This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2017.2787690, IEEE Transactions on Smart Grid

Hierarchical Location Identification of Destabilizing Faults and Attacks in Power Systems: A Frequency-Domain Approach

Sajjad Amini, *Student Member, IEEE*, Fabio Pasqualetti, *Member, IEEE*,
Masoud Abbaszadeh, *Senior Member, IEEE*, and Hamed Mohsenian-Rad, *Senior Member, IEEE*

***Abstract*—An optimization-based data-driven approach is proposed to identify the unknown location(s) of destabilizing faults and attacks in power systems. The analysis in this paper kicks in at the critical moment where the presence of destabilizing fault or attack is detected within the power system; therefore, there is an immediate need to identify the location(s) of the affected generators or loads in order to enable proper and effective post-detection measures. The proposed method works in frequency-domain. It does not require prior knowledge about the number of affected location(s). It is accurate in identifying the correct locations and also in preventing false alarms. It is computationally more efficient than its time-domain counterparts. Importantly, it is well-suited to be implemented in a hierarchical fashion, with applications such as in wide area monitoring systems. Various case studies on IEEE 9 and IEEE 39 bus test systems verified the performance of the proposed algorithms.**

***Keywords*: Fault and attack location identification, power system stability, cyber-physical security, hierarchical algorithm.**

NOMENCLATURE

$\mathcal{B}$, $\mathcal{G}, \mathcal{L}$	Set of power system, generator and load buses
H	Imaginary part of admittance matrix
M	Inertia matrix for generators
D^G, D^L	Damping coefficient matrices
K^P, K^I	Generator controller gain matrices
δ, θ	Phase angle at generator/load buses
ω, φ	Frequency deviation at generator/load buses
P^G, P^L	Vector of power injection/consumption
E, A, B, C	State-space model matrices
x, u, y	Vector of states, inputs, and outputs
u^c	Vector of affected inputs
f	Vector of fault/attack signals
$\hat{y}$	Vector of sensor measurements
$\mathcal{K}$	Set of affected inputs
ω^*	Fault/attack frequency
F	Optimal value of objective functions
S, N	Sensitivity and normalized sensitivity function
μ	Detection threshold
ϵ	Location identification threshold
$\mathcal{A}$	Set of areas in a synchrophasor network
$\mathcal{A}_a$	Set of buses in the area a
$\mathcal{P}, \mathcal{C}, \mathcal{N}$	Set of previous, current, and next areas
$\mathcal{T}$	Set of affected inputs in hierarchical approach

LIST OF ABBREVIATIONS

WAMS	Wide Area Monitoring System
AGC	Automatic Generation Control
PMU	Phasor Measurement Unit
D-LAA	Dynamic Load Altering Attack
FFT	Fast Fourier Transform
SCADA	Supervisory Control and Data Acquisition
UIO	Unknown Input Observer
LIA	Location Identification Accuracy
PDC	Phasor Data Concentrator

S. Amini and H. Mohsenian-Rad are with the Department of Electrical and Computer Engineering, University of California, Riverside, CA, USA. F. Pasqualetti is with the Department of Mechanical Engineering, University of California, Riverside, CA, USA. M. Abbaszadeh is with GE Global Research, USA. This work was supported by NSF grants 1253516, 1462530, 1405330, and the UCOP grant LFR-18-548175. The corresponding author is H. Mohsenian-Rad, e-mail: hamed@ece.ucr.edu.

I. INTRODUCTION

Natural faults and malicious attacks can affect the *dynamics* of power systems. They can be physical or cyber-physical, and can affect the generation side or the load side. Most changes in power system dynamics that are caused by faults and attacks are damped and do not cause any major harm. However, some faults and attacks may make the system *unstable*. The focus in this paper is on such *destabilizing* faults and attacks.

A. Motivation

Power system destabilization is the result of creating *oscillations* or *positive feedback* within the power system. This can happen, in particular, due to natural faults or intentional attacks at power system inputs, i.e., power generation levels or power consumption levels, e.g., see [1]–[6]. Therefore, there is a need to devise methods to not only protect power systems against such faults or attacks, i.e., take preventive actions, but also detect and identify the fault/attack location(s) in order to take timely diagnostics and corrective actions. In this regard, the focus in this paper is to develop accurate and computationally efficient centralized and hierarchical methods to identify the location(s) of destabilizing faults and attacks in power systems.

B. Related Work

The literature related to destabilizing faults and attacks in power systems can be divided into *protection*, *detection*, *identification*, and *mitigation*. Different methods have been developed to protect power systems against destabilizing faults/attacks, e.g., in [4], [7], [8]. For example, in [7], a protection and control system mechanism is designed against

1949-3053 (c) 2017 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2017.2787690, IEEE Transactions on Smart Grid

frequency instability. In [8], a measurement-based online load identification approach is proposed to assess the margin of voltage instability in order to prevent voltage collapse.

Detection and mitigation are also studied in many papers, e.g., in [9]–[11]. For example, an attack-mitigation model, based on a game-theoretic analysis, is proposed in [9] to effectively reduce the impact of attack and to maintaine physical stability of the power system. Also, in [10], an algorithm is proposed to automatically detect the fast separation of phase angles among the critical areas in the power system by using synchrophasor data, and by triggering suitable control actions.

The focus in this paper is on location identification, where a single or a group of simultaneous destabilizing faults or attacks occur at unknown location(s). Similar problems are addressed, e.g., in [12] using pattern recognition, in [10] using Kalman Filters, in [13] using observer design, and in [14] using state fault diagnosis matrix. So far, the common approach has been to conduct the analysis in *time-domain*.

C. Main Contributions

The proposed location identification approach in this paper operates in *frequency-domain* and is *customized* to work well against a class of destabilizing faults/attacks in power systems, whether in generation or load side. It has several advantages over the existing methods that operate in time-domain:

1) It makes direct use of the information that is obtained during the detection phase. In particular, it uses the frequency at which the fault/attack *signature* was detected.
2) Compared to its time-domain counterparts, such as unknown input observers, it needs a lower time resolution for measurements, because it does *not* need to reconstruct the entire unknown input signals before it can identify the location(s) of affected power system inputs.
3) Unlike in [14] and other similar work, our method does not require knowing the number of affected input location(s). In fact, one of the main contributions in this paper is to provide a means to effectively estimate the unknown number of affected fault/attack location(s).
4) The optimization-based location identification approach in this paper is computationally efficient.
5) The proposed approach is well-suited to be deployed in wide area monitoring systems (WAMS) to do fault/attack location identification in a *hierarchical* fashion.

The techniques that are developed in this paper are tested and verified on illustrative examples based on an IEEE 9 bus test system, and on a large multi-area IEEE 39 bus test system.

II. System Model

A. Power System Dynamics

Consider a power transmission system with $\mathcal{B} = \mathcal{G} \cup \mathcal{L}$ as the set of buses, where $\mathcal{G}$ and $\mathcal{L}$ are the sets of generator buses and load buses, respectively. An example is shown in Fig.1.

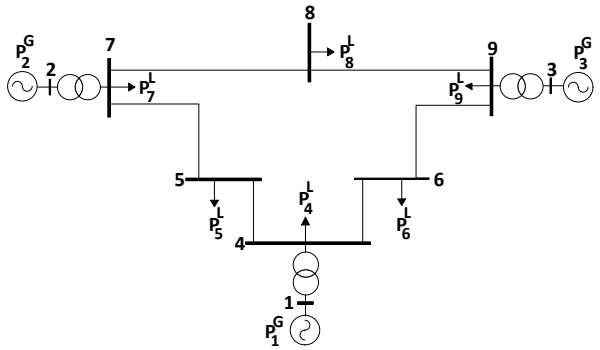

Figure 1. The IEEE 9 bus test system. $\mathcal{G} = \{1, 2, 3\}$ and $\mathcal{L} = \{4, \ldots, 9\}$.

The basic dynamics of this system are commonly modeled using the following state-space equations [15]:

$$\overbrace{\begin{bmatrix} I & 0 & 0 & 0 \\ 0 & I & 0 & 0 \\ 0 & 0 & -M & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}}^{E} \begin{bmatrix} \dot{\delta} \\ \dot{\theta} \\ \dot{\omega} \\ \dot{\varphi} \end{bmatrix} = \underbrace{\begin{bmatrix} 0 & 0 & I & 0 \\ 0 & 0 & 0 & -I \\ K^I + H^{GG} & H^{GL} & K^P + D^G & 0 \\ H^{LG} & H^{LL} & 0 & D^L \end{bmatrix}}_{A} \overbrace{\begin{bmatrix} \delta \\ \theta \\ \omega \\ \varphi \end{bmatrix}}^{x} + \underbrace{\begin{bmatrix} 0 & 0 \\ 0 & 0 \\ I & 0 \\ 0 & I \end{bmatrix}}_{B} \overbrace{\begin{bmatrix} P^G \\ P^L \end{bmatrix}}^{u}, \tag{1}$$

where H^{GG}, H^{GL}, H^{LG}, and H^{LL} are derived from the imaginary part of the Y-bus admittance matrix , i.e., we have:

$$Y_{bus} = \begin{bmatrix} H^{GG} & H^{GL} \\ H^{LG} & H^{LL} \end{bmatrix}.$$

Here, δ is the vector of voltage phase angles at all generator buses, ω is the vector of rotor angular frequency deviations at all generator buses, θ is the vector of voltage phase angles at all load buses, φ is the vector of frequency deviations at all load buses, P^L is the vector of power consumption at all load buses, and P^G is the vector of power generation at all generator buses which is zero for generators with Automatic Generation Control (AGC) and non-zero for generators without AGC. Additionally, I is the identity matrix of appropriate dimension, and M, D^G, and D^L are diagonal matrices with diagonal entries equal to the inertia, damping coefficients of generators, and damping coefficients of loads, respectively. Also, K^I and K^P are diagonal matrices with diagonal entries equal to the integral and proportional controller coefficients of generators with AGC. Note that, the coefficients corresponding to generators without AGC are zero. The system model in (1) incorporates the swing equations for generators, power flow equations for the transmission network, and the governor and load frequency controller for generators with AGC. Note that, in (1), E is a singular matrix in order to allow having both differential and algebraic equations in the system model.

In practice, several sensors, such as Phasor Measurement Units (PMU) [16], can be used to measure the system states.

1949-3053 (c) 2017 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2017.2787690, IEEE Transactions on Smart Grid

We denote such measurement outputs by y. We may have:

$$y = Cx, \tag{2}$$

where C is the measurement matrix.

B. Destabilizing Faults and Attacks

The focus in this paper is on cases where one or more power system inputs, i.e., the power generation level of generators and/or the power consumption level of loads, are either faulty due to natural causes, or compromised by adversarial actions. We are concerned with those cases where the faulty or compromised inputs have the potential to destabilize the power system at certain operating conditions. In this setup, we model faults and attacks using the following general expression:

$$u^c = u + f, \tag{3}$$

where u^c denotes the new input vector under faults and/or attacks, and f denotes the fault and/or attack vector.

We shall point out four notes with respect to (3). *First*, the faults and attacks in this paper are related to physical quantities of the power system inputs. For example, in case of a faulty generator, either there is a fault in choosing the set point or there is a fault in following the set point. In either case, the physical generation output is affected. *Second*, without loss of generality, here we assume that faults and attacks are additive. In principle, the analysis in this paper is applicable also to multiplicative faults and attacks. *Third*, if an input is neither faulty nor compromised, then the corresponding entry in f is zero. *Fourth*, the fault and attack vector f is essentially a signal. In order to cause destabilization, it must demonstrate certain dynamics. In practice, e.g., when it comes to implementing a destabilizing attack, vector f is likely to be constructed through a *positive feedback* mechanism, see [4], and also the illustrative example in Section II-C.

Once we substitute u with u^c in (1), the power system dynamics under destabilizing faults or attacks is read as

$$\begin{aligned} E\dot{x} &= Ax + Bu^c, \\ y &= Cx. \end{aligned} \tag{4}$$

The dynamics in (4) are different from those in (1). The reason is the fact that u^c is not an exogenous signal vector; rather it includes intrinsic positive feedback from system states, as we explained in the forth item in the previous paragraph.

C. Illustrative Example

Consider the IEEE 9 bus network in Fig. 1. Suppose the power system is under a *Dynamic Load Altering Attack* (D-LAA) against demand response [4]. The adversary exploits cyber-physical techniques to remotely control the trajectory of aggregated power consumption of certain load types at certain victim load bus(es) based on a positive feedback mechanism from the grid frequency. D-LAAs can destabilize power system. A class of D-LAAs is implemented by hacking into the control mechanisms in frequency-responsive loads [4].

The dynamics of the system in Fig. 1 under a D-LAA can be described by (4), where parameters of matrices E and A are as in [17]. We assume that all three generators have AGC, i.e., $P^G = 0$. Also, P_6^L and P_9^L are affected by D-LAA through the adversary's proportional controllers, with gains 25, and 24, respectively, by taking feedback from ω_3, see [4]. Accordingly, the entries in rows 6 and 9 in attack vector f are non-zero. All buses are equipped with PMUs, except for bus 7.

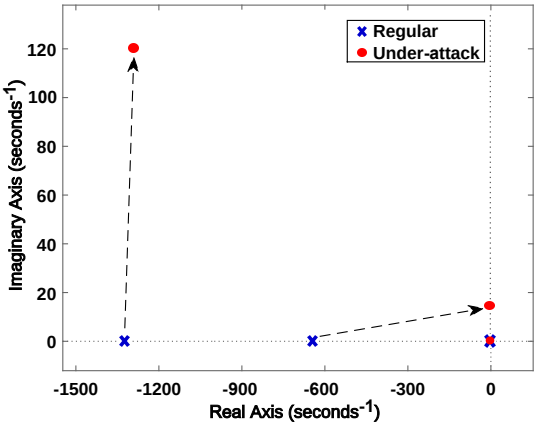

Figure 2. An example on how a destabilizing fault or attack can move the dominant eigenvalues of the power system matrix towards the $j\omega$ axis.

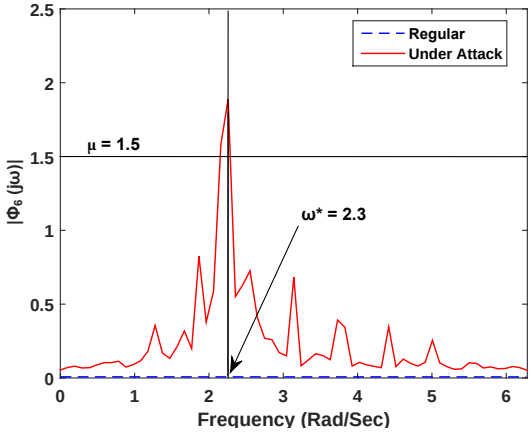

Figure 3. The attack in Section II-C creates a clear signature on frequency ω^* of the FFT magnitude of frequency deviation signal at load bus 6.

Fig. 2 shows how a destabilizing D-LAA changes the power system dynamics by moving the dominant eigenvalues of its system matrix towards the $j\omega$ axis. The power system frequencies at different buses start deviating from their nominal value, i.e., 60 Hz, putting the system at the margin of instability.

One can evaluate the destabilizing impact of the attack by performing a *frequency-domain* analysis. This requires taking the Fast Fourier Transform (FFT) [18] of the measurement outputs. The results are shown in Fig. 3 for both the regular and under-attack scenarios. Here, $\Phi_6(j\omega)$ denotes the FFT representation of the power system frequency deviation at bus 6, i.e., φ_6. The magnitude of $\Phi_6(j\omega)$ is shown by $|\Phi_6(j\omega)|$. We can see a clear *signature* and a large beam at frequency ω^* in this figure for the case with the presence of the attack. The above aforementioned fault/attack signature in frequency domain provides the grid operator with an effective tool to *detect* the fault/attack through a proper data-driven analysis,

1949-3053 (c) 2017 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2017.2787690, IEEE Transactions on Smart Grid

as explained in [11]. Accordingly, to monitor the signature at ω^*, sampling frequency of sensors must be at least two times of ω^*. In this example, since $\omega^* = 2.3$, the minimum sampling frequency must be 4.6 radian per second or 0.73 Hz.

III. Location Identification: Main Ideas

A. Problem Statement

Consider a power system such as the one in Fig. 1. Suppose some fault(s) and/or attack(s) have affected a subset of inputs, such as the power generation level of certain generators and/or the power consumption level of certain loads, putting the system at the margin of instability. Suppose *the presence of the fault or attack has already been detected* using a frequency-domain data-driven analysis, such as the one in [11]. That is, for a given threshold μ, the following expression holds:

$$\exists\, i : |Y_i(j\omega)| \geq \mu, \tag{5}$$

where Y_i is the Fourier Transform of the ith entry of the output signal y in (4). Thus, the fault/attack frequency ω^* is known:

$$\omega^* = \arg\max_{\omega} |Y_i(j\omega)|. \tag{6}$$

Parameter μ can be obtained from historical data, c.f. [11].

The next step is to answer the following two questions:

- *How many* power system inputs are affected?
- *Which* power system inputs are the ones that are affected?

We seek to answer both questions by using power system measurements. Only those measurements that capture frequency information around ω^* are of potential use. Such measurements are often provided only by advanced power system sensors such as PMUs that are used to monitor/estimate the *states* of the power system, where the reporting rate is a fraction of a second [16]. Note that, traditional SCADA systems do *not* support the reporting rate needed for this type of analysis, since their reporting rate is in the order of minutes.

B. Location Identification

In this section, we propose a novel optimization-based approach to identify which power system input(s), i.e., generators or loads, are affected by destabilizing faults and/or attacks.

1) Baseline Time-Domain Approach: Based on the existing literature, a somewhat standard approach to solve the destabilizing fault/attack location identification problem is to combine an *unknown input observer* (UIO) with any detection method, such as the one in [11]. From [19, Definition 1], an UIO is defined for the system in (4). Its goal is to have estimation error vector approach zero asymptotically, despite the presence of the unknown input in the system. Different approaches can be used to design an UIO, e.g., see [20]. In principle, all approaches essentially seek to collect a time series of measurements $\hat{y}(t)$ from field sensors over a time interval D, and then reconstruct the unknown input signal $u^c(t)$ so as to minimize the residual observation error:

$$\|\hat{y}(t) - y(t)\|_2\,, \tag{7}$$

subject to the power systems state space equations in (4) as constraints. Ideally, (7) approaches zero asymptotically. Note that, the constraints must hold at any time instance $t \in D$. Once the UIO problem is solved and the unknown input signal $u^c(t)$ is reconstructed in time-domain, then one can identify the location(s) of the power system inputs that are affected by destabilizing fault/attack using, for example, the Fourier Transform of $u^c(t)$, see [11]. Accordingly, the set of affected power system inputs, denoted by $\mathcal{K}$, is obtained as:

$$\mathcal{K} = \{i \in \mathcal{B} \;\mid\; |U_i^c(j\omega^*)| \geq \mu\}. \tag{8}$$

2) Proposed Frequency-Domain Approach: The first fundamental step in our proposed approach is to transform the power system dynamics under destabilizing fault/attack in (4) from time-domain to frequency-domain. This can be done by applying the Fourier Transform to the model in (4) as follows:

$$E(j\omega\, X(j\omega) - x_0) = AX(j\omega) + BU^c(j\omega), \tag{9}$$

$$Y(j\omega) = CX(j\omega), \tag{10}$$

where x_0 denotes the power system's initial states in time domain. From (2), x_0 is related to y_0, i.e., the power system's initial outputs in time domain through $y_0 = Cx_0$.

We propose to identify destabilizing fault/attack location(s) by solving the following optimization problem:

$$\underset{X(j\omega^*),Y(j\omega^*),U^c(j\omega^*),x_0,I}{\textbf{minimize}} \quad \left\|\hat{Y}(j\omega^*) - Y(j\omega^*)\right\|_2 \tag{11a}$$

subject to

$$E(j\omega^*\, X(j\omega^*) - x_0) = AX(j\omega^*) + BU^c(j\omega^*), \tag{11b}$$

$$Y(j\omega^*) = CX(j\omega^*), \tag{11c}$$

$$\hat{y}_0 = Cx_0, \tag{11d}$$

$$\sum_{i\in\mathcal{B}} I_i = |\mathcal{K}|, \tag{11e}$$

$$|U^c(j\omega^*)| \leq \mathrm{diag}\,(I)\, U^{\max}, \tag{11f}$$

where the variables X, Y, and U^c are complex numbers, variable x_0 is scalar, and variable I is binary and defined as

$$I_i = \begin{cases} 1 & i \in \mathcal{K}, \\ 0 & i \notin \mathcal{K}. \end{cases} \tag{12}$$

The entry of I corresponding to location $i \in \mathcal{B}$ indicates whether or not the power system input i is a fault/attack location. The characteristics of problem (11) are as follows.

First, suppose we drop I as variable and also drop (11e) and (11f) as constraints. The remainder of the optimization problem in (11a)-(11d) is intended to reconstruct the frequency-spectrum of the unknown input signal $u^c(t)$, but *only* at frequency ω^*. Here, we make no effort in reconstructing the unknown input signal $u^c(t)$ at frequencies which are not ultimately of interest to the destabilizing fault/attack location identification problem. As we will see in Section III-D, this will not only drastically reduce the computation complexity and thus the delay in identifying the fault/attack location(s), but it also will enhance the design performance, in the sense that one can now identify the destabilizing fault/attack location(s) with fewer number of sampled measurements.

Second, the binary decision making framework in optimization problem (11) eliminates the need to separately apply the data-driven method in [11], unlike in the case of the baseline

1949-3053 (c) 2017 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2017.2787690, IEEE Transactions on Smart Grid

time-domain approach in Section III-B1. Here, we assume that the number of affected power system input(s) is given, i.e., the cardinality of set $\mathcal{K}$, denoted by $|\mathcal{K}|$, is known. Accordingly, in (11e), we make sure that exactly $|\mathcal{K}|$ entries of vector I are non-zero. This assumption will be relaxed later in Section III-C, where we develop an algorithm for the case where the number of affected location(s) is unknown.

Third, as for constraint (11f), it forces the frequency spectrum of the reconstructed unknown input signal $u^c(t)$ at each location i to have no signature at the fault/attack frequency ω^*, unless such input is indeed identified as a fault/attack location, i.e., $I_i = 1$. Notation $\mathrm{diag}\,(I)$ indicates a diagonal matrix with its diagonal entries being equal to the entries of vector I. The upper bound vector parameter $U^{\max}$ includes sufficiently large numbers in its entries. It can be obtained empirically.

One can explain the feasible set of optimization problem (11) by examining its constraints. Constraint (11d) specifies the initial state of the power system based on the initial output measurements. Since a destabilizing fault or attack may affect only the system inputs but not the system outputs, from (3), $\hat{y}_0$ can directly be obtained from any given x_0. Therefore, (11d) always results in a solution for x_0. Next, consider constraints (11e) and (11f). Any arbitrary choice of I that satisfies constraint (11e) would result in a feasible solution for $U^c(j\omega^*)$ in constraint (11f). Finally, given the feasible solutions for both x_0 and $U^c(j\omega^*)$, constraints (11b) and (11c) simply provide the evolution of system states and outputs from the initial state and inputs according to the system model in (4). Hence, corresponding to the obtained feasible solutions of x_0 and $U^c(j\omega^*)$, there always exist solutions for $X(j\omega^*)$ and $Y(j\omega^*)$. Therefore, we can conclude that problem (11) always has a feasible solution. Of course, the extent of the accuracy of such feasible solutions depends on how small one can make the residual error $\hat{Y}(j\omega^*) - Y(j\omega^*)$ in the objective function of problem (11).

Although problem (11) is nonlinear and mixed-integer, it is tractable. In fact, once we slightly reformulate constraint (11f), we can present it as two separate linear inequality constraints on real and imaginary components. Therefore, the nonlinearity in (11) is solely due to the convex quadratic objective function. Accordingly, problem (11) is a standard mixed-integer least-square problem with linear constraints. Now that we established the feasibility and tractability of optimization problem (11), one can use any optimization solver, such as MOSEK [21], to solve problem (11) precisely; or use a heuristic method, such as Distributed Search Algorithm (DSA) [22], to solve the problem approximately. Throughout this paper, we solve optimization problem (11) using the MOSEK solver within the CVX software package [21]. CVX is installed in MATLAB to facilitate solving convex optimization problems.

Before we end this section, we shall point out that, an alternative option for the design in this section is to conduct a similar analysis as in the baseline design in Section III-B1, but this time in frequency-domain, and accordingly develop an UIO in frequency-domain. However, in principle, there is no advantage in doing so, as far as the reconstruction of the unknown input signal is concerned. Interestingly, we are *not* really concerned in this paper with the reconstruction of the unknown input signal. The UIO would be simply a middle step for us to ultimately identify the location(s) of power system inputs that are affected by destabilizing fault or attack. That explains why we took a rather different approach to tackle the problem, as it was described earlier in this section.

C. Proposed Algorithm

Problem (11) was formulated based on the assumption that the *number* of affected power system inputs, i.e., parameter $|\mathcal{K}|$, is *known* in advance. However, this is not always the case. In fact, the number of affected inputs is often unknown in practice. Accordingly, we propose to first conduct a sensitivity analysis of the objective function in (11a) with respect to parameter $|\mathcal{K}|$. We will then utilize the results to develop an algorithm to identify destabilizing fault/attack location(s), when the number of such location(s) is unknown.

Let $F(|\mathcal{K}|)$ denote the optimal objective value of problem (11) for a given $|\mathcal{K}|$. Next, we introduce a new definition.

Definition 1 (**Sensitivity Function**). *The difference between two consecutive optimal objective values in* (11)*, is referred to as the* sensitivity *with respect to* $|\mathcal{K}|$ *and defined as*

$$S(|\mathcal{K}|) = F(|\mathcal{K}|) - F(|\mathcal{K}|+1), \quad |\mathcal{K}| = 1, ..., |\mathcal{B}| - 1. \tag{13}$$

The main properties of the above sensitivity function can be explained in a theorem, as it is presented next.

Theorem 1 (**Properties of Sensitivity Function**). *The sensitivity function,* $S(|\mathcal{K}|)$*, has the following two key properties:*

- *Non-negative Function:* $S(|\mathcal{K}|) \geq 0$
- *Non-increasing Function:* $S(|\mathcal{K}|+1) \leq S(|\mathcal{K}|)$

Proof: To prove the first property, recall from Section III-B2 that constraint (11e) determines the number of non-zero entries in vector I. Accordingly, constraint (11f) is equivalent to

$$|U_i^c(j\omega^*)| \leq 0 \qquad i \notin \mathcal{K}, \tag{14a}$$
$$|U_i^c(j\omega^*)| \leq U_i^{\max} \qquad i \in \mathcal{K}. \tag{14b}$$

Constraint (14b) is *less restrictive* than constraint (14a). Therefore, as we increase $|\mathcal{K}|$, we expand the feasible set, i.e., we make the optimization problem more relaxed. As a result, the optimal objective value in problem (11) either decreases or remains the same. Therefore, we can conclude that function $F(|\mathcal{K}|)$ is non-increasing. That is, we have:

$$F(|\mathcal{K}|+1) \leq F(|\mathcal{K}|). \tag{15}$$

From (13) and (15), and after reordering the terms, we have:

$$S(|\mathcal{K}) = F(|\mathcal{K}|) - F(|\mathcal{K}|+1) \geq 0. \tag{16}$$

Next, we prove the second property. According to the *mixed integer problem sensitivity analysis* in [23], the optimal objective value of problem (11) is a convex function of parameter $|\mathcal{K}|$. In other words, $F(|\mathcal{K}|)$ is a convex function. From the definition of convexity, for any $0 \leq \theta \leq 1$, we have:

$$F(\theta x + (1-\theta)y) \leq \theta F(x) + (1-\theta)F(y), \ \forall x, y. \tag{17}$$

1949-3053 (c) 2017 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2017.2787690, IEEE Transactions on Smart Grid

Algorithm 1: Frequency-Domain Location Identification

Inputs: Measurements, Fault/Attack Frequency.
Parameters: System Model, Threshold ϵ
Take Fourier Transform of $\hat{y}(t)$.
for $|\mathcal{K}| = 1$ **to** $|\mathcal{B}|$ **do**
  Solve optimization problem (11).
  if condition (21) holds **then**
    break
return $\mathcal{K}$

Suppose $\theta = 0.5, x = |\mathcal{K}|$, and $y = |\mathcal{K}| + 2$. We can derive:

$$\begin{aligned} F(|K|+1) &= F(0.5|K| + 0.5(|K|+2)) \\ &\leq 0.5F(|K|) + 0.5F(|K|+2), \end{aligned} \tag{18}$$

where the inequality is due to (17). Once we multiply both sides by two, and after reordering the terms, we have:

$$F(|\mathcal{K}|+1) - F(|\mathcal{K}|+2) \leq F(|\mathcal{K}|) - F(|\mathcal{K}|+1). \tag{19}$$

From (13) and (19), we can conclude the second property. ■

From the non-increasing property of the sensitivity function in Theorem 1, we can conclude that $S(1) \geq S(|\mathcal{K}|)$ for any $\mathcal{K}$. Accordingly, we can introduce a new definition for sensitivity.

Definition 2 (Normalized Sensitivity Function). *The normalized sensitivity function is defined as*

$$N(|\mathcal{K}|) = \begin{cases} 1 & |\mathcal{K}| = 0, \\ S(|\mathcal{K}|)/S(1) & |\mathcal{K}| \neq 0. \end{cases} \tag{20}$$

Corollary 1 (Identification Threshold). *For any arbitrary choice of parameter ϵ, there always exists a location set $\mathcal{K}$ for which the following conditions hold at the same time:*

$$\begin{cases} N(|\mathcal{K}|-1) & > \epsilon, \\ N(|\mathcal{K}|) & \leq \epsilon, \end{cases} \tag{21}$$

where $0 < \epsilon < 1$ is the identification threshold.

In Corollary 1, parameter ϵ specifies the residual error in state estimation. Set $\mathcal{K}$ is then selected through optimization to meet the limit on residual error that is set forth by parameter ϵ. The proposed frequency-domain location identification method, in presence of *uncertainty* about the number of affected power system inputs, is summarized in Algorithm 1.

According to Corollary 1, the number of affected inputs, i.e., $|\mathcal{K}|$, will increase by decreasing the value of ϵ. Decreasing ϵ does not change the fact that the inputs which are selected by Algorithm 1 are the ones that are most affected by the destabilizing fault or attack. For example, if decreasing ϵ results in selecting 3 instead of 2 inputs, then the third selected input is the third most affected input by the destabilizing fault or attack, e.g., due to the use of benign negative feedback but based on a state that is highly affected by the anomaly, see the illustrative example in Section III-D. Nevertheless, one should be careful in selecting parameter ϵ, e.g., by using historical data of different fault and attack scenarios, so as to maintain a desirable sensitivity of the location identification system.

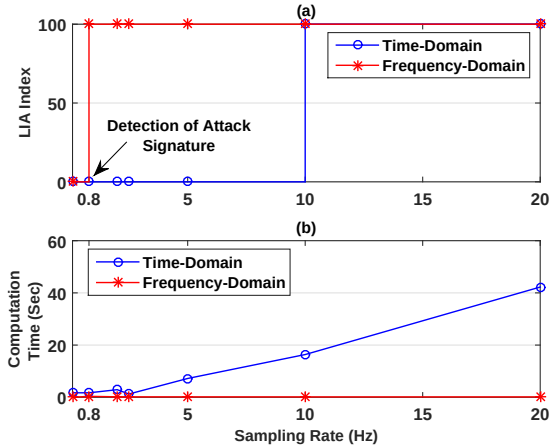

Figure 4. Comparing the performance of time-domain and frequency-domain location identification methods: a) LIA index; b) computation time.

Note that, both detection and location identification would be implemented in real-time in practice in order to allow immediate and proper reaction in presence of an anomaly. Accordingly, we conduct our analysis in a window-based fashion, similar to the Windowed FFT (W-FFT), e.g., in [24], where the FFT is taken for a window of measurements. The size of the window in our case studies is 300 seconds.

D. Illustrative Example

1) Location Identification Performance: The performance of a fault/attack identification algorithm can be evaluated in terms of two factors: the ability to find the location(s) that *are* affected; and the ability *not* to select the location(s) that are *not* affected. The latter is the ability to avoid false alarms. Therefore, we next introduce one metric, called *location identification accuracy* (LIA), that incorporates both factors:

$$\text{LIA } (\%) = \left[\frac{\#\text{ of Correct} - \#\text{ of Incorrect}}{\#\text{ of Actual}}\right]^{+} \times 100. \tag{22}$$

The numerator in (22) is the total number of correctly identified affected input(s) minus the total number of benign input(s) that are incorrectly identified as affected. The denominator is the true total number of the affected input(s). This fraction is always less than one. Using operator $[x]^{+} = \max\{x, 0\}$, LIA is always between zero and one, or between 0% and 100%. As an example, suppose the power system is under a multi-point destabilizing attack where four power system inputs are affected. Suppose a location identification algorithm is applied, and it correctly identifies three of the four affected inputs. Suppose the algorithm also incorrectly identifies a benign input as affected. In that case, the numerator is 3 - 1 = 2 and the denominator is 4. Accordingly, LIA is obtained as 50%.

Again consider the power system under destabilizing attack in the illustrative example in Section II-C. Suppose all buses are equipped with measurement devices, such as PMUs. Also, suppose the number of affected inputs (two) is known in advance. The performance, in terms of LIA, of the time-domain versus frequency-domain approaches are compared in Fig. 4(a). The x-axis is the time sampling rate of sensors. We can see that the LIA for the proposed frequency-domain

1949-3053 (c) 2017 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2017.2787690, IEEE Transactions on Smart Grid

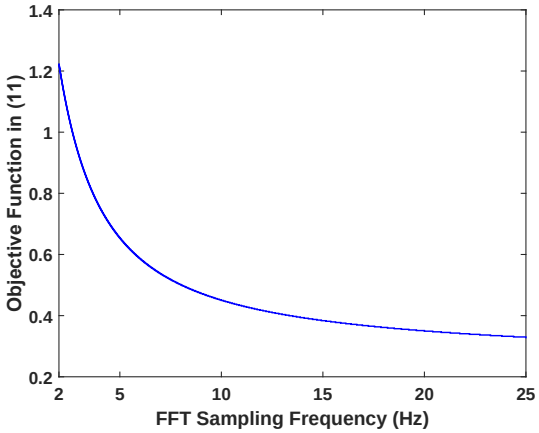

Figure 5. Residual error in state estimation obtained from objective function in (11) for different FFT sampling frequencies.

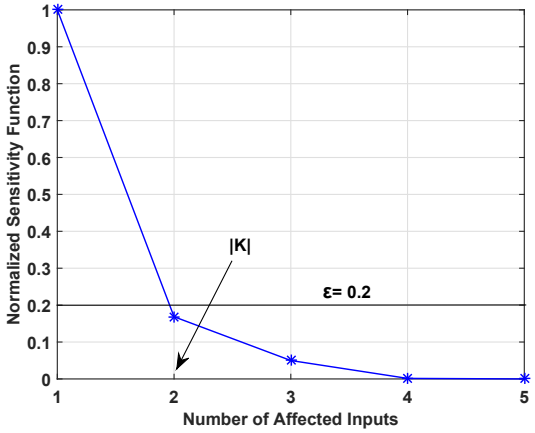

Figure 6. Identifying number of affected inputs, i.e., $|\mathcal{K}|$ using Algorithm 1.

Table I
IMPACT OF PARAMETER ϵ ON THE PERFORMANCE OF ALGORITHM 1.

ϵ	$\lvert\mathcal{K}\rvert$	$\mathcal{K}$	LIA
1	1	{**6**}	50%
0.2	2	{**6**,**9**}	100%
0.1	3	{**6**,**9**,7}	50%
0.01	4	{**6**,**9**,7,5}	0%
0.0001	5	{**6**,**9**,7,5,4}	0%
$\simeq$0	6	{**6**,**9**,7,5,4,8}	0%

method reaches 100% at only 0.8 Hz. This is in fact the same sampling rate that is required to detect the fault/attack in this example, see Section II-C. In contrast, the time-domain method has a zero LIA all the way up to 10 Hz.

Another important performance metric is computation time, i.e., the time needed by the algorithm to identify the location(s) of faults/attacks. This is shown in Fig. 4(b). We can see that, the time-domain method needs at least 17 seconds before it can reach 100% accuracy. In contrast, it takes less than 1 second for the frequency-domain method to reach 100% accuracy. The exact computation platform is not a major factor; of importance is rather the *relative* computation time. That being said, the computation platform in this example was an Intel Core i7-2600 with 3.4 GHz CPU and 8 GB memory.

2) Location Identification Reliability: From Section III-B, the extent of solution accuracy depends on how small one can make the *residual error* in the objective function in (11). Obviously, the true and accurate solution makes the residual error equal to zero; however, such zero residual error cannot be achieved in practice due to errors incurred by FFT. Specifically, FFT sampling frequency can add error to signal values in frequency domain, resulting non-zero *residual error* in state estimation, i.e., the difference between the estimated measurements and the actual measurements of the power system in frequency domain. To validate the reliability of the solution, the *residual error* is plotted versus the FFT sampling frequency in Fig. 5. We can see that, the solution accuracy can be improved by increasing the FFT sampling frequency.

3) Ability to Identify the Number of Affected Inputs: Next, suppose all buses, except for bus 7, are equipped with sensors that take two samples per second. Suppose $\mu = 1.5$, which allows detecting the presence of the fault/attack by examining the frequency-spectrum of the measurements at bus 6, as it was previously shown in Fig. 3. Now, suppose the identification threshold is $\epsilon = 0.2$, the unknown location(s) of affected power system inputs are identified using Algorithm 1. The results are shown in Fig. 6, where $N(|\mathcal{K}|)$ is plotted versus $|\mathcal{K}|$. The algorithm stops in this case at $|\mathcal{K}| = 2$, which is associated with solution $I = [0\,0\,1\,0\,0\,1]$. That is, $\mathcal{K} = \{6, 9\}$, which is exactly the correct locations of the attacks. Therefore, LIA = 100%, despite not knowing the number of affected inputs. Finally, the outcome of running Algorithm 1 for different choices of parameter ϵ is shown in Table I. If $\epsilon = 1$, then only input 6 is identified, which is one of the two affected inputs. If $\epsilon = 0.2$, then inputs 6 and 9 are identified. This is the ideal result, because inputs 6 and 9 are the exact two affected inputs. As we keep decreasing the value of ϵ, inputs 6 and 9 will continue to be identified as the affected inputs; however, additional benign inputs will be added to set $\mathcal{K}$, which degrades the LIA.

IV. HIERARCHICAL APPROACH

One possible application of the methodology developed in Section III is in WAMS to conduct fault and attack location identification in a *hierarchical* fashion. Consider a typical WAMS data collecting and data processing network, as in Fig. 7. In practice, it is divided into several *areas*. Multiple PMUs are often installed in each area, providing synchrophasor measurements at high resolutions, e.g., with 30 readings per second [16]. The PMUs in each area are connected to a Phasor Data Concentrator (PDC). PDCs are then connected to the control center. Applications of synchrophasors include state estimation, parameter identification, and model validation [16].

The way that a large-scale power system is partitioned into multiple areas for the purpose of distributed or hierarchical monitoring and control can affect the computational complexity and accuracy of the solutions. This issue is widely studied in the literature, e.g., see [25]–[27]. Accordingly, in this section, we assume that the choice of the areas is pre-determined based on a given WAMS structure and configuration because the setup for WAMS systems is often set up by operators and utilities based on a wide range of factors, and not just

1949-3053 (c) 2017 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2017.2787690, IEEE Transactions on Smart Grid

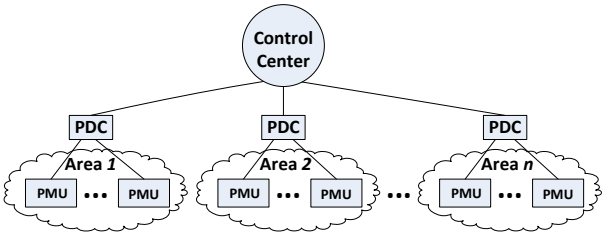

Figure 7. The hierarchical structure of a typical synchrophasor network.

for the purpose of fault/attack location identification. This is in fact one of the advantages of our proposed hierarchical approach that it is capable of being efficiently integrated into the existing WAMS without the necessity of designing and implementing additional and costly monitoring infrastructure only for the hierarchical location identification purpose. The focus in this section is on answering the following question: *How can we integrate a fault/attack location identification mechanism into a typical WAMS*? There are at least two main challenges to address. First, any such mechanism is preferred to be *hierarchical* to fit into the multi-level structure of WAMS networks. Second, any such mechanism must be *light-weight* in its computational burden so as to have minimal overhead on PDCs and their existing data processing tasks.

A. System Configuration

Suppose the set of all buses in each area within an n-area system is denoted by $\mathcal{A}_a$, for $a = 1, ..., n$. The buses in each area are classified as *internal* versus *boundary*. An internal bus does not have any direct line to a bus outside its own area. A boundary bus has at least one direct line to a bus in another area. Two areas are *neighbors* if there is at least one direct line between their boundary buses. PDCs are configured to collect data from not only the PMUs in their own area; but also the PMUs on boundary buses in their neighboring areas. For example, the PDC corresponding to $\mathcal{A}_5 = \{25, 26, 27, 28, 29, 37, 38\}$ in Fig. 8, collects PMU data from these buses: $\{2, 17, 25, 26, 27, 28, 29, 37, 38\}$. We refer to this latter set of buses as the *subsystem* of area $\mathcal{A}_5$.

B. Hierarchical Identification

The proposed hierarchical destabilizing fault/attack location identification algorithm is given in Algorithm 2. The central idea in this algorithm is to keep track of three sets, denoted by $\mathcal{P}$, $\mathcal{C}$, and $\mathcal{N}$. They specify the *previous*, *current*, and *next* areas to run Algorithm 1. In this regard, Algorithm 2 can be interpreted as an intelligent mechanism to hierarchically run Algorithm 1 across different areas in the system. In addition to breaking down the original *large system-wide* fault/attack identification problem into several *small area-level* identification tasks, Algorithm 2 is also capable of accurately identifying the fault/attack locations by examining only a small subset of the areas, see Section V. Set $\mathcal{T}$ keeps track of the identified location(s) as Algorithm 2 examines different areas.

The *Initial area* to examine, i.e., the starting point for Algorithm 2, is area $\mathcal{A}_s$, which is obtained as

$$s = \arg\max_{a} \underset{i \in \mathcal{A}_a}{\text{maximize}} |\hat{Y}_i(j\omega^*)|. \tag{23}$$

Algorithm 2: Coordination Algorithm

1 **Inputs:** Measurements Grouped into Subsystems.
2 **Parameters:** System Model.
3 **Initialization:** $\mathcal{P} = \{\}, \mathcal{C} = \{\mathcal{A}_s\}, \mathcal{T} = \{\}$.
4 **repeat**
5 $\mathcal{N} \leftarrow \{\}$
6 **for** any area $\mathcal{A}_i \in \mathcal{C}$ **do**
7 Run Algorithm 1 on subsystem of $\mathcal{A}_i$ to obtain $\mathcal{K}$.
8 **for** any boundary bus $j \in \mathcal{K} \setminus \mathcal{A}_i$ **do**
9 $\mathcal{N} \leftarrow \mathcal{N} \cup \{\mathcal{A}_a | j \in \mathcal{A}_a\}$
10 $\mathcal{T} \leftarrow \mathcal{T} \cup (\mathcal{K} \cap \mathcal{A}_i)$
11 $\mathcal{P} \leftarrow \mathcal{P} \cup \mathcal{C}$
12 $\mathcal{C} \leftarrow \mathcal{N} \setminus \mathcal{P}$
13 **until** $\mathcal{C} = \{\}$
14 **return** $\mathcal{T}$

Here, we start with the area that has detected the strongest fault/attack signature in the frequency spectrum.

The operation of Algorithm 2 is as follows. The outer loop in lines 4 to 13 is executed until the algorithm stops. The inner loop in lines 6 to 10 runs Algorithm 1 in all areas within set $\mathcal{C}$. The next areas to run Algorithm 1 are decided in line 9 based on the boundary buses that are identified as fault/attack locations. Only the internal buses that are identified as fault/attack locations are added to set $\mathcal{T}$ in line 10. From lines 11 and 12, set $\mathcal{C}$ is updated to identify a new set of areas in the next round of the algorithm. The algorithm ends if set $\mathcal{C}$ is empty, i.e., there is no need to examine any further area.

It is worth clarifying that the accuracy of the location identification approach can reach 100%, i.e., LIA=100%, when it is implemented in a centralized fashion, as long as ϵ is set properly. However, there is no similar guaranty for the hierarchical approach to achieve 100% accuracy. This is because the hierarchical approach involves *model decomposition* and such model decomposition creates *additional residual error* in the input observation aspect of the proposed design. Of course, as we will show in our case studies in Section V, the performance loss is not significant, at only 6%.

V. Additional Case Study

Consider the IEEE 39-bus test system in Fig. 8. The parameters in (1), and the loads at load buses, are set as in [28]. All generator and load buses are equipped with PMUs. The grid is partitioned into five areas. Without loss of generality, the destabilizing anomaly is assumed to be due to D-LAAs [4]. We simulated 200 different D-LAA scenarios. In scenarios 1 to 80, 81 to 120, 121 to 160, 161 to 180, 181 to 200, the adversary compromised one, two, three, four, and five power system inputs, respectively. The number of affected power system inputs is assumed to be unknown to our algorithm. The adopted test procedure tends to examine the following main features of the proposed hierarchical approach.

1) Location Identification Performance: We aim to compare the *centralized* location identification approach in Algorithm 1 for the entire power system versus the *hierarchical*

1949-3053 (c) 2017 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2017.2787690, IEEE Transactions on Smart Grid

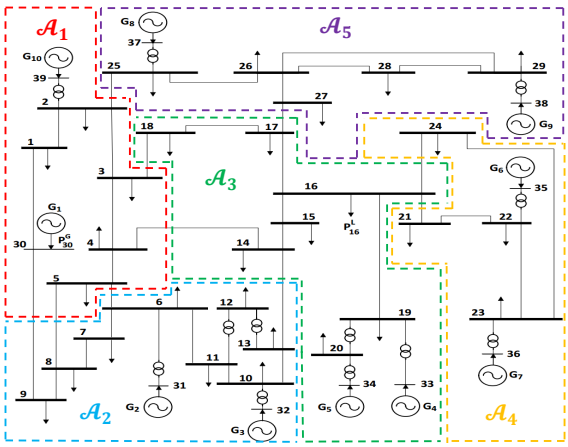

Figure 8. The IEEE 39 bus test system is partitioned into five areas.

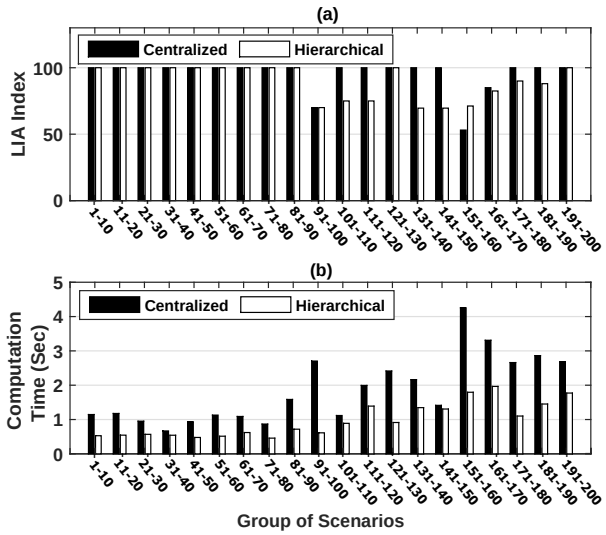

Figure 9. Comparing the centralized and hierarchical location identification methods across 200 scenarios: a) Average LIA; b) Average computation time.

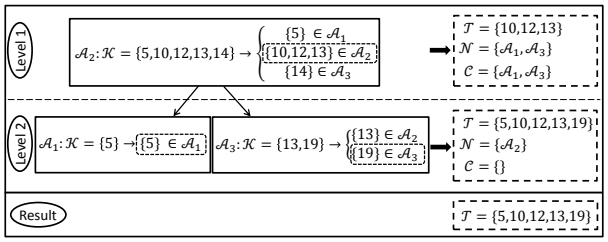

Figure 10. An example for step-by-step operation of the hierarchical approach.

approach in Algorithm 2. The results are shown in Fig. 9(a). The choice of victim bus(es) in all ten scenarios is the same within each test group, but the choices of anomaly feedback gains are different in each scenario. In total $20 \times 10 = 200$ cases are examined. Due to space limitation, we grouped together the scenarios with the same choice of victim buses and showed their average results in one bar, thus showing a total of 20 bars for each design setup. We can see that the hierarchical approach can work almost as good as the centralized approach. While the average LIA across the 200 test scenarios is 95% for the centralized approach, it drops only by 6% to 89% in the hierarchical approach. In return, the hierarchical approach provides *a much better performance with respect to computation time*, as shown in Fig. 9(b). On average, the computation time for the hierarchical approach is almost half of that for the centralized approach, i.e., 0.98 second versus 1.86 second.

Of interest is the perfect 100% LIA for both centralized and hierarchical designs on the *first 80* scenarios in Fig. 9(a), i.e., the first 8 bars. Recall from the setup of our case studies that, only one power system input is affected in each of these 80 scenarios. Accordingly, these are the cases that are more likely to occur in practice. The hierarchical approach improves the computation time significantly in all these 80 scenarios, without degrading the performance in location identification.

2) Hierarchical Monitoring: The step-by-step details of running Algorithm 2 for scenario number 200 is depicted in Fig. 10. Similar diagrams can be plotted for every other scenario. From Fig. 10, Algorithm 2 starts with $s = 2$, and by running Algorithm 1 on the subsystem of area $\mathcal{A}_2$. This results in identifying buses 5, 10, 12, 13, 14 as potential fault/attack locations. Buses 10, 12, and 13 are internal to area $\mathcal{A}_2$. Therefore, they are permanently added to set $\mathcal{T}$. However, buses 5 and 14 are boundary buses, as they belong to area $\mathcal{A}_1$ and area $\mathcal{A}_3$, respectively. Next, areas $\mathcal{A}_1$ and $\mathcal{A}_3$ are considered to run Algorithm 1. At the second level of the algorithm, running Algorithm 1 in area $\mathcal{A}_1$ results in identifying bus 5; and running Algorithm 1 in area $\mathcal{A}_3$ results in identifying buses 13 and 19. Bus 5 is internal to area $\mathcal{A}_1$ and bus 19 is internal to area $\mathcal{A}_3$. Therefore, they are added to set $\mathcal{T}$. Note that, bus 13 was already added to set $\mathcal{T}$ in the first level of the algorithm. We reach $\mathcal{C} = \{\}$ at this point. Therefore, the algorithm stops. The final set of identified fault/attack locations is $\mathcal{T} = \{5, 10, 12, 13, 19\}$.

VI. Conclusions

A novel optimization-based approach was proposed to identify the location(s) of destabilizing faults and attacks in power systems using synchronized measurements. The proposed method works in frequency-domain. It makes direct use of the information that is obtained during the detection phase. Compared to its time-domain counterpart, it needs much lower time-resolution in power system measurements. It does not require knowing the number of affected input location(s). It is also more computationally efficient. Importantly, it is well-suited to be deployed in wide area monitoring systems to do fault/attack location identification in a hierarchical fashion. Illustrative examples and extended case studies were presented in IEEE 9 and 39 bus test cases to verify the accuracy and efficiency of the proposed location identification algorithms.

References

[1] E. Hammad, A. M. Khalil, A. Farraj, D. Kundur, and R. Iravani, "A class of switching exploits based on inter-area oscillations," *IEEE Trans. Smart Grid*, vol. PP, no. 99, Feb. 2017.

[2] J. Yan, C. C. Liu, and M. Govindarasu, "Cyber intrusion of wind farm scada system and its impact analysis," in *Proc. of IEEE/PES Power Systems Conference and Exposition (PSCE)*, Phoenix, AZ, Mar. 2011.

[3] D. Soudbakhsh, A. Chakrabortty, F. Alvarez, and A. Annaswamy, "A delay-aware cyber-physical architecture for wide-area control of power systems," *Control Engineering Practice*, vol. 60, no. 1, Mar. 2017.

1949-3053 (c) 2017 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2017.2787690, IEEE Transactions on Smart Grid

[4] S. Amini, F. Pasqualetti, and H. Mohsenian-Rad, "Dynamic load altering attacks against power system stability: Attack models and protection schemes," *IEEE Trans. Smart Grid*, vol. PP, no. 99, Oct. 2016.

[5] Y. Guo, D. J. Hill, and Y. Wang, "Global transient stability and voltage regulation for power systems," *IEEE Trans. Power Systems*, vol. 16, no. 4, pp. 678–688, Aug. 2002.

[6] L. Meegahapola and D. Flynn, "Impact on transient and frequency stability for a power system at very high wind penetration," in *Proc. of IEEE PES General Meeting*, Minneapolis, MN, Jul. 2010.

[7] C. Rehtanz and J. Bertsch, "Wide area measurement and protection system for emergency voltage stability control," in *Proc. of IEEE Power Engineering Society Winter Meeting*, New York, NY, Jan. 2002.

[8] C. Liu, Z. Chen, C. L. Bak, and Z. Liu, "Adaptive voltage stability protection based on load identification using phasor measurement units," in *Proc. of IEEE APAP*, Beijing, China, Oct. 2011.

[9] P. Srikantha and D. Kundur, "A DER attack-mitigation differential game for smart grid security analysis," *IEEE Trans. Smart Grid*, vol. 7, no. 3, pp. 1476 – 1485, Aug. 2015.

[10] M. Izbicki, S. Amini, C. R. Shelton, and H. Mohsenian-Rad, "Identification of destabilizing attacks in power systems," in *Proc. of IEEE American Control Conference*, Seattle, WA, May 2017.

[11] S. Amini, F. Pasqualetti, and H. Mohsenian-Rad, "Detecting dynamic load altering attacks: A data-driven time-frequency analysis," in *Proc. of IEEE Smart Grid Communications*, Miami, FL, Nov. 2015.

[12] Y.-G. Zhang, Z.-P. Wang, J.-F. Zhang, and J. Ma, "Fault localization in electrical power systems: A pattern recognition approach," *Int. Journal of Electrical Power & Energy Systems*, vol. 33, pp. 791–798, Mar. 2011.

[13] A. Teixeira, H. Sandberg, and K. H. Johansson, "Networked control systems under cyber attacks with applications to power networks," in *Proc. of IEEE American Control Conference*, Baltimore, MD, Jul. 2010.

[14] F. Pasqualetti, F. Dorfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," *IEEE Trans. Automatic Control*, vol. 58, no. 11, pp. 2715–2729, Jun. 2013.

[15] J. D. Glover, M. S. Sarma, and T. J. Overbye, *Power System Analysis and Design*, 5th ed. Cengage Learning, 2009.

[16] A. G. Phadke and J. S. Thorp, *Synchronized Phasor Measurements and Their Applications*. Springer International Publishing, 2017.

[17] http://www.kios.ucy.ac.cy/testsystems/index.php/dynamic-ieee-test-systems.

[18] P. Duhamel and M. Vetterli, "Fast fourier transforms: a tutorial review and a state of the art," *Signal processing*, vol. 19, no. 4, Apr. 1990.

[19] J. Chen, R. J. Patton, and H.-Y. Zhang, "Design of unknown input observers and robust fault detection filters," *International Journal of control*, vol. 63, no. 1, pp. 85–105, Jan. 1996.

[20] S.-H. Wang, E. Wang, and P. Dorato, "Observing the states of systems with unmeasurable disturbances," *IEEE Trans. Automatic Control*, vol. 20, no. 5, pp. 716–717, Oct. 1975.

[21] M. Grant and S. Boyd, "CVX: Matlab software for disciplined convex programming, version 2.1," http://cvxr.com/cvx, Mar. 2014.

[22] P. Civicioglu, "Backtracking search optimization algorithm for numerical optimization problems," *Applied Mathematics and Computation*, vol. 219, no. 15, pp. 8121–8144, Apr. 2013.

[23] A. Pertsinidis, I. Grossmann, and G. McRae, "Parametric optimization of MILP programs and a framework for the parametric optimization of MINLPs," *Computers & Chemical Eng.*, vol. 22, pp. 205–212, 1998.

[24] F. Zhang, Z. Geng, and W. Yuan, "The algorithm of interpolating windowed FFT for harmonic analysis of electric power system," *IEEE Trans. Power Delivery*, vol. 16, no. 2, pp. 160–164, Apr. 2001.

[25] V. Pichai, M. E. Sezer, and D. D. Siljak, "A graph-theoretic algorithm for hierarchical decomposition of dynamic systems with applications to estimation and control," *IEEE Trans. Systems, Man, and Cybernetics*, vol. 13, no. 2, pp. 197–207, Mar. 1983.

[26] M. Vidyasagar, "Decomposition techniques for large-scale systems with nonadditive interactions: Stability and stabilizability," *IEEE Trans. Automatic Control*, vol. 25, no. 4, pp. 773–779, Aug. 1980.

[27] M. E. Sezer and D. D. Siljak, "On structural decomposition and stabilization of large-scale control systems," *IEEE Trans. Automatic Control*, vol. 26, no. 2, pp. 439–444, Apr. 1981.

[28] http://sys.elec.kitami-it.ac.jp/ueda/demo/WebPF/39-New-England.pdf.

Sajjad Amini (S'14) received the M.Sc. degree in electrical engineering - control systems from Amirkabir University of Technology, Tehran, Iran, in 2012. He is currently working toward his Ph.D. degree in electrical engineering - smart grid at the University of California, Riverside, CA, USA. His research interests include power system dynamics, cyber-physical security, demand response, Wide Area Monitoring Systems (WAMS), and large scale control systems.

Fabio Pasqualetti (S'07-M'13) is an Assistant Professor in the Department of Mechanical Engineering, University of California, Riverside. He completed a Phd degree in Mechanical Engineering at the University of California, Santa Barbara, in 2012, a Laurea Magistrale degree (M.Sc.) in Automation Engineering at the University of Pisa, Italy, in 2007, and a Laurea degree (B.Sc.) in Computer Engineering at the University of Pisa, Italy, in 2004. His main research interest is in secure control systems, with application to multi-agent networks, distributed computing, and power networks. Other interests include vehicle routing and combinatorial optimization, with application to distributed area patrolling and persistent surveillance, and computational neuroscience.

Masoud Abbaszadeh (S'06-M'08-SM'16) received the B.Sc., M.Sc. and Ph.D. degrees in electrical engineering from Amirkabir University of Technology, Tehran, Iran, Sharif University of Technology, Tehran, Iran, and University of Alberta, Edmonton, AB, Canada in 2000, 2002 and 2008, respectively. Currently, he is with GE Global Research, Niskayuna, New York, USA. From 2008 to 2011, he was with Maplesoft, Waterloo, ON, Canada. He was the principal developer of MapleSim Control Design Toolbox and was a member of a research team working on the Maplesoft-Toyota joint projects. His current research interests include estimation and detection theory, robust and nonlinear filtering and statistical machine learning with applications such as cyber-physical security, smart grid and renewable power generation. Dr. Abbaszadeh is an Associate Editor of Intelligent Industrial Systems (Springer) and serves as Technical Program Committee member in various conferences.

Hamed Mohsenian-Rad (S'04-M'09-SM'14) received the Ph.D. degree in electrical and computer engineering from the University of British Columbia Vancouver, BC, Canada, in 2008. He is currently an Associate Professor of electrical engineering at the University of California, Riverside, CA, USA. His research interests include modeling, data analytics, and optimization of power systems and smart grids. He received the National Science Foundation CAREER Award 2012, the Best Paper Award from the IEEE Power and Energy Society General Meeting 2013, and the Best Paper Award from the IEEE Conference on Smart Grid Communications 2012. He serves as an Editor for the IEEE TRANSACTIONS ON SMART GRID and the IEEE POWER ENGINEERING LETTERS.

1949-3053 (c) 2017 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.