Fuzzy Unknown Input Observer for Estimating Sensor and Actuator Cyber-Attacks in Intelligent Connected Vehicles

Juntao Pan, Tran Anh-Tu Nguyen, Sujun Wang, Huifan Deng, Hui Zhang

Fuzzy Unknown Input Observer for Estimating Sensor and Actuator Cyber-Attacks in Intelligent Connected Vehicles

Article *in* Automotive Innovation · June 2023

DOI: 10.1007/s42154-023-00228-1

CITATIONS
0

READS
115

5 authors, including:

Anh-Tu Nguyen
Université Polytechnique Hauts-de-France
140 PUBLICATIONS **2,084** CITATIONS

SEE PROFILE

Huifan Deng
Nanjing University of Aeronautics & Astronautics
21 PUBLICATIONS **134** CITATIONS

SEE PROFILE

Fuzzy Unknown Input Observer for Estimating Sensor and Actuator Cyber-Attacks in Intelligent Connected Vehicles

Juntao Pan, Anh-Tu Nguyen*, Sujun Wang, Huifan Deng, Hui Zhang

***Abstract*—The detection and mitigation of cyber-attacks in connected vehicle systems (CVSs) are critical for ensuring the security of intelligent connected vehicles. This paper presents a solution to estimate sensor and actuator cyber-attacks in CVSs. A novel method is proposed that utilizes an augmented system representation technique and a nonlinear unknown input observer (UIO) to achieve asymptotic estimation of both CVS dynamics and cyber-attacks. The nonlinear CVS dynamics are represented in a Takagi-Sugeno (TS) fuzzy form with nonlinear consequents, which allows for the effective use of the differential mean value theorem to handle unmeasured premise variables. Furthermore, via Lyapunov stability theory we propose sufficient conditions, expressed in terms of linear matrix inequalities, to design TS fuzzy UIO. Several test scenarios are performed with high-fidelity Simulink-CarSim co-simulations to show the effectiveness of the proposed cyber-attack estimation method.**

***Index Terms*—Connected vehicle systems, cyber-attacks, unknown input observers, vehicle dynamics estimation, Takagi-Sugeno fuzzy models.**

J. Pan and S. Wang are with School of Electrical and Information Engineering, North Minzu University, Yinchuan 750021, China.

A.-T. Nguyen is with the Université Polytechnique Hauts-de-France, CNRS, UMR 8201 – LAMIH, F-59313 Valenciennes, France. A.-T. Nguyen is also with the INSA Hauts-de-France, F-59313 Valenciennes, France.

H. Deng is with the Department of Vehicle Engineering, Nanjing University of Aeronautics and Astronautics, Nanjing 210016, China. Huifan Deng is also a visiting PhD student at with the Université Polytechnique Hauts-de-France, CNRS, UMR 8201 – LAMIH, F-59313 Valenciennes, France.

H. Zhang is with the School of Transportation Science and Engineering, Beihang University, Beijing 100191, China.

*Corresponding author (email: nguyen.trananhtu@gmail.com)

ACRONYMS

CACC	Cooperative Adaptive Cruise Control
CCC	Connected Cruise Control
CVS	Connected Vehicle Systems
DoS	Denial-of-Service
LMI	Linear Matrix Inequality
MAE	Mean Absolute Errors
PDE	Partial Differential Equation
PIV	Proportional-Integral-Velocity
RMSD	Root Mean Square Deviations
TS	Takagi-Sugeno
UI	Unknown Input
UIO	Unknown Input Observer
V2V	Vehicle-to-Vehicle
V2I	Vehicle-to-Infrastructure

I. INTRODUCTION

Over the past decades, with an increasing transportation demand of modern society, the number of vehicles on the road has experienced a considerable growth, which has put great pressure on the traffic system. Therefore, alleviating traffic congestion and improving driving safety and fuel economy have recently received a particular attention within the field of traffic systems [1]. Connected vehicle systems (CVS) allow connected vehicles to obtain traffic information using wireless vehicle-to-vehicle (V2V) and/or vehicle-to-infrastructure (V2I) communication. CVS technologies have been one of the most prospective solutions to alleviate traffic congestion and improve traffic safety [1]–[3].

CVSs are designed to allow vehicles to maintain a distance-dependent velocity using V2V and/or V2I information received from leading vehicles. With the benefit of those wireless communication technologies, connected autonomous vehicles can increase traffic efficiency by enabling closer vehicle following. Moreover, CVS technologies can improve the efficiency of the fuel consumption using knowledge of future vehicle trajectories, and enhance driving safety by blocking shock wave propagation [4]. Various modeling and control schemes have been investigated for CVSs [2], [5], *e.g.*, connected

cruise control (CCC) [6], [7] and cooperative adaptive cruise control (CACC) [8]–[10]. However, despite a great advance in CVS control and estimation techniques, CVSs are still vulnerable to undesired cyber-attacks from the connected networks. Such network failures may significantly deteriorate the performance of CVSs. Hence, handling effectively any potential cyber-attacks is essential for CVS technologies [1].

CVS cyber-attack related issues have been extensively studied in recent decades, see for instance [9], [11]–[13]. The risks of CVS cyber-attacks include packet dropping [14], denial of service [11], [15], communication induced-delay [16], etc. The authors in [17] present an attacker identification scheme for CVSs, which can effectively recognize the malicious actors. Using a partial differential equation (PDE) approach, false data injection attacks have been studied for a platoon of connected vehicles equipped with cooperative adaptive cruise control in [9]. The analysis of string stability is also important for CVS system under cyber-attacks. Communication-based control methods have been proposed for CVSs that can guarantee the string stability despite the time delays in the control loop [18], [19]. The authors in [20] present a state-estimation-based control method for connected cruise control with delays. An event-triggered control problem has been investigated in [21] for connected vehicles under multiple and aperiodic cyber-attacks, including denial-of-service (DoS) attacks and deception attacks. Although the modeling, the control design and the stability analysis of CVSs are widely studied in the existing literature, the problem of real-time detection of cyber-attacks of CVSs has not been well addressed despite its critical importance.

Two observer design methods have been proposed to estimate vehicle speed sensor faults in [22]. The authors in [23] proposed a sliding mode observer to detect and estimate DoS attacks of CVSs. Based on a modified unbiased finite impulse response estimator, a method has been proposed in [24] for the detection and estimation of deception attacks for a local vehicle in vehicle platooning. The authors in [25] have investigated the distributed attack detection and recovery in a vehicle platooning control system, wherein an active adversary may introduce cyber-attacks to deteriorate both sensor and control data due to the presence of the wireless communication. A cyber-attack detection method for autonomous vehicles, under attacks in the vehicle localization system, based on secure estimation of vehicle states has been proposed in [26]. Note that most of the existing results on CVSs have focused on either cyber-attacks or sensor faults, which do not allow for a simultaneous estimation/detection of cyber-attacks at both sensors and actuators levels. An unknown input (UI) observer-based fault detection method has been recently presented in [12], which can jointly detect a fault in the radar system and a cyber-attack. However, for unknown input observer (UIO) design in [12], nonlinearities in CVS dynamics must be neglected. Obviously, nonlinear behaviors involved in CVS dynamics have important impacts on the detection and estimation performance of faults and/or cyber-attacks [2], [6].

Motivated by the above-mentioned CVS issues, we develop a new nonlinear UIO-based method to estimate cyber-attacks and/or faults potentially affecting both CVS actuators and sensors. To take into account the inherent nonlinear nature of CVS dynamics, Takagi-Sugeno (TS) fuzzy technique is adopted for nonlinear UIO design. Different from the conventional TS fuzzy modeling [27], largely used in the current nonlinear control and estimation literature, the nonlinear CVS dynamics is represented in a specific TS fuzzy form with nonlinear fuzzy consequents, called N-TS fuzzy form [28]. By means of the differential mean value theorem, this N-TS fuzzy form allows dealing with the problem of unmeasured premise variables while avoiding the conservative Lipschitz assumption in TS fuzzy observer design [29]. The main contributions of this paper can be summarized as follows.

- The nonlinear CVS dynamics is represented using a N-TS fuzzy model with nonlinear consequents. This allows not only to reduce the number of fuzzy rules, *i.e.*, TS local submodels, but also to effectively deal with unmeasured nonlinearities via the differential mean value theorem for TS fuzzy UIO design.
- Using an augmented system technique, the proposed TS fuzzy UIO can achieve an asymptotic estimation convergence of both the CVS dynamics and the sensor and actuator cyber-attacks. In particular, the proposed estimation method does not require any *a priori* information on the fault/cyber-attack signals, which is typically unavailable due to the random nature of cyber-attacks, as most of existing estimation results [30], [31].
- Based on Lyapunov stability theory, the TS fuzzy UIO design condition is represented by a set of linear matrix inequality (LMI) constraints, which can be solved with existing numerical solvers. Moreover, the effectiveness of the proposed estimation method is verified through high-fidelity Simulink-CarSim co-simulation results, obtained under different types of cyber-attack signals.

The paper is organized as follows. Section II presents the modeling of the nonlinear CVS dynamics for UIO de-

sign. Section III first formulates the estimation problem, then LMI design conditions are derived using Lyapunov stability theory. Simulink-CarSim simulation results are provided in Section IV to show the effectiveness of the proposed UIO-based method for the simultaneous estimation of CVS dynamics and cyber-attacks. Section V concludes the paper with related future works.

Notation. For vector a, its jth element is denoted by a_j. For matrix Y, its transpose and Moore–Penrose pseudo-inverse are denoted by $Y^\top$ and $Y^\dagger$, respectively. $Y \succ 0$ ($Y \prec 0$) means that Y is positive (negative) definite. The symbol $\star$ represents transpose terms in a symmetric matrix. For two vectors $\mathcal{A}, \mathcal{B} \in \mathbb{R}^{n_x}$, denote $\mathrm{co}(\mathcal{A}, \mathcal{B}) = \{(1-\chi)\mathcal{B} + \chi\mathcal{A} : \ \chi \in [0,1]\}$ as the convex hull of $\mathcal{A}$ and $\mathcal{B}$. $\mathbb{N}_+$ denotes the positive integers set. $\mathcal{I}_q = \{1, \ldots, q\} \subset \mathbb{N}_+$. For $b \in \mathcal{I}_l$, denote $\varsigma_l(b) = [0, \ldots, 0, 1_{b^{\text{th}}}, 0, \ldots, 0]^\top \in \mathbb{R}^l$ as the canonical basis of $\mathbb{R}^l$. Denote I as the unit matrix. We omit the arguments of functions when the meaning is clear.

II. Connected Vehicles Modeling

This section presents a CVS model with one-vehicle look-head strategy, which is practically feasible for several existing connected vehicular platoons, *e.g.*, connected cruise control or adaptive cruise control. As shown in Fig. 1, the connected vehicles communicate with each other via wireless V2V technique represented by red dashed arrows. The symbol σ denotes the communication delay, $s(t)$ and $s_L(t)$ are the position of the front bumper of vehicles while $v(t) = \dot{s}(t)$ and $v_L(t) = \dot{s}_L(t)$ are the corresponding velocities. We adopt the symbol $\ell_L(t)$ to represent the length of the vehicle. Then, the actual inter-vehicle distance $h(t)$ can be obtained as

$$h(t) = s_L(t) - s(t) - \ell_L(t). \tag{1}$$

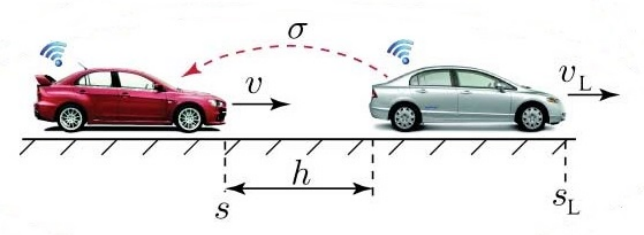

Fig. 1: Schematic of a connected vehicle system.

With an assumption of no slip condition on the wheels, the nonlinear longitudinal dynamics of connected vehicle is given by [6]

$$\dot{v}(t) = -\beta g - \frac{k_a}{m} v^2(t) + \frac{\eta}{mR} T_{en}(t), \tag{2}$$

where R is the wheel radius, β is the rolling resistance constant, m is the vehicle mass, k_a is the air drag coefficient, g is the gravitational constant, η is gear ratio. The engine torque $T_{en}(t)$ is regulated by a designed controller which is capable of keeping velocity depend on the distance. To exploit the available motion information from the leading vehicle, the following proportional-integral-velocity (PIV) controller is used:

$$\begin{aligned} T_{en}(t) &= T_{com}(t-\sigma), \\ T_{com}(t) &= k_p \dot{z}(t) + k_i z(t) + k_v \big(v_L(t) - v(t)\big), \end{aligned} \tag{3}$$

where k_p, k_i and k_v are the proportional, integral and velocity gains, respectively. The integral variable $z(t)$ in (3), defined as

$$\dot{z}(t) = \lambda\big(h(t)\big) - v(t), \tag{4}$$

is introduced to eliminate the steady-state error caused by unknown external disturbances, *e.g.*, headwind, and/or inaccurate vehicle parameters. The function $\lambda(h(t))$ is the velocity-depend range policy that should be strictly monotonously increasing such that $\lambda(h_1) = 0$ and $\lambda(h_2) = v_m$, where h_1 is the desired stopping distance, h_2 is the minimal free-flow distance, and v_m is the desired maximum velocity. To this end, we select the following range policy:

$$\lambda(h(t)) = \begin{cases} 0, & \text{if } h(t) \le h_1 \\ \frac{v_m}{2}\left(1 - \cos\left(\pi \vartheta(t)\right)\right), & \text{if } h_1 < h(t) < h_2 \\ v_m, & \text{if } h(t) \ge h_2 \end{cases} \tag{5}$$

with

$$\vartheta(t) = \frac{h(t) - h_1}{h_2 - h_1}.$$

The velocity-depend range policy defined in (5) is depicted in Fig. 2, which allows to guarantee a safe driving at a short inter-vehicle distance [6].

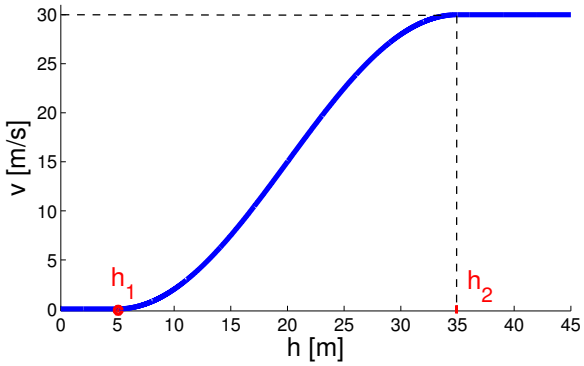

Fig. 2: Range policy of a connected vehicle system.

Using the first-order lag approximation, it follows from (3) that

$$T_{com}(t) = T_{en}(t+\sigma) \approx T_{en}(t) + \sigma \dot{T}_{en}(t). \quad (6)$$

The torque expression (6) has been widely adopted in the literature to facilitate the controller design and implementation [4]. With the approximation (6), the engine torque dynamics is rewritten as

$$\dot{w}(t) = \frac{1}{\sigma}(K_p \dot{z}(t) + K_i z(t) + K_v \epsilon_v(t) - w(t)), \quad (7)$$

with $\epsilon_v(t) = v_L(t) - v(t)$, and

$$w(t) = \frac{\eta}{mR} T_{en}(t), \quad K_p = \frac{\eta}{mR} k_p,$$
$$K_i = \frac{\eta}{mR} k_i, \qquad K_v = \frac{\eta}{mR} k_v.$$

From (1), (2), (4) and (7), the nonlinear dynamics of CVS can be established as

$$\begin{aligned} \dot{h}(t) &= v_L(t) - v(t) \\ \dot{v}(t) &= -\beta g - \frac{k_a}{m} v^2(t) + w(t) \\ \dot{z}(t) &= \lambda(h) - v(t) \\ \dot{w}(t) &= \frac{1}{\sigma}\big(K_p \dot{z}(t) + K_i z(t) + K_v \epsilon_v(t) - w(t)\big) \end{aligned} \quad (8)$$

Let $u(t) = v_L(t)$ be the CVS control input and $x(t) = \begin{bmatrix} h(t) & v(t) & z(t) & w(t) \end{bmatrix}^\top$ be the CVS state vector. Then, we derive the state-space CVS model from (8) as

$$\dot{x}(t) = A_v(x)x(t) + B_v u(t), \quad (9)$$

where

$$A_v(x) = \begin{bmatrix} 0 & -1 & 0 & 0 \\ -\frac{\beta g}{h} & -\frac{k_a}{m} v & 0 & 1 \\ \frac{\lambda(h)}{h} & -1 & 0 & 0 \\ \frac{K_p \lambda(h)}{\sigma h} & -\frac{K_p + K_v}{\sigma} & \frac{K_i}{\sigma} & -\frac{1}{\sigma} \end{bmatrix},$$
$$B_v = \begin{bmatrix} 1 & 0 & 0 & \frac{K_v}{\sigma} \end{bmatrix}^\top.$$

In real-word driving scenarios, the positions $s(t)$ and $s_L(t)$ can be obtained by the global positioning system. Using (1) and such positions information, we can deduce the actual inter-vehicle distance $h(t)$. Moreover, we assume that $T_{en}(t)$ is given by a predefined PIV controller [6] and the longitudinal velocity $v(t)$ is not directly measured from sensors. Hence, the output equation of the CVS model (9) is given by

$$y(t) = Cx(t), \quad (10)$$

with

$$C = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

For the CVS shown in Fig. 1, the vehicle receives the velocity information $v_L(t)$ from the preceding vehicle via wireless V2V communication. Hence, a undesirable fault signal may be injected due to cyber-attacks. To take into account possible cyber-attacks concerning the vehicle velocity that affect to both CVS actuator and sensor, we include the cyber-attack term $f(t)$ in the CVS dynamics (9)–(10) as

$$\begin{aligned} \dot{x}(t) &= A_v(x)x(t) + B_v u(t) + F_v f(t) \\ y(t) &= Cx(t) + Df(t) \end{aligned} \quad (11)$$

with

$$F_v = B_v = \begin{bmatrix} 1 & 0 & 0 & \frac{K_v}{\sigma} \end{bmatrix}^\top, \quad D = \begin{bmatrix} 0 & 1 \end{bmatrix}^\top.$$

Note that the CVS model (11) has three nonlinear terms in $A_v(x)$, *i.e.*, $v(t)$, $\frac{1}{h(t)}$ and $\frac{\lambda(h(t))}{h(t)}$. This induces technical challenges in designing TS fuzzy observers, especially when the variable $v(t)$ is unmeasured. Indeed, we face to the well-known problem of handling unmeasured premise variables in TS fuzzy observer design issue [29]. To overcome this problem, the CVS model (11) is reformulated in the form

$$\begin{aligned} \dot{x}(t) &= A_v(\gamma)x(t) + \phi_v(u(t)) + F_v f(t) + G_v \psi\big(x(t)\big) \\ y(t) &= Cx(t) + Df(t) \end{aligned} \quad (12)$$

with $\gamma(t) = \frac{\lambda(h(t))}{h(t)}$, $\psi\big(x(t)\big) = v^2(t)$, and

$$A_v(\gamma) = \begin{bmatrix} 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ \frac{\lambda(h)}{h} & -1 & 0 & 0 \\ \frac{K_p \lambda(h)}{\sigma h} & -\frac{K_p + K_v}{\sigma} & \frac{K_i}{\sigma} & -\frac{1}{\sigma} \end{bmatrix},$$
$$\phi_v(u) = \begin{bmatrix} v_L \\ -\beta g \\ 0 \\ \frac{K_v}{\sigma} v_L \end{bmatrix}, \quad G_v = \begin{bmatrix} 0 \\ -\frac{k_a}{m} \\ 0 \\ 0 \end{bmatrix}.$$

Hereafter, to ease the real-time implementation, the Euler's transformation is adopted to transform the continuous-time CVS model (12) into its following discrete-time counterpart:

$$\begin{aligned} x_{k+1} &= A(\gamma_k)x_k + \phi(u_k) + Ff_k + G\psi(x_k), \\ y_k &= Cx_k + Df_k, \end{aligned} \quad (13)$$

where

$$\begin{aligned} A(\gamma_k) &= T_s A_v(\gamma_k) + I, \quad F = T_s F_v, \\ \phi(u_k) &= T_s \phi_v(u_k), \qquad G = T_s G_v. \end{aligned}$$

The sampling time is given by $T_s = 0.01$ [s]. Define γ_k as the *measured* premise variable. Then, employing the

sector nonlinearity approach [32], we have the following two-rule N-TS fuzzy model of system (13):

$$\begin{aligned} x_{k+1} &= \sum_{i=1}^{2} \varrho_i(\gamma_k) A_i x_k + \phi(u_k) + F f_k + G\psi(x_k), \\ y_k &= Cx_k + Df_k. \end{aligned} \tag{14}$$

The local constant matrices A_i, for $i \in \mathcal{I}_2$, are obtained by replacing the measurable premise variable $\gamma_k = \frac{\lambda(h_k)}{h_k}$ with its maximal and minimal bounds $\overline{\gamma}$ and $\underline{\gamma}$ in $A(\gamma_k)$. The details on the local matrices A_i are given by

$$A_1 = \begin{bmatrix} 1 & -T_s & 0 & 0 \\ 0 & 1 & 0 & T_s \\ T_s\underline{\gamma} & -T_s & 1 & 0 \\ T_s K_p \underline{\gamma} & -T_s\frac{K_p+K_v}{\sigma} & T_s\frac{K_i}{\sigma} & -\frac{T_s}{\sigma}+1 \end{bmatrix},$$

$$A_2 = \begin{bmatrix} 1 & -T_s & 0 & 0 \\ 0 & 1 & 0 & T_s \\ T_s\overline{\gamma} & -T_s & 1 & 0 \\ T_s K_p \overline{\gamma} & -T_s\frac{K_p+K_v}{\sigma} & T_s\frac{K_i}{\sigma} & -\frac{T_s}{\sigma}+1 \end{bmatrix}.$$

The corresponding membership functions (MFs) are defined as

$$\varrho_1(\gamma_k) = \frac{\gamma_k - \underline{\gamma}}{\overline{\gamma} - \underline{\gamma}}, \qquad \varrho_2(\gamma_k) = \frac{\overline{\gamma} - \gamma_k}{\overline{\gamma} - \underline{\gamma}}.$$

Note that the membership functions verify the property $\varrho_1(\gamma_k) \geq 0$, $\varrho_2(\gamma_k) \geq 0$ and $\varrho_1(\gamma_k) + \varrho_2(\gamma_k) = 1$.

This paper aims at providing an effective algorithm to simultaneously estimate both the state x_k and the unknown input f_k of the CVS (8), represented by the two-rule N-TS fuzzy model (14). This estimation algorithm is based on a TS fuzzy unknown input observer, whose structure is depicted in Fig. 3. A numerically tractable UIO design is discussed in the next section.

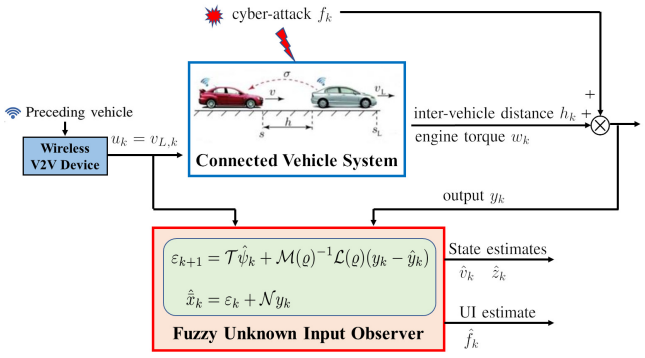

Fig. 3: Structure of the proposed TS fuzzy unknown input observer for CVS estimation.

III. Fuzzy UIO Design for Cyber-Attacks and CVS Dynamics Estimation

This section presents a method to design TS fuzzy UIO, which can be used to simultaneously estimate the states of an CVS and its potential cyber-attacks.

A. Problem Formulation

We consider the TS fuzzy model (14) in its more general form

$$\begin{aligned} x_{k+1} &= A(\varrho)x_k + \phi(\gamma_k, u_k) + F(\varrho)f_k + G(\varrho)\psi(x_k), \\ y_k &= Cx_k + Df_k, \end{aligned} \tag{15}$$

where $y_k \in \mathbb{R}^{n_y}$ is the measured output vector, $u_k \in \mathscr{B}_u \subseteq \mathbb{R}^{n_u}$ is the input vector, $x_k \in \mathscr{B}_x \subseteq \mathbb{R}^{n_x}$ is the state vector, $f_k \in \mathbb{R}^{n_f}$ is the unknown cyber-attack signal, $\gamma_k \in \mathscr{B}_\gamma \subseteq \mathbb{R}^{n_\gamma}$ is the vector of measured premise variables. The matrices in (15) are given by

$$\begin{bmatrix} A(\varrho) & F(\varrho) & G(\varrho) \end{bmatrix} = \sum_{i=1}^{n_r} \varrho_i(\gamma_k) \begin{bmatrix} A_i & F_i & G_i \end{bmatrix},$$

where the MFs $\varrho_i(\gamma_k)$ satisfying

$$\sum_{i=1}^{n_r} \varrho_i(\gamma_k) = 1, \quad 0 \leq \varrho_i(\gamma_k) \leq 1. \tag{16}$$

We denote $\varrho = \left[\varrho_1(\gamma_k), \varrho_2(\gamma_k), \ldots, \varrho_{n_r}(\gamma_k)\right]^\top \in \mathscr{F}$, $\varrho_+ = \left[\varrho_1(\gamma_{k+1}), \varrho_2(\gamma_{k+1}), \ldots, \varrho_{n_r}(\gamma_{k+1})\right]^\top \in \mathscr{F}$, where $\mathscr{F}$ is the MFs set satisfying (16). $\phi : \mathscr{B}_\gamma \times \mathscr{B}_u \to \mathbb{R}^{n_x}$ and $\psi : \mathscr{B}_x \to \mathbb{R}^{n_\psi}$ are respectively the measured and unmeasured nonlinear function. We define the Jacobian matrix of $\psi(x_k)$ as

$$\mathscr{C}_\psi(x) = \begin{bmatrix} \frac{\partial \psi_1}{\partial x_1}(x) & \cdots & \frac{\partial \psi_1}{\partial x_{n_x}}(x) \\ \vdots & \ddots & \vdots \\ \frac{\partial \psi_{n_\psi}}{\partial x_1}(x) & \cdots & \frac{\partial \psi_{n_\psi}}{\partial x_{n_x}}(x) \end{bmatrix} \in \mathbb{R}^{n_\psi \times n_x}. \tag{17}$$

In addition, we assume that the Jacobian matrix in (17) satisfies the following boundedness conditions.

Assumption 1. The elements of the matrix $\mathscr{C}_\psi(x)$ are assumed to be bounded as follows:

$$\underline{\rho}_{ij} \leq \frac{\partial \psi_i}{\partial x_j}(x) \leq \overline{\rho}_{ij}, \qquad x \in \mathscr{B}_x, \tag{18}$$

where

$$\underline{\rho}_{ij} = \min_{\mu \in \mathscr{B}_x} \left(\frac{\partial \psi_i}{\partial x_j}(\mu)\right), \quad \overline{\rho}_{ij} = \max_{\mu \in \mathscr{B}_x} \left(\frac{\partial \psi_i}{\partial x_j}(\mu)\right),$$

for $\forall (i,j) \in \mathcal{I}_{n_\psi} \times \mathcal{I}_{n_x}$. We note that the state x_k is often physically bounded for engineering systems. Hence, those lower and upper bounds of $\frac{\partial \psi_i}{\partial x_j}(x)$ in Assumption 1 can be calculated easily. For instance, as shown in

Fig. 2 we consider in this work the velocity range as $v(t) \in [0, 30]$ [m/s]. With $\psi(x) = v^2(t)$, it follows for the nonlinear observer design that $\frac{\partial \psi_i}{\partial x_j}(x) = 2v(t) \in [0, 60]$.

For estimation purposes, we extend the system (15) as

$$\begin{aligned} \bar{x}_{k+1} &= \bar{A}(\varrho)\bar{x}_k + \bar{G}(\varrho)\psi(x_k) + T_\phi \phi(\gamma_k, u_k) + T_d d_k \\ y_k &= \bar{C}\bar{x}_k \end{aligned} \tag{19}$$

where $d_k = f_{k+1}$, and

$$\bar{x}_k = \begin{bmatrix} x_k \\ f_k \end{bmatrix}, \quad \bar{A}(\varrho) = \begin{bmatrix} A(\varrho) & F(\varrho) \\ 0 & 0 \end{bmatrix},$$
$$T_\phi = \begin{bmatrix} I \\ 0 \end{bmatrix}, \qquad \bar{C} = \begin{bmatrix} C & D \end{bmatrix},$$
$$T_d = \begin{bmatrix} 0 \\ I \end{bmatrix}, \quad \bar{G}(\varrho) = \begin{bmatrix} G(\varrho) \\ 0 \end{bmatrix}.$$

Note that f_k is unknown cyber-attack signal. Then, we can regard d_k as a new UI for (19). Moreover, we introduce the following rank restriction on $\bar{C}$ and T_d:

$$\operatorname{rank} \begin{bmatrix} I & T_d \\ \bar{C} & 0 \end{bmatrix} = n_x + n_f + n_f. \tag{20}$$

Remark that the rank condition (20) is commonly used to develop unknown input observers in the literature [30], [33], [34]. Note also that the CVS model (14) verifies this rank condition for N-TS fuzzy UIO design.

We now focus on designing a TS fuzzy UIO for system (15) where the asymptotic estimation of the state and the unknown cyber-attack signal can be guaranteed. Considering the extended system (19), the estimation problem of the state x_k and the unknown signal f_k of system (15) can be converted to state estimation problem of the system (19) in the presence of the new UI d_k. To this end, we propose the TS fuzzy UIO structure

$$\begin{aligned} \varepsilon_{k+1} &= \mathcal{T}\hat{\psi}_k + \mathcal{M}(\varrho)^{-1}\mathcal{L}(\varrho)(y_k - \hat{y}_k) \\ \hat{\bar{x}}_k &= \varepsilon_k + \mathcal{N} y_k \end{aligned} \tag{21}$$

where $\hat{\psi}_k = \bar{A}(\varrho)\hat{\bar{x}}_k + T_\phi \phi(\gamma_k, u_k) + \bar{G}(\varrho)\psi(\hat{x}_k)$, $\hat{\bar{x}}_k$ is the extended state estimation. ε_k is an intermediate estimation variable. $\mathcal{T} \in \mathbb{R}^{n_x \times n_x}$, $\mathcal{M}(\varrho) \in \mathbb{R}^{n_x \times n_x}$, $\mathcal{L}(\varrho) \in \mathbb{R}^{n_x \times n_y}$, and $\mathcal{N} \in \mathbb{R}^{n_x \times n_y}$ are the gain matrices of the fuzzy UIO which need to be designed such that conditions (22a)–(22b) are verified.

$$\mathcal{T} + \mathcal{N}\bar{C} = I, \qquad \mathcal{T}T_d = 0, \tag{22a}$$

$$\mathcal{L}(\varrho) = \sum_{i=1}^{n_r} \varrho_i(\gamma_k)\mathcal{L}_i, \quad \mathcal{M}(\varrho) = \sum_{i=1}^{n_r} \varrho_i(\gamma_k)\mathcal{M}_i. \tag{22b}$$

Define $e_k = \bar{x}_k - \hat{\bar{x}}_k$ as the state estimation error. Then, from (19), (21) and (22), we have

$$e_{k+1} = \left(\mathcal{T}\bar{A}(\varrho) - \mathcal{M}(\varrho)^{-1}\mathcal{L}(\varrho)\bar{C}\right)e_k + \mathcal{T}\bar{G}(\varrho)\Delta\psi, \tag{23}$$

where $\Delta\psi = \psi(x_k) - \psi(\hat{x}_k)$. Due to the existence of the mismatching term $\Delta\psi$ in (23), several technical problems arise while designing fuzzy observers [29]. To handle $\Delta\psi$ effectively, we adopt the following differential mean value theorem [35] to reformulate $\Delta\psi$ as a function dependent to e_k.

Lemma 1 ([29])**.** Consider nonlinear function $\psi(x) : \mathbb{R}^{n_x} \to \mathbb{R}^{n_\psi}$ which is differentiable on $\operatorname{co}(\alpha, \beta)$, then there exist constant vectors $\kappa \in \operatorname{co}(\alpha, \beta)$, $\kappa \neq \alpha$, $\kappa \neq \beta$, such that

$$\psi(\alpha) - \psi(\beta) = \left(\sum_{i=1}^{n_\psi}\sum_{j=1}^{n_x} \varsigma_{n_\psi}(i)\varsigma_{n_x}^\top(j)\frac{\partial \psi_i}{\partial x_j}(\kappa)\right)(\alpha - \beta).$$

By Lemma 1, the mismatch nonlinear term $\Delta\psi$ can be reformulated as follows:

$$\begin{aligned} \Delta\psi &= \left(\sum_{i=1}^{n_\psi}\sum_{j=1}^{n_x} \varsigma_{n_\psi}(i)\varsigma_{n_x}^\top(j)\frac{\partial \psi_i}{\partial x_j}(\tau)\right)(x_k - \hat{x}_k) \\ &= \mathscr{C}_\psi(\tau)(x_k - \hat{x}_k). \end{aligned} \tag{24}$$

for $\tau \in \operatorname{co}(x_k, \hat{x}_k)$. Taking into account Assumption 1, the elements of the unknown matrix $\mathscr{C}_\psi(\tau)$ belong to a bounded convex set $\mathscr{D}_\psi$. The vertices of $\mathscr{D}_\psi$ can be obtained by

$$\mathscr{V}_\psi = \left\{ \frac{\partial \psi_i}{\partial x_j}(\tau) \in \{\underline{\rho}_{ij}, \overline{\rho}_{ij}\} \right\}, \quad \forall (i, j) \in \mathcal{I}_{n_\psi} \times \mathcal{I}_{n_x},$$

where the bounds $\underline{\rho}_{ij}$ and $\overline{\rho}_{ij}$ are given in (18). With the definition of e_k and $\bar{x}_k$, expression (24) can be rewritten as follows:

$$\Delta\psi = \underbrace{\begin{bmatrix} \mathscr{C}_\psi(\tau) & 0 \end{bmatrix}}_{\bar{\mathscr{C}}_\psi(\tau)} \underbrace{\begin{bmatrix} x_k - \hat{x}_k \\ d_k - \hat{d}_k \end{bmatrix}}_{e_k}. \tag{25}$$

From (23) and (25), the state estimation error dynamics can be rewritten as

$$e_{k+1} = \left(\mathcal{T}\mathscr{A}(\varrho, \tau) - \mathcal{M}(\varrho)^{-1}\mathcal{L}(\varrho)\bar{C}\right)e_k, \tag{26}$$

where

$$\begin{aligned} \mathscr{A}(\varrho, \tau) &= \sum_{p=1}^{n_r} \varrho_p(\gamma_k)\mathscr{A}_p(\tau), \\ \mathscr{A}_p(\tau) &= \bar{A}_p + \bar{G}_p\bar{\mathscr{C}}_\psi(\tau). \end{aligned} \tag{27}$$

The following TS fuzzy UIO design problem can be formulated.

Problem 1. Determine the gain matrices $\mathcal{M}(\varrho)$, $\mathcal{L}(\varrho)$, $\mathcal{N}$, and $\mathcal{T}$ of TS fuzzy UIO (21) such that the asymptotic convergence of the estimation error dynamics (26) can be guaranteed.

To derive the design conditions of TS fuzzy UIO, the following lemmas are adopted.

Lemma 2 ([34])**.** Given matrices $\mathcal{H}$ and $\mathcal{G}$. If the condition $\mathcal{G}\mathcal{H}^{\dagger}\mathcal{H} = \mathcal{Y}$ is verified. Then, $\mathcal{Y} = \mathcal{G}\mathcal{H}^{\dagger} + \mathcal{X}(I - \mathcal{H}\mathcal{H}^{\dagger})$ is the solution of $\mathcal{Y}\mathcal{H} = \mathcal{G}$, where $\mathcal{X}$ is an arbitrary matrix.

Lemma 3 ([36])**.** Given matrices Ω_{pql}, for $p, q, l \in \mathcal{I}_{n_r}$. The following MFs-dependent inequality

$$\Omega(\varrho, \varrho_+) = \sum_{p=1}^{n_r}\sum_{q=1}^{n_r}\sum_{l=1}^{n_r} \varrho_p(\gamma_k)\varrho_q(\gamma_k)\varrho_l(\gamma_{k+1})\Omega_{pql} \succ 0,$$

holds with $\varrho, \varrho_+ \in \mathscr{F}$ if

$$\Omega_{ppl} \succ 0, \quad p, l \in \mathcal{I}_{n_r}$$
$$\frac{2}{n_r - 1}\Omega_{ppl} + \Omega_{pql} + \Omega_{qpl} \succ 0, \quad p, q, l \in \mathcal{I}_{n_r}, \quad p \neq q.$$

B. LMI-Based UIO Design for TS Fuzzy Systems

This section provides a numerically tractable solution to the design of TS fuzzy UIO stated in Problem 1.

Theorem 1. If there exist matrices $\mathcal{N}$, $\mathcal{T}$ satisfying (22), and matrices $Q_p \in \mathbb{R}^{n_x \times n_x}$, $\mathcal{M}_p \in \mathbb{R}^{n_x \times n_x}$, $\mathcal{L}_p \in \mathbb{R}^{n_x \times n_y}$, for $p \in \mathcal{I}_{n_r}$ such that the following conditions hold:

$$\Omega_{ppl}(\tau) \succ 0, \tag{28a}$$
$$\frac{2}{n_r - 1}\Omega_{ppl}(\tau) + \Omega_{pql}(\tau) + \Omega_{qpl}(\tau) \succ 0, \tag{28b}$$

for $p, q, l \in \mathcal{I}_{n_r}$, and $p \neq q$. Then, the estimation error dynamics (23) is asymptotically stable. The quantity $\Omega_{pql}(\tau)$ is defined as

$$\Omega_{pql}(\tau) = \begin{bmatrix} Q_q & \star \\ \mathcal{M}_q\mathcal{T}\mathscr{A}_p(\tau) - \mathcal{L}_q\bar{C} & \mathcal{M}_q + \mathcal{M}_q^{\top} - Q_l \end{bmatrix},$$

with $\mathscr{A}_p(\tau)$ given in (27), for $\mathscr{C}_\psi(\tau) \in \mathscr{D}_\psi$.

Proof. Consider the fuzzy Lyapunov function candidate

$$V(e_k) = e_k^{\top}Q(\varrho)e_k, \quad Q(\varrho) = \sum_{p=1}^{n_r}\varrho_p(\gamma_k)Q_p.$$

Then, we have the following variation of $V(e_k)$ along the solution of the error dynamics (26):

$$\begin{aligned}\Delta V_k &= e_{k+1}^{\top}Q(\varrho_+)e_{k+1} - e_k^{\top}Q(\varrho)e_k \\ &= e_k^{\top}\left(\mathcal{K}^{\top}(\varrho,\tau)Q(\varrho_+)\mathcal{K}(\varrho,\tau) - Q(\varrho)\right)e(k),\end{aligned} \tag{29}$$

with $\mathcal{K}(\varrho, \tau) = \mathcal{T}\mathscr{A}(\varrho, \tau) - \mathcal{M}(\varrho)^{-1}\mathcal{L}(\varrho)\bar{C}$. Using Lemma 3 as well as the convexity property of the set $\mathscr{D}_\psi$, it follows from (28a) and (28b) that

$$\begin{bmatrix} Q(\varrho) & \star \\ \mathcal{M}(\varrho)\mathcal{T}\mathscr{A}(\varrho,\tau) - \mathcal{L}(\varrho)C & \mathscr{W}(\varrho, \varrho_+) \end{bmatrix} \succ 0, \tag{30}$$

with $\mathscr{W}(\varrho, \varrho_+) = \mathcal{M}(\varrho) + \mathcal{M}(\varrho)^{\top} - Q(\varrho_+)$, for $\varrho, \varrho_+ \in \mathscr{F}$ and $\mathscr{C}_\psi(\tau) \in \mathscr{D}_\psi$. The condition (30) implies $\mathscr{W}(\varrho, \varrho_+) \succ 0$. Note that $Q(\varrho_+) \succ 0$. Then, we have $\mathcal{M}(\varrho) + \mathcal{M}(\varrho)^{\top} \succ 0$ which guarantees the existence of $M(\varrho)^{-1}$. Multiplying (30) with $\begin{bmatrix} I & -\mathcal{K}^{\top}(\varrho,\tau)\end{bmatrix}$ on the left and $\begin{bmatrix} I & -\mathcal{K}^{\top}(\varrho,\tau)\end{bmatrix}^{\top}$ on the right, we have

$$\mathcal{K}^{\top}(\varrho,\tau)Q(\varrho_+)\mathcal{K}(\varrho,\tau) - Q(\varrho) \prec 0, \tag{31}$$

It can be seen from (29) that $\Delta V_k < 0$ can be guaranteed by (31). Hence, with the Lyapunov-based argument, we can conclude that the asymptotic stability of the estimation error dynamics (26) can be guaranteed by condition (31). □

Remark 1. The matrix conditions in (22a) can be reformulated as

$$\begin{bmatrix}\mathcal{T} & \mathcal{N}\end{bmatrix}\begin{bmatrix} I & T_d \\ \bar{C} & 0 \end{bmatrix} = \begin{bmatrix} I & 0 \end{bmatrix}. \tag{32}$$

According to Lemma 2, if the rank condition (20) is verified, the solution to (32) is given by

$$\begin{aligned}\begin{bmatrix}\mathcal{T} & \mathcal{N}\end{bmatrix} = &\begin{bmatrix} I \\ 0 \end{bmatrix}^{\top}\begin{bmatrix} I & T_d \\ \bar{C} & 0 \end{bmatrix}^{\dagger} + \\ &\mathcal{X}\left(I - \begin{bmatrix} I & T_d \\ \bar{C} & 0 \end{bmatrix}\begin{bmatrix} I & T_d \\ \bar{C} & 0 \end{bmatrix}^{\dagger}\right).\end{aligned} \tag{33}$$

The matrix of appropriate dimension $\mathcal{X}$ in (33) can be arbitrarily selected.

Remark 2. The conditions to design TS fuzzy UIO presented in Theorem 1 are expressed in terms of LMIs, which can be conveniently solved with existing LMI solvers [37]. Algorithm 4 summarizes the procedure to design the proposed TS fuzzy unknown input observer.

Algorithm 1: Fuzzy UIO Design Algorithm

Input: TS fuzzy model (15).
Output: TS fuzzy UIO (21) such that $\hat{\bar{x}}_k \to \bar{x}_k$.
1 Examine the rank conditions (20).
- If SATISFIED, move to Step 2.
- If UNSATISFIED, fuzzy UIO design failure.

2 Calculate $\mathcal{T}$ and $\mathcal{N}$ from (33).
3 Solve Theorem 1 to obtain $\mathcal{M}_i$, $\mathcal{L}_i$, for $i \in \mathcal{I}_{n_r}$.
4 Design fuzzy UIO (21) to estimate $\bar{x}_k$.

IV. Illustrative Results

This section presents illustrative results to demonstrate the effectiveness of the proposed TS fuzzy UIO design to simultaneously estimate the CVS dynamics

and cyber-attack signals. To this end, the CVS is established using a high-fidelity model in CarSim software. The TS fuzzy UIO is implemented in Matlab/Simulink. Then, Simulink-CarSim cosimulations are performed with three test scenarios with different types of cyber-attack signals to show the accurate estimation performance of proposed fuzzy UIO. The parameters of the connected vehicle are given in Table I.

To emphasize the interests of the proposed fuzzy UIO, a comparison with the conventional TS fuzzy model-based UIO design approach in [33] is performed. To this end, an eight-rule TS fuzzy model can be directly obtained from model (9) using the sector nonlinearity approach [32] with 3 premise variables $v(t)$, $\frac{1}{h(t)}$ and $\frac{\lambda(h(t))}{h(t)}$. Then, the corresponding eight-rule TS fuzzy UIO can be designed using the method in [33] with a maximum admissible Lipschitz constant $\delta_{\max} = 2.781$. However, using the optimization-based strategy in [32, Chapter 4], the real Lipschitz constant of the CVS can be computed as $\delta = 14.438$. Since $\delta \gg \delta_{\max}$, the conventional TS fuzzy model-based UIO design approach fails to provide a feasible estimation solution for the CVS. Solving Theorem 1 with SDPT3 solver, the following observer gains can be obtained:

$$\mathcal{L}_1 = \begin{bmatrix} 2.827 & 0.022 \\ -0.047 & 0.775 \\ -0.386 & -0.411 \\ -0.026 & 0.473 \\ 0.030 & -0.472 \end{bmatrix}, \quad \mathcal{L}_2 = \begin{bmatrix} 2.828 & 0.022 \\ 0.059 & 0.775 \\ -0.422 & -0.411 \\ 0.039 & 0.472 \\ -0.041 & -0.473 \end{bmatrix},$$

$$\mathcal{M}_1 = \begin{bmatrix} 5.653 & -0.004 & 0.007 & 0.004 & -0.012 \\ 0.072 & 5.700 & -1.030 & 0.766 & -0.766 \\ 0.787 & -1.033 & 2.871 & -0.418 & 0.418 \\ 0.051 & 0.681 & -0.387 & 3.274 & 2.312 \\ -0.043 & -0.681 & 0.387 & 2.312 & 3.274 \end{bmatrix},$$

$$\mathcal{M}_2 = \begin{bmatrix} 5.653 & -0.004 & 0.007 & 0.008 & -0.008 \\ 0.072 & 5.700 & -1.030 & 0.766 & -0.766 \\ 0.787 & -1.033 & 2.871 & -0.418 & 0.418 \\ 0.045 & 0.681 & -0.387 & 3.274 & 2.312 \\ -0.049 & -0.681 & 0.387 & 2.312 & 3.274 \end{bmatrix},$$

$$\mathcal{T} = \begin{bmatrix} 0.5 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1.0 & -0.0 \\ 0 & 0 & 0 & -1.0 & 0.0 \end{bmatrix}, \quad \mathcal{N} = \begin{bmatrix} 0.5 & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & -0.0 \\ 0 & 1.0 \end{bmatrix}.$$

In the sequel, three test scenarios are performed with three different types of cyber-attack signals to verify the estimation performance of the designed TS fuzzy UIO.

TABLE I: Parameters of Connected Vehicles.

Parameter	Description	Value
m	Vehicle mass	1555 [kg]
k	Air drag constant	0.46 [kg/m]
R	wheel radius	0.313 [m]
β	Rolling resistance constant	0.011
g	Gravitational constant	9.81 [m/s^2]
ℓ	Vehicle length	5 [m]
v_m	Desired maximum velocity	30 [m/s]
h_1	Desired stopping distance	5 [m]
h_2	Minimal free-flow distance	35 [m]

A. Scenario 1: Abrupt Cyber-Attack Signal

For this test scenario, the leading vehicle, with an initial velocity of 6 [m/s], drives at a constant speed after acceleration and deceleration phases as shown in Fig. 4(a). The initial inter-vehicle distance is 10 [m] while the initial velocity of the self-vehicle is 2 [m/s]. The CVS is subject to an abrupt cyber-attack as depicted in Fig. 4(b). As can be seen in Fig. 5 that the estimated CVS states quickly converge to their measurements. Moreover, Fig. 6 shows that the cyber-attack signal can be also exactly estimated by the proposed fuzzy UIO.

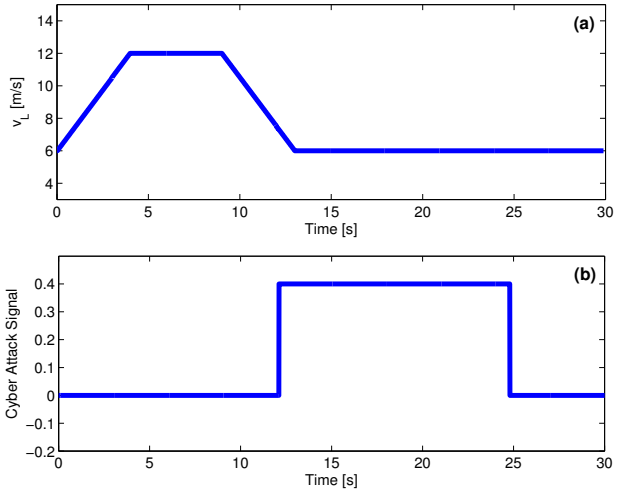

Fig. 4: Scenario 1. (a) Velocity of the leading connected vehicle v_L, (b) Cyber-attack signal.

B. Scenario 2: Repetitive Cyber-Attack Signal

For this test, the leading vehicle, with zero initial velocity, drives at a constant speed after acceleration and deceleration phases, see Fig. 7(a). The initial inter-vehicle distance is 7 [m] and the initial velocity of the self-vehicle is 1 [m/s]. To represent a repetitive cyber-attack, we select a sinusoidal signal with an amplitude of 0.35 [m/s] and a frequency as 3 [rad/s] as shown in Fig. 7(b). It can be seen from Figs. 8 and 9 that the CVS

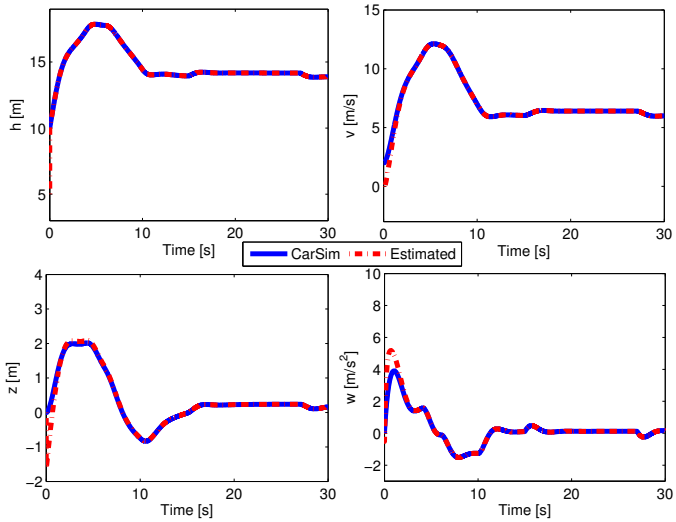

Fig. 5: Scenario 1. Estimation performance of the CVS dynamics.

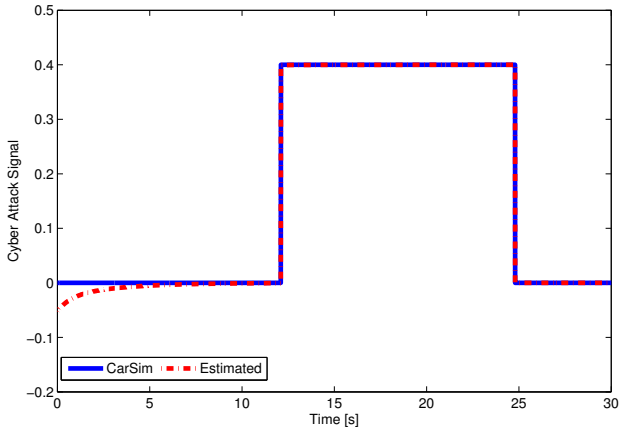

Fig. 6: Scenario 1. Estimation performance of the cyber-attack signal.

states and the unknown cyber-attack signal are able to be accurately achieved with the proposed fuzzy UIO.

C. Scenario 3: Random Cyber-Attack Signal

This scenario is performed with a random high-frequency cyber-attack signal to further emphasize the estimation performance of the proposed UIO without requiring any information about the cyber-attacks. To this end, the leading vehicle with initial velocity stops after a deceleration phase as shown in Fig. 10(a). The initial inter-vehicle distance is 15 [m] and the initial velocity of the self-vehicle is 3 [m/s]. The random attack signal is shown in Fig. 10(b), which is a band-limited white noise signal limited within $[-0.5, 0.5]$, with a sampling step of 0.25 [s] and a noise energy of 0.01. As in two previous test scenarios, Figs. 11 and 12 clearly show that

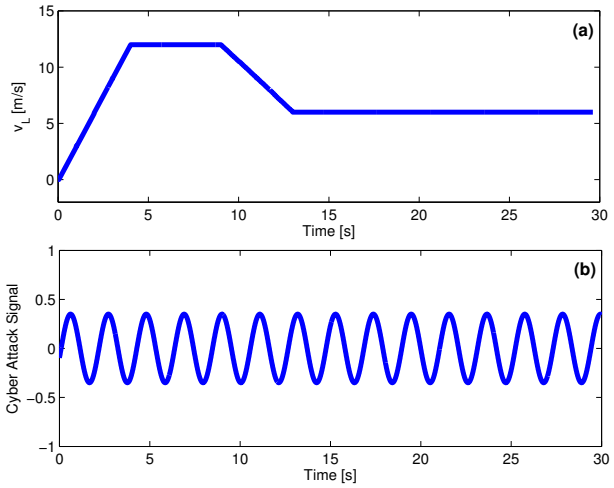

Fig. 7: Scenario 2. (a) Velocity of the leading connected vehicle v_L, (b) Cyber-attack signal.

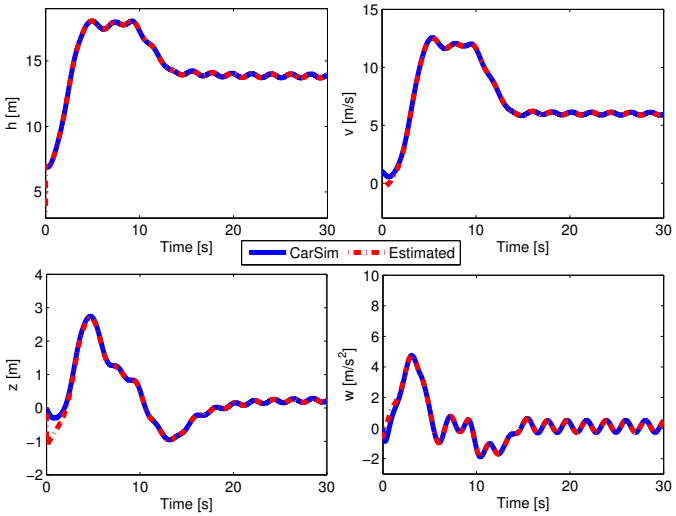

Fig. 8: Scenario 2. Estimation performance of the CVS dynamics.

not only the CVS dynamics but also the high-frequency cyber-attack signal are able to be exactly estimated with the proposed method.

D. Quantitative Performance Analysis

This section provides a quantitative estimation performance analysis for the proposed fuzzy UIO method. To this end, the root mean square deviations (RMSD) and mean absolute errors (MAE) are adopted as estimation performance indicators, which are defined as

$$\zeta_{\text{MAE}} = \frac{1}{T}\int_0^T \left|\zeta(t) - \hat{\zeta}(t)\right| dt$$

$$\zeta_{\text{RMSD}} = \sqrt{\frac{1}{T}\int_0^T \left(\zeta(t) - \hat{\zeta}(t)\right)^2 dt}$$

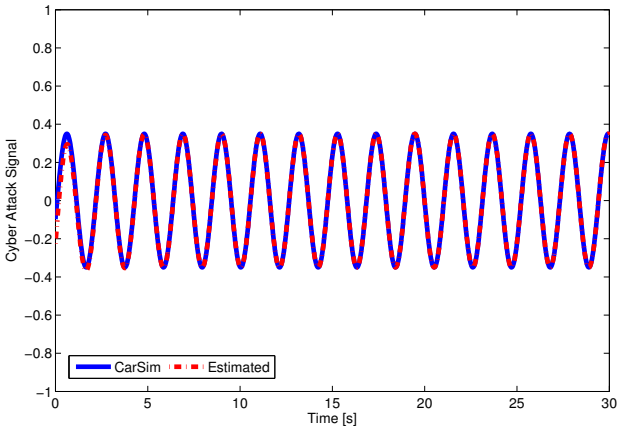

Fig. 9: Scenario 2. Estimation performance of the cyber-attack signal.

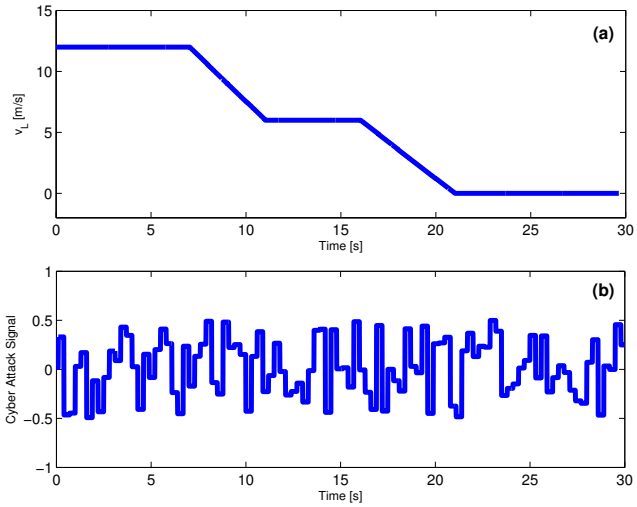

Fig. 10: Scenario 3. (a) Velocity of the leading connected vehicle v_L, (b) Cyber-attack signal.

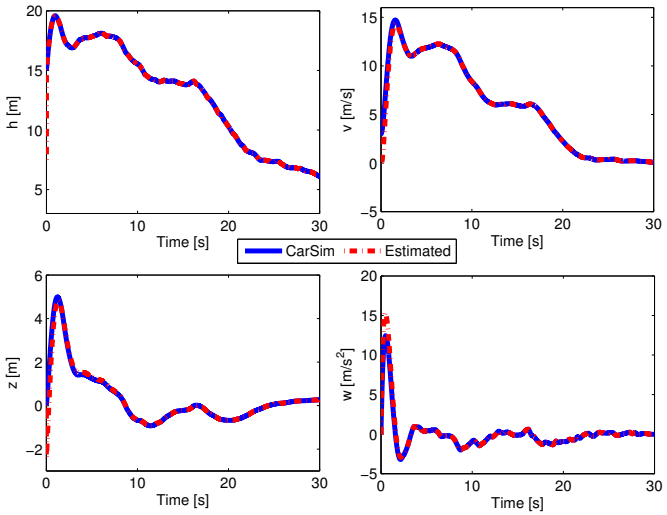

Fig. 11: Scenario 3. Estimation performance of the CVS dynamics.

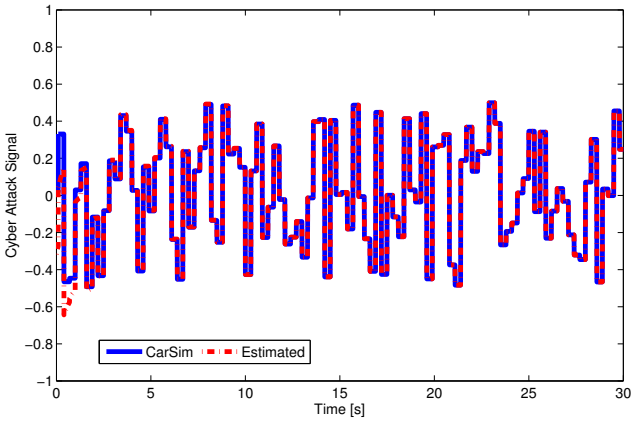

Fig. 12: Scenario 3. Random cyber-attack estimation performance.

where $\zeta(t)$ is the considered estimation variable, $\hat{\zeta}(t)$ is its estimate and T is the test duration time. The results of the performance indicators corresponding to the three above test scenarios are summarized in Table II. Since the error indicators are very small, we can conclude that an accurate estimation performance of both the unmeasured system state and the unknown cyber-attack can be achieved with the proposed TS fuzzy UIO for all considered scenarios.

TABLE II: Estimation Performance Analysis.

Error Indicator	Scenario 1	Scenario 2	Scenario 3
h_{MAE} [m]	0.0018	0.0012	0.0018
v_{MAE} [m/s]	0.0623	0.0384	0.0526
z_{MAE} [m]	0.0408	0.0429	0.0969
w_{MAE} [m/s^2]	0.0735	0.0376	0.0395
f_{MAE} [-]	0.0050	0.0037	0.0062
h_{RMSD} [m]	0.0913	0.0639	0.0913
v_{RMSD} [m/s]	0.2834	0.1543	0.1756
z_{RMSD} [m]	0.1615	0.1413	0.2528
w_{RMSD} [m/s^2]	0.3114	0.1521	0.1478
f_{RMSD} [-]	0.0233	0.0145	0.0189

V. Conclusions

This paper presents a TS fuzzy UIO to simultaneously estimate the states and sensor-actuator cyber-attacks of CVSs. Taking advantage of N-TS fuzzy modeling method, a way of dealing with unmeasured nonlinearities involved in the connected vehicle dynamics is proposed in this paper. Using an augmented system technique together with the well-known differential mean value theorem, an asymptotic convergence is guaranteed for the

estimation of both CVS dynamics and cyber-attacks. In particular, no *a prior* information on cyber-attack signals is required for TS fuzzy UIO design, which allows to deal with the random nature of CVS cyber-attacks. The proposed TS fuzzy UIO design conditions are derived in the form of LMI constraints via Lyapunov stability theory. Illustrated results obtained with Simulink-CarSim are provided to verify the effectiveness of the new UIO-based estimation scheme. Future works focus on designing resilient control for CVSs under multiple cyber-attacks using the proposed TS fuzzy UIO.

ACKNOWLEDGEMENT

This work was supported in part by the Key Research Project of North Minzu University under Grant 2021JCYJ09; in part by the French Ministry of Higher Education and Research, in part by the National Center for Scientific Research (CNRS); in part by the ANR CoCoVeIA project (ANR-19-CE22-0009); in part by the ANR HM-Science project (ANR-21-CE48-0021); in part by the Hauts-de-France Region under the project RITMEA CPER 2021-2027; in part by the National Natural Science Foundation of China under Grant 62163002; in part by the Natural Science Foundation of Ningxia Hui Autonomous Region under Grant 2021AAC05011; in part by the Advanced Intelligent Perception and Control Technology Innovative Team of Ningxia.

CONFLICT OF INTEREST STATEMENT

The authors have no conflicts of interest to declare. All co-authors have seen and agree with the contents of the manuscript and there is no financial interest to report. We certify that the submission is original work and is not under review at any other publication.

REFERENCES

[1] J. Siegel, D. Erb, and S. Sarma, "A survey of the connected vehicle landscape-architectures, enabling technologies, applications, and development areas," *IEEE Trans. Intell. Transp. Syst.*, vol. 19, no. 8, pp. 2391–2406, 2018.

[2] T. Ersal, I. Kolmanovsky, N. Masoud, N. Ozay, J. Scruggs, R. Vasudevan, and G. Orosz, "Connected and automated road vehicles: state of the art and future challenges," *Veh. Syst. Dyn.*, vol. 58, no. 5, pp. 672–704, 2020.

[3] K. Li, J. Wang, and Y. Zheng, "Cooperative formation of autonomous vehicles in mixed traffic flow: Beyond platooning," *IEEE Trans. Intell. Transp. Syst.*, pp. 1–16, 2022.

[4] R. Dollar and A. Vahidi, "Efficient and collision-free anticipative cruise control in randomly mixed strings," *IEEE Trans. Intell. Veh.*, vol. 3, no. 4, pp. 439–452, 2018.

[5] J. Wang, Y. Zheng, C. Chen, Q. Xu, and K. Li, "Leading cruise control in mixed traffic flow: System modeling, controllability, and string stability," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 8, pp. 12 861–12 876, 2022.

[6] G. Orosz, "Connected cruise control: modelling, delay effects, and nonlinear behaviour," *Veh. Syst. Dyn.*, vol. 54, no. 8, pp. 1147–1176, 2016.

[7] Z. Xu and X. Jiao, "Robust control of connected cruise vehicle platoon with uncertain human driving reaction time," *IEEE Trans. Intell. Veh.*, vol. 7, no. 2, pp. 368–376, 2022.

[8] Y.-C. Lin and H. Nguyen, "Adaptive neuro-fuzzy predictor-based control for cooperative adaptive cruise control system," *IEEE Trans. Intell. Transp. Syst.*, vol. 21, no. 3, pp. 1054–1063, 2020.

[9] R. Biroon, Z. 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, 2022.

[10] C. Huang, S. Coskun, J. Wang, P. Mei, and Q. Shi, "Robust $\mathscr{H}_\infty$ dynamic output-feedback control for CACC with ROSSs subject to rodas," *IEEE Trans. Veh. Technol.*, vol. 71, no. 1, pp. 137–147, 2021.

[11] Z. Biron, S. Dey, and P. Pisu, "Real-time detection and estimation of denial of service attack in connected vehicle systems," *IEEE Trans. Intell. Transp. Syst.*, vol. 19, no. 12, pp. 3893–3902, 2018.

[12] W. Jeon, Z. Xie, A. Zemouche, and R. Rajamani, "Simultaneous cyber-attack detection and radar sensor health monitoring in connected acc vehicles," *IEEE Sens. J.*, vol. 21, no. 14, pp. 15 741–15 752, 2021.

[13] G. Comert, M. Rahman, M. Islam, and M. Chowdhury, "Change point models for real-time cyber attack detection in connected vehicle environment," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 8, pp. 12 328–12 342, 2022.

[14] K. Halder, U. Montanaro, S. Dixit, M. Dianati, A. Mouzakitis, and S. Fallah, "Distributed $\mathscr{H}_\infty$ controller design and robustness analysis for vehicle platooning under random packet drop," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 5, pp. 4373–4386, 2022.

[15] S. Xiao, X. Ge, Q.-L. Han, and Y. Zhang, "Secure distributed adaptive platooning control of automated vehicles over vehicular ad-hoc networks under denial-of-service attacks," *IEEE Transactions on Cybernetics*, pp. 1–13, 2021.

[16] Y. Fang, H. Min, X. Wu, W. Wang, X. Zhao, and G. Mao, "On-ramp merging strategies of connected and automated vehicles considering communication delay," *IEEE Trans. Intell. Transp. Syst.*, pp. 1–15, 2022.

[17] S. Dadras, S. Dadras, and C. Winstead, "Identification of the attacker in cyber-physical systems with an application to vehicular platooning in adversarial environment," in *Annual American Control Conference (ACC)*, 2018, pp. 5560–5567.

[18] W. Qin and G. Orosz, "Experimental validation of string stability for connected vehicles subject to information delay," *IEEE Trans. Control Syst. Technol.*, vol. 28, no. 4, pp. 1203–1217, 2020.

[19] Z. Wang, S. Jin, L. Liu, C. Fang, M. Li, and S. Guo, "Design of intelligent connected cruise control with vehicle-to-vehicle communication delays," *IEEE Trans. Veh. Technol.*, vol. 71, no. 8, pp. 9011–9025, 2022.

[20] Z. Wang, Y. Gao, C. Fang, L. Liu, D. Zeng, and M. Dong, "State-estimation-based control strategy design for connected cruise control with delays," *IEEE Sys. J.*, pp. 1–12, 2022.

[21] Y. Xu and G. Guo, "Event triggered control of connected vehicles under multiple cyber attacks," *Inf. Sci.*, vol. 582, pp. 778–796, 2022.

[22] M. Boukhari, A. Chaibet, and M. Boukhnifer, "Proprioceptive sensors fault tolerant control strategy for an autonomous vehicle," *Sensors*, vol. 18, no. 6, p. 1893, 2018.

[23] Z. Abdollahi Biron, S. Dey, and P. Pisu, "Real-time detection and estimation of denial of service attack in connected vehicle

systems," *IEEE Trans. Intell. Transp. Syst.*, vol. 19, no. 12, pp. 3893–3902, 2018.

[24] Z. Ju, H. Zhang, and Y. Tan, "Deception attack detection and estimation for a local vehicle in vehicle platooning based on a modified UFIR estimator," *IEEE Internet of Things J.*, vol. 7, no. 5, pp. 3693–3705, 2020.

[25] E. Mousavinejad, F. Yang, Q.-L. Han, X. Ge, and L. Vlacic, "Distributed cyber attacks detection and recovery mechanism for vehicle platooning," *IEEE Trans. Intell. Transp. Syst.*, vol. 21, no. 9, pp. 3821–3834, 2020.

[26] D. Zhang, C. Lv, T. Yang, and P. Hang, "Cyber-attack detection for autonomous driving using vehicle dynamic state estimation," *Automotive Innovation*, vol. 4, no. 3, pp. 262–273, 2021.

[27] A.-T. Nguyen, T. Taniguchi, L. Eciolaza, V. Campos, R. Palhares, and M. Sugeno, "Fuzzy control systems: Past, present and future," *IEEE Comput. Intell. Mag.*, vol. 14, no. 1, pp. 56–68, Feb. 2019.

[28] P. Coutinho, R. Araujo, A.-T. Nguyen, and R. Palhares, "A multiple-parameterization approach for local stabilization of constrained Takagi-Sugeno fuzzy systems with nonlinear consequents," *Inf. Sci.*, vol. 506, pp. 295–307, 2020.

[29] J. Pan, A.-T. Nguyen, T.-M. Guerra, and D. Ichalal, "A unified framework for asymptotic observer design of fuzzy systems with unmeasurable premise variables," *IEEE Trans. Fuzzy Syst.*, vol. 29, no. 10, pp. 2938–2948, 2021.

[30] Q. Jia, W. Chen, Y. Zhang, and H. Li, "Fault reconstruction and fault-tolerant control via learning observers in Takagi-Sugeno fuzzy descriptor systems with time delays," *IEEE Trans. Indus. Electron.*, vol. 62, no. 6, pp. 3885–3895, 2015.

[31] Q. Luo, A.-T. Nguyen, J. Fleming, and H. Zhang, "Unknown input observer based approach for distributed tube-based model predictive control of heterogeneous vehicle platoons," *IEEE Trans. Veh. Technol.*, vol. 70, no. 4, pp. 2930–2944, 2021.

[32] Z. Lendek, T. M. Guerra, and B. De Schutter, *Stability Analysis and Nonlinear Observer Design Using Takagi-Sugeno Fuzzy Models*. Springer Berlin Heidelberg, 2011, vol. 262.

[33] B. Zhang, H. Du, J. Lam, N. Zhang, and W. Li, "A novel observer design for simultaneous estimation of vehicle steering angle and sideslip angle," *IEEE Trans. Indus. Electron.*, vol. 63, no. 7, pp. 4357–4366, July 2016.

[34] A.-T. Nguyen, T. Q. Dinh, T.-M. Guerra, and J. Pan, "Takagi-Sugeno fuzzy unknown input observers to estimate nonlinear dynamics of autonomous ground vehicles: Theory and real-time verification," *IEEE/ASME Trans. Mechatron.*, vol. 26, no. 3, pp. 1328–1338, 2021.

[35] A. Zemouche, M. Boutayeb, and I. Bara, "Observers for a class of Lipschitz systems with extension to $\mathscr{H}_\infty$ performance analysis," *Syst. Control Lett.*, vol. 57, no. 1, pp. 18–27, 2008.

[36] H.-D. Tuan, P. Apkarian, T. Narikiyo, and Y. Yamamoto, "Parameterized linear matrix inequality techniques in fuzzy control system design," *IEEE Trans. Fuzzy Syst.*, vol. 9, no. 2, pp. 324–332, 2001.

[37] J. Löfberg, "Yalmip: A toolbox for modeling and optimization in Matlab," in *IEEE Int. Symp. Comput. Aided Control Syst. Des.*, Taipei, Sept. 2004, pp. 284–289.