be either too closely spaced or too far apart.

As illustrated in sub-figure (d), the baseline 1 controller shows numerous oscillations in vehicle distance, with significant overshoots causing vehicles to move very far apart and undershoots reducing the distance to 2 m. For the baseline 2 controller, the distance reduces to zero during undershoots, resulting in a crash. In contrast, the resilient controller maintains a minimum distance of more than 3 m during undershoots.

Therefore, the baseline 1 controller, which compensates for FDI attack, performs better than the baseline 2 controller, which does not compensate for input delays or FDI attacks. However, the proposed resilient controller demonstrates the best performance, minimising the risk of crashes by compensating for both FDI attacks and input delays. Thus, the proposed nonlinear controller guarantees a safe distance between vehicles.

Table 1. Scenario 1: Root mean square error of distance.

ρ	Resilient controller	Baseline 1 controller	Baseline 2 controller
0.02	0.1155	0.1670	0.2610
0.04	0.1797	0.2922	0.7424
0.06	0.2480	0.5427	1.0369
0.08	0.3348	1.1855	1.3913

Table 2. Scenario 1: Root mean square error of FDI attack estimation.

ρ	Resilient controller	Baseline 1 controller
0.02	0.0478	0.0480
0.04	0.0482	0.0485
0.06	0.0486	0.0490
0.08	0.0490	0.0494

To enhance the clarity of Figure 4, Table 1 is presented, which shows the RMSE of the distance between vehicles and the desired distance of 5 m. The first column of the table lists the ρ values, the second column provides the RMSE of the distance between vehicles and the desired distance using the proposed resilient controller, the third column presents the RMSE using the baseline 1 controller, and the last column shows the RMSE using the baseline 2 controller. The RMSE data were collected for ρ values ranging from 0.02 to 0.08, chosen to represent a range of operational conditions under which all controllers were evaluated.

The data indicates a consistent trend: as ρ increases, the RMSE for all three controllers also increases. However, the rate of increase and the absolute RMSE values differ significantly among the controllers. For ρ values from 0.02 to 0.08, the resilient controller consistently exhibits a lower RMSE compared to the baseline controllers. This suggests that the resilient controller is more accurate under these conditions. The baseline 1 controller shows an increase in RMSE compared to the resilient controller, while the baseline 2 controller exhibits a more significant increase in RMSE, especially beyond $\rho = 0.06$. This sharp increase, particularly between ρ values of 0.06 and 0.08, indicates substantial performance degradation under more challenging conditions.

Overall, while the baseline 1 controller performs better than the baseline 2 controller, it does not perform as well as the resilient controller. The resilient controller's superior performance, as evidenced by its lower RMSE values, demonstrates its effectiveness in maintaining the desired distance between vehicles across varying operational conditions.

The velocities of the follower and leader vehicles for ρ values ranging from 0.02 to 0.08 are depicted in Figure 5. Sub-figure (a) shows that the velocity of the follower vehicle under the baseline controllers is unacceptable due to rapid and sharp changes throughout the simulation. Additional sub-figures illustrating follower velocity under the resilient controller and the baseline controllers with higher ρ values exhibit similar outcomes to sub-figure (a). The distinction lies in the fact that as the input time delay value increases, the baseline controllers performs worse. In the final sub-figure, the follower velocity under the baseline controllers increases abruptly, surpassing the leader's velocity, thereby posing a risk of causing accidents. However, the resilient controller performed well, effectively mitigating the effects of FDI attacks, input delay, noise, and disturbances, and successfully following the leader's velocity.

FDI attack estimation is depicted in Figure 6, which illustrate the FDI attack estimation in different delay values. Accuracy of estimation algorithm under resilient controller is shown in the sub-figure (a); however, baseline 1 controller is unable to estimate the FDI attack with the same accuracy. In addition, by increasing the delay value in other sub-figures; the FDI attack estimator under baseline 1 controller shows worse results.

To clarify the data presented in Figure 6, Table 2 provides a detailed comparison of the RMSE for FDI attack estimations under varying input time delays. The Table illustrates that our resilient controller consistently achieves a lower RMSE compared to the baseline 1 controller, demonstrating the superior performance of our proposed method in estimating FDI attacks. Despite the fluctuations observed in the baseline 1 controller, the RMSE values remain relatively moderate. Additionally, it is important to note that as the value of ρ increases, the RMSE values also tend to rise.

6.2.2. Scenario 2 (single input delay and varying FDI attacks)

In this section, we present the results for a scenario with a single input delay defined as $\tau_i(t) = 0.08(2\sin(t/2) + 3)$ and varying FDI attacks. We consider two models of FDI attacks: the first model includes two step functions, and the second model

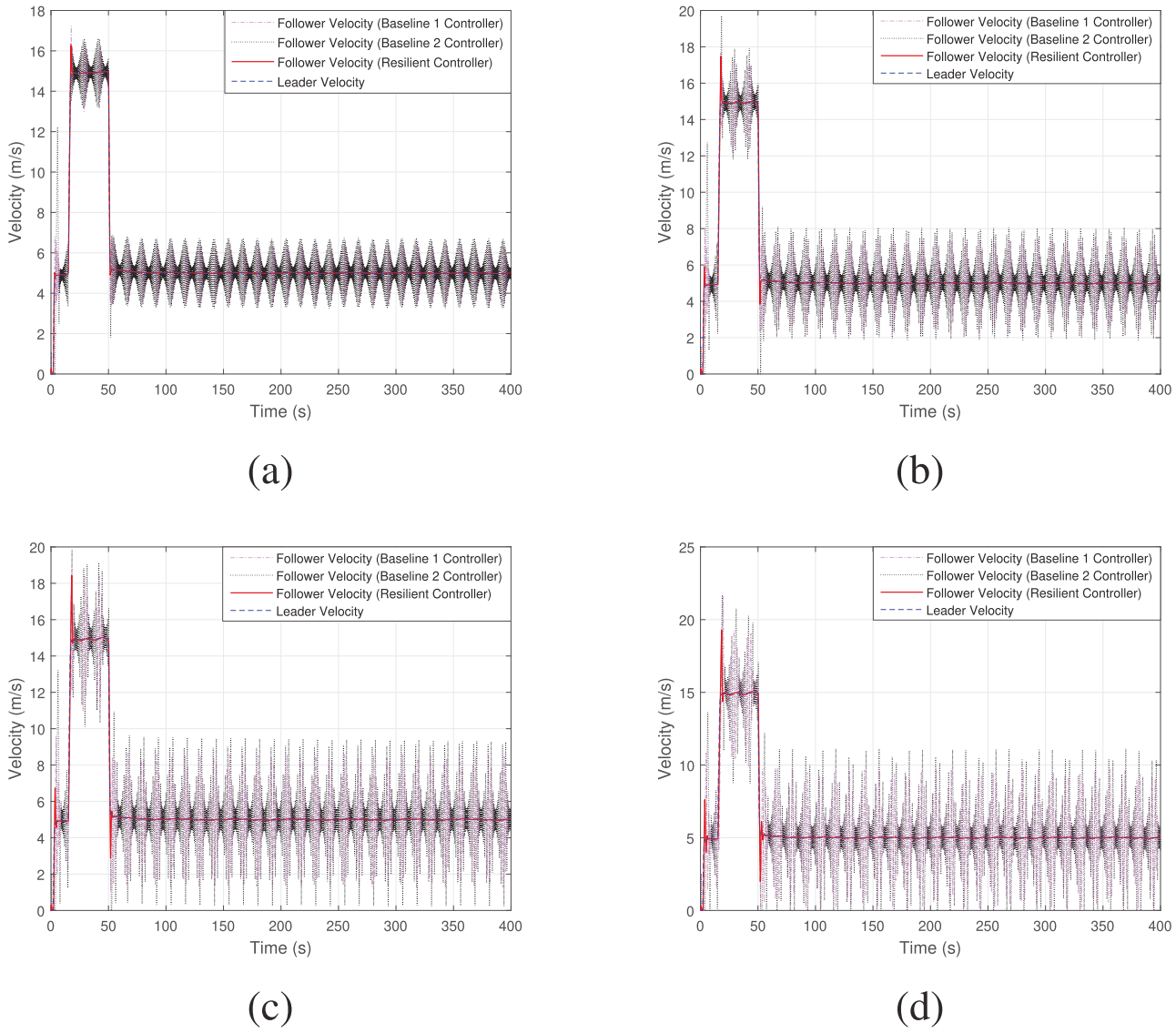

Figure 5. Scenario 1: (a) Follower and lead vehicles' velocity profile ($\rho = 0.02$). (b) Follower and lead vehicles' velocity profile ($\rho = 0.04$). (c) Follower and lead vehicles' velocity profile ($\rho = 0.06$). (d) Follower and lead vehicles' velocity profile ($\rho = 0.08$).

combines one step function and one sinusoidal function. For the first model, the FDI attack is modelled as a step function with a step time of 30 s, an initial value of 0, and a final value of 0.3, plus another step function with a step time of 80 s, an initial value of 0, and a final value of 0.05. The second model of the FDI attack combines a step function with a step time of 20 s, an initial value of 0, and a final value of 0.25, and a sinusoidal function $\sin(t/8)$. The desired distance is defined as $x_{d_i} = 5m$. Additionally, one measurement noise source is considered in Simulink. In the dynamic models of the follower and leader vehicles, as described in (1) and (2), the injected disturbance is defined as $d_i(t) = d_{i-1}(t) = 0.01\sin(t/8)$. In this scenario, we compare our proposed resilient controller, which compensates for both FDI attacks and input delays, with two baseline controllers. The first baseline controller, as described in Ansari-Bonab et al. (2024), lacks input delay compensation but compensates for FDI attacks. The second baseline controller lacks compensation for both input delays and FDI attacks.

Figure 7 illustrates the distance between follower and lead vehicles. In sub-figure (a), the FDI attack is modelled as two step functions as explained earlier, and input delay is considered. The baseline 1 controller, which compensates for the FDI attack but is unable to compensate for the input delay, exhibits some overshoots and undershoots, with a collision risk during undershoots as the vehicles' distance reduces to less than 2 m. Baseline 2 controller performs worse

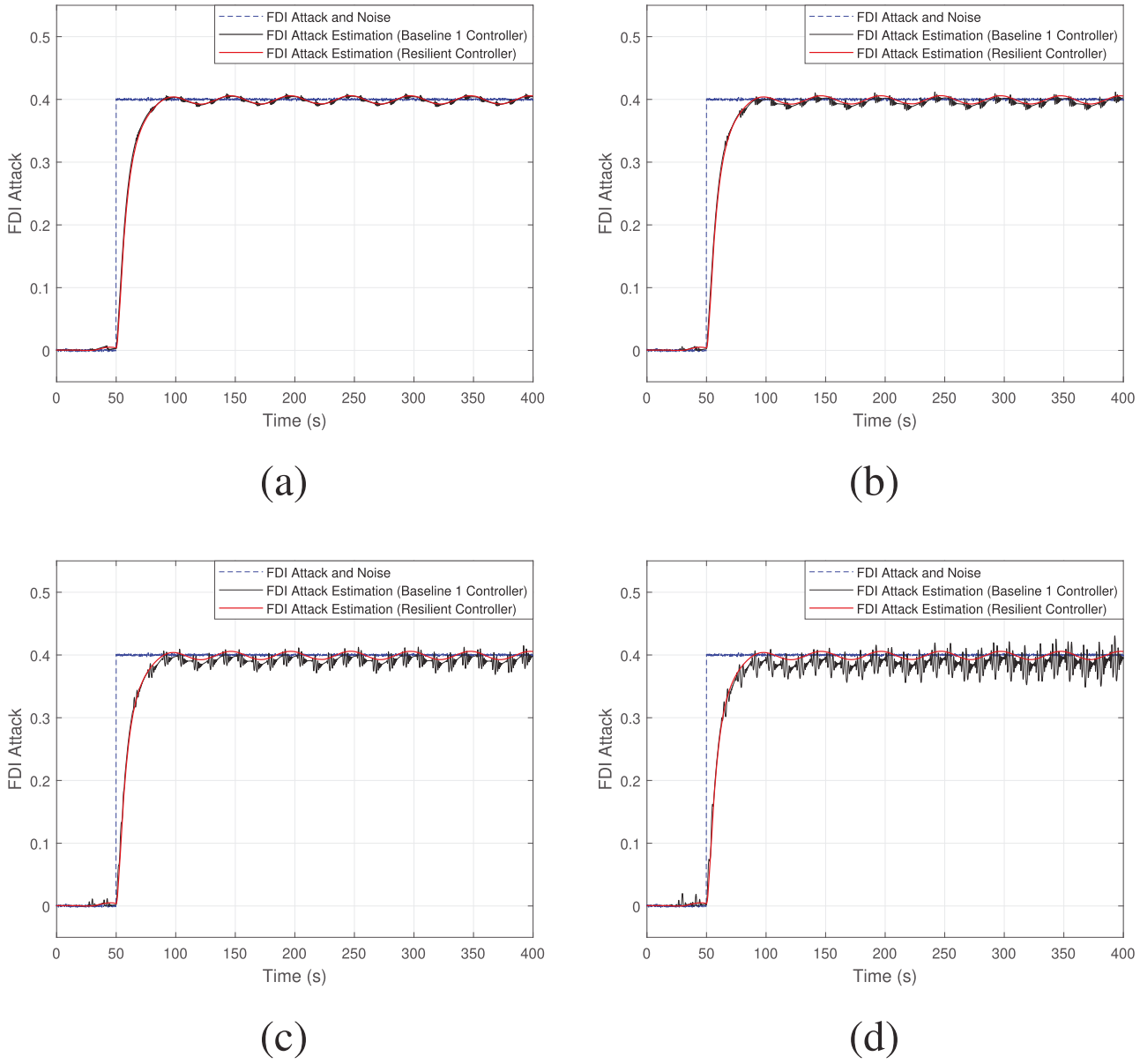

Figure 6. Scenario 1: (a) FDI attack estimation ($\rho = 0.02$). (b) FDI attack estimation ($\rho = 0.04$). (c) FDI attack estimation ($\rho = 0.06$). (d) FDI attack estimation ($\rho = 0.08$).

since it lacks compensation for both FDI attacks and delays, resulting in collisions during undershoots. The figure clearly shows that our proposed resilient controller, which mitigates the effects of both FDI attacks and input delays, maintains a safe distance between vehicles even during undershoots. In sub-figure (b), where the FDI attack is modelled as one step function and one sinusoidal function, the results are similar to those in sub-figure (a). For both types of FDI attacks, the baseline 1 controller, which compensates for FDI attacks, performs better than the baseline 2 controller, which does not compensate for input delays or FDI attacks. However, the proposed resilient controller demonstrates the best performance, minimising the risk of crashes by compensating for both FDI attacks and input delays. Consequently, the proposed nonlinear controller guarantees a safe distance between vehicles.

To provide a clearer understanding of Figure 7, Table 3 is presented, showing the RMSE of the distance between vehicles and the desired distance of 5 m. The first column of the table lists the different FDI attacks, the second column presents the RMSE of the distance under the resilient controller, and the third and fourth columns show the RMSE values under the baseline 1 and baseline 2 controllers, respectively. As

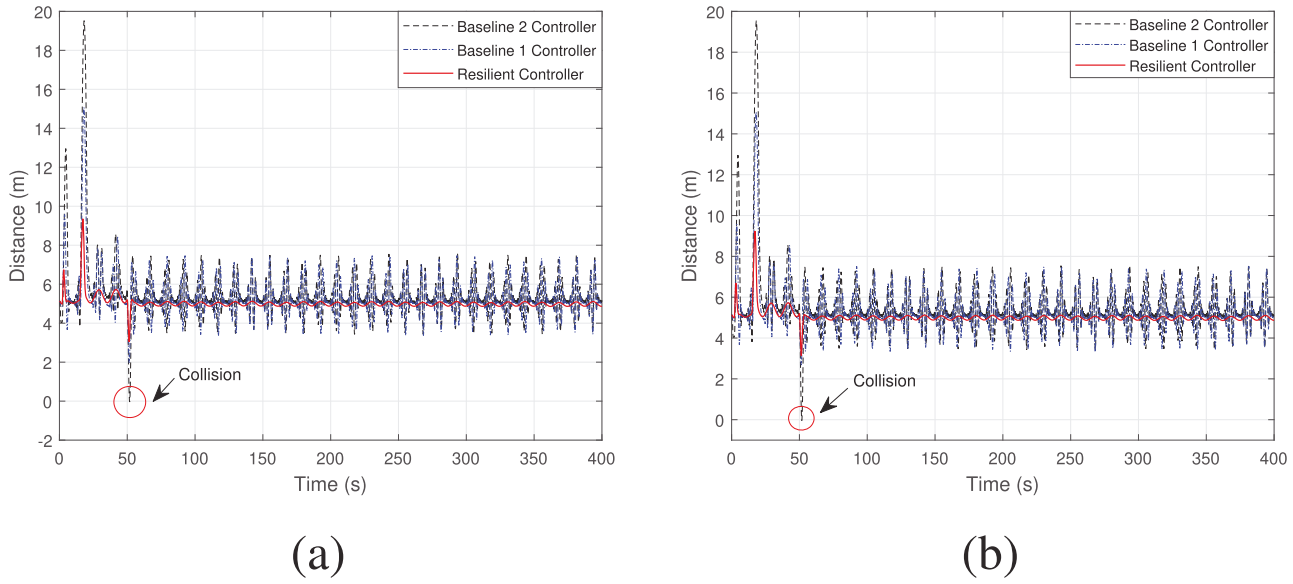

Figure 7. Scenario 2: (a) Distance between vehicles ($\tau_i(t) = 0.08(2\sin(t/2) + 3)$, and two step FDI attacks). (b) Distance between vehicles ($\tau_i(t) = 0.08(2\sin(t/2) + 3)$, and step and sinusoidal FDI attack).

Table 3. Scenario 2: Root mean square error of distance.

FDI attack	Resilient controller	Baseline 1 controller	Baseline 2 controller
Two step functions	0.3455	1.1878	1.3973
One step and one sinusoidal functions	0.1797	0.2922	0.7424

shown in the table, for both types of FDI attacks, the resilient controller effectively mitigates the impacts of FDI attacks and input delays, maintaining a safe distance between vehicles. This is evidenced by the small RMSE values between the actual and desired distances of 5 m. In contrast, under the baseline 1 controller, the RMSE value increases, indicating that while it can mitigate the impact of FDI attacks, it fails to address the delay impact, resulting in a failure to maintain the desired distance between vehicles.

Finally, the RMSE value under the baseline 2 controller is the highest, demonstrating its inability to compensate for both FDI attacks and input delays. Consequently, it fails to maintain the desired distance between vehicles, leading to potential crashes.

The velocities of the follower and lead vehicles for two types of FDI attack are depicted in Figure 8. Sub-figure (a) shows the velocities when the FDI attack is two step functions, and Sub-figure (b) shows the velocities when the FDI attack combines one step function and one sinusoidal function. In both sub-figures, the follower's velocity under baselines controllers are unacceptable due to rapid and sharp changes throughout the simulation. In contrast, the resilient controller performed well, effectively mitigating the effects of FDI attacks, input delay, noise, and disturbances, and successfully following the leader's velocity.

FDI attack estimation is depicted in Figure 9, which illustrates the estimation for different FDI attacks. Sub-figure (a) shows the estimation when the FDI attack is modelled as two step functions, while sub-figure (b) shows the estimation when the FDI attack combines one step function and one sinusoidal function. The baseline 1 controller shows worse performance compared to our proposed resilient controller. The accuracy of the estimation algorithm under the resilient controller is evident in both sub-figures. To further clarify, the following table presents the RMSE of FDI attack estimations under controllers for the two types of attacks.

To clarify the data presented in Figure 9, Table 4 provides a detailed comparison of the RMSE for various FDI attack estimations. The Table illustrates that our resilient controller consistently achieves a lower RMSE compared to the baseline 1 controller, demonstrating the superior performance of our proposed method in estimating both types of FDI attacks.

7. Conclusion

CACC is an advanced driver-assistance system that collects data from the lead vehicle and transfers to the

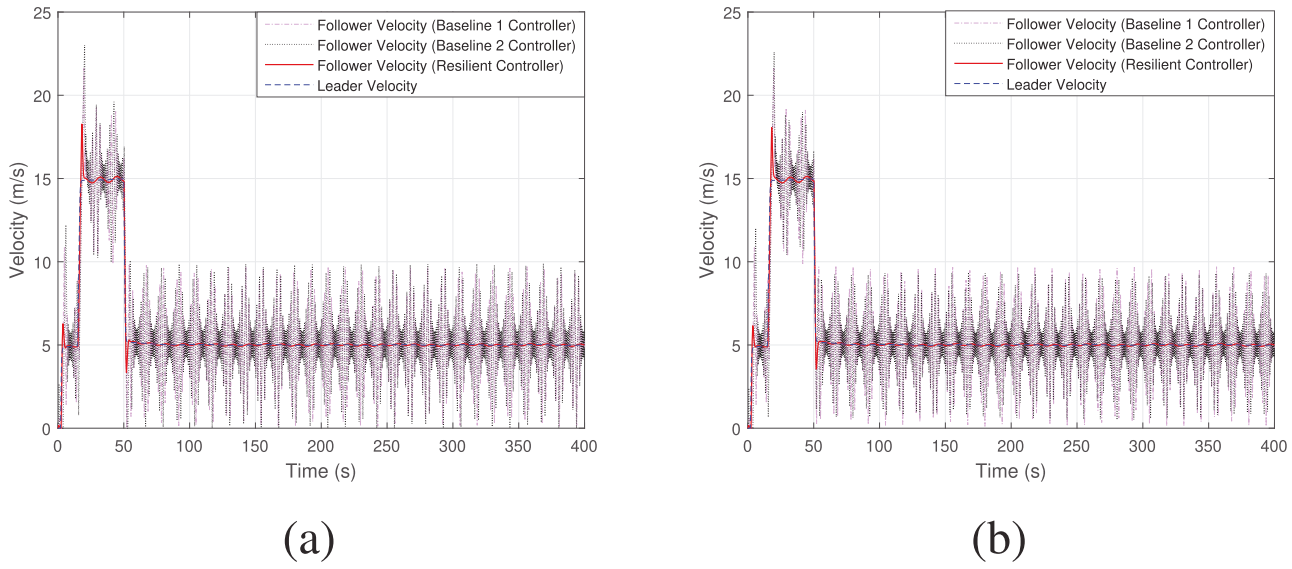

Figure 8. Scenario 2: (a) Follower and lead vehicles' velocity profile ($\tau_i(t) = 0.08(2\sin(t/2) + 3)$, and two step FDI attacks). (b) Follower and lead vehicles' velocity profile ($\tau_i(t) = 0.08(2\sin(t/2) + 3)$, and step and sinusoidal FDI attack).

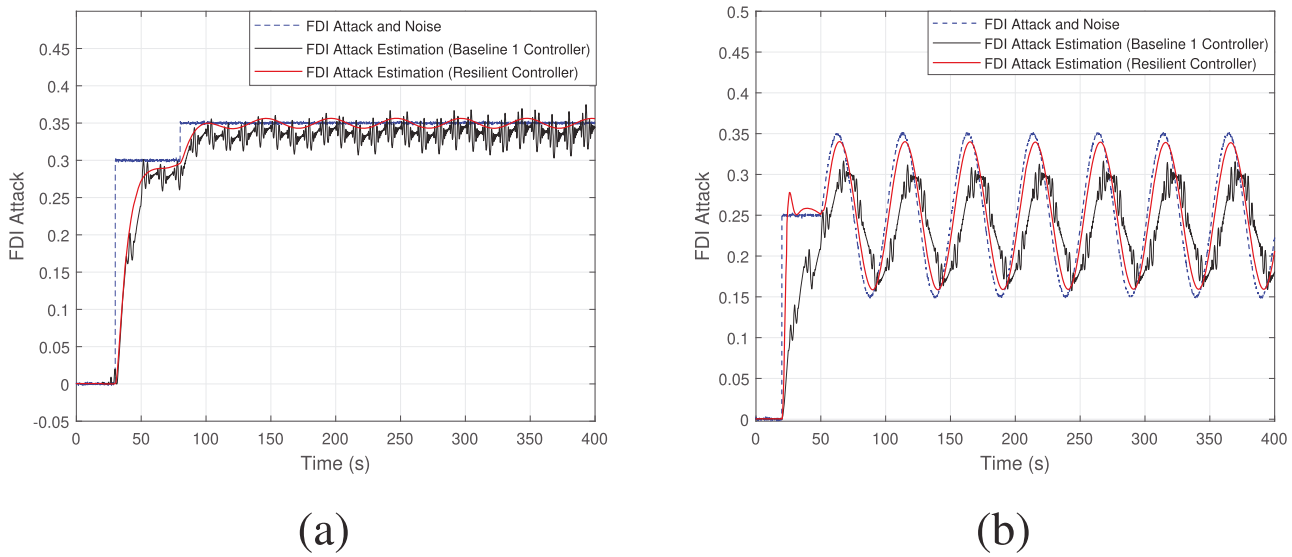

Figure 9. (a) FDI attack estimation ($\tau_i(t) = 0.08(2\sin(t/2) + 3)$, and two step FDI attacks). (b) FDI attack estimation ($\tau_i(t) = 0.08(2\sin(t/2) + 3)$, and step and sinusoidal FDI attack).

Table 4. Scenario 2: Root mean square error of FDI attack estimation.

FDI attack	Resilient controller	Baseline 1 controller
Two step functions	0.0359	0.0429
One step and one sinusoidal functions	0.0236	0.0651

follower one. To ensure the reliability of the CACC, all communications between vehicles should be safe. Therefore, all possible attacks to systems or communication channel should be recognised and removed using a secure control system. In this paper, leader's control signal is attacked by a FDI attack and noise which is an incorrect data. Also, follower vehicle's input contains a time delay; both of these can cause critical problems. In order to negate the effects of FDI attacks, noise, input time delay and disturbance, a resilient and secure control system and FDI attack estimator are designed. The proposed designs, accurately, estimate the FDI attacks and negates the effects of FDI attack, noise, time delay and disturbance, causing vehicle to maintain a safe distance throughout the

entire simulation. The simulation was run through MATLAB/Simulink. In this paper, we assumed that the lead and follower vehicles have the same dynamic models, which we obtained through an experimental setup.

7.1. Future work

Additional research could be focused on designing a secure controller with an unknown follower dynamic model. Further research into this area could outline the effects that an FDI attack has on other communication signals, primarily velocity and position. Additional research could focus on detecting and mitigating of other types of attacks such as time-delay switch, and denial of service attacks. This will be beneficial because they are the most common adversarial attacks on CAVs.

Notes

1. In real-world situations, the control signal is bounded due to the dynamic behaviour of vehicles.
2. Lyapunov–Krasovskii (LK) functionals, originating from time-delay systems and stability analysis, extend classical Lyapunov functions to handle delayed systems. They aim to provide a sufficient condition for the stability of these systems (Kolmanovskii, 1999).

Disclosure statement

No potential conflict of interest was reported by the author(s).

Data availability statement

The data that support the findings of the numerical results are available from the authors upon reasonable request.

Funding

This research is supported in part 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.

References

Ansari-Bonab, P., Holland, J. C., Cunningham-Rush, J., Noei, S., & Sargolzaei, A. (2024). Secure control design for cooperative adaptive cruise control under false data injection attack. *IEEE Transactions on Intelligent Transportation Systems*, *25*(8), 9723–9732. https://doi.org/10.1109/TITS.2024.3395208

Biroon, R. A., Abdollahi Biron, Z., & Pisu, P. (2022). False data injection attack in a platoon of CACC: Real-time detection and isolation with a pde approach. *IEEE Transactions on Intelligent Transportation Systems*, *23*(7), 8692–8703. https://doi.org/10.1109/TITS.2021.3085196

Biroon, R. A., Pisu, P., & Abdollahi, Z. (2020). Real-time false data injection attack detection in connected vehicle systems with pde modeling. In *American Control Conference*.

Bonab, P. A., Holland, J., & Sargolzaei, A. (2023). An observer-based control for a networked control of permanent magnet linear motors under a false-data-injection attack. In *2023 IEEE Conference on Dependable and Secure Computing (DSC)* (pp. 1–8).

Bonab, P. A., & Sargolzaei, A. (2024). A nonlinear control design for cooperative adaptive cruise control with time-varying communication delay. *Electronics*, *13*(10), 1875. https://doi.org/10.3390/electronics13101875.

Cai, Z., de Queiroz, M. S., & Dawson, D. M. (2006). A sufficiently smooth projection operator. *IEEE Transactions on Automatic Control*, *51*(1), 135–139. https://doi.org/10.1109/TAC.2005.861704

Campbell, M., Egerstedt, M., How, J. P., & Murray, R. M. (2010). Autonomous driving in urban environments: Approaches, lessons and challenges. *Philosophical Transactions of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, *368*(1928), 4649–4672.

Chakraborty, I., Mehta, S. S., Doucette, E., & Dixon, W. E. (2017). Control of an input delayed uncertain nonlinear system with adaptive delay estimation. In *2017 American Control Conference (ACC)* (pp. 1779–1784). IEEE.

Desjardins, C., & Chaib-draa, B. (2011). Cooperative adaptive cruise control: A reinforcement learning approach. *IEEE Transactions on Intelligent Transportation Systems*, *12*(4), 1248–1260. https://doi.org/10.1109/TITS.2011.2157145

Emirler, M. T., Güvenç, L., & Güvenç, B. A. (2018). Design and evaluation of robust cooperative adaptive cruise control systems in parameter space. *International Journal of Automotive Technology*, *19*, 359–367. https://doi.org/10.1007/s12239-018-0034-z

Faghihian, H., & Sargolzaei, A. (2023). Energy efficiency of connected autonomous vehicles: A review. *Electronics*, *12*(19), 4086. https://doi.org/10.3390/electronics12194086

Guanetti, J., Kim, Y., & Borrelli, F. (2018). Control of connected and automated vehicles: State of the art and future challenges. *Annual Reviews in Control*, *45*, 18–40. https://doi.org/10.1016/j.arcontrol.2018.04.011

Keijzer, T., & Ferrari, R. M. (2019). A sliding mode observer approach for attack detection and estimation in autonomous vehicle platoons using event triggered communication. In *2019 IEEE 58th Conference on Decision and Control (CDC)* (pp. 5742–5747). IEEE.

Kolmanovskii, V. B. (1999). On the Lyapunov–Krasovskii functionals for stability analysis of linear delay systems. *International Journal of Control*, *72*(4), 374–384. https://doi.org/10.1080/002071799221172

Liu, Y., Wang, W., Hua, X., & Wang, S. (2020). Safety analysis of a modified cooperative adaptive cruise control algorithm

accounting for communication delay. *Sustainability*, *12* (18), 7568.

Lunze, J. (2020). Design of the communication structure of cooperative adaptive cruise controllers. *IEEE Transactions on Intelligent Transportation Systems*, *21*(10), 4378–4387. https://doi.org/10.1109/TITS.6979

Milanés, V., Shladover, S. E., Spring, J., Nowakowski, C., Kawazoe, H., & Nakamura, M. (2014). Cooperative adaptive cruise control in real traffic situations. *IEEE Transactions on Intelligent Transportation Systems*, *15*(1), 296–305. https://doi.org/10.1109/TITS.2013.2278494

NHTSA. (2016). 2015 motor vehicle crashes: Overview. *Traffic Safety Facts Research Note*, *2016*, 1–9.

Niroumand, F. J., Ansari Bonab, P., & Sargolzaei, A. (2024). Security of connected and autonomous vehicles: A review of attacks and mitigation strategies. In *SoutheastCon 2024* (pp. 1197–1204).

Patre, P. M., MacKunis, W., Kaiser, K., & Dixon, W. E. (2008). Asymptotic tracking for uncertain dynamic systems via a multilayer neural network feedforward and rise feedback control structure. *IEEE Transactions on Automatic Control*, *53*(9), 2180–2185. https://doi.org/10.1109/TAC.2008.930200

Ploeg, J., Scheepers, B. T. M., van Nunen, E., van de Wouw, N., & Nijmeijer, H. (2011). Design and experimental evaluation of cooperative adaptive cruise control. In *2011 14th International IEEE Conference on Intelligent Transportation Systems (ITSC)* (pp. 260–265).

Sargolzaei, A. (2021). A secure control design for networked control system with nonlinear dynamics under False-Data-Injection attacks. In *2021 American Control Conference (ACC)* (pp. 2693–2699). IEEE.

Sargolzaei, A., Crane, C. D., Abbaspour, A., & Noei, S. (2016). A machine learning approach for fault detection in vehicular cyber-physical systems. In *2016 15th IEEE International Conference on Machine Learning and Applications (ICMLA)* (pp. 636–640). IEEE.

Sargolzaei, A., Yazdani, K., Abbaspour, A., Crane III, C. D., & Dixon, W. E. (2020). Detection and mitigation of false data injection attacks in networked control systems. *IEEE Transactions on Industrial Informatics*, *16*(6), 4281–4292. https://doi.org/10.1109/TII.9424

Shladover, S. E. (2018). Connected and automated vehicle systems: Introduction and overview. *Journal of Intelligent Transportation Systems*, *22*(3), 190–200. https://doi.org/10.1080/15472450.2017.1336053

Shladover, S. E., Nowakowski, C., Lu, X.-Y., & Ferlis, R. (2015). Cooperative adaptive cruise control: Definitions and operating concepts. *Transportation Research Record*, *2489*(1), 145–152. https://doi.org/10.3141/2489-17

Sun, X., Yu, F. R., & Zhang, P. (2022). A survey on cyber-security of connected and autonomous vehicles (CAVS). *IEEE Transactions on Intelligent Transportation Systems*, *23*(7), 6240–6259. https://doi.org/10.1109/TITS.2021.3085297

Sybis, M., Vukadinovic, V., Rodziewicz, M., Sroka, P., Langowski, A., Lenarska, K., & Wesołowski, K. (2019). Communication aspects of a modified cooperative adaptive cruise control algorithm. *IEEE Transactions on Intelligent Transportation Systems*, *20*(12), 4513–4523. https://doi.org/10.1109/TITS.6979

Yazgan, M., Arslan, H., & Vakalis, S. (2024). Non-cooperative high-efficiency multi-user ranging using ofdm signals. In *2024 IEEE Wireless and Microwave Technology Conference (WAMICON)* (pp. 1–4).

Zideh, M. J., Chatterjee, P., & Srivastava, A. K. (2023). Physics-informed machine learning for data anomaly detection, classification, localization, and mitigation: A review, challenges, and path forward.