processes

MDPI

Article

Monitoring and Reconstruction of Actuator and Sensor Attacks for Lipschitz Nonlinear Dynamic Systems Using Two Types of Augmented Descriptor Observers

Hao Wang, Zhi-Wei Gao * and Yuanhong Liu

Research Centre for Digitalization and Intelligent Diagnosis to New Energies, College of Electrical and Information Engineering, Northeast Petroleum University, Daqing 163318, China; wanghao000421@163.com (H.W.); liuyuanhong@nepu.edu.cn (Y.L.)
* Correspondence: gaozhiwei@nepu.edu.cn

Abstract: Fault data injection attacks may lead to a decrease in system performance and even a malfunction in system operation for an automatic feedback control system, which has motive to develop an effective method for rapidly detecting such attacks so that appropriate measures can be taken correspondingly. In this study, a secure descriptor estimation technique is proposed for continuous-time Lipschitz nonlinear cyber physical systems affected by actuator attacks, sensor attacks, and unknown process uncertainties. Specifically, by forming a new state vector composed of original system states and sensor faults, an equivalent descriptor dynamic system is built. A proportional and derivate sliding-mode observer is presented so that the system states, sensor attack, and actuator attack can be reconstructed successfully. The observer gains are obtained by using linear matrix inequality to secure robustly stable estimation error dynamics. Moreover, a robust descriptor fast adaptive observer estimator is presented as a complement. Finally, the efficacy levels of the proposed design approaches are validated using a vertical take-off and landing aircraft system. Comparison studies are also carried out to assess the tracking performances of the proposed algorithms.

Keywords: data injection attack; attack monitoring; attack reconstruction; augmented descriptor system approach; sliding-mode observer; adaptive observer

check for updates

Citation: Wang, H.; Gao, Z.-W.; Liu, Y. Monitoring and Reconstruction of Actuator and Sensor Attacks for Lipschitz Nonlinear Dynamic Systems Using Two Types of Augmented Descriptor Observers. *Processes* **2024**, *12*, 1383. https://doi.org/10.3390/pr12071383

Academic Editors: Ján Piteľ, Ivan Pavlenko and Sławomir Luściński

Received: 5 June 2024
Revised: 25 June 2024
Accepted: 27 June 2024
Published: 2 July 2024

1. Introduction

With the continuous development of industrial systems, cyber–physical systems (CPSs) have received more and more attention by integrating control, communication and information technology. The term CPS was firstly pioneered by Helen Gill, who explained basic theory in a workshop organized by the USNSF in 2006 [1]. In general, a cyber–physical system is defined as the integration of computation, communication, and control to achieve the desired performance of a physical process [2]. CPSs bridge cyber space and physical space, which can realize a remote control of multiple tasks. In comparison to traditional control systems, CPSs offer advantages such as high flexibility, stable and reliable operation, easy installation, and low maintenance costs [3]. However, due to the close interaction of information between physical components and cyber space, such systems are vulnerable to malicious attacks. For instance, in March 2000, the control system of a sewage treatment plant in Queensland, Australia, suffered a remote intrusion, resulting in a large amount of sewage being directly discharged, leading to a severe environmental disaster. A uranium enrichment plant was attacked by the malicious Stuxnet worm, causing the destruction of many centrifuges in June 2010 [4]. Therefore, security has become a big concern, and there is high demand for security in CPSs.

CPSs are now widely applied in various industries such as power systems, intelligent transportation, aerospace, chemical production and so forth, which play crucial roles in ensuring the normal operation of society. It is noted that there is an increasing variety of attack types targeting CPSs, primarily categorized into two types: DOS (Denial-of-Service) attacks and deception attacks (also called false data injection (FDI) attacks). DOS attacks involve attempts by attackers to temporarily or permanently disrupt services of devices connected to the internet, rendering legitimate users unable to access network resources. Deceptive data injection attacks are typically achieved by tampering with system data or packets, such as directly sending false packets to target nodes or injecting false data into original packets. In this paper, like most methods about CPS, we believe that the quality of service (QoS) of the developed communication network is adequate, that is, we assume that the signal transmission speed is very fast, and the impact of delay in the transmission process can be ignored to ensure that CPS operates under ideal conditions [5–7]. Hence, the architecture of a cyber–physical system attacked via a false data injection attack can be depicted by Figure 1. It is worth noting that a replay attack can be considered a specific type of deceptive data injection attack, where only past data can be replayed [8]. Recent literature focusing on the security of CPSs can mainly be categorized into two areas: attack detection and secure state estimation. In terms of methods, they are primarily classified into model-based [9–13] and deep learning-based approaches [14–17]. Secure state estimation is an intriguing and powerful technology that not only enables attack detection but also facilitates attack identification. Observer-based state estimation methods play a crucial role in attack detection and identification. Common secure state estimation methods include the Kalman filter method [18,19], sliding-mode estimation method [20,21], adaptive estimation methods [22,23], and proportional integral observer methods [24,25].

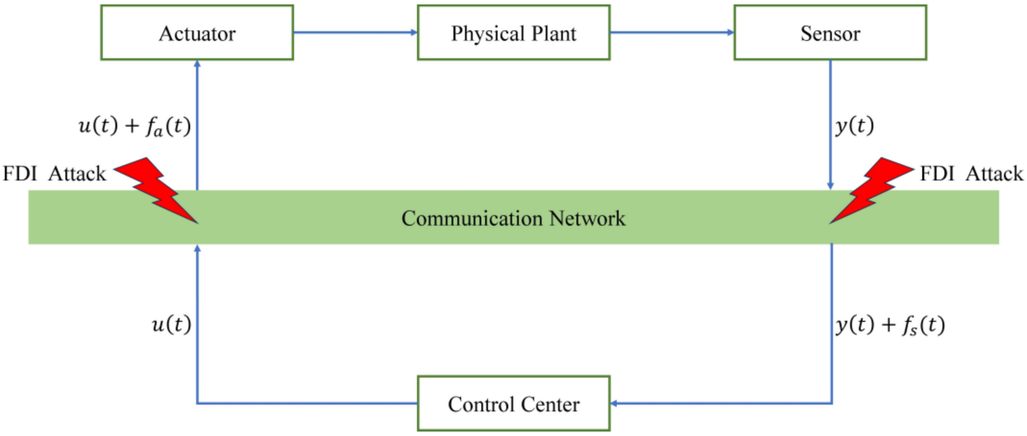

Figure 1. The schematic diagram of the CPS architecture subjected to attacks.

However, the current literature mostly concentrates on linear systems, and it either focuses on sensor attacks [26] or actuator attacks [27] or does not consider the influence of noise [28,29]. Furthermore, it is worth noting that many systems in engineering can be modeled as descriptor systems, where the nonlinear components of the system can be characterized in Lipschitz form, at least locally [30]. Descriptor system theory has been successfully applied in estimation and control for regular dynamics systems, and some pioneering works can be found in [31–33]. Compared with diagnosis and identification of physical faults, the attack reconstruction has limited results that need to be further investigated. Attack reconstruction is an advanced diagnosis strategy that can detect, isolate, and identify attacks at the same time.

In this study, Lipschitz nonlinear systems subjected to both actuator and sensor data injection attacks are investigated, and the contributions and innovations of this paper are highlighted as follows:

(i). By forming an extended state vector composed of system states and sensor attacks, a descriptor dynamic system is established that is equivalent to original regular dynamic systems.

(ii). Using proportional and derivative gain, the descriptor dynamic system is transformed into an augmented regular dynamic system, with sensor attacks as internal states but leaving actuator attacks as external unknown inputs.

(iii). For the equivalent regular dynamic system obtained in (ii), a sliding-mode observer is designed to form an augmented descriptor observer, which can achieve the simultaneous reconstruction of system states, sensor attacks, and actuator attacks.

(iv). The robust performance of the dynamics in the estimation error equation can be ensured by using the linear matrix inequality technique.

(v). An augmented descriptor adaptive observer technique is presented as well for achieving a robust simultaneous reconstruction of system states, sensor attacks, and actuator attacks.

(vi). The proposed algorithms are off-line design and on-line implementation, indicating an excellent real-time performance.

(vii). The two proposed novel attack estimation techniques are validated by an engineering-oriented example, and the performances of the two reconstruction techniques are analyzed and compared.

The remaining parts of this paper are organized as follows. Preliminaries and problem formulation are given Section 2. In Section 3, a novel augmented sliding-mode observer is presented for the secure estimation of actuator and sensor attacks. In Section 4, an adaptive descriptor augmented estimation technique is addressed for the simultaneous reconstruction of actuator and sensor attacks. Simulation studies and comparisons are shown in Section 5. The paper ends with conclusions in Section 6.

2. Preliminaries and Problem Formulation

Consider a continuous time dynamic system subjected to actuator attacks, sensor attacks, and unknown interference in the form of

$$\begin{cases} \dot{x}(t) = Ax(t) + Bu(t) + G\Phi(x(t)) + B_a f_a(t) + B_d d(t) \\ y(t) = Cx(t) + D_s f_s(t) \end{cases} \tag{1}$$

where $x(t) \in R^n$ is the state vector, $u(t) \in R^m$ is the control input vector, $\Phi(x(t))$ is a Lipschitz nonlinear function, $y(t) \in R^p$ is the measured output vector, $d(t) \in R^d$ is the unknown but bounded external disturbance vector and $\| d \| \leq \delta$, and $f_a(t) \in R^q$ and $f_s(\mathrm{t}) \in R^r$ are the malicious actuator attack and sensor attack signals injected against the CPS, respectively. A, B, G, C, B_a, B_d, and D_s are known matrices with appropriate dimensions. D_s is assumed to be full rank of column.

Cyber–physical systems (CPSs) are often susceptible to attacks such as Denial-of-Service (DoS), false data injection attacks, and replay attacks. Among these, false data injection attacks have received significant attention due to their severe impact and the challenges associated with their detection. In this type of attack, adversaries can either directly transmit false data to the target location or modify data transmitted between different parts of the network, intentionally misleading the system, affecting its stability, and potentially causing severe damage to the system. In this paper, we focus on the monitoring and reconstruction problems related to such attacks.

Assumption 1. *For any $x_1(t), x_2(t) \in R^n$, there is a constant $\gamma > 0$ such that*

$$\| \Phi(x_1(t)) - \Phi(x_2(t)) \| \leq \gamma \| x_1(t) - x_2(t) \| \tag{2}$$

Then, the nonlinear function $\Phi(x(t))$ is Lipschitz.

Assume $\Phi(x(t)) = 0$ when $x(t) = 0$. Therefore, from (2), one can have

$$\Phi(x(t)) \leq \gamma \| x(t) \| \tag{3}$$

Assumption 2. *The actuator fault and its derivative are assumed to be bounded, that is,* $\|f_a(t)\| \le \alpha$ *and* $\left\|\dot{f}_a(t)\right\| \le \beta$*, where* α *and* β *are assumed to be positive scalars.*

Remark 1. *Under Assumption 1, the nonlinear term* $\Phi(x(t))$ *is globally Lipschitz. It is noticed that in engineering practice, many nonlinear systems are locally Lipschitz in a region. The proposed methods can be easily extended to locally Lipschitz nonlinear systems (e.g., see [30]).*

3. State and Attack Estimation Using Augmented Descriptor Sliding-Mode Techniques

In this section, to estimate the system state, actuator attacks, and sensor attacks while simultaneously mitigating the impacts of unknown disturbances, a new robust reconstruction technique is proposed by integrating augmented descriptor system approach and sliding-mode observer method.

3.1. Augmented Descriptor System Approach

Motivated by [31–33], we can define $x_a(t) = \begin{bmatrix} x(t) \\ f_s(t) \end{bmatrix}$. Therefore, we can identify an augmented descriptor system in the following form:

$$\begin{cases} E\dot{x}_a(t) = A_a x_a(t) + B_{ua}u(t) + G_a\Phi(x(t)) + B_{fa}f_a(t) + B_{da}d(t) + KD_s f_s(t) \\ y(t) = C_a x_a(t) = C_{a1}x_a(t) + D_s f_s(t) \end{cases} \tag{4}$$

where

$$\begin{gathered} E = \begin{bmatrix} I & 0 \\ 0 & 0 \end{bmatrix}, A_a = \begin{bmatrix} A & 0 \\ 0 & -D_s \end{bmatrix}, B_{ua} = \begin{bmatrix} B \\ 0 \end{bmatrix}, G_a = \begin{bmatrix} G \\ 0 \end{bmatrix}, B_{fa} = \begin{bmatrix} B_a \\ 0 \end{bmatrix}, \\ B_{da} = \begin{bmatrix} B_d \\ 0 \end{bmatrix}, K = \begin{bmatrix} 0 \\ I \end{bmatrix}, C_a = \begin{bmatrix} C & D_s \end{bmatrix}, C_{a1} = \begin{bmatrix} C & 0 \end{bmatrix}. \end{gathered} \tag{5}$$

In terms of (5) and (6), the augmented descriptor system can be simplified to

$$E\dot{x}_a(t) = (A_a - KC_{a1})x_a(t) + B_{ua}u(t) + G_a\Phi(x(t)) + B_{fa}f_a(t) + B_{da}d(t) + Ky(t) \tag{6}$$

Let $S = E + KC_a$, then $S = \begin{bmatrix} I & 0 \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} 0 \\ I \end{bmatrix}\begin{bmatrix} C & D_s \end{bmatrix} = \begin{bmatrix} I & 0 \\ C & D_s \end{bmatrix}$,
Adding $KC_a\dot{x}_a(t)$ to both sides of Equation (6), we obtain

$$\begin{gathered} S\dot{x}_a(t) = (A_a - KC_{a1})x_a(t) + B_{ua}u(t) + G_a\Phi(x(t)) \\ +B_{fa}f_a(t) + B_{da}d(t) + Ky(t) + K\dot{y}(t) \end{gathered} \tag{7}$$

From $S = \begin{bmatrix} I & 0 \\ C & D_s \end{bmatrix}$, we can obtain a left-inverse as follows:

$$S^+ = \begin{bmatrix} I & 0 \\ -\left(D_s^T D_s\right)^{-1} D_s^T C & \left(D_s^T D_s\right)^{-1} D_s^T \end{bmatrix} \tag{8}$$

so that $S^+S = I$.

By left-multiplying both sides of Equation (7) by S^+, we can obtain

$$\begin{gathered} \dot{x}_a(t) = S^+(A_a - KC_{a1})x_a(t) + S^+B_{ua}u(t) + S^+G_a\Phi(x(t)) \\ +S^+B_{fa}f_a(t) + S^+B_{da}d(t) + S^+Ky(t) + S^+K\dot{y}(t) \end{gathered} \tag{9}$$

Let

$$\begin{gathered} A_e = S^+(A_a - KC_{a1}), B_e = S^+B_{ua}, G_e = S^+G_a, \\ B_{fe} = S^+B_{fa}, B_{de} = S^+B_{da}, K_e = S^+K. \end{gathered} \tag{10}$$

Then, Equation (9) can be rewritten as

$$\dot{x}_a(t) = A_e x_a(t) + B_e u(t) + G_e \Phi(x(t)) + B_{fe} f_a(t) + B_{de} d(t) + K_e y(t) + K_e \dot{y}(t) \tag{11}$$

Let

$$\xi(t) = x_a(t) - K_e y(t) \tag{12}$$

Equation (11) becomes

$$\dot{\xi}(t) = A_e x_a(t) + B_e u(t) + G_e \Phi(x(t)) + B_{fe} f_a(t) + B_{de} d(t) + K_e y(t) \tag{13}$$

Substituting $x_a(t) = \xi(t) + K_e y(t)$ into (13), we have

$$\dot{\xi}(t) = A_e \xi(t) + B_e u(t) + G_e \Phi(x(t)) + B_{fe} f_a(t) + B_{de} d(t) + (K_e + A_e K_e) y(t) \tag{14}$$

As a result, the augmented equivalent system above has been obtained by using descriptor system theory and transformation.

3.2. Augmented Sliding-Mode Observer

For the augmented system (14), a sliding-mode observer in the following form can be constructed:

$$\begin{cases} \dot{\hat{\xi}}(t) = A_e \hat{\xi}(t) + B_e u(t) + G_e \Phi(\hat{x}(t)) + B_{fe} \nu + (K_e + A_e K_e) y(t) + L(y(t) - \hat{y}(t)) \\ \hat{x}_a(t) = \hat{\xi}(t) + K_e y(t) \\ \hat{y}(t) = C_a \hat{x}_a \end{cases} \tag{15}$$

where $\hat{\xi}(t) \in R^{n+r}$ is estimate of the state $\xi(t)$, $\hat{x}_a(t) \in R^{n+r}$ is the estimate of the augmented state $x_a(t) \in R^{n+r}$, and ν is the sliding-mode term to be designed. $L \in R^{(n+r) \times p}$ is the gain to be solved.

Derived from Equation (15), one has

$$\dot{\hat{x}}_a(t) = A_e \hat{x}_a(t) + B_e u(t) + G_e \Phi(\hat{x}(t)) + B_{fe} \nu + K_e y(t) + L(y(t) - \hat{y}(t)) + K_e \dot{y}(t) \tag{16}$$

Let

$$e_a(t) = x_a(t) - \hat{x}_a(t) \tag{17}$$

$$\Phi_r(t) = \Phi(x(t)) - \Phi(\hat{x}(t)) \tag{18}$$

$$\nu = \begin{cases} \rho \frac{Fe_y}{\|Fe_y\|} & if \ \| Fe_y \| \neq 0 \\ 0 & if \ \| Fe_y \| = 0 \end{cases} \tag{19}$$

where $\rho \geq \rho_0 + \alpha$ is the sliding-mode gain to be designed, α is the upper bound of $\|f_a(t)\|$, ρ_0 is the positive scalar, $F \in R^{q \times p}$ is the gain matrix to be solved, and e_y is the output estimation error, which is $y(t) - \hat{y}(t) = C_a e_a(t)$.

Subtracting (16) from (11), we can obtain

$$\dot{e}_a(t) = (A_e - LC_a) e_a(t) + G_e \Phi_r(t) + B_{fe}(f_a(t) - \nu) + B_{de} d(t) \tag{20}$$

3.3. Stability Analysis

Lemma 1 ([25]). *For any positive scalar μ and real constant matrices $x, y \in R^n$, the following inequality holds:*

$$2x^T y \leq \mu x^T x + \frac{1}{\mu} y^T y \tag{21}$$

Lemma 2 ([34]). *Given a symmetric matrix,* $S = \begin{bmatrix} S_{11} & S_{12} \\ S_{12}^T & S_{22} \end{bmatrix}$. $S < 0$ *if and only if* $S_{22} < 0$ *and* $S_{11} - S_{12}S_{22}^{-1}S_{12}^T < 0$.

The above lemma is known as the Schur complement lemma, which is useful for the design of the observer gains in this paper.

Theorem 1. *For system (4), there exists an augmented sliding-mode observer in the form of (15) such that the estimation error dynamics in (20) is robustly stable and satisfies the robust performance index* $\parallel e_a \parallel_{T_f} \leq r \parallel d(t) \parallel_{T_f}$. *If there exist a symmetric positive definite matrix P, positive scalars μ and r, and a matrix Y for a given positive constant γ, the following inequality holds:*

$$PB_{fe} = C_a^T F^T \tag{22}$$

$$\begin{bmatrix} PA_e - YC_a + A_e^T P - C_a^T Y^T + \left(\mu\gamma^2 + 1\right)I & PB_{de} & PG_e \\ B_{de}{}^T P & -r^2 I & 0 \\ G_e^T P & 0 & -\mu I \end{bmatrix} < 0 \tag{23}$$

The observer gain can be calculated by $L = P^{-1}Y$, where $\|e_a\|_{Tf} = (\int_0^{Tf} e_a{}^T(t)e_a(t)dt)^{\frac{1}{2}}$, $\|d\|_{Tf} = (\int_0^{Tf} d^T(t)d(t)dt)^{\frac{1}{2}}$.

Proof.

(i). Asymptotic stability when $d = 0$.

Define a Lyapunov function candidate of the error dynamic system (20) as

$$V(e_a) = e_a{}^T P e_a \tag{24}$$

In terms of (20), one has

$$\begin{aligned} \dot{V}(e_a) = & e_a{}^T \left[P(A_e - LC_a) + (A_e - LC_a)^T P \right] e_a + 2e_a{}^T PG_e \Phi_r(t) \\ & + 2e_a{}^T PB_{fe}(f_a(t) - \nu) + 2e_a{}^T PB_{de} d(t). \end{aligned} \tag{25}$$

From Equations (19) and (22), and noticing that $\|f_a\| \leq \alpha$ and $\rho \geq \rho_0 + \alpha$, we can obtain

$$\begin{aligned} e_a{}^T PB_{fe}(f_a(t) - \nu) = \; & e_a{}^T PB_{fe} f_a(t) - e_a{}^T PB_{fe} \rho \tfrac{Fe_y}{\|Fe_y\|} \\ & \leq e_a{}^T PB_{fe} f_a(t) - e_a{}^T C_a^T F^T \rho \tfrac{Fe_y}{\|Fe_y\|} \\ & = e_a{}^T PB_{fe} f_a(t) - \rho \tfrac{(Fe_y)^T Fe_y}{\|Fe_y\|} \\ & \leq \parallel e_a{}^T PB_{fe} \parallel \parallel f_a(t) \parallel - \rho \parallel Fe_y \parallel \\ & = \parallel e_a{}^T PB_{fe} \parallel \parallel f_a(t) \parallel - \rho \parallel FC_a e_a \parallel \\ & = \parallel e_a{}^T PB_{fe} \parallel \parallel f_a(t) \parallel - \rho \parallel B_{fe}^T P e_a \parallel \\ & = (\alpha - \rho) \parallel e_a{}^T PB_{fe} \parallel \\ & \leq -\rho_0 \parallel e_a{}^T PB_{fe} \parallel \leq 0 \end{aligned} \tag{26}$$

Furthermore, from Assumption 1 and Lemma 1, it can be deduced that

$$2e_a{}^T PG_e \Phi_r(t) \leq \frac{1}{\mu}(G_e^T P e_a)^T (G_e^T P e_a) + \mu\gamma^2 e_a{}^T e_a \tag{27}$$

Substituting the results of Equation (26) and Equation (27) into (25), one can have

$$\dot{V}(e_a) \leq e_a{}^T \left[P(A_e - LC_a) + (A_e - LC_a)^T P + \frac{1}{\mu} PG_e G_e^T P + \mu\gamma^2 I \right] e_a + 2e_a{}^T PB_{de} d(t) \tag{28}$$

Noting that $Y = PL$ and using Schur complement shown in Lemma 2 to (23), we have

$$\Omega = \begin{bmatrix} P(A_e - LC_a) + (A_e - LC_a)^T P + \frac{1}{\mu} P G_e G_e^T P + \left(\mu\gamma^2 + 1\right) I & PB_{de} \\ {B_{de}}^T P & -r^2 I \end{bmatrix} < 0 \tag{29}$$

which means

$$P(A_e - LC_a) + (A_e - LC_a)^T P + \frac{1}{\mu} P G_e G_e^T P + \mu\gamma^2 I < 0 \tag{30}$$

From (28) and (30), we can obtain $\dot{V}(e_a) < 0$ when $d = 0$. Therefore, the estimation error dynamics in (20) is asymptotically stable when $d = 0$.

(ii). Robust stability when $d \neq 0$.

Let

$$\Gamma = \int_0^{T_f} \left({e_a}^T e_a - r^2 d(t)^T d(t)\right) dt \tag{31}$$

By using (28) and (31), one has

$$\begin{aligned} \Gamma &= \int_0^{T_f} \left({e_a}^T e_a - r^2 d(t)^T d(t) + \dot{V}(e_a)\right) dt - \int_0^{T_f} \dot{V}(e_a) dt \\ &= \int_0^{T_f} \Big\{ {e_a}^T \Big[I + P(A_e - LC_a) + (A_e - LC_a)^T P + \tfrac{1}{\mu} P G_e G_e^T P + \mu\gamma^2 I \Big] e_a \\ &\quad + 2{e_a}^T P B_{de} d(t) - r^2 d(t)^T d(t) \Big\} \mathrm{dt} - \int_0^{T_f} \dot{V}(e_a) dt \\ &= \int_0^{T_f} \Big[{e_a}^T d(t)^T \Big] \Omega \begin{pmatrix} e_a \\ d(t) \end{pmatrix} dt - \int_0^{T_f} \dot{V}(e_a) dt \end{aligned} \tag{32}$$

where Ω is defined in (29).

Under zero initial condition $e_a(0) = 0$, one has

$$\int_0^{T_f} \dot{V}(e_a) dt = {e_a}^T(T_f) P e_a(T_f) - {e_a}^T(0) P e_a(0) = V\left(e_\xi(T_f)\right) \geq 0. \tag{33}$$

Since $\Omega < 0$ and $\int_0^{Tf} \dot{V}(e_a) dt \geq 0$, from (32), we have $\Gamma \leq 0$, indicating $\| e_a \|_{T_f} \leq r \| d(t) \|_{T_f}$. As a result, the robust performance index is satisfied. □

3.4. Accessibility Analysis of Sliding Surface in Finite Time

To ensure the rapid response of the system to sliding-mode inputs, assist in the quick recovery of the system to the desired state when subjected to disturbances or external perturbations, and enhance the system's robustness, it is necessary to determine the gain ρ in the sliding term of Equation (19), ensuring that the state error system moves onto the sliding surface s within a finite time.

Theorem 2. *Consider a siding mode surface $s = (e_a(t) : e_a(t) = 0)$. For a given positive scalar σ, if the gain ρ_0 satisfies*

$$\rho_0 \geq \left(\lambda_{min}(PB_{fe})\right)^{-1} \left(\left(\| P(A_e - LC_a) \| + \gamma \| PG_e \|\right)\theta + \delta \| PB_{de} \| + \sigma\right) \tag{34}$$

the error dynamic system (20) can reach the sliding surface within a finite time.

Proof.

Define a Lyapunov function candidate as

$$V(s) = s^T P s \tag{35}$$

In terms of (19), and noting that $\rho \geq \rho_0 + \alpha$ and $\|f_a\| \leq \alpha$, one has

$$\begin{aligned} \dot{V}(s) &= 2s^T P \dot{s} \\ &= 2{e_a}^T P\Big[(A_e - LC_a)e_a(t) + G_e\Phi_r(t) + B_{fe}(f_a(t) - \nu) + B_{de}d(t)\Big] \\ &\leq 2{e_a}^T P\Big[(A_e - LC_a)e_a(t) + G_e\Phi_r(t) + B_{fe}f_a(t) - \rho B_{fe}\tfrac{Fe_y}{\|Fe_y\|} + B_{de}d(t)\Big] \\ &= 2{e_a}^T P\Big[(A_e - LC_a)e_a(t) + G_e\Phi_r(t) + B_{fe}f_a(t) - \rho B_{fe}\tfrac{FC_a e_a(t)}{\|FC_a e_a(t)\|} + B_{de}d(t)\Big] \\ &\leq 2 \parallel {e_a}^T \parallel \{\parallel P(A_e - LC_a)e_a(t) \parallel + \gamma \parallel PG_e \parallel \parallel e_a(t) \parallel + \delta \parallel PB_{de} \parallel\} \\ &+2(\alpha - \rho) \parallel {e_a}^T PB_{fe} \parallel \\ &\leq 2 \parallel {e_a}^T \parallel \{\parallel P(A_e - LC_a)e_a(t) \parallel + \gamma \parallel PG_e \parallel \parallel e_a(t) \parallel + \delta \parallel PB_{de} \parallel\} \\ &-2\rho_0 \parallel {e_a}^T PB_{fe} \parallel \end{aligned} \tag{36}$$

If the optimization problem in Theorem 1 has a feasible solution, the dynamic state error $e_a(t)$ is bounded, i.e., $sup \parallel e_a(t) \parallel \leq \theta, t \in [0, \infty)$, where θ is a smaller positive scalar. Then, from (36), one can have

$$\begin{aligned} \dot{V}(s) &\leq 2 \parallel {e_a}^T \parallel \{(\parallel P(A_e - LC_a) \parallel + \gamma \parallel PG_e \parallel)\theta + \delta \parallel PB_{de} \parallel\} \\ &-2\rho_0 \lambda_{min}(PB_{fe}) \parallel {e_a}^T \parallel \\ &\leq 2 \parallel {e_a}^T \parallel \Big\{(\parallel P(A_e - LC_a) \parallel + \gamma \parallel PG_e \parallel)\theta + \delta \parallel PB_{de} \parallel - \rho_0 \lambda_{min}\Big(PB_{fe}\Big)\Big\} \end{aligned} \tag{37}$$

When $\rho_0 \geq \Big(\lambda_{min}\Big(PB_{fe}\Big)\Big)^{-1}((\parallel P(A_e - LC_a) \parallel + \gamma \parallel PG_e \parallel)\theta + \delta \parallel PB_{de} \parallel + \sigma)$ holds, we have

$$\dot{V}(s) \leq -2\sigma \parallel {e_a}^T \parallel \leq -2\sigma\sqrt{\lambda_{min}(P^{-1})}\sqrt{V(s)} \tag{38}$$

As a result, the error dynamic system can reach the sliding surface within a finite time. This completes the proof. □

3.5. Robust State and Attack Estimation

When the error dynamic system moves to the sliding-mode surface, $e_a(t) = \dot{e}_a(t) = 0$; then, the error equation of (21) can be abbreviated as

$$B_{fe}\big(\nu_{eq} - f_a(t)\big) = G_e\Phi_r(t) + B_{de}d(t) \tag{39}$$

where ν_{eq} is the equivalent output signal of ν.

Note that $\parallel B_{fe}(\nu - f_a(t)) \parallel \leq \Upsilon$, where $\Upsilon = (\gamma \parallel G_e \parallel)\theta + \delta \parallel B_{de} \parallel$. When Υ is minimized as much as possible, we can obtain $\hat{f}_a(t) = \nu_{eq}$, and then

$$\hat{f}_a(t) = \nu_{eq} = \rho\frac{Fe_y}{\parallel Fe_y \parallel + \varpi} \tag{40}$$

where, $\varpi > 0$ is a small positive scalar that can reduce vibration during the sliding-mode motion process.

With the observer in the form of Equation (15) and the augmented state $x_a(t) = \Big[x(t)^T \quad f_s(t)^T\Big]$, we can easily obtain estimates of state and sensor attack signals, namely

$$\begin{cases} \hat{x}(t) = \begin{bmatrix} I_n & 0_{n\times r}\end{bmatrix}\hat{x}_a(t) \\ \hat{f}_s(t) = \begin{bmatrix} 0_{r\times n} & I_{r\times r}\end{bmatrix}\hat{x}_a(t) \end{cases} \tag{41}$$

Remark 2. *From Equation (40), the proposed attack signal reconstruction scheme is not limited by the type of attack signal, meaning it is applicable to step-type, sinusoidal, and other types of attack signals.*

3.6. Design Procedure of Robust SMO for FDI Estimation

The design procedure of the addressed robust sliding-model observer can be summarized as below:

(i). Construct the descriptor augmented system in the form of (4). Calculate the augmented matrices $E, A_a, B_{ua}, G_a, B_{fa}, B_{da}, C_a$, and C_{a1} in terms of (5).

(ii). Select the gain $K = \begin{bmatrix} 0 \\ I \end{bmatrix}$, so that $S = E + KC_a$ is nonsingular. Calculate the matrices $A_e, B_e, G_e, B_{fe}, B_{de}$, and K_e in terms of (10).

(iii). Compute the observer gain $L = P^{-1}Y$, where P and Y can be obtained by solving Equations (22) and (23).

(iv). Select the sliding-mode term ρ to ensure that the error dynamic system (20) can reach the sliding surface within a finite time.

(v). Establish the estimator in the form of (15), where the parameters are available from steps (i)–(iv). Carry out the real-time estimation to obtain the estimated vector $\hat{x}_a(t)$. As a result, the reconstructed signals for system state, sensor attack, and actuator attack vectors can be readily formulated as follows:

$$\begin{cases} \hat{x}(t) = \begin{bmatrix} I_n & 0_{n\times r} \end{bmatrix} \hat{x}_a(t) \\ \hat{f}_s(t) = \begin{bmatrix} 0_{r\times n} & I_{r\times r} \end{bmatrix} \hat{x}_a(t) \\ \hat{f}_a(t) = v_{eq} = \rho \frac{Fe_y}{\|Fe_y\| + \varpi} \end{cases} \tag{42}$$

4. State and Attack Estimation Using Augmented Adaptive Observers

4.1. Design of an Adaptive Augmented Observer

Based on descriptor augmented system (4) and equivalent regular dynamic system (14), we can design an augmented adaptive observer in the following form:

$$\begin{cases} \dot{\hat{\xi}}(t) = A_e\hat{\xi}(t) + B_e u(t) + G_e\Phi(\hat{x}(t)) + B_{fe}\hat{f}_a(t) + (K_e + A_eK_e)y(t) + L_F(y(t) - \hat{y}(t)) \\ \hat{y}(t) = C_a\hat{x}_a(t) \\ \hat{x}_a(t) = \hat{\xi}(t) + K_e y(t) \end{cases} \tag{43}$$

$$\dot{\hat{f}}_a(t) = \Gamma R\big(e_y(t) + \dot{e}_y(t)\big) \tag{44}$$

where $\hat{\xi}(t) \in R^{n+r}$ is the estimate of the vector $\xi(t)$ in (14), $\hat{x}_a(t) \in R^{n+r}$ is the estimated value of the augmented state $x_a(t) \in R^{n+r}$, and $\hat{f}_a(t)$ is the estimate of the actuator attack signal. $L_F \in R^{(n+r)\times p}$ is the gain to be solved; Γ is the adaptive learning rate to be designed. $e_y(t)$ is the output error, i.e., $e_y(t) = y(t) - \hat{y}(t) = C_a e_a(t)$

From (43), we have

$$\begin{aligned} \dot{\hat{x}}_a(t) = \; & A_e\hat{x}_a(t) + B_e u(t) + G_e\Phi_a(\hat{x}(t)) + B_{fe}\hat{f}_a(t) + K_e y(t) \\ & + L_F(y(t) - \hat{y}(t)) + K_e\dot{y}(t) \end{aligned} \tag{45}$$

Define

$$e_f(t) = f_a(t) - \hat{f}_a(t) \tag{46}$$

By subtracting Equation (45) from Equation (11), we can obtain

$$\dot{e}_a(t) = (A_e - L_F C_a)e_a(t) + G_e\Phi_r(t) + B_{fe}e_f(t) + B_{de}d(t) \tag{47}$$

4.2. Robust Stability Analysis

Theorem 3. *For the dynamic system (4), there is an augmented adaptive observer in the shape of (43) and (44) such that the estimation error dynamics in (47) is robustly stable with the robust performance index* $\| e_a \|_{T_f} \leq \epsilon \| d(t) \|_{T_f} + \epsilon \| \dot{f}_{\mathrm{a}}(t) \|_{T_f}$*; if there exist a symmetric positive definite matrix Q; positive scalars* ϵ*,* η_1*,* η_2*, and* η_3*; and suitable matrices* Y_F *and R such that for a given positive constant* γ*, the following inequality holds*

$$B_{fe}{}^{T}Q = RC_a \tag{48}$$

$$\Gamma_m = \begin{bmatrix} \Gamma_{m11} & -A_e^T Q B_{fe} + C_a^T Y_F^T B_{fe} & QB_{de} & 0 & 0 & QG_e & 0 \\ * & \eta_1 I - 2B_{fe}{}^T Q B_{fe} & -B_{fe}{}^T Q B_{de} & 0 & 0 & 0 & B_{fe}{}^T Q G_e \\ * & * & -\epsilon^2 I & 0 & 0 & 0 & 0 \\ * & * & * & -\epsilon^2 I & \Gamma^{-1} & 0 & 0 \\ * & * & * & * & -\eta_1 I & 0 & 0 \\ * & * & * & * & * & -\eta_2 I & 0 \\ * & * & * & * & * & * & -\eta_3 I \end{bmatrix} < 0 \tag{49}$$

$$\Gamma_{m11} = A_e^T Q + Q A_e - C_a^T Y_F^T - Y_F C_a + \left(1 + \eta_2 \gamma^2 + \eta_3 \gamma^2\right) I \tag{50}$$

The observer gain can be calculated by $L_F = Q^{-1} Y_F$.

Proof.

(i). Asymptotic stability when $d = 0$ and $\dot{f}_{\mathrm{a}} = 0$.

Define a Lyapunov function candidate of the error dynamic system (47) as

$$V_F\left(e_a, e_f\right) = e_a{}^T Q e_a + e_f^T \Gamma^{-1} e_f \tag{51}$$

Using (47) and (51), one has

$$\begin{aligned} \dot{V}_F\left(e_a, e_f\right) = \;& e_a{}^T \left[Q(A_e - L_F C_a) + (A_e - L_F C_a)^T Q\right] e_a + 2e_a{}^T Q G_e \Phi_r(t) \\ & + 2e_a{}^T Q B_{fe} e_f(t) + 2e_a{}^T Q B_{de} d(t) + 2e_f^T(t) \Gamma^{-1} \dot{e}_f(t) \end{aligned} \tag{52}$$

From Equation (44), we can deduce that

$$\begin{aligned} 2e_f^T(t)\Gamma^{-1}\dot{e}_f(t) &= 2e_f^T(t)\Gamma^{-1}\left(\dot{f}_a(t) - \dot{\hat{f}}_a(t)\right) \\ &= 2e_f^T(t)\Gamma^{-1}\dot{f}_a(t) - 2e_f^T(t)R\left(e_y(t) + \dot{e}_y(t)\right) \\ &= 2e_f^T(t)\Gamma^{-1}\dot{f}_a(t) - 2e_f^T(t)RC_a e_a - 2e_f^T(t)RC_a\dot{e}_a(\mathrm{t}) \end{aligned} \tag{53}$$

Substituting (47) and (53) into (52) and using (48), one can have

$$\begin{aligned} \dot{V}_F(e_a, e_f) &= e_a{}^T \left[Q(A_e - L_F C_a) + (A_e - L_F C_a)^T Q\right] e_a \\ &\quad + 2e_a{}^T Q G_e \Phi_r(t) + 2e_a{}^T Q B_{de} d(t) + 2e_f^T(t)\Gamma^{-1}\dot{f}_a(t) \\ &\quad - 2e_f^T(t) B_{fe}{}^T Q (A_e - L_F C_a) e_a(t) - 2e_f^T(t) B_{fe}{}^T Q G_e \Phi_r(t) \\ &\quad - 2e_f^T(t) B_{fe}{}^T Q B_{fe} e_f(t) - 2e_f^T(t) B_{fe}{}^T Q B_{de} d(t) \end{aligned} \tag{54}$$

Using Lemma 1, we can obtain

$$2e_f^T(t)\Gamma^{-1}\dot{f}_a(t) \leq \eta_1 e_f^T(t) e_f(t) + \frac{1}{\eta_1}\dot{f}_a(t)^T \Gamma^{-T}\Gamma^{-1}\dot{f}_a(t) \tag{55}$$

$$2{e_a}^T QG_e\Phi_r(t) \leq \frac{1}{\eta_2}{e_a}^T QG_eG_e^TQe_a + \eta_2\gamma^2{e_a}^Te_a \tag{56}$$

$$-2e_f^T(t){B_{fe}}^TQG_e\Phi_r(t) \leq \frac{1}{\eta_3}e_f^T(t){B_{fe}}^TQG_eG_e^TQB_{fe}e_f(t) + \eta_3\gamma^2{e_a}^Te_a \tag{57}$$

Substituting (55)–(57) into (54), one can have

$$\begin{aligned}\dot{V}_F(e_a, e_f) = \;& {e_a}^T\Big[Q(A_e - L_FC_a) + (A_e - L_FC_a)^TQ + \tfrac{1}{\eta_2}QG_eG_e^TQ + \eta_2\gamma^2I + \eta_3\gamma^2I\Big]e_a \\ & + 2{e_a}^TQB_{de}d(t) + e_f^T(t)\Big[\eta_1I + \tfrac{1}{\eta_3}e_f^T(t){B_{fe}}^TQG_eG_e^TQB_{fe}e_f(t) - 2{B_{fe}}^TQB_{fe}\Big]e_f(t) \\ & - 2e_f^T(t){B_{fe}}^TQ(A_e - L_FC_a)e_a(t) - 2e_f^T(t){B_{fe}}^TQB_{de}d(t) \\ & + \tfrac{1}{\eta_1}\dot{f}_a(t)^T\Gamma^{-T}\Gamma^{-1}\dot{f}_a(t)\end{aligned} \tag{58}$$

Letting $Y_F = QL_F$, and applying the Schur complement to (50), we have

$$\Pi = \begin{bmatrix} \Pi_{11} & -(A_e - L_FC_a)^TQB_{fe} & QB_{de} & 0 \\ * & \eta_1I + \frac{1}{\eta_3}{B_{fe}}^TQG_eG_e^TQB_{fe} - 2{B_{fe}}^TQB_{fe} & -{B_{fe}}^TQB_{de} & 0 \\ * & * & -\epsilon^2I & 0 \\ * & * & * & -\epsilon^2I + \frac{1}{\eta_1}\Gamma^{-T}\Gamma^{-1}\end{bmatrix} < 0 \tag{59}$$

$$\Pi_{11} = I + Q(A_e - L_FC_a) + (A_e - L_FC_a)^TQ + \frac{1}{\eta_2}QG_eG_e^TQ + \eta_2\gamma^2I + \eta_3\gamma^2I \tag{60}$$

It is clear that (59) indicates

$$\begin{bmatrix} \Pi_{11m} & -(A_e - L_FC_a)^TQB_{fe} \\ * & \eta_1I + \frac{1}{\eta_3}{B_{fe}}^TQG_eG_e^TQB_{fe} - 2{B_{fe}}^TQB_{fe}\end{bmatrix} < 0 \tag{61}$$

where

$$\Pi_{11m} = Q(A_e - L_FC_a) + (A_e - L_FC_a)^TQ + \frac{1}{\eta_2}QG_eG_e^TQ + \eta_2\gamma^2I + \eta_3\gamma^2I \tag{62}$$

Therefore, (61) means $\dot{V}_F\left(e_a, e_f\right) < 0$ when $d = 0$ and $\dot{f}_{\mathrm{a}} = 0$. Therefore, the estimation error dynamics (47) is asymptotically stable when $d = 0$ and $\dot{f}_{\mathrm{a}} = 0$.

(ii). Robust stability when $d \neq 0$ and $\dot{f}_{\mathrm{a}} \neq 0$.

Let

$$\Theta = \int_0^{T_f}\left({e_a}^Te_a - \epsilon^2d(t)^Td(t) - \epsilon^2\dot{f}_a(t)^T\dot{f}_a(t)\Big)dt\right. \tag{63}$$

By using (58) and (63), one has

$$\begin{aligned}\Theta &= \textstyle\int_0^{T_f}({e_a}^Te_a - \epsilon^2d(t)^Td(t) - \dot{f}_a(t)^T\dot{f}_a(t) + \dot{V}_F(e_a))dt - \int_0^{T_f}\dot{V}_F(e_a)dt \\ &= \textstyle\int_0^{T_f}\Big\{{e_a}^T\Big[I + Q(A_e - L_FC_a) + (A_e - L_FC_a)^TQ + \frac{1}{\eta_2}QG_eG_e^TQ + \eta_2\gamma^2I + \eta_3\gamma^2I\Big]e_a \\ &\quad + 2{e_a}^TQB_{de}d(t) + e_f^T(t)\Big[\eta_1I + \tfrac{1}{\eta_3}e_f^T(t){B_{fe}}^TQG_eG_e^TQB_{fe}e_f(t) - 2{B_{fe}}^TQB_{fe}\Big]e_f(t) \\ &\quad - 2e_f^T(t){B_{fe}}^TQ(A_e - L_FC_a)e_a(t) - 2e_f^T(t){B_{fe}}^TQB_{de}d(t) + \tfrac{1}{\eta_1}\dot{f}_a(t)^T\Gamma^{-T}\Gamma^{-1}\dot{f}_a(t) \\ &\quad - \epsilon^2d(t)^Td(t) - \epsilon^2\dot{f}_a(t)^T\dot{f}_a(t)\Big\}dt - \textstyle\int_0^{T_f}\dot{V}_F(e_a)dt \\ &= \textstyle\int_0^{T_f}[\zeta^T\Pi\zeta]dt - \int_0^{T_f}\dot{V}_F(e_a)dt\end{aligned} \tag{64}$$

where

$$\zeta = \begin{bmatrix} e_a(t) \\ e_f(t) \\ d(t) \\ \dot{f}_a(t) \end{bmatrix} \tag{65}$$

and Π is defined as shown on the left-hand side of (59). As $\Pi < 0$ and $\int_0^{T_f} \dot{V}_F(e_a)dt \geq 0$, from (64), we have $\Theta \leq 0$, indicating $\| e_a \|_{T_f} \leq \epsilon \| d(t) \|_{T_f} + \epsilon \| \dot{f}_{\text{a}}(t) \|_{T_f}$. As a result, the robust performance index is satisfied. The proof is completed. □

4.3. Robust State and Attack Reconstruction

From Equation (44), we can easily obtain

$$\hat{f}_a(t) = \int_{t_f}^{t} \Gamma R\big(e_y(t) + \dot{e}_y(t)\big)dt \tag{66}$$

where t_f denotes the instant when the attack occurs.

The state and sensor attack signals can be reconstructed as follows:

$$\begin{cases} \hat{x}(t) = \begin{bmatrix} I_n & 0_{n\times r} \end{bmatrix} \hat{x}_a(t) \\ \hat{f}_s(t) = \begin{bmatrix} 0_{r\times n} & I_{r\times r} \end{bmatrix} \hat{x}_a(t) \end{cases} \tag{67}$$

4.4. Design Procedure for the Reconstruction of the Attack Signals

The design procedure of the proposed robust fast adaptive observer for attack signal reconstruction can be highlighted as shown:

(i). Build the augmented system as shown in (4). Calculate the augmented matrices $E, A_a, B_{ua}, G_a, B_{fa}, B_{da}, C_a$, and C_{a1} in terms of (5).

(ii). Select the gain $K = \begin{bmatrix} 0 \\ I \end{bmatrix}$, so that the matrix $S = E + KC_a$ is nonsingular. Calculate the changed matrix $A_e, B_e, G_e, B_{fe}, B_{de}$, and K_e in terms of (10).

(iii). Select the adaptive learning rate Γ

(iv). Compute $L_F = Q^{-1}Y_F$, where Q and Y_F can be obtained by solving Equations (48) and (49).

(v). Establish estimators (43) and (44) where the parameters are available from steps (i)–(iv) and apply real-time simulation to identify the estimated vector $\hat{x}_a(t)$. Hence, the estimated signals for the system state, sensor attack, and actuator attack vectors can be readily formulated as follows:

$$\begin{cases} \hat{x}(t) = \begin{bmatrix} I_n & 0_{n\times r} \end{bmatrix} \hat{x}_a(t) \\ \hat{f}_s(t) = \begin{bmatrix} 0_{r\times n} & I_{r\times r} \end{bmatrix} \hat{x}_a(t) \\ \hat{f}_a(t) = \int_{t_f}^{t} \Gamma R\big(e_y(t) + \dot{e}_y(t)\big)dt \end{cases} \tag{68}$$

5. Simulation Study

In this section, considering the linearized longitudinal dynamic system of the VTOL aircraft [35] to validate the effectiveness of the proposed method, we assume that the system is subjected to nonlinear dynamics, unknown disturbances, actuator attacks, and sensor attacks simultaneously. Therefore, the state-space dynamic expression can be described as shown in (1), where the states $x(t)$ include horizontal velocity, vertical velocity, pitch rate, and pitch angle. The system parameters are as follows:

$$\begin{aligned}
A &= \begin{bmatrix} -9.9477 & -0.7476 & 0.2632 & 5.0337 \\ 52.1659 & 2.7452 & 5.5532 & -24.4221 \\ 26.0922 & 2.6361 & -4.1975 & -19.2774 \\ 0 & 0 & 1.0000 & 0 \end{bmatrix} \\
B &= \begin{bmatrix} 0.4422 & 0.1761 \\ 3.5446 & -7.5922 \\ -5.5200 & 4.4900 \\ 0 & 0 \end{bmatrix}, \\
G &= \begin{bmatrix} 0 \\ -0.1 \\ 0 \\ 0 \end{bmatrix},\ B_a = \begin{bmatrix} 0.1761 \\ -7.5922 \\ 4.4900 \\ 0 \end{bmatrix}, C = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{bmatrix}, \\
B_d &= \begin{bmatrix} 0.01 & 0 \\ 0.02 & 0 \\ 0 & -0.01 \\ 0 & 0.01 \end{bmatrix},\ \Phi(x(t)) = \sin(x_4),\ D_s = \begin{bmatrix} 1 & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & 1 \end{bmatrix}.
\end{aligned} \tag{69}$$

From the parameter matrices mentioned above, the augmented matrices E and $A_e, B_e, G_e, B_{fe}, B_{de}, K_e$ in the form of Equations (5) and (10) can be calculated.

In this simulation, the disturbance signals $d(t) = \begin{bmatrix} d_1^T(t) & d_2^T(t) \end{bmatrix}^T$ are depicted in Figure 2, which are high-frequency signals corrupted by band-limited white noises.

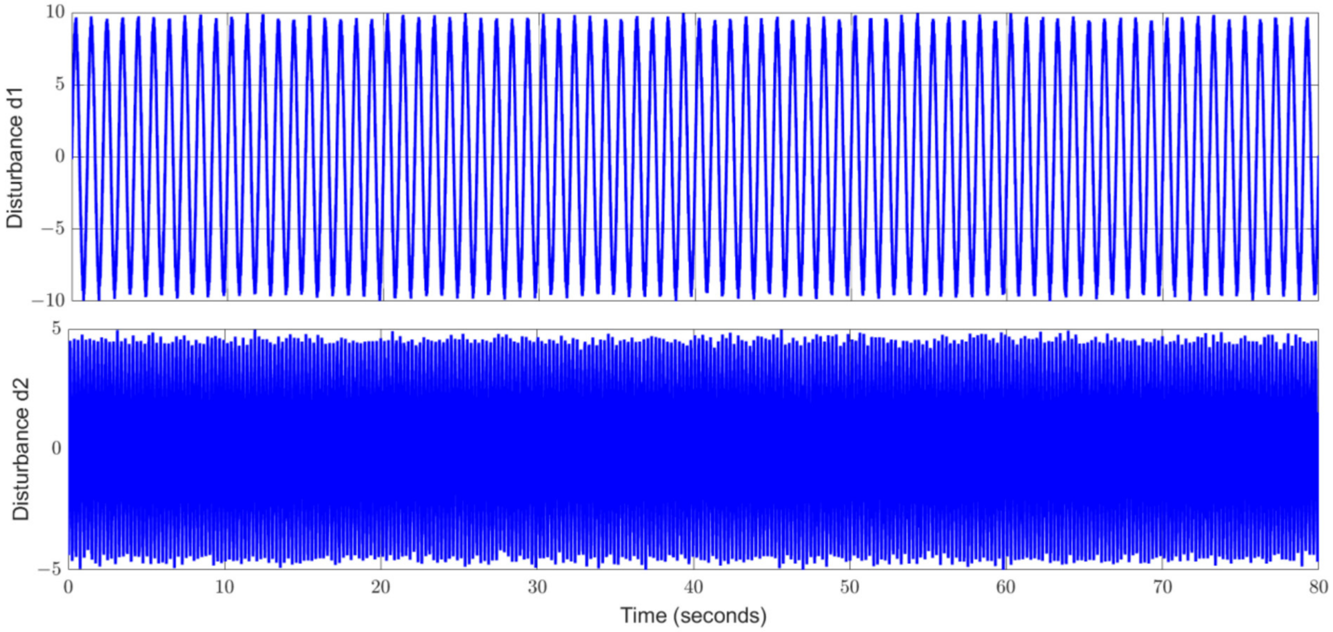

Figure 2. Input disturbance signals.

(i). Robust augmented sliding-mode observer

To evaluate the performance of the estimator, one can consider the following actuator time-varying attack signal $f_a(t)$ and sensor attack signals $f_{s1}(t)$ and $f_{s2}(t)$:

$$f_a(t) = \begin{cases} sin^2(0.5t), & 12.5 < t \le 30 \\ cos(5t), & 40 < t \le 50 \\ cos(10t), & 60 < t \le 80 \\ 0, & else \end{cases} \tag{70}$$

$$f_{s1}(t) = \begin{cases} -0.25y_1(t), & 15 < t \leq 55 \\ \textit{square wave signal}, & 60 < t \leq 77.5 \\ 0, & \textit{else} \end{cases} \tag{71}$$

$$f_{s2}(t) = \begin{cases} 1, & 10 < t \leq 30 \\ -0.01t^2 + 0.5(t-30), & 30 < t \leq 50 \\ -0.2(t-50), & 50 < t \leq 75 \\ 0, & \textit{else} \end{cases} \tag{72}$$

By solving (22) and (23), the gains are calculated as

$$L = \begin{bmatrix} -4.2916 & 25.7162 & 11.9250 & 5.0171 \\ 3.1577 & 48.3240 & 24.7412 & -53.6838 \\ -1.1818 & 17.5667 & -7.3616 & 3.1981 \\ -9.1213 & 14.1767 & -20.9020 & 4.0719 \\ 4.9909 & -24.4892 & -14.8587 & 13.5067 \\ -29.0488 & 88.2902 & 11.4565 & 3.0402 \end{bmatrix} \tag{73}$$

$$F = \begin{bmatrix} 0.0000 & -3.5095 & 1.3120 & 0.5494 \end{bmatrix}. \tag{74}$$

Therefore, utilizing the estimator in the form of Equation (15) with the gains provided above, we can obtain curves for the states, attacks, and their respective estimates. Figures 3–6 display the system states and their estimates, and Figures 7–9 exhibit the attacks and their estimates. One can see that the estimated curves track the system states and attacks excellently.

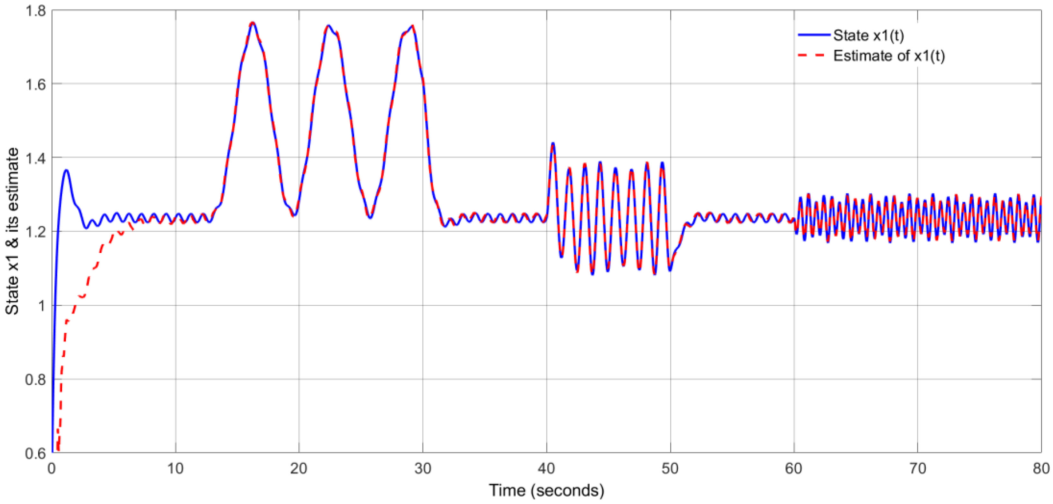

Figure 3. State $x_1(t)$ and its estimate: augmented sliding-mode technique.

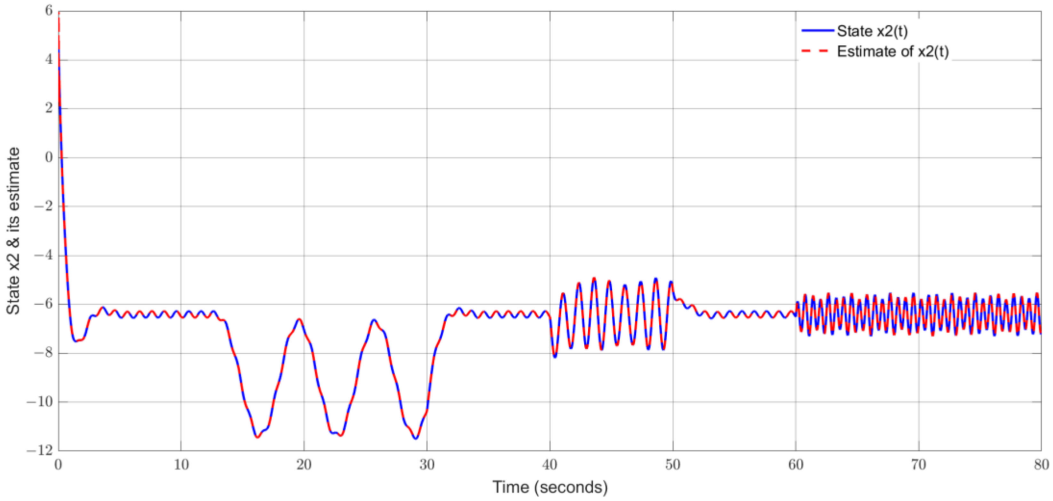

Figure 4. State $x_2(t)$ and its estimate: augmented sliding-mode technique.

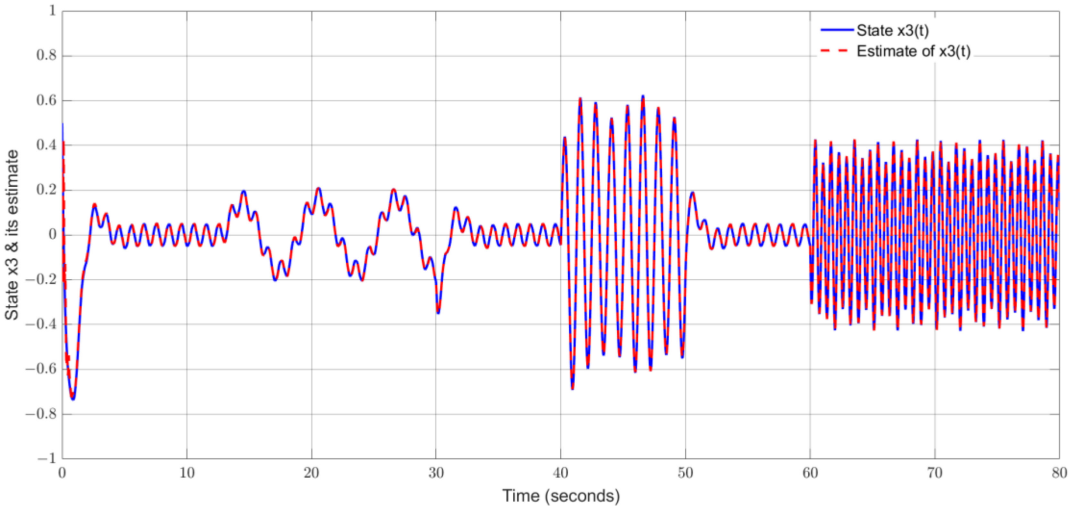

Figure 5. State $x_3(t)$ and its estimate: augmented sliding-mode technique.

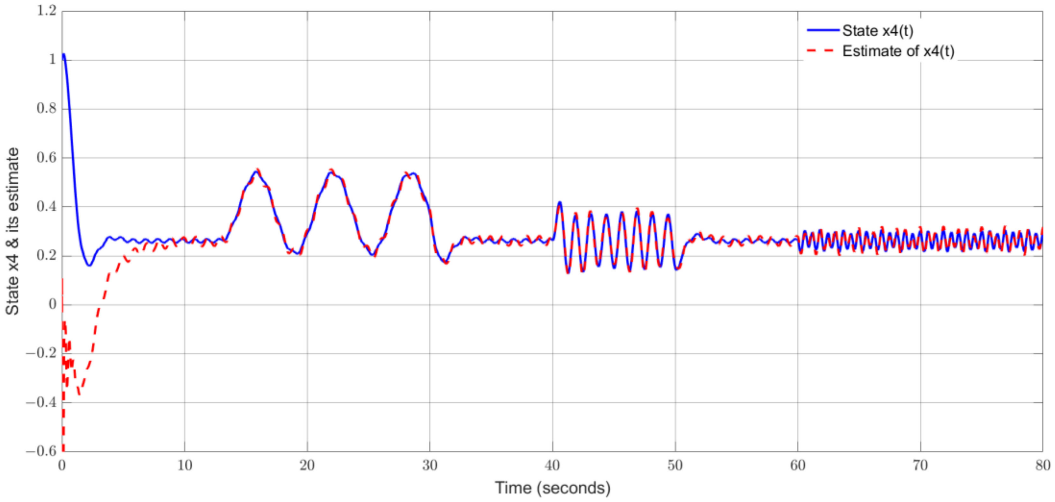

Figure 6. State $x_4(t)$ and its estimate: augmented sliding-mode technique.

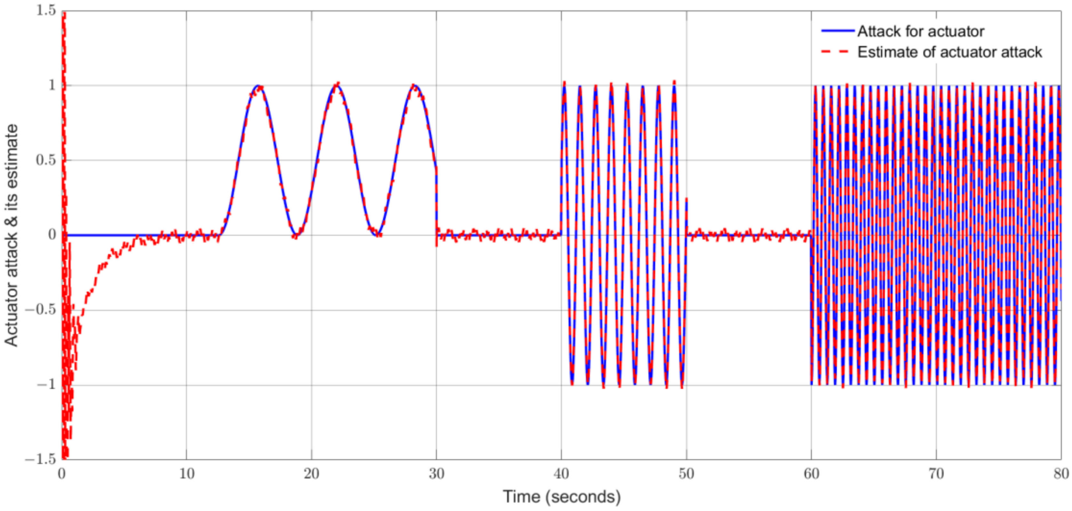

Figure 7. Actuator attack signal and its estimate: augmented sliding-mode technique.

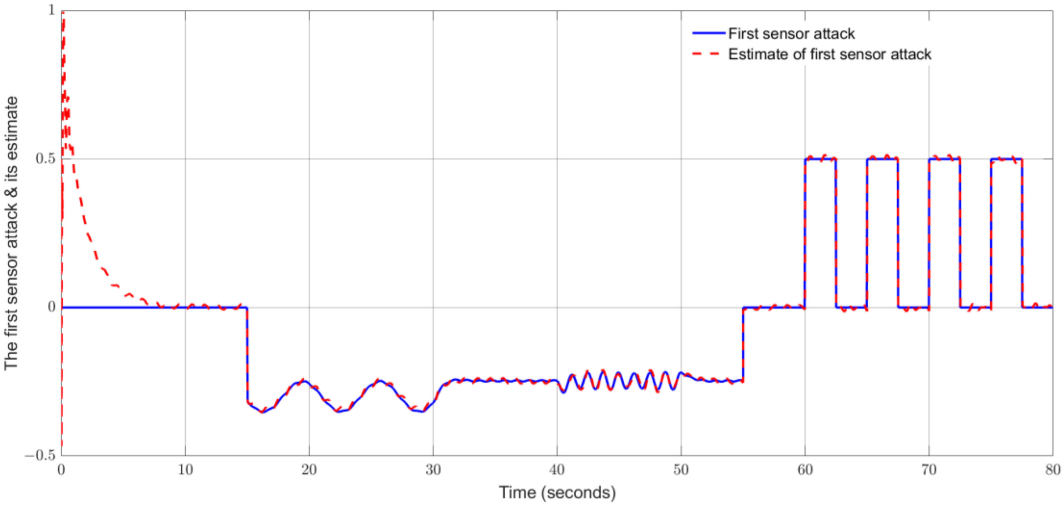

Figure 8. The first sensor attack signal and its estimate: augmented sliding-mode technique.

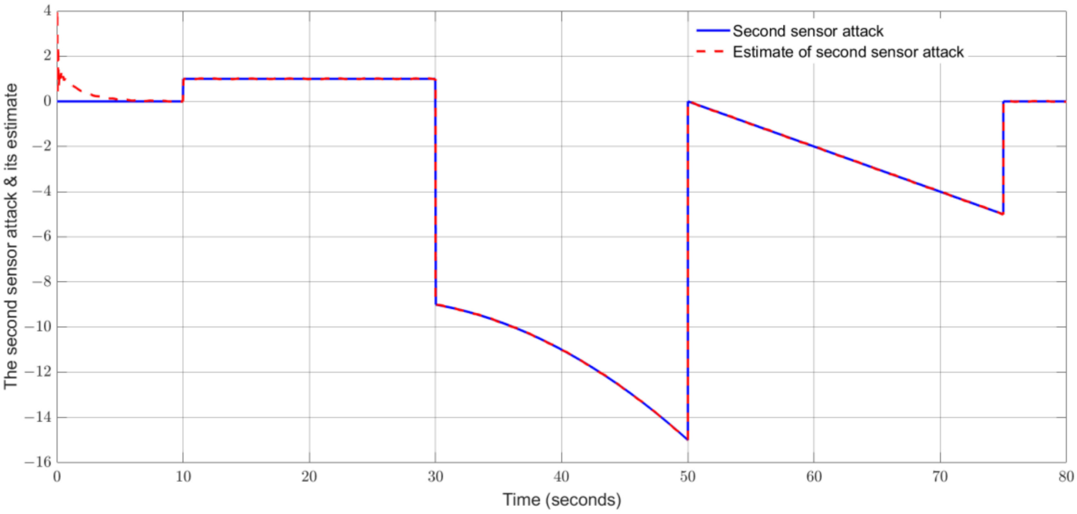

Figure 9. The second sensor attack signal and its estimate: augmented sliding-mode technique.

(ii). Adaptive augmented observer

To assess the performance of the estimator, we use the same attack signals as used in (i) above (e.g., see Equations (70)–(72)).

To solve LMIs (48) and (49), the following gains can be obtained:

$$L_F = \begin{bmatrix} -3.8377 & 16.2173 & 28.3712 & -9.9091 \\ 10.2563 & -3.3335 & -5.4297 & 1.0501 \\ 4.7222 & -2.2512 & -5.8988 & -0.0564 \\ -0.3313 & -13.8613 & -22.5174 & 9.4375 \\ 3.3490 & -12.6870 & -22.4017 & 8.3864 \\ -16.3518 & 16.8364 & 29.4332 & -9.1642 \end{bmatrix}, \tag{75}$$

$$R = \begin{bmatrix} -0.0000 & -59.1527 & 101.5045 & -10.5879 \end{bmatrix}. \tag{76}$$

Therefore, utilizing the estimator in the form of (43) and the gains obtained above, we can obtain the curves for the states, attacks, and their respective estimates. Figures 10–13 show the states and their estimates, in which we can see that the estimated curves track the system states well, but the dynamic variations at initial time are relatively large. Figures 14–16 exhibit the attacks and their estimates where the sensor attack signals in Figures 15 and 16 are well tracked. It is noted that in Figure 14, the estimation curve can trace the actuator attack signal generally well, but there are significant dynamic response processes with noteworthy variations in the estimated actuator signal.

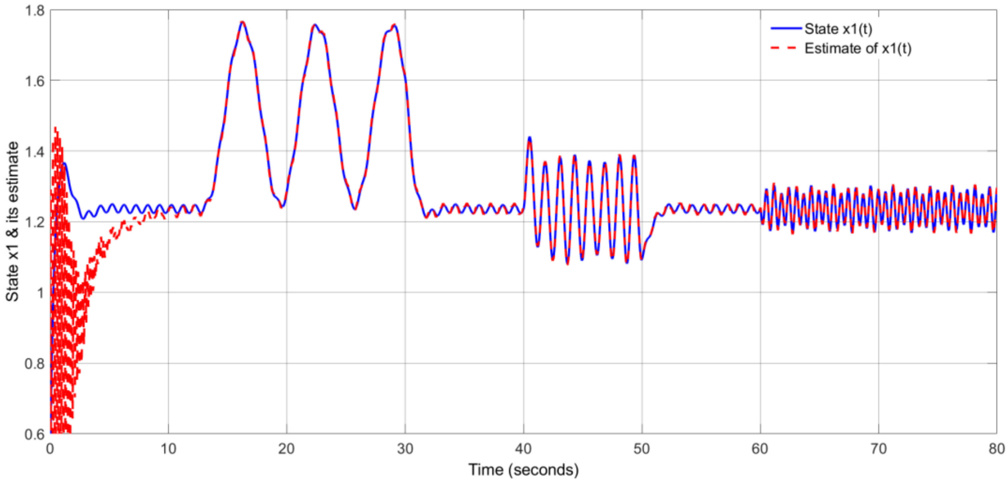

Figure 10. State $x_1(t)$ and its estimate: augmented adaptive technique.

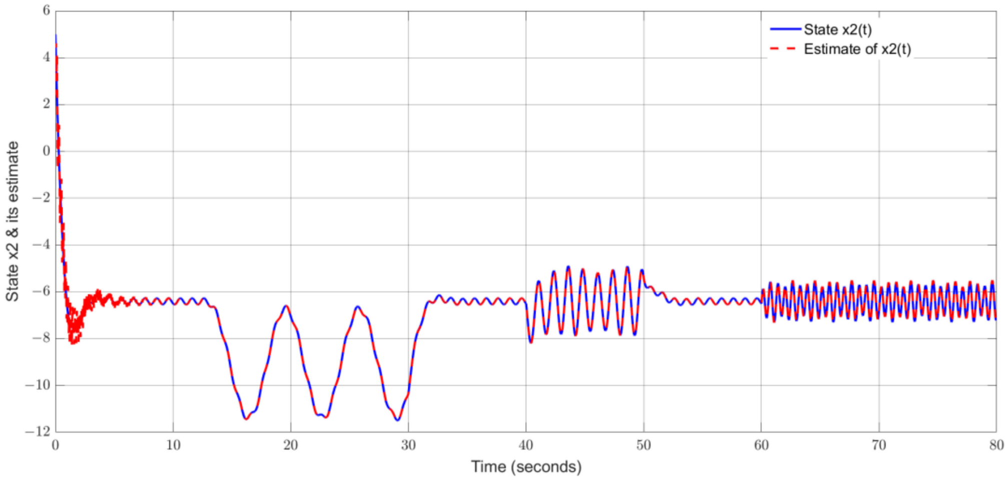

Figure 11. State $x_2(t)$ and its estimate: augmented adaptive technique.

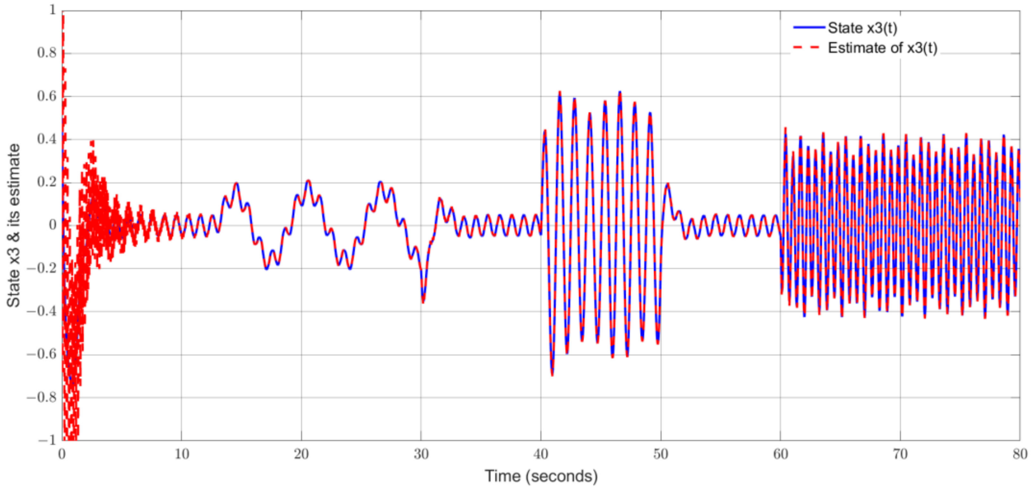

Figure 12. State $x_3(t)$ and its estimate: augmented adaptive technique.

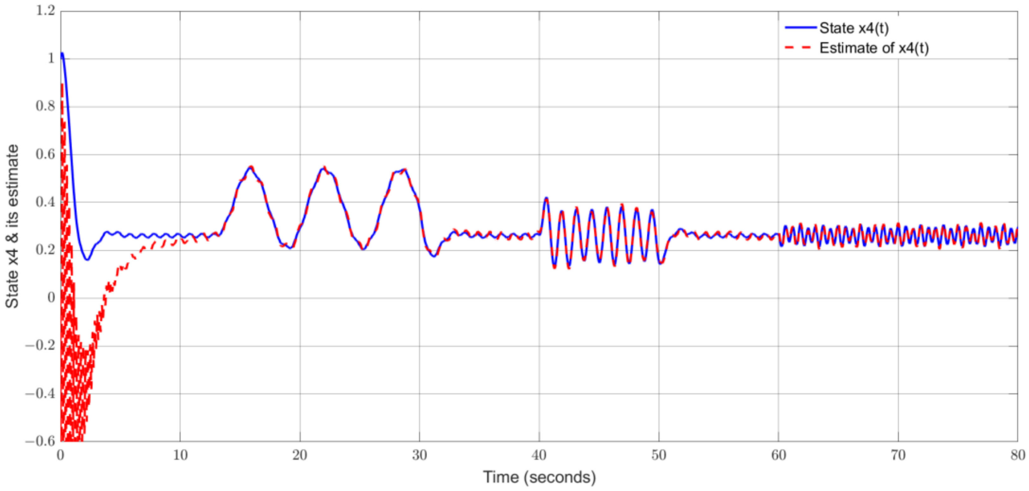

Figure 13. State $x_4(t)$ and its estimate: augmented adaptive technique.

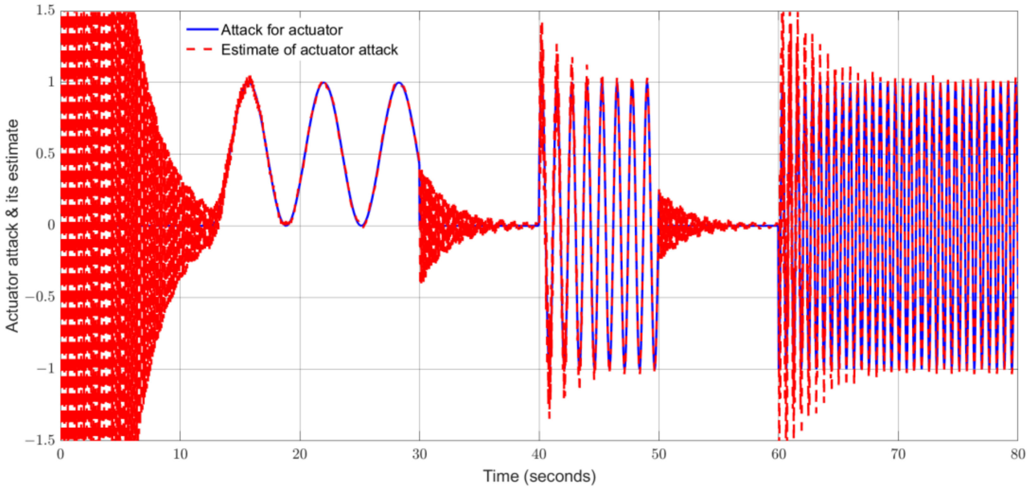

Figure 14. Actuator attack signal and its estimate: augmented adaptive technique.

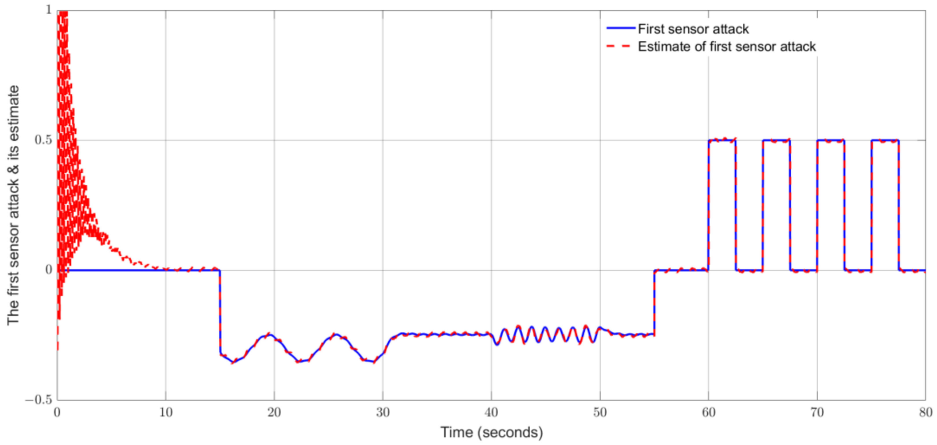

Figure 15. The first sensor attack signal and its estimate: augmented adaptive technique.

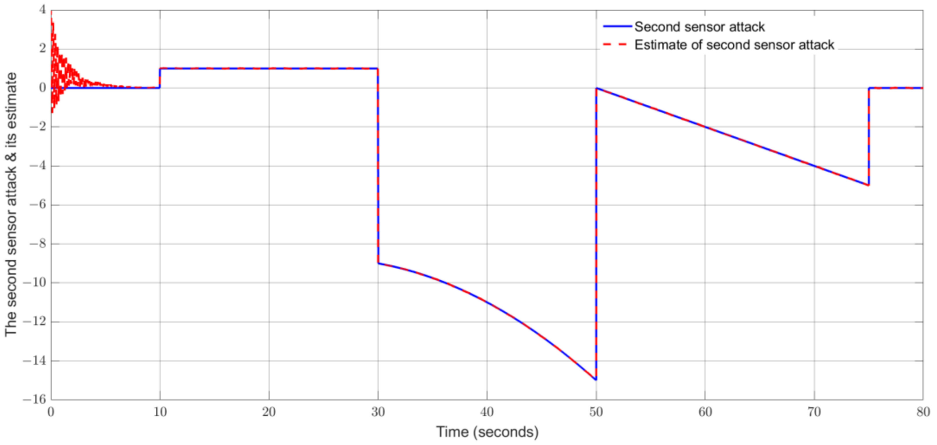

Figure 16. The second sensor attack signal and its estimate: augmented adaptive technique.

(iii). Comparison study

For comparison studies, the algorithm proposed in reference [36] is simulated here.

Let $\overline{x} = \begin{bmatrix} x \\ \dot{f}_a \\ \dot{f}_s \\ f_a \\ f_s \end{bmatrix}$, system (1) can be augmented to the following form:

$$\begin{cases} \dot{\overline{x}}(t) = \overline{A}\overline{x}(t) + \overline{B}u(t) + \overline{G\Phi}(x(t)) + \overline{B}_d d(t) \\ y(t) = \overline{C}\overline{x}(t) \end{cases} \tag{77}$$

where

$$\overline{A} = \begin{bmatrix} A & 0_{4\times1} & 0_{4\times2} & B_a & 0_{4\times2} \\ 0_{1\times4} & 0 & 0_{1\times2} & 0 & 0_{1\times2} \\ 0_{2\times4} & 0_{2\times1} & 0_{2\times2} & 0_{2\times1} & 0_{2\times2} \\ 0_{1\times4} & 1 & 0_{1\times2} & 0 & 0_{1\times2} \\ 0_{2\times4} & 0_{2\times1} & I_2 & 0_{2\times1} & 0_{2\times2} \end{bmatrix}, \overline{B} = \begin{bmatrix} B \\ 0_{1\times2} \\ 0_{2\times2} \\ 0_{1\times2} \\ 0_{2\times2} \end{bmatrix}, \ \overline{B}_d = \begin{bmatrix} B_d \\ 0_{1\times2} \\ 0_{2\times2} \\ 0_{1\times2} \\ 0_{2\times2} \end{bmatrix},$$

$$\overline{C} = \begin{bmatrix} C & 0_{4\times1} & 0_{4\times2} & 0_{4\times1} & D_s \end{bmatrix}, \ \overline{\Phi}(x(t)) = \begin{bmatrix} \Phi_s(x(t)) \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \ \Phi_s(x(t)) = \begin{bmatrix} 0 \\ -0.1sin(x_4) \\ 0 \\ 0 \end{bmatrix}.$$

The nonlinear augmented unknown input observer is given in the form of

$$\begin{cases} \dot{\bar{z}}(t) = \overline{R}\bar{z}(t) + \overline{TB}u(t) + \overline{T\Phi}(\hat{x}(t)) + \overline{K}y(t) \\ \hat{\hat{x}}(t) = \bar{z}(t) + \overline{H}\,y(t) \end{cases} \tag{78}$$

Using Theorem 3 from the literature [36], one can obtain the gains of the UIO-augmented observer. The simulated curves of the attacks and their estimates are depicted in Figures 17–19. One can see that the augmented UIO approach can track step signals, slope signals, and parabola signals excellently. The UIO approach can also track the effectiveness of the loss signal and square wave signal generally well, but there are some spikes caused by abrupt changes from other attack signals. The UIO method can track the low-frequency sinusoidal signals well, but the tracking performance reduces as the frequency of the signal increases.

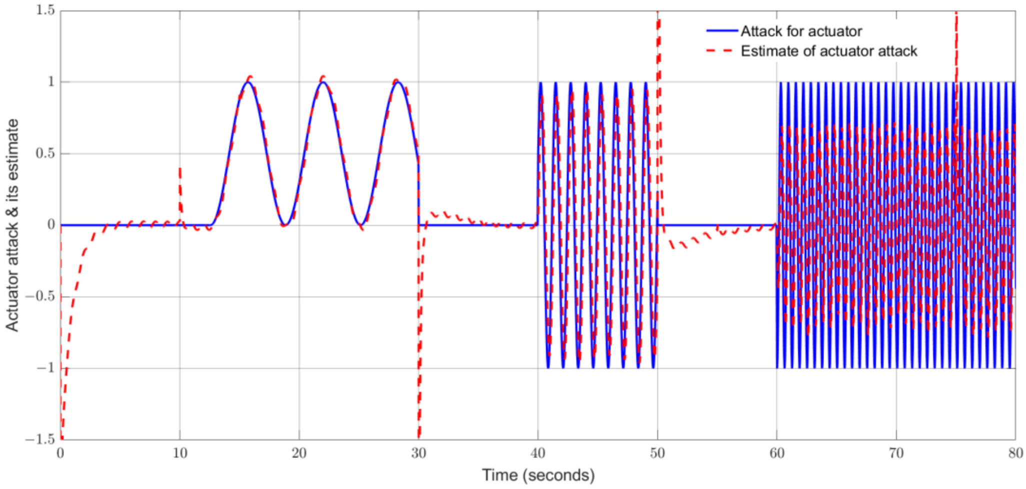

Figure 17. Actuator attack signal and its estimate: augmented UIO.

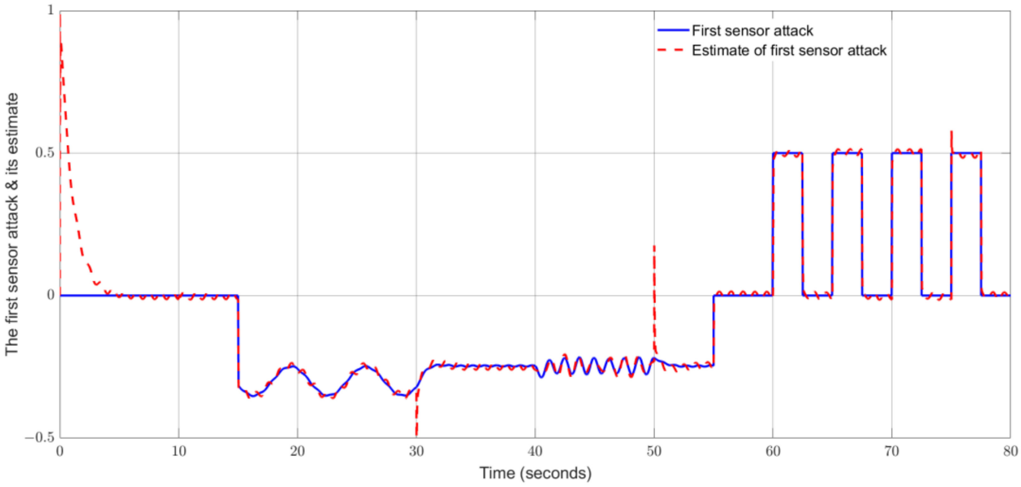

Figure 18. The first sensor attack signal and its estimate: augmented UIO.

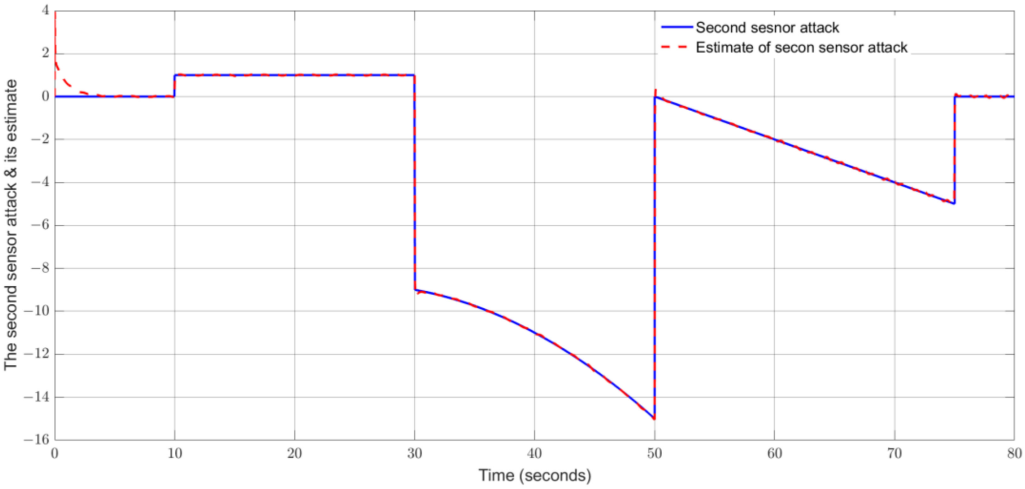

Figure 19. The second sensor attack signal and its estimate: augmented UIO.

By comparing Figures 7–9 in (i), Figures 14–16 in (ii), and Figures 17–19 in (iii), one can summarize the comments in Table 1.

Table 1. Comparison among three attack estimation methods.

Attack Signal	Proposed Sliding-Mode Technique	Proposed Adaptive Technique	Existing Augmented UIO Technique [36]
First sensor attack signal (a combination of measurement effectives loss and square waveform signals)	Tracks well	Tracks well	Tracks well
Second sensor attack signal (a combination of step, slope, and parabola signals)	Tracks well	Tracks well	Tracks well with quick response speed
Actuator signal (a combination of low-frequency and high-frequency periodic signals)	Tracks low-frequency and high-frequency signals excellently, and the tracking performance is best among the three methods	Tracks low-frequency signal well and traces high-frequency signal acceptably but with significant dynamic response time. There are evident variations at starting points when following the signal and its subsequent waveform change	Tracks low-frequency signal well, but the estimation performance reduces as the frequency increases. There are some spikes at the time instants when other signals change abruptly

6. Conclusions

In this paper, two simultaneous estimation techniques for state and false data injection attacks on the Lipschitz nonlinear systems affected by actuator attacks, sensor attacks, and unknown input disturbances have been proposed based on descriptor system theory, sliding-mode estimation, and adaptive estimation techniques. The robust stability conditions of the system have been analyzed based on the Lyapunov stability and linear matrix inequality methods. The proposed algorithms have been validated using simulation and comparison studies. The proposed algorithms have provided new insights into the reconstruction of multiple attacks, improving the safety and reliability of industrial systems.

Author Contributions: Conceptualization, Z.-W.G.; writing—original draft preparation, H.W. and Z.-W.G.; writing—revision, Z.-W.G.; supervision, Z.-W.G.; project administration, Z.-W.G. and Y.L.; Software, H.W. and Y.L.; validation, H.W. and Z.-W.G.; formal analysis, H.W. and Z.-W.G. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the Starting Research Fund for Talents (13051202202) of Northeast Petroleum University, the Featured Research Team Fund from the Fundamental Research Grant of Heilongjiang Province (2023TSTD-03) and the Innovative Talent Scheme of NNSFC (10230026).

Data Availability Statement: No new data were created in this study. Data sharing is not applicable to this article.

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

References

1. Singh, S.; Yadav, N.; Chuarasia, P.K. A review on cyber physical system attacks: Issues and challenges. In Proceedings of the 2020 International Conference on Communication and Signal Processing (ICCSP), Chennai, India, 28–30 July 2020; pp. 1133–1138.
2. Mahmoud, M.S.; Hamdan, M.M.; Baroudi, U.A.N. Modeling and control of cyber-physical systems subject to cyber attacks: A survey of recent advances and challenges. *Neurocomputing* **2019**, *338*, 101–115. [CrossRef]
3. Sánchez, H.S.; Rotondo, D.; Escobet, T.; Puig, V.; Quevedo, J. Bibliographical review on cyber attacks from a control oriented perspective. *Annu. Rev. Control* **2019**, *48*, 103–128. [CrossRef]
4. Pasqualetti, F.; Dörfler, F.; Bullo, F. Attack detection and identification in cyber-physical systems. *IEEE Trans. Autom. Control* **2013**, *58*, 2715–2729. [CrossRef]
5. Baroumand, S.; Zaman, A.; Mihaylova, L. Attack detection and fault-tolerant control of interconnected cyber-physical systems against simultaneous replayed time-delay and false-data injection attacks. *IET Control Theory Appl.* **2023**, *17*, 527–541. [CrossRef]
6. Sadeghikhorami, L.; Varadharajan, V.; Safavi, A.A. A novel secure observer-based controller and attack detection scheme for Networked Control Systems. *Inf. Sci.* **2021**, *575*, 185–205. [CrossRef]
7. Dong, K.; Yang, G.-H.; Wang, H. Estimator-based event-triggered output synchronization for heterogeneous multi-agent systems under denial-of-service attacks and actuator faults. *Inf. Sci.* **2024**, *657*, 119955. [CrossRef]
8. Zhang, D.; Wang, Q.-G.; Feng, G.; Shi, Y.; Vasilakos, A. A survey on attack detection, estimation and control of industrial cyber–physical systems. *ISA Trans.* **2021**, *116*, 1–16. [CrossRef]
9. Guo, Z.; Shi, D.; Quevedo, D.E.; Shi, L. Secure state estimation against integrity attacks: A Gaussian mixture model approach. *IEEE Trans. Signal Process.* **2018**, *67*, 194–207. [CrossRef]
10. Gao, Y.; Sun, G.; Liu, J.; Shi, Y.; Wu, L. State estimation and self-triggered control of CPSs against joint sensor and actuator attacks. *Automatica* **2020**, *113*, 108687. [CrossRef]
11. Lv, M.; Lv, Y.; Yu, W.; Meng, H. Finite-Time Attack Detection and Secure State Estimation for Cyber-Physical Systems. *IEEE/CAA J. Autom. Sin.* **2023**, *10*, 2032–2034. [CrossRef]
12. Lv, Y.; Lu, J.; Liu, Y.; Zhang, L. A class of stealthy attacks on remote state estimation with intermittent observation. *Inf. Sci.* **2023**, *639*, 118964. [CrossRef]
13. Kazemi, Z.; Safavi, A.A.; Arefi, M.M.; Naseri, F. Finite-time secure dynamic state estimation for cyber–physical systems under unknown inputs and sensor attacks. *IEEE Trans. Syst. Man Cybern. Syst.* **2021**, *52*, 4950–4959. [CrossRef]
14. Liu, G.; Zhao, H.; Fan, F.; Liu, G.; Xu, Q.; Nazir, S. An enhanced intrusion detection model based on improved kNN in WSNs. *Sensors* **2022**, *22*, 1407. [CrossRef] [PubMed]
15. Xiao, Y.; Xing, C.; Zhang, T.; Zhao, Z. An intrusion detection model based on feature reduction and convolutional neural networks. *IEEE Access* **2019**, *7*, 42210–42219. [CrossRef]
16. Almalaq, A.; Albadran, S.; Mohamed, M.A. Deep machine learning model-based cyber-attacks detection in smart power systems. *Mathematics* **2022**, *10*, 2574. [CrossRef]
17. Wang, Z.; Li, Z.; Wang, J.; Li, D. Network intrusion detection model based on improved BYOL self-supervised learning. *Secur. Commun. Netw.* **2021**, 9486949. [CrossRef]
18. Liu, Y.; Yang, G.-H. Event-triggered distributed state estimation for cyber-physical systems under DoS attacks. *IEEE Trans. Cybern.* **2020**, *52*, 3620–3631. [CrossRef]
19. Zhang, J.; Sun, J. Optimal cooperative multiple-attackers scheduling against remote state estimation of cyber-physical systems. *Syst. Control Lett.* **2020**, *144*, 104771. [CrossRef]
20. Liu, Z.; Chen, X.; Yu, J. Adaptive sliding mode security control for stochastic Markov jump cyber-physical nonlinear systems subject to actuator failures and randomly occurring injection attacks. *IEEE Trans. Ind. Inform.* **2022**, *19*, 3155–3165. [CrossRef]
21. Yang, H.; Yin, S.; Han, H.; Sun, H. Sparse actuator and sensor attacks reconstruction for linear cyber-physical systems with sliding mode observer. *IEEE Trans. Ind. Inform.* **2021**, *18*, 3873–3884. [CrossRef]
22. Yan, J.-J.; Yang, G.-H. Adaptive fault estimation for cyber-physical systems with intermittent DoS attacks. *Inf. Sci.* **2021**, *547*, 746–762. [CrossRef]
23. An, L.; Yang, G.-H. Secure state estimation against sparse sensor attacks with adaptive switching mechanism. *IEEE Trans. Autom. Control* **2017**, *63*, 2596–2603. [CrossRef]
24. Dong, L.; Xu, H.; Zhang, L.; Li, Z.; Chen, Y. Adjustable proportional-integral multivariable observer-based FDI attack dynamic reconstitution and secure control for cyber-physical systems. *Appl. Math. Comput.* **2023**, *443*, 127762. [CrossRef]
25. Wang, X.; Ding, D.; Dong, H.; Yi, X. PI-based security control against joint sensor and controller attacks and applications in load frequency control. *IEEE Trans. Syst. Man Cybern. Syst.* **2022**, *53*, 970–980. [CrossRef]

26. Huo, J.-R.; Li, X.-J. False data injection attacks on sensors against state estimation in cyber-physical systems. *J. Frankl. Inst.* **2023**, *360*, 6110–6130. [CrossRef]
27. He, K.; Li, T.; Long, Y.; Park, J.H.; Chen, C.P. Secure state estimation and actuator attack reconstruction for cyber-physical systems based on sliding-mode observer. *Int. J. Robust Nonlinear Control* **2023**, *33*, 8508–8523. [CrossRef]
28. Zhao, Z.; Xu, Y. Performance based attack detection and security analysis for cyber-physical systems. *Int. J. Robust Nonlinear Control* **2023**, *33*, 3267–3284. [CrossRef]
29. Keijzer, T.; Ferrari, R.M.; Sandberg, H. Secure State Estimation under Actuator and Sensor Attacks using Sliding Mode Observers. *IEEE Control Syst. Lett.* **2023**, *7*, 2071–2076. [CrossRef]
30. Gao, Z. Estimation and compensation for Lipschitz nonlinear discrete-time systems subjected to unknown measurement delays. *IEEE Trans. Ind. Electron.* **2015**, *62*, 5950–5961. [CrossRef]
31. Gao, Z. Fault estimation and fault-tolerant control for discrete-time dynamic systems. *IEEE Trans. Ind. Electron.* **2015**, *62*, 3874–3884. [CrossRef]
32. Gao, Z.; Ding, S.X. Actuator fault robust estimation and fault-tolerant control for a class of nonlinear descriptor systems. *Automatica* **2007**, *43*, 912–920. [CrossRef]
33. Gao, Z.; Wang, H. Descriptor observer approaches for multivariable systems with measurement noises and application in fault detection and diagnosis. *Syst. Control Lett.* **2006**, *55*, 304–313. [CrossRef]
34. Boyd, S.; El Ghaoui, L.; Feron, E.; Balakrishnan, V. *Linear Matrix Inequalities in System and Control Theory*; Society for Industrial and Applied Mathematics (SIAM): Philadelphia, PA, USA, 1994.
35. Han, J.; Liu, X.; Wei, X.; Zhang, H.; Hu, X. Adjustable dimension descriptor observer based fault estimation of nonlinear system with unknown input. *Appl. Math. Comput.* **2021**, *396*, 125899. [CrossRef]
36. Gao, Z.; Liu, X.; Chen, M.Z.Q. Unknown input observer-based robust fault estimation for systems corrupted by partially decoupled disturbances. *IEEE Trans. Ind. Electron.* **2015**, *63*, 2537–2547. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.