Préparée à Université de Lorraine

Development of new advanced estimation algorithms for improving the resilience of the autonomous and connected vehicle

Soutenue par
Quang Huy NGUYEN
Le xx mois 202x

École doctorale n°xxx
Titre de l'école doctorale

Spécialité
Automatique

Préparée au
Centre de Recherche Nancy

Composition du jury :

Prénom NOM 1 Affiliation	*Président du jury* *Examinateur*
Prenom NOM 2 Affiliation	*Rapporteur*
Prenom NOM 3 Affiliation	*Rapporteur*
Prenom NOM 4 Affiliation	*Rapporteur*
Prenom NOM 5 Affiliation	*Rapporteur*
Prenom NOM 6 DR Affiliation	*Directeur de thèse*

UNIVERSITÉ DE LORRAINE

Remerciements

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

Résumé

Mots clés : Estimation, mot clé 2, mot clé 3, mot clé 4

Abstract

The reliability and safety of Connected and Autonomous Vehicles (CAVs) rely heavily on the real-time availability of precise dynamic variables. However, equipping vehicles with high-end sensors to measure every necessary variable—such as sideslip angles or vehicle trajectories—is often economically unfeasible or physically impossible. Furthermore, CAVs are increasingly vulnerable to sensor faults and cyber-attacks targeting inter-vehicle communications (V2V/V2I), which can lead to critical failures. To address these challenges without incurring the high cost of physical hardware redundancy, this thesis proposes the development of an embedded electronic board functioning as a resilient "soft sensor" based on analytical redundancy.

The research adopts a hybrid modeling methodology that integrates physical differential equations with online learning-based neuro-adaptive neural networks. This approach allows for the accurate representation of complex, time-varying parameters and unknown inputs within the vehicle's dynamics. Based on these models, advanced nonlinear estimation algorithms—specifically Unknown Input Observers (UIO) and neuro-adaptive observers—are developed to reconstruct missing state variables and ensure system resilience against data loss and malicious signal injection.

The proposed estimation strategies are applied to two primary control challenges:

— Resilience to Cyber-Attacks in Adaptive Cruise Control (ACC): The thesis investigates specific architectures for detecting and mitigating cyber-attacks, such as Denial of Service (DoS) and False Data Injection (FDI), within autonomous and cooperative ACC systems.

— Vehicle Tracking and Platooning: Novel estimation algorithms are proposed to handle the nonlinear dynamics and unknown forces inherent in tracking surrounding vehicles, which is essential for decision-making in maneuvers like lane changes and platooning.

The final contribution of this work is the design and fabrication of a prototype embedded electronic board. This hardware integrates the developed algorithms, validating the theoretical contributions and demonstrating a cost-effective, scalable solution for enhancing the autonomy, security, and fault tolerance of next-generation vehicles.

Keywords : State Estimation, keyword 2, keyword 3, keyword 4

Table des matières

Liste des figures

Liste des tableaux

Chapitre 1

Resilient State Estimation and Cyber-Attack Reconstruction for Connected Autonomous Vehicles

Objectifs

The primary objective of this work is to develop a resilient controller and state observers capable of:
Estimating unmeasured quantities necessary for the SA-ACC.
Detecting and reconstructing false data injected into the communication channel exactly and in finite time.
Compensating for these attack signals to maintain vehicle autonomy.

Sommaire

1 Introduction and Problem Statement

1.1 Context

The advent of autonomous and connected vehicles (CAVs) represents the future of mobility, leveraging advanced technologies such as artificial intelligence to ensure automated driving. These systems promise increased safety, improved energy efficiency, and a comfortable driving experience by utilizing Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communication. However, the reliability and availability of sensors constitute critical challenges that hinder the full development of these vehicles.

1.2 The Cyber-Security Challenge

A specific vulnerability in CAVs is the susceptibility of the communication channels to cyber-attacks. The VEHALSECU project specifically addresses the problem of estimating necessary variables for a Semi-Autonomous Adaptive Cruise Control (SA-ACC) system when communication is corrupted by cyber-attacks. Specifically, False Data Injection (FDI) attacks can bypass conventional security measures, allowing attackers to compromise sensor measurements and disrupt network operations.

While machine learning techniques have been proposed for detection, they are often computationally expensive and unsuitable for the real-time constraints of embedded vehicle control. Furthermore, existing research often assumes attack signals are constant, which limits the scope of protection against time-varying or arbitrary unbounded attacks.

2 Design of Resilient Observers

The core scientific challenge lies in the "Unknown Input Observer" (UIO) design. Standard UIOs require two mathematical conditions: strong detectability and a specific rank condition on the system matrices18181818. While the SA-ACC model satisfies the detectability condition 19, it fails the rank condition ($rank(CW) \neq rank(W)$)20. Consequently, standard UIOs cannot be directly applied.To overcome this, two distinct methodological approaches were developed: a discrete-time approach using delayed observations and a continuous-time approach using sliding mode differentiation.

2.1 CACC modeling subject to cyberattack

Basically, the dynamics of i^{th} vehicle are a Position-Velocity-Acceleration third-order linear model given by the following set of equations:

$$\begin{cases} \dot{p}_i(t) = v_i(t) \\ \dot{v}_i(t) = a_i(t) \\ \dot{a}_i(t) = \frac{1}{\tau_i} u_i(t) - \frac{1}{\tau_i} a_i(t) \end{cases} \tag{1.1}$$

where

— $p_i(t), v_i(t)$ and $a_i(t)$ denote the position, velocity and acceleration of the i^{th} vehicle, respectively;

— $u_i(t)$ is the i^{th} vehicle control input representing the desired driving/braking force or acceleration;

— τ is the engine's constant time lag.

The actual spacing between vehicles are $\varepsilon_{i,act} = p_{i-1} - p_i$ and the desired spacing between vehicles in the constant time-gap spacing policy is given by $\varepsilon_{i,des} = L + hv_i$. It follows that the spacing error can be written as:

$$\varepsilon_{i,des} - \varepsilon_{i,act} \triangleq p_i - p_{i-1} + L + hv_i = \varepsilon_i + hv_i, \tag{1.2}$$

where L is the minimum safety distance and h is the time-gap. Then, the controller u_{i} is given by [Rajamani, 2002] :

$$u_{\mathrm{i}} = -k_1 a_{i-1} + (k_1 + hk_1k_2)a_i - \frac{1}{h}(1 - hk_1k_2)\dot{\varepsilon}_i - \frac{k_2}{h}\varepsilon_i - k_2 v_i \tag{1.3}$$

where a_{i-1} is the acceleration of the preceding vehicle obtained by using inter-vehicle communication. The scalar gains k_1 and k_2 are the controller design parameters to be designed according to the detailed procedure introduced in [Rajamani, 2002].

The controller u_{i} defined in (1.3) is convenient in perfect situation where the acceleration of the preceding vehicle, a_{i-1}, provided through V2V communication channel is not corrupted by intruders. Unfortunately, in CACC platoons, the V2V communication may provide unreliable acceleration due to potential tampering by attackers. To develop a resilient controller to cyberattacks, we have to consider the attack signal in the design of the controller. To this purpose, we assume that the following vehicle receives the signal $\mu(t)$ corrupted by injected false data in the wireless communication channel:

$$\mu(t) = a_{i-1}(t) + f^c(t) \tag{1.4}$$

where $a_{i-1}(t)$ is the true acceleration and $f^c(t)$ is the additive cyberattack signal. This cyberattack scheme under additive false signals can cover several cyberattack architectures. These may include message falsification attacks, spoofing attacks, and denial of service (DoS) attacks. For instance, in the DoS case, by using the differential mean value theorem, there exists $\theta_t \in [t - \tau(t),\ t]$ such that the delayed signal $a_{i-1}(t - \tau(t))$ can be represented as follows:

$$\begin{aligned}\mu(t) = a_{i-1}(t - \tau(t)) &= a_{i-1}(t) \underbrace{-\frac{\mathrm{d}a_{i-1}}{\mathrm{d}t}(\theta_t)\tau(t)}_{f^c} \\ &= a_{i-1}(t) + f^c.\end{aligned} \tag{1.5}$$

Under a cyberattack, the following vehicle receives μ and will utilize it in its controller. Then, instead of (1.3), the controller u_{i} will be implemented as follows:

$$\begin{aligned} u_{\mathrm{i}} = & -k_1\mu(t) + (k_1 + hk_1k_2)a_i \\ & - \frac{1}{h}(1 - hk_1k_2)\dot{\varepsilon}_i - \frac{k_2}{h}\varepsilon_i - k_2v_i. \end{aligned} \tag{1.6}$$

As shown in Figure **??**, the radar-measured rear-to-bumper distance is defined as follows:

$$\delta_i = p_{i-1} - p_i - l_{i-1}, \tag{1.7}$$

Then, taking the time derivative of δ_i results in:

$$\dot{\delta}_i = v_{i-1} - v_i, \ddot{\delta}_i = a_{i-1} - a_i, \dddot{\delta}_i = \dot{a}_{i-1} - \dot{a}_i \tag{1.8}$$

where $\dot{\delta}_i$, $\ddot{\delta}_i$, and $\dddot{\delta}_i$ are the relative speed, acceleration, and jerk (rate of acceleration changes) between two adjacency vehicle. By using (1.7) and (1.8), the controller (1.6) becomes

$$\begin{aligned} u_{\mathrm{i}} = & \left(hk_1k_2\right)\mu - \left(k_1 + hk_1k_2\right)f^c - k_2v_i - \frac{k_2}{h}\left(L - l_{i-1}\right) \\ & - \left(k_1 + hk_1k_2\right)\ddot{\delta}_i + \frac{1}{h}\left(1 - hk_1k_2\right)\dot{\delta}_i + \frac{k_2}{h}\delta_i. \end{aligned} \tag{1.9}$$

We obtain acceleration information of the preceding vehicle directly through wireless communication. As a result, we assume the jerk of the preceding vehicle to be zero, without considering its lower-order dynamics.

$$\dot{a}_{i-1} = 0 \tag{1.10}$$

Substituting equation (1.9) into (1.1) and using (1.10) and the notation $x = \begin{bmatrix}\delta_i & \dot{\delta}_i & \ddot{\delta}_i\end{bmatrix}^\top$, we obtain the model expressed under the following condensed matrix form:

$$\begin{cases} \dot{x} = Ax + Bv_i + F\mu + \Delta - Wf^c \\ y = Cx \end{cases} \tag{1.11}$$

with

$$A = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ \frac{-k_2}{\tau h} & \frac{-k_3}{\tau h} & \frac{(k_1-k_3)}{\tau} \end{bmatrix}, B = \begin{bmatrix} 0 \\ 0 \\ \frac{k_2}{\tau} \end{bmatrix}, F = \begin{bmatrix} 0 \\ 0 \\ \frac{k_3}{\tau} \end{bmatrix},$$

$$\Delta = \begin{bmatrix} 0 \\ 0 \\ \frac{k_2(L-l_{i-1})}{\tau h} \end{bmatrix}, W = \begin{bmatrix} 0 \\ 0 \\ \frac{k_3-k_1}{\tau} \end{bmatrix}, C = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$$

where $k_3 \triangleq 1 - hk_1k_2$.

Notice that to avoid cumbersome equations, the interaction between two cars in the CACC scenario is represented without the subscripts i and $i-1$. These are deleted from the matrices A, B, F, Δ, W, and C and from the vectors x, y and f_c. Only v_i is kept to avoid confusion with

the previous equations.

2.2 Problem formulation and objectives

The main objective in the CACC control problem consists in estimating the false data, f^c, and compensating it in the controller u_{i}. The natural solution is the use of the well-known UIO technique to estimate simultaneously the state x and the false data f^c as an unknown input. To this end, it is well-known in the literature [Chaouche, 2022; Trinh, 2011] that a necessary rank condition is required, namely $\text{rank}(CW) = \text{rank}(W)$. Unfortunately, in the case of the CACC with the matrices given in (1.11) such a rank constraint is not satisfied since we have $\text{rank}(CW) = 0$ and $\text{rank}(W) = 1$. To overcome the fall in rank condition, we need additional information, namely the relative acceleration. This information is typically obtained using a real-time differentiator whose role is to estimate online the derivative of relative velocity. Indeed, since $CB = CF = C\Delta = CW = 0$, then with the derivative of y as a pseudo-measurement, i.e. :

$$\bar{y} \triangleq \dot{y} = CAx = \bar{C}x \tag{1.12}$$

we can construct a UIO to estimate x and f^c since $\text{rank}(\bar{C}W) = \text{rank}(W) = 1$. Of course, some additional conditions are required to ensure an exponential UIO.

There are numerical differentiators in the literature allowing the online calculation of the derivative of a given signal, such as the famous sliding mode observer [Zhu, 2012], and the high-gain observer [Dabroom, 1997]. However, these numerical differentiators fail in some situations, namely in the presence of sensor noises. An alternative solution to avoid real-time estimation of the derivative of y consists in investigating the problem by using the discrete-time version of the model, as shown in Figure 1.1 which considers additive sensor noise ω.

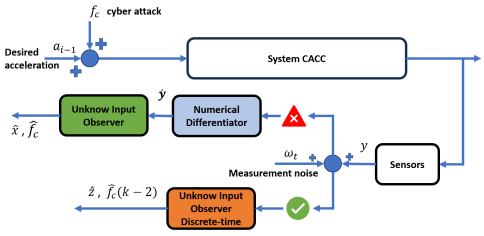

FIGURE 1.1 – Discrete-time model-based UIO.

Indeed, in discrete time, there is no differentiation since the measured signal is a sequence of numbers. The discrete-time version of equation (1.11) is given as follows:

$$\begin{cases} x_{k+1} = \mathcal{A}x_k + \mathcal{B}v_{i,k} + \mathcal{F}\mu_k + \bar{\Delta} - \mathcal{W}f_k^c \\ y_k = Cx_k \end{cases} \tag{1.13}$$

where

$$\mathcal{A} = (\mathbb{I}_3 + TA),\ \mathcal{B} = TB,$$

$$\mathcal{F} = TF,\ \mathcal{W} = TW,\ \bar{\Delta} = T\Delta,$$

and T being the sampling time. In such case, we need to shift the output equation backward using the state equation in discrete-time (1.28) such that the output y_k is expressed as a function of delayed state $x_{k-\tau}$ where τ is the smallest positive integer that allows the necessary rank condition to be held. In the next section, we follow this strategy and develop a discrete-time model-based UIO for the studied CACC system to estimate the cyberattack false signal f^c.

3 Discrete-Time Model-Based UIO design for CACC system

This section is devoted to the development of a new unknown input observer based on the discrete-time model (1.28). By introducing the variables

$$z_t \triangleq x_{k-1} \text{ and } \bar{y}_t \triangleq y_{k-1} \tag{1.14}$$

with $t = k-1$ and considering additive vector noises, ω_t, in both the output measurements and in the process equation, we obtain the following new system

$$\begin{cases} z_{t+1} = \mathcal{A}z_t + \mathcal{B}v_{i,t} + \mathcal{F}\mu_t \\ \qquad\quad +\bar{\Delta} - \mathcal{W}f_t^c + E_\omega\omega_t \\ \bar{y}_t = \mathcal{C}z_t + D_\omega\omega_t \end{cases} \tag{1.15}$$

for which the rank condition is satisfied, i.e.:

$$\text{rank}(\mathcal{C}\mathcal{W}) = \text{rank}(\mathcal{W}) = 1. \tag{1.16}$$

3.1 UIO structure for the shifted system

By using an UIO corresponding to the shifted system (1.15), we will estimate simultaneously z_t and f_{t-1}^c. By using the notation

$$\xi_t \triangleq \begin{bmatrix} z_t \\ f_{t-1}^c \end{bmatrix},$$

$$\mathbb{E} = \begin{bmatrix} \mathbb{I}_3 & \mathcal{W} \end{bmatrix},\ A_\xi = \begin{bmatrix} \mathcal{A} & 0 \end{bmatrix},\ C_\xi = \begin{bmatrix} \mathcal{C} & 0 \end{bmatrix}$$

the system (1.15) is written under the following descriptor form:

$$\begin{cases} \mathbb{E}\xi_{t+1} = A_\xi\xi_t + \mathcal{B}v_t + \mathcal{F}\mu_t + \Delta + E_\omega\omega_t \\ \bar{y}_t = C_\xi\xi_t + D_\omega\omega_t. \end{cases} \tag{1.17}$$

From (1.16), we have

$$\text{rank}\left(\begin{bmatrix} \mathbb{E} \\ C_\xi \end{bmatrix}\right) = n + \text{rank}(\mathcal{C}\mathcal{W}) = n + 1.$$

Now, let P_z and Q_z be two matrices of appropriate dimensions such that

$$\begin{bmatrix} P_z & Q_z \end{bmatrix} = \left(\begin{bmatrix} \mathbb{E} \\ C_\xi \end{bmatrix}^\top \begin{bmatrix} \mathbb{E} \\ C_\xi \end{bmatrix} \right)^{-1} \begin{bmatrix} \mathbb{E} \\ C_\xi \end{bmatrix}^\top. \tag{1.18}$$

It follows that

$$P_z\mathbb{E} + Q_z C_\xi = \mathbb{I}_p \tag{1.19}$$

where p is the number of output measurements.

By considering the following two-stage observer

$$\begin{cases} \kappa_{t+1} = \Big(P_z A_\xi - K C_\xi\Big)\kappa_t + P_z \mathcal{B} v_{i,t} \\ \qquad\quad + \Big[\Big(P_z A_\xi - K C_\xi\Big) Q_z + K\Big]\, \bar{y}_t \\ \qquad\quad + P_z \mathcal{F} \mu_t + P_z \Delta \\ \hat{\xi}_t = \kappa_t + Q_z \bar{y}_t \end{cases} \tag{1.20}$$

the estimation error $\tilde{\xi}_t = \hat{\xi}_t - \xi_t$ satisfies the equation:

$$\begin{aligned} \tilde{\xi}_{t+1} = &\Big(P_z A_\xi - K C_\xi\Big)\tilde{\xi}_t \\ &+ \Big[\Big(K D_\omega - P_z E_\omega\Big) \quad Q_z D_\omega\Big]\, \bar{\omega}_t, \end{aligned} \tag{1.21}$$

where $\bar{\omega}_t$ is defined as follows:

$$\bar{\omega}_t \triangleq \begin{bmatrix} \omega_t^\top & \omega_{t+1}^\top \end{bmatrix}^\top. \tag{1.22}$$

Remark 1. *The central focus of this paper does not lie in the details of designing controller parameters k_1 and k_2. Rather, our attention is directed towards the development of a novel cyberattack detection algorithm. It is crucial to note that in the proposed methodology, we make an assumption that the control design phase, specifically ensuring the string stability of the controller (1.3), is considered as a distinct and independent process from the estimation design procedure outlined in this paper. As demonstrated in [Rajamani, 2002], the controller (1.3) achieves string stability under specific conditions. This stability depends on the transfer function $H(s) = \frac{\bar{\varepsilon}_i}{\bar{\varepsilon}_{i-1}}$, where $\bar{\varepsilon}_i$ is defined in (1.2), satisfying the inequality $|H(j\omega)| \leq 1$. Detailed analysis in [Rajamani, 2002] reveals that such a condition is met when two critical parameters adhere to certain criteria. Specifically, the condition holds when $-k_1 h > \tau$ and $k_2 > 0$, as meticulously explained in the calculations provided in [Rajamani, 2002, Eqs.(32)-(34)].*

3.2 LMI-Baed ISS design method

The objective consists in determining the observer gain K such that the estimation error $\tilde{\xi}_t$ is exponentially robust with respect to the bounded disturbance ω_t. The next theorem provides sufficient conditions expressed in terms of LMIs ensuring the robust exponential stability of $\tilde{\xi}_t$. For the sake of brevity, we put $\mathcal{A}_z \triangleq P_z A_\xi$, $\mathcal{D}_z \triangleq Q_z D_\omega$, and $\mathcal{E}_z \triangleq P_z E_\omega$.

Theorem 1. *Assume there exist two symmetric and positive definite matrices $\mathcal{P}$ and $\mathcal{S}$, a matrix*

$\mathcal{Z}$ of appropriate dimension, and a scalar α, with $\alpha \in]0,1[$, such that the following LMI condition holds:

$$\begin{bmatrix} -\alpha\mathcal{P} & 0 & \mathcal{A}_z^\top \mathcal{P} - C_\xi^\top \mathcal{Z} \\ (\star) & -\mathcal{S} & \begin{bmatrix} D_\omega^\top \mathcal{Z} - \mathcal{E}_z^\top \mathcal{P} \\ \mathcal{D}_z^\top \mathcal{P} \end{bmatrix} \\ (\star) & (\star) & -\mathcal{P} \end{bmatrix} < 0 \tag{1.23}$$

Then the estimation error $\tilde{\xi}_k$, with $K = \mathcal{P}^{-1}\mathcal{Z}^\top$, satisfies the following exponential Input-to-State Stable (ISS) bound:

$$\boxed{\begin{aligned} \left\|\tilde{\xi}_t\right\| \leq \sqrt{\frac{\lambda_{\max}(\mathcal{P})}{\lambda_{\min}(\mathcal{P})}} \left\|\tilde{\xi}_0\right\| \alpha^{\frac{t}{2}} \\ + \sqrt{\frac{\lambda_{\max}(\mathcal{S})}{(1-\alpha)\lambda_{\min}(\mathcal{P})}} \max_{0\leq k\leq t} \|\bar{\omega}_k\| . \end{aligned}} \tag{1.24}$$

Démonstration. The proof is based on the Lyapunov function $\vartheta_t \triangleq \tilde{\xi}_t^\top \mathcal{P} \tilde{\xi}_t$. By expanding the expression of ϑ_{t+1} along the trajectories of (1.21), we can deduce easily that under the LMI condition (1.23), we have

$$\vartheta_{t+1} - \alpha\vartheta_t \leq \bar{\omega}_t^\top \mathcal{S} \bar{\omega}_t.$$

Hence, by induction technique and backward substitution, we deduce that

$$\vartheta_t \leq \vartheta_0 \alpha^t + \frac{\lambda_{\max}(\mathcal{S})}{1-\alpha} \max_{0\leq k\leq t} \|\bar{\omega}_k\|^2 .$$

Consequently, we can conclude by using the double inequality

$$\lambda_{\min}(\mathcal{P}) \left\|\tilde{\xi}_t\right\|^2 \leq \vartheta_t \leq \lambda_{\max}(\mathcal{P}) \left\|\tilde{\xi}_t\right\|^2 .$$

□

3.3 Defense strategy

The key idea consists of developing a Resilient, Robust, and Reliable CACC (3ℝ−CACC) controller able to cope with cyberattacks, external disturbances, and data loss. The 3ℝ−CACC defense mechanism is as depicted in Figure 1.2. As soon as an attack or a significant external disturbance is detected, the CACC controller (1.3) will switch to the ACC controller to forget the false data in communication data.

$$u_{\mathrm{i}} = -\frac{1}{h}(v_i - v_{i-1} + \lambda\bar{\epsilon}_i) \tag{1.25}$$

with the condition $h > 2\tau$ and $\lambda > 0$ in order to ensure the string stability. After implementing the controller (1.25), the system no longer remains the same as (1.28). Therefore, we need to transform the controller (1.25) in terms of x and rewrite a new system similar to (1.28). This enables the system to detect cyberattacks, which will be treated as unknown inputs.

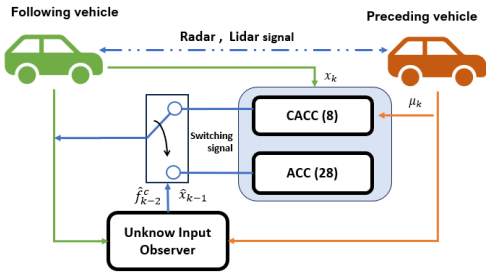

FIGURE 1.2 – Resilient control for CACC system.

Remark 2. *The LMI conditions (1.23) correspond to the system without uncertainties, which guarantee certain robustness with respect to the parameter uncertainties in the sense of the exponential ISS criterion (1.24). Indeed, with the proposed method, if we have uncertainties, i.e.: $A + \delta A$ and $C + \delta C$ instead of A and C, for instance, we can add $\delta A x(t)$ and $\delta C x(t)$ in the disturbance vector ω and then the LMIs ensure the exponential ISS bound with respect to the new vector of disturbances, ω, containing the parameter uncertainties. However, such a technique does not ensure exponential convergence of the estimation and tracking errors to zero in the free-disturbance case (with the initial vector of disturbances without including the uncertain parameters), and the boundedness of δA and δC does not imply necessarily the boundedness of $\delta A x(t)$ and $\delta C x(t)$. To overcome this issue, we need to develop an extended LMI condition that consider both the structure and magnitude of uncertainties.*

4 Simulation results by Using Matlab and Carla Platform

We demonstrate the effectiveness of the proposed observer by conducting MATLAB and CARLA simulations with two cyberattack scenarios. The parameters of the CACC system and its controller are given in Table 1.1.

Parameter	τ	L	l_i	h	k_1	k_2	t_s
Value	0.4	7.3	5	0.5	-0.8	2.5	0.01
Unit	s	m	m	s	-	-	-

TABLE 1.1 – Parameters of CACC system and the controller gains.

It is assumed that two vehicles are driving longitudinally on the road, and each vehicle is equipped with a cruise control system. The preceding vehicle should pursue the following desired trajectory: $a_{i-1}(t) = 3\sin(\frac{2\pi}{10})t$. The two simulation scenarios of cyberattacks explored here are outlined below:

Case 1: *Sparse attack, DoS, packet-loss:*

$$f^c(t) = \begin{cases} X(t) & 6 \leq t < 8 \\ a_{i-1}(t) & 10 \leq t < 15 \\ 0 & \text{otherwise} \end{cases} \tag{1.26}$$

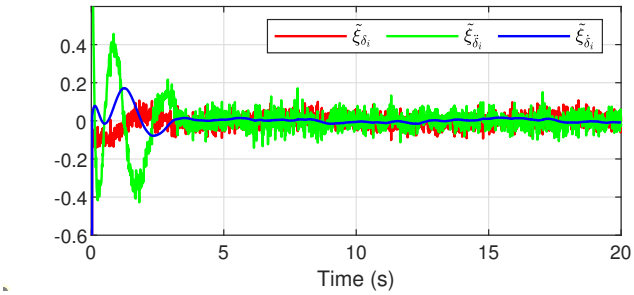

FIGURE 1.3 – State estimation case 1.

Case 2: *False data injected :*

$$f^c(t) = \begin{cases} -5 & 6 \leq t < 8 \\ 2(t-4) & 10 \leq t < 15 \\ 0 & \text{otherwise} \end{cases} \tag{1.27}$$

where $X(t) \sim U(-5, 5)$ is a random variable following a uniform distribution, with probability $P(X(t)) = 0.2$.

4.1 Simulation result using Matlab

By solving the LMI condition (1.23), we obtain the observer gain K given by:

$$K = \begin{bmatrix} 0.5000 & -0.005 & 0.0498 & -8.9295 \\ -0.005 & 1.000 & -99.9950 & 1427.22 \end{bmatrix}^\top.$$

The proposed observer is designed to estimate the state vector, including relative position, relative velocity, and relative acceleration, as well as provide an accurate estimation of any cyberattacks even in the presence of a Gaussian noise $\omega_t = \mathcal{N}(0.02^2[m])$ for both system and measurement. For both attack scenarios, we set the initial conditions of the actual system as $\xi_0 = \begin{bmatrix} 5 & 10 & 0 & 0 \end{bmatrix}^\top$, while the initial state of the observer is set to $\hat{\xi}_0 = \begin{bmatrix} 0 & 0 & 0 & 0 \end{bmatrix}^\top$.

Simulation results for the first scenario of cyberattack (1.26) are presented in Figure 1.3 and Figure 1.4. In Figure 1.3, we can see the error of the relative position, relative velocity, and relative acceleration along with their estimates. The observer demonstrates similar good performance in accurately reconstructing a random cyberattack and packet-loss, as depicted in Figure 1.4. As we can see, the estimated delay attack is exactly 2 steps.

For the second case of time-varying and bounded attack signal (1.27), it can be observed from the Figure 1.5 that the cyberattack signal is accurately estimated, and the estimation error is bound.

We can see that the proposed observer can estimate the the full state with good accuracy, while the unknown input is reconstructed with a fixed delay of two units based on the available output measurements.

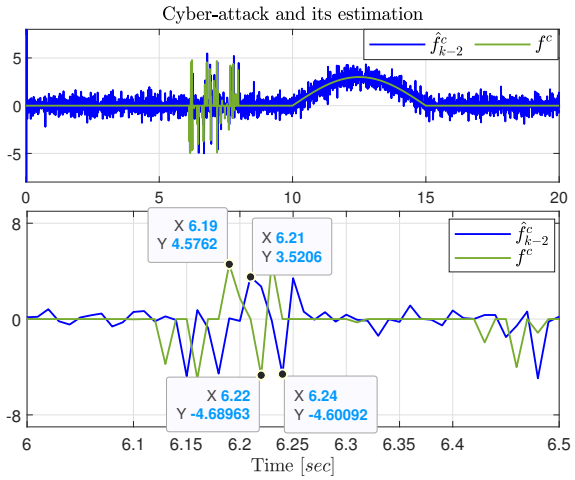

FIGURE 1.4 – Attack estimation using UIO case 1.

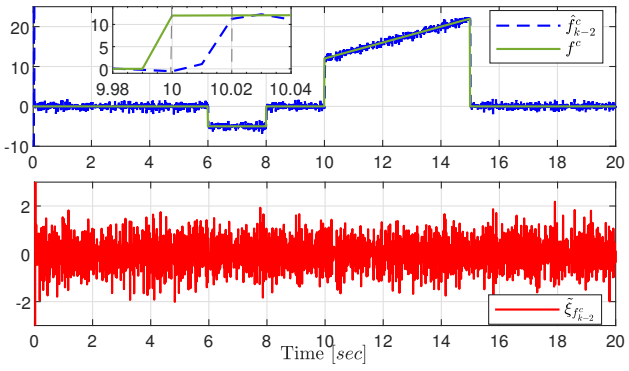

FIGURE 1.5 – Attack estimation and the errors case 2.

4.2 Simulation result using Carla

To evaluate the system under more realistic conditions, we conducted simulations within the CARLA simulator. Specifically, we simulated a scenario where a leading vehicle utilized a PID controller for cruise control, aiming to maintain a velocity of $10m/s$. We kept the parameters consistent with those listed in Table 1.1 and adopted a time step of $t_s = 0.04$. We also implemented a deterministic attack signal that varies over time and is defined by equation (1.27). As depicted in Fig 1.7, the error state vectors for relative position and relative velocity exhibit good tracking, but the third vector $\tilde{\xi}_a$ falls short of perfection. This is because the acceleration of the preceding vehicle in Fig 1.8 sent to the network is inconsistent, which affects the attack estimation performance. Fig 1.8 illustrates the observer taking at least 5 seconds to converge to the actual state, and the estimated value being influenced by noise and imperfection of the model. However, the leading vehicle retains its ability to detect the cyberattack signal, ensuring a safe distance effectively. A video showcasing the simulation scenario is provided in GitHub repository. Fig. 1.6 displays a thumbnail from the video.

FIGURE 1.6 – Carla Simulator platform (GitHub repository).

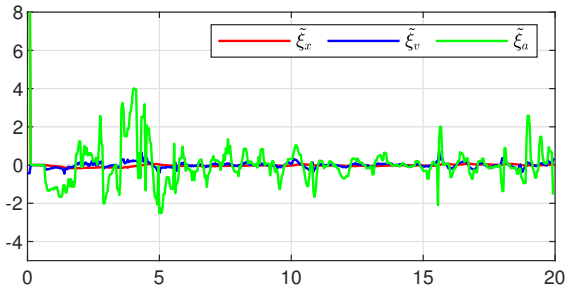

FIGURE 1.7 – State estimation using CARLA under attack case 2.

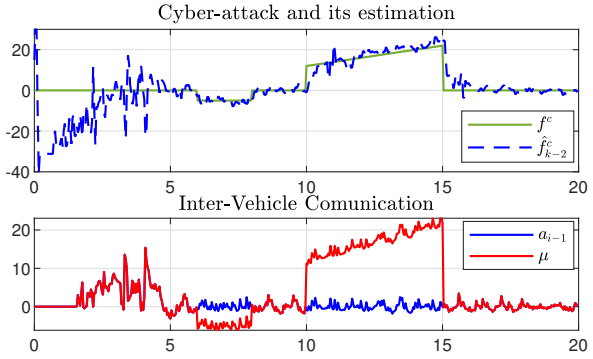

FIGURE 1.8 – Cyberattack signal and inter-vehicle communication case 2.

5 Conclusion

In this paper, we proposed a novel UIO design technique ensuring a theoretical ISS bound on the cyberattack detection error in the context of the CACC system. To guarantee such an ISS bound, a new LMI condition is proposed. The key idea consists in shifting the original output measurement to satisfy the well-known matching condition. The theoretical result is validated through two simulation scenarios of cyberattacks by using the Matlab software and the Carla simulator.

Our future endeavors will focus on exploring the challenge in the presence of model parameter uncertainties. This will entail designing a robust observer-based controller, necessitating simultaneous synthesis of the observer and controller gains by addressing a unified LMI condition.

6 Exact discretization

To overcome the above limitation, we propose discretizing the system. Previous studies [**nguyen2020cyberattack**] have applied state discretization with a delay that satisfies the necessary rank condition. This approach represents an alternative solution to the rank condition problem. However, the introduction of delays can affect control system performance and stability, leading to reduced responsiveness and complicating the design of the observer and controller, especially in the presence of measurement noise. To address these challenges, we propose the use of an exact discretization method, as suggested in the literature [**M.Zhang**] allowing us to estimate both the state and cyberattacks using an UIO. Additionally, we will introduce conditions to ensure the exponential convergence of the estimation error, which will be discussed in the next section.

Figure fig. 1.9 illustrates the structure of the proposed observer-based cyberattack estimation framework.

The discrete-time version of equation is presented as follows, according to the approach detailed in reference [**M.Zhang**] :

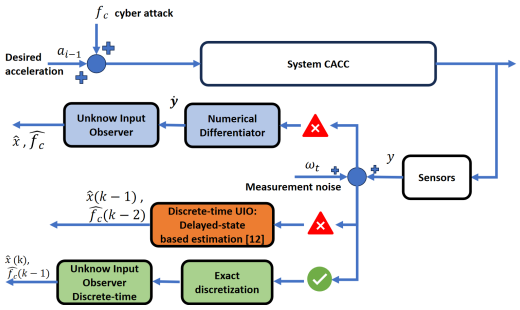

FIGURE 1.9 – Discrete-time model-based UIO

$$\begin{cases} x_{k+1} = A_d x_k + B_d v_{i,k} + F_d \mu_k + \hat{\Delta} - W_d f_k^c \\ y_k = C_d x_k \end{cases} \tag{1.28}$$

where

$$A_d = e^{A_c T_s},\ B_d = \int_0^{T_s} e^{A_c \eta} B_c d\eta,\ C_d = C_c$$

$$F_d = \int_0^{T_s} e^{A_c \eta} F_c d\eta,\ W_d = \int_0^{T_s} e^{A_c \eta} W_c d\eta,$$

$$\hat{\Delta} = \int_0^{T_s} e^{A_c \eta} \Delta \eta$$

and T_s is a sampling period

We verify the rank condition of the newly discretized system (6) :

$$C_d W_d = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1.14e^{-06} \\ 3.41e^{-04} \\ 6.75e^{-02} \end{pmatrix} = 1e^{-03} \begin{pmatrix} 0.0011 \\ 0.3419 \end{pmatrix}$$

The rank condition is satisfied:

$$\text{rank}(CW) = \text{rank}(W)$$

Conclusion et perspectives

1 Conclusions de l'étude

Sed feugiat. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Ut pellentesque augue sed urna. Vestibulum diam eros, fringilla et, consectetuer eu, nonummy id, sapien. Nullam at lectus. In sagittis ultrices mauris. Curabitur malesuada erat sit amet massa. Fusce blandit. Aliquam erat volutpat. Aliquam euismod. Aenean vel lectus. Nunc imperdiet justo nec dolor.

2 Ouverture et perspectives

Aliquam lectus. Vivamus leo. Quisque ornare tellus ullamcorper nulla. Mauris porttitor pharetra tortor. Sed fringilla justo sed mauris. Mauris tellus. Sed non leo. Nullam elementum, magna in cursus sodales, augue est scelerisque sapien, venenatis congue nulla arcu et pede. Ut suscipit enim vel sapien. Donec congue. Maecenas urna mi, suscipit in, placerat ut, vestibulum ut, massa. Fusce ultrices nulla et nisl.

Liste des publications

Articles à comité de lecture

Co Auteur 1, Co Auteur 2, Co Auteur 3. "*Un long titre d'article*". Un journal qui a accepté mon travail.
DOI: a1b2c3d4.xxxxx.99999

Articles en préparation

Co Auteur 1, Co Auteur 2, Co Auteur 3. "*Le long titre de mon second article*". Le journal de mes rêves.

Conférences internationales (premier auteur)

Co Auteur 1, Co Auteur 2, Co Auteur 3, Co Auteur 4. "*Titre de la présentation*". Conférence de Sciences, Quelque part, 2020.

Bibliographie

[Chaouche, 2022] A. Chaouche, A. Zemouche, M. Ramdani, K. Chaib Draa et D. Delattre. « Unknown input estimation algorithms for a class of LPV/nonlinear systems with application to wastewater treatment process ». *Proceedings of the Institution of Mechanical Engineers, Part I: Journal of Systems and Control Engineering* 236.7 (2022), p. 1372-1385 (cf. p. 5).

[Dabroom, 1997] A. Dabroom et H.K. Khalil. « Numerical differentiation using high-gain observers ». *Proceedings of the 36th IEEE Conference on Decision and Control*. T. 5. 1997, 4790-4795 vol.5 (cf. p. 5).

[Rajamani, 2002] R. Rajamani et C. Zhu. « Semi-autonomous adaptive cruise control systems ». *IEEE Transactions on Vehicular Technology* 51.5 (2002), p. 1186-1192 (cf. p. 3, 7).

[Trinh, 2011] H. Trinh et T. Fernando. *Functional observers for dynamical systems*. T. 420. Springer Science & Business Media, 2011 (cf. p. 5).

[Zhu, 2012] Fanglai Zhu. « State estimation and unknown input reconstruction via both reduced-order and high-order sliding mode observers ». *Journal of Process Control* 22.1 (2012), p. 296-302 (cf. p. 5).

UNIVERSITÉ DE LORRAINE

RÉSUMÉ

MOTS CLÉS

Estimation, mot clé 2, mot clé 3, mot clé 4

ABSTRACT

The reliability and safety of Connected and Autonomous Vehicles (CAVs) rely heavily on the real-time availability of precise dynamic variables. However, equipping vehicles with high-end sensors to measure every necessary variable—such as sideslip angles or vehicle trajectories—is often economically unfeasible or physically impossible. Furthermore, CAVs are increasingly vulnerable to sensor faults and cyber-attacks targeting inter-vehicle communications (V2V/V2I), which can lead to critical failures. To address these challenges without incurring the high cost of physical hardware redundancy, this thesis proposes the development of an embedded electronic board functioning as a resilient "soft sensor" based on analytical redundancy.

The research adopts a hybrid modeling methodology that integrates physical differential equations with online learning-based neuro-adaptive neural networks. This approach allows for the accurate representation of complex, time-varying parameters and unknown inputs within the vehicle's dynamics. Based on these models, advanced nonlinear estimation algorithms—specifically Unknown Input Observers (UIO) and neuro-adaptive observers—are developed to reconstruct missing state variables and ensure system resilience against data loss and malicious signal injection.

The proposed estimation strategies are applied to two primary control challenges:

— Resilience to Cyber-Attacks in Adaptive Cruise Control (ACC): The thesis investigates specific architectures for detecting and mitigating cyber-attacks, such as Denial of Service (DoS) and False Data Injection (FDI), within autonomous and cooperative ACC systems.

— Vehicle Tracking and Platooning: Novel estimation algorithms are proposed to handle the nonlinear dynamics and unknown forces inherent in tracking surrounding vehicles, which is essential for decision-making in maneuvers like lane changes and platooning.

The final contribution of this work is the design and fabrication of a prototype embedded electronic board. This hardware integrates the developed algorithms, validating the theoretical contributions and demonstrating a cost-effective, scalable solution for enhancing the autonomy, security, and fault tolerance of next-generation vehicles.

KEYWORDS

State Estimation, keyword 2, keyword 3, keyword 4