processes

MDPI

Article

Sigmoid-like Event-Triggered Security Cruise Control under Stochastic False Data Injection Attacks

Pengfei Zhang [1], Hongtao Sun [1,2,*], Chen Peng [2] and Cheng Tan [1]

[1] School of Engineering, Qufu Normal University, Rizhao 276800, China; zhang1627460015@163.com (P.Z.); tancheng1987love@163.com (C.T.)
[2] School of Mechatronic Engineering and Automation, Shanghai University, Shanghai 200444, China; c.peng@shu.edu.cn
* Correspondence: huntsun@qfnu.edu.cn

Abstract: This paper presents a Sigmoid-like event-triggered scheme (Sigmoid-like ETS) for security cruise control systems (CCSs) under stochastic false data injection (FDI) attacks. In order to improve the sensitivity of the ETS, a Sigmoid-like function is first proposed to adjust the event-triggered threshold, dynamically. In what follows, by considering a class of stochastic FDI attacks which obey Bernoulli distribution, the Sigmoid-like event-triggered security control strategy is proposed to ensure both the security and resource saving of the CCSs. Thus, a sufficient stability and stabilization criterion is well derived to present the co-design of an H_∞ control and event-triggered parameter. Finally, some simulation experiments are conducted to verify the effectiveness of the proposed Sigmoid-like event-triggered security cruise control for networked vehicles.

Keywords: security control; event-triggered scheme; false data injection attacks; autonomous driving

Citation: Zhang, P.; Sun, H.; Peng, C.; Tan, C. Sigmoid-like Event-Triggered Security Cruise Control under Stochastic False Data Injection Attacks. *Processes* **2022**, *10*, 1326. https://doi.org/10.3390/pr10071326

Academic Editor: Wen-Jer Chang

Received: 31 May 2022
Accepted: 4 July 2022
Published: 6 July 2022

1. Introduction

Cruise control is the key technology of autonomous driving, which requires vehicles to cruise at a set velocity and meanwhile keep a safe distance from other cars [1]. The driver does not need to keep his foot on the gas pedal or break pedal, thereby greatly reducing their fatigue. Cruising at a set speed can also improve fuel economy. Therefore, some critical points should be considered in designing cruise control systems (CCSs). For example, the vehicle suddenly accelerating or decelerating can create a bad experience for passengers, and may also cause a pile-up on a congested road [2,3]. Due to the introduction of the in-and-out networks of vehicles, related studies have become more challenging in a complicated networked control environment.

On the one hand, a large amount of information exchange can easily cause signal congestion due to the finite communication resource [4,5]. As a result, the braking system and power system of a vehicle are delayed in response and this puts higher control requirements on CCSs. In fact, an in-vehicle network includes varieties of sensors and actuators, a large number of electronic control units and complicated CAN buses [6]. Numerous data packets exchanged through a shared communication network, which leads to the CCSs, become a typically resource-constrained system. At present, most communication schemes are based on being time-triggered [7]. However, these time-triggered-based schemes cannot utilize limited network resources efficiently and this promotes the event-triggered control scheme which implements control actions as required. Essentially, the design of ETSs considers the sampled-data error (namely threshold) which consists of the last transmitted instant state and the current instant state. Therefore, the event-triggered thresholds' adjustment will be used to realize the maximize communication efficiency. In recent years, many ETSs have been proposed to address the problem of resource constraint, such as discrete-time ETSs [8,9], adaptive ETSs [10], dynamic ETSs [11], memory-based ETSs [12], distributed ETSs [13], etc. These ETSs play a significant role in resource saving under a networked

control environment. However, these ETSs are generally more complicated and a simplified adaptive ETS is expected.

On the other hand, vehicles' communication is generally vulnerable to cyber attacks, such as denial of service attacks and FDI attacks [14,15]. CCSs are very different from other control systems because they will do harm to human safety once cruise control actions are invalid. Many studies have confirmed that it is easy to disturb a vehicle by injecting maliciously false data into the controller area network (CAN) bus [16,17]. This will lead to a sudden acceleration or deceleration of the vehicle which poses a great threat to the safety of passengers. Based on this observation, one should spare no effort to ensure the stability of a vehicle under cyber attack. In general, an FDI attack is a class of harmful attack which can tamper with the real data in a hidden way and cause wrong control actions. Recently, there have been some studies focusing on security issues around FDI attacks. For example, an unscented Kalman filter based on an SE algorithm with a weighted least square was proposed to identify FDI attacks in [18]. An exhaustive review on the different detection algorithms of FDI attacks is presented in smart grids, and two different solutions for detecting secret cyber-physical attacks are proposed in [19]. However, these studies only focus on FDI attack detection. Recent studies provide some new solutions to FDI attacks and have placed their attention on security control under FDI attacks [20–22]. The key idea of security control is that one can guarantee the stability of the control system from the perspective of control strategy design rather than information protection.

Based on the above observations, security control and resource saving the two main limitations of the cruise system, which create a real challenge to the safety of networked autonomous vehicles. Thus, the contributions of this paper can be described in two respects:

- A novel Sigmoid-like ETS is proposed to cope with the co-design of the control and communication of CCSs. Compared with the traditional static ETSs [23], adaptive ETSs [21,22] and dynamic ETSs [6,11], the proposed Sigmoid-like ETS will guarantee the upper bound of event-triggered thresholds while making full use of the state perception;
- The security control of CCSs under stochastic FDI attacks is well characterized with the proposed Sigmoid-like ETS. Rather than detecting the FDI attacks in a complicated way [18,19,24], the studied event-triggered security control of CCSs is of H_∞ performance even on the condition that the FDI attack detection fails.

The remainder of this article is organized as follows. Section 2 describes the Sigmoid ETS for cruise control as well as the longitudinal vehicle dynamics model and the overall control objectives. Section 3 presents the stabilization criteria and controller design method for networked cruise control systems. In Section 4, some simulation studies are presented to show the advantages of Sigmoid-like ETS. Section 5 draws the final conclusions.

2. Preliminaries

The cruise control of an autonomous vehicle described in this paper is to obtain an expected acceleration and make the vehicle able to cruise at a specific velocity. The longitudinal dynamic model of vehicle is described as follows:

$$\begin{cases} \dot{x}_p(t) = x_v(t); \\ \dot{x}_v(t) = x_a(t); \\ \dot{x}_a(t) = -\frac{1}{\eta_d}x_a(t) + \frac{1}{\eta_d}u_c(t) + \frac{1}{\eta_d}w_\eta(t), \end{cases} \tag{1}$$

where $x_p(t)$ denotes the position with respect to the origin; $x_v(t)$ denotes real velocity; $x_a(t)$ denotes the acceleration produced by the engine; $\eta_d > 0$ represents the inertia delay of the vehicle powertrain; $u_c(t)$ denotes the desired control input; and $w_\eta(t)$ denotes the generally unmodeled but bounded road disturbance input vector. If the state vector is denoted by $x_c(t) = [x_p(t), x_v(t), x_a(t)]^{\mathrm{T}}$, the state space model of CCSs can be written as:

$$\dot{x}_c(t) = \mathcal{A}x_c(t) + \mathcal{B}u_c(t) + \mathcal{B}w_\eta(t), \tag{2}$$

where $\mathcal{A} = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & -\frac{1}{\eta_d} \end{bmatrix}$, $\mathcal{B} = \begin{bmatrix} 0 \\ 0 \\ \frac{1}{\eta_d} \end{bmatrix}$.

By considering the fact that the sensors, controllers and actuators communicate through an open communication network, a networked event-triggered CCS is shown in Figure 1. It is clear that the feedback measurements and control actions would be disrupted when there are malicious FDI attacks.

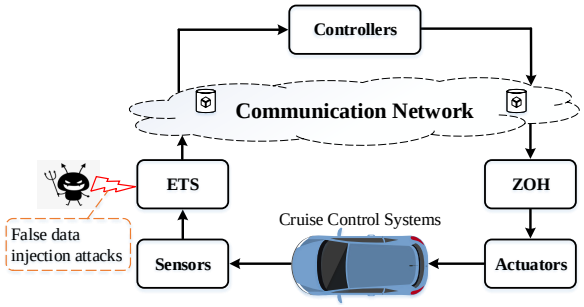


Figure 1. The networked cruise control systems.

In order to understand the proposed Sigmoid-like event-triggered control more clearly, some assumptions are presented at first.

Assumption 1. *The sampled data are sent to the controller with a constant period h. The sampling set $\Theta_1 = \{0, h, 2h, \cdots, kh\}$ is assumed for all $k \in \mathbb{N}$.*

Assumption 2. *The sampled data, whether transmitted or not, are dependent on the designed event-triggered scheme. Then the successful transmitted signals set is $\Theta_2 = \{0, t_1 h, t_2 h, \cdots, t_k h\}$, where $t_k \in \mathbb{N}$ and $\lim_{k\to\infty} t_k \to \infty$. Obviously, $\Theta_2 \subseteq \Theta_1$.*

Assumption 3. *Zero-order hold (ZOH) converts a discrete control signal into a continuous one during the time interval $t \in [t_k h + \eta_k, t_{k+1} h + \eta_{k+1})$. Here, η_k is the packet transmission delay at $t_k h$.*

Under the above assumptions, the CCSs' state feedback form based on the sampled-data control framework is given by:

$$\begin{cases} \dot{x}_c(t) = \mathcal{A}x_c(t) + \mathcal{B}u_c(t) + \mathcal{B}w_\eta(t); \\ z(t) = \mathcal{C}x_c(t) + \mathcal{D}u_c(t); \\ u_c(t) = \mathcal{K}x_c(t_k h), t \in [t_k h + \eta_k, t_{k+1} h + \eta_{k+1}), \end{cases} \tag{3}$$

where $z(t) \in \mathbb{R}^p$ is a controlled output vector; $\mathcal{C}$ and $\mathcal{D}$ are suitable constant matrices; and $\mathcal{K}$ is the designed controller gain. Assuming v^* is the expected cruise velocity, then $\lim_{t\to\infty} \dot{x}_c(t) = [v^*, 0, 0]^{\mathrm{T}}$.

2.1. Sigmoid-like ETS

In this section, a novel event-triggered scheme with a Sigmoid-like threshold function is first proposed.

Firstly, denote the sampled-data error as:

$$e(i_k h) = x_c(i_k h) - x_c(t_k h), \tag{4}$$

where $x_c(t_k h)$ is the last transmitted sampling instant state, $x_c(i_k h)$ is the current state, $i_k h = t_k h + lh, l \in \mathbb{N}$.

Thus, by virtue of (4), the Sigmoid-like ETS is described as:

$$t_{k+1}h = t_k h + \min_l\{lh|e^{\mathrm{T}}(i_k h)\Lambda e(i_k h) \geqslant \tilde{\delta}(t_k h)\vartheta(t_k h)\}, \tag{5}$$

where $\tilde{\delta}(t_k h) = \frac{\phi_\epsilon}{\exp(a\|x_c(t_k h)\|^2)+\epsilon}$, ϵ, a and ϕ_ϵ are some given constants, $||\cdot||$ is the Euclidian norm of a vector, $\vartheta(t_k h) = x_c^{\mathrm{T}}(t_k h)\Lambda x_c(t_k h)$ with $\Lambda = \Lambda^{\mathrm{T}}$ is a designed positive weighting matrix.

In fact, the Sigmoid-like function $\tilde{\delta}(t_k h)$ plays an important role in the adjustment of the event-triggered threshold, i.e.,:

- The $\tilde{\delta}(t_k h)$ is a monotonic decreasing function along with $||x_c(t_k h)||^2$;
- It is obvious that $\tilde{\delta}(t_k h) \in (0, \frac{\phi_\epsilon}{1+\epsilon}]$ is held.

The above two features of the dynamic event-triggered parameter $\tilde{\delta}(t_k h)$ are beneficial to facilitating the stability analysis with Sigmoid-like ETS. In fact, the event-triggered threshold $\tilde{\delta}(t_k h)$ can adjust with the change of state $x_c(t_k h)$. When $\|x_c(t_k h)\|^2$ becomes bigger, implying that the system state has become unstable, a smaller $\tilde{\delta}$ will encourage the ETS (5) to release more packets. On the contrary, it is easy to see that if the system reaches a stable state, that is $\|x_c(t_k h)\|^2 \to 0$, then the ETS (5) can reach the largest $\tilde{\delta}$, which means that a fewer packets should be transmitted.

Remark 1. *As a special case, if $\tilde{\delta} = \frac{\phi_\epsilon}{1+\epsilon}$ in (5), a static ETS is obtained as in [23].*

2.2. Stochastic FDI Attacks

FDI attacks capture real signals in the case where the real transmitted signal $x_c(t_k h)$ is replaced by a false $f(x_c(t_k h))$, which would lead to non-ideal control actions. Usually, a stochastic-type FDI attack follows the below rules:

Assumption 4. *Energy constraints: With regard to a given matrix S_{EC}, the signals of FDI attacks are supposed to satisfy:*

$$\| f(x_c(t_k h)) \|_2 \leqslant \| S_{EC} x_c(t_k h) \|_2, \tag{6}$$

where S_{EC} is an upper bound of the nonlinear function $f(x_c(t_k h))$.

Assumption 5. *Probability constraints: Denote $\theta_s(t)$ is the probability of FDI attacks; it satisfies the following condition:*

$$\theta_s(t) = \begin{cases} 1, & \textit{FDI attack is activated;} \\ 0, & \textit{FDI attack is slept,} \end{cases}$$

with the stochastic properties of $\theta_s(t)$ satisfying:

$$\mathbb{E}(\theta_s(t)) = \theta, \mathbb{E}(\theta_s(t) - \theta)^2 = \sigma^2, \tag{7}$$

where the probability mean value is θ and the variance of $\theta_s(t)$ is σ^2, the expectation of stochastic variable is represented by $\mathbb{E}(\cdot)$.

Remark 2. *In order to characterize FDI attacks in a more reasonable way, both energy and probability constraints are presented by Assumptions 4 and 5, respectively. For such assumptions, one can refer to [14,20,22], etc.*

2.3. Control Objectives

We are now in position to model the issues of the Sigmoid-like event-triggered cruise control. According to [23], the sampling-interval-like subsets $[t_k h + \eta_k, t_{k+1} h + \eta_{k+1})$ can be expressed as the adjacent sampling interval with:

$$\Theta = \bigcup_{l=0}^{t_{k+1}-t_k-1} \Theta_l,$$

where $\Theta_l = [i_k h + \eta_k, i_k h + h + \eta_{k+1})$, $i_k h = t_k h + lh$.

Then, by defining $\eta(t) = t - i_k h$, one can obtain the piecewise-linear function $\eta(t)$ which satisfies $\dot{\eta}(t) = 1, 0 \leq \eta(t) \leq h + \max\{\eta_k, \eta_{k+1}\} = \overline{\eta}$.

Thus, by considering the FDI attacks, the actual state feedback control actions are written as follows:

$$u_c(t) = \theta_s(t)\mathcal{K}f(x_c(t_k h)) + (1 - \theta_s(t))\mathcal{K}x_c(t_k h). \tag{8}$$

Under the Sigmoid-like ETS, the CCSs (3) with stochastic FDI attacks can be rewritten in the following form:

$$\begin{cases} \dot{x}_c(t) = \mathcal{A}x_c(t) + \theta_s(t)\mathcal{B}\mathcal{K}f(x_c(t_k h)) + (1 - \theta_s(t))\mathcal{B}\mathcal{K}x_c(t_k h) + \mathcal{B}w_\eta(t) \\ \text{subjects to :} \\ e^{\mathrm{T}}(i_k h)\Phi e(i_k h) \geqslant \tilde{\delta}(t_k h)\vartheta(t_k h), \end{cases} \tag{9}$$

where ψ_0 is defined as the initial state $x_c(t_0)$ for all variables $t \in [t_0 - \overline{\eta}, t_0)$, $x_c(t_k h) = x_c(t - \eta(t)) - e(i_k h)$.

With respect to the Sigmoid-like event-triggered CCSs (9) under stochastic FDI attacks, the control objectives of this technical note are presented as follows:

1. Under the Sigmoid-like ETS (5) and stochastic FDI attacks (6), the CCSs (9) are asymptotically stable when there is no disturbance ($w_\eta(t) = 0$);
2. Under the Sigmoid-like ETS (5) and stochastic FDI attacks (6), the desired H_∞ attenuation level with $\mathbb{E}\{||z(t)||_2\} \leq \mathbb{E}\{\gamma||w_\eta(t)||_2\}$ is held under its zero initial condition.

For facilitating the further analysis and synthesis of the CCSs (9), the definition named infinitesimal operator $\mathcal{L}$ is well defined to derive the main results of this paper.

Definition 1 ([25]). *For a given function $V : C^B_{F_0}([-\overline{\eta}, 0], R^n) \times S$, its infinitesimal operator $\mathcal{L}$ is defined as:*

$$\mathcal{L}(V(t, x_t)) = \lim_{\Delta \to 0^+} \frac{1}{\Delta}[\mathbb{E}\{V(x_t + \Delta)|x_t\} - V(x_t)], \tag{10}$$

where $x_t = \{x(t + \theta) : -\overline{\eta} \leq \theta \leq 0\}$ for $t \geq 0$.

3. Main Results

In this part, the criterions of stability and stabilization for Sigmoid-like event-triggered CCSs (9) under stochastic FDI attacks (6) are carefully derived. In addition, an algorithm is presented to implement the controller gain and event-triggered parameter co-design.

Theorem 1. *For some designed positive scalars σ, $\overline{\eta}$, $\frac{\phi_\epsilon}{1+\epsilon}$, θ and γ, if there exist real positive matrices $\mathcal{Z}$, $\mathcal{H}$, $\mathcal{R}$ and Λ with suitable dimensions, such that the LMIs hold*

$$\begin{bmatrix} \Xi_{11} & \Xi_{21}^{\mathrm{T}} & \Xi_{31}^{\mathrm{T}} \\ \Xi_{21} & \Xi_{22} & 0 \\ \Xi_{31} & 0 & \Xi_{33} \end{bmatrix} < 0, \quad \begin{bmatrix} \mathcal{R} & \mathcal{U}^{\mathrm{T}} \\ \mathcal{U} & \mathcal{R} \end{bmatrix} > 0, \tag{11}$$

where

$$\begin{aligned} \Xi_{11} = [(1,1) &= \mathcal{A}^{\mathrm{T}}\mathcal{Z} + \mathcal{Z}\mathcal{A} + \mathcal{H} - \mathcal{R}, (1,6) = \mathcal{Z}\mathcal{B}, \\ (1,2) &= (1-\theta)\mathcal{Z}\mathcal{B}\mathcal{K} + \mathcal{R}^{\mathrm{T}} - \mathcal{U}^{\mathrm{T}}, (1,3) = \mathcal{U}^{\mathrm{T}}, \\ (1,4) &= -(1-\theta)\mathcal{Z}\mathcal{B}\mathcal{K}, (1,5) = \theta\mathcal{Z}\mathcal{B}\mathcal{K}, \end{aligned}$$

$$
\begin{aligned}
(2,2) &= \frac{\phi_\epsilon}{1+\epsilon}\Lambda - 2\mathcal{R} + \mathcal{U} + \mathcal{U}^{\mathrm{T}},\\
(3,2) &= \mathcal{R} - \mathcal{U}, (3,3) = -\mathcal{H} - \mathcal{R},\\
(4,2) &= -\frac{\phi_\epsilon}{1+\epsilon}\Lambda, (4,4) = \frac{\phi_\epsilon}{1+\epsilon}\Lambda - \Lambda,\\
(5,5) &= -\theta\mathcal{Z}, (6,6) = -\gamma^2 I];\\
\Xi_{21} &= \overline{\eta}\mathcal{R} * \mathrm{col}\{\mathcal{I}_1, \mathcal{I}_2\}, \Xi_{22} = \mathrm{diag}\{-\mathcal{R}, -\mathcal{R}\};\\
\Xi_{31} &= \begin{bmatrix} \mathcal{C} & \mathcal{D}\mathcal{K} & 0 & -\mathcal{D}\mathcal{K} & 0 & 0 \\ \sqrt{\theta}\mathcal{Z}S_{EC} & 0 & 0 & 0 & 0 & 0 \end{bmatrix};\\
\Xi_{33} &= \mathrm{diag}\{-I, -\mathcal{Z}\};\\
\mathcal{I}_1 &= [\mathcal{A}, (1-\theta)\mathcal{B}\mathcal{K}, 0, -(1-\theta)\mathcal{B}\mathcal{K}, \theta\mathcal{B}\mathcal{K}, \mathcal{B}],\\
\mathcal{I}_2 &= [0, -\sigma\mathcal{B}\mathcal{K}, 0, \sigma\mathcal{B}\mathcal{K}, \sigma\mathcal{B}\mathcal{K}, 0].
\end{aligned}
$$

Then, CCSs (9) under the stochastic FDI attacks are mean-square asymptotically stable with an H_∞ index γ.

Proof. Consider a Lyapunov–Krasovskii functional candidate as:

$$V(t, x_c) = x_c^{\mathrm{T}}(t)\mathcal{Z}x_c(t) + \int_{t-\overline{\eta}}^{t} x_c^{\mathrm{T}}(\nu)\mathcal{H}x_c(\nu)d\nu + \overline{\eta}\int_{t-\overline{\eta}}^{t}\int_{\nu}^{t} \dot{x}_c^{\mathrm{T}}(u)\mathcal{R}\dot{x}_c(u)dud\nu. \tag{12}$$

By using the infinitesimal operator in Definition 1 for $V(t, x_c)$, $t \in \Theta_l$, then the mathematical expectation of it can be obtained as:

$$
\begin{aligned}
\mathbb{E}\{\mathcal{L}(V(t, x_c))\} &= 2x_c^{\mathrm{T}}(t)\mathcal{Z}\mathcal{I}_1 F(t) + x_c^{\mathrm{T}}(t)\mathcal{H}x_c(t)\\
&- x_c^{\mathrm{T}}(t-\overline{\eta})\mathcal{H}x_c(t-\overline{\eta}) + \overline{\eta}^2\mathbb{E}\{\dot{x}_c^{\mathrm{T}}(t)\mathcal{R}\dot{x}_c(t)\}\\
&- \overline{\eta}\int_{t-\overline{\eta}}^{t} \dot{x}_c^{\mathrm{T}}(\nu)\mathcal{R}\dot{x}_c(\nu)d\nu - z^{\mathrm{T}}(t)z(t)\\
&+ \gamma^2 w_\eta^{\mathrm{T}}(t)w_\eta(t) + z^{\mathrm{T}}(t)z(t) - \gamma^2 w_\eta^{\mathrm{T}}(t)w_\eta(t),
\end{aligned} \tag{13}
$$

where

$$
\begin{aligned}
F^{\mathrm{T}}(t) &\triangleq [x_c^{\mathrm{T}}(t), x_c^{\mathrm{T}}(t-\eta(t)), x_c^{\mathrm{T}}(t-\overline{\eta}), e^{\mathrm{T}}(t), f^{\mathrm{T}}(x), w_\eta^{\mathrm{T}}(t)],\\
\mathbb{E}\{\dot{x}_c^{\mathrm{T}}(t)\mathcal{R}\dot{x}_c(t)\} &= F^{\mathrm{T}}(t)(\mathcal{I}_1^{\mathrm{T}}\mathcal{R}\mathcal{I}_1 + \mathcal{I}_2^{\mathrm{T}}\mathcal{R}\mathcal{I}_2)F(t).
\end{aligned}
$$

Furthermore, according to [26], when positive matrix $\mathcal{R}$ satisfies $\mathcal{U}_\mathcal{R} = \begin{bmatrix} \mathcal{R} & \mathcal{U}^{\mathrm{T}} \\ \mathcal{U} & \mathcal{R} \end{bmatrix} > 0$, then the cross item in (13) can be dealt with in the following.

$$-\overline{\eta}\int_{t-\overline{\eta}}^{t} \dot{x}_c^{\mathrm{T}}(\nu)\mathcal{R}\dot{x}_c(\nu)d\nu \le -\varsigma^{\mathrm{T}}(t)\mathcal{U}_\mathcal{R}\varsigma(t), \tag{14}$$

where

$$\varsigma^{\mathrm{T}}(t) = [x_c^{\mathrm{T}}(t) - x_c^{\mathrm{T}}(t-\eta(t)), x_c^{\mathrm{T}}(t-\eta(t)) - x_c^{\mathrm{T}}(t-\overline{\eta})].$$

Applying Schur complement lemma, $e^{\mathrm{T}}(i_k h)\Lambda e(i_k h) - \frac{\phi_\epsilon}{1+\epsilon}\vartheta(t_k h) < 0$ and Assumption 4, which satisfies $\theta f^{\mathrm{T}}(x_c(t_k h))\mathcal{Z}f(x_c(t_k h)) - \theta x_c^{\mathrm{T}}(t)S_{EC}^{\mathrm{T}}\mathcal{Z}S_{EC}x_c(t) \le 0$ to (13), the following relationship is held,

$$\mathbb{E}\{\mathcal{L}(V(t))\} \le -z^{\mathrm{T}}(t)z(t) + \gamma^2 w_\eta^{\mathrm{T}}(t)w_\eta(t), \tag{15}$$

by taking H_∞ performance into consideration.

Because $\mathbb{E}\{V(t)\}$ is continuous in time, then one could integrate the Equation (15) from 0 to $+\infty$, then:

$$\mathbb{E}\{V(+\infty)\} - V(0) \leq \int_0^{+\infty} (\gamma^2 w_\eta^{\mathrm{T}}(\nu) w_\eta(\nu) - z^{\mathrm{T}}(\nu) z(\nu)) d\nu. \tag{16}$$

In the case of $V(0) = 0$, from (16) the final results are obtained as:

$$\int_0^{+\infty} z^{\mathrm{T}}(\nu) z(\nu) d\nu \leq \int_0^{+\infty} \gamma^2 w_\eta^{\mathrm{T}}(\nu) w_\eta(\nu) d\nu, \tag{17}$$

which implies that $\|z(t)\|_2 \leq \gamma \|w_\eta(t)\|_2$ for any non-zero $w_\eta(t) \in \mathcal{L}_2[0, \infty)$.

If there is no disturbance, under the condition (11), the CCSs (9) are mean-square asymptotically stable. This completes the proof. □

Remark 3. *Obviously, all the event-triggered thresholds given by Sigmoid-like ETS (5) will be confined within* $(0, \frac{\phi_\epsilon}{1+\epsilon}]$*, thus, mean-square asymptotic stability is guaranteed during the proof. In addition, due to Sigmoid-like ETS (5), the threshold can be determined immediately rather than by adding an extra evolution calculation; this is very different from other adaptive ETSs such as [21,22].*

On the basis of Theorem 1, the state feedback controller gain as well as event-triggered parameter to CCSs (9) are presented in Theorem 2.

Theorem 2. *For some designed positive scalars* σ, $\overline{\eta}$, $\frac{\phi_\epsilon}{1+\epsilon}$, θ *and* γ*, if there exist real positive matrices* X, $\widetilde{\mathcal{H}}$, $\widetilde{\mathcal{R}}$, $\widetilde{\Lambda}$ *and* Y *with suitable dimensions, such that the LMIs hold*

$$\begin{bmatrix} \widetilde{\Xi}_{11} & \widetilde{\Xi}_{21}^{\mathrm{T}} & \widetilde{\Xi}_{31}^{\mathrm{T}} \\ \widetilde{\Xi}_{21} & \widetilde{\Xi}_{22} & 0 \\ \widetilde{\Xi}_{31} & 0 & \widetilde{\Xi}_{33} \end{bmatrix} < 0, \quad \begin{bmatrix} \widetilde{\mathcal{R}} & \widetilde{\mathcal{U}}^{\mathrm{T}} \\ \widetilde{\mathcal{U}} & \widetilde{\mathcal{R}} \end{bmatrix} > 0, \tag{18}$$

where

$$\begin{aligned}
\widetilde{\Xi}_{11} = [&(1,1) = \mathcal{A}X + X\mathcal{A}^{\mathrm{T}} + \widetilde{\mathcal{H}} - \widetilde{\mathcal{R}}, (1,6) = \mathcal{B}, \\
&(1,2) = (1-\theta)\mathcal{B}Y + \widetilde{\mathcal{R}}^{\mathrm{T}} - \widetilde{\mathcal{U}}^{\mathrm{T}}, (1,3) = \widetilde{\mathcal{U}}^{\mathrm{T}}, \\
&(1,4) = -(1-\theta)\mathcal{B}Y, (1,5) = \theta\mathcal{B}Y, \\
&(2,2) = \frac{\phi_\epsilon}{1+\epsilon}\widetilde{\Lambda} - 2\widetilde{\mathcal{R}} + \widetilde{\mathcal{U}} + \widetilde{\mathcal{U}}^{\mathrm{T}}, \\
&(3,2) = \widetilde{\mathcal{R}} - \widetilde{\mathcal{U}}, (3,3) = -\widetilde{\mathcal{H}} - \widetilde{\mathcal{R}}, \\
&(4,2) = -\frac{\phi_\epsilon}{1+\epsilon}\widetilde{\Lambda}, (4,4) = \frac{\phi_\epsilon}{1+\epsilon}\widetilde{\Lambda} - \widetilde{\Lambda}, \\
&(5,5) = -\theta X, (6,6) = -\gamma^2 I]; \\
\widetilde{\Xi}_{21} = \overline{\eta} * \mathrm{col}\{\widetilde{\mathcal{I}}_1, \widetilde{\mathcal{I}}_2\}, &\widetilde{\Xi}_{22} = \mathrm{diag}\{\rho^2\widetilde{\mathcal{R}} - 2\rho X, \rho^2\widetilde{\mathcal{R}} - 2\rho X\}; \\
\widetilde{\Xi}_{31} = &\begin{bmatrix} \mathcal{C}X & \mathcal{D}Y & 0 & -\mathcal{D}Y & 0 & 0 \\ \sqrt{\theta}S_{EC}X & 0 & 0 & 0 & 0 & 0 \end{bmatrix}; \\
\widetilde{\Xi}_{33} = &\mathrm{diag}\{-I, -X\}; \\
\widetilde{\mathcal{I}}_1 = &[\mathcal{A}X, (1-\theta)\mathcal{B}Y, 0, -(1-\theta)\mathcal{B}Y, \theta\mathcal{B}Y, \mathcal{B}], \\
\widetilde{\mathcal{I}}_2 = &[0, -\sigma\mathcal{B}Y, 0, \sigma\mathcal{B}Y, \sigma\mathcal{B}Y, 0].
\end{aligned}$$

Then, the state feedback controller gain to CCSs (9) can be obtained by $\mathcal{K} = YX^{-1}$ *while* H_∞ *performance* γ *is achieved.*

Proof. Define $X = \mathcal{Z}^{-1}$, $\widetilde{\mathcal{H}} = X\mathcal{H}X$, $\widetilde{\mathcal{R}} = X\mathcal{R}X$, $\widetilde{\Lambda} = X\Lambda X$, $\widetilde{\mathcal{U}} = X\mathcal{U}X$. Then, pre- and post-multiplying LMIs (11) left matrix with $\mathrm{diag}\{X, X, X, X, X, I, \mathcal{R}^{-1}, \mathcal{R}^{-1}, I, X\}$, and right matrix with $\mathrm{diag}\{X, X\}$, respectively. Next, we utilize $-X\widetilde{\mathcal{R}}^{-1}X \leqslant \rho^2\widetilde{\mathcal{R}} - 2\rho X$ to cope with the nonlinear terms $-X\widetilde{\mathcal{R}}^{-1}X$. Based on the above analysis, we can get the controller gain $\mathcal{K}$. This completes the proof. □

At the end of this section, the Algorithm 1 to find the controller $\mathcal{K}$ of CCSs (9) is presented in brief.

Algorithm 1: Find the controller gain $\mathcal{K}$, event-triggered parameter $\frac{\phi_\epsilon}{1+\epsilon}$ and weighting matrix Λ

1: Set the positive scalars ϵ, $\overline{\eta}$ and the initial event-triggered parameter ϕ_ϵ. Give the increasing step $\Delta > 0$ and an optimization target $topt < 0$;
2: While $topt < 0$;
3: $\phi_\epsilon = \phi_\epsilon + \Delta$;
4: Solve LMIs (18), if there is a feasible solution X, $\widetilde{\mathcal{H}}$, $\widetilde{\mathcal{R}}$ and $\widetilde{\Lambda}$ satisfying LMIs (18), go to the next step. Otherwise, return *Step* 1;
5: Return $\phi_\epsilon - \Delta$ and calculate $\mathcal{K}$, Λ.

4. Simulation Examples

To verify the proposed Sigmoid-like event-triggered security control strategy, we conducted the following simulation experiments by using Matlab (R2018b) in Win10 OS with 8 GHz Intel Core i5 CPU, 4 GB RAM.

4.1. Parameters Setting

- *System parameters:*
  Set the vehicle to cruise with different velocities: 5 m/s, 10 m/s, 15 m/s. In the system (3), the disturbance is $w_\eta(t) = 0.01e^{-t}$, $t \in [0, 30]$ s, and the other parameters are $\eta_d = 0.5$ s, $\sigma = 0.16$ s, $\overline{\eta} = 0.2$ s, $\rho = 0.63$, $\gamma = 200$, the initial state $x_c(0) = [-0.5; 0; 1]$;
- *FDI attack parameters:*
  The probability of FDI attack is θ with $\| f(x_c(t_k h)) \|_2 \leqslant \| S_{EC} x_c(t_k h) \|_2$ and $f(x_c(t_k h)) = [-\tanh(0.2x_1(t_k h)); -\tanh(0.1x_2(t_k h)); -\tanh(0.2x_3(t_k h))]$, where the weighting matrix $S_{EC} = \mathrm{diag}\{0.2\ 0.1\ 0.2\}$;
- *Event-triggered parameters:*
  The event-triggered related parameter $\epsilon = 1$, $\tilde{\delta}(0) = 0$, $a = 0.01$ (a is in Sigmoid-like function).

4.2. Discussions of Simulation Results

In what follows, the following two cases are shown to compare our main results.

- **Case I: FDI-free case**

If there are no FDI attacks, we set $\theta = 0$, the other parameters are the same as above, the controller gain can be solved from Theorem 2.

$$\overline{\mathcal{K}} = \begin{bmatrix} -1.0373 & -1.7486 & -0.8822 \end{bmatrix},$$

with respect to weighting matrix

$$\overline{\Lambda} = \begin{bmatrix} 75.3100 & 31.3757 & -154.0642 \\ 31.3757 & 114.8064 & -230.9179 \\ -154.0642 & -230.9179 & 764.1387 \end{bmatrix}.$$

Figures 2 and 3 represent the cruising response with different velocities, positions and accelerations of the vehicle, as well as release intervals when $v = 10$ m/s. The following results are easily achieved: (1) Figure 2a shows the vehicle tracking path with 5 m/s in a stable way. Figure 3a shows it can cruise at different velocities in a more stable way. Then the proposed Sigmoid-like ETS can realize a favorable balance between the cruising accuracy and the passenger experience; (2) Figure 2d shows 75 packets are allowed to transmit and the average release interval is 0.3824s. The sampled-data are transmitted only when the CCSs are in a worse case. Figure 3d shows that 110 packets are transmitted and the average release interval is 0.2664 s. Both static ETS and Sigmoid-like ETS can achieve mean-square asymptotic stability; however, the proposed Sigmoid-like ETS shows a better control performance by sending more packets. All these enhancements are due to the change of dynamic event-triggered parameter $\widetilde{\delta}(t_k h)$, as can be see in Figure 3e.

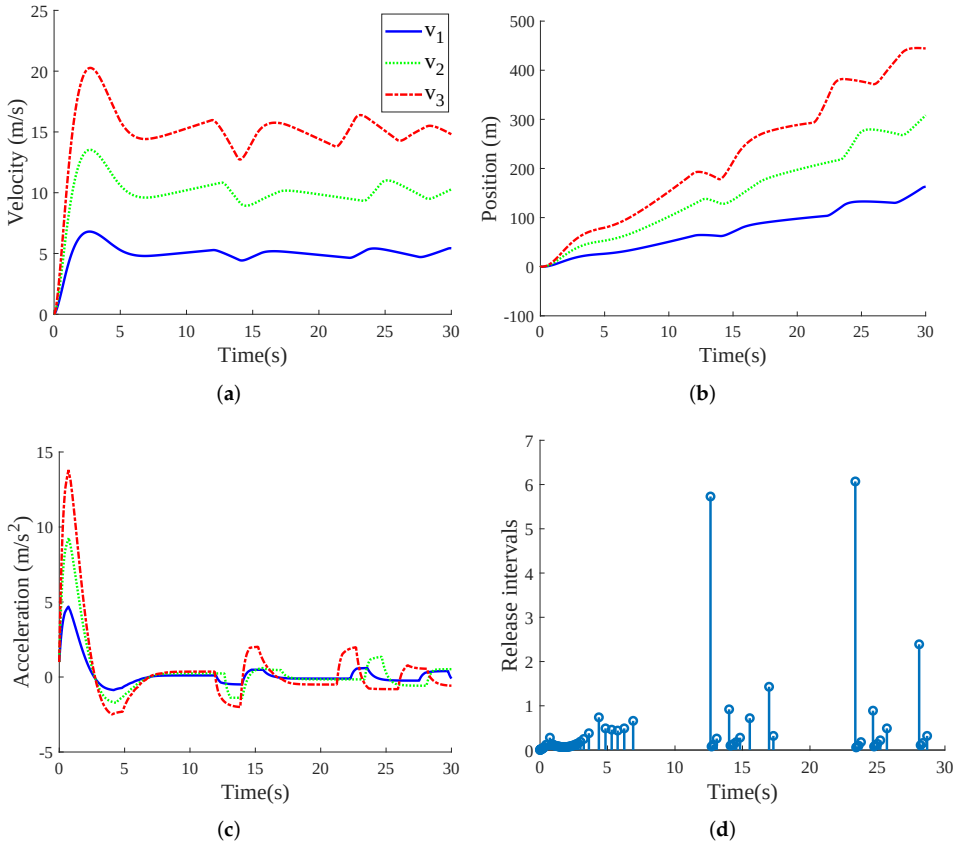


Figure 2. Simulation results under static ETS ($\tilde{\delta}(t_k h) \equiv 0.01$): velocities (**a**); positions (**b**); accelerations (**c**); and release intervals with v_2 (**d**).

- **Case II: FDI attack case**

If there are random FDI attacks appearing in CCSs (3), we create the following control experiment. It is obvious to see from Figure 4 that CCSs cannot be stable in [23]. Then, one can apply the designed feedback gain $\mathcal{K}$ and weighting matrix Λ to the experiment system (9) by Theorem 2. According to Algorithm 1, one can find $\phi_\epsilon = 0.01$ and the corresponding controller gain is:

$$\mathcal{K} = \begin{bmatrix} -0.7885 & -1.7248 & -0.7910 \end{bmatrix},$$

with respect to weighting matrix

$$\Lambda = \begin{bmatrix} 18.5638 & 11.6150 & -45.2334 \\ 11.6150 & 84.6116 & -185.6069 \\ -45.2334 & -185.6069 & 461.4976 \end{bmatrix}.$$

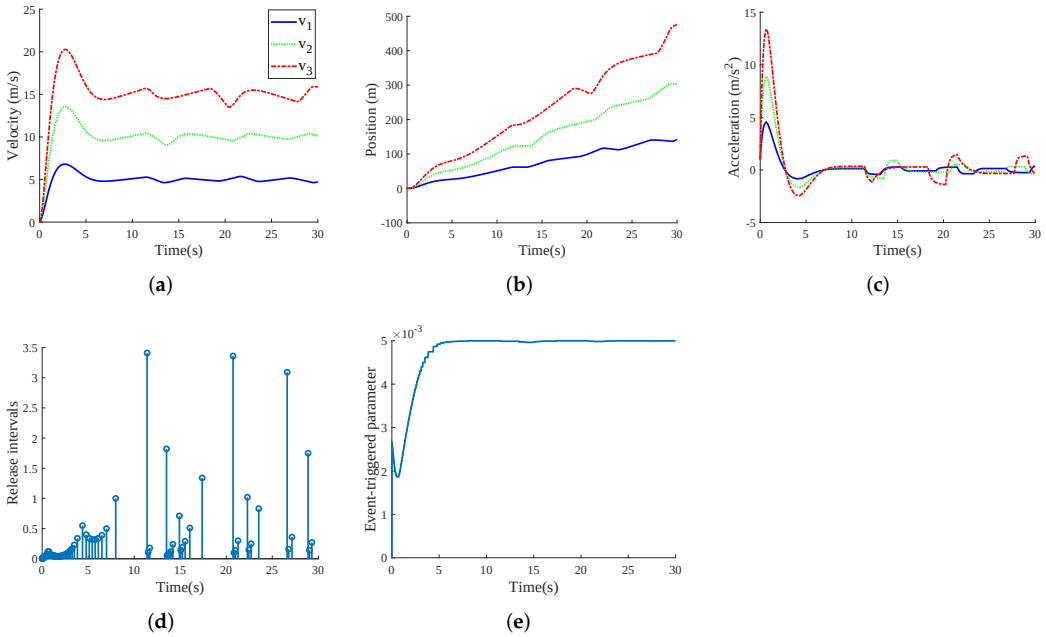
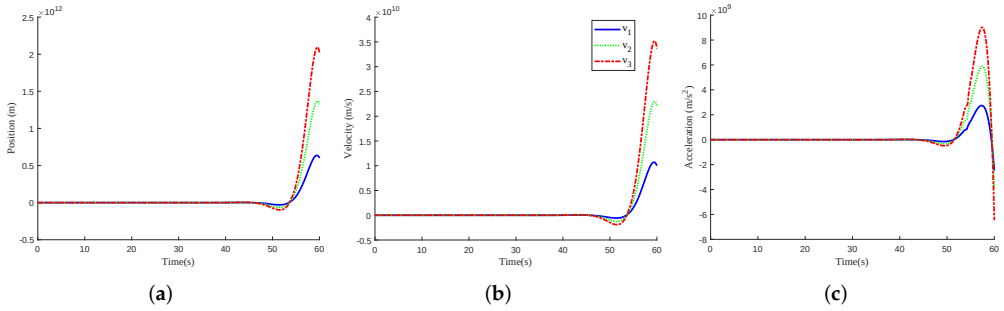


Figure 3. Simulation results under Sigmoid-like ETS: velocities (**a**); positions (**b**); accelerations (**c**); release intervals with v_2 (**d**); evolution of $\tilde{\delta}(t_k h)$ (**e**).

In order to see the overall change process more clearly, set a longer simulation time of 60 s.



(**a**) (**b**) (**c**)

Figure 4. Simulation results under Sigmoid-like ETS and FDI attacks ($\theta = 0.2$) in [23]: velocities (**a**); positions (**b**); accelerations (**c**).

It can be observed from Figures 5 and 6 that: (1) The proposed Sigmoid-like ETS can guarantee the security (mean square asymptotic stability) of cruise control under FDI attacks. On the contrary, the static ETS is seriously disturbed by the FDI attacks; (2) Figures 5d and 6d show that 117, 155 packets are transmitted and the average release interval is 0.5072, 0.3742 s, respectively. It clear to see that more packets are transmitted under the proposed Sigmoid-like ETS. As we know, a greater number of packets transmission and shorter release intervals are more beneficial to improving control performance. Therefore, the proposed Sigmoid-like ETS releases more packets to make up for the loss of control performance under FDI attacks by adjusting the event-triggered parameter $\tilde{\delta}(t_k h)$, see Figure 6e.

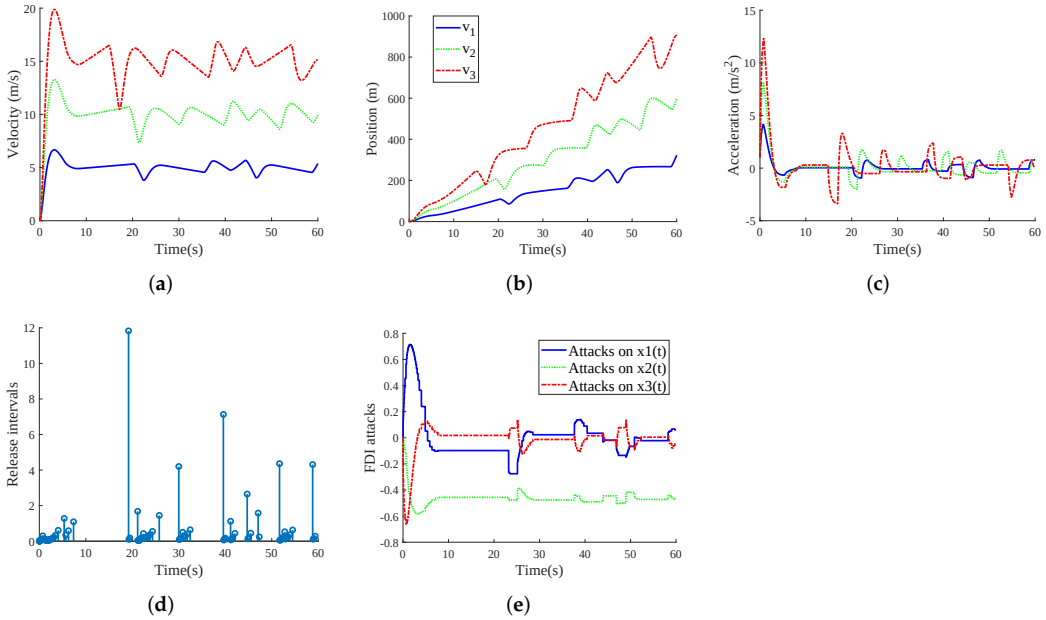


Figure 5. Simulation results under static ETS and FDI attacks ($\theta = 0.2$): velocities (**a**); positions (**b**); accelerations (**c**); release intervals with v_2 (**d**); signals after FDI attacks (**e**).

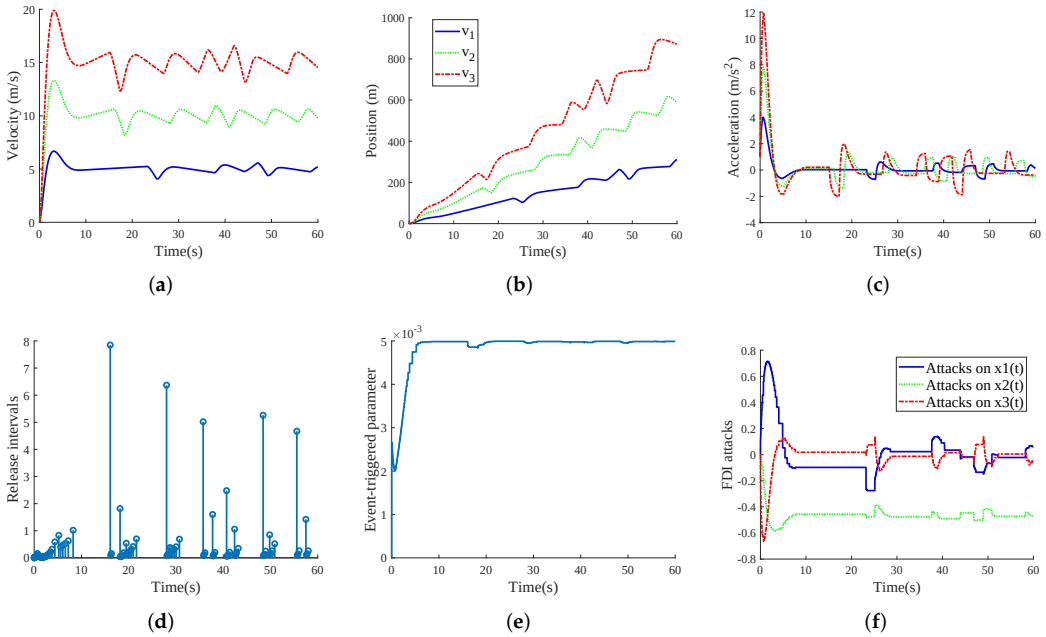


Figure 6. Simulation results under Sigmoid-like ETS and FDI attacks($\theta = 0.2$): velocities (**a**); positions (**b**); accelerations (**c**); release intervals with v_2 (**d**); evolution of $\widetilde{\delta}(t_k h)$ (**e**); signals after FDI attacks (**f**).

For different FDI attack probabilities θ, Table 1 lists the static ETS packets transmitted number N and average transmission period T, the proposed Sigmoid-like ETS packets transmitted number $\widetilde{N}$ and average transmission period $\widetilde{T}$. It can be seen that the Sigmoid-like ETS scheme sends a large number of packets especially when θ is greater than 0.5. In Figure 7, instead, the systems achieve unprecedented stability under high-probability attacks $\theta = 0.7$ since the transmission frequency can be adaptively changed to compensate for the influence of FDI attacks. Higher frequency attacks induce the Sigmoid-like ETS scheme to release a great number of packets, see Figure 7d. Obviously, the static ETS cannot

stabilize the systems with fewer packets. Theorem 2 can solve the controller gain $\mathcal{K}$ until $\theta = 0.8$, which suggests the upper bound of mean-square asymptotic stability.

Table 1. Packets number N, $\widetilde{N}$ and average transmission period T, $\widetilde{T}$ with different θ.

θ	N	$\widetilde{N}$	T	$\widetilde{T}$
0.2	75	114	0.3824	0.2599
0.3	72	111	0.3321	0.2508
0.4	63	118	0.4563	0.2536
0.5	61	158	0.4633	0.1271
0.6	69	418	0.4046	0.0710
0.7	71	2357	0.4189	0.0126
0.8	-	-	-	-

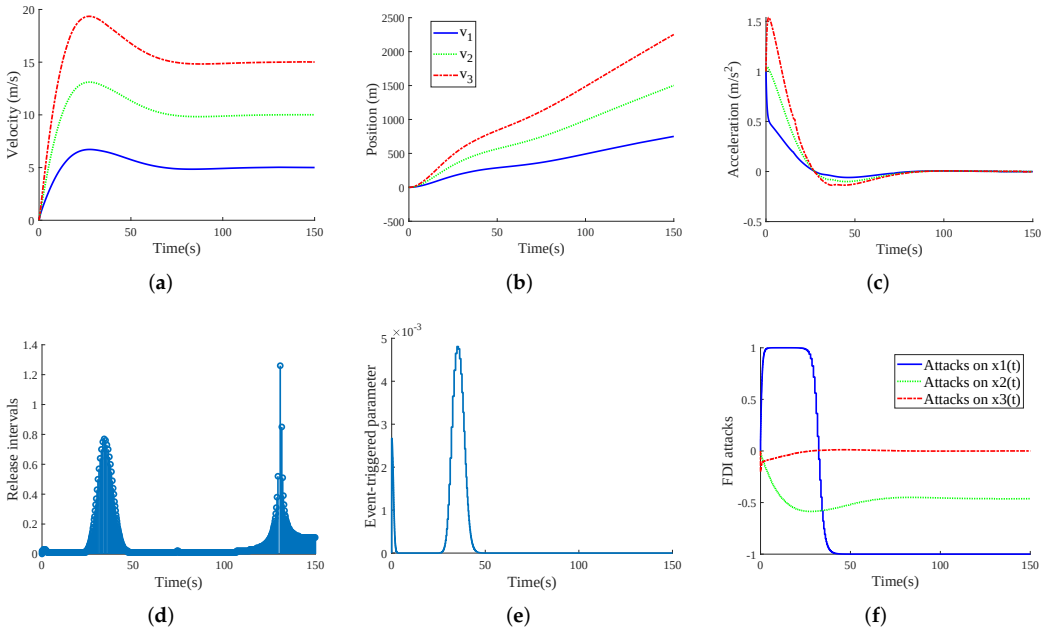


Figure 7. Simulation results under Sigmoid-like ETS and FDI attacks ($\theta = 0.7$): velocities (**a**); positions (**b**); accelerations (**c**); release intervals with v_2 (**d**); evolution of $\widetilde{\delta}(t_k h)$ (**e**); signals after FDI attacks (**f**).

5. Conclusions

A novel Sigmoid-like ETS for networked cruise control under FDI attacks has been proposed in this paper. Based on the proposed Sigmoid-like ETS, the mean-square asymptotical stability and stabilization criteria for the CCSs under a class of stochastic FDI attacks have been well derived by Lyapunov theory and the LMIs technique. In fact, both resource-saving and the security of the CCSs can be guaranteed by using the proposed controller algorithm. Finally, some simulation experiments have been shown to verify the proposed Sigmoid-like ETS. Although the proposed event-triggered controller has some advantages, the proposed Sigmoid-like event-triggered scheme does not guarantee an optimal control performance for CCSs; this is left for our future work.

Author Contributions: Conceptualization, P.Z. and H.S.; methodology, C.P.; software, P.Z.; validation, P.Z.; formal analysis, H.S.; investigation, C.T.; writing—original draft preparation, P.Z.; writing—review and editing, H.S. and C.T.; visualization, P.Z.; supervision, C.P. and H.S.; project administration, H.S.; funding acquisition, C.P., H.S. and C.T. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported in part by the National Natural Science Foundation of China under Grants 62103229, 61833011, 62173218, 62173206, the Natural Science Foundation of Shandong Province under Grant ZR2021QF026, the China Postdoctoral Science Foundation under Grant 2021M692024, 2021M691849, the International Corporation Project of Shanghai Science and Technology Commission under Grant 21190780300, the National Key R & D Program of China under Grant 2021YFE0193900.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: We would like to thank anonymous reviewers for constructive suggestions to improve the quality of this paper.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Plessen, M.; Bernardini, D.; Esen, H.; Bemporad, A. Spatial-based predictive control and geometric corridor planning for adaptive cruise control coupled with obstacle avoidance. *IEEE Trans. Control Syst. Technol.* **2018**, *26*, 38–50. [CrossRef]
2. Dey, K.; Yan, L.; Wang, X.; Wang, Y.; Shen, H.; Chowdhury, M.; Yu, L.; Qiu, C.; Soundararaj, V. A review of communication, driver characteristics, and controls aspects of cooperative adaptive cruise control. *IEEE Trans. Intell. Transp. Syst.* **2016**, *17*, 491–509. [CrossRef]
3. Zhu, Y.; Zhao, D.; Zhong, Z. Adaptive optimal control of heterogeneous CACC system with uncertain dynamics. *IEEE Trans. Control Syst. Technol.* **2019**, *27*, 1772–1779. [CrossRef]
4. Dolk, V.; Heemels, M. Event-triggered control systems under packet losses. *Automatica* **2017**, *80*, 143–155. [CrossRef]
5. Zhang, X.; Wang, Y.; Geng, G.; Yu, J. Delay-optimized multicast tree packing in software-defined networks. *IEEE Trans. Serv. Comput.* **2021**, 1–14. [CrossRef]
6. Ge, X.; Ahmad, I.; Han, Q.-L.; Wang, J.; Zhang, X.-M. Dynamic event-triggered scheduling and control for vehicle active suspension over controller area network. *Mech. Syst. Sig. Process.* **2021**, *152*, 107481. [CrossRef]
7. Peng, C.; Tian, Y.; Yue, D. Output feedback control of discrete-time systems in networked environments. *IEEE Trans. Syst. Man Cybern. A Syst. Humans* **2011**, *41*, 185–190. [CrossRef]
8. Heemels, W.; Donkers, M. Model-based periodic event-triggered control for linear systems. *Automatica* **2013**, *49*, 698–711. [CrossRef]
9. Xu, W.; Ho, D.; Zhong, J.; Chen, B. Event/self-triggered control for leader-following consensus over unreliable network with DoS attacks. *IEEE Trans. Neural Netw. Learn. Syst.* **2019**, *30*, 3137–3149. [CrossRef]
10. Peng, C.; Yang, M.; Zhang, J. Network-based H_∞ control for T-S fuzzy systems with an adaptive event-triggered communication scheme. *Fuzzy Sets Syst.* **2017**, *329*, 61–76. [CrossRef]
11. Dolk, V.; Borgers, D.; Heemels, W.P.M.H. Output-based and decentralized dynamic event-triggered control with guaranteed $\mathcal{L}_p$-gain performance and Zeno-freeness. *IEEE Trans. Autom. Control* **2017**, *62*, 34–49. [CrossRef]
12. Wang, K.; Tian, E.; Liu, J.; Wei, L.; Yue, D. Resilient control of networked control systems under deception attacks: A memory-event-triggered communication scheme. *Int. J. Robust Nonlinear Control* **2020**, *30*, 1534–1548. [CrossRef]
13. Guo, G.; Ding, L.; Han, Q.-L. A distributed event-triggered transmission strategy for sampled-data consensus of multi-agent systems. *Automatica* **2014**, 50, 1489–1496. [CrossRef]
14. Gu, Z.; Park, J.; Yue, D.; Wu, Z.; Xie, X. Event-triggered security output feedback control for networked interconnected systems subject to cyber-attacks. *IEEE Trans. Syst. Man Cybern. Syst.* **2021**, *51*, 6197–6206. [CrossRef]
15. Sun, H.-T.; Peng, C.; Ding, F. Self-discipline predictive control of autonomous vehicles against denial of service attacks. *Asian J. Control* **2022**, 1–14. [CrossRef]
16. Takemori, K.; Mizoguchi, S.; Kawabata, H.; Kubota, A. In-vehicle network security using secure element. *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.* **2016**, *E99.A*, 208–216. [CrossRef]
17. Sun, H.-T.; Peng, C.; Tan, C. Self-discipline predictive control against large-scale packet dropouts using input delay approach. *Int. J. Syst. Sci.* **2022**, *53*, 934–947. [CrossRef]
18. Zivkovic, N.; Saric, A. Detection of false data injection attacks using unscented Kalman filter. *J. Mod. Power Syst. Clean Energy* **2018**, *6*, 847–859. [CrossRef]
19. Deng, R.; Zhuang, P.; Liang, H. CCPA: Coordinated cyber-physical attacks and countermeasures in smart grid. *IEEE Trans. Smart Grid* **2017**, *8*, 2420–2430. [CrossRef]
20. Tian, E.; Peng, C. Memory-based event-triggering H_∞ load frequency control for power systems under deception attacks. *IEEE Trans. Cybern.* **2020**, *50*, 4610–4618. [CrossRef]
21. Sun, H.; Peng, C.; Yue, D.; Wang, Y.; Zhang, T. Resilient load frequency control of cyber-physical power systems under QoS-dependent event-triggered communication. *IEEE Trans. Syst. Man Cybern. Syst.* **2021**, *51*, 2113–2122. [CrossRef]

22. Liu, J.; Gu, Y.; Zha, L.; Liu, Y.; Cao, J. Event-triggered H_∞ load frequency control for multiarea power systems under hybrid cyber attacks. *IEEE Trans. Syst. Man Cybern. Syst.* **2019**, *49*, 1665–1678. [CrossRef]
23. Peng, C.; Yang, T. Event-triggered communication and H_∞ control co-design for networked control systems. *Automatica* **2013**, *49*, 1326–1332. [CrossRef]
24. Musleh, A.; Chen, G.; Dong, Z. A survey on the detection algorithms for false data injection attacks in smart grids. *IEEE Trans. Smart Grid* **2019**, *11*, 2218–2234. [CrossRef]
25. Liu, J.; Xia, J.; Tian, E.; Fei, S. Hybrid-driven-based H_∞ filter design for neural networks subject to deception attacks. *Appl. Math. Comput.* **2018**, *320*, 157–174. [CrossRef]
26. Han, Q.-L. Absolute stability of time-delay systems with sector-bounded nonlinearity. *Automatica* **2005**, *41*, 2171–2176. [CrossRef]