PeerJ Computer Science

System recovery of MIMO nonlinear systems against false data injection attack

Guokai Liang[1], Jiangwei Wu[1], Xuechao Li[1], Shibo Li[1], Jie Zhou[1], Jianxin Zhu[1], Yilong Gao[1], Yanyan Zhang[2] and Zhe Li[3]

[1] Guangzhou Power Supply Bureau, Guangdong Power Grid Co, Guangzhou, China
[2] Ji'an College, Ji'an, China
[3] Hunan University, Changsha, China

ABSTRACT

This article investigates the system recovery problem for a class of multi-input multi-output (MIMO) nonlinear systems under false data injection attack. Under the conditions that the attack is norm-bounded and the system has a vector relative degree and a trivial zero dynamics, the nonlinear system is transformed into a linear one by means of feedback-linearizing design. Then, a high-gain approximate differentiator is adopted to obtain the system states with any arbitrary accuracy. After that, by using a technique of replacing real-time with a small time delay, a recursive attack-compensation input signal is constructed and added into the system input to almost fully compensate for the impact of the attack on the system's transient performance. At this time, the input of the nonlinear system includes two parts: desired input (or called reference input), which is designed according to the nominal model, and additional attack-compensation input. Theoretical analysis shows for the first time that the system can be almost fully recovered in the sense of the mapping relationship between the desired input and nonlinear system states, *i.e.*, the aforementioned mapping is almost the same as the one in the nominal system. Finally, a simulation on a near-space vehicle is provided for verifying the theoretical results.

Subjects Algorithms and Analysis of Algorithms, Data Science
Keywords System recovery, Cyber-physical system, Attack-compensation, False data injection attack, Nonlinear systems, Feedback-linearization

Submitted 30 May 2025
Accepted 18 September 2025
Published 22 October 2025

Corresponding author
Zhe Li, zheli@hnu.edu.cn

Academic editor
Davide Chicco

Additional Information and Declarations can be found on page 20

DOI **10.7717/peerj-cs.3280**

INTRODUCTION

The integration of computation, communication and control units has led to the birth and rapid development of a new generation of intelligent systems (*Khan et al., 2025b*; *Alsinai et al., 2025*), *i.e.*, the cyber-physical systems (CPSs), which have been increasingly used in transportation systems, smart grids, power systems, remote surveillance and other fields (*Cheng, Shi & Sinopoli, 2017*). Due to the openness of information exchange and the complexity of physical dynamics, the long-time running of CPSs may cause security problems (*Alrslani et al., 2025*). Security vulnerabilities of CPSs provide the malicious attackers with the opportunity to implement them with ulterior motives (*Khan et al., 2025a*).

Generally, the cyberattacks can be broadly categorized as three main categories: denial-of-service (DoS) attacks, replay attacks and false data injection (FDI) attacks. DoS attackers obstruct the communication between networked agents (*Wang et al., 2025*). Relay

attackers record and cover the communication data to degrade the system performances (*Markantonakis et al., 2024*). Different from them, FDI attacks, which intend to tamper transmitted data packages causing false feedback information, are more dangerous and complicated (*Li, Shi & Chen, 2018*). For this reason, the researches on CPSs under FDI attacks recently become one of the main topics.

In the past decade, fruitful results have been made for CPSs under attacks on attack strategy design (*Zhang & Ye, 2020b*; *Zhang, Ye & Shi, 2022*), attack detection (*Alfriehat et al., 2024*; *Tanyıldız et al., 2025*), secure estimation (*Sun & Yang, 2025*) and secure control (*Yang et al., 2024*; *Khan et al., 2025c*). To name a few, based on self-generated FDI attacks, *Zhang & Ye (2020b)* proposed a necessary and sufficient condition for attack parameters such that FDI attacks can achieve complete stealthiness. Subsequently, they investigated decentralized FDI attacks that destabilize the estimation error dynamics but eliminate their influences on the residual in each sensor node. *Pasqualetti, Dörfler & Bullo (2013)* designed centralized and distributed attack detection and identification monitors for continuous-time descriptor systems. In addition, secure estimation and secure control have also received great attention, especially in recent years. In *An & Yang (2019)*, with the help of a constrained set partitioning approach, a state estimation scheme was proposed for discrete-time linear CPSs to relieve the computational complexity on the premise of the estimation correctness. Besides, they also investigated the secure control problem for nonlinear interconnected systems against intermittent DoS attacks (*An & Yang, 2018a*). Although these approaches proved their efficiency in attack design, attack detection, secure estimation and secure control, they ignored the impact of the attack on the system itself and did not consider how to recover the system. Actually, depending on desired precision and safety criticality of a system, changes in the transient response can be highly undesirable (*Chakrabortty & Arcak, 2007*, *2009*). This inspired research on performance recovery (*Atassi & Khalil, 1999*).

In the past dozen years, performance recovery for nonlinear control has begun to attract attention in the literature, where the controller recovers the nominal transient trajectory in the presence of plant uncertainties and external disturbances. Such results for certain nonlinear control designs were proved in *Back & Shim (2007*, *2009)*, *Chakrabortty & Arcak (2007*, *2009)*, where singular perturbation methods are adopted to prove performance recovery. However, disturbance and its derivative are assumed to be bounded in *Back & Shim (2007*, *2009)*, and the uncertainty is assumed to be a sufficiently smooth function in *Chakrabortty & Arcak (2007*, *2009)*. Additionally, the tracking problem was studied in *Freidovich & Khalil (2008)* for a partially feedback linearizable single-input-single-output (SISO) nonlinear system with stable zero dynamics, where the closed-loop system under the observer-based controller recovers the performance of the nominal linear model as the observer gain becomes sufficiently high. However, the disturbance and its derivative are required to be bounded. An extension of *Freidovich & Khalil (2008)* to multi-input multi-output (MIMO) nonlinear systems was presented in *Wang, Isidori & Su (2015)* where the system is required to have a well-defined vector relative degree. After that, in

Table 1 Comparisons between the proposed approach and the existing relevant methods.

Methods	Robustness	Strengths or weaknesses
Secure control, *e.g.*, *Back & Shim (2007, 2009)*	Enhancing the robustness of the controller	/
Back & Shim (2007, 2009)	Performance recovery	Disturbance and its derivative are assumed to be bounded
Chakrabortty & Arcak (2007, 2009)	Performance recovery	Uncertainty is assumed to be a sufficiently smooth function
Freidovich & Khalil (2008)	Performance recovery	Disturbance and its derivative are required to be bounded
Wang, Isidori & Su (2015), *Wu et al. (2019)*	Performance recovery	Uncertainty is required to be a smooth function
Our approach	System recovery (enhancing the robustness of the plant)	Only boundedness of the attack is required

order to relax the condition on vector relative degree, *Wu et al. (2019)* investigated the performance recovery for MIMO nonlinear systems under the (substantially weak) assumption of invertibility. One should note that the uncertainty is required to be a smooth function in *Wang, Isidori & Su (2015)*, *Wu et al. (2019)*. Despite these efforts on performance recovery for nonlinear systems, a common drawback of them is that the disturbances or uncertainties are differentiable, even smooth. For the attack signal, it is deliberately designed by hackers to harm the system. Thus, the attack signal may be a discontinuous and fast changing signal. This feature makes the existing results on performance recovery cannot be applied to CPSs under FDI attacks without assumption on its derivative, and to our knowledge, there is still no result available on system recovery problem of CPSs under attacks. This motivates the present study.

To more intuitively demonstrate the necessity of researching the system recovery problem for MIMO nonlinear systems under attack, Table 1 compares the proposed approach with existing methods.

This article deals with the system recovery problem for a class of MIMO nonlinear systems subject to FDI attacks without assumption on its derivative. The system under consideration has a vector relative degree and a trivial zero dynamics, which can be transformed into a linear one by means of feedback-linearizing design. Then, a recursive attack-compensation input signal is constructed skillfully and added into the system input to almost fully compensate the attack, so that the system can be almost fully recovered. Compared to the existing results, our approach consists of the following main contributions and advantages: (i) A new perspective is provided for designing attack compensation scheme by compensating for the state deviation caused by the attack, which is helpful for designing an attack-compensated signal to recover the system. In fact, unlike the existing methods that enhance the robustness of control algorithms (*e.g.*, *Yang et al., 2024*), the proposed method enhances the robustness of the plant itself; (ii) The existing results on CPSs mainly focus on attack design, attack detection, state estimation and secure control, but do not consider the state deviation of the system caused by the attack. In contrast, this article systematically investigates the recovery of CPSs under attacks for the first time; (iii) A common limitation of performance recovery for nonlinear system is that

disturbances or uncertainties are required to be differentiable, even smooth (*Back & Shim, 2007*, *2009*; *Chakrabortty & Arcak, 2007*, *2009*; *Freidovich & Khalil, 2008*; *Wang, Isidori & Su, 2015*; *Wu et al., 2019*). Unlike disturbances and uncertainties, the attacks under consideration are not restricted to be differentiable or smooth.

Notations: Let $O(T)$ represent the infinitesimal of the same order as T. For a matrix A, let A' denote its transpose and $\lambda_{\min}(A)$ denote its minimum eigenvalue. $L_f h(x) \triangleq \frac{\partial h}{\partial x} f(x)$ is called the *Lie Derivative* of h with respect to f. For any positive integer r, A_r denotes a shift matrix of $r \times r$ dimension, $B_r \triangleq [0, \ldots, 0, 1]' \in \mathbb{R}^d$, and $C_r \triangleq [1, 0, \ldots, 0] \in \mathbb{R}^{1\times d}$. For a matrix b, the notation b^+ represents the pseudo-inverse.

PROBLEM STATEMENT

Consider the system recovery problem of the following MIMO nonlinear systems under FDI attack,

$$\dot{x} = f(x) + g(x)(u + u_a), \quad y = h(x), \tag{1}$$

where $x \in \mathbb{R}^n$, $u \in \mathbb{R}^m$ and $y \in \mathbb{R}^q$ denote the state vector, the control input and the output, respectively. $f(x)$, $g(x) = [g_1(x), \ldots, g_m(x)]$ and $h(x) = [h_1(x), \ldots, h_q(x)]' = [y_1, \ldots, y_q]'$ are known smooth mappings with $f(0) = 0$ and $h(0) = 0$. The vector $u_a \in \mathbb{R}^m$ denotes the norm bounded FDI attack (*Zhang & Ye, 2020b*; *Zhang, Ye & Shi, 2022*), which is injected into the system by a malicious attacker.

Remark 1. *Although u_a represents an attack in this article, it can also be used to represent actuator faults, process faults, additive uncertainties, unknown inputs, external disturbances, or a combination of them (Arab et al., 2025).*

Definition 1. *(Isidori, 1985) A multivariable nonlinear system of the form Eq. (1) has a vector relative degree $\{r_1, \ldots, r_q\}$ at a point x_0 if the following two conditions hold:*

(i) for all $1 \le j \le m$, $k < r_i - 1$, $1 \le i \le q$, and for all x in a neighborhood of x_0, the following Lie Derivative

$$L_{g_j} L_f^k h_i(x) = 0 \tag{2}$$

holds where $L_f^k h_i(x) \triangleq L_f L_f^{k-1} h_i(x)$.

(ii) the $q \times m$ matrix

$$b(x) = \begin{bmatrix} L_{g_1} L_f^{r_1-1} h_1(x) & \cdots & L_{g_m} L_f^{r_1-1} h_1(x) \\ L_{g1} L_f^{r_2-1} h_2(x) & \cdots & L_{g_m} L_f^{r_2-1} h_2(x) \\ \vdots & \vdots & \vdots \\ L_{g_1} L_f^{r_q-1} h_q(x) & \cdots & L_{g_m} L_f^{r_q-1} h_q(x) \end{bmatrix} \tag{3}$$

is row full rank at $x = x_0$.

Assumption 1. *The system Eq. (1) has a vector relative degree $\{r_1, \ldots, r_q\}$ for all $x \in \mathbb{R}^n$, and has a trivial zero dynamics.*

Under Assumption 1, with the help of the Structure Algorithm (*Teel & Praly, 1995*; *Freidovich & Khalil, 2008*), there exist a diffeomorphism

$$\Phi(x) = \begin{bmatrix} h_1(x) \\ L_f h_1(x) \\ \vdots \\ L_f^{r_1-1} h_1(x) \\ \vdots \\ h_q(x) \\ L_f h_q(x) \\ \vdots \\ L_f^{r_q-1} h_q(x) \end{bmatrix} \tag{4}$$

which brings the system Eq. (1) to the system modeled by equations of the normal form:

$$\begin{cases} \dot{x}_{1,i} &= x_{1,i+1}, \quad \forall 1 \le i \le r_1 - 1 \\ \dot{x}_{1,r_1} &= a_1(x) + b_1(x)(u + u_a) \\ y_1 &= x_{1,1} \end{cases}$$
$$\begin{cases} \dot{x}_{2,i} &= x_{2,i+1}, \quad \forall 1 \le i \le r_2 - 1 \\ \dot{x}_{2,r_2} &= a_2(x) + b_2(x)(u + u_a) \\ y_2 &= x_{2,1} \end{cases}$$
$$\begin{cases} \dot{x}_{k,i} &= x_{k,i+1}, \quad \forall 1 \le i \le r_k - 1 \\ \dot{x}_{k,r_k} &= a_k(x) + b_k(x)(u + u_a) \\ y_k &= x_{k,1} \end{cases} \tag{5}$$

with $k = 3, \ldots, q$, $r_1 + r_2 + \cdots + r_q = n$, where $b_k(x)$ is the k-th row of $b(x)$ and $\Phi(x) = [x_{1,1}, \ldots, x_{1,r_1}, \ldots, x_{q,1}, \ldots, x_{q,r_q}]'$.

Assumption 2. *There exists a positive constant number b_{max} such that*

$$\|b(x)\| \le b_{\max}. \tag{6}$$

Remark 2. *For Assumption 1, some practical systems are capable of meeting it, such as high-speed train system (Zhang et al., 2024; Xie et al., 2025) and near-space vehicle system (Yao, Tao & Jiang, 2016). In addition, Assumption 2 can be found in Back & Shim (2007), Freidovich & Khalil (2008), Wang, Isidori & Su (2015), and this assumption is necessary to ensure the boundness of the signal $b(x)u_a$ which is injected into the nominal system by the attacker.*

By feedback linearization, the input u of the system Eq. (5), which is also the input of the system Eq. (1), is designed against the attack as

$$u = b^+(x)[-a(x) + v + v_c] = \underbrace{b^+(x)[-a(x) + v]}_{u_d} + \underbrace{b^+(x)v_c}_{u_c} \tag{7}$$

with $a(x) = [a_1(x), \ldots, a_q(x)]'$, where u_d denotes the desired input (or called reference input) which is designed according to the nominal model, and u_c is the attack-compensation signal which is added into the system input and will be designed skillfully to almost fully compensate the attack u_a.

Under the above system input Eq. (7), the input-output model Eq. (5) will be transformed into the following linear one

$$\dot{\xi} = A\xi + B[v + (v_c + a)], \quad y = C\xi, \tag{8}$$

where $a \triangleq b(x)u_a$, $\xi \triangleq [x_{1,1}, \ldots, x_{1,r_1}, \ldots, x_{q,1}, \ldots, x_{q,r_q}]'$, $A \triangleq \text{blkdiag}(A_{r_1}, \ldots, A_{r_q})$, $B \triangleq \text{blkdiag}(B_{r_1}, \ldots, B_{r_q})$, $C \triangleq \text{blkdiag}(C_{r_1}, \ldots, C_{r_q})$, and the operator blkdiag$(\cdot)$ builds a block diagonal matrix from its argument. Furthermore, one can check that a is bounded under Assumption 2.

For convenience of expression, let x_n, ξ_n and y_n denote the nominal values of x, ξ and y respectively (*i.e.*, the values in the attack-free system or called the values in the nominal system). That is, x_n, ξ_n and y satisfy

$$\dot{x}_n = f(x_n) + g(x_n)u, \quad \dot{\xi}_n = A\xi_n + Bv, \quad y_n = C\xi_n \tag{9}$$

with $x_n(t_0) = x(t_0)$ and $\xi_n(t_0) = \xi(t_0)$.

Design objective: The purpose of this article is to design the additional attack-compensation input u_c in Eq. (7) for the MIMO nonlinear system Eq. (1) such that the mapping relationship between the desired input u_d and system states x is almost the same as the one in the nominal system. In other words, the attack is almost fully compensated such that the system under consideration is almost recovered.

For the linear system Eq. (8), since $CB = 0$ which violates the observer matching condition (*Corless & Tu, 1998*), the attack-related term a is hard to be estimated and compensated effectively by the existing results. Fortunately, this system has another obvious feature which makes it possible to almost completely compensate for the attacks-related term a. That is, all states of the linear system Eq. (8) are derivatives of the output, *i.e.*, $x_{i,j} = y_i^{(j-1)}$ for all $i = 1, \ldots, q$ and $j = 1, \ldots, r_i$. Many approaches (*e.g.*, high-gain approximate differentiators (*Kalsi et al., 2010*) and sliding mode exact differentiator (*Floquet, Edwards & Spurgeon, 2007*)) have been proposed to obtain the estimation of system states. As in *Kalsi et al. (2010)*, the following lemma is established to obtain the system states with any arbitrary accuracy.

Lemma 1. *(Kalsi et al., 2010) Consider the linear system Eq. (8). For the following high-gain observer Eq. (10) under Assumptions 1–2 and the boundness of ξ, there exist a positive constant β_i and a finite time $T_i(\varepsilon)$ such that $\|\zeta_i\| \leq \beta_i \varepsilon$ for $t \geq t_0 + T_i(\varepsilon)$ where t_0 denotes the start time of the system Eq. (1). Moreover, $\lim_{\varepsilon \to 0^+} T_i(\varepsilon) = 0$.*

$$\begin{cases} \dot{x}_{i,h} &= A_{r_i} x_{i,h} + B_{r_i} v + l_i (y_i - y_{i,h}) \\ y_{i,h} &= C_{r_i} x_{i,h} \end{cases} \tag{10}$$

with $l_i \triangleq [\alpha_{i,1}/\varepsilon, \ldots, \alpha_{i,r_i}/\varepsilon^{r_i}]'$, where $x_{i,h} \triangleq [x_{i,1,h}, \ldots, x_{i,r_i,h}]'$ denotes the estimation of $x_i \triangleq [x_{i,1}, \ldots, x_{i,r_i}]'$, $\varepsilon \in (0,1)$ and $\alpha_{i,j}$ are selected such that the roots of $s^{r_i} + \alpha_{i,1} s^{r_i - 1} + \cdots + \alpha_{i,r_i} = 0$ have negative real part. $\zeta_i = [\zeta_{i,1}, \ldots, \zeta_{i,r_i}]'$ is defined with $\zeta_{i,j} = (x_{i,j} - x_{i,j,h})/\varepsilon^{r_i - j}$.

Obviously, one can see easily from Lemma 1 that $x_{i,j}$ can be replaced by $x_{i,j,h}$ with any arbitrary accuracy. For this reason and the convenience of description, it is reasonable to

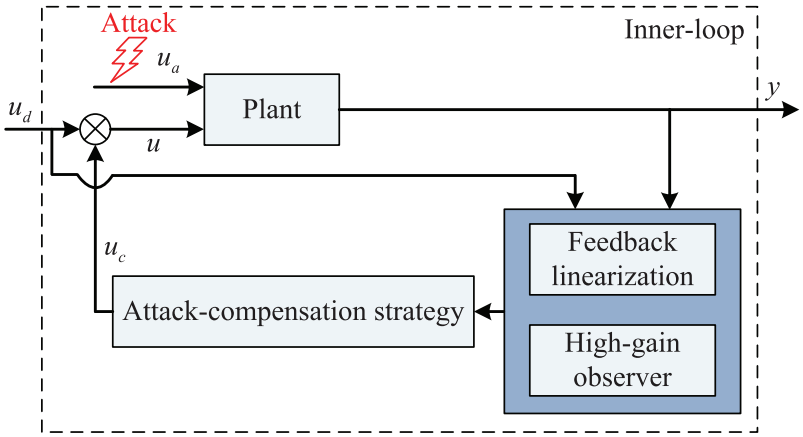

Figure 1 **Block diagram of the proposed system recovery strategy.**
Full-size DOI: 10.7717/peerj-cs.3280/fig-1

assume that ξ is available for system recovery design. Also, the system input Eq. (7) can be rewritten as

$$u = \underbrace{b^+(\Phi^{-1}(\xi))[-a(\Phi^{-1}(\xi)) + v]}_{u_d} + \underbrace{b^+(\Phi^{-1}(\xi))v_c}_{u_c} \tag{11}$$

where $\Phi^{-1}(\cdot)$ represents the inverse operator of $\Phi(\cdot)$.

In order to show the proposed system recovery strategy more clearly, its block diagram is drawn in Fig. 1. The proposed attack-compensation strategy has the following obvious feature: it is an inner-loop controller so that it can be added on the existing closed-loop system working in harmony with a pre-designed outer-loop controller.

SYSTEM RECOVERY DESIGN IN A RECURSIVE FASHION

Define an auxiliary variable $\eta = [\eta_1, \ldots, \eta_q]'$ with

$$\eta_i \triangleq \ell_{i,1} y_i + \ell_{i,2} y_i^{(1)} + \cdots + \ell_{i,r_i-1} y_i^{(r_i-2)} + y_i^{(r_i-1)}, \tag{12}$$

for all $1 \leq i \leq q$, where the parameters $\ell_{i,1}, \ldots, \ell_{i,r_i-1}$ are selected such that the roots of the equation $\ell_{i,1} + \ell_{i,2} s + \cdots + \ell_{i,r_i-1} s^{r_i-2} + s^{r_i-1} = 0$ have negative real parts.

Obviously, η can be rewritten as

$$\eta = L\xi \tag{13}$$

where $L \triangleq \text{blkdiag}(L_1, \ldots, L_q)$ with $L_i \triangleq [\ell_{i,1}, \ldots, \ell_{i,r_i-1}, 1]$.

According to the knowledge of calculus, η meets

$$\eta(t) = Le^{A}(t - t_0)\xi(t_0) + \int_{t_0}^{t} Le^{A(t-\tau)} B[v(\tau) + v_c(\tau) + a(\tau)]d\tau \tag{14}$$

where t_0 denotes the start time of the system under consideration.

Before analyzing the impact of attacks on the original nonlinear system Eq. (1), we first analyze the impact of attacks on auxiliary variable η which will provide great convenience

for analyzing the original system. So let's start now. If $v_c(t)$ can fully compensate for the impact of the attack on the auxiliary variable η, the following condition must be satisfied obviously.

$$\int_{t_0}^{t} Le^{A(t-\tau)}B[v_c(\tau)+a(\tau)]d\tau \equiv 0, \forall t \geq t_0 \tag{15}$$

that is, $v_c(t)+a(t) \equiv 0, \forall t \geq t_0$. In other words, $a(t)$ is required to be known in real-time *a priori*. Nevertheless, this condition is too strict for many practical systems, and thus, the following problem will naturally be encountered: whether the impact of the attack on the auxiliary variable η can be compensated by removing the aforementioned restriction? The answer happens to be yes, and we will show that the impact of the attack on η can almost completely compensated by a skillfully designed attack-compensation input signal $v_c(t)$.

The design process of the attack-compensation input signal includes the following two steps.

Step 1: Removing the strict requirements of real-time.

In order to eliminate the strict requirement of real-time, small time-delay will be adopted to replace real-time. In details, for the auxiliary variable η in Eq. (14), we divide the whole time-domain of the right-hand side into interval segments with period $T>0$, as follows

$$\begin{aligned}
\eta(nT+t_0) &= Le^{A(nT)}\xi(t_0) + \int_{t_0}^{nT+t_0} Le^{A(nT+t_0-\tau)}Bv(\tau)d\tau + \int_{t_0}^{nT+t_0} Le^{A(nT+t_0-\tau)}B[v_c(\tau) \\
&\quad + a(\tau)]d\tau = Le^{A(nT)}\xi(t_0) + \int_{t_0}^{nT+t_0} Le^{A(nT+t_0-\tau)}Bv(\tau)d\tau \\
&\quad + \int_{t_0}^{T+t_0} Le^{A(nT+t_0-\tau)}Bv_c(\tau)d\tau + \int_{T+t_0}^{2T+t_0} Le^{A(nT+t_0-\tau)}Bv_c(\tau)d\tau + \cdots \\
&\quad + \int_{kT+t_0}^{(k+1)T+t_0} Le^{A(nT+t_0-\tau)}Bv_c(\tau)d\tau + \cdots + \int_{(n-1)T+t_0}^{nT+t_0} Le^{A(nT+t_0-\tau)}Bv_c(\tau)d\tau \\
&\quad + \int_{t_0}^{T+t_0} Le^{A(nT+t_0-\tau)}Ba(\tau)d\tau + \int_{T+t_0}^{2T+t_0} Le^{A(nT+t_0-\tau)}Ba(\tau)d\tau + \cdots \\
&\quad + \int_{kT+t_0}^{(k+1)T+t_0} Le^{A(nT+t_0-\tau)}Ba(\tau)d\tau + \cdots + \int_{(n-1)T+t_0}^{nT+t_0} Le^{A(nT+t_0-\tau)}Ba(\tau)d\tau
\end{aligned} \tag{16}$$

where n represents any positive integer and the positive constant T is called the period of compensation signal. Also, T is a small positive constant which denotes the small time-delay.

To remove the strict requirement of real-time, one way is to adopt $v_c(t)$ in the interval $t \in [kT+t_0, (k+1)T+t_0)$ for compensating the impact of $a(t)$ on auxiliary variable η in the interval $t \in [(k-1)T+t_0, kT+t_0)$ (please see Fig. 2). Obviously, by choosing a small T, the attack can still be compensated timely to avoid the continuous impact of the attack on the auxiliary variable η. According to this design thinking, $\forall k \in \{0,1,2,\cdots\}$, let

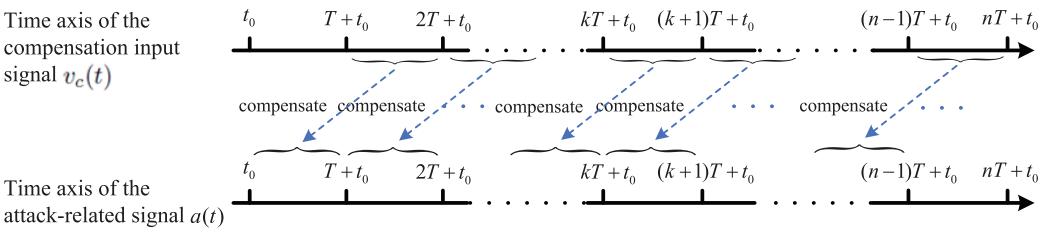

Figure 2 **Block diagram of the attack-compensation strategy based on a small time-delay.**
Full-size DOI: 10.7717/peerj-cs.3280/fig-2

$$\int_{kT+t_0}^{(k+1)T+t_0} Le^{A(nT+t_0-\tau)}Bv_c(\tau)d\tau + \int_{(k-1)T+t_0}^{kT+t_0} Le^{A(nT+t_0-\tau)}Ba(\tau)d\tau = 0. \tag{17}$$

Under Eq. (17), one has

$$\eta(nT+t_0)=Le^{A(nT)}\xi(t_0)+\int_{t_0}^{nT+t_0} Le^{A(nT+t_0-\tau)}Bv(\tau)d\tau+\int_{(n-1)T+t_0}^{nT+t_0} Le^{A(nT+t_0-\tau)}a(\tau)d\tau. \tag{18}$$

Obviously, when T is small enough, $\eta(nT+t_0) \approx Le^{A(nT)}\xi(t_0) + \int_{t_0}^{nT+t_0} Le^{A(nT+t_0-\tau)} Bv(\tau)d\tau$. One can see that, at time instants $t = nT + t_0, \forall n \in \mathbb{N}$, the auxiliary variable η is almost the same as the one in the nominal system (when the system is not attacked). Thus, at time instants $t = nT + t_0, \forall n \in \mathbb{N}$, the attack-compensation input signal $v_c(t)$ defined in Eq. (17) can almost eliminate the impact of $a(t)$ on the auxiliary variable η with a small time-delay T. It should be pointed out that the same result can be guaranteed for the interval $(nT + t_0, (n + 1)T + t_0), \forall n \in \mathbb{N}$ which will be proved in the next section.

By some mathematical calculation, Eq. (17) can be rewritten for all $k \in \{0, 1, 2, \ldots\}$ as

$$e^{A(n-k)T}\int_{kT+t_0}^{(k+1)T+t_0} Le^{A(kT+t_0-\tau)}Bv_c(\tau)d\tau + e^{A(n-k)T}\int_{(k-1)T+t_0}^{kT+t_0} Le^{A(kT+t_0-\tau)}Ba(\tau)d\tau = 0 \tag{19}$$

which is equivalent to

$$\int_0^T Le^{-A\tau}Bv_c(kT+t_0+\tau)d\tau + \int_{(k-1)T+t_0}^{kT+t_0} Le^{A(kT+t_0-\tau)}Ba(\tau)d\tau = 0. \tag{20}$$

Let $v_c(kT + t_0 + \tau) = -B'e^{-A'\tau}L'\bar{v}_c(k), \tau \in (0, T)$. By substituting it into Eq. (20), one has

$$\bar{v}_c(k) = -\left(\int_0^T Le^{-A\tau}BB'e^{-A'\tau}L'd\tau\right)^{-1}\int_{(k-1)T+t_0}^{kT+t_0} Le^{A(kT+t_0-\tau)}Ba(\tau)d\tau \tag{21}$$

where we have used the fact that $\int_0^T Le^{-A\tau}BB'e^{-A'\tau}L'd\tau$ is invertible since the pair (A, B) is controllable and L is row full rank. Therefore, it is pretty easy to obtain for all $k \in \{0, 1, 2, \ldots\}$ and $\tau \in (0, T)$ that

$$v_c(kT+t_0+\tau)=-B'e^{-A'\tau}L'\left(\int_0^T Le^{-A\tau}BB'e^{-A'\tau}L'd\tau\right)^{-1}\int_{(k-1)T+t_0}^{kT+t_0} Le^{A(kT+t_0-\tau)}Ba(\tau)d\tau \tag{22}$$

which is equivalent to

$$v_c(\tau) = -B'e^{A'(kT+t_0-\tau)}L'\left(\int_0^T Le^{-A\tau}BB'e^{-A'\tau}L'd\tau\right)^{-1}\int_{(k-1)T+t_0}^{kT+t_0} Le^{A(kT+t_0-\tau)}Ba(\tau)d\tau \quad (23)$$

holds for all $k \in \{0,1,2,\ldots\}$ and $\tau \in (kT+t_0,(k+1)T+t_0)$. Unfortunately, $\int_{(k-1)T+t_0}^{kT+t_0} Le^{A(kT+t_0-\tau)}Ba(\tau)d\tau$ in Eq. (23) is not directly implementable if the attack signal is unknown. In the following Step 2, we will propose an alternative approach to solve the above problem.

Step 2: An alternative approach for solving the term $\int_{(k-1)T+t_0}^{kT+t_0} Le^{A(kT+t_0-\tau)}Ba(\tau)d\tau$.

It is easy to get from Eq. (8) that

$$\int_{(k-1)T+t_0}^{kT+t_0} Le^{A(kT+t_0-\tau)}Ba(\tau)d\tau = L\xi(kT+t_0) - Le^{AT}\xi((k-1)T+t_0) - \int_{(k-1)T+t_0}^{kT+t_0} Le^{A(kT+t_0-\tau)}B[v(\tau)+v_c(\tau)]d\tau\,. \quad (24)$$

With the help of Steps 1–2, and by combining Eqs. (23) and (24), one can obtain the following causal and implementable recursive attack-compensation input signal

$$v_c(t) = -B'e^{A'(kT+t_0-t)}L'\left(\int_0^T Le^{-A\tau}BB'e^{-A'\tau}L'd\tau\right)^{-1}\left[L\xi(kT+t_0) - Le^{AT}\xi((k-1)T+t_0) - \int_{(k-1)T+t_0}^{kT+t_0} Le^{A(kT+t_0-\tau)}B(v(\tau)+v_c(\tau))d\tau\right] \quad (25)$$

which holds for all $k \in \{0,1,2,\ldots\}$ and $t \in (kT+t_0,(k+1)T+t_0)$.

Remark 3. *The term of $\int_0^T Le^{-A\tau}BB'e^{-A'\tau}L'd\tau$ is an infinitesimal of the same order as T. Thus, ill-conditioned matrix inversion will not be occurred in the calculation process of $(\int_0^T Le^{-A\tau}BB'e^{-A'\tau}L'd\tau)^{-1}$.*

Remark 4. *One can see from Eq. (23) that $v_c(t) \equiv 0$ when $a(t) \equiv 0$, which implies that $u_c \equiv 0$ when $u_a \equiv 0$. Therefore, the attack-compensation input signal will be disappeared and doesn't change any system dynamics when the system is not attacked. This reflects one of the merits of the proposed method: it is easy to implement in practical systems.*

Note that, the boundness of ξ is required to be satisfied *a priori* of the high-gain observer Eq. (10) in Lemma 1. This condition is quite easy to satisfy, as will be proved in the following.

Theorem 1. *Consider the linear system Eq. (8), and the attack-compensation input signal Eq. (25). Under the assumptions that the FDI attack signal is norm-bounded and v stabilizes the following system Eq. (28), then ξ and v_c are both uniformly bounded.*

Proof On the one hand, for $t \in (kT+t_0,(k+1)T+t_0)$, one can see from Eq. (23) that

$$\begin{aligned}\|v_c(t)\| &\le \max_{\tau\in[0,T]}\|B'e^{-A'\tau}L'\|\left\{T\min_{\tau\in[0,T]}\|Le^{-A\tau}BB'e^{-A'\tau}L'\|\right\}^{-1}T\max_{\tau\in[0,T]}\|Le^{A\tau}B\| \\ &\times \max_{\tau\in[(k-1)T+t_0,kT+t_0]}\|a(t)\| \\ &= \frac{\max_{\tau\in[0,T]}\|B'e^{-A'\tau}L'\|\times\max_{\tau\in[0,T]}\|Le^{A\tau}B\|}{\min_{\tau\in[0,T]}\|Le^{-A\tau}BB'e^{-A'\tau}L'\|}\max_{\tau\in[(k-1)T+t_0,kT+t_0]}\|a(t)\| \end{aligned} \tag{26}$$

which implies that the signal $v_c(t)$ is uniformly bounded. Also, one can further check that

$$\lim_{T\to 0}\min_{\tau\in[0,T]}\|Le^{-A\tau}BB'e^{-A'\tau}L'\| = 1. \tag{27}$$

On the other hand, let's consider the linear system Eq. (8), which can be rewritten as

$$\dot{\xi} = A\xi + Bv + d \tag{28}$$

where the pair (A, B) is controllable, and $d \triangleq B(v_c + a)$ is bounded since v_c and a are both bounded. Thus, according to Lyapunov stability theorem, it is pretty easy to see that ξ is uniformly bounded when v stabilizes the system Eq. (28).

STABILITY ANALYSIS

In this section, the stability of the original nonlinear system Eq. (1) with the system input Eq. (11) will be established.

Let η_n denote the nominal value of the signal η. That is,

$$\eta_n = L\xi_n \tag{29}$$

with $\eta_n(t_0) = \eta(t_0)$.

Now, let us analyze the impact of the attacks on the auxiliary variable η.

Theorem 2. *Consider the linear system Eq. (8), and the attack-compensation input signal Eq. (25). Under Assumptions 1–2 and the assumption that v stabilizes the system Eq. (28), then there exists an upper bound of $\|\tilde{\eta}(t)\|$ which is an infinitesimal of the same order as T, where $\tilde{\eta}(t) \triangleq \eta(t) - \eta_n(t)$ denotes the deviation caused by the attack. Also, $\tilde{\eta}(t)$ can be arbitrary small when a small enough period T is selected.*

Proof The proof is divided into the following two cases: (1) $t = kT + t_0$; and (2) $t \in (kT + t_0, (k+1)T + t_0)$.

Case 1: $t = kT + t_0$. It is quite natural to obtain from Eqs. (8), (9), (14) and (29) that

$$\begin{aligned}\|\tilde{\eta}(kT+t_0)\| &= \left\|Le^{A(kT)}\tilde{\xi}(t_0) + \int_{(k-1)T+t_0}^{kT+t_0} Le^{A(kT+t_0-\tau)}Ba(\tau)d\tau\right\| \\ &= \left\|\int_{(k-1)T+t_0}^{kT+t_0} Le^{A(kT+t_0-\tau)}Ba(\tau)d\tau\right\| \\ &\le T\times\max_{\tau\in[0,T]}\|Le^{A\tau}B\|\times\max_{\tau\in[(k-1)T+t_0,kT+t_0]}\|a(t)\| \end{aligned} \tag{30}$$

where $\tilde{\xi} \triangleq \xi - \xi_n$.

Case 2: $t \in (kT + t_0, (k+1)T + t_0)$. One can see from Eqs. (14) and (29) that

$$\begin{aligned}\tilde{\eta}(t) &= Le^{A(t-t_0)}\tilde{\xi}(t_0) + \int_{t_0}^{t} Le^{A(t-\tau)}B[v_c(\tau)+a(\tau)]d\tau \\ &= \int_{t_0}^{t_0+T} Le^{A(t-\tau)}Bv_c(\tau)d\tau + \cdots + \int_{kT+t_0}^{(k+1)T+t_0} Le^{A(t-\tau)}Bv_c(\tau)d\tau \\ &- \int_{t}^{(k+1)T+t_0} Le^{A(t-\tau)}Bv_c(\tau)d\tau + \int_{t_0}^{T+t_0} Le^{A(t-\tau)}Ba(\tau)d\tau + \cdots \\ &+ \int_{(k-1)T+t_0}^{kT+t_0} Le^{A(t-\tau)}Ba(\tau)d\tau + \int_{kT+t_0}^{t} Le^{A(t-\tau)}Ba(\tau)d\tau \\ &= -\int_{t}^{(k+1)T+t_0} Le^{A(t-\tau)}Bv_c(\tau)d\tau + \int_{kT+t_0}^{t} Le^{A(t-\tau)}Ba(\tau)d\tau \end{aligned} \tag{31}$$

Therefore, with the help of Eq. (23), the deviation $\tilde{\eta}(t)$ satisfies

$$\begin{aligned}\|\tilde{\eta}(t)\| &\le \left\| \int_{t}^{(k+1)T+t_0} Le^{A(t-\tau)}Bv_c(\tau)d\tau \right\| + \left\| \int_{kT+t_0}^{t} Le^{A(t-\tau)}Ba(\tau)d\tau \right\| \\ &\le \left\| \int_{t}^{(k+1)T+t_0} Le^{A(t-\tau)}Bv_c(\tau)d\tau \right\| + T\max_{\tau\in[0,T]}\|Le^{A\tau}B\| \times \max_{\tau\in[kT+t_0,(k+1)T+t_0]}\|a(\tau)\| \end{aligned} \tag{32}$$

where the first term on the right-hand side of the above inequality for $t \in (kT+t_0, (k+1)T+t_0)$ obeys that

$$\begin{aligned}\left\| \int_{t}^{(k+1)T+t_0} Le^{A(t-\tau)}Bv_c(\tau)d\tau \right\| &= \left\| \int_{t}^{(k+1)T+t_0} Le^{A(t-\tau_1)}BB'e^{A'(kT+t_0-\tau_1)}L' \right. \\ &\quad \times \left(\int_0^T Le^{-A\tau}BB'e^{-A'\tau}L'd\tau \right)^{-1} \left. \int_{(k-1)T+t_0}^{kT+t_0} Le^{A(kT+t_0-\tau_2)}Ba(\tau_2)d\tau_2 d\tau_1 \right\| \\ &\le \int_{t}^{(k+1)T+t_0} \left\| Le^{A(t-\tau_1)}BB'e^{A'(kT+t_0-\tau_1)}L' \right\| d\tau_1 \left\| \left(\int_0^T Le^{-A\tau}BB'e^{-A'\tau}L'd\tau \right)^{-1} \right\| \\ &\quad \times \left\| \int_{(k-1)T+t_0}^{kT+t_0} Le^{A(kT+t_0-\tau_2)}Ba(\tau_2)d\tau_2 \right\| \\ &\le \max_{\tau_1,\tau_2\in[0,T]} \|Le^{-A\tau_1}BB'e^{-A'\tau_2}L'\| \max_{\tau\in[0,T]}\|Le^{A\tau}B\| \\ &\quad \times \max_{\tau\in[(k-1)T+t_0,kT+t_0]}\|a(\tau)\| T^2 \left\| \int_0^T Le^{-A\tau}BB'e^{-A'\tau}L'd\tau \right\|^{-1}. \end{aligned} \tag{33}$$

Combining Eqs. (32) and (33), one can conclude that

$$\begin{aligned}\|\tilde{\eta}(t)\| &\le T \times \max_{\tau\in[0,T]}\|Le^{A\tau}B\| \times \max_{\tau\in[kT+t_0,(k+1)T+t_0]}\|a(\tau)\| + T^2\Delta^{-1}(T) \\ &\quad \times \max_{\tau_1,\tau_2\in[0,T]} \|Le^{-A\tau_1}BB'e^{-A'\tau_2}L'\| \times \max_{\tau\in[0,T]}\|Le^{A\tau}B\| \times \max_{\tau\in[(k-1)T+t_0,kT+t_0]}\|a(\tau)\| \end{aligned} \tag{34}$$

holds for $t \in (kT+t_0, (k+1)T+t_0)$, where $\Delta(T) \triangleq \| \int_0^T Le^{-A\tau}BB'e^{-A'\tau}L'd\tau \|$.

To sum up, one can conclude from Cases 1-2 that the deviation $\tilde{\eta}(t)$ satisfies

$$\begin{aligned}\|\tilde{\eta}(t)\| &\leq T\max_{\tau\in[0,T]}\|Le^{A\tau}B\|\times\max_{\tau\in[(k-1)T+t_0,(k+1)T+t_0]}\|a(\tau)\|+T^2\Delta(T)^{-1}\\&\times\max_{\tau_1,\tau_2\in[0,T]}\|Le^{-A\tau_1}BB'e^{-A'\tau_2}L'\|\times\max_{\tau\in[0,T]}\|Le^{A\tau}B\|\times\max_{\tau\in[(k-1)T+t_0,kT+t_0]}\|a(\tau)\|\\&=O(T)\end{aligned}\tag{35}$$

where we have used the fact that $\Delta(T)=O(T)$, and $a=b(x)u_a$ is bounded under Assumption 2. The right-hand side of the above inequality is an infinitesimal of the same order as T, and thus $\tilde{\eta}(t)$ can be arbitrary small when a small enough period T is chosen. Hence, the proof is completed.

In the sequel, let us analyze the impact of attacks on the linear system Eq. (8).

Theorem 3. *Consider the linear system Eq. (8), and the attack-compensation input signal Eq. (25). Under assumptions of Theorem 2, then there exists an upper bound of $\|\tilde{x}_{i,j}(t)\|$ which is an infinitesimal of the same order as T, where $\tilde{x}_{i,j}(t)\triangleq x_{i,j}(t)-x_{i,j,n}(t)$ denotes the state deviation caused by the attack and $x_{i,j,n}(t)$ represents the nominal value of $x_{i,j}(t)$ (i.e., the value in the attack-free system). Also, $\|\tilde{x}_{i,j}(t)\|$ can be arbitrary small when a small enough T is selected.*

Proof It is can be seen easily form Eqs. (9), (12) and (29) that

$$\tilde{\eta}_i(t)\triangleq\ell_{i,1}\tilde{y}_i(t)+\ell_{i,2}\tilde{y}_i^{(1)}(t)+\cdots+\ell_{i,r_i-1}\tilde{y}_i^{(r_i-2)}(t)+\tilde{y}_i^{(r_i-1)}(t)\tag{36}$$

holds for $1\leq i\leq q$, where $\tilde{y}_i^{(j)}(t)\triangleq y_i^{(j)}(t)-y_{n,i}^{(j)}(t)=\tilde{x}_{i,j+1}(t)$ with $\tilde{y}_i^{(j)}(t_0)=0$.

Also, Eq. (36) can be rewritten as

$$\frac{d}{dt}\begin{bmatrix}\tilde{y}_i(t)\\ \tilde{y}_i^{(1)}(t)\\ \vdots\\ \tilde{y}_i^{(r_i-2)}(t)\end{bmatrix}=\underbrace{\begin{bmatrix}0&1&0&\cdots&0\\0&0&1&\cdots&0\\\vdots&\vdots&\vdots&\ddots&\vdots\\0&0&0&\cdots&1\\-\ell_{i,1}&-\ell_{i,2}&-\ell_{i,3}&\cdots&-\ell_{i,r_i-1}\end{bmatrix}}_{\bar{A}_i}\begin{bmatrix}\tilde{y}_i(t)\\ \tilde{y}_i^{(1)}(t)\\ \vdots\\ \tilde{y}_i^{(r_i-2)}(t)\end{bmatrix}+\underbrace{\begin{bmatrix}0\\0\\\vdots\\1\end{bmatrix}}_{\bar{B}_i}\tilde{\eta}_i(t)\tag{37}$$

where $\bar{A}_i$ is Hurwitz since $\ell_{i,1},\ldots,\ell_{i,r_i-1}$ are selected such that the roots of the equation $\ell_{i,1}+\ell_{i,2}s+\ldots+\ell_{i,r_i-1}s^{r_i-2}+s^{r_i-1}=0$ have negative real parts. One can see from Eq. (37) that $[\tilde{y}_i(t),\ldots,\tilde{y}_{(r_i-2)}(t)]'=\int_{t_0}^{t}e^{\bar{A}_i(t-\tau)}\bar{B}_i\tilde{\eta}_i(\tau)d\tau$. Since $\bar{A}_i$ is Hurwitz, it is always exists an invertible matrix P_i such that $\bar{A}_i=P_i\Lambda_iP_i^{-1}$, where Λ_i denotes the diagonal matrix with the eigenvalue of $\bar{A}_i$ on its main diagonal. Thus, one has

$$\begin{aligned}\|[\tilde{x}_{i,1}(t),\ldots,\tilde{x}_{i,r_{i-1}}(t)]\|&=\|[\tilde{y}_i(t),\tilde{y}_i^{(1)}(t),\ldots,\tilde{y}_i^{(r_{i-2})}(t)]\|\left\|\int_{t_0}^{t}P_{ie}^{\Lambda_i(t-\tau)}P_i^{-1}\bar{B}_i\tilde{\eta}_i(\tau)d\tau\right\|\\&\leq\|P_i\|\|P_i^{-1}\|\max_{t\geq t_0}\|\tilde{\eta}_i(t)\|\int_{t_0}^{t}\|e^{\Lambda_i(t-\tau)}\|d\tau=\|P_i\|\|P_i^{-1}\|\max_{t\geq t_0}\|\tilde{\eta}_i(t)\|\int_{t_0}^{t}e^{\lambda_{\min}(\bar{A}_i)(t-\tau)}d\tau\\&\leq\frac{\|P_i\|\|P_i^{-1}\|}{-\lambda_{\min}(\bar{A}_i)}\max_{t\geq t_0}\|\tilde{\eta}_i(t)\|=O(T)\end{aligned}\tag{38}$$

where $\lambda_{\min}(\bar{A}_i)$ denotes the minimum eigenvalue of $\bar{A}_i$ and we have used the fact that $\|\tilde{\eta}(t)\|=O(T)$.

Furthermore, one can see from Eq. (36) that

$$\begin{aligned}\|\tilde{x}_{i,r_i}(t)\| = \|\tilde{y}_i^{(r_i-1)}(t)\| &\le \|\tilde{\eta}_i(t)\| + \|\ell_{i,1}\tilde{y}_i(t) + \ell_{i,2}\tilde{y}_i^{(1)}(t) + \cdots + \ell_{i,r_i-1}\tilde{y}_i^{(r_i-2)}(t)\| \\ &\le \max_{t\ge t_0}\|\tilde{\eta}_i(t)\| + \|[\ell_{i,1},\ldots,\ell_{i,r_i-1}]\|\|[\tilde{y}_i(t),\tilde{y}_i^{(1)}(t),\ldots,\tilde{y}_i^{(r_i-2)}(t)]\| \\ &\le \left\{1 + \frac{\|P_i\|\|P_i^{-1}\|}{-\lambda_{\min}(\bar{A}_i)}\|[\ell_{i,1},\ldots,\ell_{i,r_i-1}]\|\right\}\max_{t\ge t_0}\|\tilde{\eta}_i(t)\| \\ &= O(T). \end{aligned} \tag{39}$$

To sum up, it is easy to get that $\|\tilde{x}_{i,j}(t)\|$ is an infinitesimal of the same order as T, and thus $\tilde{x}_{i,j}(t)$ can be arbitrary small when a small enough T is chosen.

Next, let us analyze the impact of attacks on the original nonlinear system Eq. (1).

Theorem 4. *Consider the original nonlinear system Eq. (1), and the system input Eq. (11) with the attack-compensation input signal Eq. (25). Under assumptions of Theorem 2, then there exists an upper bound of $\|\tilde{x}\|$ which is an infinitesimal of the same order as T, where $\tilde{x} \triangleq x - x_n$ denotes the state deviation caused by the attack. Furthermore, the system is almost fully recovered when a small enough T is selected.*

Proof One can see from Assumption 1 that there exists a diffeomorphism $\Phi(x)$ such that

$$\xi = \Phi(x), \quad \xi_n = \Phi(x_n) \tag{40}$$

and thus

$$\|\tilde{x}\| = \|\Phi^{-1}(\xi) - \Phi^{-1}(\xi_n)\| \le \Gamma\|\tilde{\xi}\| \tag{41}$$

where Γ denotes the Lipschitz constant of the differentiable function $\Phi^{-1}(\cdot)$ in the compact set $\Omega \supseteq \{\xi, \xi_n\}$.

It is worth noting that, $\tilde{\xi} = \xi - \xi_n = [\tilde{x}_{1,1},\ldots,\tilde{x}_{1,r_1},\ldots,\tilde{x}_{q,1},\ldots,\tilde{x}_{q,r_q}]'$, together with Theorem 3, one has

$$\|\tilde{\xi}\| = O(T). \tag{42}$$

Naturally, $\|\tilde{x}\| = O(T)$, which means that the system states under attacks can approximate the nominal states with arbitrary accuracy when a small enough T is selected.

In addition, let u_{dn} denote the nominal value of the desired input $u_d = b^+(\Phi^{-1}(\xi))[-a(\Phi^{-1}(\xi)) + v]$. That is, $u_{dn} \triangleq b^+(\Phi^{-1}(\xi_n))[-a(\Phi^{-1}(\xi_n)) + v$. Similarity, based on the facts that $f(x), g(x), h(x)$ are smooth functions and $\|\tilde{\xi}\| = O(T)$, it is easy to prove that $\|u_d - u_{dn}\| = O(T)$ when T is small enough.

To sum up the above arguments, one can conclude that

$$\lim_{T\to 0}(u_d, x) = (u_{dn}, x_n). \tag{43}$$

Thus, the mapping relationship between the desired input u_d and system states x is almost the same as the one in the nominal system when T is small enough. In other words, the system is almost fully recovered when T is small enough.

Remark 5. *Compared with the existing results on the secure control of CPSs (Deng & Wen, 2020; Xu et al., 2019; Feng & Hu, 2019; Zhang & Ye, 2020a; Yang et al., 2020; Wang et al., 2020; Yang, Li & Yue, 2020; Zhang, Shen & Han, 2019; Shao & Ye, 2020; An &*

Yang, 2018a; *Su & Ye, 2018*; *Hu et al., 2019*; *Chen et al., 2021*; *Wu et al., 2021*; *Gu et al., 2021*; *Huang & Dong, 2020*; *He et al., 2021*; *Chen et al., 2022b*; *Farivar et al., 2019*; *Chen et al., 2022a*; *Lu & Yang, 2017*; *He et al., 2020*; *An & Yang, 2018b*; *Ao, Song & Wen, 2018*; *Zhou et al., 2020*; *Chen et al., 2022b*), *there are several merits of the proposed system recovery scheme: (i) the proposed method can be well applied to the existing methods, because the system can be almost fully recovered; (ii) the proposed approach not only can ensure a good enough performance, but also does not require any knowledge of attack's model and other strict-preconditions; (iii) the proposed approach helps to ensure state performances and state constraints, since the proposed attack-compensation approach can ensure that the trajectory of the system states is almost not affected by the attack.*

Remark 6. *In existing results for nonlinear systems (Back & Shim, 2007, 2009; Chakrabortty & Arcak, 2007, 2009; Freidovich & Khalil, 2008; Wang, Isidori & Su, 2015; Wu et al., 2019), performance recovery was investigated for compensating the disturbances or uncertainties. A common limitation of these results is that the disturbances or uncertainties are required to be differentiable, even smooth. However, the proposed method is not subject to this limitation; and unlike the disturbances and uncertainties, the attacks under consideration are not restricted to be differentiable or smooth. Furthermore, this article systematically studies the system recovery of CPSs under attacks for the first time.*

Remark 7. *Generally speaking, the smaller the value of the positive parameter T, the better the system recovery performance tends to be. In addition, T can be any positive constant, with zero as its lower bound.*

Remark 8. *As shown in this article, the proposed approach can nearly completely restore the attacked system to its attack-free state, ensuring that the original system's control method remains effective under attacks. This also means that, unlike the existing methods that enhance the robustness of control algorithms* (e.g., *Yang et al., 2024*), *the proposed method enhances the robustness of the plant itself. Furthermore, we plan to apply the proposed method to microgrid systems.*

SIMULATION STUDIES

Consider the following attitude dynamic equations of a near-space vehicle at a velocity of 3.16 Mach and at an altitude of 97,167 ft (*Yao, Tao & Jiang, 2016*):

$$\dot{x} = f(x) + g(x)(u + u_a), \quad y = h(x), \tag{44}$$

where $x = [x_1, x_2, x_3, x_4, x_5, x_6]' = [\gamma', \omega']'$, $\gamma = [\mu, \beta, \alpha]'$, $\omega = [p, q, r]'$ and

$$f(x) = \begin{bmatrix} \Xi(\gamma)\omega \\ J^{-1}\Omega(\omega)J\omega \end{bmatrix}, \Omega(\omega) = \begin{bmatrix} 0 & r & -q \\ -r & 0 & p \\ q & -p & 0 \end{bmatrix}, h(x) = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix},$$

$$\Xi(\gamma) = \begin{bmatrix} cos(\alpha) & 0 & sin(\alpha) \\ sin(\alpha) & 0 & -cos(\alpha) \\ 0 & 1 & 0 \end{bmatrix}, J = \begin{bmatrix} 554486 & 0 & -23002 \\ 0 & 1136949 & 0 \\ -23002 & 0 & 1376852 \end{bmatrix}$$

$$g(x) = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ -0.2883 & 0.2883 & -0.8654 & 0.8654 & 0 & 0.0025 \\ -0.0857 & -0.0857 & -0.5263 & -0.5263 & 0.0098 & -0.0073 \\ -0.0959 & 0.0959 & 0.2079 & -0.2079 & -0.0045 & -0.0051 \end{bmatrix}, \tag{45}$$

and $\mu, \beta, \alpha, p, q, r$ represent the bank angle, the sideslip angle, the angle of attack, the roll rate, the pitch rate and the yaw rate, respectively. It can be verified from Definition 1 that this system has a vector relative degree $\{r_1, r_2, r_3\} = \{2, 2, 2\}$, which means that the system can be exactly feedback linearized. Define the following diffeomorphism

$$\Phi(x) = \begin{bmatrix} x_1 \\ cos(x_3)x_4 + sin(x_3)x_6 \\ x_2 \\ sin(x_3)x_4 - cos(x_3)x_6 \\ x_3 \\ x_5 \end{bmatrix} \tag{46}$$

which brings the system Eq. (1) to the system modeled by Eq. (5), where

$$\begin{aligned} a_1(x) &= [0, 0, cos(x_3)x_6 - sin(x_3)x_4, cos(x_3), 0, sin(x_3)]f(x) \\ a_2(x) &= [0, 0, cos(x_3)x_4 + sin(x_3)x_6, sin(x_3), 0, -cos(x_3)]f(x) \\ a_3(x) &= [0, 0, 0, 0, 1, 0]f(x) \end{aligned} \tag{47}$$

and

$$\begin{aligned} b_1(x) = \; & [-0.2883cos(x_3) - 0.0959sin(x_3), 0.2883cos(x_3) + 0.0959sin(x_3), \\ & -0.8654cos(x_3) + 0.2079sin(x_3), 0.8654cos(x_3) - 0.2079sin(x_3), \\ & -0.0045sin(x_3), 0.0025cos(x_3) - 0.0051sin(x_3)] \\ b_2(x) = \; & [-0.2883sin(x_3) + 0.0959cos(x_3), 0.2883sin(x_3) - 0.0959cos(x_3), \\ & -0.8654sin(x_3) - 0.2079cos(x_3), 0.8654sin(x_3) + 0.2079cos(x_3), \\ & 0.0045cos(x_3), 0.0025sin(x_3) + 0.0051cos(x_3)] \\ b_3(x) = \; & [-0.0857, -0.0857, -0.5263, -0.5263, 0.0098, -0.0073]. \end{aligned} \tag{48}$$

In the simulation, the parameters are specified as $T = 10^{-4}s$, $x(0) = [2, 0.3, 5, -3, 0.3, -10]'$, $L = [1, 1, 0, 0, 0, 0; 0, 0, 1, 1, 0, 0; 0, 0, 0, 0, 1, 1]$, and the attack signal $u_a(t)$ is randomly selected from $[0, 2], \forall t \geq 0$ which is shown in Fig. 3.

The system input u in Eq. (44) is chosen as

$$u = \underbrace{b^+(\Phi^{-1}(\xi))[-a(\Phi^{-1}(\xi)) + v]}_{u_d} + \underbrace{b^+(\Phi^{-1}(\xi))v_c}_{u_c} \tag{49}$$

where v_c is defined in Eq. (25) with $v = K\xi$, where K is chosen as

$$K = \begin{bmatrix} -1 & -1.7321 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & -1.7321 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & -1.7321 \end{bmatrix}$$

such that $A + BK$ is Hurwitz.

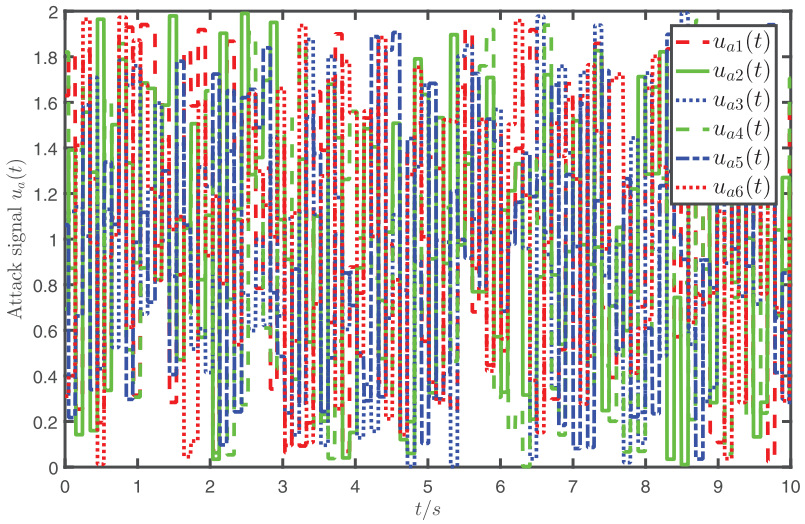

Figure 3 **Profiles of the attack signal u_a where u_{ai} represents the i-th element of u_a.**
Full-size DOI: 10.7717/peerj-cs.3280/fig-3

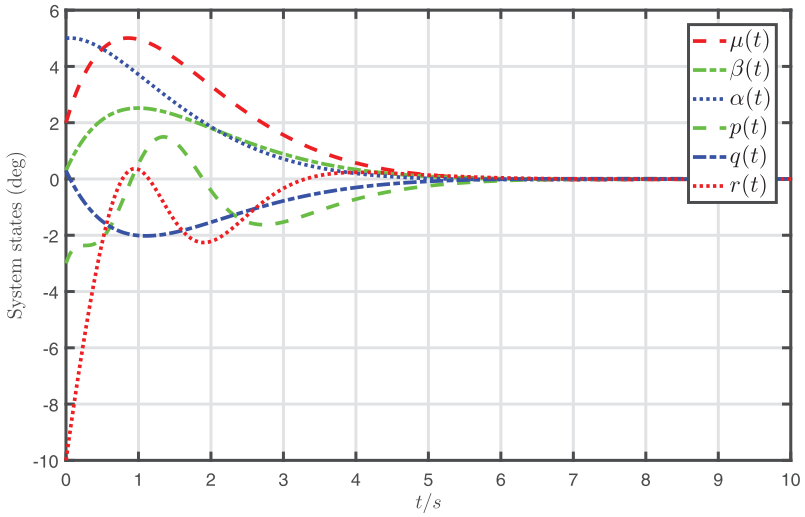

Figure 4 **Profiles of system states under the desired input u_d and the attack-compensation input u_c.**
Full-size DOI: 10.7717/peerj-cs.3280/fig-4

The simulation results of the nonlinear system, which is jointly controlled by the desired input u_d and the attack-compensation input u_c, are demonstrated in Fig. 4. In addition, the state trajectories of the nonlinear system, which is only controlled by the desired input $u_d = b^+(\Phi^{-1}(\xi))[-a(\Phi^{-1}(\xi)) + v]$, are depicted in Fig. 5.

It is shown from Fig. 4 that the system states almost converge to zero when the system controlled by the proposed attack-compensation approach. On the contrary, if the desired input designed for the nominal model is applied to the system under FDI attack, the behavior of the system degrades severely, as shown in Fig. 5. The simulation results

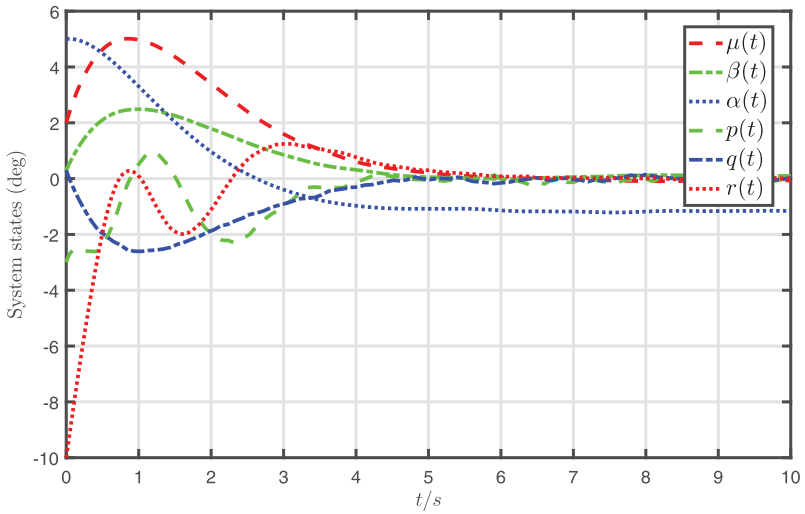

Figure 5 **Profiles of system states under the desired input u_d.**
Full-size DOI: 10.7717/peerj-cs.3280/fig-5

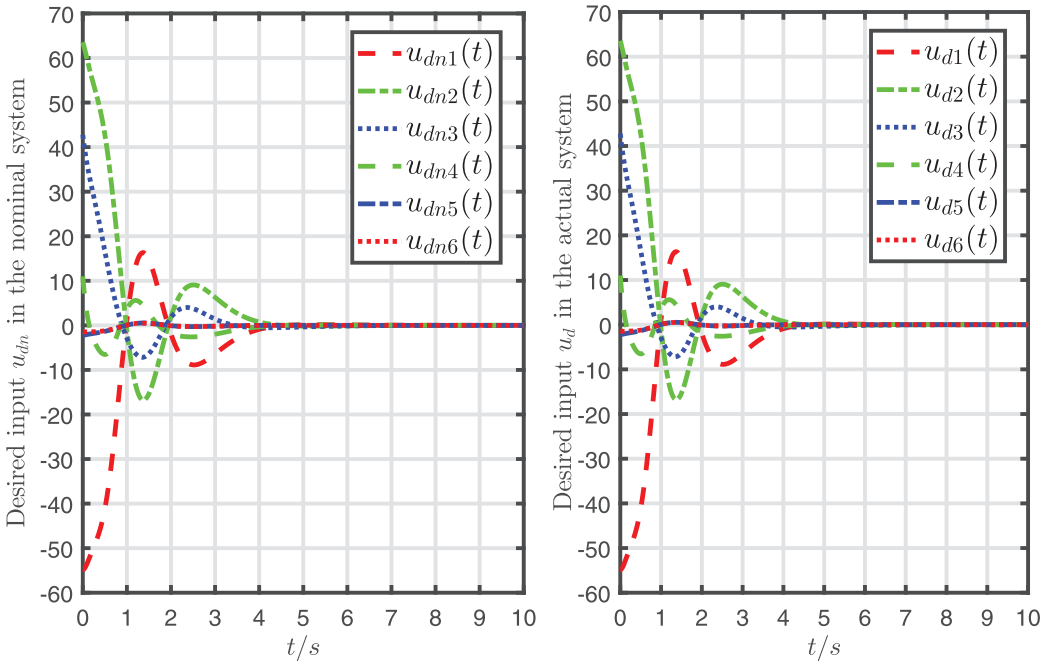

Figure 6 **Desired input u_{dn} in the nominal system and the desired input u_d in the actual system.**
Full-size DOI: 10.7717/peerj-cs.3280/fig-6

demonstrate that very satisfactory compensation performances are achieved by the proposed attack-compensation approach for the system even in the presence of the attack, and much better performances can be achieved than the desired-input-based control, which verify that the proposed attack-compensation scheme is very effective to cope with the attack.

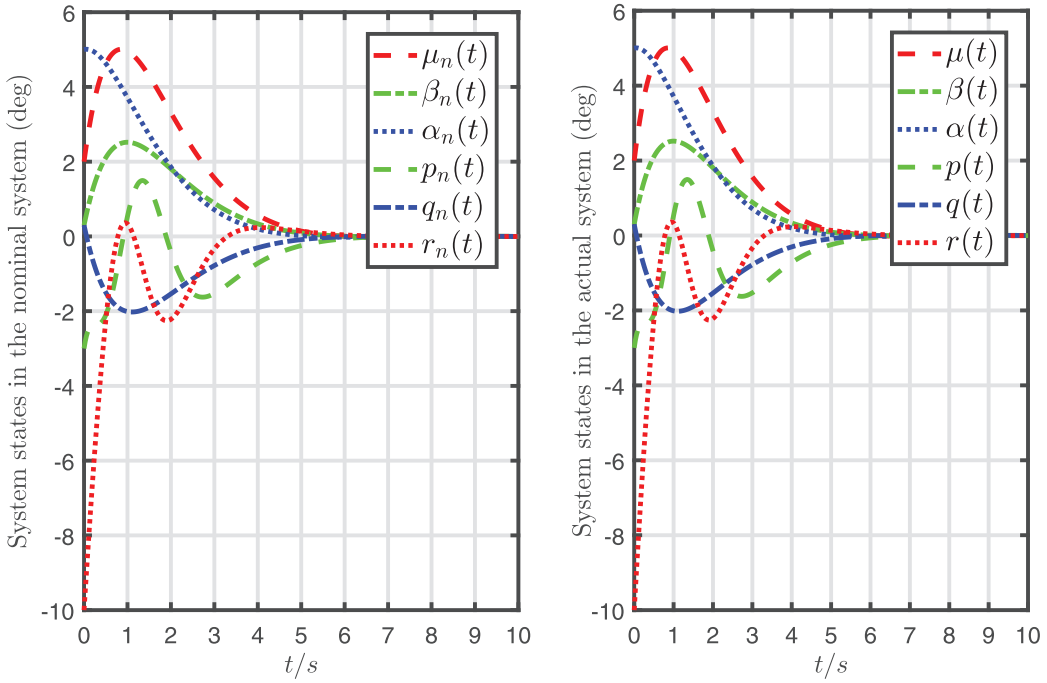

Figure 7 **System states in the nominal system controlled by the desired input u_{dn} and the ones in the actual system controlled by the desired input u_d and the attack-compensation input u_c.**
Full-size DOI: 10.7717/peerj-cs.3280/fig-7

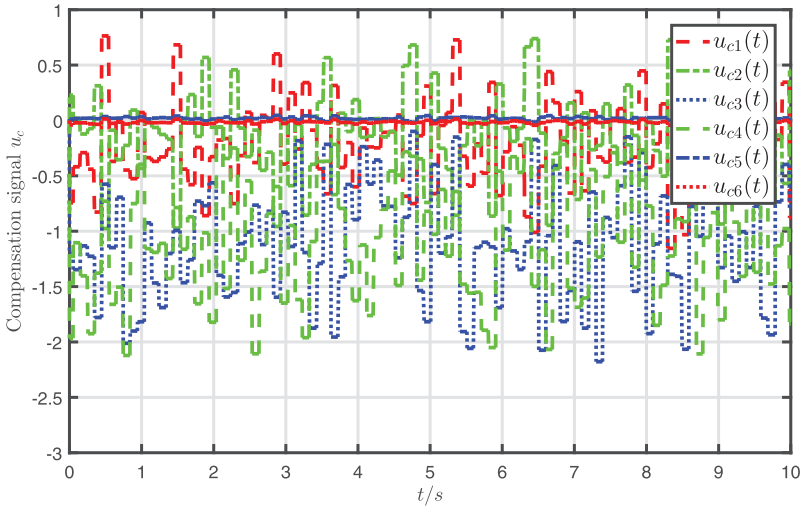

Figure 8 **Profiles of compensation signal u_c.** Full-size DOI: 10.7717/peerj-cs.3280/fig-8

To display the effect of system recovery, the desired input and its nominal input are drawn in Fig. 6, and the actual system state and its nominal state are drawn in Fig. 7.

It can be seen from Figs. 6, 7 that the mapping relationship between the desired input u_d and system states x is almost the same as u_{dn} and x_n in the nominal system. In other words,

Table 2 Statistical results of root mean square error (RMSE).

Indices under the proposed approach	RSME of $\tilde{\mu}(t)$	RSME of $\tilde{\beta}(t)$	RSME of $\tilde{\alpha}(t)$	RSME of $\tilde{p}(t)$	RSME of $\tilde{q}(t)$	RSME of $\tilde{r}(t)$
Values	1.0608×10^{-10}	1.7125×10^{-11}	2.8589×10^{-9}	5.4717×10^{-9}	2.2806×10^{-9}	1.0228×10^{-9}
Indices without the proposed approach	**RSME of $\tilde{\mu}(t)$**	**RSME of $\tilde{\beta}(t)$**	**RSME of $\tilde{\alpha}(t)$**	**RSME of $\tilde{p}(t)$**	**RSME of $\tilde{q}(t)$**	**RSME of $\tilde{r}(t)$**
Values	0.0026	0.0042	1.1961	0.2099	0.0358	0.3036

the system is almost fully recovered (that is because the recursive attack-compensation input signal added into the system input can almost fully compensate the attack).

In addition, the attack-compensation input signal $u_c(t)$ is presented in Fig. 8, which shows that $u_c(t)$ is the same order of magnitude as the attack signal u_a.

To provide a more intuitive and clear description of the system recovery performance of the proposed approach, the root mean squared error (RMSE) index is used. Table 2 lists the RMSE and mean absolute error (MAE) values for state deviation caused by the attack, where $\tilde{\mu} \triangleq \mu - \mu_n$, $\tilde{\beta} \triangleq \beta - \beta_n$, $\tilde{\alpha}(t) \triangleq \alpha(t) - \alpha_n(t)$, $\tilde{p}(t) \triangleq p(t) - p_n(t)$, $\tilde{q}(t) \triangleq q(t) - q_n(t)$ and $\tilde{r}(t) \triangleq r(t) - r_n(t)$. The results demonstrate that the proposed strategy achieves superior system recovery performance.

CONCLUSIONS

In this article, the system recovery problem has been studied for MIMO nonlinear systems under FDI attack. With the help of feedback-linearizing design technique, the nonlinear system has been transformed into a linear one. In order to obtain the system states, a high-gain approximate differentiator has been utilized. After that, a recursive attack-compensation input signal has been skillfully designed and added into the system input to almost fully recover the system. It has been proved that an upper bound of the state deviation caused by the attack is an infinitesimal of the same order as the period of the attack-compensation input signal, and thus the system can be almost fully recovered when a small enough period is selected.

ADDITIONAL INFORMATION AND DECLARATIONS

Funding

This work was supported by the Science & Technology Project of China Southern Power Grid (030100KC23110071) and by the Jiangxi Provincial Natural Science Foundation (20232BAB202032). There was no additional external funding received for this study. The funders had no role in study design, data collection and analysis, decision to publish, or preparation of the manuscript.

Grant Disclosures

The following grant information was disclosed by the authors:
Science & Technology Project of China Southern Power Grid: 030100KC23110071.
Jiangxi Provincial Natural Science Foundation: 20232BAB202032.

Competing Interests

The authors declare that they have no competing interests.

Guokai Liang, Jiangwei Wu, Xuechao Li, Shibo Li, Jie Zhou, Jianxin Zhu and Yilong Gao are employed by Guangdong Power Grid Co.

Author Contributions

- Guokai Liang conceived and designed the experiments, prepared figures and/or tables, and approved the final draft.
- Jiangwei Wu performed the experiments, prepared figures and/or tables, and approved the final draft.
- Xuechao Li conceived and designed the experiments, performed the experiments, authored or reviewed drafts of the article, and approved the final draft.
- Shibo Li analyzed the data, prepared figures and/or tables, and approved the final draft.
- Jie Zhou performed the experiments, prepared figures and/or tables, and approved the final draft.
- Jianxin Zhu analyzed the data, authored or reviewed drafts of the article, and approved the final draft.
- Yilong Gao analyzed the data, performed the computation work, authored or reviewed drafts of the article, and approved the final draft.
- Yanyan Zhang performed the computation work, authored or reviewed drafts of the article, and approved the final draft.
- Zhe Li performed the computation work, authored or reviewed drafts of the article, and approved the final draft.

Data Availability

The following information was supplied regarding data availability:

The data is available at GitHub and Zenodo:

- https://github.com/yhp321/RowData.

- haopeng, . yan . (2025, July 30). rowdata. Zenodo. https://doi.org/10.5281/zenodo.16593905.

The source code is available in the Supplemental Files.

Supplemental Information

Supplemental information for this article can be found online at http://dx.doi.org/10.7717/peerj-cs.3280#supplemental-information.

REFERENCES

Alfriehat N, Anbar M, Aladaileh M, Hasbullah I, Shurbaji TA, Karuppayah S, Almomani A. 2024. RPL-based attack detection approaches in IoT networks: review and taxonomy. *Artificial Intelligence Review* **57(9)**:248 DOI 10.1007/s10462-024-10907-y.

Alrslani FA, Alohali MA, Aljebreen M, Alqahtani H, Alshuhail A, Alshammeri M, Almukadi WS. 2025. Enhancing cybersecurity via attribute reduction with deep learning model for false data injection attack recognition. *Scientific Reports* **15**:3944 DOI 10.1038/s41598-024-82566-6.

Alsinai A, Ullah Khan Niazi A, Zeeshan Babar M, Jamil A, Faisal N. 2025. Robust resilient base containment control of fractional order multiagent systems with disturbance and time delays. *Mathematical Methods in the Applied Sciences* **48(8)**:8851–8863 DOI 10.1002/mma.10758.

An L, Yang G-H. 2018a. Decentralized adaptive fuzzy secure control for nonlinear uncertain interconnected systems against intermittent DoS attacks. *IEEE Transactions on Cybernetics* **49(3)**:827–838 DOI 10.1109/tcyb.2017.2787740.

An L, Yang G-H. 2018b. LQ secure control for cyber-physical systems against sparse sensor and actuator attacks. *IEEE Transactions on Control of Network Systems* **6(2)**:833–841 DOI 10.1109/tcns.2018.2878507.

An L, Yang G-H. 2019. State estimation under sparse sensor attacks: a constrained set partitioning approach. *IEEE Transactions on Automatic Control* **64(9)**:3861–3868 DOI 10.1109/tac.2018.2885063.

Ao W, Song Y, Wen C. 2018. Distributed secure state estimation and control for CPSs under sensor attacks. *IEEE Transactions on Cybernetics* **50(1)**:259–269 DOI 10.1109/tcyb.2018.2868781.

Arab M, Zaman A, Niazi AUK, Balti M. 2025. Impulsive fault-tolerant control for multi-agent systems with stochastic disturbances. *AIMS Mathematics* **10(3)**:7414–7429 DOI 10.3934/math.2025340.

Atassi AN, Khalil HK. 1999. A separation principle for the stabilization of a class of nonlinear systems. *IEEE Transactions on Automatic Control* **44(9)**:1672–1687 DOI 10.1109/9.788534.

Back J, Shim H. 2007. Analysis and synthesis of disturbance observer as a tool for nonlinear robust control. *IFAC Proceedings Volumes* **40(12)**:387–394 DOI 10.3182/20070822-3-za-2920.00064.

Back J, Shim H. 2009. An inner-loop controller guaranteeing robust transient performance for uncertain MIMO nonlinear systems. *IEEE Transactions on Automatic Control* **54(7)**:1601–1607 DOI 10.1109/tac.2009.2017962.

Chakrabortty A, Arcak M. 2007. A two-time-scale redesign for robust stabilization and performance recovery of uncertain nonlinear systems. In: *2007 American Control Conference*. Piscataway: IEEE, 4643–4648.

Chakrabortty A, Arcak M. 2009. Time-scale separation redesigns for stabilization and performance recovery of uncertain nonlinear systems. *Automatica* **45(1)**:34–44 DOI 10.1016/j.automatica.2008.06.004.

Chen X, Hu S, Li Y, Yue D, Dou C, Ding L. 2022b. Co-estimation of state and FDI attacks and attack compensation control for multi-area load frequency control systems under FDI and DoS attacks. *IEEE Transactions on Smart Grid* **13(3)**:2357–2368 DOI 10.1109/tsg.2022.3147693.

Chen B, Tan Y, Sun Z, Yu L. 2022a. Attack-resilient control against FDI attacks in cyber-physical systems. *IEEE/CAA Journal of Automatica Sinica* **9(6)**:1099–1102 DOI 10.1109/jas.2022.105641.

Chen G, Zhang Y, Gu S, Hu W. 2021. Resilient state estimation and control of cyber-physical systems against false data injection attacks on both actuator and sensors. *IEEE Transactions on Control of Network Systems* **9(1)**:500–510 DOI 10.1109/tcns.2021.3113265.

Cheng P, Shi L, Sinopoli B. 2017. Guest editorial special issue on secure control of cyber-physical systems. *IEEE Transactions on Control of Network Systems* **4(1)** DOI 10.1109/tcns.2017.2667233.

Corless M, Tu J. 1998. State and input estimation for a class of uncertain systems. *Automatica* **34(6)**:757–764 DOI 10.1016/s0005-1098(98)00013-2.

Deng C, Wen C. 2020. Distributed resilient observer-based fault-tolerant control for heterogeneous multiagent systems under actuator faults and DoS attacks. *IEEE Transactions on Control of Network Systems* **7(3)**:1308–1318 DOI 10.1109/tcns.2020.2972601.

Farivar F, Haghighi MS, Jolfaei A, Alazab M. 2019. Artificial intelligence for detection, estimation, and compensation of malicious attacks in nonlinear cyber-physical systems and industrial IoT. *IEEE Transactions on Industrial Informatics* **16(4)**:2716–2725 DOI 10.1109/tii.2019.2956474.

Feng Z, Hu G. 2019. Secure cooperative event-triggered control of linear multiagent systems under DoS attacks. *IEEE Transactions on Control Systems Technology* **28(3)**:741–752 DOI 10.1109/tcst.2019.2892032.

Floquet T, Edwards C, Spurgeon SK. 2007. On sliding mode observers for systems with unknown inputs. *International Journal of Adaptive Control and Signal Processing* **21(8–9)**:638–656 DOI 10.1002/acs.958.

Freidovich LB, Khalil HK. 2008. Performance recovery of feedback-linearization-based designs. *IEEE Transactions on Automatic Control* **53(10)**:2324–2334 DOI 10.1109/tac.2008.2006821.

Gu Y, Yu X, Guo K, Qiao J, Guo L. 2021. Detection, estimation, and compensation of false data injection attack for UAVs. *Information Sciences* **546(2)**:723–741 DOI 10.1016/j.ins.2020.08.055.

He W, Mo Z, Han Q-L, Qian F. 2020. Secure impulsive synchronization in lipschitz-type multi-agent systems subject to deception attacks. *IEEE/CAA Journal of Automatica Sinica* **7(5)**:1326–1334 DOI 10.1109/jas.2020.1003297.

He H, Qi W, Liu Z, Wang M. 2021. Adaptive attack-resilient control for Markov jump system with additive attacks. *Nonlinear Dynamics* **103(2)**:1585–1598 DOI 10.1007/s11071-020-06085-5.

Hu S, Yuan P, Yue D, Dou C, Cheng Z, Zhang Y. 2019. Attack-resilient event-triggered controller design of DC microgrids under DoS attacks. *IEEE Transactions on Circuits and Systems I: Regular Papers* **67(2)**:699–710 DOI 10.1109/tcsi.2019.2948015.

Huang X, Dong J. 2020. An adaptive secure control scheme for T-S fuzzy systems against simultaneous stealthy sensor and actuator attacks. *IEEE Transactions on Fuzzy Systems* **29(7)**:1978–1991 DOI 10.1109/tfuzz.2020.2990772.

Isidori A. 1985. *Nonlinear control systems: an introduction*. Cham: Springer.

Kalsi K, Lian J, Hui S, Żak SH. 2010. Sliding-mode observers for systems with unknown inputs: a high-gain approach. *Automatica* **46(2)**:347–353 DOI 10.1016/j.automatica.2009.10.040.

Khan A, Javeed MA, Hassan WU, Niazi AUK, Ahmed S, Zhong Y, Riaz S. 2025a. Stability analysis and resilient communication in connected vehicle platooning: addressing input communication delays and disruptions through Lyapunov analysis and event-triggered control. *Alexandria Engineering Journal* **116(12)**:342–350 DOI 10.1016/j.aej.2024.12.063.

Khan A, Javeed MA, Hassan WU, Zhong Y, Ahmed S, Niazi AUK. 2025b. Event-triggered consensus control with dynamic agents and communication delays in heterogeneous multi-agent systems. *Alexandria Engineering Journal* **128(6)**:1–11 DOI 10.1016/j.aej.2025.04.100.

Khan A, Niazi AUK, Rehman S, Shaheen S, Saidani T, Rajab AB, Javeed MA, Zhong Y. 2025c. Robust neural network-driven control for multi-agent formation in the presence of byzantine attacks and time delays. *AIMS Mathematics* **10(6)**:12956–12979 DOI 10.3934/math.2025583.

Li Y, Shi D, Chen T. 2018. False data injection attacks on networked control systems: a Stackelberg game analysis. *IEEE Transactions on Automatic Control* **63(10)**:3503–3509 DOI 10.1109/tac.2018.2798817.

Lu A-Y, Yang G-H. 2017. Event-triggered secure observer-based control for cyber-physical systems under adversarial attacks. *Information Sciences* **420(4)**:96–109 DOI 10.1016/j.ins.2017.08.057.

Markantonakis K, Meister JA, Gurulian I, Shepherd C, Naeem Akram R, Hani Abu Ghazalah S, Kasi M, Sauveron D, Hancke G. 2024. Using ambient sensors for proximity and relay attack

detection in NFC transactions: a reproducibility study. *IEEE Access* **12(7)**:150372–150386 DOI 10.1109/access.2024.3479729.

Pasqualetti F, Dörfler F, Bullo F. 2013. Attack detection and identification in cyber-physical systems. *IEEE Transactions on Automatic Control* **58(11)**:2715–2729 DOI 10.1109/tac.2013.2266831.

Shao X, Ye D. 2020. Fuzzy adaptive event-triggered secure control for stochastic nonlinear high-order MASs subject to DoS attacks and actuator faults. *IEEE Transactions on Fuzzy Systems* **29(12)**:3812–3821 DOI 10.1109/tfuzz.2020.3028657.

Su L, Ye D. 2018. A cooperative detection and compensation mechanism against denial-of-service attack for cyber-physical systems. *Information Sciences* **444(12)**:122–134 DOI 10.1016/j.ins.2018.02.066.

Sun Q, Yang G-H. 2025. Secure state estimation for continuous-time cyber-physical systems under stochastic attacks and faults. *IEEE Transactions on Automatic Control* **70(9)**:6119–6126 DOI 10.1109/TAC.2025.3552018.

Tanyıldız H, Şahin CB, Dinler Ö.B, Migdady H, Saleem K, Smerat A, Gandomi AH, Abualigah L. 2025. Detection of cyber attacks in electric vehicle charging systems using a remaining useful life generative adversarial network. *Scientific Reports* **15(1)**:10092 DOI 10.1038/s41598-025-92895-9.

Teel A, Praly L. 1995. Tools for semiglobal stabilization by partial state and output feedback. *SIAM Journal on Control and Optimization* **33(5)**:1443–1488 DOI 10.1137/s0363012992241430.

Wang L, Isidori A, Su H. 2015. Output feedback stabilization of nonlinear MIMO systems having uncertain high-frequency gain matrix. *Systems & Control Letters* **83(6)**:1–8 DOI 10.1016/j.sysconle.2015.06.001.

Wang J, Liu H, Liu C, Ren X, Wang X. 2025. Optimal scheduling of importance-based DoS attack in multi-systems. *IEEE Sensors Journal* **25(9)**:15770–15779 DOI 10.1109/jsen.2025.3553093.

Wang X, Park JH, Liu H, Zhang X. 2020. Cooperative output-feedback secure control of distributed linear cyber-physical systems resist intermittent DoS attacks. *IEEE Transactions on Cybernetics* **51(10)**:4924–4933 DOI 10.1109/tcyb.2020.3034374.

Wu Y, Isidori A, Lu R, Khalil HK. 2019. Performance recovery of dynamic feedback-linearization methods for multivariable nonlinear systems. *IEEE Transactions on Automatic Control* **65(4)**:1365–1380 DOI 10.1109/tac.2019.2924176.

Wu C, Yao W, Pan W, Sun G, Liu J, Wu L. 2021. Secure control for cyber-physical systems under malicious attacks. *IEEE Transactions on Control of Network Systems* **9(2)**:775–788 DOI 10.1109/tcns.2021.3094782.

Xie C-H, Yang H, Zhang K, Wang H. 2025. Computationally inexpensive decentralized adaptive asymptotic tracking control for a single under-actuated high-speed train. *IEEE Transactions on Intelligent Transportation Systems* **26(8)**:12287–12299 DOI 10.1109/TITS.2025.3554658.

Xu W, Hu G, Ho DW, Feng Z. 2019. Distributed secure cooperative control under denial-of-service attacks from multiple adversaries. *IEEE Transactions on Cybernetics* **50(8)**:3458–3467 DOI 10.1109/tcyb.2019.2896160.

Yang S, Lao K-W, Hui H, Chen Y. 2024. Secure distributed control for demand response in power systems against deception cyber-attacks with arbitrary patterns. *IEEE Transactions on Power Systems* **39(6)**:7277–7290 DOI 10.1109/tpwrs.2024.3381231.

Yang Y, Li Y, Yue D. 2020. Event-trigger-based consensus secure control of linear multi-agent systems under DoS attacks over multiple transmission channels. *Science China Information Sciences* **63(5)**:150208 DOI 10.1007/s11432-019-2687-7.

Yang Y, Li Y, Yue D, Tian Y-C, Ding X. 2020. Distributed secure consensus control with event-triggering for multiagent systems under DoS attacks. *IEEE Transactions on Cybernetics* **51(6)**:2916–2928 DOI 10.1109/tcyb.2020.2979342.

Yao X, Tao G, Jiang B. 2016. Adaptive actuator failure compensation for multivariable feedback linearizable systems. *International Journal of Robust and Nonlinear Control* **26(2)**:252–285 DOI 10.1002/rnc.3309.

Zhang M, Shen C, Han S. 2019. A compensation control scheme against DoS attack for nonlinear cyber-physical systems. In: *2019 Chinese Control Conference (CCC)*. Piscataway: IEEE, 144–149.

Zhang J-P, Yang H, Zhang K, Xie C-H. 2024. Tracking control for high-speed train with coupler constraints. *IEEE Transactions on Intelligent Transportation Systems* **25(10)**:14654–14668 DOI 10.1109/tits.2024.3392629.

Zhang T-Y, Ye D. 2020a. Distributed secure control against denial-of-service attacks in cyber-physical systems based on K-connected communication topology. *IEEE Transactions on Cybernetics* **50(7)**:3094–3103 DOI 10.1109/tcyb.2020.2973303.

Zhang T-Y, Ye D. 2020b. False data injection attacks with complete stealthiness in cyber–physical systems: a self-generated approach. *Automatica* **120**:109117 DOI 10.1016/j.automatica.2020.109117.

Zhang T-Y, Ye D, Shi Y. 2022. Decentralized false-data injection attacks against state omniscience: existence and security analysis. *IEEE Transactions on Automatic Control* **68(8)**:4634–4649 DOI 10.1109/tac.2022.3209396.

Zhou Y, Vamvoudakis KG, Haddad WM, Jiang Z-P. 2020. A secure control learning framework for cyber-physical systems under sensor and actuator attacks. *IEEE Transactions on Cybernetics* **51(9)**:4648–4660 DOI 10.1109/tcyb.2020.3006871.