

Article

Adaptive Resilient Control of AC Microgrids under Unbounded Actuator Attacks

Shan Zuo *, Yi Zhang  and Yichao Wang

Department of Electrical and Computer Engineering, University of Connecticut, Storrs, CT 06269, USA

* Correspondence: shan.zuo@uconn.edu

Abstract: Existing secondary control methods using fault-tolerant and/or H_∞ control techniques for multi-inverter microgrids generally assume bounded faults and/or disturbances. Herein, we study unknown unbounded attacks on the input channels of both frequency and voltage control loops of inverters that could deteriorate the cooperative performance and affect the microgrid stability. We propose a fully distributed attack-resilient control framework using adaptive control techniques that, using stability analysis with Lyapunov techniques, are shown to preserve the uniformly ultimately bounded consensus for frequency regulation and voltage containment. Moreover, the ultimate bound can be set by adjusting the tuning parameters. The proposed result is validated for a modified IEEE 34-bus test feeder benchmark system augmented with four inverters.

Keywords: containment; inverters; microgrids; resilience; unbounded attacks

1. Introduction

Distributed cooperative control of AC microgrids relies on consensus and containment approaches to accomplish frequency regulation [1] and voltage containment [2], respectively. The distributed communication network among inverters poses security concerns as individual inverters lack the global perspective with limited information exchanged among neighboring inverters [3–6]. Some existing methods detect, identify, and then isolate or recover the compromised inverters [7–9] but would require a number of inverters to be healthy. Moreover, stealthy attacks launched by intelligent attackers are generally undetectable. Specifically, attackers could exploit the intrinsic characteristics or internal dynamics of the system modeling and/or configuration to launch deliberately designed attacks without being detected by existing attack-detection algorithms [10]. The vulnerability assessment and consequences of power system state estimation with respect to such unobservable or undetectable false data injection (FDI) attacks were presented in [10–13]. Protection and prevention against stealthy and intelligent attackers are not always possible using the attack-detection methods, and a paradigm shift to enhance the self-resilience of the large-scale networked microgrids by developing attack-resilient control protocols is the overarching objective for safeguarding the nation’s critical infrastructures.

Distributed resilient control protocols were investigated recently in [14–21] to provide self-resilience against external attacks without detecting and identifying the compromised agents. The above-mentioned resilient control protocols for microgrids mainly deal with disturbances, noises, and/or faults that are unintentionally caused and are assumed to be bounded. However, in practice, malicious attackers could launch unknown and unbounded FDI attacks to maximize their damage, distorting cooperative performance and even leading to system instability [22]. To address unbounded FDI attacks for AC microgrids, an attack-resilient control framework, using observer-based techniques, was studied in [2] to maintain the bounded frequency regulation and voltage containment at the cost of additional communication channels among observers. Alternatively, this paper explores adaptive techniques to address unknown unbounded attacks on input signals of the control



Citation: Zuo, S.; Zhang, Y.; Wang, Y. Adaptive Resilient Control of AC Microgrids under Unbounded Actuator Attacks. *Energies* **2022**, *15*, 7458. <https://doi.org/10.3390/en15207458>

Academic Editor: Nicu Bizon

Received: 9 September 2022

Accepted: 4 October 2022

Published: 11 October 2022

Publisher’s Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2022 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

loops, which are referred to as the actuator attacks. This paper considers the unbounded actuator attacks on both frequency and voltage control loops of an inverter, as illustrated in Figure 1, which could severely destabilize the synchronization mechanism among microgrid inverters. The contributions of this paper are two-fold:

- A resilient control method is proposed for both secondary frequency and voltage control loops in the face of unknown unbounded actuator attacks. Compared to the observer-based techniques in [2], this control method does not need additional cyber layers for information exchange among observers, offering reduced computational complexity and system vulnerability to cyber attacks.
- A stability analysis using Lyapunov techniques shows that the proposed method is resilient to unbounded actuator attacks by preserving the uniformly ultimately bounded (UUB) consensus for frequency regulation and voltage containment. Moreover, the ultimate bound can be set by adjusting the tuning parameters. That is, the frequency and voltage terms can be tuned to converge to an arbitrarily small neighborhood around their respective reference values.

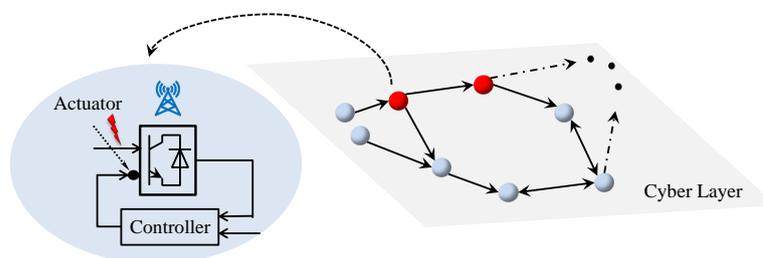


Figure 1. A networked multi-inverter system under actuator attacks.

The rest of this paper is organized as follows: Preliminaries on graph theory and notations are given in Section 2. Section 3 reviews the conventional cooperative secondary control of AC microgrids. Section 4 formulates the attack-resilient frequency and voltage control problems. The distributed resilient controller design is discussed in Section 5. The efficacy of the proposed control method is verified for an AC microgrid in Section 6. Section 7 concludes the paper.

2. Preliminaries on Graph Theory and Notations

There are N inverters, with two leader nodes, mapped on a communication network, which is represented by a time-invariant weighted digraph \mathcal{G} . The interactions among the inverters are represented by a subgraph \mathcal{G}_f with the associated adjacency matrix $\mathcal{A} = [a_{ij}] \in \mathbb{R}^{N \times N}$. Define $\mathcal{D} = \text{diag}(d_i) \in \mathbb{R}^{N \times N}$ and $\mathcal{L} = \mathcal{D} - \mathcal{A}$ as the in-degree matrix and the corresponding Laplacian matrix, respectively, where $d_i = \sum_{j=1}^N a_{ij}$. There are two leader nodes to issue the upper and lower reference values. g_{ik} is the pinning gain from the (upper/lower) k^{th} leader to the i^{th} inverter, brought together in the diagonal matrix $\mathcal{G}_k = \text{diag}(g_{ik})$.

$\sigma_{\min}(\cdot)$ and $\sigma_{\max}(\cdot)$ are the minimum and maximum singular values of a given matrix, respectively. \mathcal{F} and \mathcal{L} denote the sets of $\{1, 2, \dots, N\}$ and $\{N + 1, N + 2\}$, respectively. $\mathbf{1}_N \in \mathbb{R}^N$ is a column vector where all entries are one. \otimes , $\text{diag}\{\cdot\}$, $\|\cdot\|$, and $|\cdot|$ denote the Kronecker product, a block diagonal matrix, the Euclidean norm of a given vector, and the absolute value of a given scalar, respectively.

3. Conventional Cooperative Secondary Control of AC Microgrids

Conventional secondary control acts as an actuator by providing the input control signals for tuning the setpoints of decentralized primary controls. These primary droop mechanisms are given by the following for the i th inverter

$$\omega_i = \omega_{n_i} - m_{P_i} P_i, \quad (1)$$

$$v_{odi} = V_{n_i} - n_{Q_i} Q_i, \quad (2)$$

where P_i and Q_i are the active and reactive powers, respectively. ω_i and v_{odi} are the operating angular frequency and terminal voltage, respectively. ω_{n_i} and V_{n_i} are the setpoints for the primary droop mechanisms fed from the secondary control layer. m_{P_i} and n_{Q_i} are $P - \omega$ and $Q - v$ droop coefficients selected for each inverter's power ratings.

We differentiate the droop relations in (1) and (2), with respect to time, to obtain

$$\dot{\omega}_{n_i} = \dot{\omega}_i + m_{P_i} \dot{P}_i = u_{f_i}, \quad (3)$$

$$\dot{V}_{n_i} = \dot{v}_{odi} + n_{Q_i} \dot{Q}_i = u_{v_i}, \quad (4)$$

where u_{f_i} and u_{v_i} are auxiliary control inputs. To synchronize the terminal frequency and voltage of each inverter to their respective references, the leader-follower containment-based secondary control is adopted [23]. The local cooperative frequency and voltage control protocols using the relative information with respect to the neighboring inverters and the leaders are given by

$$u_{f_i} = c_{f_i} \left(\sum_{j \in \mathcal{F}} a_{ij} (\omega_j - \omega_i) + \sum_{k \in \mathcal{L}} g_{ik} (\omega_k - \omega_i) + \sum_{j \in \mathcal{F}} a_{ij} (m_{P_j} P_j - m_{P_i} P_i) \right), \quad (5)$$

$$u_{v_i} = c_{v_i} \left(\sum_{j \in \mathcal{F}} a_{ij} (v_{odj} - v_{odi}) + \sum_{k \in \mathcal{L}} g_{ik} (v_k - v_{odi}) + \sum_{j \in \mathcal{F}} a_{ij} (n_{Q_j} Q_j - n_{Q_i} Q_i) \right), \quad (6)$$

where c_{f_i}, c_{v_i} are positive constant coupling gains. ω_k and v_k are the frequency and voltage reference values of the k^{th} leader, respectively. The frequency reference for both leaders is set as ω_{ref} . The upper and lower leaders have their voltage reference values set as v_{ref}^u and v_{ref}^l , respectively. The setpoints for the primary-level droop control, ω_{n_i} and V_{n_i} , are then computed from u_{f_i} and u_{v_i} as

$$\omega_{n_i} = \int u_{f_i} dt, \quad (7)$$

$$V_{n_i} = \int u_{v_i} dt. \quad (8)$$

Using (5) and (6) to rewrite (3) and (4) yields

$$\dot{\omega}_{n_i} = c_{f_i} \left(\sum_{j \in \mathcal{F}} a_{ij} (\omega_{n_j} - \omega_{n_i}) + \sum_{k \in \mathcal{L}} g_{ik} (\omega_{n_k} - \omega_{n_i}) \right), \quad (9)$$

$$\dot{V}_{n_i} = c_{v_i} \left(\sum_{j \in \mathcal{F}} a_{ij} (V_{n_j} - V_{n_i}) + \sum_{k \in \mathcal{L}} g_{ik} (V_{n_k} - V_{n_i}) \right), \quad (10)$$

where $\omega_{n_k} = \omega_k + m_{P_i} P_i$ and $V_{n_k} = v_k + n_{Q_i} Q_i$. Define $\Phi_k = \frac{1}{2} \mathcal{L} + \mathcal{G}_k$. Then, the global forms of (9) and (10) are

$$\dot{\omega}_n = -\text{diag}(c_{f_i}) \sum_{k \in \mathcal{L}} \Phi_k (\omega_n - \mathbf{1}_N \otimes \omega_{n_k}), \quad (11)$$

$$\dot{V}_n = -\text{diag}(c_{v_i}) \sum_{k \in \mathcal{L}} \Phi_k (V_n - \mathbf{1}_N \otimes V_{n_k}), \tag{12}$$

where $\omega_n = [\omega_{n_1}^T, \dots, \omega_{n_N}^T]^T$ and $V_n = [V_{n_1}^T, \dots, V_{n_N}^T]^T$. Define the global frequency and voltage containment error vectors as

$$e_f = \omega_n - \left(\sum_{r \in \mathcal{L}} \Phi_r \right)^{-1} \sum_{k \in \mathcal{L}} \Phi_k (\mathbf{1}_N \otimes \omega_{n_k}), \tag{13}$$

$$e_v = V_n - \left(\sum_{r \in \mathcal{L}} \Phi_r \right)^{-1} \sum_{k \in \mathcal{L}} \Phi_k (\mathbf{1}_N \otimes V_{n_k}). \tag{14}$$

Definition 1 (Secondary Frequency Containment Control Objective). *The secondary frequency control objective is to make the local frequency of each inverter converge to the range of the two frequency references issued by the upper and lower leaders. Since these two reference values are identical, the frequency regulation is achieved.*

Definition 2 (Secondary Voltage Containment Control Objective). *The secondary voltage containment control objective is to make each inverter voltage converge to the range spanned by the two references of the upper and lower leaders.*

The following assumption is needed for the communication graph topology to guarantee the cooperative consensus.

Assumption 1. *The communication graph \mathcal{G} includes a directed path from, at least, one leader to each inverter.*

Lemma 1 ([24]). *Suppose that Assumption 1 holds; $\sum_{k \in \mathcal{L}} \Phi_k$ is non-singular and positive-definite. Moreover, the frequency and voltage containment control objectives are achieved if $\lim_{t \rightarrow \infty} e_f(t) = 0$ and $\lim_{t \rightarrow \infty} e_v(t) = 0$, respectively.*

4. Problem Formulation

This section formulates the resilient secondary frequency and voltage control problems for a networked AC microgrid. In particular, we consider the general unknown unbounded attack injections to the local input channels of both frequency and voltage control loops, which modifies (9) and (10) to

$$\dot{\omega}_{n_i} = c_{f_i} \left(\sum_{j \in \mathcal{F}} a_{ij} (\omega_{n_j} - \omega_{n_i}) + \sum_{k \in \mathcal{L}} g_{ik} (\omega_{n_k} - \omega_{n_i}) \right) + \varpi_{f_i}, \tag{15}$$

$$\dot{V}_{n_i} = c_{v_i} \left(\sum_{j \in \mathcal{F}} a_{ij} (V_{n_j} - V_{n_i}) + \sum_{k \in \mathcal{L}} g_{ik} (V_{n_k} - V_{n_i}) \right) + \varpi_{v_i}, \tag{16}$$

where ϖ_{f_i} and ϖ_{v_i} denote the unbounded attack signals injected to the input channels of frequency and voltage control loops at the i^{th} inverter, respectively.

Assumption 2. $\dot{\varpi}_{f_i}$ and $\dot{\varpi}_{v_i}$ are bounded.

Remark 1. *Assumption 2 is reasonable since attack signals, with an excessively large change in values, could be easily detected in practice. In the event that the attacker does launch an attack signal with an infinite magnitude of the rate of change, the microgrids can incorporate a defensive mechanism to detect and reject such an injection. Since the intentionally injected attacks could be unbounded, the bounded noises and/or disturbances that are unintentionally caused can also be addressed using the attack-resilient controller to be designed.*

Since ω_{f_i} and ω_{v_i} are unbounded, conventional cooperative control protocols fail to regulate the frequency and voltage terms. One then needs attack-resilient control methods to preserve the frequency regulation and voltage containment performances and to ensure closed-loop stability. The following convergence definition is needed.

Definition 3 ([25]). *Signal $x(t)$ is UUB with an ultimate bound b if there exist positive constants b and c , independent of $t_0 \geq 0$ and, for every $a \in (0, c)$, there exist $t_1 = t_1(a, b) \geq 0$, independent of t_0 , such that $\|x(t_0)\| \leq a \Rightarrow \|x(t)\| \leq b, \forall t \geq t_0 + t_1$.*

Now, the following distributed resilient secondary frequency and voltage control problems are defined.

Definition 4 (Attack-Resilient Frequency Control Problem). *The goal is to design an input control signal u_{f_i} in (3) for each inverter such that e_f in (13) is UUB under unbounded attacks to the local frequency control loop. That is, the inverter frequency goes to a small neighborhood around the reference value.*

Definition 5 (Attack-Resilient Voltage Control Problem). *The goal is to design an input control signal u_{v_i} in (4) for each inverter such that e_v in (14) is UUB under unbounded attacks to the local voltage control loop. That is, each inverter voltage goes to a small neighborhood around the range spanned by the two upper and lower references.*

5. Distributed Resilient Controller Design

We propose a fully distributed control method to solve the attack-resilient frequency and voltage control problems. For convenience, denote

$$\zeta_{f_i} = \sum_{j \in \mathcal{F}} a_{ij} (\omega_{n_j} - \omega_{n_i}) + \sum_{k \in \mathcal{L}} g_{ik} (\omega_{n_k} - \omega_{n_i}), \tag{17}$$

$$\zeta_{v_i} = \sum_{j \in \mathcal{F}} a_{ij} (V_{n_j} - V_{n_i}) + \sum_{k \in \mathcal{L}} g_{ik} (V_{n_k} - V_{n_i}). \tag{18}$$

Then, we present the following attack-resilient control framework for both frequency and voltage control loops

$$\begin{cases} \dot{\omega}_{n_i} = (\rho_{f_i} + \dot{\rho}_{f_i}) \zeta_{f_i} + \omega_{f_i}, \\ \dot{\rho}_{f_i} = \chi_{f_i} |\zeta_{f_i}|, \end{cases} \tag{19}$$

$$\begin{cases} \dot{V}_{n_i} = (\rho_{v_i} + \dot{\rho}_{v_i}) \zeta_{v_i} + \omega_{v_i}, \\ \dot{\rho}_{v_i} = \chi_{v_i} |\zeta_{v_i}|, \end{cases} \tag{20}$$

where χ_{f_i} and χ_{v_i} are given positive constants, and ρ_{f_i} and ρ_{v_i} are time-varying coupling weights, with $\rho_{f_i}(0) \geq 0$ and $\rho_{v_i}(0) \geq 0$. Figure 2 shows the communication network among inverters and the proposed secondary control for an inverter.

Theorem 1. *Under Assumptions 1 and 2 and using the cooperative resilient frequency control protocols consisting of (17) and (19), e_f in (13) is UUB. Furthermore, by increasing χ_{f_i} in (19), the ultimate bound of e_f can be adjusted to be an arbitrarily small value, i.e., inverter frequency converges to an arbitrarily small neighborhood around the reference value.*

Proof. Consider the Lyapunov function candidate:

$$E = \frac{1}{2} \sum_{i=1}^N \int_0^{\zeta_{f_i}^2(t)} (\rho_{f_i}(s) + \dot{\rho}_{f_i}(s)) \, ds. \tag{21}$$

□

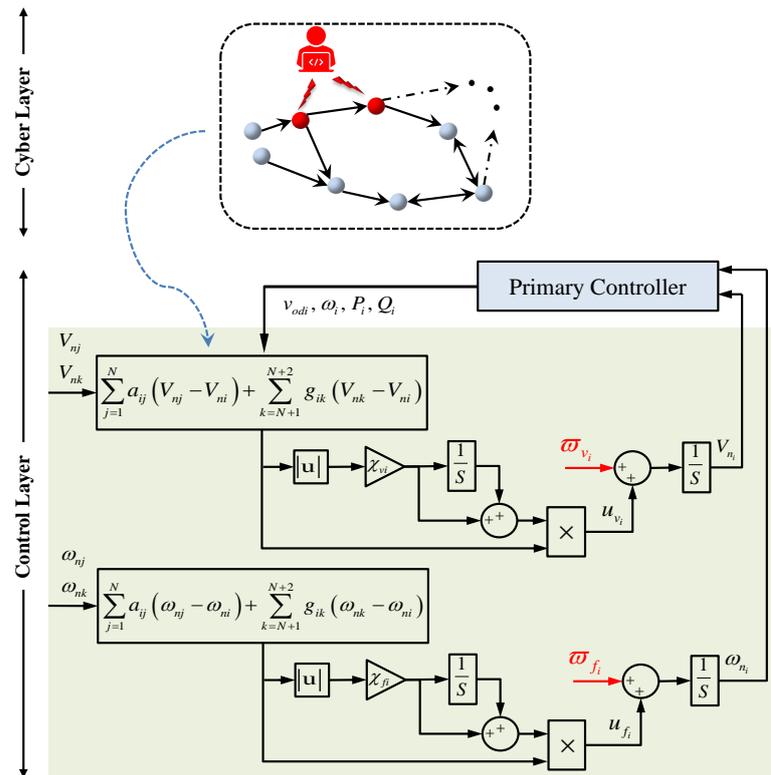


Figure 2. Communication layer among inverters and the proposed attack-resilient secondary control framework for an inverter.

Combine (19) and (21) to obtain

$$\begin{aligned}
 \dot{E} &= \frac{1}{2} \sum_{i=1}^N (\rho_{f_i} + \dot{\rho}_{f_i}) 2\zeta_{f_i} \dot{\zeta}_{f_i} \\
 &= \zeta_f^T \text{diag}(\rho_{f_i} + \dot{\rho}_{f_i}) \dot{\zeta}_f \\
 &= \zeta_f^T \text{diag}(\rho_{f_i} + \dot{\rho}_{f_i}) \left(- \sum_{k \in \mathcal{L}} \Phi_k \dot{\omega}_n \right) \\
 &= -\zeta_f^T \text{diag}(\rho_{f_i} + \dot{\rho}_{f_i}) \left(\sum_{k \in \mathcal{L}} \Phi_k \right) \times \left(\text{diag}(\rho_{f_i} + \dot{\rho}_{f_i}) \zeta_f + \omega_f \right),
 \end{aligned} \tag{22}$$

where $\zeta_f = [\zeta_{f_1}^T, \dots, \zeta_{f_N}^T]^T$.

Recalling Sylvester’s inequality and noting that $\sum_{k \in \mathcal{L}} \Phi_k$ is positive-definite, one can then obtain

$$\begin{aligned}
 \dot{E} &\leq -\sigma_{\min} \left(\sum_{k \in \mathcal{L}} \Phi_k \right) \left\| \text{diag}(\rho_{f_i} + \dot{\rho}_{f_i}) \zeta_f \right\|^2 + \sigma_{\max} \left(\sum_{k \in \mathcal{L}} \Phi_k \right) \left\| \text{diag}(\rho_{f_i} + \dot{\rho}_{f_i}) \zeta_f \right\| \left\| \omega_f \right\| \\
 &\leq -\sigma_{\min} \left(\sum_{k \in \mathcal{L}} \Phi_k \right) \left\| \text{diag}(\rho_{f_i} + \dot{\rho}_{f_i}) \zeta_f \right\| \times \left(\left\| \text{diag}(\rho_{f_i} + \dot{\rho}_{f_i}) \zeta_f \right\| - \frac{\sigma_{\max} \left(\sum_{k \in \mathcal{L}} \Phi_k \right)}{\sigma_{\min} \left(\sum_{k \in \mathcal{L}} \Phi_k \right)} \left\| \omega_f \right\| \right).
 \end{aligned} \tag{23}$$

Next, we prove that $\exists \tau > 0$, such that

$$\left\| \text{diag}(\rho_{f_i} + \dot{\rho}_{f_i}) \zeta_f \right\| \geq \frac{\sigma_{\max} \left(\sum_{k \in \mathcal{L}} \Phi_k \right)}{\sigma_{\min} \left(\sum_{k \in \mathcal{L}} \Phi_k \right)} \left\| \omega_f \right\|, \forall t \geq \tau. \tag{24}$$

A sufficient condition to guarantee (24) is

$$\left| (\rho_{f_i} + \dot{\rho}_{f_i}) \zeta_{f_i} \right| \geq \frac{\sigma_{\max} \left(\sum_{k \in \mathcal{L}} \Phi_k \right)}{\sigma_{\min} \left(\sum_{k \in \mathcal{L}} \Phi_k \right)} \left| \omega_{f_i} \right|, \quad \forall t \geq \tau. \tag{25}$$

Since both ρ_{f_i} and $\dot{\rho}_{f_i}$ are non-negative, we further obtain the following sufficient condition:

$$\rho_{f_i} \left| \zeta_{f_i} \right| \geq \frac{\sigma_{\max} \left(\sum_{k \in \mathcal{L}} \Phi_k \right)}{\sigma_{\min} \left(\sum_{k \in \mathcal{L}} \Phi_k \right)} \left| \omega_{f_i} \right|, \quad \forall t \geq \tau. \tag{26}$$

Note that (26) is guaranteed if both $\rho_{f_i} \geq \left| \omega_{f_i} \right|$ and $\left| \zeta_{f_i} \right| \geq \frac{\sigma_{\max}(\sum_{k \in \mathcal{L}} \Phi_k)}{\sigma_{\min}(\sum_{k \in \mathcal{L}} \Phi_k)}$ hold. Since

$$\frac{d \left| \omega_{f_i} \right|}{dt} = \frac{\omega_{f_i} \dot{\omega}_{f_i}}{\left| \omega_{f_i} \right|} \leq \left| \dot{\omega}_{f_i} \right|, \tag{27}$$

from Assumption 2, $\dot{\omega}_{f_i}$ is bounded. Hence, $\frac{d \left| \omega_{f_i} \right|}{dt}$ is also bounded. Using (19) and choosing

$$\left| \zeta_{f_i} \right| \geq \max \left\{ \frac{\sigma_{\max} \left(\sum_{k \in \mathcal{L}} \Phi_k \right)}{\sigma_{\min} \left(\sum_{k \in \mathcal{L}} \Phi_k \right)}, \frac{1}{\chi_{f_i}} \frac{d \left| \omega_{f_i} \right|}{dt} \right\}, \tag{28}$$

we then obtain that $\exists \tau > 0$, such that (26) holds. Furthermore, we obtain that (24) holds. Using (23), we now obtain that $\forall t \geq \tau$

$$\dot{E} \leq 0, \quad \forall \left| \zeta_{f_i} \right| \geq \max \left\{ \frac{\sigma_{\max} \left(\sum_{k \in \mathcal{L}} \Phi_k \right)}{\sigma_{\min} \left(\sum_{k \in \mathcal{L}} \Phi_k \right)}, \frac{1}{\chi_{f_i}} \frac{d \left| \omega_{f_i} \right|}{dt} \right\}. \tag{29}$$

Therefore, ζ_{f_i} is bounded. Note that

$$\zeta_f = \sum_{k \in \mathcal{L}} \Phi_k e_f. \tag{30}$$

Hence, e_f is also bounded. Moreover, using LaSalle’s invariance principle [26], it is seen from (29) that ζ_{f_i} is bounded by $\max \left\{ \frac{\sigma_{\max}(\sum_{k \in \mathcal{L}} \Phi_k)}{\sigma_{\min}(\sum_{k \in \mathcal{L}} \Phi_k)}, \frac{1}{\chi_{f_i}} \frac{d \left| \omega_{f_i} \right|}{dt} \right\}$, where $\frac{\sigma_{\max}(\sum_{k \in \mathcal{L}} \Phi_k)}{\sigma_{\min}(\sum_{k \in \mathcal{L}} \Phi_k)}$ is a positive constant. Hence, the ultimate bound can be reduced by properly increasing the adaptive tuning parameter ω_{f_i} in (19).

Theorem 2. Under Assumptions 1 and 2 and using the cooperative resilient voltage control protocols consisting of (18) and (20), e_v in (14) is UIUB. Furthermore, by increasing χ_{v_i} in (20), the

ultimate bound of e_v can be set arbitrarily small, i.e., the inverter voltage converges to an arbitrarily small neighborhood around the range covered by the two references.

Proof. The proof follows that of Theorem 1. \square

Remark 2. To mitigate the propagated adverse effects caused by the unbounded actuator attacks, ω_{f_i} and ω_{v_i} , the time-varying coupling weights, ρ_{f_i} and ρ_{v_i} , are designed based on adaptive tuning laws. As seen from the proof of Theorem 1, such adaptively updated coupling weights can successfully compensate for the externally injected attack signals.

Remark 3. Compared to [2], the proposed control protocols (17)–(20) have the following merits: (i) Local observers with additional communication information flow were constructed in [2] to estimate the actual state measurements. This, however, could introduce additional computational complexity. Moreover, the additional communication channels for exchanging observer states could potentially increase the system vulnerability to malicious cyber attacks. (ii) While both [2] and this paper preserve the UUB convergences for both frequency and voltage terms, in this paper, the ultimate bound can be reduced by properly increasing the adaptive tuning parameters.

6. Case Studies

The proposed resilient control method is studied in the context of an IEEE 34-bus feeder system, islanded at bus 800, and augmented with four inverters and two leaders, as shown in Figure 3. The specifications of inverters and its grid interconnections are adopted from [1,27], respectively. Inverters 1 and 2 have twice the power ratings of inverters 3 and 4. The inverter droop gains are set as $m_{P_1} = m_{P_2} = 9.4 \times 10^{-5}$, $m_{P_3} = m_{P_4} = 18.8 \times 10^{-5}$, $n_{Q_1} = n_{Q_2} = 1.3 \times 10^{-3}$, and $n_{Q_3} = n_{Q_4} = 2.6 \times 10^{-3}$. Inverters communicate on a bidirectional communication network with the adjacency matrix of $\mathcal{A} = [0 \ 1 \ 0 \ 1; 1 \ 0 \ 1 \ 0; 0 \ 1 \ 0 \ 1; 1 \ 0 \ 1 \ 0]$. The pinning gains are $g_{15} = g_{36} = 1$. The frequency reference, upper voltage reference, and lower voltage reference are 60 Hz, 340 V, and 330 V, respectively. The unbounded attack injections to the frequency and voltage control loops are set as $\omega_{f_i} = 1t, i = 1, 2, 3, 4$ and $\omega_{v_i} = 10t, i = 1, 2, 3, 4$, respectively. The performance of the resilient control protocols, (17)–(20), is compared with the conventional secondary control method in (5) and (6). The coupling gains for the conventional control protocols are set as $c_{f_i} = 10, c_{v_i} = 20, i = 1, 2, 3, 4$. The adaptive tuning parameters for the resilient control method are set as $\chi_{f_i} = 3, \chi_{v_i} = 3, i = 1, 2, 3, 4$.

Figure 4 compares the frequency response for the proposed and the conventional methods. Under ideal conditions (no attacks), inverters frequencies synchronize to $f = 60$ Hz using both control methods. Once the unbounded attack to frequency control loops is initiated at $t = 4$ s, the conventional method fails to preserve the system stability. By contrast, the proposed resilient method contains frequencies at a small neighborhood around 60 Hz. Figure 5 shows that, without attacks, both methods share active powers among inverters based on their droop gains. After initiating the unbounded attacks to frequency control loops at $t = 4$ s, the active power performance from the conventional method becomes unstable. Meanwhile, the proposed method contains active powers in a small neighborhood around the value of properly shared powers. Figure 6 compares inverters' voltages using both control methods. Without attacks, voltage values stay in the range of 330 V to 340 V. After initiating the unbounded attacks to voltage control loops at $t = 4$ s, the voltages terms using the conventional method diverge, while those produced by the proposed method remain stable within 330~340 V.

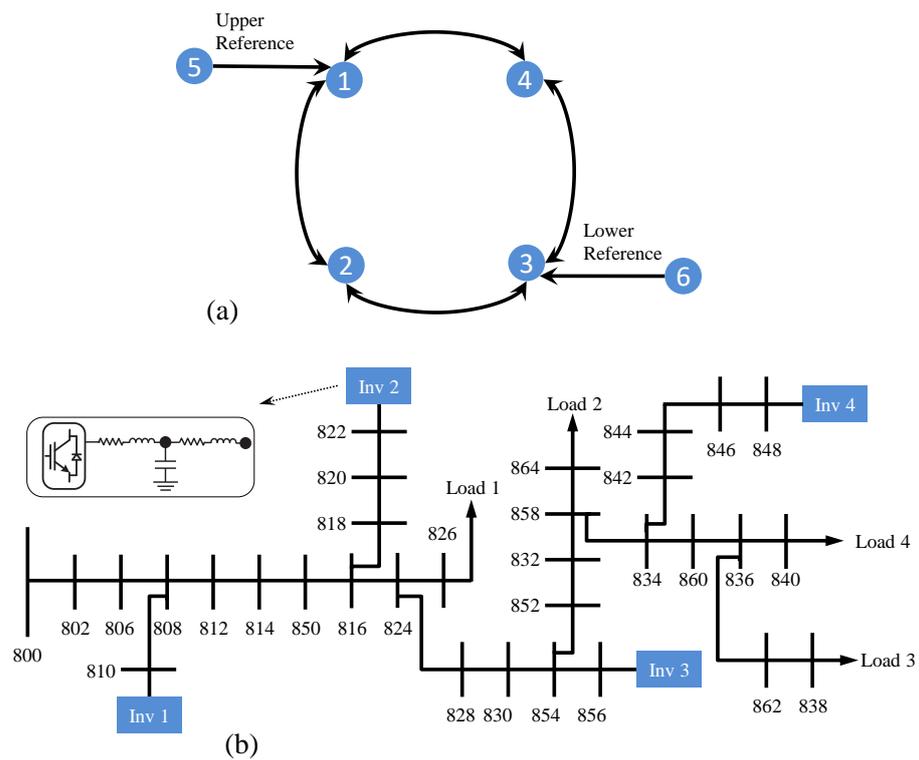


Figure 3. Cyber-physical microgrid system: (a) communication graph topology among four inverters and two leaders and (b) IEEE 34-bus system with four inverters.

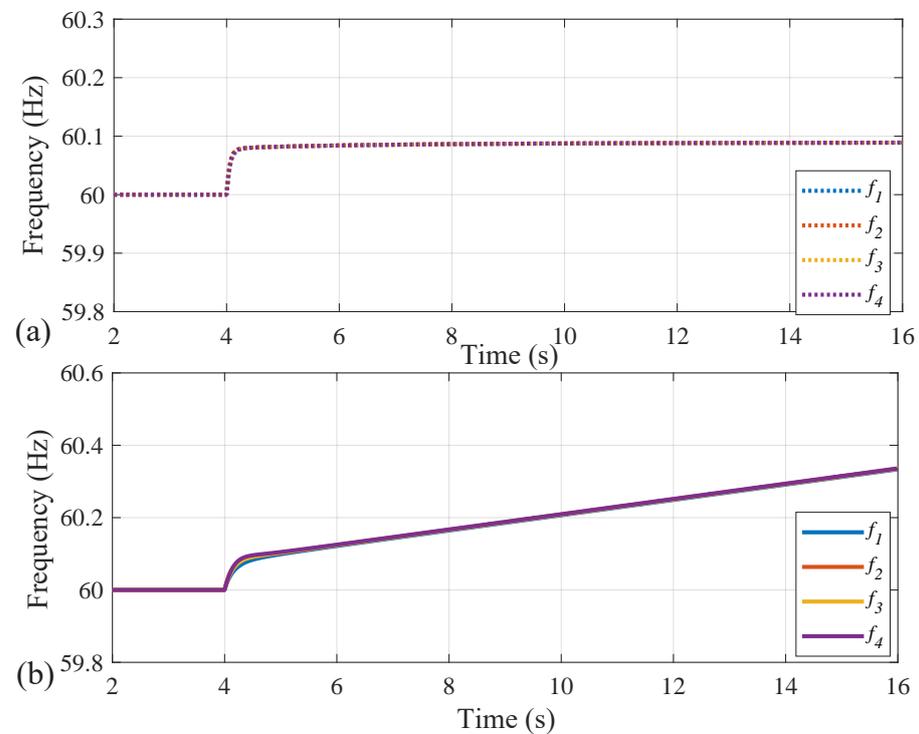


Figure 4. Frequency response under unbounded actuator attacks: (a) proposed resilient method and (b) conventional control method.

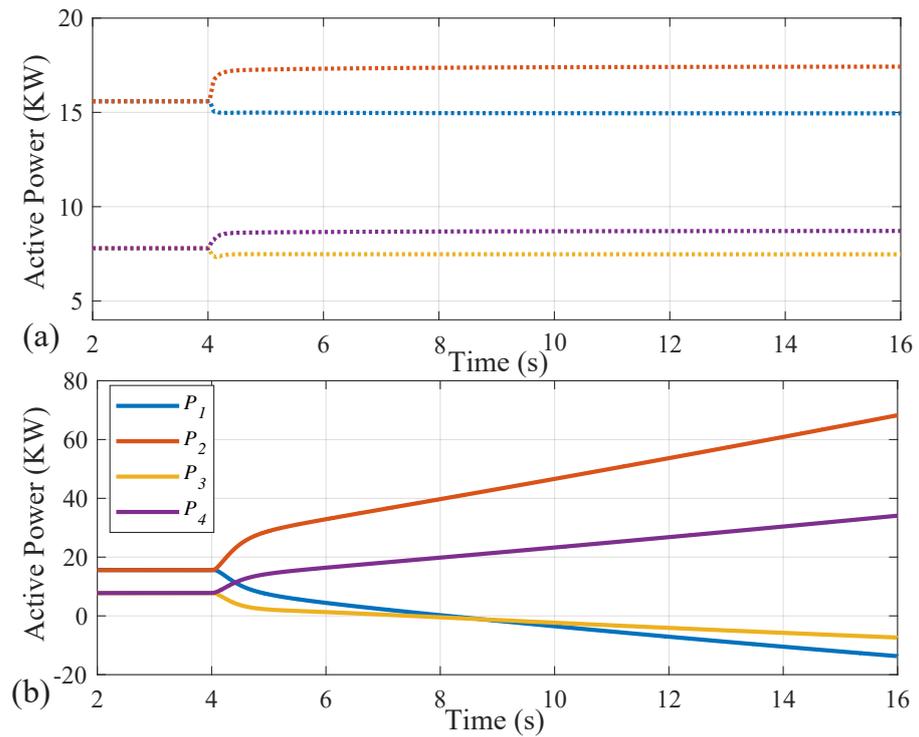


Figure 5. Active powers of inverters subjected to unbounded actuator attacks: (a) proposed resilient method and (b) conventional method.

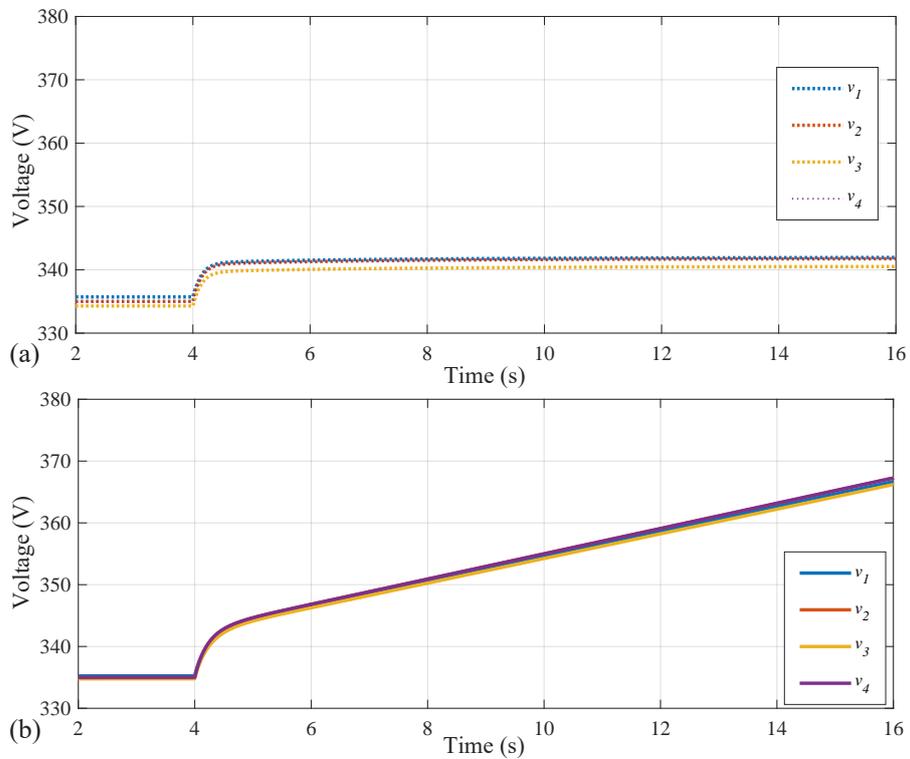


Figure 6. Voltage performance under unbounded actuator attacks: (a) proposed resilient method and (b) conventional control method.

The ultimate bound of the UUB convergence can be adjusted to be an arbitrarily small value by increasing the adaptive tuning parameters. Figures 7 and 8 show the frequency and active power waveforms, where the performance with $\chi_{f_i} = 3$ and $\chi_{f_i} = 10$ are

illustrated with solid and dashed lines, respectively. As seen, the ultimate bound can be reduced by increasing χ_{f_i} .

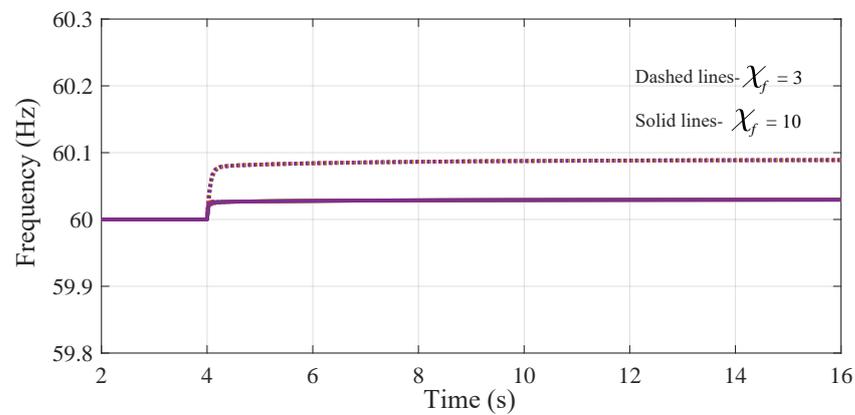


Figure 7. Comparative frequency performance under unbounded actuator attacks with different adaptive tuning parameters.

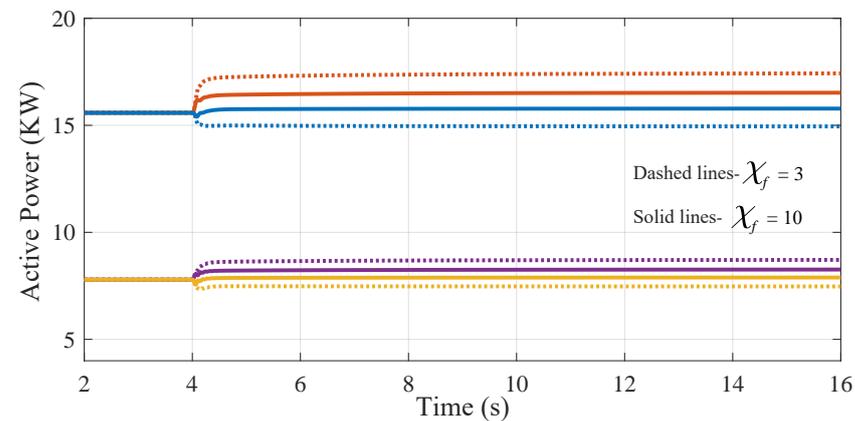


Figure 8. Comparative active power performance under unbounded actuator attacks with different adaptive tuning parameters.

7. Conclusions

This paper presents a novel resilient secondary controller for multi-inverter AC microgrids against unknown unbounded actuator attacks on both frequency and voltage control loops. A fully distributed adaptive control framework ensures the UUB stability of the closed-loop system by preserving the UUB regulation for both frequency and voltage terms. Moreover, the ultimate bound can be set by adjusting the tuning parameters. The resilient performance of the proposed method has been verified using a modified IEEE 34-bus system.

Author Contributions: Conceptualization, S.Z.; methodology, S.Z.; validation, S.Z. and Y.Z.; formal analysis, S.Z. and Y.W.; investigation, S.Z., Y.Z. and Y.W.; resources, S.Z.; data curation, S.Z. and Y.Z.; writing—original draft preparation, S.Z., Y.Z. and Y.W.; writing—review and editing, S.Z., Y.Z. and Y.W.; visualization, Y.Z. and Y.W.; supervision, S.Z.; project administration, S.Z.; funding acquisition, S.Z. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Not applicable.

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

Abbreviations

The following abbreviations are used in this manuscript:

AC	Alternating Current
FDI	False Data Injection
UUB	Uniformly ultimately bounded

References

- Bidram, A.; Lewis, F.L.; Davoudi, A. Distributed control systems for small-scale power networks: Using multiagent cooperative control theory. *IEEE Control Syst. Mag.* **2014**, *34*, 56–77.
- Zuo, S.; Beg, O.A.; Lewis, F.L.; Davoudi, A. Resilient networked AC microgrids under unbounded cyber attacks. *IEEE Trans. Smart Grid* **2020**, *11*, 3785–3794. [[CrossRef](#)]
- Kosut, O.; Jia, L.; Thomas, R.J.; Tong, L. Malicious data attacks on the smart grid. *IEEE Trans. Smart Grid* **2011**, *2*, 645–658. [[CrossRef](#)]
- Sridhar, S.; Hahn, A.; Govindarasu, M. Cyber-physical system security for the electric power grid. *Proc. IEEE* **2011**, *100*, 210–224. [[CrossRef](#)]
- He, H.; Yan, J. Cyber-physical attacks and defences in the smart grid: A survey. *IET Cyber-Phys. Syst. Theory Appl.* **2016**, *1*, 13–27. [[CrossRef](#)]
- Deng, R.; Xiao, G.; Lu, R.; Liang, H.; Vasilakos, A.V. False data injection on state estimation in power systems—Attacks, impacts, and defense: A survey. *IEEE Trans. Industr. Inform.* **2016**, *13*, 411–423. [[CrossRef](#)]
- Beg, O.A.; Nguyen, L.V.; Johnson, T.T.; Davoudi, A. Signal temporal logic-based attack detection in DC microgrids. *IEEE Trans. Smart Grid* **2018**, *10*, 3585–3595. [[CrossRef](#)]
- Zhang, J.; Sahoo, S.; Peng, J.C.-H.; Blaabjerg, F. Mitigating concurrent false data injection attacks in cooperative DC microgrids. *IEEE Trans. Power Electron.* **2021**, *36*, 9637–9647. [[CrossRef](#)]
- Tan, S.; Guerrero, J.M.; Xie, P.; Han, R.; Vasquez, J.C. Brief survey on attack detection methods for cyber-physical systems. *IEEE Syst. J.* **2020**, *14*, 5329–5339. [[CrossRef](#)]
- Liu, Y.; Ning, P.; Reiter, M.K. False data injection attacks against state estimation in electric power grids. *ACM Trans. Inf. Syst. Secur.* **2011**, *14*, 1–33. [[CrossRef](#)]
- Hug, G.; Giampapa, J.A. Vulnerability assessment of AC state estimation with respect to false data injection cyber-attacks. *IEEE Trans. Smart Grid* **2012**, *3*, 1362–1370. [[CrossRef](#)]
- Liang, J.; Sankar, L.; Kosut, O. Vulnerability analysis and consequences of false data injection attack on power system state estimation. *IEEE Trans. Power Syst.* **2015**, *31*, 3864–3872. [[CrossRef](#)]
- Pan, K.; Teixeira, A.; Cvetkovic, M.; Palensky, P. Cyber risk analysis of combined data attacks against power system state estimation. *IEEE Trans. Smart Grid* **2018**, *10*, 3044–3056. [[CrossRef](#)]
- Chen, Y.; Qi, D.; Dong, H.; Li, C.; Li, Z.; Zhang, J. A FDI attack-resilient distributed secondary control strategy for islanded microgrids. *IEEE Trans. Smart Grid* **2020**, *12*, 1929–1938. [[CrossRef](#)]
- Liu, X.-K.; Wen, C.; Xu, Q.; Wang, Y.-W. Resilient control and analysis for DC microgrid system under DoS and impulsive FDI attacks. *IEEE Trans. Smart Grid* **2021**, *12*, 3742–3754. [[CrossRef](#)]
- Lu, J.; Zhang, X.; Hou, X.; Wang, P. Generalized extended state observer-based distributed attack-resilient control for DC microgrids. *IEEE Trans. Sustain. Energy* **2022**, *13*, 1469–1480. [[CrossRef](#)]
- Deng, C.; Wang, Y.; Wen, C.; Xu, Y.; Lin, P. Distributed resilient control for energy storage systems in cyber-physical microgrids. *IEEE Trans. Industr. Inform.* **2020**, *17*, 1331–1341. [[CrossRef](#)]
- Abhinav, S.; Modares, H.; Lewis, F.L.; Ferrese, F.; Davoudi, A. Synchrony in networked microgrids under attacks. *IEEE Trans. Smart Grid* **2017**, *9*, 6731–6741. [[CrossRef](#)]
- Dehkordi, N.M.; Baghaee, H.R.; Sadati, N.; Guerrero, J.M. Distributed noise-resilient secondary voltage and frequency control for islanded microgrids. *IEEE Trans. Smart Grid* **2018**, *10*, 3780–3790. [[CrossRef](#)]
- Shahab, M.A.; Mozafari, B.; Soleymani, S.; Dehkordi, N.M.; Shourkaei, H.M.; Guerrero, J.M. Distributed consensus-based fault tolerant control of islanded microgrids. *IEEE Trans. Smart Grid* **2019**, *11*, 37–47. [[CrossRef](#)]
- Afshari, A.; Karrari, M.; Baghaee, H.R.; Gharehpetian, G.B.; Karrari, S. Cooperative fault-tolerant control of microgrids under switching communication topology. *IEEE Trans. Smart Grid* **2019**, *11*, 1866–1879. [[CrossRef](#)]
- Fawzi, H.; Tabuada, P.; Diggavi, S. Secure estimation and control for cyber-physical systems under adversarial attacks. *IEEE Trans. Automat. Contr.* **2014**, *59*, 1454–1467. [[CrossRef](#)]
- Han, R.; Meng, L.; Ferrari-Trecate, G.; Coelho, E.A.A.; Vasquez, J.C.; Guerrero, J.M. Containment and consensus-based distributed coordination control to achieve bounded voltage and precise reactive power sharing in islanded AC microgrids. *IEEE Trans. Ind. Appl.* **2017**, *53*, 5187–5199. [[CrossRef](#)]
- Zuo, S.; Song, Y.; Lewis, F.L.; Davoudi, A. Output containment control of linear heterogeneous multi-agent systems using internal model principle. *IEEE Trans. Cybern.* **2017**, *47*, 2099–2109. [[CrossRef](#)] [[PubMed](#)]
- Khalil, H.K. *Nonlinear Systems*, 3rd ed.; Prentice-Hall: Upper Saddle River, NJ, USA, 2002.

-
26. LaSalle, J. Some extensions of Liapunov's second method. *IRE Trans. Circuit. Theory* **1960**, *7*, 520–527. [[CrossRef](#)]
 27. Mwakabuta, N.; Sekar, A. Comparative study of the IEEE 34 node test feeder under practical simplifications. In Proceedings of the 2007 39th North American power symposium, Las Cruces, NM, USA, 30 September–2 October 2007.