# PHYSICAL AND CYBER ANOMALY MANAGEMENT IN MASSIVELY DIGITIZED POWER SYSTEMS

A Dissertation

by

TONG HUANG

Submitted to the Office of Graduate and Professional Studies of
Texas A&M University
in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

| | |
|---|---|
| Chair of Committee, | Le Xie |
| Committee Members, | P. R. Kumar |
| | Thomas Overbye |
| | Jianhua Huang |
| Head of Department, | Miroslav M. Begovic |

August 2021

Major Subject: Electrical Engineering

# ABSTRACT

The past century has witnessed a digitization trend of electric power grid where increasing digital solutions are being integrated into the grid infrastructure. The digital solutions do not only provide opportunities for enhancing monitoring, control and protection of the power grid, but also pose challenges of ensuring both cyber and physical security of the grid. This dissertation provides three concrete examples in order to leverage the emerging opportunities and to address pressing challenges in massively digitized grid. By using rich streaming synchrophasor data in bulk power transmission systems, a purely data-driven algorithm is proposed in order to locate sources of forced oscillations. To enhance the cyber resilience of the grid, this dissertation develops a theoretically rigorous yet practically implementable method for detecting cyber attacks in Automatic Generation Control. A learning-based framework is designed for assessing physical security of networked microgrids. Furthermore, an advanced Energy Management System for future digitized power grids is envisioned and thereby future research directions are pointed out.

# DEDICATION

To my parents, Mr. Shuliang Huang and Ms. Lang Chen, and my girlfriend, Xuenan

# ACKNOWLEDGMENTS

I would like to express my sincere gratitude to my academic advisor Professor Le Xie for his constant support and valuable guidance on both of my research and life in the past few years. Professor Xie kept encouraging me to identify/solve problems that can really shake my field and motivating me to venture into my neighboring fields. He also taught me how to effectively deliver my ideas to others and helped me build my self-confidence. The nurture was delivered by thousands of our discussions and conversations in the past few years. I believe he is my lifetime role model who I can constantly learn from.

My sincere appreciations are extended to my dissertation committee members for their constructive suggestions on my dissertation. In addition, I would like to thank Professor Kumar who guided me to explore the fields of control, signal processing, and optimization and patiently helped me improve my writing. I am thankful to Professor Overbye who helped me to systematically build a solid theoretical foundation of power system dynamics. I would like also to thank Professor Huang for enthusiastically encouraging me to translate statistical learning approaches to power system applications.

I would like also to thank my mentors during my internships and the coauthors of my publications: Dr. Xiaochuan Luo, Dr. Slava Maslennikov, Mr. Qiang Zhang, Dr. Song Zhang, and Dr. Eugene Litvinov of ISO New England; Dr. Hongbo Sun, Dr. Kyeong Jin Kim, and Dr. Daniel Nikovski of Mitsubishi Electric Research Laboratories (MERL); Professor Nikolaos Freris of the University of Science and Technology of China (USTC); Dr. Bharadwaj Satchidanandan of Massachusetts Institute of Technology (MIT); Professor Sicun Gao of University of California San Diego (UCSD); Dr. Jorge Ramos-Ruiz, Dr. Woo-Hyun Ko, Mr. Jaewon Kim and Professor Prasad Enjeti of Texas A&M University; Dr. Bin Wang of National Renewable Energy Laboratory (NREL); and Dr. Xun Long of

Delta Electronics.

My gratitude also goes to my friends during my Ph.D. journey. They are Sadegh, Xinbo, Meng, Bainan, Yuqi, Benjamin Wiseman, Hao, Hung-ming, Dongqi, Xiangtian, Rayan, Yuanyuan, Gracie, Cheng (Peter), Siva, Athindra, Haotian, Sicheng, Dian, Haibo, Shuang, Xin and Yida, Chao, Xiaolin, Guangchun, Amit, Xia and Xinhui, Rupamathi, Yixuan, Chenyang, Chenhao, Yunting, Gang, Zichao, Stacey Johnson (and his parents, Mr. and Ms. Johnson), Jordan Davison, Dongzuo, Xiaoqian, and so on.

Last but not the least, I would like to thank my parents, Mr. Shuliang Huang and Ms. Lang Chen, for their constant, unconditional love and support. Special thanks to Xuenan who understands, loves, and supports me.

It is the above people who make my Ph.D. journey full of fruits and happiness.

# CONTRIBUTORS AND FUNDING SOURCES

## Contributors

This work was conducted with the guidance from a dissertation committee containing Professor Le Xie, Professor P. R. Kumar, Professor Thomas Overbye of the Department of Electrical and Computer Engineering and Professor Jianhua Huang of the Department of Statistics.

Part of work in Chapter 2 was performed in collaboration with Professor Nikolaos M. Freris of the University of Science and Technology of China (USTC). Part of work in Chapter 3 was completed with Dr. Bharadwaj Satchidanandan of Massachusetts Institute of Technology (MIT). Part of work in Chapter 4 was conducted in collaboration with Professor Sicun Gao of University of California San Diego (UCSD). All other work conducted for this dissertation was completed by the student independently.

## Funding Sources

Graduate study was in part supported by the following funding resources:

- National Science Foundation (NSF) Grants ECCS-1611301, 2038963
- Power Systems Engineering Research Center (PSERC)
- Electric Reliability Council of Texas (ERCOT)
- Department of Energy (DOE) Grant DE-EE0009031

TABLE OF CONTENTS

Page

LIST OF FIGURES

FIGURE Page

LIST OF TABLES

TABLE Page

# 1. INTRODUCTION

Electric power systems are in the trend of digitization where increasing digital solutions are being integrated into the grid infrastructure. The digitization trend is manifested by the following aspects. First, there are increasing advanced sensors deployed in the grid. For example, a synchrophasor can steam finely-sampled yet synchronized measurements to a control center of a power transmission system. There are more than $2500$ commercial-grade synchrophasors (as of 2017) across North America [6], whereas only $200$ research-grade synchrophasors were installed in 2009 [7]. Second, many countries over the world aim to shrink their carbon footprint by deepening renewable penetration to their energy systems. The renewable resources are interfaced with the AC grid via inverters. As a result, the dynamics of the modern power grid are not only governed by giant, rotating synchronous generators, but also by the control strategies deployed in the power electronic interfaces. Third, some originally mechanical, isolated grid components gradually evolve into digital devices possessing communication and computation capacities. For example, mechanical protection relays are generally replaced by their digital version in the modern grid, and Internet of Things (IoT) devices, such as smart thermostats and plugs, emerge at the grid edge.

On the one hand, the digitization of the grid provides immense opportunities for enhancing transparency of the grid operation. The sensor proliferation allows for developing real-time decision-aid tools in order to detect, classify, locate, and mitigate anomalies in the grid. For example, in transmission systems, synchrophasor data can be used to monitor critical oscillations [8] and to detect events [9] (e.g., line/generator tripping) at their early stages. In distribution systems, AMI (Advanced Metering Infrastructure) data can be leveraged to determine which phase each customer connects to [10].

On the other hand, the massively digitized grid arises concerns about cyber and physical security of the grid. In the digitized grid, many decision making processes possess a feedback structure where a controller issues control commands to drive physical infrastructure based on sensors. Examples of these processes include Automatic Generation Control (AGC), Automatic Voltage Regulator (AVR), grid-forming/following control of inverters, and so on. Such a feedback structure arises cyber vulnerability where adversaries may compromise the grid by maliciously manipulating the sensors. Besides the cyber vulnerability, inverters serving as interfaces between renewable generation resources and the grid may incur physical security issues in both power transmission and distribution systems. In transmission systems, wind/solar farms interfaces with the AC grid via inverters. Malfunctioning inverters may lead to renewable curtailment. On August 16, 2016, there was such a kind of event reported in California, where the the malfunctioning inverters caused about 700-MW photovoltaic resources to disconnect from the grid [11]. In distribution systems, installing rooftop solar panels provides a promising solution to enhancing grid resilience and achieving carbon neutrality. The solar panels interact with the AC grid through inverters. It poses a significant challenge to distribution system operators (DSOs) who need to manage hundreds of inverter-based generation resources and to ensure the physical security of the inverter-based distribution systems [4, 12, 13].

This dissertation provides three concrete examples of leveraging the emerging opportunities and addressing pressing challenges in massively digitized grid. To be specific, Chapter 2 proposes a synchrophasor approach to locating sources of forced oscillations; Chapter 3 develops a theoretically rigorous yet practically implementable methods to detecting cyber attacks in AGC; Chapter 4 designs a learning-based framework for transient stability assessment of networked microgrids; and Chapter 5 envisions an Energy Management System (EMS) for future digitized power grids and points out future research directions. The techniques developed from Chapter 2 to Chapter 4 serve as building blocks of

the next generation of the EMS which provides a holistic solution to future grid operation. Each chapter uses an independent notation system.

# 2. A SYNCHROPHASOR DATA-DRIVEN METHOD FOR FORCED OSCILLATION LOCALIZATION UNDER RESONANCE CONDITIONS[1]

## 2.1 Motivation

Phasor measurement units (PMUs) enhance the transparency of bulk power systems by streaming the fast-sampled and synchronized measurements to system control centers. Such finely-sampled and time-stamped PMU measurements can reveal several aspects of the rich dynamical behavior of the grid which are invisible to conventional supervisory control and data acquisition (SCADA) systems. Among the system dynamical behaviors exposed by PMUs, *forced oscillations* (FOs) have attracted significant attention within the power community. FOs are driven by periodical exogenous disturbances that are typically injected by malfunctioning power apparatuses such as wind turbines, steam extractor valves of generators, or poorly-tuned control systems [14–16]. Cyclic loads, such as cement mills and steel plants, constitute another category of oscillation sources [14]. The impact of such injected periodic perturbation propagates through transmission lines and results in FOs throughout the grid; some real-world events of FOs since 1966 are reported in [14].

The presence of FOs compromises the security and reliability of power systems. For example, FOs may trigger protection relays to trip transmission lines or generators, potentially causing uncontrollable cascading failures and unexpected load shedding [17]. Moreover, sustained FOs reduce device lifespans by introducing undesirable vibrations and additional wear and tear on power system components; consequently, failure rates and maintenance costs of compromised power apparatuses might increase [17]. Therefore,

[1] ©2020 IEEE. Reprinted, with permission, from Tong Huang, Nikolaos M. Freris, P. R. Kumar and Le Xie, "A Synchrophasor Data-driven Method for Forced Oscillation Localization under Resonance Conditions," in *IEEE Transactions on Power Systems*, vol. 35, no. 5, pp. 3927-3939, Sept. 2020.

timely suppression of FOs is important to system operators.

One effective way of suppressing a forced oscillation is to locate the oscillation's source, a canonical problem that we call *forced oscillation localization*, and then to disconnect it from the power grid. A natural attempt to conduct forced oscillation localization could be tracking the largest oscillation over the power grid, under the assumption that measurements near the oscillatory source are expected to exhibit the most severe oscillations, based on engineering intuition. However, counter-intuitive cases may occur when the frequency of the periodic perturbation lies in the vicinity of one of the natural modes of the power system, whence a *resonance phenomenon* is triggered [18]. In such cases, PMU measurements exhibiting the most severe oscillations may be geographically far from where the periodic perturbation is injected, posing a significant challenge to system operators in pinpointing the forced oscillation source. It is worth noting that such counter-intuitive cases are more than a mere theoretical concern: one example occurred at the Western Electricity Coordinating Council (WECC) system on Nov. 29, 2005, when a 20-MW forced oscillation initiated by a generation plant at Alberta incurred a tenfold larger oscillation at the California-Oregon Inter-tie line that is 1100 miles away from Alberta [16]. Such a severe oscillation amplification significantly compromises the security and reliability of the power grid. Hence, it is imperative to develop a forced oscillation localization method that is effective even in the challenging but highly hazardous cases of resonance [1].

In order to pinpoint the source of FOs, several localization techniques have been developed. In [19], forced oscillation localization is achieved based on the following observation: the measurements near the source manifest distinct signatures in their magnitude or phase responses, in comparison to far away measurements. Such an observation is interpretable based on classic generator models, but whether it is valid or not in a power system with complex generator dynamics remains an open question [19]. In [15], the au-

thors leverage the oscillation energy flows in power networks to locate the source of sustained oscillations. In this energy-based method, the energy flows can be computed using the preprocessed PMU data, and the power system components generating the oscillation energy are identified as the oscillation sources. In spite of the promising performance of the energy-based method [15], the rather stringent assumptions pertaining to knowledge of load characteristics and the grid topology may restrict its usefulness to specific scenarios [1], [20]. Reference [20] provides a comprehensive summary of FO localization methods. More recent research on FO localization is reported in [21] and [22]. In [21], the oscillation source is located by comparing the measured current spectrum of system components with one predicted by the effective admittance matrix. However, the construction of the effective admittance matrix requires accurate knowledge of system parameters that may be unavailable in practice. In [22], generator parameters are learned from measurements based on prior knowledge of generator model structures, and, subsequently, the admittance matrix is constructed and used for FO localization. Nevertheless, model structures of generators might not be known beforehand, owing to the unpredictable switching states of power system stabilizers [23]. Thus, it is highly desirable to design a FO localization method that does not heavily depend upon availability of the first-principle model and topology information of the power grid.

In this chapter, we propose a *purely data-driven* yet *physically interpretable* approach to pinpoint the source of FOs in the challenging resonance case. By leveraging the sparsity of the FO sources and the low-rank nature of high-dimensional synchrophasor data, the problem of forced oscillation localization is formulated as computing the sparse and low-rank components of the measurement matrix using Robust Principal Component Analysis (RPCA) [24]. Based on this problem formulation, an algorithm for real-time operation is designed to pinpoint the source of FOs. The main merits of the proposed approach include the following: 1) It does not require any information on dynamical system model

parameters or topology, thus providing an efficient and easily deployable practical implementation; 2) It can locate the source of FOs with high accuracy, even when resonance phenomena occur; and 3) Its efficacy can be interpreted by physical model-based analysis.

The rest of this chapter is organized as follows: Section 2.2 elaborates on the forced oscillation localization problem and its main challenges; in Section 3.2, the FO localization is formulated as a matrix decomposition problem and a FO localization algorithm is designed; Section 2.4 provides theoretical justification of the efficacy of the algorithm; Section 2.5 validates the effectiveness of the proposed method in synthetic cases based on benchmark systems and real-world forced oscillations in the power grid of Texas; Section 2.6 summarizes the chapter and poses future research questions.

## 2.2 Localization of Forced Oscillations and Challenges

### 2.2.1 Mathematical Interpretation

The dynamic behavior of a power system in the vicinity of its operation condition can be represented by a continuous linear time-invariant (LTI) state-space model:

$$\dot{\mathbf{x}}(t) = A\mathbf{x}(t) + B\mathbf{u}(t), \tag{2.1a}$$

$$\mathbf{y}(t) = C\mathbf{x}(t) + D\mathbf{u}(t), \tag{2.1b}$$

where state vector $\mathbf{x} \in \mathbb{R}^n$, input vector $\mathbf{u} \in \mathbb{R}^r$, and output vector $\mathbf{y} \in \mathbb{R}^m$ collect the *deviations* of state variables, generator/load control setpoints, and measurements, from their respective steady-state values. Accordingly, matrices $A \in \mathbb{R}^{n\times n}$, $B \in \mathbb{R}^{n\times r}$, $C \in \mathbb{R}^{m\times n}$, and $D \in \mathbb{R}^{m\times r}$ are termed as the state matrix, the input matrix, the output matrix, and the feed-forward matrix, respectively. Typically, the input vector $\mathbf{u}$ is not streamed to control centers, so the feed-forward matrix $D$ is assumed to be a zero matrix of appropriate dimension. Denote by $\mathcal{L} = \{\lambda_1, \lambda_2, \ldots, \lambda_n\}$ the set of all eigenvalues of the state matrix

$A$. The power system (2.1) is assumed to be stable, with all eigenvalues $\lambda_i \in \mathbb{C}$ being distinct, i.e., $\mathrm{Re}\{\lambda_i\} < 0$ for all $i \in \{1, 2, \ldots, n\}$ and $\lambda_i \neq \lambda_j$ for all $i \neq j$. Note that the assumption on eigenvalue distinctness is only used for the purpose of simplifying the process of obtaining the time-domain solution of outputs in Section 2.4. Due to a large amount of symbols in this chapter, the key symbols are summarized in the appendix for the convenience of readers.

We proceed to formally define the concepts of a forced oscillation source and source measurements. Suppose that the $l$-$th$ input $u_l(t)$ in the input vector $\mathbf{u}(t)$ varies periodically due to malfunctioning components (generators/loads) in the grid. In such a case, $u_l(t)$ can be decomposed into $J$ frequency components, viz.,

$$u_l(t) = \sum_{j=1}^{J} P_j \sin(\omega_j t + \theta_j), \tag{2.2}$$

where $\omega_j \neq 0$, $P_j \neq 0$ and $\theta_j$ are the frequency, amplitude and phase displacement of the $j$-$th$ frequency component of the $l$-$th$ input, respectively. Equation (2.2) is effectively equivalent to the Fourier series representation of a periodic signal [25]. As a consequence, the periodic input will result in sustained oscillations present in the measurement vector $\mathbf{y}$. The generator/load associated with input $l$ is termed as the *forced oscillation source*, and the measurements at the bus directly connecting to the forced oscillation source are termed as *source measurements*.

In particular, suppose that the frequency $\omega_d$ of an injection component is close to the frequency of a poorly-damped mode, i.e., there exists $j^* \in \{1, 2, \ldots, n\}$,

$$\omega_d \approx \mathrm{Im}\{\lambda_{j^*}\}, \quad \mathrm{Re}\{\lambda_{j^*}\} \approx 0. \tag{2.3}$$

In such a case, resonance phenomena can be observed [18]. Hence, (2.3) is adopted as the

*resonance condition* in this chapter. Studies on envelop shapes of FOs are reported in [26].

In a power system with PMUs, the measurement vector $\mathbf{y}(t)$ is sampled at a frequency of $f_{\mathrm{s}}$ (samples per second). Within a time interval from the FO starting time up to time instant $t$, the time evolution of the measurement vector $\mathbf{y}(t)$ can be discretized by sampling and represented by a matrix called a *measurement matrix* $Y_t = [y^t_{p,q}]$, which we formally define next. Without loss of generality, we assume that the FOs start at time $0$. The following column concatenation defines the measurement matrix $Y_t$ up to time $t$:

$$Y_t := \left[\mathbf{y}(0), \quad \mathbf{y}(1/f_{\mathrm{s}}), \quad \dots \quad \mathbf{y}(\lfloor t f_{\mathrm{s}} \rfloor / f_{\mathrm{s}})\right], \tag{2.4}$$

where $\lfloor \cdot \rfloor$ denotes the floor operation. The $i$-$th$ column of the measurement matrix $Y_t$ in (2.4) suggests the "snapshot" of all synchrophasor measurements over system at the time $(i-1)/f_{\mathrm{s}}$. The $k$-$th$ row of $Y_t$ denotes the time evolution of the $k$-$th$ measurement deviation in the output vector of the $k$-th PMU. Due to the fact that the output vector may contain multiple types of measurements (e.g., voltage magnitudes, frequencies, etc.), a normalization procedure is introduced as follows. Assume that there are $K$ measurement types. Denote by $Y_{t,i} = [y^{t,i}_{p,q}] \in \mathbb{R}^{r_0 \times c_0}$ the measurement matrix of measurement type $i$, where $i = \{1, 2, \dots, K\}$. The normalized measurement matrix $Y_{\mathrm{n}t} = [y^{\mathrm{n},t}_{p,q}]$ is defined by

$$Y_{\mathrm{n}t} = \left[\frac{Y^\top_{t,1}}{\|Y_{t,1}\|_{\max}}, \quad \frac{Y^\top_{t,2}}{\|Y_{t,2}\|_{\max}}, \quad \dots \quad \frac{Y^\top_{t,K}}{\left\|Y_{t,K}\right\|_{\max}}\right]^\top, \tag{2.5}$$

where $\|\cdot\|_{\max}$ returns the largest absolute element of a matrix.

The forced oscillation localization problem is equivalent to pinpointing the forced oscillation source using measurement matrix $Y_t$. Due to the complexity of power system dynamics, the precise power system model (2.1) may not be available to system operators, especially in real-time operation. Therefore, it is assumed that the only known information

for forced oscillation localization is the measurement matrix $Y_t$. In brief, the first-principle model (2.1) as well as the perturbation model (2.2) is introduced mainly for the purpose of defining FO localization problem and theoretically justifying the data-driven method proposed in Section 3.2, but is not needed for the proposed algorithm.

### 2.2.2 Main Challenges of Pinpointing the Sources of Forced Oscillation

The topology of the power system represented by (2.1) can be characterized by an undirected graph $G = (\mathcal{B}, \mathcal{T})$, where vertex set $\mathcal{B}$ comprises all buses in the power system, while edge set $\mathcal{T}$ collects all transmission lines. Suppose that the PMU measurements at bus $i_{\rm s} \in \mathcal{B}$ are the source measurements. Then bus $j$ is said to be in the vicinity of the FO source if bus $j$ is a member of the following vicinity set:

$$\mathcal{V}_0 = \{j \in \mathcal{B} | d_G(i_{\rm s}, j) \leq N_0\}, \tag{2.6}$$

where $d_G(i, j)$ denotes the $i$-$j$ distance, viz., the number of transmission lines (edges) in a shortest path connecting buses (vertices) $i$ and $j$; the threshold $N_0$ is a nonnegative integer. In particular, $\mathcal{V}_0 = \{i_{\rm s}\}$ for the source measurement at bus $i_{\rm s}$, if $N_0$ is set to zero.

Intuitively, it is tempting to presume that the source measurement can be localized by finding the maximal absolute element in the normalized measurement matrix $Y_{{\rm n}t}$, i.e., expecting that the most severe oscillation should be manifested in the vicinity of the source. However, a major challenge for pinpointing the FO sources arises from the following (perhaps counter-intuitive) fact: the most severe oscillation does not necessarily manifest near the FO source, in the presence of *resonance phenomena*. Following the same notation as in (2.4) and (2.6), we term a normalized measurement matrix $Y_{\rm nt}$ as *counter-intuitive case*, if

$$i^* \notin \mathcal{V}_0, \tag{2.7}$$

where $i^*$ can be obtained by finding the row index of the maximal element in the measurement matrix $Y_t$, i.e.,

$$[i^*, j^*] = \arg\max_{i,j} \left| y_{i,j}^{\mathrm{n},t} \right|. \tag{2.8}$$

It is such counter-intuitive cases that make pinpointing the FO source challenging [18]. Figure 2.1 illustrates one such counter-intuitive case, where the source measurement (red) does not correspond to the most severe oscillation. Additional examples of counter-intuitive cases can be found in [1]. Although the counter-intuitive cases are much less likely to happen than the intuitive ones (in terms of frequency of occurrence), it is still imperative to design an algorithm to pinpoint the FO source even in the counter-intuitive cases due to the hazardous consequences of the FOs under resonance conditions.

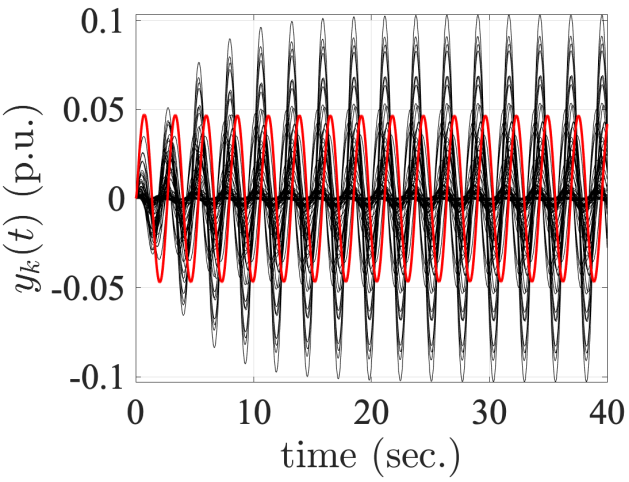



Figure 2.1: One counter-intuitive case [1] from the IEEE 68-bus benchmark system [2]: the black curves correspond to the non-source measurements; the red curve corresponds to the source measurement.

## 2.3 Problem Formulation and Proposed Methodology

In this section, we formulate the FO localization problem as a matrix decomposition problem. Then, we present a FO localization algorithm for real-time operation.

### 2.3.1 Problem Formulation

Given a measurement matrix $Y_t$ up to time $t$ with one type of measurement (without loss in generality), the FO source localization is formulated as decomposing the measurement matrix $Y_t$ into a low-rank matrix $L_t$ and a sparse matrix $S_t$:

$$Y_t = L_t + S_t, \tag{2.9a}$$

$$\operatorname{rank} L_t \leq \gamma, \tag{2.9b}$$

$$\|S_t\|_0 \leq \beta, \tag{2.9c}$$

where the pseudo-norm $\|\cdot\|_0$ returns the number of non-zero elements of a matrix; the non-negative integer $\gamma$ is the upper bound of the rank of the low-rank matrix $L_t$, and the non-negative integer $\beta$ is the upper bound on the number of non-zero entries in the sparse matrix $S_t$. Given non-negative integers $\gamma$ and $\beta$, it is possible to numerically find $\{L_t, S_t\}$ via *alternating projections* [1]. The source measurement index $p^*$ can be tracked by finding the largest absolute value in the sparse matrix $S_t$, viz.,

$$[p^*, q^*]^\top = \arg\max_{p,q} \left| s^t_{p,q} \right|. \tag{2.10}$$

The intuition behind the formulation (2.9) is as follows. As the power grid is an interconnected system, measurements at different buses have certain electrical couplings, resulting in correlations between the measurements. As a result, the measurements at different buses should exhibit a "general trend," [1] which can be captured by a low-rank

matrix $L_t$. The measurements near the FO source are assumed to deviate most from its corresponding component in "general trend" (the low-rank matrix $L_t$). The deviation is supposed to be captured by the matrix $S_t$. As the number of the measurements near the FO source is limited, the matrix $S_t$ is assumed to be sparse.

Due to the prior unavailability of the upper bounds $\gamma$ and $\beta$ [1], the matrix decomposition problem shown in (2.9) is reformulated as an instance of *Robust Principal Component Analysis (RPCA)* [24]:

$$\min_{S_t} \quad \|Y_t - S_t\|_\star + \xi \|S_t\|_1, \tag{2.11}$$

where $\|\cdot\|_\star$ and $\|\cdot\|_1$ denote the nuclear norm and $l_1$ norm, respectively; the tunable parameter $\xi$ regulates the extent of sparsity in $S_t$. The formulation in (2.11) is a convex relaxation of (2.9). Under some assumptions, the sparse matrix $S_t$ and the low-rank matrix $L_t$ can be disentangled from the measurement matrix $Y_t$ [24] by diverse algorithms [27]. The exact Lagrange Multiplier Method (ALM) is used for numerically solving the formulation (2.11). Recall that the measurement matrix $Y_t$ has $r_0$ rows and $c_0$ columns. The tunable parameter $\xi$ is suggested to be $1/\sqrt{k_0}$, where $k_0 = \max\{r_0, c_0\}$. Such selection of $\xi$ is justified via the mathematical analysis in [24]. For a measurement matrix containing multiple measurement types, (2.11) can be modified by replacing $Y_t$ with $Y_{\mathrm{n}t}$.

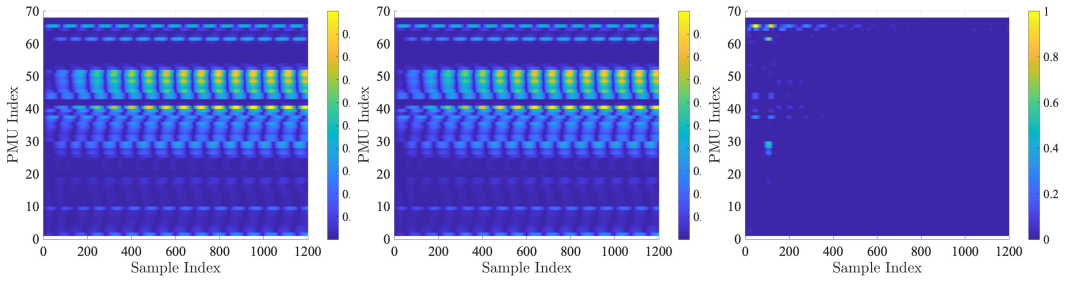
### 2.3.2 FO Localization Algorithm for Real-time Operation

Next, we present a FO localization algorithm for real-time operation, using the formulation (2.11). In order to determine the starting time of forced oscillations, we can leverage the methods reported in [28, 29]. The method reported in [28] is used to detect FOs by comparing the periodogram of PMU measurements with a frequency-dependent threshold. In [29] the authors propose a method that uses geometric analysis on streaming synchrophasor data to estimate the starting and end times of FOs. Once periodic FOs are detected by the method reported in [28], the starting time of the FOs can be estimated by

the time-localization algorithm proposed in [29]. A window of measurements with the starting time is collected into forming the measurement matrix. Then Algorithm 1 is triggered for pinpointing the FO source. In Algorithm 1, $T_0$ and $\xi$ are user-defined parameters.

**Algorithm 1** Real-time FO Localization

1: Update $Y_{T_0}$ by (2.4);
2: Obtain $Y_{\mathrm{n}T_0}$ by (2.5);
3: Find $S_t$ in (2.11) via the exact ALM for chosen $\xi$;
4: Obtain $p^*$ by (2.10);
5: **return** $p^*$ as the source measurement index.




(a) (b) (c)

Figure 2.2: Visualization of the measurement matrix $Y_t$ (a), the low-rank matrix $L_t$ (b), and the sparse matrix $S_t$ (c)

.

Algorithm 1 can be leveraged to illustrate the intuition behind formulation (2.9) described in Section III-A. A measurement matrix $Y_t$ can be formed based on the measurements visualized in Figure 2.1. Algorithm 1 can decompose $Y_t$ into a low-rank matrix $L_t$ and a sparse matrix $S_t$. Figure 2.2 visualizes $Y_t$, $L_t$, and $S_t$ in a *normalized* fashion. For each matrix, we take the absolute values of their entries and normalize the absolute version

of the entries by the maximal absolute entry in the corresponding matrix. The magnitudes of the *normalized* entries are represented by color: The bigger the magnitude of an entry, the yellower is its color, and conversely the smaller the magnitude of an entry, the bluer is its color. The "general trend" of the measurements is captured by the low-rank matrix $L_t$ in Figure 2.2(b). The deviations from the "general trend" are captured by the sparse matrix $S_t$. In Figure 2.2(c), very few entries are colored with yellow, and these entries correspond measurements deviating most from the "general trend", while most entries are colored with dark blue, suggesting that most entries are close to zero. The entry colored with brightest color corresponds to Bus $65$ which is the bus closest to the force oscillation source (Generator $13$).

## 2.4 Theoretical Interpretation of the RPCA-based Algorithm

This section aims to develop a theoretical connection between the first-principle model in Section 2.2 and the data-driven approach presented in Section 3.2. We start such an investigation by deriving the time-domain solution to PMU measurements in a power system under resonance conditions. Then, the resonance component matrix for the power grid is obtained from the derived solution to PMU measurements. Finally, the efficacy of the proposed method is interpreted by examining the rank of the resonance component matrix.

### 2.4.1 PMU Measurement Decomposition

For the power system with $r$ inputs and $m$ PMU measurements modeled using (2.1), the $k$-th measurement and the $l$-th input can be related by

$$\dot{\mathbf{x}}(t) = A\mathbf{x}(t) + \mathbf{b}_l u_l(t) \tag{2.12a}$$

$$y_k(t) = \mathbf{c}_k \mathbf{x}(t), \tag{2.12b}$$

where column vector $\mathbf{b}_l \in \mathbb{R}^n$ is the $l$-th column of matrix $B$ in (2.1), and row vector $\mathbf{c}_k \in \mathbb{R}^n$ is the $k$-th row of matrix $C$. With the assumption on eigenvalue distinctness, let $\mathbf{x} = M\mathbf{z}$, where $\mathbf{z}$ denotes the transformed state vector and matrix $M$ is chosen such that the similarity transformation of $A$ is diagonal, then

$$\dot{\mathbf{z}}(t) = \mathbf{\Lambda}\mathbf{z}(t) + M^{-1}\mathbf{b}_l u_l(t) \tag{2.13a}$$

$$y_k(t) = \mathbf{c}_k M\mathbf{z}(t), \tag{2.13b}$$

where $\mathbf{\Lambda} = \text{diag}(\lambda_1, \lambda_2, \ldots, \lambda_n) = M^{-1}AM$ is a diagonal matrix stacking the eigenvalues of $A$. Denote by column vector $\mathbf{r}_i \in \mathbb{C}^n$ and row vector $\mathbf{l}_i \in \mathbb{C}^n$ the right and left eigenvectors associated with the eigenvalue $\lambda_i$, respectively. Accordingly, the transformation matrices $M$ and $M^{-1}$ can be written as $[\mathbf{r}_1, \mathbf{r}_2, \ldots, \mathbf{r}_n]$ and $[\mathbf{l}_1^\top, \mathbf{l}_2^\top, \ldots, \mathbf{l}_n^\top]^\top$, respectively. The transfer function in the Laplace domain from $l$-th input to $k$-th output is

$$H(s) = \mathbf{c}_k M(sI - \Lambda)^{-1}M^{-1}\mathbf{b}_l = \sum_{i=1}^{n} \frac{\mathbf{c}_k\mathbf{r}_i\mathbf{l}_i\mathbf{b}_l}{s - \lambda_i}. \tag{2.14}$$

For simplicity, assume that the periodic injection $u_l$ only contains one component with frequency $\omega_d$ and amplitude $P_d$, namely, $J = 1$, $\omega_1 = \omega_d$ and $P_1 = P_d$ in (2.2). Furthermore, we assume that before $t = 0^-$ the system is in steady state, viz., $\mathbf{x}(0^-) = \mathbf{0}$. Let sets $\mathcal{N}$ and $\mathcal{M}'$ consist of the indices of real eigenvalues, and the indices of complex eigenvalues with positive imaginary parts, respectively, viz.,

$$\mathcal{N} = \{i \in \mathbb{Z}^+ | \lambda_i \in \mathbb{R}\}; \quad \mathcal{M}' = \{i \in \mathbb{Z}^+ | \, \text{Im}(\lambda_i) > 0\}. \tag{2.15}$$

Then the Laplace transform for PMU measurement $y_k$ is

$$\begin{aligned} Y_k(s) &= \left( \sum_{i=1}^{n} \frac{\mathbf{c}_k \mathbf{r}_i \mathbf{l}_i \mathbf{b}_l}{s - \lambda_i} \right) \frac{P_d \omega_d}{s^2 + \omega_d^2} \\ &= \left[ \sum_{i \in \mathcal{N}} \frac{\mathbf{c}_k \mathbf{r}_i \mathbf{l}_i \mathbf{b}_l}{s - \lambda_i} + \sum_{i \in \mathcal{M}'} \left( \frac{\mathbf{c}_k \mathbf{r}_i \mathbf{l}_i \mathbf{b}_l}{s - \lambda_i} + \frac{\mathbf{c}_k \bar{\mathbf{r}}_i \bar{\mathbf{l}}_i \mathbf{b}_l}{s - \bar{\lambda}_i} \right) \right] \frac{P_d \omega_d}{s^2 + \omega_d^2} \end{aligned} \tag{2.16}$$

where $\bar{(\cdot)}$ denotes complex conjugation.

Next, we analyze the components resulting from the real eigenvalues and the components resulting from the complex eigenvalues, individually. *1) Components Resulting from Real Eigenvalues:* In the Laplace domain, the component resulting from a real eigenvalue $\lambda_i$ is

$$Y_{k,i}^{\mathrm{D}}(s) = \frac{\mathbf{c}_k \mathbf{r}_i \mathbf{l}_i \mathbf{b}_l}{s - \lambda_i} \frac{P_d \omega_d}{s^2 + \omega_d^2}. \tag{2.17}$$

The inverse Laplace transform of $Y_{k,i}^{\mathrm{D}}$(s) is

$$y_{k,i}^{\mathrm{D}}(t) = \frac{\mathbf{c}_k \mathbf{r}_i \mathbf{l}_i \mathbf{b}_l P_d \omega_d}{\lambda_i^2 + \omega_d^2} e^{\lambda_i t} + \frac{\mathbf{c}_k \mathbf{r}_i \mathbf{l}_i \mathbf{b}_l P_d}{\sqrt{\lambda_i^2 + \omega_d^2}} \sin(\omega_d t + \phi_{i,l}) \tag{2.18}$$

where $\phi_{i,l} = \angle \left( \sqrt{\lambda_i^2 + \omega_l^2} + j\lambda_i \right)$, and $\angle(\cdot)$ denotes the angle of a complex number.

*2)Components Resulting from Complex Eigenvalues:* In the Laplace domain, the component resulting from a complex eigenvalue $\lambda_i = -\sigma_i + j\omega_i$ is

$$Y_{k,i}^{\mathrm{B}}(s) = \left( \frac{\mathbf{c}_k \mathbf{r}_i \mathbf{l}_i \mathbf{b}_l}{s - \lambda_i} + \frac{\mathbf{c}_k \bar{\mathbf{r}}_i \bar{\mathbf{l}}_i \mathbf{b}_l}{s - \bar{\lambda}_i} \right) \frac{P_d \omega_d}{s^2 + \omega_d^2}. \tag{2.19}$$

The inverse Laplace transform of $Y^{\mathrm{B}}_{k,i}$(s) is

$$
\begin{aligned}
&y^{\mathrm{B}}_{k,i}(t) = \\
&\frac{2P_d\omega_d|\mathbf{c}_k\mathbf{r}_i\mathbf{l}_i\mathbf{b}_l|}{\sqrt{(\sigma_i^2+\omega_d^2-\omega_i^2)^2+4\omega_i^2\sigma_i^2}}e^{-\sigma_i t}\cos(\omega_i t+\theta_{k,i}-\psi_i)+ \\
&\frac{2P_d|\mathbf{c}_k\mathbf{r}_i\mathbf{l}_i\mathbf{b}_l|\sqrt{\omega_d^2\cos^2\theta_{k,i}+(\sigma_i\cos\theta_{k,i}-\omega_i\sin\theta_{k,i})^2}}{\sqrt{(\sigma_i^2-\omega_d^2+\omega_i^2)^2+4\omega_d^2\sigma_i^2}}\times \\
&\cos(\omega_d t+\phi_i-\alpha_i),
\end{aligned}
\tag{2.20}
$$

where $\theta_{k,i} = \angle(\mathbf{c}_k\mathbf{r}_i\mathbf{l}_i\mathbf{b}_l)$; $\psi_i = \angle(\sigma_i^2+\omega_d^2-\omega_i^2-j2\sigma_i\omega_i)$; $\phi_i = \angle(\sigma_i^2-\omega_d^2+\omega_i^2-j2\omega_i\sigma_i)$, and $\alpha_i = \angle[\omega_d\cos\theta_{k,i}+j(\sigma_i\cos\theta_{k,i}-\omega_i\sin\theta_{k,i})]$.

*2) Resonance Component:* Under the resonance condition defined in (2.3), the injection frequency $\omega_d$ is in the vicinity of one natural modal frequency $\omega_{j^*}$, and the real part of the natural mode is small. We define a new set $\mathcal{M}\subset\mathcal{M}'$ as $\mathcal{M} = \{i\in\mathbb{Z}^+|\,\mathrm{Im}(\lambda_i)>0, |\omega_i-\omega_{j^*}|<\kappa_1, |\mathrm{Re}(\lambda_i)|<\kappa_2\}$, where $\kappa_1$ and $\kappa_2$ are small and nonnegative real numbers. For $i\in\mathcal{M}$, the eigenvalue $\lambda_i = -\sigma_i+j\omega_i$ satisfies $\omega_i\approx\omega_d$ and $\sigma_i\approx 0$. Then $\psi_i\approx-\frac{\pi}{2}$, $\phi_i\approx-\frac{\pi}{2}$, and $\alpha_i\approx-\theta_{k,i}$. Therefore, equation (2.20) can be simplified as

$$
y^{\mathrm{B}}_{k,i}(t)\approx y^{\mathrm{R}}_{k,i}(t) = \frac{P_d|\mathbf{c}_k\mathbf{r}_i\mathbf{l}_i\mathbf{b}_l|}{\sigma_i}(1-e^{-\sigma_i t})\sin(\omega_d t+\theta_{k,i}) \tag{2.21}
$$

for $i\in\mathcal{M}$. In this chapter, $y^{\mathrm{R}}_{k,i}$ in (2.21) is termed the *resonance component* in the $k$-th measurement.

In summary, a PMU measurement $y_k(t)$ in a power system (2.1) under resonance conditions can be decomposed into three classes of components, i.e.,

$$
y_k(t) = \sum_{i\in\mathcal{N}} y^{\mathrm{D}}_{k,i}(t) + \sum_{i\notin\mathcal{M}\cup\mathcal{N}} y^{\mathrm{B}}_{k,i}(t) + \sum_{i\in\mathcal{M}} y^{\mathrm{R}}_{k,i}(t). \tag{2.22}
$$

### 2.4.2 Observations on the Resonance Component and the Resonance-free Component

*1) Severe Oscillations Arising from Resonance Component:* Figure 2.3(a) visualizes the resonance component of a PMU measurement (at Bus $40$[2]) in the IEEE 68-bus benchmark system. As can be observed from Figure 2.3(a), the upper envelop of the oscillation increases concavely at the initial stage before reaching a steady-stage value (about $0.1$ in this case). The closed-form approximation for such a steady-state value is $P_d|\mathbf{c}_k\mathbf{r}_i\mathbf{l}_i\mathbf{b}_l|/\sigma_i$. For a small positive $\sigma_{j^*}$ associated with eigenvalue $\lambda_{j^*}$, the steady-state amplitude of the resonance component may be the dominant one. If a PMU measurement far away from the source measurements is tightly coupled with the eigenvalue $\lambda_{j^*}$, it may manifest the most severe oscillation, thereby confusing system operators with regard to FO source localization. Therefore, the presence of resonance components may cause the counter-intuitive cases defined by (2.7), (2.8).

*2) Location Information on FO Source from the Resonance-free Component:* As the resonance components of the set of all PMU measurements mislead system operators with respect to FO localization, we proceed by excluding the resonance component from (2.22), and checking whether if the remaining components exhibit any spatial information concerning the FO source. The superposition of the remaining components is termed as *resonance-free*. Specifically, for a power system with known physical model (2.1), the resonance-free component $y_k^{\mathrm{F}}$ in the $k$-th PMU measurement time series can be obtained by:

$$y_k^{\mathrm{F}}(t) = \sum_{i\in\mathcal{N}} y_{k,i}^{\mathrm{D}}(t) + \sum_{i\notin\mathcal{M}\cup\mathcal{N}} y_{k,i}^{\mathrm{B}}(t). \tag{2.23}$$

The visualization of the resonance-free component for all PMU measurements in the IEEE

[2]The measurements at Bus $40$ exhibit the largest oscillations but they are non-source measurements.

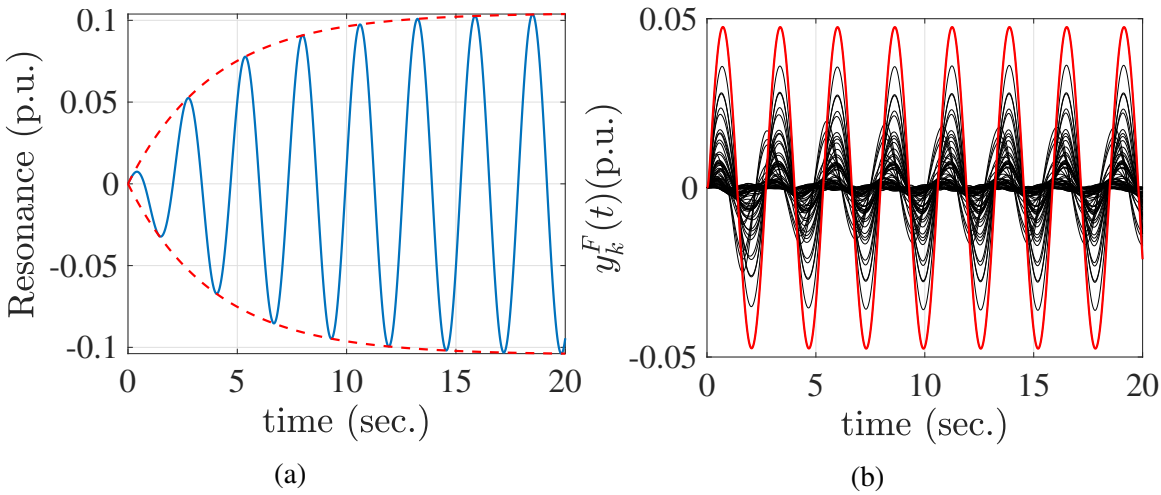



Figure 2.3: (a) Visualization of the resonance component of bus voltage magnitudes in the IEEE 68-bus benchmark system based on equation (2.21): the resonance components of the voltage magnitude measurement at Bus 40 (blue curve) and its envelopes (red-dash curves). (b) Resonance-free components of the source voltage magnitude measurement (red) and the non-source voltage magnitude measurement (black) in the IEEE 68-bus benchmark system.

68-bus system is shown in Figure 2.3(b) under a certain FO scenario[3]. Under the same FO scenario, Figure 2.1 visualizes all PMU measurements $y_k(t)$ in (2.22). In Figure 2.3(b), while the complete measurements $y_k(t)$ are counter-intuitive, the resonance-free components $y_k^{\mathrm{F}}(t)$ convey the location information on the FO source–the resonance-free component of the source measurement exhibits the largest oscillation. Such localized response of resonance-free components might be an extension of the no-gain property of an electric network rigorously justified in [30, 31]. Future work will examine what kinds of power systems possess localization property of resonance-free components in a theoretically rigorous fashion.

[3]A sinusoidal waveform with amplitude $0.05$ per unit (p.u.) and frequency $0.38$ Hz is injected into the IEEE 68-bus system via the voltage setpoint of generator 13. The information on the test system is elaborated in Section 2.5.

### 2.4.3 Low-rank Nature of Resonance Component Matrix

The physical interpretation of the efficacy of the RPCA-based algorithm is illustrated by examining the rank of the matrix containing all resonance components for all measurements, which we call the *resonance component matrix*, formally defined next. Similar to (2.4), the resonance component $y_k^{\mathrm{R}}(t)$ in the $k$-th measurement can be discretized into a row vector $\mathbf{y}_{k,t}^{\mathrm{R}}$:

$$\mathbf{y}_{k,t}^{\mathrm{R}} := \left[ y_k^{\mathrm{R}}(0), \quad y_k^{\mathrm{R}}(1/f_{\mathrm{s}}), \quad \dots \quad y_k^{\mathrm{R}}(\lfloor t f_{\mathrm{s}} \rfloor / f_{\mathrm{s}}) \right]. \tag{2.24}$$

Then, the resonance component matrix $Y_t^{\mathrm{R}}$ can be defined as a row concatenation as follows:

$$Y_t^{\mathrm{R}} := \left[ \left(\mathbf{y}_{1,t}^{\mathrm{R}}\right)^\top, \quad \left(\mathbf{y}_{2,t}^{\mathrm{R}}\right)^\top, \quad \dots \quad \left(\mathbf{y}_{m,t}^{\mathrm{R}}\right)^\top \right]^\top. \tag{2.25}$$

**Theorem 1.** *For the linear time-invariant dynamical system* (2.1)*, the rank of the resonance component matrix $Y_t^R$ defined in* (2.25) *is at most* 2*.*

*Proof.* Based on (2.21), define $E_k := P_d |\mathbf{c}_k \mathbf{r}_i \mathbf{l}_i \mathbf{b}_l| / \sigma_i$. Then

$$\begin{aligned} y_{k,i}^{\mathrm{R}}(t) =& (1 - e^{-\sigma_i t}) \sin(\omega_d t) E_k \cos(\theta_{k,i}) + \\ & (1 - e^{-\sigma_i t}) \cos(\omega_d t) E_k \sin(\theta_{k,i}). \end{aligned}$$

We further define functions $f_1(t)$, $f_2(t)$ and variables $g_1(k)$, $g_2(k)$ as follows: $f_1(t) := (1 - e^{-\sigma_i t}) \sin(\omega_d t)$; $f_2(t) := (1 - e^{-\sigma_i t}) \cos(\omega_d t)$; $g_1(k) := E_k \cos(\theta_{k,i})$; and $g_2(k) := E_k \sin(\theta_{k,i})$. Then, $y_{k,i}^{\mathrm{R}}(t)$ can be represented by $y_{k,i}^{\mathrm{R}}(t) = f_1(t) g_1(k) + f_2(t) g_2(k)$.

The resonance component matrix $Y_t^{\mathrm{R}}$ up to time $t$ can be factored as follows:

$$Y_t^{\mathrm{R}} = \begin{bmatrix} g_1(1) & g_2(1) \\ g_1(2) & g_2(2) \\ \vdots & \vdots \\ g_1(m) & g_2(m) \end{bmatrix} \begin{bmatrix} f_1(0) & f_1(\frac{1}{f_{\mathrm{s}}}) & \dots & f_1(\frac{\lfloor tf_{\mathrm{s}} \rfloor}{f_{\mathrm{s}}}) \\ f_2(0) & f_2(\frac{1}{f_{\mathrm{s}}}) & \dots & f_2(\frac{\lfloor tf_{\mathrm{s}} \rfloor}{f_{\mathrm{s}}}) \end{bmatrix}. \tag{2.26}$$

Denote by vectors $\mathbf{g}_1$ and $\mathbf{g}_2$ the first and second columns of the first matrix in the right hand side (RHS) of (2.26), respectively; and by vectors $\mathbf{f}_1$ and $\mathbf{f}_2$ the first and second rows of the second matrix in the RHS of (2.26). Then (2.26) turns to be

$$Y_t^{\mathrm{R}} = \begin{bmatrix} \mathbf{g}_1 & \mathbf{g}_2 \end{bmatrix} \begin{bmatrix} \mathbf{f}_1 \\ \mathbf{f}_2 \end{bmatrix}. \tag{2.27}$$

Given (2.27), it is clear that the rank of the resonance component matrix $Y_t^{\mathrm{R}}$ is at most 2. □

Typically, for a resonance component matrix $Y_t^{\mathrm{R}}$ with $m$ rows and $\lfloor tf_{\mathrm{s}} \rfloor$ columns, owing to $\min(m, \lfloor tf_{\mathrm{s}} \rfloor) \gg 2$, the resonance component matrix $Y_t^{\mathrm{R}}$ is a low-rank matrix, which is assumed to be integrated by the low-rank component $L_t$ in equation (2.9). As discussed in Section 2.4.2, the source measurement can be tracked by finding the maximal absolute entry of the resonance-free matrix $(Y_t - Y_t^{\mathrm{R}})$. According to (2.10), the PMU measurement containing the largest absolute entry in the sparse component $S_t$ is considered as the source measurement. Then, it is reasonable to conjecture that the sparse component $S_t$ in (2.9) captures the part of the resonance-free matrix that preserves the location information of FO source. Thereby, a theoretical connection between the proposed data-driven method in Algorithm 1 and the physical model of power systems described in equation (2.1) can be established. Although forced oscillation phenomena have been extensively studied in physics [32], the low-rank property, to the best of our knowledge, is first inves-

tigated in this chapter.

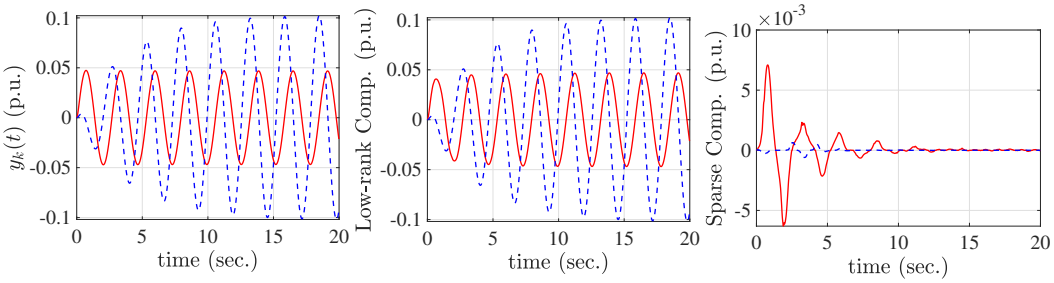



Figure 2.4: Visualization of voltage magnitudes (a), components in low-rank matrix $L_t$ (b) and components in sparse matrix $S_t$ (c) at Bus 65 (red) and Bus 40 (blue dash): Bus 65 is the bus closest to the source, while the most severe oscillation appear at Bus 40.

Through the FO case shown in Figure 2.1, we next examine the entries corresponding to the largest amplitude channel (Bus $40$) and the source measurement (Bus $65$) in the measurement matrix $Y_t$, the low-rank matrix $L_t$, and the sparse matrix $S_t$. In Figure 2.4(a), the blue-dash curve and the red curve respectively present voltage magnitudes at the largest amplitude channel (Bus $40$) and the source measurement (Bus $65$). Figure 2.4(b) shows the components captured by the low-rank matrix $L_t$ corresponding to measurements at Bus $40$ (blue-dash) and Bus $65$ (red). Figure 2.4(c) shows the components captured by the sparse matrix $S_t$ corresponding to measurements at Bus $40$ (blue-dash) and Bus $65$ (red). As can be observed in Figure 2.4(a), the measurement at Bus $40$ (blue-dash curve) comprises mainly the resonance component. As we have established in Theorem 1, the resonance component matrix is by nature low-rank. Therefore, the measurement at Bus $40$ is better captured by the low-rank matrix than the measurement at Bus $65$, as is shown in Figure 2.4(b). What is left in the sparse matrix pinpoints the forced oscillation source. Besides, in Figure 2.4, part of resonance-free component is also captured by the low-rank

matrix, which cannot be explained by Theorem 1. Note that Theorem 1 offers one possible interpretation of the effectiveness of the proposed algorithm, but it is not claimed to be a fully rigorous interpretation of why the algorithm works, however as is verified by the above figure it indeed sheds a lot of light in its interpretation. As this chapter focuses on the development of one possible data-driven localization algorithm, future work will investigate a broader category of possible algorithms and their theoretical underpinnings.

A natural question is if the robust-PCA procedure can pinpoint the source of other types of oscillations, such as natural oscillations. The difficulty to answering this question is that "source of natural oscillation" is not well defined. In a forced oscillation event, the FO source is defined as the power system component with external periodic perturbations, and one obvious solution to suppressing the oscillation is to disconnect the source from the grid. In a natural oscillation event, one may suppress it by tuning control apparatus of a set of generators or by decreasing the load level. In such a case, should the source be deemed the tuned generators or the decreased load? In brief, we believe it is challenging to consent on a definition of the "source" of natural oscillations. Due to the ambiguity in the definition of natural oscillation sources, this chapter only focuses on the localization of forced oscillations.

## 2.5 Case Study

In this section, we validate the effectiveness of Algorithm 1 using data from IEEE 68-bus benchmark system and WECC 179-bus system. We first describe the key information on the test systems, the procedure for obtaining test data, the parameter settings of the proposed algorithm, and the algorithm performance over the obtained test data. Then the impact of different factors on the performance of the localization algorithm is investigated. Finally, we compare the proposed algorithm with the energy-based method reported in [15]. As will be seen, the proposed method can pinpoint the FO sources with high accuracy

*without any information on system models and grid topology*, even when resonance exists.

### 2.5.1 Performance Evaluation of the Localization Algorithms in Benchmark Systems

*1) IEEE 68-bus Power System Test Case:* The system parameters of the IEEE 68-bus power system are reported in the Power System Toolbox (PST) [2] and its topology is shown in Figure 2.5. Let $\mathcal{V} = \{1, 2, \ldots, 16\}$ consist of the indices of all $16$ generators in the 68-bus system. Based on the original parameters, the following modifications are made: 1) the power system stabilizers (PSS) at all generators, except the one at Generator $9$, are removed, in order to create more poorly-damped oscillatory modes; 2) for the PSS at Generator $9$, the product of PSS gain and washout time constant is changed to $250$. Based on the modified system, the linearized model of the power system (2.1) can be obtained using the command "`svm_mgen`" in PST. There are $25$ oscillatory modes whose frequencies range from $0.1$ Hz to $2$ Hz, which are shown in Figure 2.8(a). Denote by $\mathcal{W} = \{\omega_1, \omega_2, \ldots, \omega_{25}\}$ the set consisting all $25$ modal frequencies of interest. The periodic perturbation $u_l$ in (2.2) is introduced through the voltage setpoints of generators. The analytical expression of $u_l$ is $0.05\sin(\omega_d t)$, where $\omega_d \in \mathcal{W}$.

We create FOs in the 68-bus system according to set $\mathcal{V} \times \mathcal{W}$, where $\times$ is the Cartesian product. For element $(i, \omega_j) \in \mathcal{V} \times \mathcal{W}$, the periodic perturbation $u_l(t)$ with frequency $\omega_j$ is injected into the grid through the voltage setpoint of generator $i$ at time $t = 0$. Then, the system response is obtained by conducting a $40$-second simulation. The bus voltage magnitude deviations constitute the output/measurement vector $\mathbf{y}(t)$ in (2.1). Finally, the measurement matrix is constructed based on (2.4), where the sampling rate $f_{\mathrm{s}}$ is $60$ Hz. By repeating the above procedure for each element in set $\mathcal{V} \times \mathcal{W}$, we obtain $400$ measurement matrices ($|\mathcal{V} \times \mathcal{W}|$). Among the $400$ measurement matrices, $44$ measurement matrices satisfy the resonance criteria (2.7), (2.8) with $N_0 = 0$ and they are marked as the counter-

intuitive cases which are used for testing the performance of the proposed method. Some typical waveforms in the $44$ test cases are shown in [1].

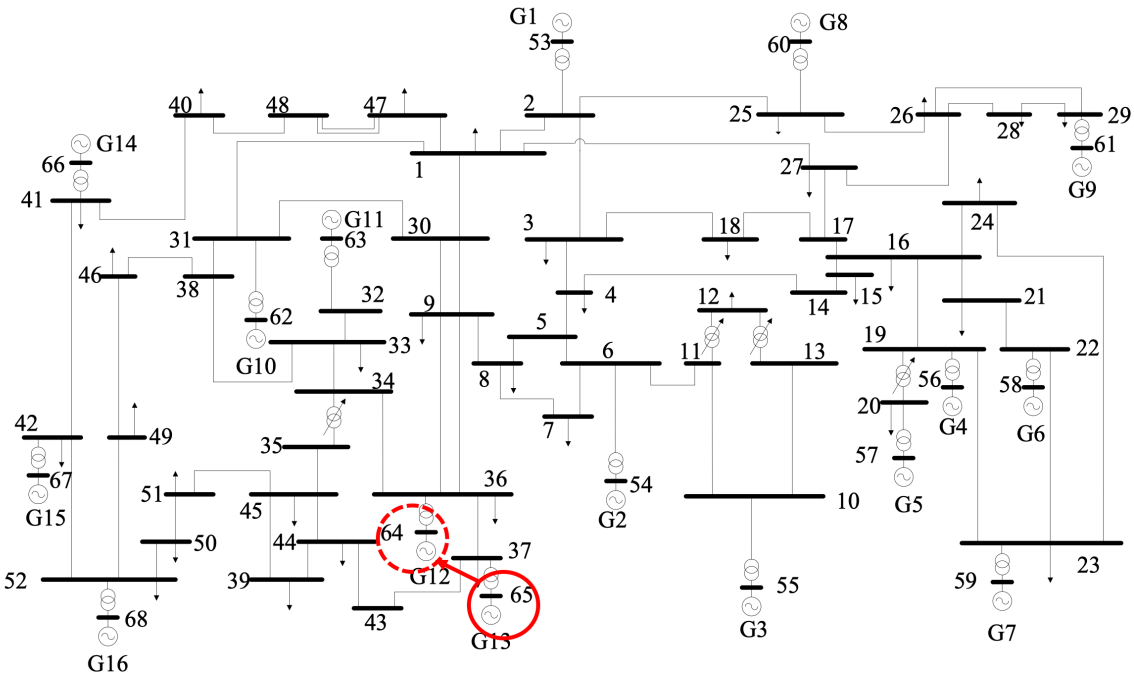



Figure 2.5: The IEEE 68-bus power system [1]: the generator in the solid circle is the actual source generator; the generator in the dash circle is the identified source.

The tunable parameters $T_0$ and $\xi$ in Algorithm 1 are set to $10$ and $0.0408$, respectively. Measurements of voltage magnitude, phase angle and frequency are used for constituting the measurement matrix. Then, we apply Algorithm 1 to the $44$ counter-intuitive cases. Algorithm 1 pinpoints the source measurements in $43$ counter-intuitive cases and, therefore, achieves $97.73\%$ accuracy without any knowledge of system models and grid topology.

Next, we scrutinize the geographic proximity between the identified and actual source measurements in the single failed case. The algorithm outputs that the source measurement is located at Bus $64$ (highlighted with a solid circle in Figure 2.5), when a periodic

perturbation with frequency $1.3423$ Hz is injected into the system through the generator directly connecting to Bus $65$ (highlighted with a dash circle in Figure 2.5). As can be seen in Figure 2.5, the identified and actual source measurements are geographically close. Therefore, even in the failed cases, the proposed method can effectively narrow the search space.

*2) WECC 179-bus System Test Case:* This subsection leverages the open-source forced oscillation dataset [3] to validate the performance of the RPCA-based method. The offered dataset is generated via the WECC 179-bus power system [3] whose topology is shown in Figure 2.7(a). The procedure for synthesizing the data is reported in [3]. The available dataset includes $15$ forced oscillation cases with single oscillation source, which are used to test the proposed method. The visualization for Case `F-3` is shown in Figure 2.6. In each forced oscillation case, the measurements of voltage magnitude, voltage angle and frequency at all generation buses are used to construct the measurement matrix $Y_t$ in (2.4), from the $10$-second oscillatory data, i.e., $T_0 = 10$. Then, the $15$ measurement matrices are taken as the input for Algorithm 1, where the tunable parameter $\xi$ is set to $0.0577$.

For the WECC 179-bus system, the proposed method achieved $93.33\%$ accuracy. Next, we present how geographically close the identified FO sources are to the ground truth in the seemingly incorrect case. In Case `FM-6-2`, a periodic rectangular perturbation is injected into the grid through the governor of the generator at Bus $79$ which is highlighted with a red solid circles in Figure 2.7(b). The source measurement identified by the proposed method is at Bus $35$ which is highlighted by a red dash circle. As can be seen in Figure 2.7(b), the identified FO source is geographically close to the actual source. Again, even the seemingly wrong result can help system operators substantially narrow down the search space for FO sources.

*3) ERCOT Forced Oscillation Event:* We leverage the field measurements from a collaborative project with Electric Reliability Council of Texas (ERCOT), in order to test the

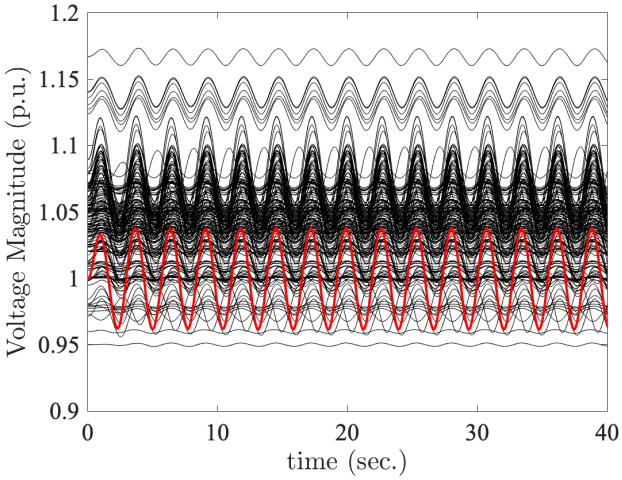
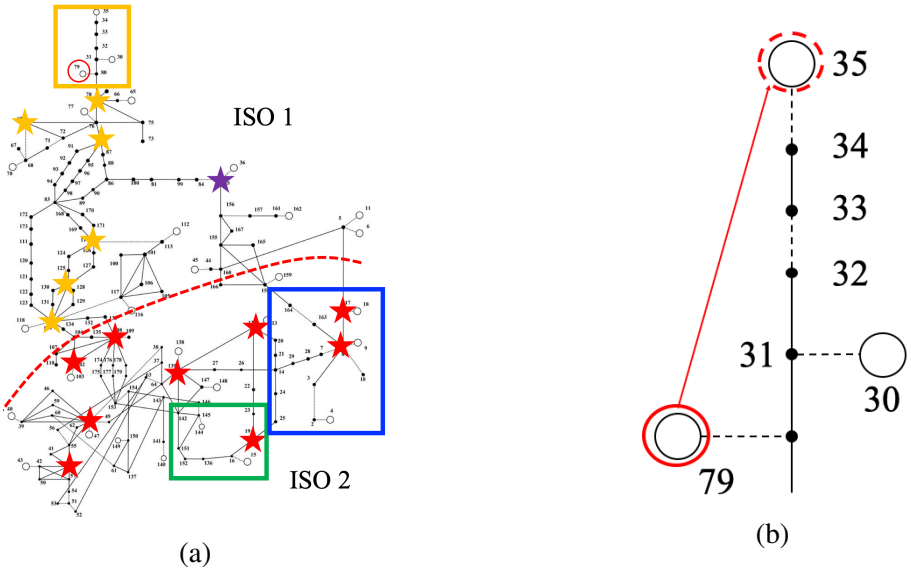



Figure 2.6: Voltage magnitude visualization in Case `F-3`: the voltage magnitude of the bus connected with the forced oscillation source (red); the voltage magnitudes of the remaining buses (black).

localization algorithm in a realistic setting. Figure 2.9 shows the FOs observed by ERCOT. The FOs manifested themselves in seven PMU measurements on voltage magnitudes. For information privacy, the names of the PMU locations are replaced by indices $1, 2, \ldots, 7$, and the FO starting point is set to $0$ seconds. In Figure 2.9, it can be observed that the PMU measurements contain high frequency components resulting from measurement noise and load fluctuation. We apply a band-pass filter from $0.1$ Hz to $1$ Hz to process the raw PMU measurements. Subsequently, we use a $10$-second time window of the filtered data for forming the measurement matrix. Finally, the proposed algorithm indicates that PMU $4$ is the one near the FO source. The localization result was reported to ERCOT, and ERCOT confirmed the correctness of the result. It is worth noting that no topology information was provided to our research team. Therefore, localization algorithms based on system topology, such as the Dissipating Energy Flow approach, are not applicable in this study.




(a) (b)

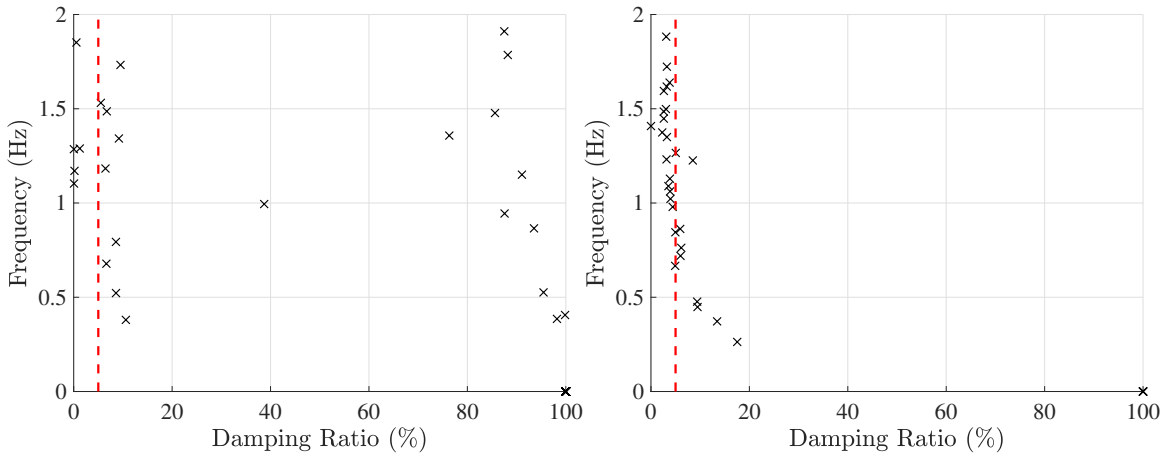
Figure 2.7: WECC 179-bus power system [3]: (a) complete topology; (b) zoomed-in version of the area in the yellow box in the left figure.

### 2.5.2 Algorithm Robustness

The subsection focuses on testing the robustness of the proposed algorithm under different factors which include measurement types, noise, and partial coverage of PMUs. The impact of each factor on the algorithm performance will be demonstrated as follows.

*1) Impact of Measurement Types on Algorithm Performance:* Under all possible combinations of nodal measurements (voltage magnitude $|V|$, voltage angle $\angle V$ and frequency $f$), the localization accuracies of the proposed algorithm in the two benchmark systems are reported in Table 2.1. As can be observed in Table 2.1, the maximal accuracy is achieved when voltage magnitudes, voltage angles and frequencies are used to constitute the measurement matrix in (2.4).

*2) Impact of Noise on Algorithm Performance:* Table 2.2 records the localization accuracy under different levels of noise. In Table 2.2, the signal-to-noise ratio (SNR) is defined




(a) (b)

Figure 2.8: Eigenvalues of the IEEE 68-bus system (a) and the WECC 179-bus system in Cases `F-1` and `FM-1` (b): the eigenvalues whose damping ratio less than $5\%$ are in the left-hand side of the red-dash line.

Table 2.1: Impact of Measurement Types on Localization Performance

| **Types** | $\|V\|$ | $\angle V$ | $\|V\|, \angle V$ | $f$ |
|---|---|---|---|---|
| 68-bus System | $84.09\%$ | $50.00\%$ | $84.09\%$ | $52.27\%$ |
| 179-bus System | $86.67\%$ | $33.33\%$ | $73.33\%$ | $20.00\%$ |
| **Types** | $\|V\|, f$ | $\angle V, f$ | $\|V\|, \angle V, f$ | N/A |
| 68-bus System | $93.18\%$ | $59.09\%$ | $\mathbf{97.73}\%$ | N/A |
| 179-bus System | $80.00\%$ | $46.67\%$ | $\mathbf{93.33}\%$ | N/A |

as follows:

$$SNR = 10\log(W_{\text{s}}/W_{\text{n}}) \quad \text{(dB)}$$

where $W_{\text{s}}$ is the sum of squared measurement *deviations* over a period (10 seconds in this chapter); and $W_{\text{n}}$ is the sum of squared magnitudes of the corresponding noise over the same period. The noise superimposed upon each measurement has a Gaussian distribution with zero mean and variance $\sigma_{\text{n}}$. At each experiment for each measurement, the variance $\sigma_{\text{n}}$ is chosen such that the corresponding SNR is achieved. From Table 2.2, we conclude

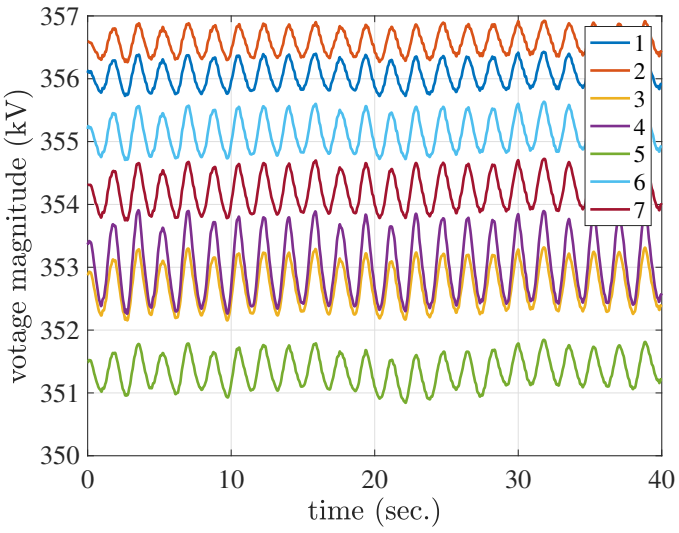



Figure 2.9: Voltage Magnitudes during the ERCOT forced oscillation event.

Table 2.2: Impact of Noise Level on Localization Performance

| SNR | 90dB | 70dB | 50dB | 30dB | 10dB |
|---|---|---|---|---|---|
| 68-Bus | 97.73% | 97.73% | 97.73% | 97.73% | 56.82% |
| 179-Bus | 93.33% | 93.33% | 93.33% | 93.33% | 73.33% |

the proposed algorithm performs well under the cases with SNR less than 30 dB.

*3) Impact of Partial Coverage of Synchrophasors on Algorithm Performance* In practice, not all buses are equipped with PMUs. Besides, available PMUs may be installed on buses near oscillation sources, instead of buses on which oscillation sources are directly connected. A test case is designed for testing the performance of the proposed algorithm in the scenario described above. In this test case, the locations of all available PMUs are marked with stars in Figure 2.7(a). The test result is listed in Table 2.3. As illustrated in Table 2.3, the proposed method can effectively identify the available PMUs that are close to oscillation sources, even though no PMU is installed on generation buses.

Independent System Operators (ISOs) may also need to know whether FO sources

Table 2.3: Impact of Partial Coverage of Synchrophasor on Algorithm Performance

| **Case Name** | F-1 | FM-1 | F-2 | F-3 | FM-3 | F-4-1 | F-4-2 | F-4-3 |
|---|---|---|---|---|---|---|---|---|
| **Identified Source** | 8 | 8 | 78 | 69 | 69 | 69 | 78 | 78 |
| **Nearest PMU** | 8 | 8 | 78/69 | 78/69 | 78/69 | 78/69 | 78/69 | 78/69 |
| **Case Name** | F-5-1 | F-5-2 | F-5-3 | F-6-1 | F-6-2 | F-6-3 | FM-6-2 | N/A |
| **Identified Source** | 78 | 78 | 78 | 78 | 78 | 78 | 78 | N/A |
| **Nearest PMU** | 78/69 | 78/69 | 78/69 | 78/69 | 78/69 | 78/69 | 78/69 | N/A |

are within their control areas. However, ISOs might not be able to access PMUs near FO sources, limiting the usefulness of the proposed algorithm. For example, assume that there are two ISOs, i.e., ISO $1$ and ISO $2$, in Figure 2.7(a), where the red dash line is the boundary between the control areas of the two ISOs. It is possible that FO sources are at the ISO $1$ control area, whereas ISO $2$ only can access the PMUs at the buses marked with red stars. In order to apply the RPCA-based method, ISO $2$ needs to access one PMU in the area controlled by ISO $1$, say, the PMU marked with a purple star in Figure 2.7(a). In the $\texttt{F}-2$ dataset, the FO source is located at Bus $79$ which is marked with a red circle in Figure 2.7(a). With the data collected from PMUs marked with red and purple stars, the proposed algorithm outputs the bus marked with a purple star, indicating that the FO source is outside the control area of ISO $2$.

*4) Impact of External Excitation on Localization Performance* The external excitation is assumed to result mainly from load fluctuation. In order to introduce load fluctuation, load dynamics are included in the $68$-bus benchmark system, and $33$ real power setpoints along with $33$ reactive power setpoints on load are considered as the augmented inputs. The above modification on the $68$-bus system can be achieved by enabling load modulation in the Power System Toolbox (PST) [2]. Following the procedure described in Section V-A-1, $43$ counter-intuitive cases are obtained. For the $j$-th case of the 43 counter-intuitive cases, we have a pair of numbers $(i'_j, \omega'_j)$, where $\omega'_j$ is the frequency of a periodic

perturbation and $i'_j$ is the source generator index. Let set $\mathcal{P}$ consist of such pairs, i.e., $\mathcal{P} = \{(i'_1, \omega'_1), (i'_2, \omega'_2), \ldots, (i'_j, \omega'_j), \ldots, (i'_{43}, \omega'_{43})\}$.

Note that the number of state variables in the $68$-bus system with load dynamics is $268$, whereas the number of state variables in the $68$-bus system used in Section V-A is $202$. Effectively, the $68$-bus system in this subsection is a different system from the $68$-bus system used in Section V-A, from the perspective of control theory, as the numbers of their state variables are distinct. Therefore, it is not surprising that the number of counter-intuitive cases in this subsection is different from that in Section V-A.

The $66$ augmented setpoints fluctuate around their nominal values, which can be considered to be external excitations. Denote by $\Delta \mathbf{u}_{\text{Ld}}(t) \in \mathbb{R}^{66}$ the load setpoint deviations from their nominal values at time $t$. Assume that vector $\Delta \mathbf{u}_{\text{Ld}}$ has a Gaussian distribution with zero mean and covariance matrix $\sigma_{\text{ext}} I_{66}$, i.e., $\Delta \mathbf{u}_{\text{Ld}}(t) \sim \mathcal{N}(0, \sigma_{\text{ext}} I_{66})$, where $\sigma_{\text{ext}}$ is a scalar, and $I_{66}$ is a $66$ by $66$ identity matrix. Due to the excitation $\Delta \mathbf{u}_{\text{Ld}}$, the frequency fluctuates under normal operating condition as observed in Figure 2.10(a). Figure 2.10(b) shows how the system frequency range varies as scalar $\sigma_{\text{ext}}$ changes. In Figure 2.10(b), each vertical line segment corresponds to the frequency range under a load fluctuation with parameter $\sigma_{\text{ext}}$: the upper terminal is the highest system frequency for each given $\sigma_{\text{ext}}$; and the lower terminal is the lowest system frequency with corresponding $\sigma_{\text{ext}}$. One observation from Figure 2.10(b) is that as scalar $\sigma_{\text{ext}}$ increases, it is more likely that the system frequencies lie in a wider range. The normal range of frequency in power systems is from $59.96$ Hz to $60.04$ Hz [33, 34]. As shown in Figure 2.10(b), the range of system frequencies are out of the normal range under the excitation with $\sigma_{\text{ext}} = 0.2$. We use the random excitations $\Delta \mathbf{u}_{\text{Ld}}(t)$ with $\sigma_{\text{ext}} = 0.15$ to mimic real-world load fluctuation.

The random excitations $\Delta \mathbf{u}_{\text{Ld}}$ with $\sigma_{\text{ext}} = 0.15$ and set $\mathcal{P}$ are leveraged to obtain $43$ test cases. The data acquisition procedure is described in what follows. For element $(i'_j, \omega'_j) \in \mathcal{P}$, the periodic perturbation $u_l(t)$ with frequency $\omega'_j$ is injected into the system

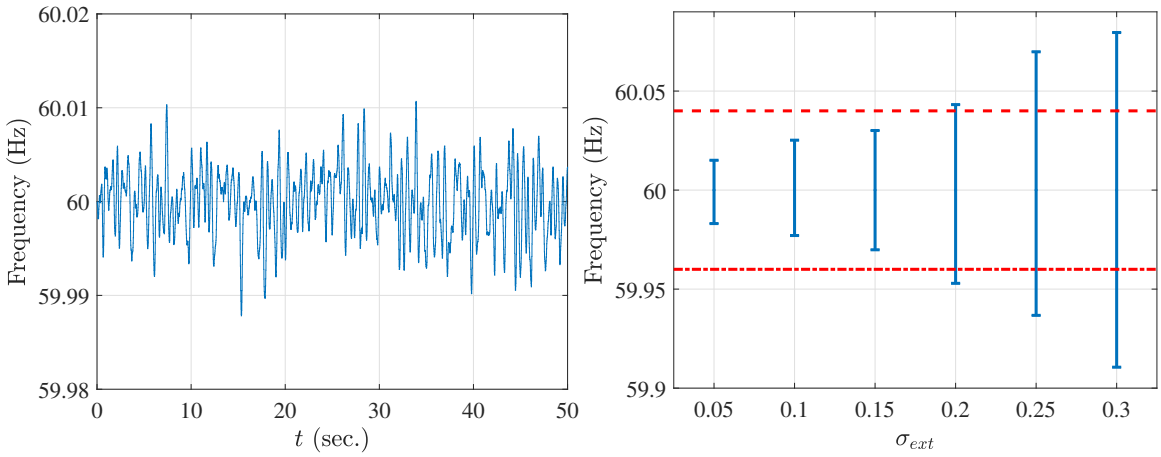



Figure 2.10: (a) Frequency at Bus 1 under normal operation condition with load fluctuation; (b) Ranges of system frequency (vertical blue-solid line segments) due to different levels of load fluctuation: the normal frequency range (59.96-60.04 Hz) is represented by two horizontal red-dash lines.

via the voltage setpoint of generator $i'_j$ at $t = 0$. At each experiment, the 68-bus system is excited by one realization of $\Delta \mathbf{u}_{\text{Ld}}$. Then, a 40-second simulation is conducted in order to obtain the system response. By repeating the above procedure for all elements, 43 test cases with load fluctuation are obtained. For these test cases, a 2-Hz low-pass filter is applied to process the measurements. The proposed algorithm achieves $90.70\%$ localization accuracy.

*5) Impact of Time-window Length on Localization Performance:* In this section, we investigate the impact of the window width $T_0$ on the algorithm's performance. Fig. 2.11 summarizes the localization accuracy with different time-window widths $T_0$ in both the 68-bus and 179-bus systems. In Fig. 2.11, we observe a trade-off between the time required for decision making and the localization accuracy for the 68-bus system (the blue-dash line) with the given range of $T_0$: $100\%$ accuracy can be achieved with $T_0 = 12$ (or 13) seconds; the price we pay for the high localization accuracy is a wider time window, i.e.,

more decision-making time.

In practice, the optimal window width $T_0^*$ can be obtained by off-line studies on physical model-based simulations or historical FO events. Assume that we have $N_1$ options for the window width $T_0$, represented by $\mathcal{T}_0 := \{T_{01}, T_{02}, \ldots, T_{0N_1}\}$. For each window width option, say, $T_{0i}$, we run the localization algorithm on all available FO events and compute the localization accuracy $\eta_i$. The optimal window width $T_0^*$ is the $i^*$-th element in the set $\mathcal{T}_0$, which maximizes $\eta_i$ for $i = 1, 2, \ldots, N_1$. Such an optimal window width $T_0^*$ is applied in the localization algorithm 1 during real-time operation.

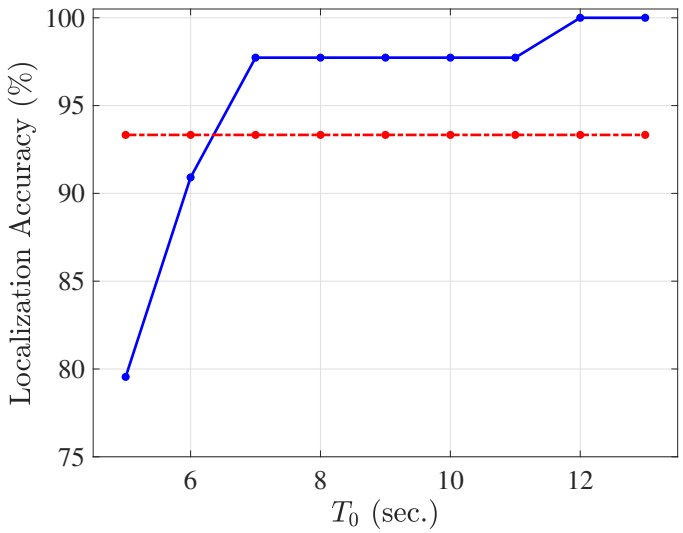



Figure 2.11: Impact of $T_0$ on Localization Performance: the localization accuracy for the 68-bus system (blue-solid line) and the 179-bus system (red-dash line).

### 2.5.3 Comparison with Energy-based Localization Method

This subsection aims to compare the proposed localization approach with the Dissipating Energy Flow (DEF) approach [15]. We use the `FM-1` dataset (Bus 4 is the source measurement) [3] for the purpose of comparing DEF method with the proposed algorithm.

PMUs are assumed to be installed at all generator buses except ones at Buses $4$ and $15$. Besides, Buses 7, $15$ and $19$ are also assumed to have PMUs. *Without any information on grid topology*, the RPCA-based method suggests the source measurement is at Bus 7 which is in the vicinity of the actual source. However, topology errors may cause DEF-based method to incur both false negative and false positive errors, as will be shown in the following two scenarios.

*1) Scenarios 1:* The zoomed-in version of the area within the blue box in Figure 2.7(a) is shown in Figure 2.12, where the left and right figures are the actual system topology and the topology reported to a control center, respectively. All available PMUs are marked with yellow stars in Figure 2.12. Based on these available PMUs, the relative magnitudes and directions of dissipating energy flows are computed according to the `FM-1` dataset and the method reported in [15]. With the true topology, the FO source cannot be determined, as the energy flow direction along Branch $8$-$3$ cannot be inferred based on the available PMUs. However, with the topology error shown in Figure 2.12(b), i.e., it is mistakenly reported that Bus 29 (Bus 17) is connected to Bus 3 (Bus 9), it can be inferred that the energy flow with relative magnitude of $0.4874$ is injected into the Bus $4$, indicating that Bus $4$ is *not* the source measurement. Such a conclusion contradicts the ground truth. Therefore, with such a topology error, the dissipating energy flow method leads to a false negative error.

*2) Scenarios 2:* Similar to Scenario 1, topology errors exist within the area highlighted by a green box in Figure 2.7(a), whose zoomed-in version is shown in Figure 2.13. As shown in Figure 2.13(a), it can be inferred that an energy flow with relative magnitude of $0.171$ injects into Bus $15$ with the information of actual topology and available PMUs, indicating Bus $15$ is not a source. However, with the reported system topology, the generator at Bus $15$ injects to the rest of grid an energy flow with magnitude of $0.0576$, suggesting the source measurement is at Bus $15$. Again, such a conclusion contradicts with the ground

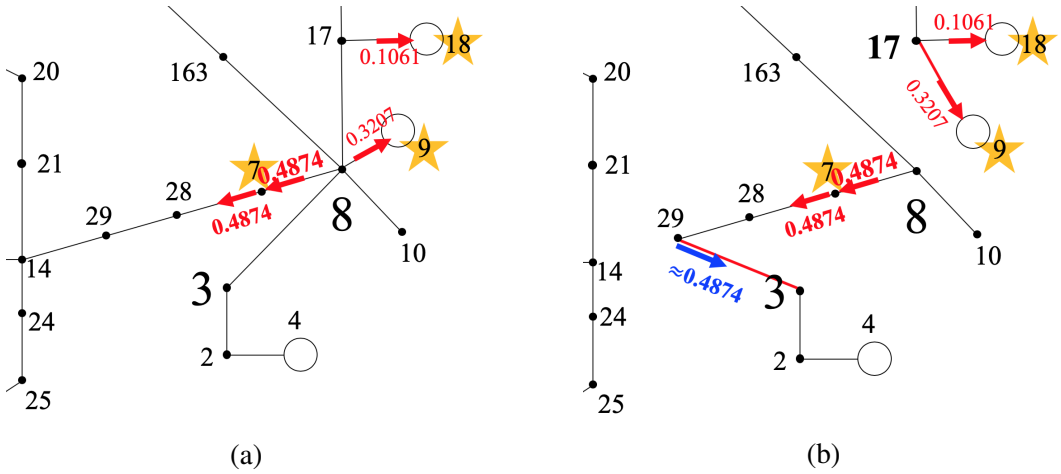



Figure 2.12: Zoomed-in version of the area in the blue box at Figure 2.7 (a): actual topology (left); topology reported in a control center (right). Relative magnitudes and direction of energy flows are labeled with red numbers and arrows, respectively.

truth and, hence, incurs a false positive error.

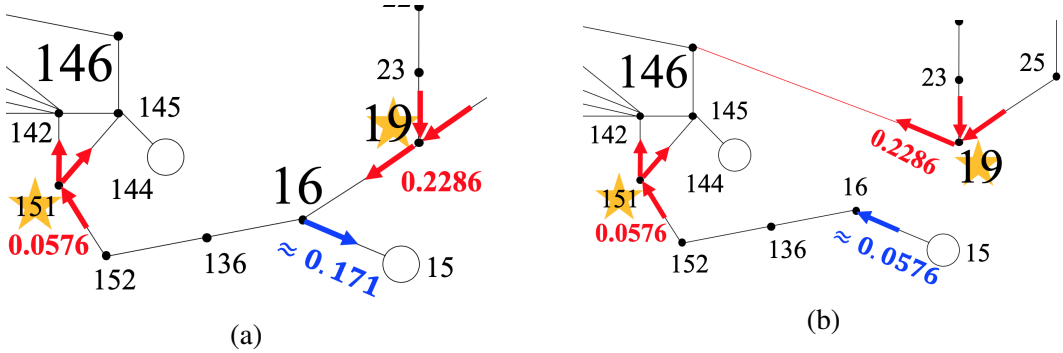



Figure 2.13: Zoomed-in version of the area in the green box at Figure 2.7 (a): actual topology (left); topology reported in a control center (right).

## 2.6 Concluding Remarks

In this chapter, a purely data-driven but physically interpretable method is proposed in order to locate forced oscillation sources in power systems. The localization problem

is formulated as an instance of matrix decomposition, i.e., how to decompose the high-dimensional synchrophasor data into a low-rank matrix and a sparse matrix, which can be done using Robust Principal Component Analysis. Based on this problem formulation, a localization algorithm for real-time operation is presented. The proposed algorithm does not require any information on system models nor grid topology, thus providing an efficient and easily deployable solution for real-time operation. Without the availability of system topology, the proposed algorithm can achieve high localization accuracy in synthetic cases based on benchmark systems and real-world forced oscillation in the power grid of Texas. In addition, a possible theoretical interpretation of the efficacy of the algorithm is provided based on physical model-based analysis, highlighting the fact that the rank of the resonance component matrix is at most 2. Future work will test the proposed localization algorithm in conjunction with FO detection algorithms, and explore a broader set of algorithms and their theoretical performance analysis for large-scale realistic power systems.

# 3. AN ONLINE DETECTION FRAMEWORK FOR CYBER ATTACKS ON AUTOMATIC GENERATION CONTROL[1]

## 3.1 Motivation

The role of Automatic Generation Control (AGC) in large power systems is indispensable. It maintains nominal frequency while minimizing generation costs. The operation of the AGC involves close interaction between the cyber and the physical layers. By tracking Area Control Error (ACE) deviation collected from distributed sensors, the power outputs of generators are modified via AGC to balance random fluctuation of loads, and the electric grid frequency is thereby maintained within a tight range around the nominal value (50/60 Hz). However, due to the consequent tight coupling between the cyber and physical layers, there arises a vulnerability in that both grid stability and security can be compromised by malicious attacks on the cyber layer for sensing. Rather than compromising the strongly secured cyber layers of the control centers, cyber attacks on distributed measurements feeding the AGC might in fact significantly disrupt the operational goals of the power system [35]. There have been several efforts at examining the potential mechanisms by which such cyber attacks on AGCs can be carried out and their negative impacts on the system operation. For example, as described in [36], several attempts for cyber attacks on AGCs, namely, scaling, ramp, pulse, and random attacks, may compromise both the physical system stability and the electricity market operation. Experiments based on CPS testbeds suggest that the corrupted measurements feeding the AGC might bring power systems to under-frequency condition and cause unnecessary load shedding [37], [38]. By replacing the original measurements with an "optimal attack sequence", the malicious attackers can

[1] ©2018 IEEE. Reprinted, with permission, from Tong Huang, Bharadwaj Satchidanandan, P. R. Kumar and Le Xie, "An Online Detection Framework for Cyber Attacks on Automatic Generation Control," in *IEEE Transactions on Power Systems*, vol. 33, no. 6, pp. 6816-6827, Nov. 2018.

disrupt the system frequency in the shortest time without triggering certain pre-defined data quality alarms [35]. Besides cyber attacks on AGC, potential risks can also be posed from the load side: adversaries may be able to trip targeted generators by manipulating the controller parameters of the loads offering emulated inertia control services [39], [40]. This chapter focuses on the detection of cyber attacks on AGC.

All of the above attack strategies on AGC are based on the assumption that the cyber layer of the AGC transporting the physical measurements is vulnerable to attacks, so that a malicious adversary can manipulate these measurements. Unfortunately, this assumption is validated by several recent real-world incidents. Examples include computer viruses such as Dragonfly [41] and Stuxnet [42] targeting Industrial Control Systems (ICS). Therefore, although no real-world attack specifically targeting the AGC has been reported thus far, the aforementioned attack strategies on AGC are more than theoretical concerns. As grid operation becomes more and more data-dependent, it is imperative to prepare the operators with an online defense mechanism against all possible cyber attacks on AGCs.

There have been several detection techniques for cyber attacks on AGCs. In [36], cyber attacks following predefined attack strategies are detected by checking the statistical and temporal characterization of area control errors (ACE). In [43], a statistical model learned from frequency and tie-line flow measurements is exploited to predict their short-term values. Measurements in the vicinity of their corresponding predictions are tagged as normal measurements. Otherwise, alarms are triggered. In [35], the compromised tie-line flow measurements are detected by capturing the discrepancy between the meter readings of frequency deviation and its predicted value based on reported tie-line flow measurements and an identified linear-regression model. Also, DC state estimation (SE) is modified to be executed every AGC cycle and serves as an additional layer for data purification in [35].

Although the aforementioned approaches increase the attack costs to some extent, the

measurements feeding the AGC may still be compromised by an attacker equipped with the following capabilities. First, the malicious adversaries are not constrained to follow the prescribed attack templates in order to cause significant impact on the grid [35]. Although the anomaly detection engine proposed in [36] is capable of identifying the predefined attack templates, there is no theoretical guarantee that the proposed algorithm can detect arbitrary cyber attacks. Second, extensive information on the system model might be exposed to the adversary. There are two ways by which a malicious adversary can obtain information about the power system model: 1) The detailed physical model may be directly leaked to the attacker via disgruntled employees or malicious insiders [44]; 2) The statistical model of the power system can be learned using mathematical tools based on the leaked system operating data. The attackers in the former case can bypass the SE-based detection algorithm by conducting "unobservable attacks" described in [45] or by conducting the packet-reordering integrity attack reported in [46], whereas the adversaries in the latter case can tamper with the measurements without triggering the alarm defined in [43] by replacing the actual measurement sequence with a different sequence that still conforms to the learned statistical model [47]. Besides, the authors of [35] exclude the attacks on frequency sensors from their framework. Therefore, a subtle but malicious distortion of frequency measurements based on the physical/statistical model of the power system is not likely to be detected by the algorithm proposed in [35].

In this chapter, we introduce a first-of-its-kind online detection framework of false data injection attacks in power systems. The recent dynamic watermarking technique [47], [48] is employed in the framework and serves as the core algorithm to detect any tampered measurements feeding the AGC. Through deliberately superimposing a private signal of small magnitude upon the control commands sent by the AGC, we "watermark" the measurements feeding the AGC with certain indelible characteristics [47], by which cyber attacks on the AGC can be identified. To the best of the authors' knowledge, this is the first time

that the dynamic watermarking technique has been applied to address cyber-security issues in power systems. The proposed framework has the following advantages. 1) The detection algorithm used with the dynamic watermarking is theoretically rigorous and ensures that any manipulation of the measurements feeding the AGC can be detected regardless of the attack strategy that the attackers follow, as long as the controlled generators can execute commands from AGC honestly; 2) the algorithm can be used when attackers possess detailed information of the physical/statistical models of the power system; 3) the proposed framework is practically implementable, as it needs no hardware update on generation units.

The rest of this chapter is organized as follows. Section 3.2 formulates the problem of detection of cyber attacks by mathematically describing a system equipped with AGC and by presenting typical attack models; Section 3.3 presents the dynamic watermarking-based detection algorithm in the context of AGC; Section 3.4 validates the efficacy of the proposed algorithm via an illustrative example; Section 3.5 concludes the chapter.

## 3.2 Problem Formulation

In this section, a power system equipped with multiple AGCs is described mathematically, and typical attack templates are presented.

### 3.2.1 The Model of a Multi-area Power System without AGC

The dynamics of a multi-area power system in the vicinity of an operating condition can be described approximately by a continuous state-space model [49]:

$$\dot{\boldsymbol{x}}(t) = A\boldsymbol{x}(t) + B\boldsymbol{u}(t) + \boldsymbol{\gamma}'(t), \tag{3.1a}$$

$$\boldsymbol{y}(t) = C\boldsymbol{x}(t) + \boldsymbol{n}'(t), \tag{3.1b}$$

where $\boldsymbol{x}(t) \in \mathbb{R}^{n' \times 1}$, $\boldsymbol{u}(t) \in \mathbb{R}^{d \times 1}$ and $\boldsymbol{y}(t) \in \mathbb{R}^{m \times 1}$ are states, inputs and measurements vectors in the time instant $t$, respectively, and the matrices $A$, $B$ and $C$ are system parameters of appropriate dimensions. Above $\boldsymbol{\gamma}'(t) \sim \mathcal{N}(0, Q')$ and $\boldsymbol{n}'(t) \sim \mathcal{N}(0, R')$ denote the white process noise and the measurement noise respectively that are independent of each other (A more mathematical description would entail stochastic differential equations). Suppose that there are $r$ control areas. Then, the measurement vector $\boldsymbol{y}(t)$ in (3.1) can be reorganized as $\boldsymbol{y}(t) = \begin{bmatrix} \boldsymbol{y}_1(t)^T & \boldsymbol{y}_2(t)^T & \cdots & \boldsymbol{y}_i(t)^T \cdots & \boldsymbol{y}_r(t)^T \end{bmatrix}^T$, where $(\cdot)^T$ is the transpose operation, and $\boldsymbol{y}_i(t)$ is a column vector incorporating all tie-line flow deviations $\boldsymbol{p}_{ti}(t)$, as well as the frequency deviation $\omega_i(t)$ in the control area $i$, i.e.,

$$\boldsymbol{y}_i(t) = \begin{bmatrix} \boldsymbol{p}_{ti}(t)^T & \omega_i(t) \end{bmatrix}^T. \tag{3.2}$$

Similarly, the variables in $\boldsymbol{u}(t)$ can be grouped area-wise into $\boldsymbol{u}(t) = [\boldsymbol{u}_1(t)^T, \ldots, \boldsymbol{u}_r(t)^T]^T$, where the column vector $\boldsymbol{u}_i(t)$ includes the load reference setpoints $\boldsymbol{p}_{\text{s}i}(t) \in \mathbb{R}^{d' \times 1}$ of all generators participating in AGC in the area $i$, as well as local load fluctuation $\boldsymbol{p}_{\text{load}i}(t) + j\boldsymbol{q}_{\text{load}i}(t)$ at time instant $t$, i.e.,

$$\boldsymbol{u}_i(t) = \begin{bmatrix} \boldsymbol{p}_{\text{s}i}(t)^T & \boldsymbol{u}_{\text{load}i}(t)^T \end{bmatrix}^T, \tag{3.3}$$

where $\boldsymbol{u}_{\text{load}i} = \begin{bmatrix} \boldsymbol{p}_{\text{load}i}(t)^T & \boldsymbol{q}_{\text{load}i}(t)^T \end{bmatrix}^T$.

### 3.2.2 The Model of a Multi-area System Regulated by AGC

From a system-theoretic perspective, the AGC can be regarded as a multi-variable feedback loop added to the plant described in (3.1). In order to achieve independent regulation for the local tie-line flows and frequency, the Balancing Authority in one area only actuates the local generators participating in AGC without interference from generators in

other areas. Therefore, the multi-area control policy can be decentralized area-wise as

$$\begin{aligned}\mathbf{u}[t] &= \boldsymbol{f}(\boldsymbol{y}^t) \\ &= \begin{bmatrix} \boldsymbol{f}_1(\boldsymbol{y}_1^t)^T & \boldsymbol{f}_2(\boldsymbol{y}_2^t)^T & \cdots & \boldsymbol{f}_i(\boldsymbol{y}_i^t)^T & \cdots & \boldsymbol{f}_r(\boldsymbol{y}_r^t)^T \end{bmatrix}^T,\end{aligned} \tag{3.4}$$

where $\boldsymbol{y}_i^t$ is the telemetered measurement sequence up to time $t$ at area $i$. To elaborate on the control policy, suppose that there are $\psi$ local generation units in the AGC and $\phi$ measurements in area $i$, then the control policy of AGC $\boldsymbol{f_i}(\cdot) : \mathbb{R}^\phi \to \mathbb{R}^\psi$ consists of the following operations between two successive economic dispatches:

1. Area control error (ACE) is calculated from the telemetered tie-line flows and frequency measurements sampled every two to four seconds as

$$ACE_i = \sum_{s=1}^{\phi} p_{ti,s} + \beta_i \omega_i,$$

   where the adjustable parameter $\beta_i$ is a bias factor.

2. The ACE is smoothed by passing it through a low-order filter in order to mitigate the fatigue of generation control devices, e.g., turbine valves and governor motors [50].

3. At the balancing authority, a control command is computed from the ACE according to the control policy reported in [51], and is executed every two to four seconds [50], [44]. Denote by $\kappa_i \tau$ the time period between two consecutive commands.

4. The control command computed by AGC is sent to the $\psi$ local generation units and its magnitude for each controlled generator is proportional to the coefficient updated by the economic dispatch algorithm [52], [53].

The above procedure (also summarized in Fig. 3.2) indicates that only the measurements at the chosen sample instants contribute to the computation of the control commands sent

by the AGC at area $i$. The sequence $\boldsymbol{y}_i^t$ formed by these measurements is denoted by

$$\boldsymbol{y}_i^t := \left\{ \boldsymbol{y}_i(0), \boldsymbol{y}_i(\kappa_i\tau), \cdots, \boldsymbol{y}_i\left( \left\lfloor \frac{t}{\kappa_i\tau} \right\rfloor \kappa_i\tau \right) \right\} \tag{3.5}$$

where $\lfloor \cdot \rfloor$ is the floor function. The above control policy yields the load reference setpoints $\boldsymbol{p}_{\mathrm{s}i}(t)$, so that

$$\boldsymbol{p}_{\mathrm{s}i}(t) = \boldsymbol{f}_i(\boldsymbol{y}_i^t) \quad \forall i \in \{1, 2, \cdots, r\}. \tag{3.6}$$

The above equation couples the physical infrastructure (generation units) and the cyber layer (control centers) together. In summary, (3.1), (3.4) and (3.6) constitute a hybrid model for a multi-area power system regulated by AGCs.

Note that a commercial-level AGC includes more functions, which are assumed to be included into the control law $\boldsymbol{f}_i(\cdot)$. Fig. 3.2 shows a simplified version of a realistic AGC.

### 3.2.3 Discretization of the Hybrid AGC Model

Suppose that the time period between two consecutive control commands of AGC in each area is an integer multiple of a sampling time $\tau$, namely, $\kappa_i$ is assumed to be an integer. Then the continuous-time state space model (3.1) can be discretized at $\tau$ using the approach reported in [54]. For the sake of convenience, the discrete state-space model is denoted as $\mathcal{M}_{\mathrm{d}}''$. Similarly, the AGC control policies in area can also be sampled at $\tau$. Denote the discrete control policies by $\boldsymbol{f}_{\mathrm{d}i}(\cdot)$ for all $i \in \{1, 2, \cdots, r\}$. It is worth noting that all areas are sampled with the same interval $\tau$, and the AGC in area $i$ sends control signals only after every $\kappa_i\tau$ seconds, for $i \in \{1, 2, \cdots, r\}$.

For the control area $i$, we temporarily open its AGC feedback loop and keep the AGC loops in other areas $j$ connected, for $j \in \{1, 2, \cdots, r\}$ and $j \neq i$. As shown in Fig. 3.1, we focus on modeling the open-loop behavior of the system for area $i$ in terms of its inputs, i.e., the setpoints $\boldsymbol{p}_{\mathrm{s}i}$ of the controlled generators in the area $i$, and all load

fluctuations $\boldsymbol{u}_{\text{load}j}$ for all $j \in \{1, 2, \cdots, r\}$, and its outputs, i.e., all tie-line flow deviations $\boldsymbol{p}_{ti}$ and frequency deviations $\omega_i$ in (3.2). As is standard in linear control theory [55], the discrete model of the aforementioned open-loop system can be obtained by interconnecting the entire system model $\mathcal{M}''_{\text{d}}$ and the discrete AGC control policies $\boldsymbol{f}_{\text{d}j}(\cdot)$, where $j \in \{1, 2, \cdots, r\}$ and $j \neq i$. Denote the resulting interconnected state-space model for area $i$ by $\mathcal{M}'_{\text{d}i}$. It is worth noting that the state variables of $\mathcal{M}'_{\text{d}i}$ include all state variables in both state-space model $\mathcal{M}''_{\text{d}}$ and discrete control policies $\boldsymbol{f}_{\text{d}j}$, where $j \in \{1, 2, \cdots, r\}$ and $j \neq i$. We specify setpoint $\boldsymbol{p}_{si}$ as the control inputs of system $\mathcal{M}'_{\text{d}i}$, and further assume $\mathcal{M}'_{\text{d}i}$ is stabilizable [54]. Finally, the discrete state-space model $\mathcal{M}'_{\text{d}i}$ can be minimally realized by a controllable and observable model $\mathcal{M}_{\text{d}i}$ with reduced order [54], namely,

$$\begin{aligned} \boldsymbol{x}_{\text{d}i}(k+1) =& A_{\text{d}i}\boldsymbol{x}_{\text{d}i}(k) + B^{\text{ref}}_{\text{d}i}\boldsymbol{p}_{si}(k) \\ &+ B^{\text{load}}_{\text{d}i}\boldsymbol{u}_{\text{load}}(k) + \boldsymbol{\gamma}(k+1) \end{aligned} \tag{3.7a}$$

$$\boldsymbol{y}_i(k) = C_{\text{d}i}\boldsymbol{x}_{\text{d}i}(k) + \boldsymbol{n}(k) \tag{3.7b}$$

where $\boldsymbol{x}_{\text{d}i} \in \mathbb{R}^{n\times 1}$ collects all state variables in the reduced-order model $\mathcal{M}_{\text{d}i}$ and $\boldsymbol{u}_{\text{load}}(k) = \begin{bmatrix} \boldsymbol{u}^T_{\text{load}1} & \boldsymbol{u}^T_{\text{load}2} & \cdots & \boldsymbol{u}^T_{\text{load}r} \end{bmatrix}^T$. Vector $\boldsymbol{\gamma}(t) \sim \mathcal{N}(0, Q)$ and $\boldsymbol{n}(t) \sim \mathcal{N}(0, R)$ are the white process and measurement noises, where $R$ is positive definite. We assume that the rank of matrix $C_{\text{d}i}B^{\text{ref}}_{\text{d}i}$ equals $\phi$, which is the number of rows of $C_{\text{d}i}$.

### 3.2.4 Cyber Attack Models and Their Impacts

Due to the close interaction between the AGC and the generation units indicated by (3.6), the adversary can compromise the physical layer of the power system by distorting the measurements $\boldsymbol{y}^t$. Denote by $\boldsymbol{z}^t$ the measurements *reported* by the sensors. The sensors are supposed to report the actual value measured, i.e., they are supposed to re-

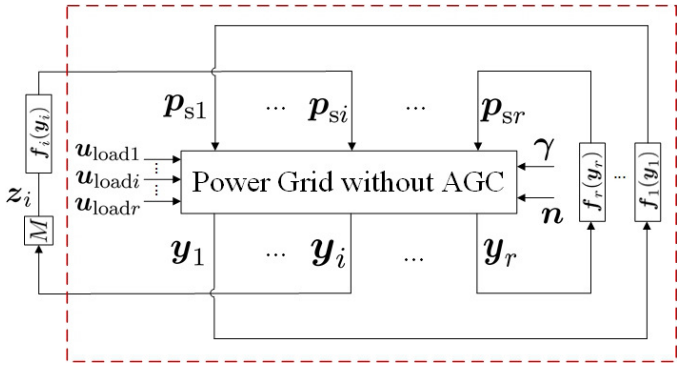



Figure 3.1: A multi-area power system with AGC systems.

port truthfully with $\boldsymbol{z}^t = \boldsymbol{y}^t$. However, an adversarial sensor might declare values that are different from the actual measurements, so that $\boldsymbol{z}^t \neq \boldsymbol{y}^t$. The purpose of this chapter is to detect the inconsistency between the actual and the reported measurements caused deliberately by the attacker. The attackers are assumed to be able to manipulate the distributed sensors feeding into AGC, i.e., frequency and tie-line flow measurements. Before describing the remedy for the problem, we present three typical attack templates.

*1) Replay Attack:* Before the attack, the adversary records the measurements during normal operating condition for some duration. During the attack, the actual measurements observed by the adversarial sensors are replaced by the recorded measurements and reported to the control center [56].

*2) Noise-injection Attack:* Under this attack model, the adversarial sensors add a bounded random value to the actual measurement and then report it to the control center.

*3) Destabilization Attack:* In a destabilization attack, the compromised sensors of the AGC in area $i$ report a sequence $\{\boldsymbol{z}_i\}$ which is a filtered version of the actual measurement sequence $\{\boldsymbol{y}_i\}$. If $M$ denotes such a filter, the attack consists of inserting the filter $M$ to the system model, with $M$ so chosen such that the original system becomes unstable. It is

worth noting that the output sequence $\boldsymbol{z}_i$ of a malicious filter $M$ can be obtained through a simple tuning procedure, even without any information on the system model, as will be described in Section 3.4.1.

Note that the attackers are not limited to follow any attack templates, in their attempt to bring harm to power systems. Correspondingly, a defense method should be designed not only for detecting the three types of attacks defined above, but also for securing AGC from any manipulation on the distributed measurements feeding into AGC.

## 3.3 Dynamic Watermarking-based Defense

In this section, we apply the approach of dynamic watermarking reported in [47], [48], [57] to secure the distributed measurements feeding AGC in power systems. The fundamental idea of Dynamic Watermarking is as follows. The actuators (generation units in this case) superimpose on the control policy-specified input, a “small" random signal chosen according to a certain probability distribution. While this probability distribution is made public, so that even the adversary knows it, the actual realization of the random signal is known only to that particular generation unit, and it doesn't reveal that to any other party. For this reason, the random signal is also called the private excitation of the generators. In such a scenario, the honest sensors and the malicious sensors are distinguished by the following fact: the truthful measurements reported by the honest sensors exhibit certain expected statistical properties that are relevant to the statistics of the private excitation, whereas, as shown in [47], [48], measurements reported by the malicious sensors, if excessively distorted, do not exhibit these properties. Therefore, by subjecting the reported measurements to certain tests for these statistical properties, malicious activity in the system can be detected.

In this chapter, we will demonstrate the application of this approach in the context of power systems. For control area $i$, an independent and identically distributed (i.i.d.) private

excitation $\{\boldsymbol{e}_i(k)\}$ is superimposed on the control inputs $\{\boldsymbol{p}_{si}(k)\}$ [48]. Consequently, the input applied at time $k$ is

$$\boldsymbol{p}_{si}(k) = \boldsymbol{f}_i(\boldsymbol{y}_i^k) + \boldsymbol{e}_i(k), \tag{3.8}$$

where $\boldsymbol{e}_i(k) \sim \mathcal{N}(0, \sigma_e^2 I)$. It is worth noting that (3.8) can be implemented by modifying the AGC software at the balancing authorities without any hardware updates on the generation units. With the private injection $\{\boldsymbol{e}_i(k)\}$, any attempt to distort the measurements fed to AGC will be detected by subjecting the reported measurements to the two tests [48] described below. A detailed proof for this conclusion can be found in [48].

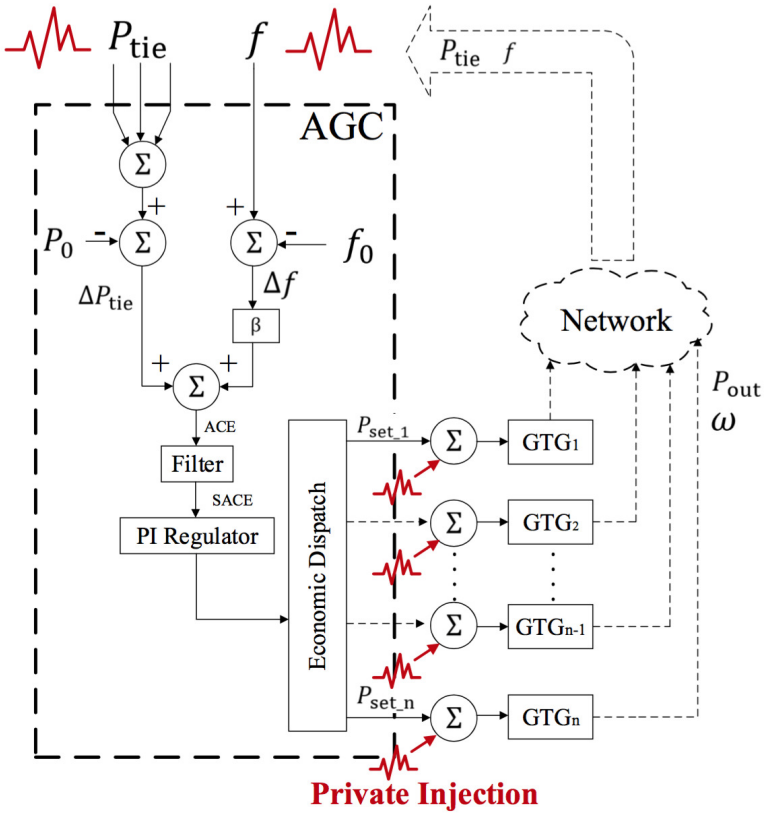



Figure 3.2: Location of Private Injection in a Simplified Functional Diagram of AGC

### 3.3.1 Two Indicators of Dynamic Watermarking

Given the input sequence $\boldsymbol{u}_i$ and measurement sequence $\boldsymbol{y}_i$ of the discrete system (3.7) up to the $k$th unit of time, the system state $\boldsymbol{x}_{\mathrm{d}i}(k|k)$ can be estimated by the Kalman filter as

$$\begin{aligned}\boldsymbol{x}_{\mathrm{d}i}(k+1|k) = A_{\mathrm{d}i}(I - L_{\mathrm{d}i}C_{\mathrm{d}i})\boldsymbol{x}_{\mathrm{d}i}(k|k-1)+ \\ \begin{bmatrix} B_{\mathrm{d}i}^{\mathrm{ref}} & B_{\mathrm{d}i}^{\mathrm{load}} & A_{\mathrm{d}i}L_{\mathrm{d}i} \end{bmatrix} \begin{bmatrix} \boldsymbol{p}_{\mathrm{s}i}(k) \\ \boldsymbol{u}_{\mathrm{load}}(k) \\ \boldsymbol{y}_i(k) \end{bmatrix},\end{aligned} \tag{3.9a}$$

$$\boldsymbol{x}_{\mathrm{d}i}(k|k) = (I - L_{\mathrm{d}i}C_{\mathrm{d}i})\boldsymbol{x}_{\mathrm{d}i}(k|k-1) + L_{\mathrm{d}i}\boldsymbol{y}_i(k), \tag{3.9b}$$

where $L_{\mathrm{d}i}$ is the steady-state Kalman filtering gain given by

$$L_{\mathrm{d}i} = PC_{\mathrm{d}i}^T(C_{\mathrm{d}i}PC_{\mathrm{d}i}^T + R)^{-1}. \tag{3.10}$$

In the above, $P$ is obtained as the unique positive definite solution of the Algebraic Riccati Equation [58].

We define

$$\begin{aligned}\boldsymbol{\zeta}_k :=& \boldsymbol{x}_{\mathrm{d}i}(k|k) - A_{\mathrm{d}i}\boldsymbol{x}_{\mathrm{d}i}(k-1|k-1) - B_{\mathrm{d}i}^{\mathrm{ref}}\boldsymbol{f}_i(\boldsymbol{z}_i^{k-1}) \\ & - B_{\mathrm{d}i}^{\mathrm{ref}}\boldsymbol{e}(k-1) - B_{\mathrm{d}i}^{\mathrm{load}}\boldsymbol{u}_{\mathrm{load}}.\end{aligned} \tag{3.11}$$

*1) Test 1:* Check if

$$\lim_{T\to\infty}\frac{1}{T}\sum_{k=1}^{T}\boldsymbol{\zeta}_k\boldsymbol{\zeta}_k^T = L_{\mathrm{d}i}\Sigma_i L_{\mathrm{d}i}^T, \tag{3.12}$$

where

$$\Sigma_i := C_{\mathrm{d}i}PC_{\mathrm{d}i}^T + R. \tag{3.13}$$

Correspondingly, we choose a time window $T$ and define an indicator matrix $W$ by

$$W(T) := \frac{1}{T}\sum_{k=1}^{T} \boldsymbol{\zeta}_k \boldsymbol{\zeta}_k^T - L_{\mathrm{d}i}\Sigma_i L_{\mathrm{d}i}^T. \tag{3.14}$$

*2) Test 2:* Check if

$$\lim_{T\to\infty} \frac{1}{T}\sum_{k=1}^{T} \boldsymbol{e}(k-1)\boldsymbol{\zeta}_k^T = 0. \tag{3.15}$$

As before, we define

$$V(T) := \frac{1}{T}\sum_{k=1}^{T} \boldsymbol{e}(k-1)\boldsymbol{\zeta}_k^T. \tag{3.16}$$

This measure can be calculated by the system operators. The reported measurements of interest, $\{\boldsymbol{z}_i(k)\}$, will pass both tests if $\boldsymbol{z}_i(k) \equiv \boldsymbol{y}_i(k)$ for all $k$; if the sensors distort the measurements beyond adding a zero-power signal, then, as shown in [48], at least one of the above tests will fail. While tests (3.12) and (3.15) are asymptotic in nature, they can be converted to statistical tests that can be performed in finite time. For example, we expect much bigger entries in $W$ or $V$ during cyber attacks, than their counterparts when no attack happens. This leads naturally to a threshold test for detecting malicious distortion.

### 3.3.2 Online Algorithm for Detection of Cyber Attacks

The computation of the aforementioned indicators requires a sequence of reported measurements $\{\boldsymbol{z}_i\}$, private injections $\{\boldsymbol{e}_i\}$, load fluctuations of the whole grid $\{\boldsymbol{u}_{\text{load}}\}$ and AGC command signals $\{\boldsymbol{f}_i(\boldsymbol{z}_i^{k-1})\}$ over a period of time. Therefore, in order to check whether the reported measurements pass the two tests (3.12), (3.15), the generation unit processes a block of $\{\boldsymbol{z}_i\}$, $\{\boldsymbol{e}_i\}$, $\{\boldsymbol{u}_{\text{load}}\}$ and $\{\boldsymbol{f}_i(\boldsymbol{z}_i^{k-1})\}$ within a time window $T$. Suppose that each block of the above sequences includes $T$ samples. Then, up to time $t = j \times T \times \kappa_i\tau$, we will have $j$ blocks of above sequences. The $j$th block of above

sequences in area $i$ are denoted by $\boldsymbol{z}_i^{\mathrm{BL}j}$, $\boldsymbol{e}_i^j$, $\boldsymbol{u}_{\text{load}}^j$ and $\boldsymbol{f}_i^j$, respectively:

$$\boldsymbol{z}_i^{\mathrm{BL}j} := \{\boldsymbol{z}_i((j-1)T), \boldsymbol{z}_i((j-1)T+1), \cdots, \boldsymbol{z}_i(jT)\},$$

$$\boldsymbol{e}_i^j := \{\boldsymbol{e}_i((j-1)T), \boldsymbol{e}_i((j-1)T+1), \cdots, \boldsymbol{e}_i(jT)\},$$

$$\boldsymbol{u}_{\text{load}}^j := \{\boldsymbol{u}_{\text{load}}((j-1)T), \boldsymbol{u}_{\text{load}}((j-1)T+1), \cdots, \boldsymbol{u}_{\text{load}}(jT)\},$$

and

$$\boldsymbol{f}_i^j := \{\boldsymbol{f}_i(\boldsymbol{z}_i^{(j-1)T-1}), \boldsymbol{f}_i(\boldsymbol{z}_i^{(j-1)T}), \cdots, \boldsymbol{f}_i(\boldsymbol{z}_i^{jT-1})\}.$$

In terms of online application, let $W^j = [w_{g,h}^j]$ and $V^j = [v_{g,h}^j]$ be $W$ and $V$ calculated within the $jth$ time window, respectively. Then the indicator scalars $\xi_1^j$ and $\xi_2^j$ are defined as follows

$$\xi_1^j := \left|\mathrm{tr}(W^j)\right| \tag{3.17a}$$

$$\xi_2^j := \sqrt{\sum_{g=1}^{d'}\sum_{h=1}^{n}(v_{g,h}^j)^2} \tag{3.17b}$$

where $\mathrm{tr}(\cdot)$ is the trace operator. As mentioned in (3.2) and (3.7), $d'$ is the number of the controlled generators in AGC of area $i$ and $n$ is the order of the reduced-order model in (3.7). Finally, we expect $\xi_1^j \geq \eta_1$ or $\xi_2^j \geq \eta_2$, if attacks are launched in the $jth$ time window, where $\eta_1$ and $\eta_2$ are pre-defined thresholds. The thresholds $\eta_1$ and $\eta_2$ can be obtained from the following training procedure:

1. based on (3.14) and (3.16), first compute $W^\infty = W(T_\infty)$ and $V^\infty = V(T_\infty)$ under normal operating condition, where $T_\infty$ is a large integer that is set to $1800$ in this chapter;

2. obtain the general indicators $\xi_1^\infty$ and $\xi_2^\infty$ under a normal condition by (3.17);

3. the thresholds $\eta_1$ and $\eta_2$ are calculated by

$$\eta_1 = \kappa' \xi_1^{\infty} \quad \eta_2 = \kappa' \xi_2^{\infty} \tag{3.18}$$

where $\kappa'$ is an empirically adjustable parameter.

The detection thresholds $\eta_1$, $\eta_2$ can also be determined using the Neyman-Pearson criterion based on the maximum tolerable false alarm rate. Algorithm 2 specifies the subroutine for computing the two indicators $\xi_1^j$ and $\xi_2^j$ for the $jth$ block of measurements.

For area $i$, private signals $\boldsymbol{e}_i$ are superimposed upon the AGC commands according to (3.8) and Fig. 3.2. Then Algorithm 2 enables the balancing authority of area $i$ to detect cyber attacks on the measurements feeding the AGC. Once attacks in area $i$ are detected, the balancing authority stops sending commands to the generators in the AGC. Similarly, attacks to other areas can be detected by the corresponding balancing authorities similarly equipped with Algorithm 2. Additionally, it is worth emphasizing that Fig. 3.2 is a *simplified* functional diagram of AGC, where the optimal power setpoints are the actual outputs of the simplified AGC. In the proposed method, the private excitations $\boldsymbol{f}_i(\boldsymbol{y}_i^k)$ are supposed to be superimposed upon the actual outputs of AGC, which is not necessary to be the calculated optimal power setpoint in a realistic AGC.

After a cyber attack is detected by the proposed framework, the AGC should be deactivated. It is worth noting that an efficient procedure for finding malicious sensors should be initiated after deactivating the AGC. Such a procedure may include dispatching a panel to investigate the distributed measurements after an alarm. Also, the procedure is required to correct the malicious sensors quickly. This requirement is achievable due to the limited number of the distributed measurements feeding to AGC. After clearing the cyberattacks, the AGC should be back to service. Therefore, the AGC is actually absent only for a short period of time, instead of permanently out of service.

**Algorithm 2** Online Algorithm for Detection of Cyber Attack

$H \leftarrow L_{\mathrm{d}i}\Sigma_i L_{\mathrm{d}i}^T$; $j \leftarrow 1$
**while** $k = 1, 2, \cdots$, **do**
  **if** $k \geq jT$ **then**
    Obtain the sequence $\boldsymbol{z}_i^{\mathrm{BL}j}$, $\boldsymbol{e}_i^j$, $\boldsymbol{u}_{\mathrm{load}}^j$, $\boldsymbol{f}_i^j$;
    Compute $\boldsymbol{x}_{\mathrm{e}} := \{\boldsymbol{x}(k'|k')\}$ by (3.6) and (3.9) for all $k' = (j-1)T, (j-1)T+1, \cdots, jT$;
    $\xi_1^j, \xi_2^j \leftarrow$ `Indicators`($\boldsymbol{x}_{\mathrm{e}}^j$, $\boldsymbol{e}_i^j$, $\boldsymbol{u}_{\mathrm{load}}^j$, $\boldsymbol{f}_i^j$, $j$, $H$);
    $j \leftarrow j + 1$
    **if** $\xi_1 \geq \eta_1 \vee \xi_2 \geq \eta_2$ **then**
      Claim attacks and stop sending commands to the generators on AGC;
    **end if**
  **end if**
**end while**

**Algorithm 3** Computation of $\xi_1^j$ and $\xi_2^j$ at the $j$th block

**function** `Indicators`($\boldsymbol{x}_{\mathrm{e}}^j$, $\boldsymbol{e}_i^j$, $\boldsymbol{u}_{\mathrm{load}}^j$, $\boldsymbol{f}_i^j$, $j$, $H$)
  $\Sigma_{s1} \leftarrow 0$; $\Sigma_{s2} \leftarrow 0$
  **while** $k = (j-1)T, (j-1)T+1, \cdots, jT$, **do**
    Compute $\boldsymbol{\zeta}_k$ by (3.11)
    $\Sigma_{s1} \leftarrow \Sigma_{s1} + \boldsymbol{\zeta}_k\boldsymbol{\zeta}_k^T$; $\Sigma_{s2} \leftarrow \Sigma_{s2} + \boldsymbol{e}(k-1)\boldsymbol{\zeta}_k^T$
  **end while**
  $W^j = \frac{1}{T}\Sigma_{s1} - H$; $V_2^j = \frac{1}{T}\Sigma_{s2}$
  Obtain $\xi_1^j$ and $\xi_2^j$ via (3.17)
  **return** $\xi_1^j$, $\xi_2^j$
**end function**

One might wonder if the temporary absence of AGC significantly impacts the system frequency. The answer is that the temporary absence of AGC should not be a big concern, as the AGC is allowed to be deactivated in real-world system operation during some situations such as intentional tripping of load/generation [50]. Even without fine adjustments of frequency owing to AGC, the primary frequency control is capable of maintaining the system frequency within an acceptable range, say, from 59.96 Hz to 60.04 Hz [34], and the frequency falling into such a range will not trigger any load shedding events [59]. However, if stealthy cyberattacks on AGC are not detected in a timely fashion, they may keep compromising the control performance of the frequency regulation. For example, if a replay attack is not detected in time, the energy consumed by AGC actually bring no benefit to the grid in terms of regulating frequency, and the control performance of AGC is compromised.

## 3.4 Numerical Examples

This section presents the results on the efficacy of the dynamic-watermarking-based online defense algorithm on a four-area power system and the Northeastern Power Coordinating Council (NPCC) 140-bus power system. The malicious attacks to the synthetic system will be launched based on the attack templates presented in Sec. 3.2.4. As will be shown, these attacks can be detected in a timely manner via the proposed approach without sacrificing the performance of the system.

### 3.4.1 Performance Validation of the Proposed Algorithm on the Four-area System

*1) Four-area System Description:* This test system has four areas and ten generators, as shown in Fig. 3.3. The system is linearized about the given operating condition by Power System Toolbox (PST) [60], and the system matrices for the linear model, i.e., $A$, $B$ and $C$ in (3.1), are extracted. In order to mimic the behavior of AGC, in each area, we add a discrete proportional-integral (PI) feedback loop, where the proportional gain constant is

set to $-0.0745$ and the integral gain is set to $-0.0333$. For each area, the PI controller takes its local measurements of tie-line power flows and frequency as its inputs and computes a control signal to change the load reference setpoint of the generator. This is done every 2 seconds, i.e., $\tau = 2$ and $\kappa_i \equiv 1$ for $i \in \{1, 2, 3, 4\}$. The load deviations around the scheduled values are modeled as independent and identically distributed (i.i.d.) Gaussian white noise with zero mean and covariance matrix $\sigma_L^2 I_8$, where $I_8$ is a $8 \times 8$ identity matrix. The variance $\sigma_L^2 = 0.0025$ is chosen such that the frequency fluctuates within the normal range, i.e., $60 \pm 0.03$ Hz [34] with high probability. The measurement noise of frequency and real power are normally distributed with zero mean. The variance of the frequency measurement noise, $\sigma_f^2 = 9.1891 \times 10^{-12}$, is tuned such that the accuracy of frequency measurement falls within $\pm 0.0005$ Hz [61] with high probability, and the signal-to-noise ratio (SNR) of deviation measurements of tie-line flow is 20 dB. The covariance matrix of the process noise $Q'$ is $10^{-9} I_{n'}$, where $I_{n'}$ is an identity matrix of dimension of $n'$.

*2) Parameter Setting of the Proposed Algorithm:* For the implementation of Algorithms 2 and 3, we have the following settings of the parameters:

- The number of samples in each block $T$ is 30, so that $\xi_1^j$ and $\xi_2^j$ are computed every 60 seconds;
- The threshold $\eta_1$ is set to $2.5207 \times 10^{-4}$ with $\xi_1^\infty = 3.6010 \times 10^{-5}$ and $\kappa' = 7$;
- the variance of the private injections $\sigma_e$ in both Area 1 and Area 2 is set to $10^{-7}$.

We first examine the impact of the private injection on the performance of the AGC in terms of frequency regulation. Fig. 3.4 records the control commands from AGC 1, and it shows that the private injection does not cause significant deviation of the actual input from the control policy-specified input. The percentage of variance change of control command of AGC 1 and frequency are $0.26\%$ and $1.73\%$, respectively, and the small change of the variance suggests negligible sacrifice of performance resulting from the private injection.

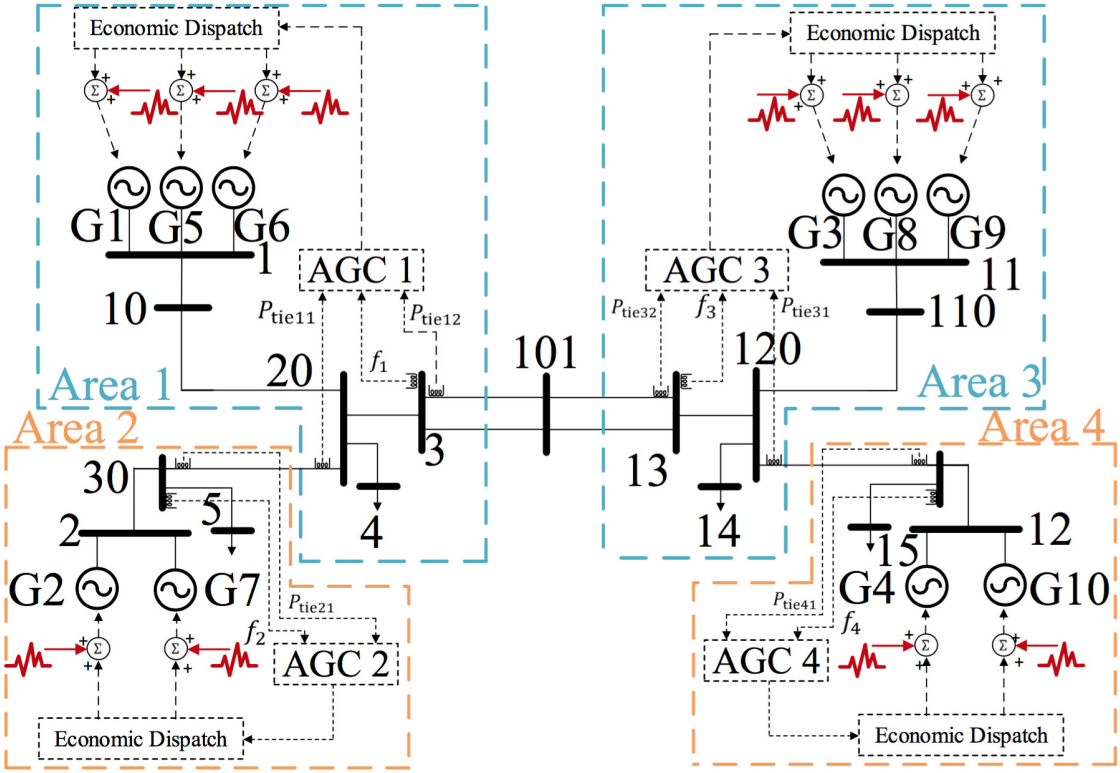



Figure 3.3: Four-area synthetic system with AGC in each area.

*3) Detection of Replay Attack:* We next demonstrate the efficacy of the dynamic watermarking approach for detecting replay attacks. Figure 3.5 shows the frequency measurements in Area 1. Beginning at 30 min, the frequency sensor reports a pre-recorded sequence of measurements instead of the actual measurements. No anomaly can be identified from Fig. 3.5, as no frequency constraint is violated within the time period of interest.

Next, the proposed Algorithms 1 and 2 are applied to detect the replay attack. In each area, the online detection algorithms compute the indicators $\xi_1^j$ and $\xi_2^j$ based on their local measurements of frequency and tie-line flow. The evolution of $\xi_1^j$ over time in Area 1 is presented in Figure 3.6(a). It is seen that $\xi_1^j$ exceeds the threshold $\eta_1$ after 31 minutes, indicating that the attack starts between the $30th$ and $31st$ minutes. A similar result can be observed from Fig. 3.6(b) which presents the evolution of $\xi_1^j$ under the replay attack to

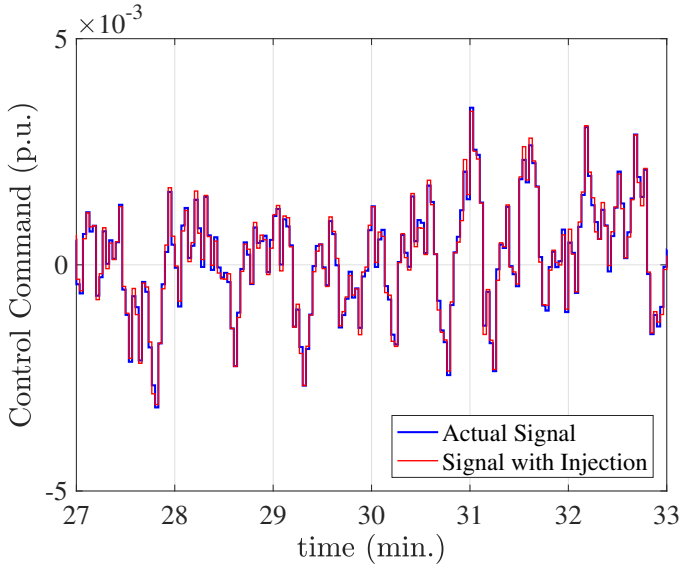



Figure 3.4: The impact of the private injection on the command signal showing that watermarking does not lead to any loss of performance under normal operation.

tie-line flow measurement of Area 1. After the attacks are detected, one mitigation action is to deactivate the AGC.

*4) Detection of Noise-injection Attack:* In this section, we demonstrate the efficacy of the proposed approach for detection of noise-injection attacks. As mentioned in Sec. 3.2.4, additional noise is superimposed on the actual frequency measurement after the $30th$ minute, and it is chosen so that the frequency is still within the normal range. Fig. 3.7 shows the measurements of the frequency before and after the attack, and, again, we cannot notice any anomaly since the frequency is within the normal range all the time and no distinct feature ever appears after 30 minutes. Using the proposed algorithm, the noise injection attack on the frequency measurements (Fig. 3.8) is identified successfully between the 30th and 31st minutes.

*5) Detection of Destabilization Attack:* This section deals with securing the system from destabilization attacks. A destabilization attack is carried out on the tie-line flow measurements in Area 1. The output sequence of a malicious filter $M$ can be obtained

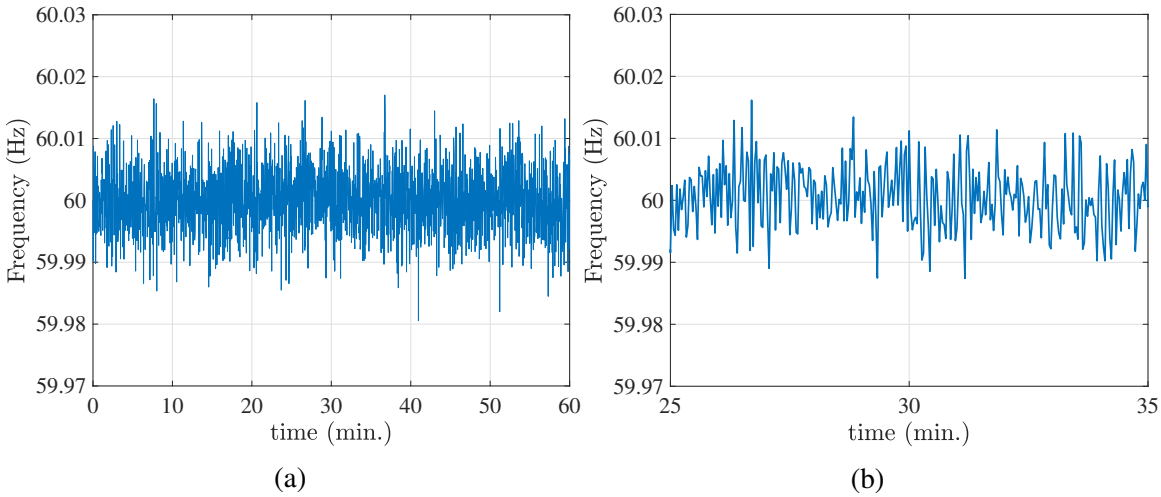



Figure 3.5: Frequency measurement (a) from $0$ min to $60$ min, and (b) zoom-in frequency measurement from $25$ min to $35$ min, under the **replay** attack to the frequency measurement of Area 1 launched at $30$ min.

via a simple tuning procedure, as follows. The adversaries may first force the sensor to report to the control center the scheduled tie-line flow plus a scaled version of actual flow deviation, i.e., $p_{\text{sch}} + \lambda \Delta p$ with an arbitrary chosen $\lambda$, as opposed to the actual flow measurement $p_{\text{sch}} + \Delta p$. Then the attackers can gradually tune $\lambda$ such that the frequency exhibits unstable/oscillatory behavior. In the four-area system, the scalar $\lambda$ is $-0.89$, and the attack starts at the $10th$ minute. Based on the scaled flow measurement $\Delta p$, the control command is computed according to the AGC control law, and the load reference setpoint of Generators $1$, $5$ and $6$ are changed accordingly. As evident from Fig 3.9(a), the closed-loop system is unstable and the frequency grows in an unbounded fashion.

Now we observe the process of destabilization attack from the perspective of the system operator. Suppose that the system operator keeps monitoring the reported frequency and tie-line flow measurements at the balancing authority of Area 1. Then, Fig. 3.9(b) and Fig. 3.9(d) are what the operator can observe from the $8th$ minute to the $20th$ minute. The operator might not realize the anomaly until around the $16th$ minute at which time several

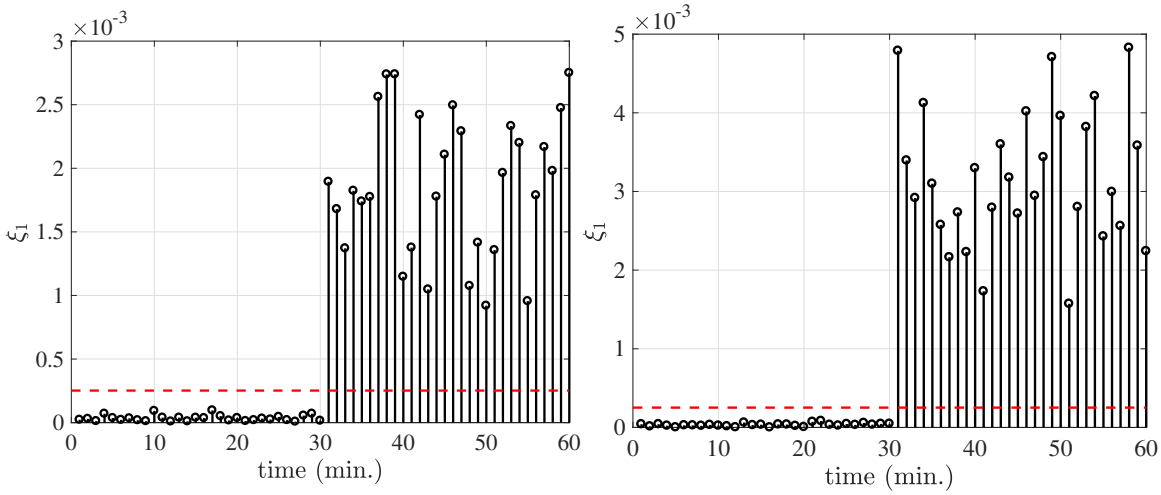



Figure 3.6: The evolutions of indicator $\xi_1^{\mathrm{j}}$ under the **replay** attack to the (a) **frequency** measurement and (b) **tie flow** measurement of **Area 1** starting at 30 min.

samples of frequency exceed the upper limit of the normal frequency range. However, the proposed approach can detect the destabilization attack between the $10th$ minute and $11th$ minutes, as we can see from Fig. 3.10.

One might wonder if the ACE will always ultimately exceed its limits under a destabilization attack, in which case the operator will notice it anyway, thereby rendering the proposed approach superfluous. The answer is that there are sophisticated destabilization attacks where the ACE might not exhibit instability. Consider an attack template which is the same as earlier, except that $\lambda$ is set to $-0.84$. This results in the frequency measurement in Area 1 shown in Fig. 3.11(a). It can be seen that though some frequency samples exceed the constraint occasionally, these violations might be attributed to measurement error, and consequently be ignored by the operators since the frequency reverts to the normal range after several abnormal samples. In contrast the indicator signals under watermarking exhibit the consecutive spikes shown in Fig. 3.11(b) thereby detecting the attack on Area 1. It can be seen that, in contrast to performing fine adjustments of the

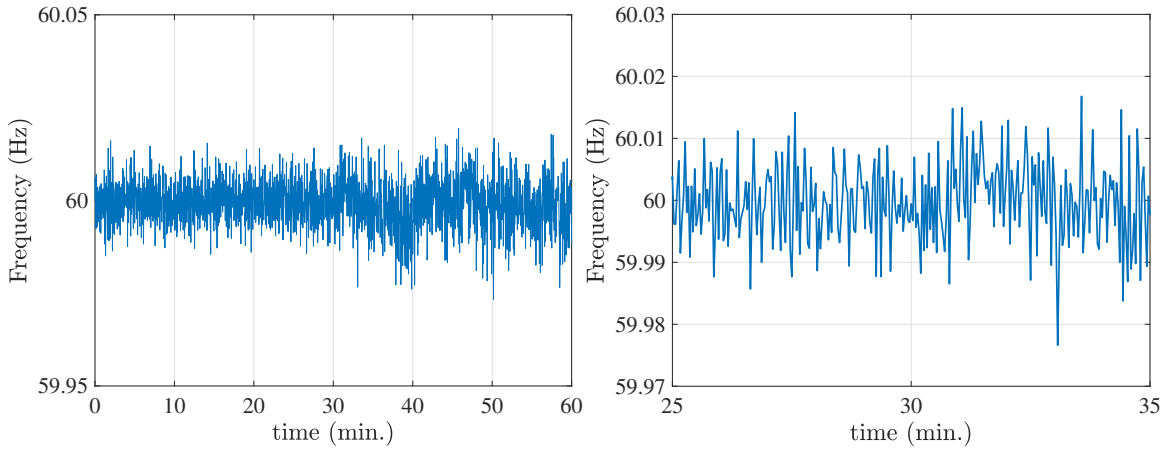



Figure 3.7: Frequency measurement in Area 1 (a) from 0 min to 60 min and (b) zoom-in frequency measurement from 25 min to 35 min, under the **noise-injection** attack to the frequency measurement of Area 1 launched at 30 min.

system frequency, the energy consumed by AGC drives the frequency to oscillate within a wider range compared to the frequency before the cyber attack.

### 3.4.2 Performance Validation of the Proposed Algorithm on the NPCC 140-bus System

*1) NPCC 140-bus System Description and Parameter Setting of the Proposed Algorithm:* This benchmark system has 140 buses and 48 generators, and its raw parameters are available in the file named "`datanp48.m`" in PST [60]. In this chapter, the NPCC 140-bus system is divided into two areas based on the geographical locations of buses [62], [63]. Accordingly, eight transmission lines are chosen as the tie lines connecting the two areas; they are Line 78-81 [2], 76-77, 66-134, 67-138, 105-111, 105-106, 105-107, and 105-101. There are 9 generators in AGC loop, which are Generators 1, 2, 18, 19, 20, 21, 22, 23, and 24. The system matrices $A$, $B$, and $C$ are extracted by PST. In Area 1, we add a discrete PI feedback loop, where both of the proportional gain constant and the inte-

[2]Line 78-81 represents the transmission line from Bus 78 to 81.

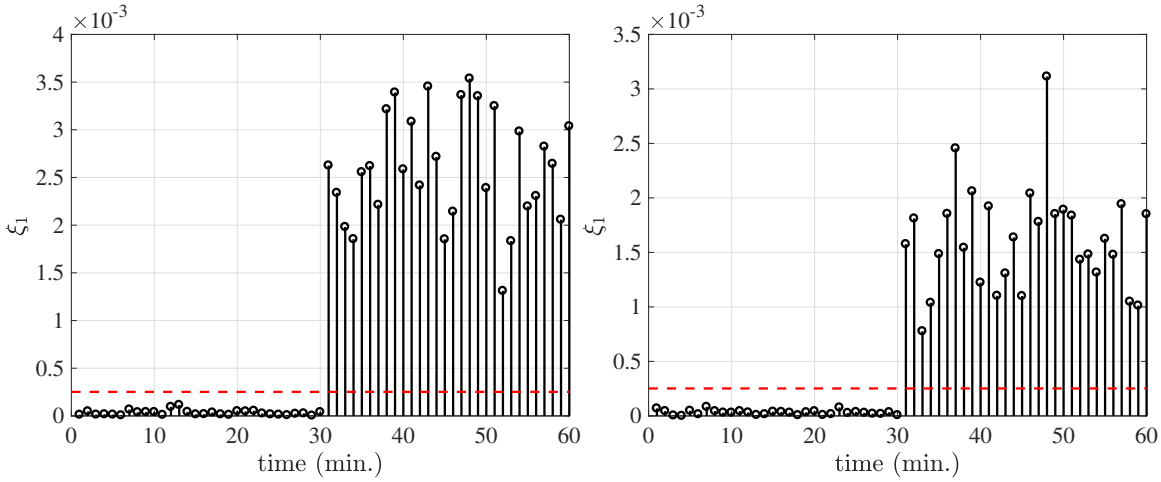



Figure 3.8: The evolutions of indicator $\xi_1^{\mathrm{j}}$ under the **noise-injection** attack on (a) the **frequency** measurement, and (b) the **tie flow** measurement, of **Area 1** starting at 30 min.

gral gain are set to $-0.0451$. The variance parameter of the load deviations $\sigma_{\mathrm{L}}^2 = 0.001$ is chosen such that the frequency fluctuates within the normal range, i.e., $60 \pm 0.03$ Hz [34] with high probability. The thresholds $\eta_1 = 0.0045$ with $\eta_1^{\infty} = 6.3935 \times 10^{-4}$ and $\kappa' = 7$. The settings of $\tau$, $\kappa_i$, $\sigma_f^2$, $Q'$, $T$, $\sigma_e$, and SNR of deviation measurements of tie-line flow are the same as those in Section 3.4.1.

Again, we examine the impact of the private injection on the performance of the AGC in terms of frequency regulation. Figure 3.12 records the control commands from AGC. It shows that the control command with the private injection does not deviate significantly from the control policy-specified input.

*2) Detection of Three Types of Cyber Attack:* In this section, we demonstrate the efficacy of the proposed approach for detecting the three types of cyber attack defined in Sec. 3.2.4, through simulations on the NPCC 140-bus power system. We first validate the performance of the proposed algorithm in terms of detecting the replay attack and the noise-injection attack on the frequency measurement in the NPCC 140-bus system. Both

types of cyber attack begin at $30$ min. As shown in Fig. 3.13, both types of cyber attack are identified successfully between the $30th$ and $31st$ minutes. We next deal with securing the NPCC 140-bus system from the destabilization attacks. The destabilization attack on the flow measurement of Line 78-81 starts at the $5th$ min, resulting in a growing trend of frequency deviation as shown in Fig. 3.14(a). The scalar $\lambda$ defined in Section 3.4.1 is $-5$. The evolution of $\xi_1^j$ over time is presented in Fig. 3.14(b). It is observed that consecutive spikes exceed the threshold after the $6th$ min, suggesting that the attack appears between the $5th$ and $6th$ minutes.

### 3.4.3 Comparison with the Regression-based Approach

In this section, we compare the dynamic-watermarking approach with the regression-based approach [35] in the four-area system described in Section 3.4.1. In Reference [35], the cyber attacks on AGC are detected based on the following linear regression which characterizes the relationship between frequency (output) and load fluctuations (input), i.e.,

$$\hat{\omega}(k) \approx \sum_{h=0}^{H-1} \boldsymbol{\alpha}_h \boldsymbol{u}_{\text{load}}(k-h). \tag{3.19}$$

Equation (3.19) assumes that the current frequency deviation $\hat{\omega}(k)$ is a linear combination of the current load fluctuation vector $\boldsymbol{u}_{\text{load}}(k)$ and the past load fluctuation vectors, i.e., $\boldsymbol{u}_{\text{load}}(k-h)$ for $h = 1, 2, \ldots, H-1$. $\boldsymbol{\alpha}_h$ is the combination coefficient vector, and the integer $H$ is the order of the linear regression, which is an adjustable factor. The state-space version of (3.19) can be identified by the MATLAB System Identification Toolbox [64]. The attack is detected by checking the discrepancies between the reported frequency measurement $\omega(k)$ and its estimated value $\hat{\omega}(k)$. Hence, the indicator $\gamma(k)$ in the regression-based framework is defined by $\gamma(k) := \omega(k) - \hat{\omega}(k)$. An alarm is triggered if

$$|\gamma(k)| > \eta', \tag{3.20}$$

where $\eta'$ is the maximal $|\gamma(k)|$ under the normal condition or during the training stage [35].

However, the regression-based approach may not detect the following cyber attacks on AGC. The linear regression (3.19) can be learned by a sophisticated adversary, based on the input-output measurements. Then, the threshold $\eta'$ can be approximately estimated. Finally, the actual measurement can be replaced by the following malicious measurement sequence $\omega_a$ without being detected by the criteria (3.20):

$$\omega_{\mathrm{a}} = \hat{\omega} - \eta'. \tag{3.21}$$

Next, we test the performance of the proposed algorithm in terms of detecting the attack defined in (3.21). The attack with $\eta' = 9.024 \times 10^{-5}$ starts at 30 min in the four-area system. Fig. 3.15(a) presents the evolution of the $|\gamma(t)|$ defined in the regression-based approach. It can be seen that $|\gamma(t)|$ does not exceed the threshold $\eta'$ after the $30th$ minute, although it keeps being close to $\eta'$. In contrast, the indicator under the proposed method exceeds a predefined threshold consecutively after the $30th$ minute, suggesting that the attack defined in (3.21) can still be identified successfully, as shown in Fig. 3.15(b). Note that, although the regression-based approaches are not guaranteed to detect any cyber attacks, it can serve as a screening tool for the proposed framework.

### 3.4.4 Robustness Test

Due to the effect of deadband in generation units, some generators might not be responsive to small change in setpoints, and these generators are termed as non-responsive generators (NRGs). The number of non-responsive generators in AGC may impact the performance of the proposed framework. In order to investigate such an impact, we first define a performance indicator $\theta$. In the context of Section 3.4.2, where the cyber attack (replay/injection) starts from the $30th$ min, the performance indicator $\theta$ can be defined as

follows:

$$\theta = \frac{\min_p \xi_1^p}{\max_q \xi_1^q} \quad \forall p \in \{31, 32, \ldots, 60\} \wedge q \in \{1, 2, \ldots, 30\}, \tag{3.22}$$

where the numerator suggests the minimal value of $\xi_1^j$ under the attack, while the denominator is the maximal value of $\xi_1^j$ under the normal condition. If the ratio $\theta > 1$, $\xi_1^j$ under the attack can be linearly separated from that under the normal condition by setting a threshold, i.e, the attack can be detected by the proposed method.

In Section 3.4.2, we assume that all $9$ generators in the AGC loop are responsive to small changes in their setpoints. Here, we increase the number of the NRGs from $0$ to $5$, and compute the corresponding performance indicators $\theta$ under the replay attack and the noise-injection attack. The results are presented in Table 3.1. It is seen that both $\theta_R$ and $\theta_I$ are greater than $1$ under all scenarios, suggesting that the replay attack and the noise injection attack can still be detected, even though some non-responsive generators exist.

Table 3.1: The Impact of Number of Responsive Generators ($\theta_R$: $\theta$ under the Replay Attack; $\theta_I$: $\theta$ under the Injection Attack)

| % of NRGs | NRG Index | $\theta_{\text{R}}$ | $\theta_{\text{I}}$ |
|---|---|---|---|
| $0/9$ | N/A | 6.5039 | 7.1692 |
| $1/9$ | $24$ | 6.4115 | 7.0572 |
| $2/9$ | $23, 24$ | 6.3088 | 6.9370 |
| $3/9$ | $22, 23, 24$ | 6.1079 | 6.6742 |
| $4/9$ | $21, 22, 23, 24$ | 6.1480 | 6.7020 |
| $5/9$ | $20, 21, 22, 23, 24$ | 6.0231 | 6.5594 |

## 3.5 Concluding Remarks

In this chapter, an online framework to detect cyber attacks on AGC is proposed. In the proposed defense framework, a theoretically rigorous attack detection algorithm based on dynamic watermarking is developed to detect sophisticated adversaries equipped with

extensive and even complete knowledge of the physical and statistical models of the power system. The proposed framework needs no hardware update of the generation units. The efficacy of the proposed framework is demonstrated in a four-area synthetic power system and a 140-bus power system. Future work will investigate the scaling up of the proposed method to larger-scale power systems.

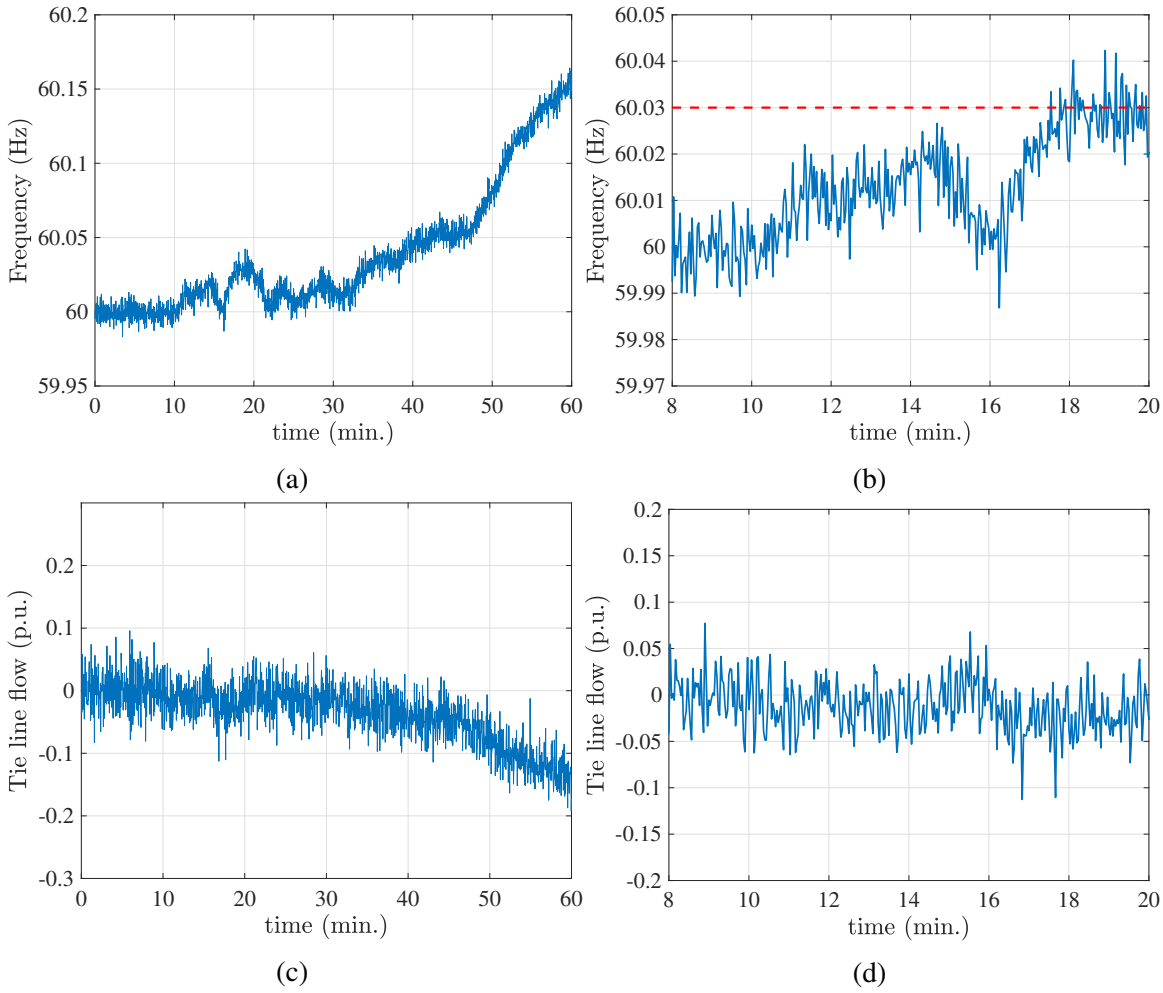



Figure 3.9: Frequency measurement in Area 1 from 0 min to 60 min (a) and its zoom-in frequency measurement (b), tie-line flow measurement in Area 1 from 0 min to 60 min (c), and its zoom-in tie-line flow measurement (d) under the **destabilization** attack to the tie-line flow measurement of Area 1 launched at 10 min.

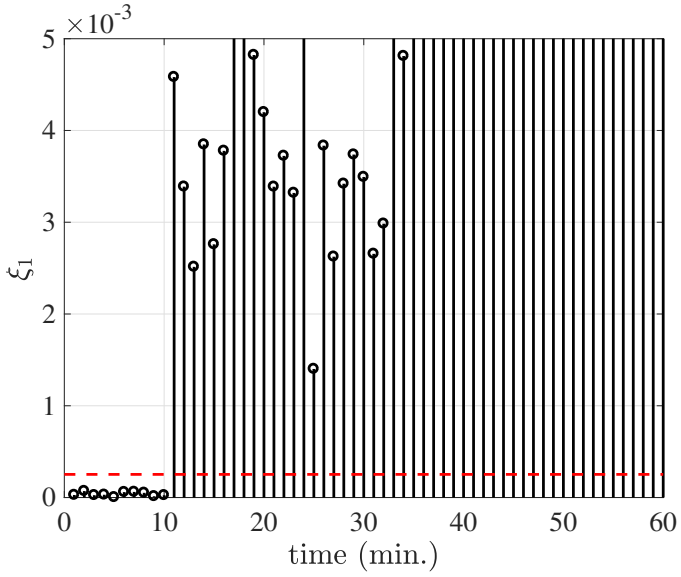



Figure 3.10: The evolution of indicator $\xi_1^j$ under the **destabilization** attack on the **tie flow** measurement of **Area** 1 starting at 10 min.

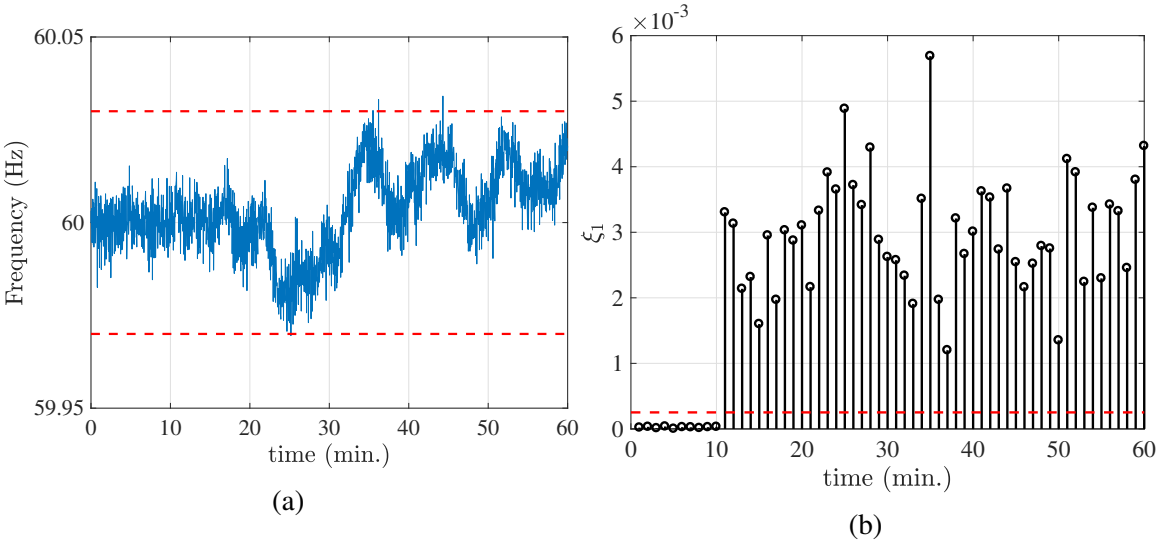



Figure 3.11: Frequency measurement under **destabilization attack** to the **tie-line flow** measurement in Area 1 (a), and the evolution of corresponding $\xi_1^j$ (b).

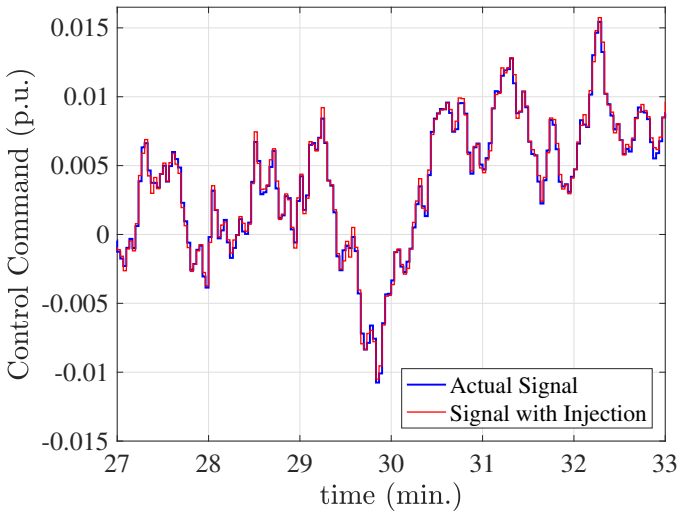



Figure 3.12: Control command comparison in the NPCC 140-bus power system.

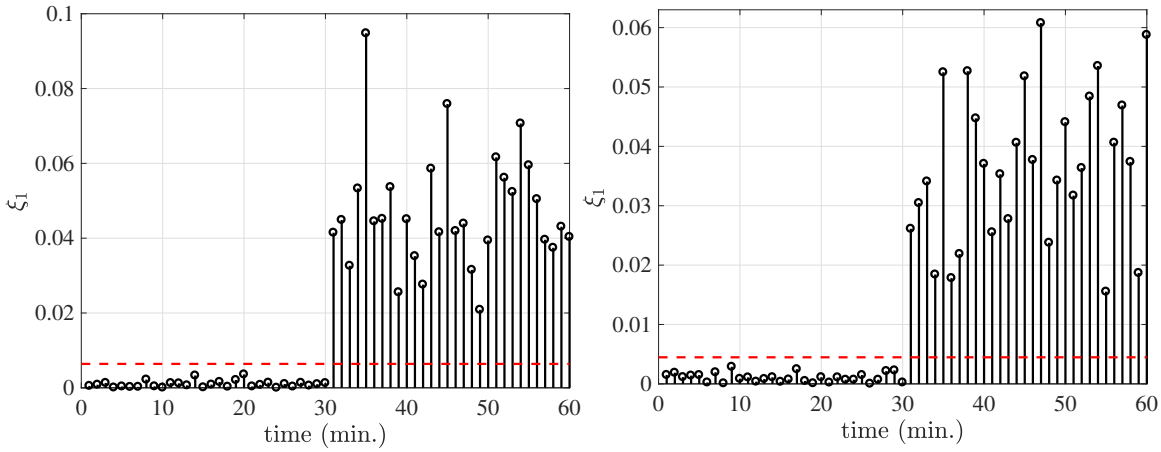
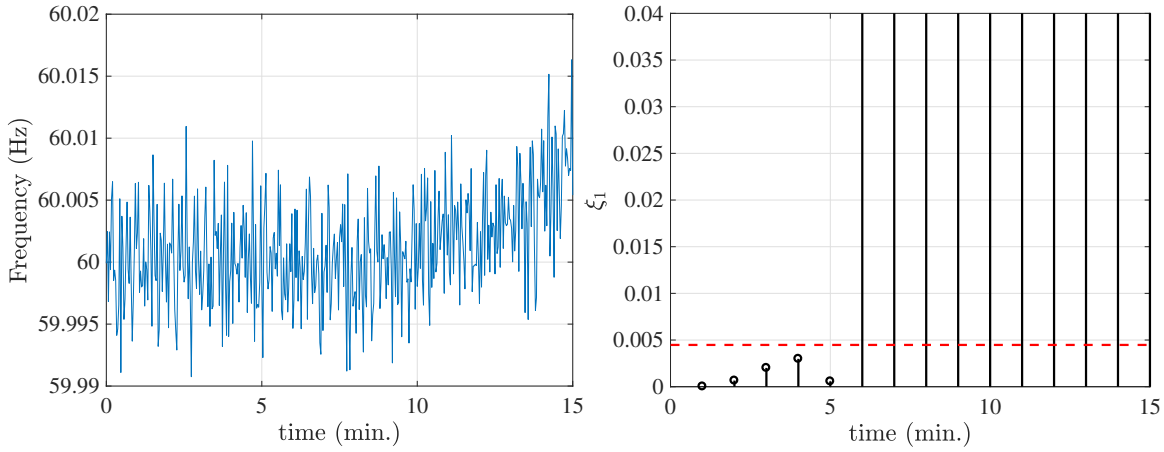
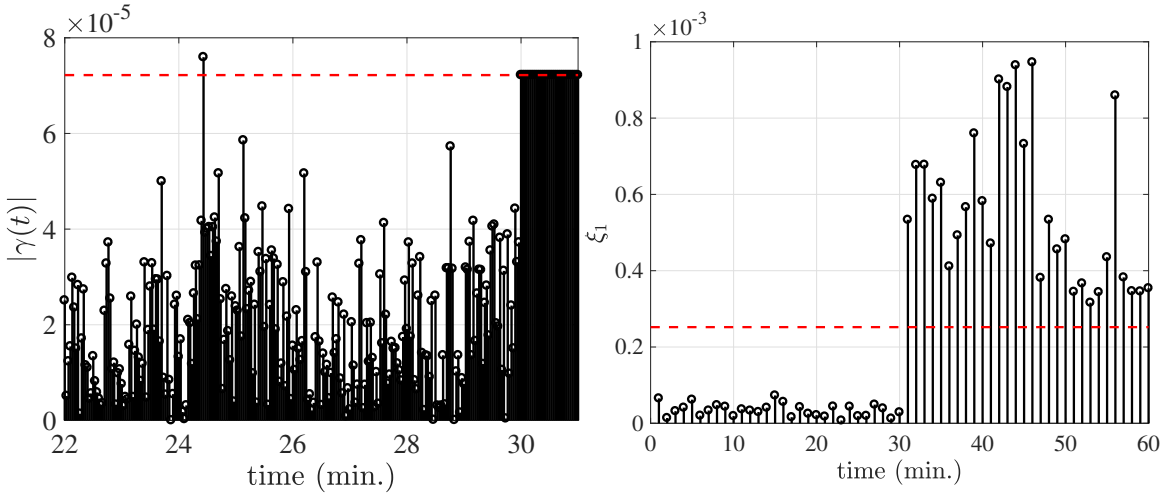



Figure 3.13: The evolutions of indicator $\xi_1^j$ under (a) the replay attack and (b) the injection attack on the NPCC 140-bus power system.




(a) (b)

Figure 3.14: (a) The time-domain frequency measurements under the destabilization attack; (b) the evolutions of indicator $\xi_1^j$ under the destabilization attack.




(a) (b)

Figure 3.15: The evolutions of (a) $|\gamma_(t)|$ and (b) $\xi_i^j$ over time under the attack defined in (3.21).

# 4. A NEURAL LYAPUNOV APPROACH TO ASSESSING NETWORKED MICROGRIDS TRANSIENT STABILITY[1]

## 4.1 Motivation

The past decade has witnessed increasing deployment of distributed energy resources (DERs) in the electric distribution grid. DERs play a crucial role of decarbonizing the energy sector and enhancing the resilience of the grid. However, deepening penetration of DERs leads to unprecedented complexity for distribution system operation in monitoring, control, and protection. One promising architecture to manage the massive integration of DERs is to reconfigure the distribution system as *networked microgrids* shown in Figure 4.1. A microgrid packages interconnected Distributed Generation Units (DGUs) and loads which are regulated locally by the Microgrid Central Controller (MGCC) [5]. The microgrid has a power-electronic (PE) interface [5] that physically connects to its host distribution system via a point of common coupling (PCC). Microgrids are networked with each other through PCCs and distribution lines. With such a configuration, instead of managing massive DGUs at grid edges, a Distribution System Operator (DSO) only needs to coordinate a few PE interfaces of microgrids [5], by which the system management complexity at the DSO level is significantly reduced. Reference [65] reports a real-world demonstration of networked microgrids.

Given the microgrid-based distribution system, a key function of its Distribution Management System (DMS) is to assess the physical security of networked microgrids. Functionally speaking, this task should be comprised of both static security assessment (SSA) and transient stability assessment (TSA). The SSA scrutinizes if physical variables of net-

[1]This chapter is from "A Neural Lyapunov Approach to Assessing Networked Microgrids Transient Stability" by Tong Huang, Sicun Gao and Le Xie, which has been submitted to *IEEE Transactions on Smart Grid*.

worked microgrids in the steady-state time scale are within predefined normal operating ranges. It is typically considered as optimization constraints when researchers develop coordination strategies of networked microgrids [66] for grid resilience enhancement and economical efficiency maximization. The TSA examines the dynamic behaviors of networked microgrids in a faster time scale. The TSA tool aims to characterize (large) disturbances that the networked microgrids can tolerate. Such characterization allows for efficient design and planning of the microgrid-based distribution systems [4], and it also enables a DSO to maintain situational awareness in real-time operation [4]. This chapter focuses on assessing transient stability of *networked* microgrids. Such a topic concerns the DSO, because excessive energy transactions among microgrids may lead to stability issues, even though each individual microgrid is stabilized by its local MGCC [5].

There are several approaches to the design of TSA tools for networked microgrids. One approach is to tailor the TSA development in bulk transmission systems for microgrid application. A prevailing TSA method in transmission systems is based on time-domain simulation. In such a method, system security is evaluated by examining the simulated system responses to all credible contingencies. This method can be tailored to screen out critical contingencies in networked microgrids. However, it cannot certify stability rig-

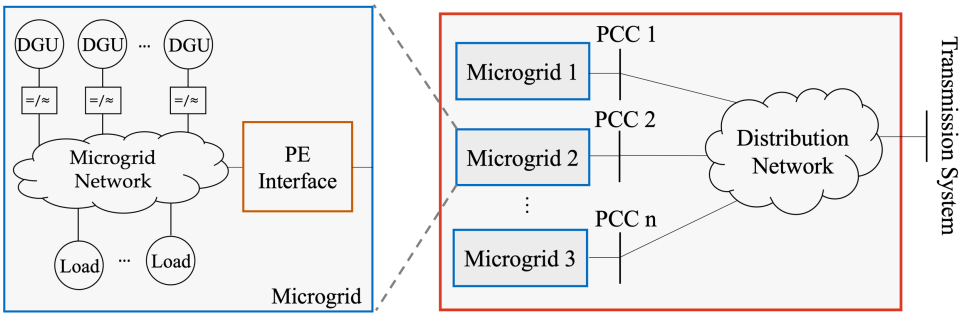



Figure 4.1: A microgrid-based distribution system: inside the left blue box shows the physical structure of a microgrid.

orously, as by definition, stability [67] requires one to examine system responses under infinite number of disturbances, which is not possible for simulation-based time-domain methods. Another TSA method developed for the transmission system is the energy function method [68, 69]. By assuming transmission lines are lossless, this method aims to construct an energy function that can certify stability. While the lossless-line assumption is plausible in transmission systems, it does not hold in networked microgrids due to large R/X ratios of distribution lines [5], thereby resulting in non-existence of the energy function in networked microgrids [68]. Reference [68] constructs a quadratic Lyapunov function which can be used for TSA of a power system with line loss. However, the DSO tool developed based on [68] may be overly conservative. Besides the TSA tools developed for transmission systems, References [5, 70] develop stability assessment tools specifically for networked microgrids. Reference [70] has proposed a framework capable of assessing the small-signal stability of networked microgrids in a distributed manner, but it cannot certify the stability when large disturbances occur. Reference [5] utilizes linear matrix inequalities (LMIs) in order to certify global asymptotic stability of networked microgrids. The framework proposed in [5] requires a special form of interface dynamics and it cannot characterize disturbances that can be tolerated by networked microgrids when global asymptotic stability is not guaranteed.

In this chapter, we develop a novel machine learning-inspired TSA tool for networked microgrids. Assessing the transient stability of networked microgrids is formulated as a problem of computing the security region. We leverage neural networks to learn a local Lyapunov function in the state space. The optimal security region is estimated based on the Lyapunov function learned, and is used for characterizing disturbances that the networked microgrids can tolerate. The proposed TSA tool has the following merits: 1) It can provide less conservative characterization of disturbances that can be tolerated by networked microgrids, compared with methods based on quadratic Lyapunov functions; and 2) It can

assess the transient stability of networked microgrids with heterogeneous interface dynamics. Building upon our preliminary work [4], this chapter substantially expands the scope by the following improvement: 1) We refine the Lyapunov risk, allowing for assessing transient stability of networked microgrids with mixed interface dynamics; 2) We develop a prerequisite checking condition to ensure the existence of Lyapunov functions; 3) We present a tuning procedure for the user-defined parameters in the proposed algorithms; 4) We propose an algorithm for estimating the largest security region given a Lyapunov function learned; and 5) The proposed algorithm is tested in networked microgrids with mixed interface dynamics and a realistic 123-node feeder.

The rest of this chapter is organized as follows: Section 4.2 describes the dynamics of networked microgrids; Section 4.3 presents the Neural Lyapunov method to TSA; and Section 4.4 tests and validates the tool in three numerical experiments; and Section 4.5 concludes the chapter and points out future direction.

## 4.2 Dynamics of Microgrids with PE Interfaces

With the physical configuration of the networked microgrids in Figure 4.1, the dynamics that a microgrid exhibits at the DSO-level control are mainly determined by the control strategy deployed at its PE interface [5,70]. This section characterizes the dynamics of the PE interfaces by presenting a typical control scheme deployed at the microgrid interfaces. Based on the interface dynamics, we provide a mathematical description for the dynamics of networked microgrids.

### 4.2.1 PE Interface Dynamics

The typical components of a PE interface are summarized in Figure 4.2. Next, we describe the dynamics of the PE interface by presenting the dynamics of each component in Figure 4.2.

*1) Power Controller:* As shown in Figure 4.2, the power controller includes two func-

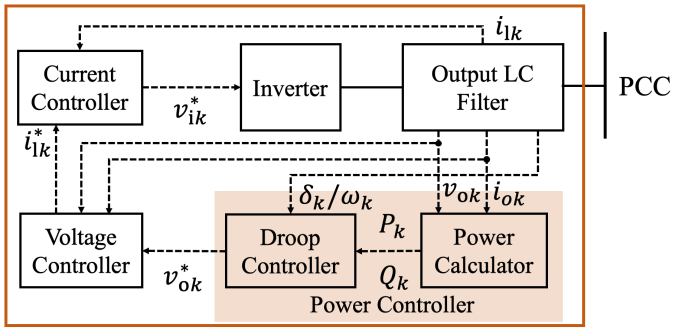



Figure 4.2: Block diagram of the $k$-th PE interface

tional blocks: a power calculator, and a droop controller. The power calculator takes as inputs the instantaneous voltage $v_{ok}$ and current $i_{ok}$ from the LC filter, and it aims to compute the fundamental components of real and reactive power $P_k$ and $Q_k$ of the $k$-th interface. The dynamics of the power calculator can be described by [71]

$$\dot{P}_k = -\omega_c P_k + \omega_c (v_{odk} i_{odk} + v_{oqk} i_{oqk}) \tag{4.1a}$$

$$\dot{Q}_k = -\omega_c Q_k + \omega_c (v_{oqk} i_{odk} - v_{odk} i_{oqk}) \tag{4.1b}$$

where $\omega_c$ denotes the cut-off frequency of the low-pass filters in the power calculator [71]; and $v_{odk}$ ($i_{odk}$) and $v_{oqk}$ ($i_{oqk}$) are the direct and quadrature components of $v_{ok}$ ($i_{ok}$). The droop controller leverages some local signals as the power balance indicators [5], and the it tunes the interface response according to the measurements of these signals. Common selections of these local signals include frequency, voltage magnitude and voltage angle that are measured at the microgrid PCC. Specifically, the *frequency droop control* takes the terminal frequency $\omega_k$ as the balance indicator for real power [5]. Such a control strategy requires no communication between PE interfaces and it introduces the following dynamics:

$$\dot{\delta}_k = \omega_k - \omega_n, \quad M_{fk}\dot{\omega}_k = -D_{fk}(\omega_k - \omega_n) + P^*_k - P_k \tag{4.2}$$

where $\omega_{\rm n}$ denotes the nominal frequency; $M_{{\rm f}k}$ and $D_{{\rm f}k}$ are control parameters for the frequency droop controller; and $P_k^*$ and $Q_k^*$ are dispatched by the DSO. The *angle droop control* considers the voltage phase angle $\delta_k$ as the balance indicator [5,72,73]. Though the angle droop control requires communication, it provides better frequency regulation [72], compared with the frequency droop control. The angle droop control will introduce the following dynamics:

$$M_{{\rm a}k}\dot{\delta}_k + (\delta_k - \delta_k^*) = D_{{\rm a}k}(P_k^* - P_k), \quad \omega_k = \dot{\delta}_k + \omega_{\rm n} \tag{4.3}$$

where $M_{{\rm a}k}$ and $D_{{\rm a}k}$ denote control parameters of the angle droop controllers; and $\delta_k^*$ and $P_k^*$ are dispatched by the DSO. Besides, the droop controller tunes the setpoint $v_{{\rm o}k}^*$ of the voltage controller in Figure 4.2 according to

$$M_{{\rm v}k}\dot{v}_{{\rm od}k}^* = D_{{\rm v}k}(Q_k^* - Q_k) - (v_{{\rm od}k}^* - E_k^*), \quad v_{{\rm oq}k}^* = 0 \tag{4.4}$$

where $v_{{\rm od}k}^*$ and $v_{{\rm oq}k}^*$ are the direct and quadrature components of $v_{{\rm o}k}^*$, respectively; and $E_k^*$, $Q_k^*$ are dispatched by the DSO.

*2) Voltage and Current Controllers:* The dynamics of the voltage and current controllers in Figure 4.2 can be described by the following differential and algebraic equa-

tions [71]:

$$\dot{\xi}_{\mathrm{d}k} = v^*_{\mathrm{od}k} - v_{\mathrm{od}k}, \quad \dot{\xi}_{\mathrm{q}k} = v^*_{\mathrm{oq}k} - v_{\mathrm{oq}k}, \tag{4.5a}$$

$$\dot{\psi}_{\mathrm{d}k} = i^*_{\mathrm{ld}k} - i_{\mathrm{ld}k}, \quad \dot{\psi}_{\mathrm{q}k} = i^*_{\mathrm{oq}k} - i_{\mathrm{lq}k}, \tag{4.5b}$$

$$i^*_{\mathrm{ld}k} = K_{\mathrm{iv}k}\xi_{\mathrm{d}k} + F_k i_{\mathrm{od}k} + K_{\mathrm{pv}k}(v^*_{\mathrm{od}k} - v_{\mathrm{od}k}) - \omega_{\mathrm{n}} C_{\mathrm{f}k} v_{\mathrm{oq}k} \tag{4.5c}$$

$$i^*_{\mathrm{lq}k} = K_{\mathrm{iv}k}\xi_{\mathrm{q}k} + F_k i_{\mathrm{oq}k} + K_{\mathrm{pv}k}(v^*_{\mathrm{oq}k} - v_{\mathrm{oq}k}) + \omega_{\mathrm{n}} C_{\mathrm{f}k} v_{\mathrm{od}k} \tag{4.5d}$$

$$v^*_{\mathrm{id}k} = K_{\mathrm{ic}k}\psi_{\mathrm{d}k} + K_{\mathrm{pc}k}(i^*_{\mathrm{ld}k} - i_{\mathrm{ld}k}) - \omega_{\mathrm{n}} L_{\mathrm{f}k} i_{\mathrm{lq}k} \tag{4.5e}$$

$$v^*_{\mathrm{iq}k} = K_{\mathrm{ic}k}\psi_{\mathrm{q}k} + K_{\mathrm{pc}k}(i^*_{\mathrm{lq}k} - i_{\mathrm{lq}k}) + \omega_{\mathrm{n}} L_{\mathrm{f}k} i_{\mathrm{ld}k} \tag{4.5f}$$

where $\xi_{\mathrm{d}k}$ and $\xi_{\mathrm{q}k}$ are state variables of the voltage controller; $\psi_{\mathrm{d}k}$ and $\psi_{\mathrm{q}k}$ are state variables of the current controller; $K_{\mathrm{iv}k}$, $F_k$, and $K_{\mathrm{pv}k}$ are control parameters of the voltage controller; $C_{\mathrm{f}k}$ and $L_{\mathrm{f}k}$ are capacitance and inductance of the output LC filter; $i^*_{\mathrm{ld}k}$, $i^*_{\mathrm{lq}k}$ are the setpoints of the current controller; and $v^*_{\mathrm{id}k}$, $v^*_{\mathrm{iq}k}$ are the setpoints of the inverter in Figure 4.2.

*3) Output Filter:* With the switching dynamics ignored in the inverter, we have $v^*_{\mathrm{id}k} = v_{\mathrm{id}k}$ and $v^*_{\mathrm{iq}k} = v_{\mathrm{iq}k}$, where $v_{\mathrm{id}k}$ and $v_{\mathrm{iq}k}$ are two state variables of the output filter associated with the $k$-th interface. The following differential equations describe the dynamics of the output filter associated with the $k$-th PE interface [71]:

$$L_{\mathrm{f}k}\dot{i}_{\mathrm{ld}k} = -r_{\mathrm{f}k} i_{ld} + \omega_k L_{\mathrm{f}k} i_{\mathrm{lq}k} + v_{\mathrm{id}k} - v_{\mathrm{od}k} \tag{4.6a}$$

$$L_{\mathrm{f}k}\dot{i}_{\mathrm{lq}k} = -r_{\mathrm{f}k} i_{lq} + \omega_k L_{\mathrm{f}k} i_{\mathrm{ld}k} + v_{\mathrm{iq}k} - v_{\mathrm{oq}k} \tag{4.6b}$$

$$C_{\mathrm{f}k}\dot{v}_{\mathrm{od}k} = \omega_k C_{\mathrm{f}k} v_{\mathrm{oq}k} + i_{\mathrm{ld}k} - i_{\mathrm{od}k} \tag{4.6c}$$

$$C_{\mathrm{f}k}\dot{v}_{\mathrm{oq}k} = \omega_k C_{\mathrm{f}k} v_{\mathrm{od}k} + i_{\mathrm{lq}k} - i_{\mathrm{oq}k} \tag{4.6d}$$

where $r_{\mathrm{f}k}$ is the resistance of the output filter; and $v_{\mathrm{od}k}$, $v_{\mathrm{oq}k}$, $i_{\mathrm{od}k}$ and $i_{\mathrm{oq}k}$ are the variables

interfacing with the distribution system network.

Equations (4.1)-(4.6) define detailed dynamics of a PE interface. However, such detailed dynamics may be complicated for analytically assessing transient stability of the networked microgrids from the DSO perspective. Next, we simplify the microgrid interface model.

### 4.2.2 Simplified PE Interface Dynamics

In order to simplify the interface model, we assume that dynamics (4.1), (4.5), and (4.6) are stabilized fast. The simplified dynamics of the $k$-th interface are (4.2) or (4.3), and

$$M_{\mathrm{v}k}\dot{E}_k = D_{\mathrm{v}k}(Q_k^* - Q_k) - (E_k - E_k^*) \tag{4.7}$$

where $E_k = v_{\mathrm{od}k}^*$. In such a case, the variables interfacing with the distribution system network are $\delta_k$, $E_k$, $P_k$, and $Q_k$.

Here, we demonstrate that the simplified dynamics can approximate the behavior of the PE interface modeled with details. Consider a microgrid interface connecting to its host distribution system via a tie line. At the tie line, suppose that a three-phase-to-ground fault occurs at the 1st second and it is cleared 3 cycles later. Figure 4.3 shows the simulation of the microgrid interface response to the event based on the detailed model and the simplified model. It can be observed in Figure 4.3 that the simplified model can reflect the general trend of the response of the interface modeled with details. Therefore, we use the simplified dynamics to model the behaviors of the PE interfaces.

### 4.2.3 Networked Microgrid Dynamics

For the $n$ networked microgrids in Figure 4.1, without loss of generality, suppose that the angle droop control is deployed in the $k$-th microgrid's PE interface, where $k = 1, 2, \ldots, n$. Define $\delta_k' := \delta_k - \delta_k^*$ and $E_k' := E_k - E_k^*$. The simplified interface dynamics

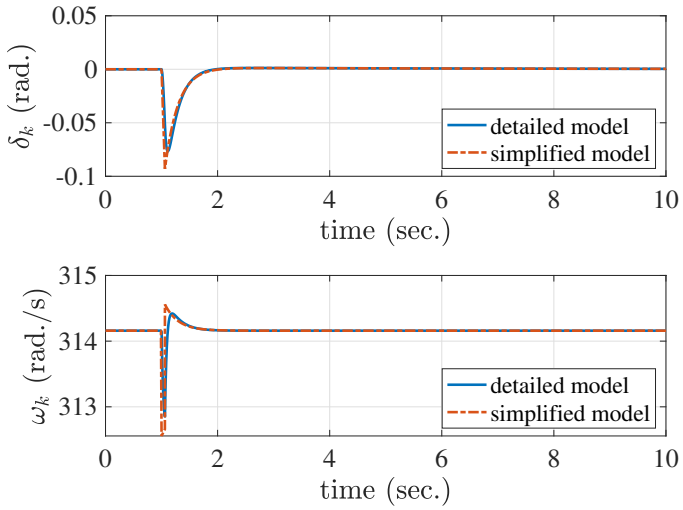



Figure 4.3: Comparison between the full and simplified microgrid interface dynamics: $\delta_k$ and $\omega_k$.

of the $k$-th microgrid are [5, 13, 70]

$$M_{\mathrm{ak}}\dot{\delta}'_k + \delta'_k = D_{\mathrm{ak}}(P^*_k - P_k) \tag{4.8a}$$

$$M_{\mathrm{vk}}\dot{E}'_k + E'_k = D_{\mathrm{vk}}(Q^*_k - Q_k). \tag{4.8b}$$

The $n$ microgrids are networked via distribution network which introduces constrains

$$P_k - G_{kk}E_k^2 - \sum_{i\neq k} E_k E_i Y_{ki}\cos\left(\delta_{ki} - \sigma_{ki}\right) = 0 \tag{4.9a}$$

$$Q_k + B_{kk}E_k^2 - \sum_{i\neq k} E_k E_i Y_{ki}\sin\left(\delta_{ki} - \sigma_{ki}\right) = 0, \forall k, \tag{4.9b}$$

where $\delta_{ki} = \delta_k - \delta_i$; $G_{kk} + \mathbb{j}B_{kk}$ is the $k$-th diagonal entry in the admittance matrix of the distribution network; and $Y_{ki}\angle\sigma_{ki}$ is the $(k, i)$-th entry of the admittance matrix. The steady-state values $\delta^*_k$, $E^*_k$, $P^*_k$ and $Q^*_k$ are designed based on economic dispatch and they

satisfy the following equality constrains:

$$P_k^* - G_{kk}E_k^{*2} - \sum_{i\neq k} E_k^* E_i^* Y_{ki} \cos\left(\delta_{ki}^* - \sigma_{ki}\right) = 0 \tag{4.10a}$$

$$Q_k^* + B_{kk}E_k^{*2} - \sum_{i\neq k} E_k^* E_i^* Y_{ki} \sin\left(\delta_{ki}^* - \sigma_{ki}\right) = 0, \forall k, \tag{4.10b}$$

where $\delta_{ki}^* = \delta_k^* - \delta_i^*$. Differential equations (4.8) with algebraic equations (4.9) characterize the dynamics of the $n$ networked microgrids, and their compact form is

$$\dot{\mathbf{x}} = \mathbf{f}(\mathbf{x}) \tag{4.11}$$

where $\mathbf{x} = [\delta_1', \delta_2', \ldots, \delta_n', E_1', E_2', \ldots, E_n']$; and $\mathbf{f}(\cdot)$ is determined by (4.8) and (4.9). Note that the equilibrium point $\mathbf{o}$ of the dynamic system (4.11) is the origin of the state space.

If $M_{\mathrm{v}k} \gg M_{\mathrm{a}k}$, the *time-scale separation* can be assumed [4, 5]. In such a case, the voltage deviation $E_k'$ evolves much slower than the phase angle deviation $\delta_k'$ and, therefore, $E_k'$ is assumed to be constant [5]. Furthermore, if only angular stability is of interest, the dynamics of the $n$ networked microgrids can be described by

$$M_{\mathrm{a}k}\dot{\delta}_k' + \delta_k' = D_{\mathrm{a}k}(P_k^* - P_k), \forall k, \tag{4.12}$$

where $P_k = G_{kk}E_k^{*2} + \sum_{i\neq k} E_k^* E_i^* Y_{ki} \cos\left(\delta_{ki}' + \delta_{ki}^* - \sigma_{ki}\right)$. The compact form of (4.12) can be also expressed as (4.11) where $\mathbf{x}$ and $\mathbf{f}(\cdot)$ should be revised accordingly. Besides, with the time-scale separation assumption, if the frequency droop control is deployed in the $j$-th microgrid, the $j$-th differential equation in (4.12) is replaced by

$$\dot{\delta}_j' = \omega_j', \quad M_{\mathrm{f}j}\dot{\omega}_j' + D_{\mathrm{f}j}\omega_j' = P_j^* - P_j$$

where $\omega'_j = \omega_j - \omega_{\mathrm{n}}$.

With the networked microgrids (4.11) and its equilibrium point $\mathbf{o}$, a DSO may have the following two questions [4]: 1) Is $\mathbf{o}$ asymptotically stable? 2) How "large" are the disturbances that the networked microgrids can tolerate? The transient stability assessment framework proposed in this chapter aims to answer these two questions.

## 4.3 Neural Lyapunov Methods

This section addresses two important questions from a DSO's perspective. We first point out the asymptotic stability of networked microgrids can be certified by the Lyapunov linearization method [67] and formulate the second DSO's question as the one of estimating a security region of networked microgrids. Then an optimal security region is estimated via learning a Lyapunov function. Finally, how to empirically tune the parameters of proposed algorithms is discussed.

### 4.3.1 Asymptotic Stability Check and Security Region

Given the networked microgrids (4.11) and its equilibrium $\mathbf{o}$, the Lyapunov linearization method [67] suggests the asymptotic stability of $\mathbf{o}$ can be determined by examining the linearized version of (4.11), i.e.,

$$\dot{\mathbf{x}} = A\mathbf{x}. \tag{4.13}$$

In (4.13), $A \in \mathbb{R}^{m\times m}$ is a system matrix, where $m$ is the length of the state vector $\mathbf{x}$. The system matrix $A$ is obtained by linearizing (4.11) around its equilibrium point $\mathbf{o}$ based on the linearization technique. Suppose that matrix $A$ has $m$ eigenvalues $\lambda_1, \lambda_2, \ldots, \lambda_m$. The equilibrium point $\mathbf{o}$ of (4.11) is asymptotically stable [67], if

$$\mathrm{Re}(\lambda_i) < 0 \quad \forall i = 1, 2, \ldots m. \tag{4.14}$$

Condition (4.14) answers the first question raised in Section 4.2.

For the second DSO's question, a *security region* can be leveraged to characterize the disturbances that the networked microgrids (4.11) operating at $\mathbf{o}$ are able to tolerate. The definition of a security region is as follows [4]:

**Definition 1.** *$\mathcal{S} \subseteq \mathbb{R}^m$ is a security region if*

$$\mathbf{x}(0) \in \mathcal{S} \Longrightarrow \mathbf{x}(\infty) = \mathbf{0}_m \wedge \forall t (t > 0 \implies \mathbf{x}(t) \in \mathcal{S}).$$

In Definition 1, $\mathbf{x}(0)$ is resulting from the microgrid interconnection-level events, say, topology changes of distribution system network, and one of the microgrids enters an islanded/grid-connected mode; and $\mathbf{0}_m$ denotes the origin of the state space with $m$ states. Definition 1 essentially says that the system trajectory starting in the security region $\mathcal{S}$ will stay in $\mathcal{S}$ and tends to the equilibrium point $\mathbf{o}$. The second DSO's question can be answered if such an security region is obtained.

A security region $\mathcal{S}$ can be estimated based on a system behavior-summary function, i.e., a Lyapunov function, in conjunction with the Local Invariant Set Theorem [67]. The Lyapunov function is given by the following definition [4]:

**Definition 2.** *A continuous differentiable scalar function $V(\mathbf{x})$ is a Lyapunov function, if, in a region $\mathcal{B}_u := \{\mathbf{x} \in \mathbb{R}^m | u > 0, \|\mathbf{x}\|_2^2 < u^2\}$, 1) $V$ is positive definite in $\mathcal{B}_u$, and 2) $\dot{V}$ is negative definite in $\mathcal{B}_u$.*

Once a legitimate Lyapunov function $V(\mathbf{x})$ becomes available, a region $\mathcal{S}_d$ can be found by

$$\mathcal{S}_d = \{\mathbf{x} \in \mathcal{B}_u | d > 0, V(\mathbf{x}) < d\}. \tag{4.15}$$

The region $\mathcal{S}_d$ is an invariant set due to the decreasing nature of the Lyapunov function $V(\mathbf{x})$. Besides, the Invariant Set Theorem [67] suggests that with the Lyapunov function

$V(\mathbf{x})$, a system trajectory $\mathbf{x}(t)$ starting in $\mathcal{S}_d$ converges to the origin of the state space. Therefore, the region $\mathcal{S}_d$ is a security region. In order to characterize the disturbances that the networked microgrids can tolerate, the remaining questions are: 1) How to find a legitimate Lyapunov function in a valid region $\mathcal{B}_u$; and 2) with a Lyapunov function valid in $\mathcal{B}_u$, how to make the security region $\mathcal{S}_d$ as large as possible by tuning $d$ in (4.15). These two questions are addressed in Sections 4.3-B and 4.3-C.

### 4.3.2 Learning Lyapunov Function from State Space

*1) Lyapunov Function with Neural-network Structure:* We assume that a Lyapunov function candidate is a neural network. The neural network has a hidden layer and an output layer. The input of the hidden layer is the state vector $\mathbf{x} \in \mathbb{R}^m$ and the output is a vector $\mathbf{v}_1 \in \mathbb{R}^p$ where $p$ is the number of neurons in the hidden layer. Function $g_1 : \mathbb{R}^m \to \mathbb{R}^p$ describes the relationship between $\mathbf{x}$ and $\mathbf{v}_1$ and its definition is

$$\mathbf{v}_1 = g_1(\mathbf{x}) := \texttt{tanh}(W_1\mathbf{x} + \mathbf{b}_1) \tag{4.16}$$

where $W_1 \in \mathbb{R}^{p\times m}$; $\mathbf{b}_1 \in \mathbb{R}^p$; and $\texttt{tanh}(\cdot)$ is an entry-wised hyperbolic function [4]. Furthermore, we define an intermediate vector $\mathbf{c}_1 = [c_{1,1}, c_{1,2}, \ldots, c_{1,p}]^\top$ for the hidden layer by $\mathbf{c}_1 = W_1\mathbf{x} + \mathbf{b}_1$. For the output layer, its input is vector $\mathbf{v}_1$ and its output is $V_{\boldsymbol{\theta}} \in \mathbb{R}$ which is interpreted as the Lyapunov candidate evaluated at vector $\mathbf{x}$. $V_{\boldsymbol{\theta}}$ is related with $\mathbf{v}_1$ via function $g_2 : \mathbb{R}^p \to \mathbb{R}$ defined by

$$V_{\boldsymbol{\theta}} = g_2(\mathbf{v}_1) := \tanh(W_2\mathbf{v}_1 + b_2) \tag{4.17}$$

where $W_2 \in \mathbb{R}^{1\times p}$; and $b_2 \in \mathbb{R}$. The intermediate variable $c_2$ associated with the output layer is defined by $c_2 = W_2\mathbf{v}_1 + b_2$. In sum, the Lyapunov function candidate is

$$V_{\boldsymbol{\theta}}(\mathbf{x}) = g_2(g_1(\mathbf{x})). \tag{4.18}$$

Denote by $\boldsymbol{\theta}$ the vector that consists of all unknown entries in $W_1$, $\mathbf{b}_1$, $W_2$, and $b_2$. The subscript of $V_{\boldsymbol{\theta}}$ indicates that the Lyapunov function candidate depends on $\boldsymbol{\theta}$.

*2) Lyapunov Risk Minimization:* We proceed to tune $\boldsymbol{\theta}$ such that $V_{\boldsymbol{\theta}}(\mathbf{x})$ in (4.18) meets the two conditions in Definition 2. Suppose that there are $q$ state vectors $\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_q$. Let set $\mathcal{X}$ collect these $q$ vector samples. To tune $\boldsymbol{\theta}$, we introduce a cost function called (empirical) Lyapunov risk, i.e.,

$$\begin{aligned} R_q(\boldsymbol{\theta}) = &\frac{\alpha}{q}\sum_{i=1}^{q}\left(\texttt{ReLU}(-V_{\boldsymbol{\theta}}(\mathbf{x}_i))\right) \\ &+ \frac{\beta}{q}\sum_{i=1}^{q}\Big(\texttt{ReLU}(\dot{V}_{\boldsymbol{\theta}}(\mathbf{x}_i)+\tau)\Big) + \gamma V_{\boldsymbol{\theta}}^2(\mathbf{0}_m) \end{aligned} \tag{4.19}$$

where the tunable parameters $\alpha$, $\beta$, $\gamma$ and $\tau$ are positive scalars; $\texttt{ReLU}(\cdot)$ denotes the rectified linear unit; and $\dot{V}_{\boldsymbol{\theta}}$ is given by [4]

$$\dot{V}_{\boldsymbol{\theta}} = \frac{\partial V_{\boldsymbol{\theta}}}{\partial \mathbf{x}}\mathbf{f}(\mathbf{x}) = \frac{\partial V_{\boldsymbol{\theta}}}{\partial c_2}\frac{\partial c_2}{\partial \mathbf{v}_1}\frac{\partial \mathbf{v}_1}{\partial \mathbf{c}_1}\frac{\partial \mathbf{c}_1}{\partial \mathbf{x}}\mathbf{f}(\mathbf{x}). \tag{4.20}$$

In (4.20), the dynamics $\mathbf{f}(\mathbf{x})$ is provided in (4.11);

$$\begin{aligned} &\frac{\partial V_{\boldsymbol{\theta}}}{\partial c_2} = 1 - V_{\boldsymbol{\theta}}^2; \frac{\partial c_2}{\partial \mathbf{v}_1} = W_2; \frac{\partial \mathbf{c}_1}{\partial \mathbf{x}} = W_1; \text{and} \\ &\frac{\partial \mathbf{v}_1}{\partial \mathbf{c}_1} = \text{diag}\left(1-\tanh^2(c_{1,1}), \ldots, 1-\tanh^2(c_{1,p})\right). \end{aligned}$$

The interpretation of the Lyapunov risk (4.19) is presented as follows. In (4.19), The

first "ReLU" term incurs positive penalty if $V_{\boldsymbol{\theta}}(\mathbf{x}_i)$ is negative. The second "ReLU" term results to positive penalty if $\dot{V}_{\boldsymbol{\theta}}(\mathbf{x}_i)$ is greater than $-\tau$. If the evaluation of $V_{\boldsymbol{\theta}}$ at the origin of the state space is not zero, the Lyapunov risk also increases according to (4.19). Parameters $\alpha$, $\beta$, $\gamma$ and $\tau$ determine the importance of the three terms of (4.19) and their tuning procedure is discussed in Section 4.3.4.

Given the training set $\mathcal{X}$, in order to find a Lyapunov function valid in $\mathcal{B}_u$, unknown parameters $\boldsymbol{\theta}$ should be chosen such that the Lyapunov risk $R_q(\boldsymbol{\theta})$ is minimized, viz.

$$\min_{\boldsymbol{\theta}} R_q(\boldsymbol{\theta}). \tag{4.22}$$

The gradient decent algorithm can be leveraged to solve (4.22). Algorithm 4 presents a procedure to update $\boldsymbol{\theta}$, where $\boldsymbol{\theta}_0$ is the initial guess of $\boldsymbol{\theta}$; $r \in \mathbb{Z}_+$ denotes the times of updating $\boldsymbol{\theta}$; and the positive scalar $\eta$ is the learning rate. Note that merely using Algorithm 4 to update $\boldsymbol{\theta}$ is not sufficient even with a large $r$. One reason is that $\mathcal{X}$ solely covers a finite number of training samples in $\mathcal{B}_u$. With the $\boldsymbol{\theta}$ obtained by Algorithm 4 based on $\mathcal{X}$, it is possible that one or both of the two conditions in Definition 2 are violated in some part of $\mathcal{B}_u$ that is not included in $\mathcal{X}$. This issue is addressed in Section 4.3.2.

**Algorithm 4** Lyapunov Risk Minimization

**function** `MinRisk`($\boldsymbol{\theta}_0, \mathcal{X}, \mathbf{f}, p, r, \eta, \alpha, \beta, \gamma, \tau$)
  $\boldsymbol{\theta} \leftarrow \boldsymbol{\theta}_0$
  **while** $i \leq r$ **do**
    Update $V_{\boldsymbol{\theta}}$ and $\dot{V}_{\boldsymbol{\theta}}$ by (4.18), (4.20) with $\boldsymbol{\theta}$
    Compute $R_{|\mathcal{X}|,\rho}(\boldsymbol{\theta})$ via (4.19) over $\mathcal{X}$
    $\boldsymbol{\theta} \leftarrow \boldsymbol{\theta} - \eta \nabla_{\boldsymbol{\theta}} R_{|\mathcal{X}|,\rho}(\boldsymbol{\theta})$; $i \leftarrow i + 1$
  **end while**
  **return** $\boldsymbol{\theta}$
**end function**

*3) Augment of Training Samples:* Here, we utilize the satisfiability modulo theories (SMT) solver [74] to analytically check if the function learned by `MinRisk` is a legitimate Lyapunov function. This is equivalent to searching for state vectors $\mathbf{x} \in \mathcal{B}_u$ that satisfy

$$(V_{\boldsymbol{\theta}}(\mathbf{x}) \leq 0 \vee \dot{V}_{\boldsymbol{\theta}} \geq 0) \wedge (\|\mathbf{x}\|_2^2 \geq l^2) \tag{4.23}$$

where $l$ is a small scalar; and $\|\mathbf{x}\|_2^2 \geq l^2$ is added for avoiding numerical issues of the SMT solver [75]. The state vectors $\mathbf{x} \in \mathcal{B}_u$ satisfy condition (4.23) are termed *counterexamples* which can be found by the SMT solver, such as `dReal` [74]. Denote by $\mathcal{C}$ the set that consists of the counterexamples found by the SMT solver. If $\mathcal{C}$ is not an empty set, the learned function is not a Lyapunov function and the richness of the training set $\mathcal{X}$ is enhanced by adding counterexamples in $\mathcal{C}$ to $\mathcal{X}$. The procedure of augmenting the training samples is presented in the "`AddSample`" function of Algorithm 5.

The function `LearnFunc` of Algorithm 5 summarizes the overall procedure of updating the unknown parameter $\boldsymbol{\theta}$ and augmenting the training set $\mathcal{X}$. In `LearnFunc`, $n_{\mathrm{i}}$ is the maximum iteration times defined by users.

**Remark:** The proposed method requires the availability of dynamics (4.11). The neural network (4.18) in this chapter is merely for the purpose of learning a Lyapunov function for (4.11), instead of identifying the networked microgrids dynamics (4.11).

### 4.3.3 Security Region Estimation Algorithm

Given a Lyapunov function $V_{\boldsymbol{\theta}^*}$ with its valid region $\mathcal{B}_u$, we proceed to tune $d$ in (4.15) so that the estimated security region is maximized. The optimal $d^*$ is determined by solv-

**Algorithm 5** Learning Lyapunov Function

**function** `AddSample`($\mathcal{X}, V_{\boldsymbol{\theta}}, \mathbf{f}, u$)
  $\kappa \leftarrow 1$
  Check (4.23) in $\mathcal{B}_u$ and find $\mathcal{C}$ by `dReal`
  **if** $\mathcal{C} = \emptyset$ **then** $\kappa \leftarrow 0$ ▷ No counterexamples found
  **else** $\mathcal{X} \leftarrow \mathcal{C} \cup \mathcal{X}$ ▷ Add counterexamples to $\mathcal{X}$
  **end if**
  **return** $\mathcal{X}, \kappa$
**end function**
**function** `LearnFunc`($\mathcal{X}, \boldsymbol{\theta}_0, \mathbf{f}, u, p, r, \eta, \alpha, \beta, \gamma, \tau, n_{\mathrm{i}}$)
  $\kappa \leftarrow 1; j \leftarrow 0$
  **while** $(\kappa = 1) \wedge (j \leq n_{\mathrm{i}})$ **do**
    $\boldsymbol{\theta} \leftarrow$ `MinRisk`$(\boldsymbol{\theta}_0, \mathcal{X}, \mathbf{f}, p, r, \eta, \alpha, \beta, \gamma, \tau)$
    $\boldsymbol{\theta}_0 \leftarrow \boldsymbol{\theta}; j \leftarrow j + r$
    $\mathcal{X}, \kappa \leftarrow$ `AddSample`$(\mathcal{X}, V_{\boldsymbol{\theta}}, \mathbf{f}, u)$
  **end while**
  **if** $\kappa = 0$ **then** $V_{\boldsymbol{\theta}^*} \leftarrow V_{\boldsymbol{\theta}} - V_{\boldsymbol{\theta}}(\mathbf{0}_m)$
  **else** $V_{\boldsymbol{\theta}^*} \leftarrow \emptyset$
  **end if**
  **return** $V_{\boldsymbol{\theta}^*}$
**end function**

ing [69]

$$d^* = \min_{\mathbf{x}} V_{\boldsymbol{\theta}^*}(\mathbf{x}) \tag{4.24a}$$

$$\text{s.t.} \quad \|\mathbf{x}\|_2^2 = u^2. \tag{4.24b}$$

The state vectors satisfying the equality constrain (4.24b) constitute the boundary of the valid region $\mathcal{B}_u$ of $V_{\boldsymbol{\theta}^*}$. Equation (4.24a) essentially says that $d^*$ is the minimal value of $V_{\boldsymbol{\theta}^*}(\mathbf{x})$ evaluated along $\mathcal{B}_u$'s boundary.

The optimization (4.24) can be solved by finding *critical points* defined as follows. The Lagrangian $L(\mathbf{x}, \phi)$ of (4.24) is

$$L(\mathbf{x}, \phi) = \phi(\|\mathbf{x}\|_2^2 - u^2) + V_{\boldsymbol{\theta}^*}(\mathbf{x}). \tag{4.25}$$

where $\phi \in \mathbb{R}$. Define a set $\mathcal{P}$ by

$$\mathcal{P} := \left\{ \mathbf{x} \in \mathbb{R}^m \middle| \frac{\partial L(\mathbf{x}, \phi)}{\partial \mathbf{x}} = 0, \|\mathbf{x}\|_2^2 - u^2 = 0 \right\}. \tag{4.26}$$

Each element of the set $\mathcal{P}$ is a critical point. The global minimum of $V_{\boldsymbol{\theta}^*}$ over $\mathcal{B}_u$'s boundary occurs at one of the critical points. Finding $\mathcal{P}$ is equivalent to obtaining all solutions to

$$2\phi\mathbf{x} + \frac{\partial V_{\boldsymbol{\theta}^*}}{\partial \mathbf{x}} = \mathbf{0}_m; \quad \|\mathbf{x}\|_2^2 - u^2 = 0. \tag{4.27}$$

Unknown parameters $W_1$, $W_2$, $\mathbf{b}_1$, and $\mathbf{b}_2$ in (4.16) and (4.17) can be updated by the $\theta^*$ returned by Algorithm 5. Denote by $W_1^*$, $W_2^*$, $\mathbf{b}_1^*$, and $\mathbf{b}_2^*$ the updated version of $W_1$, $W_2$, $\mathbf{b}_1$, and $\mathbf{b}_2$, respectively. In (4.27),

$$\frac{\partial V_{\boldsymbol{\theta}^*}}{\partial \mathbf{x}} = (1 - V_{\boldsymbol{\theta}^*}(\mathbf{x})^2) W_2^* W_1^* \Lambda \tag{4.28}$$

where $\Lambda = \text{diag}\left(1 - \tanh^2(c^*_{1,1}), \ldots, 1 - \tanh^2(c^*_{1,p})\right)$, whence $[c^*_{1,1}, \ldots, c^*_{1,p}]^\top = W_1^* \mathbf{x} + \mathbf{b}_1^*$. With (4.28), (4.27) becomes algebraic equations whose compact form is

$$\mathbf{h}(\mathbf{x}, \phi) = \mathbf{0}_{m+1}. \tag{4.29}$$

The Newton-Krylov (NK) method [76] can solve (4.29) for $\mathbf{x}$ and $\phi$ with the initial guesses $\mathbf{x}_0$ and $\phi_0$ on solutions. If set $\mathcal{P}$ is available,

$$d^* = \min_{\mathbf{x} \in \mathcal{P}} V_{\boldsymbol{\theta}^*}(\mathbf{x}). \tag{4.30}$$

Then, the corresponding security region is

$$\mathcal{S}_{d^*} = \{\mathbf{x} \in \mathcal{B}_u | V_{\boldsymbol{\theta}^*}(\mathbf{x}) < d^*\}. \tag{4.31}$$

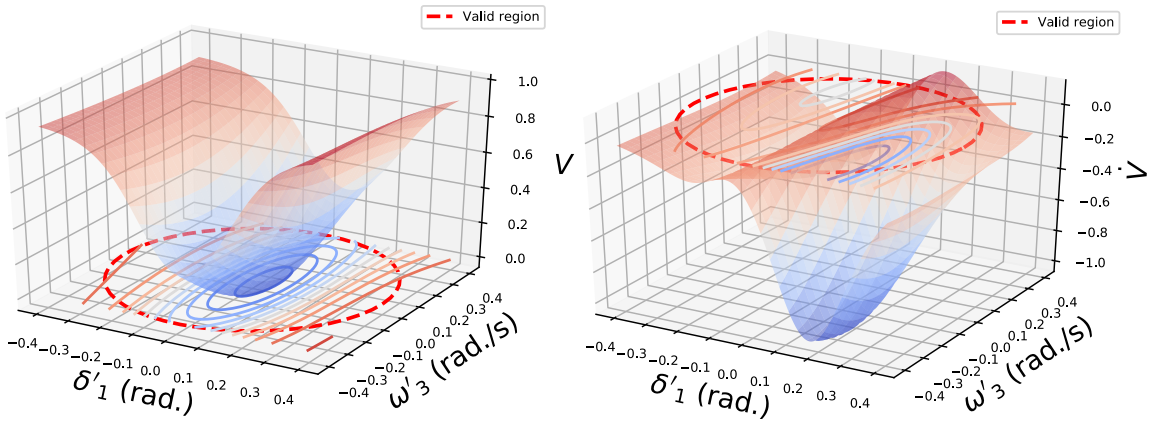
With the Lyapunov function learned by `LearnFunc`, the procedure to estimating a security region is provided by the `SREst` function of Algorithm 6, where $\texttt{NK}(\mathbf{h}, \mathbf{x}_0, \phi_0)$ denotes the procedure of solving $\mathbf{h}(\mathbf{x}, \phi) = \mathbf{0}_{m+1}$ with the initial guesses $\mathbf{x}_0$ and $\phi_0$ using the NK method; and the `NK` procedure returns $\mathbf{x}^*$ and $\phi^*$ which constitute a solution to $\mathbf{h}(\mathbf{x}, \phi) = \mathbf{0}_{m+1}$. The solution found by the `NK` procedure depends on the initial guesses $\mathbf{x}_0$ and $\phi_0$. To find all critical points, the `SREst` function repetitively solves (4.29) for $n_{\text{sr}}$ times. For each time of solving (4.29), $\mathbf{x}_0$ and $\phi_0$ are randomly realized. The `Main` function of Algorithm 6 summarizes the procedure described in Sections 4.3.1, 4.3.2, and 4.3.3. Note that checking asymptotic stability of the given equilibrium (Lines 14-16 of Algorithm 6) is a prerequisite for learning a Lyapunov function and estimating an optimal security region.

**Algorithm 6** Security Region Estimation

**function** $\texttt{SREst}(V_{\boldsymbol{\theta}^*}, u, n_{\text{sr}})$
  $\mathcal{P} \leftarrow \emptyset$; construct $\mathbf{h}$ by (4.27), (4.28)
  **for** $k = 1, 2, \ldots, n_{\text{sr}}$ **do**
    Pick a random $\mathbf{x}_0$ in $\{\mathbf{x}_0 \in \mathbb{R}^m | \|\mathbf{x}_0\|_2^2 = u^2\}$
    Pick a random $\phi_0 \in \mathbb{R}$
    $\mathbf{x}^*, \phi^* \leftarrow \texttt{NK}(\mathbf{h}, \mathbf{x}_0, \phi_0)$
    **if** $\mathbf{x}^* \notin \mathcal{P}$ **then** $\mathcal{P} \leftarrow \mathcal{P} \cup \mathbf{x}^*$
    **end if**
  **end for**
  Obtain $S_{d^*}$ via (4.30), (4.31)
  **return** $S_{d^*}$
**end function**
**function** $\texttt{Main}(\mathbf{f}, u, p, q, \boldsymbol{\theta}_0, r, \eta, \alpha, \beta, \gamma, \tau, n_{\text{sr}}, n_{\text{i}})$
  Linearize $\mathbf{f}$ to obtain $A$ in (4.13)
  Compute eigenvalues $\lambda_i$ of $A$ $\forall i = 1, 2, \ldots m$
  **if** (4.14) holds **then** ▷ Asymptotic stability check
    Construct $\mathcal{X}$ by randomly picking $q$ vectors in $\mathcal{B}_u$
    $V_{\boldsymbol{\theta}^*} \leftarrow \texttt{LearnFunc}(\mathcal{X}, \boldsymbol{\theta}_0, \mathbf{f}, u, p, r, \eta, \alpha, \beta, \gamma, \tau, n_{\text{i}})$
    **if** $V_{\boldsymbol{\theta}^*} \neq \emptyset$ **then**
      $S_{d^*} \leftarrow \texttt{SREst}(V_{\boldsymbol{\theta}^*}, u, n_{\text{sr}})$
      **return** $V_{\boldsymbol{\theta}^*}$, $S_{d^*}$
    **else** Request for tunning user-defined parameters
    **end if**
  **else** Request for tuning parameters in (4.11)
  **end if**
**end function**

### 4.3.4 Parameter Tuning

In Algorithm 6, the empirical settings of $\boldsymbol{\theta}_0, p, q, r, \eta$, $n_{\text{sr}}$, $n_{\text{i}}$ and $\tau$ are provided as follows: the random initial guess $\boldsymbol{\theta}_0$ is obtained by the initialization procedure reported in [77]; $p \geq 2m$; $q$, $n_{\text{sr}}$, and $n_{\text{i}}$ are $500$, $100$, and $5000$, respectively; integer $r \in [10, 30]$; $\tau \in [0.1, 0.5]$; and $\eta \in [0.01, 0.02]$.




(a) (b)

Figure 4.4: Visualization of the function (a) and its time derivative (b) after $n_{\text{i}}$ times of parameter update: the function is NOT a Lyapunov function.

Given a set of user-defined parameters, it is possible that the `Main` function returns an empty set $\emptyset$, meaning that the function fails to find a Lyapunov function valid in $\mathcal{B}_u$ within $n_{\text{i}}$ iterations. Solutions to such a situation include 1) decreasing $u$; 2) changing $\boldsymbol{\theta}_0$; and 3) tunning $\alpha$, $\beta$, and $\gamma$. Solution 1 works because there may not be a Lyapunov function in a large ball. Solving (4.22) using gradient-based methods depends on the initial guess on the solution, which justifies Solution 2.

Next we present an empirical procedure to tune $\alpha$, $\beta$, and $\gamma$. Denote by $\boldsymbol{\theta}_{n_{\text{i}}}$ the $n_{\text{i}}$-th update of $\boldsymbol{\theta}$ in `LearnFunc`. The function $V_{\boldsymbol{\theta}_{n_{\text{i}}}}$ and its time derivative $\dot{V}_{\boldsymbol{\theta}_{n_{\text{i}}}}$ can be

visualized in subspace of $\mathcal{B}_u$. The visualization may suggest which condition(s) in Definition 2 is (are) violated, thereby pointing out the "direction" of tunning $\alpha$, $\beta$, and $\gamma$. For example, suppose that one needs to learn a Lyapunov function for a system whose state variables are $[\delta_1', \delta_2', \delta_3', \omega_3']$ using `LearnFunc`. After $n_{\text{i}}$-time parameter updates, the function with parameter $\boldsymbol{\theta}_{n_{\text{i}}}$ and its time derivative can be visualized by numerically evaluating the functions within $\mathcal{B}_u$'s projection to the $\delta_1'$-$\omega_3'$ plane with $\delta_2' = \delta_3' = 0$. Suppose that the visualization is given in Figure 4.4. As shown in Figure 4.4, the function with parameter $\boldsymbol{\theta}_{n_{\text{i}}}$ is *not* a Lyapunov function in $\mathcal{B}_{0.4}$, because its time derivative is not negative in $\mathcal{B}_{0.4}$, although the function is positive. Figure 4.4 indicates that with other parameters fixed, one may need to increase the penalty resulting from the violation of the second condition of Definition 2, i.e., increasing $\beta$ in (4.19).

## 4.4 Numerical Experiments

This section tests and validates the proposed method in a grid-connected microgrid, a three-microgrid interconnection with mixed dynamics, and the IEEE 123-node feeder. All experiments in this section are conducted on a MacBook Pro ($2.6$ GHz Intel Core i5) with Python $3.7.7$.

### 4.4.1 A Grid-connected Microgrid

A grid-connected microgrid (MG) with angle-droop control is shown in Figure 4.5. The user-defined parameters required in Algorithm 6 are listed in Table 4.1.

*1) Learned Lyapunov Function:* After $500$ times of parameter updates, which takes $32.18$ seconds, Algorithm 5 outputs a Lyapunov function. Figure 4.6 shows the Lyapunov function learned and its time derivative. As shown in Figure 4.6, the function learned is positive definite in the valid region (VR) $\mathcal{B}_{1.5}$ and its time derivative is negative definite in $\mathcal{B}_{1.5}$. This suggests that the function learned is a Lyapunov function.

*2) Estimated Security Region:* Given the Lyapunov function learned with its VR $\mathcal{B}_{1.5}$,

Table 4.1: User-defined Parameters

| **Case Name** | $p$ | $q$ | $n_{\text{sr}}$ | $n_{\text{i}}$ | $r$ | $\tau$ |
|---|---|---|---|---|---|---|
| A Grid-connected Microgrid | 6 | 500 | 100 | 5000 | 10 | 0.1 |
| Three Networked Microgrids | 8 | 500 | 100 | 5000 | 30 | 0.1 |
| IEEE 123-node Feeder | 8 | 500 | 100 | 5000 | 10 | 0.5 |
| **Case Name** | $\eta$ | $u$ | $\alpha$ | $\beta$ | $\gamma$ | N/A |
| A Grid-connected Microgrid | 0.01 | 1.5 | 1 | 5 | 0 | N/A |
| Three Networked Microgrids | 0.02 | 0.4 | 3 | 1 | 3 | N/A |
| IEEE 123-node Feeder | 0.01 | 0.7 | 1 | 1 | 0 | N/A |

the security region (SR) estimated by Algorithm 6 is $\mathcal{S}_{1.01}$ which is defined by (4.31). In Figure 4.7, the red-solid circle is the boundary of $\mathcal{S}_{1.01}$, while the red-dash circle is the boundary of $\mathcal{B}_{1.5}$; and the region enclosed by the red-solid circle is a SR. Besides, the `SREst` function suggests that $d^*$ in (4.24) is $1.01$ which is attained when $\delta_1' = -0.82$ and $E_1' = 1.26$.

We proceed to check the correctness of the estimated SR $\mathcal{S}_{1.01}$. Since the test system only has two state variables, given the Lyapunov function learned, the largest SR can be found without solving optimization (4.24). For example, we can visualize a SR $\mathcal{S}_d$ with a small $d$, say, $d = 0.15$. Figure 4.7-(b) visualize $\mathcal{S}_{0.15}$. We keep increasing $d$ gradually until the boundary of $\mathcal{S}_d$ touches the boundary of $\mathcal{B}_{1.5}$ for the first time. As can be observed in Figure 4.7-(b), when $d = 1.01$, the boundaries of $\mathcal{S}_d$ and $\mathcal{B}_{1.5}$ touch with each other

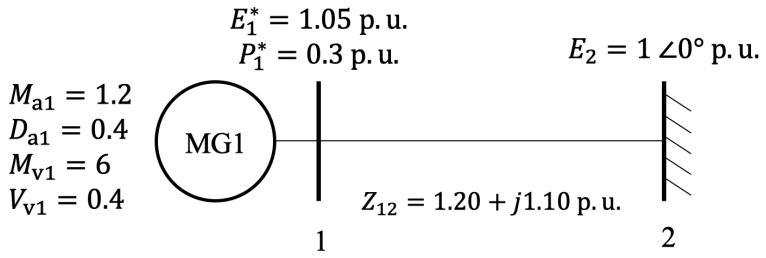
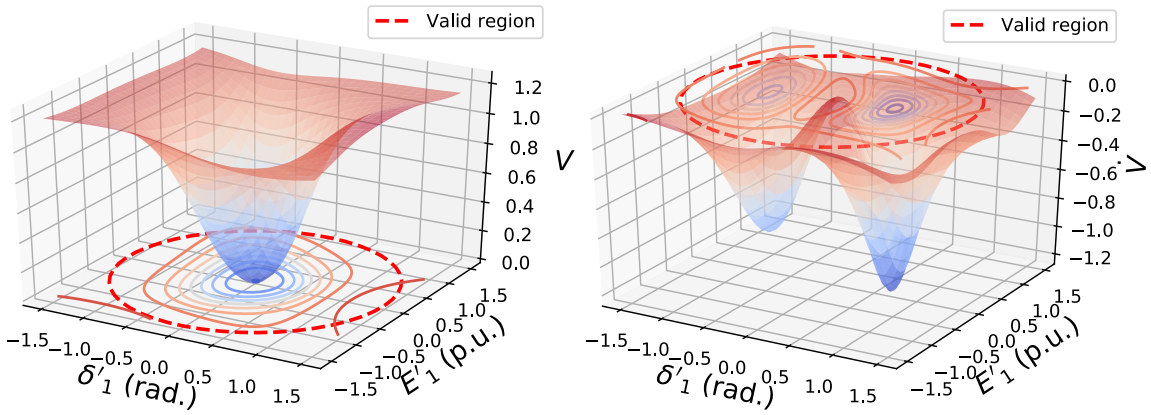



Figure 4.5: A grid-connected microgrid [4]



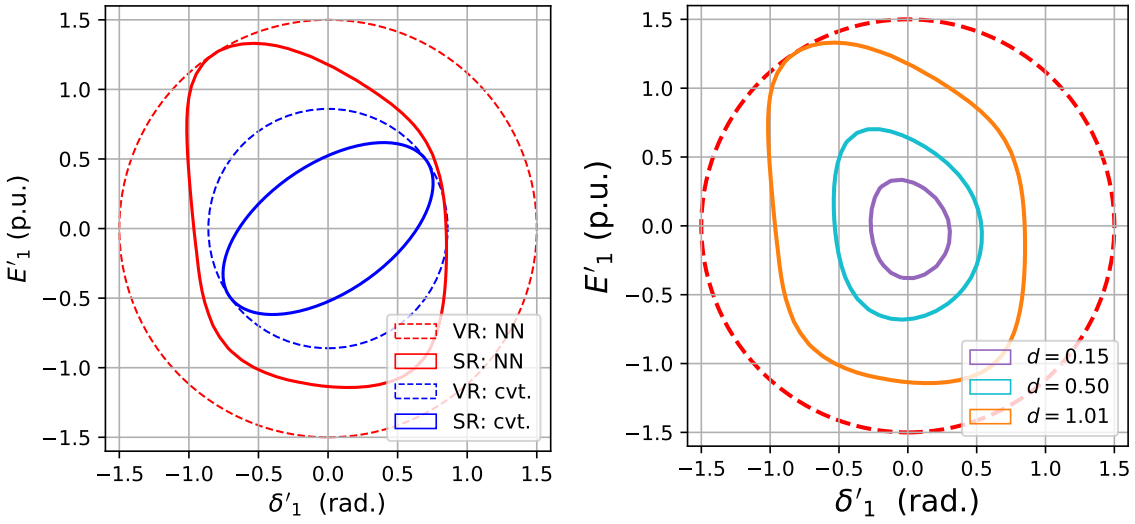

(a) (b)

Figure 4.6: (a) Lyapunov function and (b) its time derivative for a grid-tied MG

at $(-0.82, 1.26)$. Therefore, $\mathcal{S}_{1.01}$ is the largest SR that can be estimated based on the learned Lyapunov function. The SR obtained by such a procedure is consistent with the one estimated by function `SREst`.

*3) Comparison:* The proposed method is compared with a conventional method reported in [68]. Denote by $\mathcal{S}'$ the SR estimated based on a quadratic Lyapunov function constructed in [68]. In Figure 4.7, the region enclosed by the blue-solid circle is $\mathcal{S}'$, while the blue-dash circle is the boundary of the VR of the quadratic Lyapunov function. It can be observed that $\mathcal{S}_{1.01}$ is larger than $\mathcal{S}'$. This suggests that the propose method can provide a less conservative characterization of the SR than the conventional method.

Suppose that the grid-connected MG has an initial condition $\mathbf{x}(0) = [-0.5, 1]^\top$, due to a disturbance. Such an initial condition is inside $\mathcal{S}_{1.01}$, but outside $\mathcal{S}'$. Therefore, $\mathcal{S}_{1.01}$ *can conclude that the system trajectory tends to its equilibrium point, whereas* $\mathcal{S}'$ *can conclude nothing about the system's asymptotic behavior under such a disturbance.* The time-domain simulation shown in Figure 4.8 confirms that all state variables tend to their pre-dispatched steady-state values.




(a) (b)

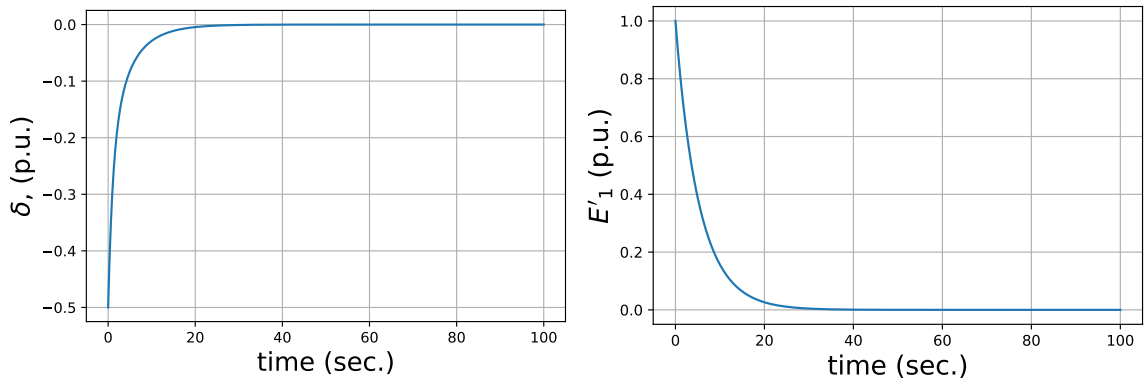
Figure 4.7: (a) Comparison between the proposed (NN) and conventional (cvt.) methods: SR and VR (b) An alternative way to find $\mathcal{S}_{d^*}$ by tuning $d$.

### 4.4.2 Three Networked Microgrids with Mixed Dynamics

Figure 4.9 shows a three-MG interconnection with mixed interface dynamics: the angle droop control is deployed in the PE interfaces of MGs 1 and 2, whereas the frequency droop control is deployed in the PE interfaces of MG 3. Since $M_{\mathrm{v}k} \gg M_{\mathrm{a}k}$ for $k = 1, 2$ and $M_{\mathrm{v}3} \gg M_{\mathrm{f}3}$, the time-scale separation is assumed [5]. We focus on the asymptotic behavior of phase angle and frequency. The user-defined parameters of Algorithm 6 are listed in Table 4.1.

*1) Learned Lyapunov Function:* After taking 23737.53 seconds, Algorithm 6 outputs a Lyapunov function $V_{\boldsymbol{\theta}^*}$ valid in $\mathcal{B}_{0.4}$. Given $\delta'_3 = 0$ and $\omega'_3 = 0$, $V_{\boldsymbol{\theta}^*}$ and $\dot{V}_{\boldsymbol{\theta}^*}$ are visualized in Figure 4.10, where it is observed that $V_{\boldsymbol{\theta}^*} > 0$ and $\dot{V}_{\boldsymbol{\theta}^*} < 0$ in $\mathcal{B}_{0.4}$, suggesting $V_{\boldsymbol{\theta}^*}$ behaves like a Lyapunov function.

*2) Estimated Security Region:* With the learned Lyapunov function, Algorithm 6 provides an estimated SR $\mathcal{S}_{0.37}$. Figure 4.11-(a) visualizes $\mathcal{S}_{0.37}$ and $\mathcal{B}_{0.4}$ in the $\delta'_1$-$\delta'_2$ space




(a) (b)

Figure 4.8: Time-domain simulation for the grid-connected MG with initial conditions $\delta_1'(0) = -0.5$ rad. and $E_1'(0) = 1$ p.u.

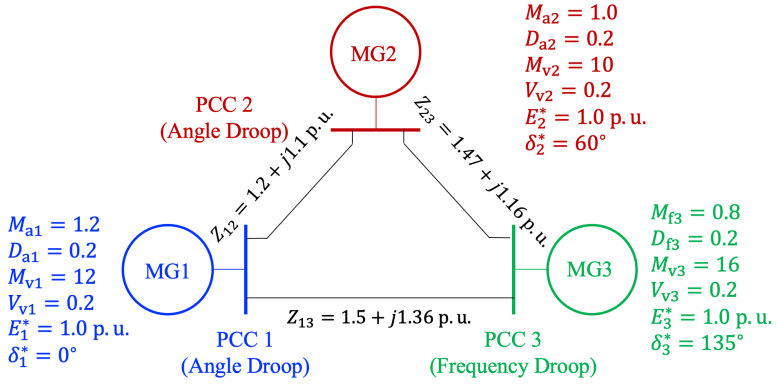
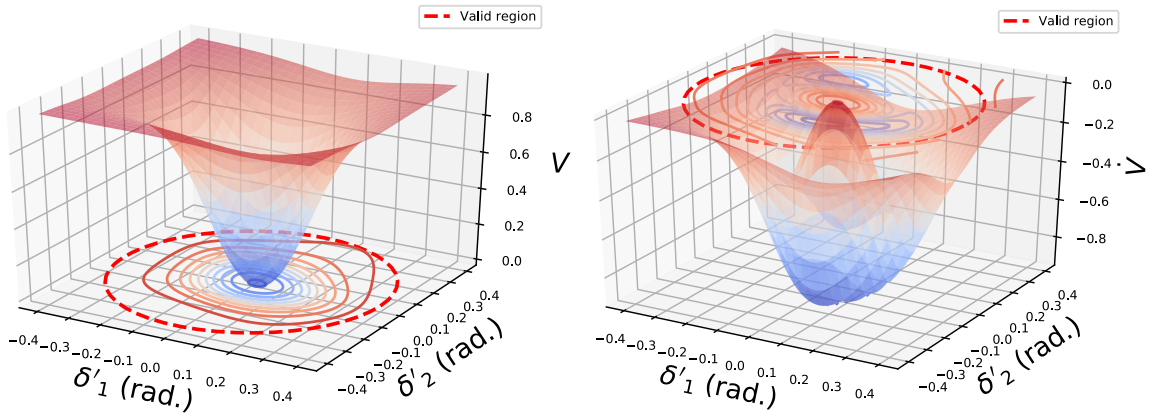



Figure 4.9: Three Networked Microgrids with Mixed Dynamics

with $\delta_3' = 0.37$ and $\omega_3' = -0.14$, where the red-solid circle is the boundary of $\mathcal{S}_{0.37}$, and the red-dash circle is the boundary of $\mathcal{B}_{0.4}$. The `SREst` function suggests that $d^*$ in (4.24) is $0.37$ which is attained when $\mathbf{x}$ is $[-0.07, 0.01, 0.37, -0.14]^\top$. Figure 4.11-(a) shows that the boundary of $\mathcal{S}_{0.37}$ touches the boundary of $\mathcal{B}_{0.4}$ at point $(-0.07, 0.01)$.

*3) Comparison:* Denote by $\mathcal{S}''$ the SR estimated based on the Lyapunov function proposed in [68]. The blue-solid circle in Figure 4.11-(b) represents the boundary of $\mathcal{S}''$ in the $\delta_1'$-$\delta_2'$ plane, given $\delta_3' = \omega_3' = 0$. Suppose that the pre-event condition $\mathbf{x}(0)$ is




(a) (b)

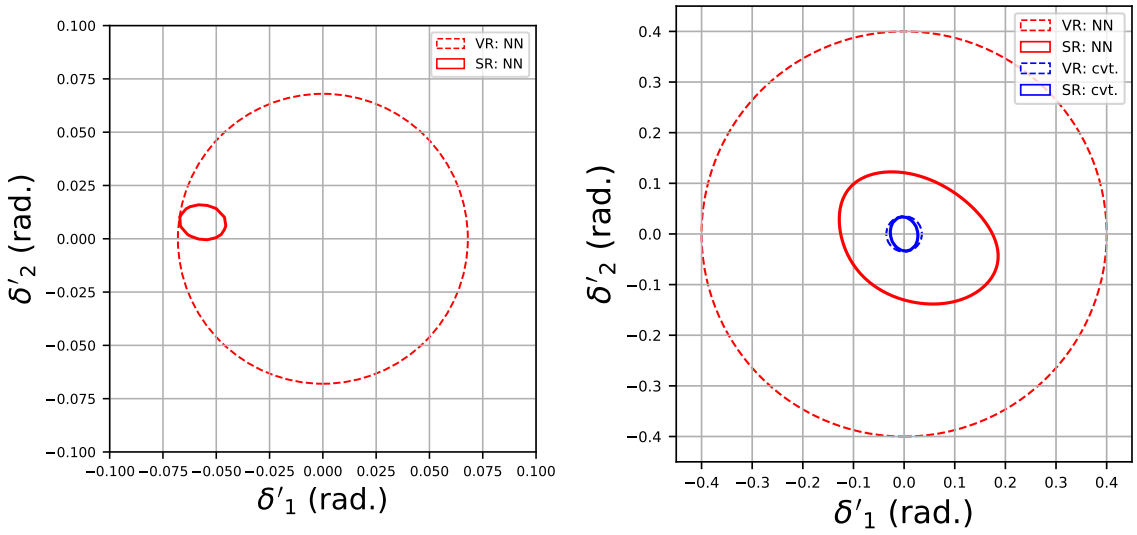
Figure 4.10: (a) Lyapunov function and (b) time derivative for 3 networked MGs

$[0.1, -0.1, 0, 0]^\top$. Since $\mathbf{x}(0)$ is inside $\mathcal{S}_{0.37}$ but outside $\mathcal{S}''$, one can conclude that *all states tend to the equilibrium based on* $\mathcal{S}_{0.37}$*, while the asymptotic behavior the system cannot be assessed by* $\mathcal{S}''$ *with* $\mathbf{x}(0)$. The time-domain simulation confirms that all state variables indeed converge to their post-event steady-state values. In Figure 4.11-(a) and 4.11-(b), the reason why we observe different security (valid) regions estimated from the proposed method is that $\delta_3'$ and $\delta_4'$ are set to different values in these two cases.

### 4.4.3 IEEE 123-node Test Feeder

Figure 4.13 shows a 123-node distribution system [78] which is partitioned into 5 networked MGs [5]. We assume that each MG is managed by its MGCC and connects to the grid via a PE interface with angle droop control [5]. The impedances of the interconnection distribution lines are reported in Table 4.2. The control parameters and predispatched setpoints are listed in Table 4.3. The user-defined parameters in Algorithm 6 are reported in Table 4.1. Note that the time-scale separation is assumed, as $M_{\text{v}k} \gg M_{\text{a}k}$ for $k = 1, 2, \ldots, 5$ in Table 4.3.

*1) Online Application of Estimated Security Region* Suppose that at time $t = 0$, MG



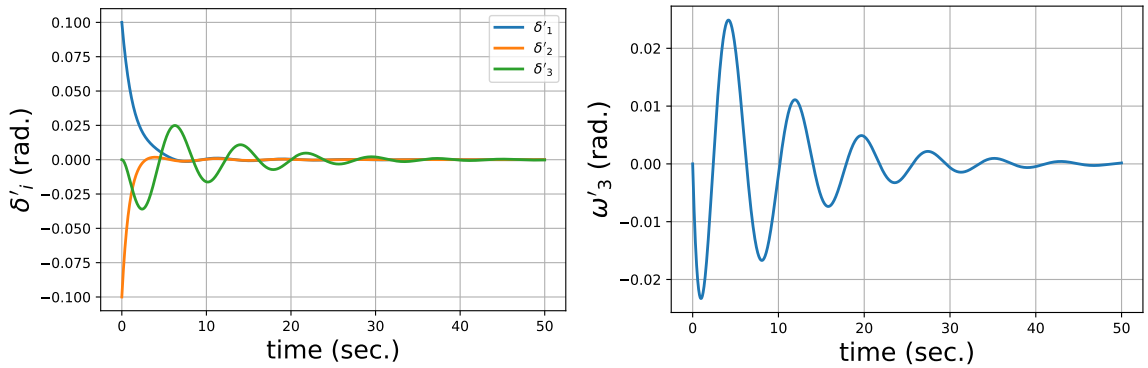

(a) (b)

Figure 4.11: (a) SR and VR around the touching point. (b) Comparison between the proposed (NN) and conventional (cvt.) methods.

Table 4.2: Distribution Line Parameters

| From-node # | To-node # | $R$ (p.u.) | $X$ (p.u.) |
|---|---|---|---|
| 18 | 135 | 1.2030 | 1.1034 |
| 13 | 152 | 1.0300 | 0.7400 |
| 151 | 300 | 1.4512 | 1.3083 |
| 54 | 94 | 1.5042 | 1.3554 |
| 97 | 197 | 1.4680 | 1.1550 |

5 enters an islanded mode and the DSO would like to know if the remaining 4 networked MGs can be stabilized at a pre-dispatched operating point. During offline planning, Algorithm 6 computes a Lyapunov function $V_{\boldsymbol{\theta}^*}$ and a security region $\mathcal{S}_{0.69}$ for the contingency. $\mathcal{S}_{0.69}$ can be leveraged during real-time operation, in order to determine if the remaining MGs can tolerate the disturbance due to islanding of MG 5. The initial condition $\mathbf{x}(0)$ can be obtained by collecting pre-event measurements at the MG interfaces. In this case




(a) (b)

Figure 4.12: Time-domain simulation of the 3 networked MGs with $\mathbf{x}(0) = [0.1, -0.1, 0, 0]^\top$: (a) angle deviation and (b) frequency deviation.

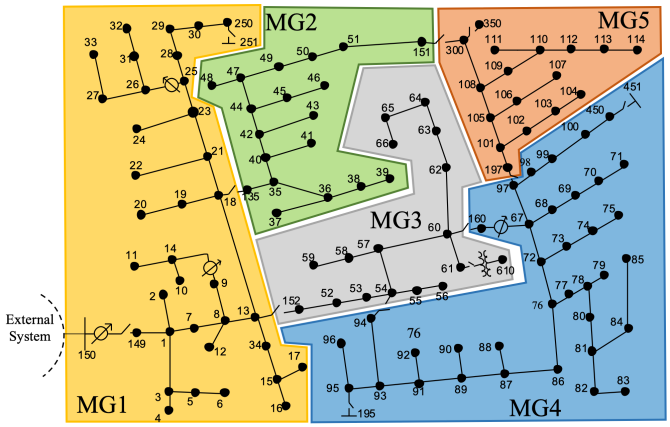



Figure 4.13: IEEE 123-node Test Feeder [5]

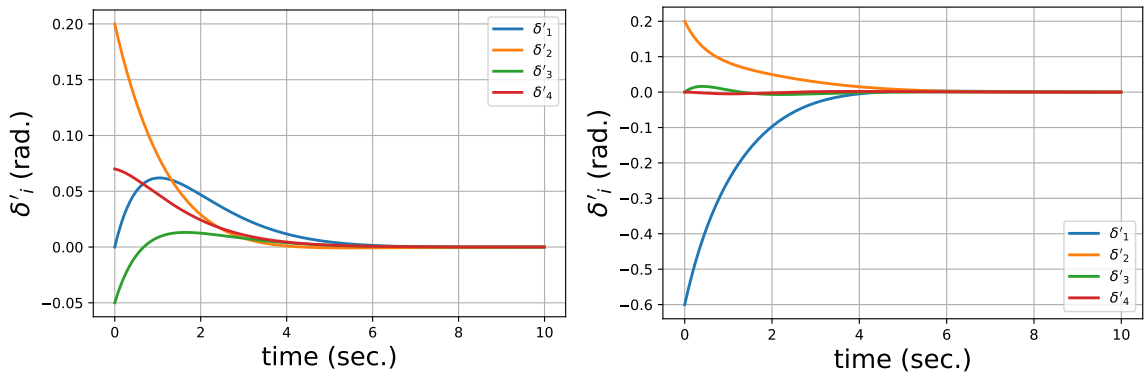
study, $V_{\boldsymbol{\theta}^*}(\mathbf{x}(0)) = 0.12 < 0.69$, suggesting that $\mathbf{x}(0) \in \mathcal{S}_{0.69}$. Thus, without any simulation, the DSO can almost instantaneously conclude that all interface variables tend to their pre-dispatched values. Such a conclusion is confirmed by the time-domain simulation in Figure 4.14-(a).

*2) Learned Lyapunov Function and Estimated Security Region:* It takes 2901.69 seconds to learn the Lyapunov function $V_{\boldsymbol{\theta}^*}$. Figure 4.15 visualizes $V_{\boldsymbol{\theta}^*}$ and $\dot{V}_{\boldsymbol{\theta}^*}$. With $V_{\boldsymbol{\theta}^*}$,

Table 4.3: Control Parameters, Pre-event Measurements and Post-event Setpoints of the IEEE 123-node Feeder

| | MG1 | MG2 | MG3 | MG4 | MG5 |
|---|---|---|---|---|---|
| $M_{ak}$ | 1.2 | 1 | 0.8 | 1 | 1.2 |
| $D_{ak}$ | 1.2 | 1.2 | 1.2 | 1.2 | 1.2 |
| $M_{vk}$ | 12 | 10 | 16 | 10 | 12 |
| $D_{vk}$ | 0.2 | 0.2 | 0.2 | 0.2 | 0.2 |
| Pre-event $\delta_k$ (rad.) | 0 | $-0.8472$ | 2.3062 | 0.5936 | 0.7732 |
| $\delta_k^*$ (rad.) | 0 | $-1.0472$ | 2.3562 | 0.5236 | N/A |
| $E_k^*$ (p.u.) | 1.0 | 1.0 | 1.0 | 1.0 | N/A |

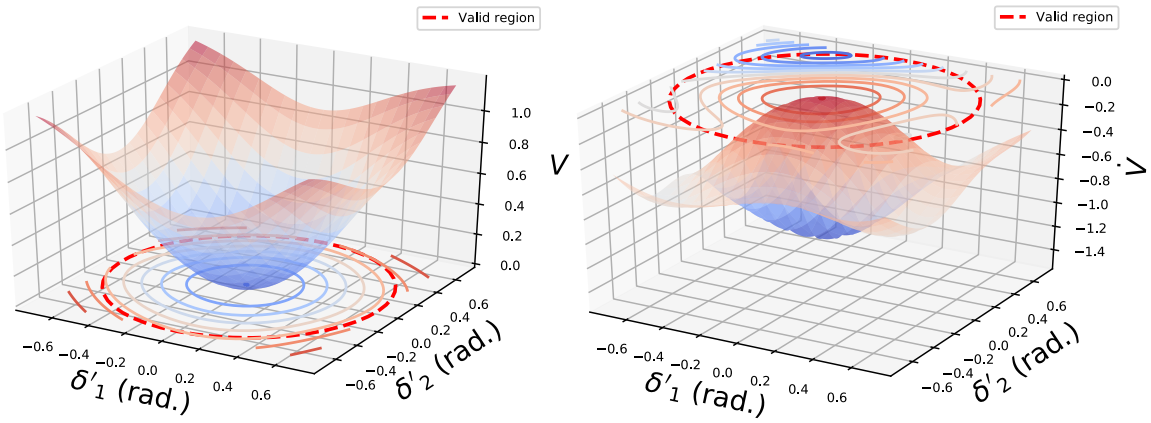
`SREst` computes an security region which is visualized in Figure 4.16 and it suggests that the solution to (4.24) is $[-0.66, 0.03, 0.06, 0.22]^\top$. Figure 4.16-(a) visualizes the region $\mathcal{S}_{0.69}$ in the $\delta_1'$-$\delta_2'$ plane with $\delta_3' = 0.06$ and $\delta_4' = 0.22$. It is observed that the touching point of the boundaries of $\mathcal{S}_{0.69}$ and $\mathcal{B}_{0.7}$ is $(0.66, 0.03)$.




(a) (b)

Figure 4.14: Time-domain simulation of interface variables in the 123-node feeder: (a) with MG 5 islanded; (b) with $\mathbf{x}(0) = [-0.6, 0.2, 0, 0]^\top$ rad.

*3) Comparison:* The comparison between the security region estimated based on the proposed and conventional methods is shown in Figure 4.16-(b). Denoted by $\mathcal{S}'''$ the SR



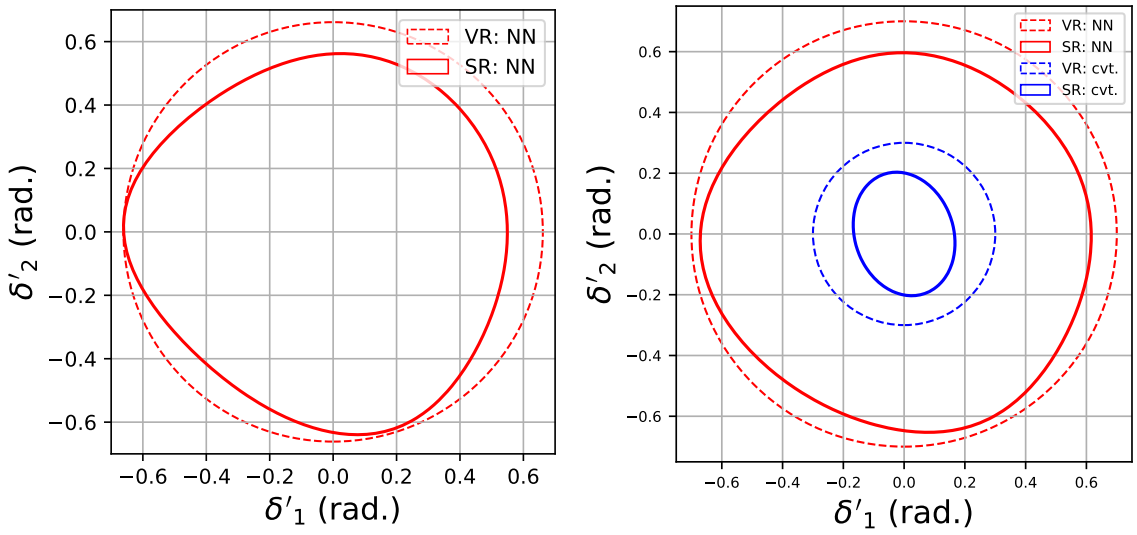

(a) (b)

Figure 4.15: (a) $V_{\theta^*}$ and (b) $\dot{V}_{\theta^*}$ in the 123-node feeder.

estimated based on the conventional approach. Suppose that pre-event operating condition $\mathbf{x}(0)$ is $[-0.6, 0.2, 0, 0]^\top$. Such a condition is outside $\mathcal{S}'''$ but inside $\mathcal{S}_{0.69}$. Therefore, $\mathcal{S}_{0.69}$ can conclude that *the system trajectory will converge to the equilibrium whereas* $\mathcal{S}'''$ *cannot*. The time-domain simulation shown in Figure 4.14-(b) confirms the convergence of the states given the pre-event condition.

## 4.5 Concluding Remarks

In this chapter, we propose a TSA tool for networked microgrids based on tailor-designed Neural Lyapunov methods. Assessing transient stability is formulated as a problem of estimating the security region of networked microgrids. We use neural networks to learn a Lyapunov function in the state space. The optimal security region is estimated based on the function learned, and it can be used for both offline design and online operation. The effectiveness of the proposed TSA tool is tested and validated in 3 scenarios: 1) a grid-connected microgrid, 2) a three networked microgrids with heterogeneous dynamics, and 3) the IEEE 123-node test feeder. Future work will investigate computationally more efficient algorithms to speed up the procedure of learning a Lyapunov function in larger




(a) (b)

Figure 4.16: (a) SR and VR around the touching point with $\delta'_3 = 0.06$ and $\omega'_3 = 0.22$; (b) comparison between the proposed (NN) and conventional (cvt.) methods with $\delta'_3 = \omega'_4 = 0$.

networked microgrids.

# 5. CONCLUSION AND FUTURE WORK

This dissertation is motivated by the emerging opportunities and pressing challenges in massively digitized grid and it provides three concrete examples to leverage the opportunities and to address the challenges. By leveraging rich streaming synchrophasor data in bulk power transmission systems, a purely data-driven approach is proposed in order to locate sources of forced oscillations. To enhance the cyber resilience of the grid, we develop a theoretically rigorous yet practically implementable method of detecting cyber attacks in AGC. Besides, a learning-based framework is designed for assessing physical security of networked microgrids.

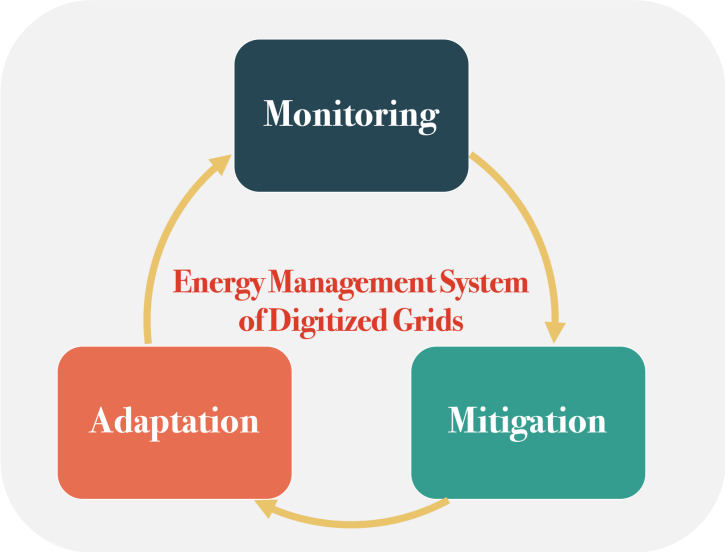



Figure 5.1: Three key functions of a future Energy Management System (EMS)

Next, we envision an advanced Energy Management System (EMS) for massively digitized grids, in order to point out future research directions. As shown in Figure 5.1, we

envision that there are three key functions of the future EMS for physical operation of the grid: 1) Monitoring; 2) Mitigation; and 3) Adaptation. The monitoring function of the future EMS aims to detect, classify and locate physical and cyber anomalies. Since power systems are safety-critical infrastructure, the decisions made by the monitoring function should be physically interpretable. The cyber attack detection and the forced oscillation localization tool proposed in this dissertation serve as building blocks of the monitoring function of the EMS. Once physical/cyber anomalies are identified, the anomaly mitigation function will follow. In Chapter 2, the mitigation measure refers to tripping the generators causing forced oscillations. In Chapter 3, the mitigation measure is disabling the AGC control loop. Integrating mitigation solutions into the grid may change underlying dynamics of the digitized grid. As a result, it may solve one problem but introduce other ones. Therefore, the grid may need to be reconfigured in order to integrate the mitigation solutions with safety guarantee. The adaptation function in Figure 5.1 aims to 1) reshape the grid dynamics by tuning algorithms embedded into power-electronic (PE) interfaces and reconfiguring grid topology; and 2) certify safety of the adapted grid. Chapter 4 presents a framework to certify the safety of networked microgrids.

Under such an EMS architecture, future work will investigate: 1) how to add more values to massively streaming data and to form an end-to-end solution to grid monitoring; 2) how to enrich anomaly mitigation solutions by reprogramming grid dynamics; and 3) how to develop online safety certification procedures that make the grid more adaptive to uncertainties from deep renewable penetration and natural disasters.

# REFERENCES


[1] T. Huang *et al.*, "Localization of forced oscillations in the power grid under resonance conditions," in *52nd CISS*, pp. 1–5, March 2018.

[2] J. H. Chow *et al.*, "A toolbox for power system dynamics and control engineering education and research," *IEEE Trans. on Power Systems*.

[3] S. Maslennikov *et al.*, "A test cases library for methods locating the sources of sustained oscillations," in *IEEE PESGM*, pp. 1–5, July 2016.

[4] T. Huang, S. Gao, X. Long, and L. Xie, "A neural lyapunov approach to transient stability assessment in interconnected microgrids," in *Proceedings of the 54th Hawaii International Conference on System Sciences*, p. 3330, 2021.

[5] Y. Zhang and L. Xie, "A transient stability assessment framework in power electronic-interfaced distribution systems," *IEEE Transactions on Power Systems*, vol. 31, no. 6, pp. 5106–5114, 2016.

[6] M. U. Usman and M. O. Faruque, "Applications of synchrophasor technologies in power systems," *Journal of Modern Power Systems and Clean Energy*, vol. 7, no. 2, pp. 211–226, 2019.

[7] "Synchrophasor technology fact sheet," tech. rep., NASPI, 2014.

[8] D. J. Trudnowski, J. W. Pierre, N. Zhou, J. F. Hauer, and M. Parashar, "Performance of three mode-meter block-processing algorithms for automated dynamic stability assessment," *IEEE Transactions on Power Systems*, vol. 23, pp. 680–690, May 2008.

[9] L. Xie, Y. Chen, and P. R. Kumar, "Dimensionality reduction of synchrophasor data for early event detection: Linearized analysis," *IEEE Trans. on Power Systems*, vol. 29, no. 6, 2014.

[10] M. S. Modarresi, T. Huang, H. Ming, and L. Xie, "Robust phase detection in distribution systems," in *2017 IEEE Texas Power and Energy Conference (TPEC)*, pp. 1–5, 2017.

[11] "1200 mw fault induced solar photovoltaic resource interruption disturbance report," tech. rep., NERC, 2017.

[12] T. Huang, S. Gao, and L. Xie, "Transient stability assessment of networked microgrids using neural lyapunov methods," *arXiv preprint arXiv:2012.01333*, 2020.

[13] T. Huang, H. Sun, K. J. Kim, D. Nikovski, and L. Xie, "A holistic framework for parameter coordination of interconnected microgrids against disasters," in *2020 IEEE Power Energy Society General Meeting (PESGM)*, pp. 1–5, 2020.

[14] M. Ghorbaniparvar and N. Zhou, "A survey on forced oscillations in power system," *CoRR*, vol. abs/1612.04718, 2016.

[15] S. Maslennikov *et al.*, "Dissipating energy flow method for locating the source of sustained oscillations," *IJEPES*, 2017.

[16] S. Sarmadi *et al.*, "Analysis of november 29, 2005 western american oscillation event," *IEEE Trans. on Power Systems*, vol. 31, no. 6, 2016.

[17] S. Maslennikov, "Detection the source of forced oscillations," tech. rep.

[18] S. Sarmadi *et al.*, "Inter-area resonance in power systems from forced oscillations," *IEEE Trans. on Power Systems*, vol. 31, no. 1, 2016.

[19] N. Zhou *et al.*, "Locating sources of forced oscillations using transfer functions," in *IEEE PECI*, pp. 1–8, 2017.

[20] W. Bin and S. Kai, "Location methods of oscillation sources in power systems: a survey," *JMPSCE*, vol. 5, no. 2, 2017.

[21] S. Chevalier *et al.*, "Using effective generator impedance for forced oscillation source location," *IEEE Trans. on Power Systems*, 2018.

[22] S. Chevalier *et al.*, "A Bayesian approach to forced oscillation source location given uncertain generator parameters," *IEEE Trans. on Power Systems*, 2018.

[23] "Var 501 wecc-3 power system stabilizer," tech. rep.

[24] E. J. Candès, X. Li, Y. Ma, and J. Wright, "Robust Principal Component Analysis?," *Journal of the ACM (JACM)*, vol. 58, no. 3, p. 11.

[25] S. H. AV Oppenheim, Alan S. Willsky, *Signal and Systems*. Prentice Hall, 1997.

[26] H. Ye, Y. Liu, P. Zhang, and Z. Du, "Analysis and detection of forced oscillation in power system," *IEEE Transactions on Power Systems*, vol. 32, no. 2, pp. 1149–1160, 2017.

[27] Z. Lin *et al.*, "The Augmented Lagrange Multiplier method for exact recovery of corrupted low-rank matrices," *arXiv preprint arXiv:1009.5055*.

[28] J. Follum and J. W. Pierre, "Detection of periodic forced oscillations in power systems," *IEEE Trans. on Power Systems*, vol. 31, no. 3, 2016.

[29] J. Follum and J. Pierre, "Time-localization of forced oscillations in power systems," in *2015 IEEE Power Energy Society General Meeting*, pp. 1–5, July 2015.

[30] M. Ilic-Spong, M. Spong, and R. Fischl, "The no-gain theorem and localized response for the decoupled p -hetapower network with active power losses included," *IEEE Transactions on Circuits and Systems*, vol. 32, no. 2, pp. 170–177, 1985.

[31] M. Ilic-Spong, J. Thorp, and M. Spong, "Localized response performance of the decoupled q -v network," *IEEE Transactions on Circuits and Systems*, vol. 33, no. 3, pp. 316–322, 1986.

[32] N. Wiener, *Cybernetics or Control and Communication in the Animal and the Machine*, vol. 25. MIT press, 1965.

[33] T. Huang, B. Satchidanandan, P. R. Kumar, and L. Xie, "An online detection framework for cyber attacks on automatic generation control," *IEEE Trans. on Power Systems*, vol. 33, Nov 2018.

[34] EPRI, *EPRI Power System Dynamic Tutorial*. Electric Power Research Institution, July 2009.

[35] R. Tan, H. H. Nguyen, E. Y. S. Foo, D. K. Y. Yau, Z. Kalbarczyk, R. K. Iyer, and H. B. Gooi, "Modeling and mitigating impact of false data injection attacks on automatic generation control," *IEEE Transactions on Information Forensics and Security*, vol. 12, pp. 1609–1624, July 2017.

[36] S. Sridhar and M. Govindarasu, "Model-based attack detection and mitigation for automatic generation control," *IEEE Transactions on Smart Grid*, vol. 5, pp. 580–591, March 2014.

[37] A. Ashok, P. Wang, M. Brown, and M. Govindarasu, "Experimental evaluation of cyber attacks on automatic generation control using a cps security testbed," in *2015 IEEE Power Energy Society General Meeting*, pp. 1–5, July 2015.

[38] A. Ashok, S. Sridhar, A. D. McKinnon, P. Wang, and M. Govindarasu, "Testbed-based performance evaluation of attack resilient control for agc," in *2016 Resilience Week (RWS)*, pp. 125–129, Aug 2016.

[39] C. L. DeMarco, "Design of predatory generation control in electric power systems," in *Proceedings of the Thirty-First Hawaii International Conference on System Sciences*, vol. 3, pp. 32–38 vol.3, 1998.

[40] H. E. Brown and C. L. DeMarco, "Risk of cyber-physical attack via load with emulated inertia control," *IEEE Transactions on Smart Grid*, vol. PP, no. 99, pp. 1–1, 2017.

[41] "Dragonfly: Cyberespionage attacks against energy suppliers," tech. rep., Symantec Security Response, July 2014.

[42] "Stuxnet,"

[43] M. Q. Ali, R. Yousefian, E. Al-Shaer, S. Kamalasadan, and Q. Zhu, "Two-tier data-driven intrusion detection for automatic generation control in smart grid," in *2014 IEEE Conference on Communications and Network Security*, pp. 292–300, Oct 2014.

[44] A. Ashok, M. Govindarasu, and J. Wang, "Cyber-physical attack-resilient wide-area monitoring, protection, and control for the power grid," *Proceedings of the IEEE*, vol. 105, pp. 1389–1407, July 2017.

[45] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," in *Proceedings of the 16th ACM Conference on Computer and Communications Security*, CCS '09, (New York, NY, USA), pp. 21–32, ACM, 2009.

[46] Z. Guo, K. H. Johansson, and L. Shi, "A study of packet-reordering integrity attack on remote state estimation," in *2016 35th Chinese Control Conference (CCC)*, pp. 7250–7255, July 2016.

[47] B. Satchidanandan and P. R. Kumar, "Dynamic watermarking: Active defense of networked cyber physical systems," *Proceedings of the IEEE*, vol. 105, pp. 219–240, Feb 2017.

[48] B. Satchidanandan and P. R. Kumar, "On minimal tests of sensor veracity for dynamic watermarking-based defense of cyber-physical systems," in *2017 9th Interna-*

*tional Conference on Communication Systems and Networks (COMSNETS)*, pp. 23–30, Jan 2017.

[49] T. Huang, M. Wu, and L. Xie, "Prioritization of PMU location and signal selection for monitoring critical power system oscillations," *IEEE Transactions on Power Systems*, 2017.

[50] P. Kundur, N. J. Balu, and M. G. Lauby, *Power system stability and control*, vol. 7. McGraw-hill New York, 1994.

[51] Ibraheem, P. Kumar, and D. P. Kothari, "Recent philosophies of automatic generation control strategies in power systems," *IEEE Transactions on Power Systems*, vol. 20, pp. 346–357, Feb 2005.

[52] J. Carpentier, "To be or not to be modern that is the question for automatic generation control (point of view of a utility engineer)," *International Journal of Electrical Power & Energy Systems*, vol. 7, no. 2, pp. 81–91, 1985.

[53] A. A. Thatte, F. Zhang, and L. Xie, "Frequency aware economic dispatch," in *2011 North American Power Symposium*, pp. 1–7, Aug 2011.

[54] J. S. Bay, *Fundamentals of linear state space systems*. McGraw-Hill Science, Engineering & Mathematics, 1999.

[55] The MathWorks Inc, *Matlab Documentation*.

[56] Y. Mo and B. Sinopoli, "Secure control against replay attacks," in *2009 47th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, pp. 911–918, Sept 2009.

[57] Y. Mo, R. Chabukswar, and B. Sinopoli, "Detecting integrity attacks on scada systems," *IEEE Transactions on Control Systems Technology*, vol. 22, pp. 1396–1407, July 2014.

[58] P. R. Kumar and P. Varaiya, *Stochastic systems: Estimation, identification, and adaptive control*. SIAM, 2015.

[59] "Standard prc-006-npcc-1 automatic underfrequency load shedding," tech. rep., North American Electric Reliability Corporation.

[60] J. H. Chow and K. W. Cheung, "A toolbox for power system dynamics and control engineering education and research," *IEEE transactions on Power Systems*, vol. 7, no. 4, pp. 1559–1564, 1992.

[61] Y. Zhang, P. Markham, T. Xia, L. Chen, Y. Ye, Z. Wu, Z. Yuan, L. Wang, J. Bank, J. Burgett, R. W. Conners, and Y. Liu, "Wide-area frequency monitoring network (fnet) architecture and applications," *IEEE Transactions on Smart Grid*, vol. 1, pp. 159–167, Sept 2010.

[62] J. Qi, K. Sun, and W. Kang, "Optimal pmu placement for power system dynamic state estimation by using empirical observability gramian," *IEEE Transactions on Power Systems*, vol. 30, pp. 2041–2054, July 2015.

[63] C. Liu, B. Wang, F. Hu, K. Sun, and C. L. Bak, "Online voltage stability assessment for load areas based on the holomorphic embedding method," *IEEE Transactions on Power Systems*, vol. PP, no. 99, pp. 1–1, 2017.

[64] L. Ljung, "System identification toolbox," *The Matlab user guide*, 1988.

[65] M. Shahidehpour, Z. Li, S. Bahramirad, Z. Li, and W. Tian, "Networked microgrids: Exploring the possibilities of the iit-bronzeville grid," *IEEE Power and Energy Magazine*, vol. 15, no. 4, pp. 63–71, 2017.

[66] M. N. Alam, S. Chakrabarti, and A. Ghosh, "Networked microgrids: State-of-the-art and future perspectives," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 3, pp. 1238–1250, 2019.

[67] J.-J. E. Slotine, W. Li, *et al.*, *Applied nonlinear control*, vol. 199. Prentice hall Englewood Cliffs, NJ, 1991.

[68] H. . Chiang, "Study of the existence of energy functions for power systems with losses," *IEEE Transactions on Circuits and Systems*, vol. 36, no. 11, pp. 1423–1429, 1989.

[69] T. L. Vu and K. Turitsyn, "Lyapunov functions family approach to transient stability assessment," *IEEE Transactions on Power Systems*, vol. 31, no. 2, pp. 1269–1277, 2016.

[70] Y. Zhang, L. Xie, and Q. Ding, "Interactive control of coupled microgrids for guaranteed system-wide small signal stability," *IEEE Transactions on Smart Grid*, vol. 7, no. 2, pp. 1088–1096, 2016.

[71] N. Pogaku, M. Prodanovic, and T. C. Green, "Modeling, analysis and testing of autonomous operation of an inverter-based microgrid," *IEEE Transactions on Power Electronics*, vol. 22, no. 2, pp. 613–625, 2007.

[72] R. R. Kolluri, I. Mareels, T. Alpcan, M. Brazil, J. de Hoog, and D. A. Thomas, "Power sharing in angle droop controlled microgrids," *IEEE Transactions on Power Systems*, vol. 32, no. 6, pp. 4743–4751, 2017.

[73] Y. Pan, L. Chen, X. Lu, J. Wang, F. Liu, and S. Mei, "Stability region of droop-controlled distributed generation in autonomous microgrids," *IEEE Transactions on Smart Grid*, vol. 10, no. 2, pp. 2288–2300, 2019.

[74] S. Gao, J. Avigad, and E. M. Clarke, "$\delta$-complete decision procedures for satisfiability over the reals," in *International Joint Conference on Automated Reasoning*, pp. 286–300, Springer, 2012.

[75] Y.-C. Chang, N. Roohi, and S. Gao, "Neural lyapunov control," *arXiv preprint arXiv:2005.00611*, 2020.

[76] D. A. Knoll and D. E. Keyes, "Jacobian-free newton–krylov methods: a survey of approaches and applications," *Journal of Computational Physics*, vol. 193, no. 2, pp. 357–397, 2004.

[77] K. He, X. Zhang, S. Ren, and J. Sun, "Delving deep into rectifiers: Surpassing human-level performance on imagenet classification," in *Proceedings of the IEEE international conference on computer vision*, pp. 1026–1034, 2015.

[78] K. P. Schneider, B. A. Mather, B. C. Pal, C. . Ten, G. J. Shirek, H. Zhu, J. C. Fuller, J. L. R. Pereira, L. F. Ochoa, L. R. de Araujo, R. C. Dugan, S. Matthias, S. Paudyal, T. E. McDermott, and W. Kersting, "Analytic considerations and design basis for the ieee distribution test feeders," *IEEE Transactions on Power Systems*, vol. 33, no. 3, pp. 3181–3188, 2018.