Detection and Characterization of Intrusions to Network Parameter Data in Electric Power Systems

Daniel K. Molzahn, *Member, IEEE* and Jianhui Wang, *Senior Member, IEEE*

***Abstract*—The potential for cyberattacks is an emerging challenge to maintaining reliable and economic operation of electric power systems. Possible cyberattacks include intrusions to the parameter data at a control center. In this class of attacks, algorithms at the control center are correctly executed, but the attacker's modification of the associated parameter data yields improper results. This paper proposes an algorithm for detecting and characterizing cyberattacks to the network parameter data, with specific application to optimal power flow problems. The proposed algorithm evaluates whether historical operating point data are consistent with the network parameters. Inconsistencies indicating potential cyberattacks are characterized using historical operational data (power injections and voltage phasors) along with network parameter data. Simulated test cases illustrate the proposed algorithm's detection and characterization capabilities.**

***Index Terms*—Cybersecurity, Optimal power flow**

I. Introduction

CYBERSECURITY is a major concern in the operation of electric power systems. The substantial public interest in power system cybersecurity is demonstrated by publications in the popular press (e.g., a recent Associated Press investigation [1] and a bestselling book [2]) as well as industry and government reports (e.g., [3]–[5]). The research community has made significant efforts to detect and respond to cyberattacks on power systems. These efforts relate to securing the information technology infrastructure (e.g., improving authentication and encryption) as well as work in power systems engineering to identify and mitigate cyberattacks.

Much cybersecurity-related work has focused on sensor and control networks. The power systems literature includes a plethora of studies regarding false data injection attacks on state estimation [6]–[17]. Other related publications include [18] and [19], which focus on the impact of false data injection attacks on real-time markets, [20] and [21], which focus on attacks to phasor measurement unit (PMU) networks, and [22], which analyzes likely attacker strategies for false data injection attacks. Other literature considers cyberattacks on demand response programs [23], smart meters with load disconnection capabilities [24], automatic generation control [25], and modal estimation algorithms [26].

Another class of attacks modifies the data corresponding to power system parameters stored at a control center (e.g., transmission line impedances, generator limits, shunt admittances, etc.). In this class of attack, power system algorithms are executed correctly but with inaccurate parameter values. Changing the parameter values may alter market outcomes, leading to potentially significant economic impacts, or to outages and physical damage resulting from specification of an unsafe operating point.

There is limited research related to this class of cyberattacks. Among the existing work, [27] proposes an algorithm that detects attacks on the parameter data associated with optimal power flow (OPF) problems. An OPF problem determines a minimum cost operating point for an electric power system subject to both network constraints and engineering limits. The algorithm in [27] applies Principle Component Analysis (PCA) to historical data in order to detect an anomalous operating point. Using PCA, [27] constructs "regular" and "irregular" subspaces from the historical data. An operating point that has a large projection onto the "irregular" subspace is flagged as suspicious, suggesting the potential for the operating point to have resulted from a cyberattack on the parameter values. Extension of this work in [28] uses a neural network approach to determine an appropriate threshold for flagging an operating point as anomalous, and related work in [29] applies a vector autoregressive model to detect network anomalies in distribution systems. Similar approaches use statistical analyses [30], [31] and graphical model based techniques [32] to detect changes to the network topology based on measurement data. Additional related work includes [33], which solves a graph matching problem to compare the characteristics of a historical, presumed-accurate reference network to the network data used in real-time operations.

Historical operational data, as used in [27]–[29], is less likely to be vulnerable to an attack since it is not needed for operational purposes. While network parameter data must be modified in near-real-time to account for changing conditions (e.g., line outages and changes to facility parameters due to weather conditions), there is little reason to modify historical data. Thus, access to historical data can be better restricted and secured without a significant trade-off in user convenience. For instance, historical data can be stored in an environment with "read only" access in real-time and restricted to a smaller subset of users.

One downside of using statistical approaches such as [27] is the potential for false positives due to a large change in operating point, which may result from, e.g., contingencies. For instance, a line failure may result in a new operating point that is significantly different than historic operation. If the new, post-contingency operating point has a large projection on the "irregular" subspace, a false-positive cyberattack warning

Daniel K. Molzahn is with the Energy Systems Division at Argonne National Laboratory, Lemont, IL, USA (email: dmolzahn@anl.gov).

Jianhui Wang is with the Department of Electrical Engineering at Southern Methodist University, Dallas, TX, USA (email: jianhui@smu.edu).

This work is supported by the U.S. Department of Energy (DOE)'s Office of Electricity Delivery and Energy Reliability.

could be triggered.

This paper proposes a complementary approach for identifying cyberattacks on network parameter data. Again, historical data are used for validation. However, rather than comparing the *current operating point* to historical operating point data as in [27]–[29], we propose to compare the *specified parameter data* to historical operating point data. Specifically, the proposed approach evaluates the feasibility of historical data (modified to consider specific operational conditions at the time, such as line outages) with the specified parameter values. With access to both the power injections and the voltages associated with historical operating points, the proposed approach calculates the residual of the current injection equations constructed using the specified parameter data. A large residual identifies a potential cyberattack and characterizes which parameter values are most likely to have been modified. Note that this approach is conceptually similar to many fault detection methods in that redundant measurements are used to identify parameter inconsistencies; see, e.g., [34]–[36].

This paper is organized as follows. Section II overviews the physics and associated parameter data of power system networks. Section III discusses the threat model considered in this paper. Section IV presents the proposed cyberattack detection and characterization algorithm. Section V applies the proposed algorithm to three test cases. The first test case illustrates the potential for a combined cyber and physical attack to affect power system reliability. The second test case demonstrates the potential impact to the market dispatch from an attack on the network parameters of an OPF problem. The third test case is a random attack on the parameters associated with a variety of lines. The proposed algorithm detects and characterizes all three attacks. Section VI concludes the paper.

II. Overview of the Power System Network Equations

The cyberattack detection and characterization algorithm proposed in this paper relies on the relationship between the voltage phasors and current injections in an electric power system. This section overviews this relationship in terms of complex voltage and current phasors and then discusses the equations for the active and reactive power injections.

Consider a balanced, single-phase equivalent model of an n-bus system where $\mathcal{N} = \{1, \ldots, n\}$ denotes the set of buses, $\mathcal{L}$ denotes the set of lines, and $(l, m) \in \mathcal{L}$ denotes the line from bus l to bus m.[1] Let $\mathcal{N}(i)$ denote the set of buses that are neighbors to bus i. The admittance matrix containing the network topology and electrical parameters is denoted $\mathbf{Y} = \mathbf{G} + \mathbf{jB}$, where $\mathbf{j}$ is the imaginary unit. Let $P_k + \mathbf{j}Q_k$ represent the active and reactive power injections, V_k the voltage phasor, and I_k the current injection phasor at each bus $k \in \mathcal{N}$. The network physics imposes a linear relationship between the voltage phasors and current phasors:

$$I = \mathbf{Y}V. \tag{1}$$

[1]Extension of the proposed algorithm to unbalanced network models is possible but not explicitly considered in this paper.

The relationship between the voltage phasors, current phasors, and power injections is

$$P_k + \mathbf{j}Q_k = V_k \cdot \overline{I}_k \qquad \forall k \in \mathcal{N} \tag{2}$$

where $\overline{(\cdot)}$ denotes the complex conjugate.

Given the importance of (1) and (2) to a wide variety of operational tasks (e.g., optimal power flow, state estimation, unit commitment, etc. [37]), accuracy of the parameters contained in the admittance matrix $\mathbf{Y}$ is key to reliable and economic operation of electric power systems.

III. Overview of the Cyberattack Threat Model and Defense Strategy Motivation

Much of the cybersecurity literature, e.g., [6]–[25], focuses on threats to data and control signals that are accessible to attackers in remote locations (generators, sensors at substations such as Phasor Measurement Units, etc.). These threats include false data injection attacks to the sensor measurements used for state estimation as well as malicious modifications to the control signals used for demand response programs, automatic generation control, etc. The challenges inherent to securing many remote locations suggests that an attacker may be able to more easily compromise these data and control signals. Previous literature has hence primarily focused on these threats.

In contrast to the remote locations studied in much of the previous literature, this paper considers attacks that are aimed at the control centers themselves. Power system control centers consolidate the measurement data from remote locations, run algorithms to compute the system state and appropriate control actions, and transmit control signals back to the remote locations. Control centers typically have significant security against cyberattacks, thus making them more challenging targets for attackers. However, their great importance in maintaining system reliability and economic efficiency makes cyberattacks to control centers particularly rewarding from an attacker's perspective. Highly motivated and resourced attackers may be able to penetrate even well-secured facilities such as power system control centers. As one relevant example, the Stuxnet worm infected thousands of industrial control systems, including a uranium enrichment facility [38].

To reduce the risk of cyberattacks on critical facilities such as power system control centers, the US Department of Homeland Security's National Cybersecurity and Communications Integration Center recommends a "defense-in-depth" strategy that provides multiple layers of security [39]. By augmenting security practices focused on information technology components, such as strong password requirements, firewalls, access controls, user training, etc., a defense-in-depth strategy for power system control centers can be strengthened via cyberattack identification and characterization approaches that exploit the physical aspects of the power system. One relevant approach is to ensure that various data are consistent with the physical laws of the power system. Indeed, related approaches are used extensively in the aforementioned power system cybersecurity literature relevant to remote data and control signals.

The class of cyberattacks considered in this paper consists of malicious modifications to the admittance matrix $\mathbf{Y}$. Specifically, an attacker is assumed to have obtained access to the

control center's database containing the network parameter data and is therefore able to modify the line impedance and shunt admittance parameters that determine the admittance matrix. Algorithms run at the control center use the admittance matrix parameters in a wide variety of algorithms, including state estimation, optimal power flow, unit commitment, etc. Even in the absence of attacks to the algorithms that manage system operations, an attack to the network parameters could result in economically inefficient operation or harm system reliability. For instance, a cyberattack on the network parameters may result in an optimal power flow algorithm computing an insecure operating point. Operating the system at this insecure point may either directly cause a failure or could be combined with physical attacks to cause a blackout. Moreover, an attack to network parameter data could lead to inaccurate state estimator computations that may be used to disguise other physical and cyber attacks.As discussed in the introduction, see [27]–[29], [33] for prior power systems research that recognizes the potential relevance of cyberattacks to the network parameter data.

While identifying potential strategies available to an attacker is not the focus of this paper, an attacker considered in this threat model could attempt to choose malicious network parameters that result in overloading of several key lines identified via a cascading failure analysis [40]. Failures of these key lines would cause a widescale blackout. Determining such malicious parameters could be achieved by solving a bi-level optimization problem. The upper-level problem chooses malicious network parameters that maximize the difference between the actual flows and the flows modeled by the attacked parameters. For a certain choice of attacked network parameters, these flows are determined by a lower-level problem that represents the OPF computed by the system operator. Formalizing and solving this bi-level optimization problem to determine an attacker's optimal strategy is a topic for future work. An attacker could also conceivably combine network parameter attacks and false data injection attacks. Such a combination could obfuscate an attacker's actions and possibly worsen the impact of an attack. Detailed investigation of the potential vulnerability to combinations of attacks on network parameter data and false data injection attacks is another topic for future work.

While the threat model in this paper considers an attacker that is capable of altering the database containing the network parameters, the attacker is assumed to be unable to modify the database of historical operational data. In particular, we make the following assumption:

Assumption 1 (Security of Historical Data)**.** *For various time points indexed by $t = 1, \ldots, T$, there exist historical operating point data consisting of power flow solutions (i.e., voltage phasors $V(t)$ and active and reactive power injections $P(t)+\mathbf{j}Q(t)$ at each bus in the system) and the corresponding network topology (i.e., a list of line outages at each time period t). These data are assumed to be accurate.*

Operational data are available in near-real-time from the output of the state estimator, and system operators generally archive operational data in order to perform post-event analyses. The proposed algorithm specifically uses the power injections and voltage phasors returned by the state estimator which are consistent with one another rather than the noisy measurement data that are inputs to the state estimator.

In contrast to network parameter data which must be changed in near real-time to account for, e.g., maintenance activities, line failures, construction of new transmission facilities, etc., modifications to historical operational data are much less prevalent. Thus, a large number of users may need to frequently modify system parameters relative to the number of users who need to edit historical operational data. Permissions for editing historical operational data can therefore be more restrictive in order to improve security without overly burdening users. Moreover, with no need for near real-time editing, historical data can be stored in a separate location that is more secure than the that used for the network parameter data. For instance, the historical data can be stored with "read-only" permissions for real-time access. The ability to separately store and enforce more restrictive access permissions for historical data makes the accuracy of historical data a reasonable expectation. Note that similar assumptions regarding the security of historical operational data are made in [27]–[29].

However, even if Assumption 1 is violated by a sophisticated attacker who compromises the databases of both the network parameters and the historical operational data, algorithms that aim to identify and characterize cyberattacks are still justified by a defense-in-depth strategy. Algorithms such as the one proposed in this paper provide an additional layer of protection in that an attacker must modify both the network parameter data and the historical operational data in a carefully selected manner that maintains mutual consistency between these data in order to avoid detection. Thus, the additional layer of security provided by algorithms such as the one proposed in this paper increases the complexity faced by an attacker, hence increasing the difficulty of successfully carrying out an undetected attack.

Moreover, algorithms such as the one proposed in this paper also increase the attacker's likelihood of triggering additional intrusion detection technologies. In particular, ensuring that an attack to the network parameter data is undetected by the algorithm proposed in this paper would require modifications to many rows of historical data. An attackers substantial change to the historical data is likely to leave a significantly different signature in the database logs than the behavior of typical non-malicious users. This raises the likelihood of the attacker being detected by other intrusion detection systems which monitor for such anomalous behavior, thus showing the benefit of the proposed algorithm as part of a defense-in-depth strategy. In other words, when implemented as part of a defense-in-depth strategy, the presence of algorithms such as the one proposed in this paper can deter and identify even the actions of sophisticated attackers.

IV. An Algorithm for Detecting Attacks to Network Parameters

In order to provide a layer of protection against the cyberattack threat model described in the previous section, this section proposes an algorithm for detecting and characterizing attacks to the network parameter data.

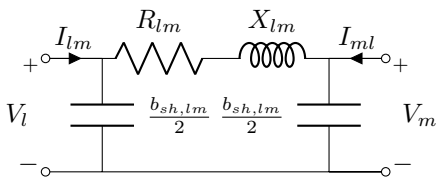


Fig. 1. Π-circuit line model.

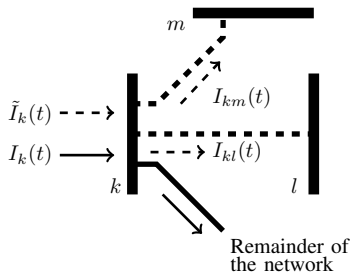


Fig. 2. Illustrative example of adjusting historical operational data to account for out-of-service lines. Lines $(k,m) \in \mathcal{L}^-(t)$ and $(l,k) \in \mathcal{L}^-(t)$ are out-of-service at time t. The solid arrows represent the currents associated with the in-service lines. The dashed arrows represent the currents which would have been induced by the historical voltage phasors if the out-of-service lines had been in-service at time t. (See equations (3) and (4).)

Algorithm 1 Cyberattack Detection and Characterization

Input: Historical operational data (for times $t = 1, \ldots, T$, the power injections $P(t) + \mathbf{j}Q(t)$, the voltage phasors $V(t)$, and a list of line outages), network parameter data in the admittance matrix $\mathbf{Y}$, the inconsistency threshold ϵ, and the singular value threshold ϵ_σ.

OFF-LINE COMPUTATIONS:

Compute current injections $I(t)$ using (2).

Compute modified current injections $\tilde{I}(t)$ to account for historical line outages using (4).

Optional: Compute the singular value decomposition of the matrix $\mathbf{V}$ and form $\hat{V}(t)$ and $\hat{I}(t)$ according to (8) with ϵ_σ in order to ensure detectability of any attack.

ON-LINE COMPUTATIONS:

Compute $r(t)$ using (5) (with $\hat{V}(t)$ and $\hat{I}(t)$ for $V(t)$ and $\tilde{I}(t)$ if using optional step 4).

if $||r(t)||_\infty \geq \epsilon$ for some $t \in \{1, \ldots, T\}$ **then**

    Indicate the possibility of a cyberattack.

    Characterize the possible attack by identifying lines $(l,m) \in \mathcal{L}$ where both $|r_l(t)| \geq \epsilon$ and $|r_m(t)| \geq \epsilon$ for some $t \in \{1, \ldots, T\}$ or shunt elements where $|r_i(t)| \geq \epsilon$ and $|r_k(t)| < \epsilon$, $\forall k \in \mathcal{N}(i)$.

A. Mathematical Description

The proposed approach for cyberattack detection and characterization is summarized in Algorithm 1. The algorithm first solves (2) using the power injections $P(t)+\mathbf{j}Q(t)$ at each time period $t = 1, \ldots, T$ to obtain the vector of current injection phasors $I(t)$.

The vector of current injections $I(t)$ is modified to account for the line outages specified in the historical data at each time period t. Using a Π-circuit model shown in Fig. 1 for the line (l,m) with admittance $g_{lm} + \mathbf{j}b_{lm} = 1/(R_{lm} + \mathbf{j}X_{lm})$ and total shunt susceptance $b_{sh,lm}$,[2] the current flow into terminal bus l is

$$I_{lm}(t) = (g_{lm} + \mathbf{j}b_{lm})(V_l(t) - V_m(t)) + \frac{b_{sh,lm}}{2}|V_l(t)|^2. \tag{3}$$

The current flow into terminal m of line (l,m) is given by (3) with the l and m indices switched. The relationship between the current flow and terminal voltage phasors given in (3) is next used to compute the current injections that would have been induced by the terminal voltage phasors in the historical data if the out-of-service lines had been in service. Specifically, the current injection vector $I(t)$ is modified to $\tilde{I}(t)$ as follows:

$$\tilde{I}_k(t) = I_k(t) + \sum_{(k,m)\in\mathcal{L}^-(t)} I_{km}(t) + \sum_{(l,k)\in\mathcal{L}^-(t)} I_{kl}(t), \quad \forall k \in \mathcal{N},\ t = 1, \ldots, T \tag{4}$$

where $\mathcal{L}^-(t)$ is the set of lines that are out of service at time t and subscripts indicate the entries of the corresponding vectors. (See Fig. 2 for an illustrative example.) By adding the current outflows that would have existed if the out-of-service lines in $\mathcal{L}^-(t)$ had been in-service, the modification (4) determines the current injections $\tilde{I}(t)$ that would have occurred if the historical network topology matched the network topology specified in the network parameter data, thus enabling a consistent comparison to the historical data. For simplicity, this modification considers network parameter data with all lines in service. Further analogous modifications to the current injection vector $\tilde{I}(t)$ are needed to remove the effect of any lines that are out-of-service in the network parameter data but were in-service in the historical data. Moreover, certain time-varying impacts on network parameters from, e.g., component aging, transformer tap statuses, etc. can be accounted for in a similar manner. Near-real-time updates to the network parameters from weather and temperature changes may be more difficult to distinguish from a cyberattack. While not currently widespread in practice, there are research efforts regarding near-real-time updates to network parameters based on weather conditions [42]–[44]. If such near-real-time updates become commonplace in practice, future work will be needed to study and adapt the proposed cyberattack detection and characterization algorithm. One possible approach for devices whose parameters have significant, near-real-time updates is to enforce a higher threshold value for identifying a possible cyberattack during periods where authorized changes to the associated parameters are expected, leaving a more stringent threshold for other time periods and the other devices' parameters.

After computing the current injections $\tilde{I}(t)$, the proposed algorithm computes the residual $r(t) \in \mathbb{C}^n$ of the network equation (1) at each time period, i.e.,

$$r(t) = \tilde{I}(t) - \mathbf{Y}V(t) \qquad t = 1, \ldots, T \tag{5}$$

The admittance matrix $\mathbf{Y}$ in (5) is constructed using the

[2]More detailed line models which include non-zero phase shifts and off-nominal voltage ratios can also be considered. The numerical results in Section V use the line model in MATPOWER [41].

network parameters currently specified in the database. Computation of (5) can be formulated by collecting the voltage and current phasors at each time period in the columns of corresponding matrices:

$$\mathbf{R} = \tilde{\mathbf{I}} - \mathbf{YV} \tag{6}$$

where $\mathbf{R}, \mathbf{V}, \tilde{\mathbf{I}} \in \mathbb{C}^{n \times T}$ are $\mathbf{R} = \begin{bmatrix} r(1) & \cdots & r(T) \end{bmatrix}$, $\mathbf{V} = \begin{bmatrix} V(1) & \cdots & V(T) \end{bmatrix}$, and $\tilde{\mathbf{I}} = \begin{bmatrix} \tilde{I}(1) & \cdots & \tilde{I}(T) \end{bmatrix}$.

A non-zero residual $r(t)$ at any time period t indicates an inconsistency between the historical operational data and the network parameters, which may be the result of a cyberattack. A cyberattack is detected using the infinity norm $||\cdot||_\infty$ (i.e., the maximum absolute value) of the residual:

$$||r(t)||_\infty \geq \epsilon \quad \text{for any} \quad t \in \{1, \ldots, T\} \tag{7}$$

where ϵ is a specified tolerance parameter. The parameter ϵ is chosen by operator experience in combination with an off-line study. Specifically, ϵ is determined by examining the consistency of historical operational data with known-accurate network parameter data; i.e., the historical level of consistency between the power injections and the voltage phasors resulting from the state estimator's solution.

Satisfaction of (7) indicates an inconsistency between the network parameter data and the historical operating point data that is suggestive of a cyberattack. Furthermore, the residual $r(t)$ also aids in characterizing the specific parameters that are attacked. Entries of the residual vector which satisfy $|r_i(t)| \geq \epsilon$ for some $t \in \{1, \ldots, T\}$ correspond to buses where the operational data and the network parameter data are inconsistent. The parameters for any line where both terminal buses have inconsistencies have potentially been subject to a cyberattack. A large residual at a bus (particularly if no neighboring buses have inconsistencies) suggests a potential cyberattack to the admittance parameter of a shunt element at that bus. See Algorithm 1 for a mathematical description of these conditions. Note that spurious characterizations may occur for unattacked lines whose terminal buses are both shared with other attacked lines (for instance, an unattacked line in parallel with an attacked line).

The percentage change in the network parameters that can be detected by the proposed algorithm depends on a variety of factors, including the threshold ϵ and the characteristics of the historical operational data. The user has direct control over the threshold ϵ, with smaller values resulting in more sensitive detection capabilities. While it is difficult to analytically determine the minimum percentage modifications that can be detected by Algorithm 1, the empirical results in Section V suggest that parameter modifications on the order of 2% are detectable for reasonable test cases.

With a focus on the detection and characterization of cyberattacks to the network parameter data, the question of mitigation and response is largely beyond the scope of this paper. However, we next briefly summarize suggestions regarding these issues. In the immediate aftermath of detecting and characterizing an attack, a reasonable initial response for the system operator is to verify the boundary results of state estimator and optimal power flow algorithms with neighboring operators who may have not been attacked. In combination with their knowledge of typical system operation, information from the neighboring operators could help engineers determine the actual state of the system and identify proper corrective actions as needed. The system operators could also coordinate with one another and with member utilities to develop a plan for recovering from a system parameter cyberattack suffered by any individual control center through redundancy at other control centers.

B. Augmenting the Historical Operating Point Data to Improve Detectability

An attack would remain undetected by the algorithm if the perturbation to the network parameter data, denoted $\Delta\mathbf{Y}$, was in the left nullspace of the voltage phasor matrix $\mathbf{V}$ in (6), i.e., $\Delta\mathbf{YV} = \mathbf{0}$ such that $\mathbf{R} = \tilde{\mathbf{I}} - (\mathbf{Y} + \Delta\mathbf{Y})\mathbf{V} = \mathbf{0}$. In other words, the left nullspace of the voltage phasor data matrix dictates the range of undetectable attacks. Use of historical data with little variation, and thus a large left nullspace, would leave an attacker with more freedom to modify parameters, while historical data that contains a wide range of operating points would highly constrain or eliminate an attacker's ability to remain undetected. The numerical simulations in Section V suggest that one year of hourly data is likely to be sufficient for highly restraining an attacker's capabilities in practice.

In order to further reduce or eliminate an attacker's flexibility to remain undetected, an off-line analysis can optionally be used to augment the historical data with "fictitious" loading scenarios that are consistent with known-accurate network parameter data and eliminate the left nullspace. The approach used in the optional step 4 of Algorithm 1 adds a set of basis vectors for the left nullspace of the matrix $\mathbf{V}$ to the historical voltage data. Specifically, consider a singular value decomposition $\mathbf{V} = \mathbf{M\Sigma N}$ where $\mathbf{M} \in \mathbb{C}^{n \times n}$ contains the left singular vectors, $\mathbf{\Sigma} \in \mathbb{C}^{n \times T}$ is a diagonal matrix containing the singular values, and $\mathbf{N} \in \mathbb{C}^{T \times T}$ contains the right singular vectors [45]. Let $\sigma = \{\sigma_1, \ldots, \sigma_\rho\}$ denote the set of singular values (with corresponding left singular vectors $\mu_i \in \mathbb{C}^n$, $i = 1, \ldots, \rho$) less than a specified threshold ϵ_σ, where ρ denotes the number of these singular values. (The numerical results in Section V use $\epsilon_\sigma = 1 \times 10^{-4}$.) Define the set of vectors $\hat{V}(t)$ and $\hat{I}(t)$ as

$$\hat{V}(t) = \begin{cases} V(t), & t = 1, \ldots, T, \\ \mu_{t-T}, & t = T+1, \ldots, T+\rho, \end{cases} \tag{8a}$$

$$\hat{I}(t) = \begin{cases} \tilde{I}(t), & t = 1, \ldots, T, \\ \mathbf{Y}\mu_{t-T}, & t = T+1, \ldots, T+\rho. \end{cases} \tag{8b}$$

By construction, the matrix $\hat{\mathbf{V}} = \begin{bmatrix} \hat{V}_1 & \cdots & \hat{V}_{T+\rho} \end{bmatrix}$ has an empty left nullspace. Thus, using $\hat{V}(t)$ and $\hat{I}(t)$ in (5) ensures that Algorithm 1 will detect any attack. While the numerical results in Section V use this approach, we emphasize that the proposed algorithm is capable of significantly restricting an attackers flexibility in remaining undetected even without augmenting $V(t)$ and $I(t)$ with the singular vectors, thus relying solely on historical operational data.

Note that the matrix $\mathbf{Y}$ in (8b) is constructed off-line from known-correct network parameters. An infrequently occurring (e.g., seasonal) off-line setting provides more opportunities for verification of the network parameter data by, for instance,

comparing power flow results with typical engineering intuition and system knowledge. For the purposes of the optional Step 4, we therefore assume the ability to access network parameter data that have not been attacked during the off-line stage in order to improve the algorithm's ability to detect attacks in the on-line stage (Steps 5–8).

We also emphasize that the step of computing fictitious operating points to ensure detection of all attacks is optional. As demonstrated in the following section, numerical experiments suggest that typical power system variability yields operating points that span a relatively wide range of the voltage subspace. Therefore, even with a non-empty left nullspace, the proposed algorithm still significantly restricts the modifications an attacker can make while remaining undetected. Thus, the optional Step 4 can be bypassed in case of any doubts regarding the validity of the network parameter data used in (8b).

C. Computational Effort

The computational effort required to execute Algorithm 1 is modest. Steps 2 through 4 in Algorithm 1 are computed off-line, negating the need for fast computational performance. Nevertheless, these steps can be computed quickly. The calculation of the current injections from the power injections and voltages in Step 2 is a computationally simple task that only requires one division operation per bus for each time period (i.e., $n \times T$ division operations). The modifications to the current injections in Step 3 are only conducted for the small number of lines that are out-of-service in each period (i.e., $\sum_{t=1}^{T} |\mathcal{L}^{-}(t)|$, where $|\mathcal{L}^{-}(t)|$ indicates the number of out-of-service lines at time t), and the requisite computations are again simple algebraic operations. The most computationally burdensome operation is the singular value decomposition of the $n \times T$ matrix $\mathbf{V}$ in the optional Step 4, but the fact that this computation is done off-line means that this step is tractable for even large systems with many measurements. For instance, the singular value decomposition for the test cases in Section V with several thousand buses and a year of hourly data is computed in approximately one minute on a typical laptop computer.

The on-line computations in Algorithm 1 are also tractable. Computation of (5) in Step 5 requires only a single sparse $n \times n$ matrix–vector multiplication and vector subtraction per time period. Equivalently, the voltage and current phasors at each time period can be collected as the columns of corresponding matrices to formulate the computation of (5) as a single matrix-matrix multiplication and subtraction (i.e., multiplication of the sparse $n \times n$ admittance matrix by the $n \times T$ matrix $\mathbf{V}$). Checking the residual in Step 6 and characterizing a possible cyberattack in Steps 7 and 8 are the result of maximization operation along the rows of an $n \times T$ matrix and a comparison operation over the resulting n values.

The modesty of the computational requirements is demonstrated empirically by the numerical results in the following section. In particular, computing the residual using a year of hourly data is accomplished for systems with thousands of buses in less than one second. Since many operationally relevant algorithms (e.g., state estimation, optimal power flow, etc.) are computed on timescales of seconds to minutes, Algorithm 1 is suitable for on-line applications. If the computational burden were problematic (perhaps for systems with tens of thousands of buses or with a larger quantity of historical data), the speed of the proposed algorithm could be improved by selecting a subset of historical data that captures most of the relevant variation. This can be accomplished off-line by evaluating the singular value decomposition of the matrix $\mathbf{V}$ in (6), as in the optional Step 4 of the algorithm.

V. Application to Test Cases

This section demonstrates the capabilities of Algorithm 1 to quickly detect and characterize attacks. After describing the test systems, three scenarios are used to illustrate possible cyberattacks and the performance of the proposed algorithm.

A. Descriptions of Test Cases and Computational Setup

This section uses simulated operational data for three test cases: the RTS-96 system [46], [47], the 2869-bus PEGASE system [48], and the 1354-bus PEGASE system [48]. The latter two test cases represent different portions of the European electric grid. For all three test cases, one year of hourly load data is constructed using the seasonal, hourly, and weekly load variation prescribed for the RTS-96 system [46], [47], multiplied at each bus by a normal random variable with mean 1 and standard deviation of 5%. Over the year of data, the total load demand ranges from 100% to 34% of the summer peak loading, which is comparable to the load demand variations for typical power systems. The test cases also consider generator and line outages, with each line and generator having a failure probability of 0.05% per hour. For simplicity, only line failures that did not result in islanding of the network were considered. The recovery times for the failure of lines and generators were specified to be eight hours and four hours, respectively. The historical operational data is generated by applying MATPOWER's AC OPF algorithm [41] to each hour of data.

Note that practical OPF implementations often rely on the DC power flow approximation rather than the AC power flow model. This necessitates a postprocessing step with the possibility of various solution adjustments in order to ensure AC feasibility. Since these adjustments are difficult to model, the test cases used in this paper directly solve AC OPF problems. Depending solely on historical operational data from state estimator solutions, the proposed algorithm is not reliant on the specific power flow model.

These choices for the simulations determine the range of operational data that is generated. As discussed in Section IV, the variation in the operational data input to the proposed algorithm determines an attacker's freedom to perform an undetected attack (in the absence of the optional step 4 of Algorithm 1).

Using only historical operational data (i.e., without step 4), Algorithm 1 is successful in detecting and characterizing many attacks using a year of simulated data created with the aforementioned simulation specifications. To exemplify this, Figs. 3a, 3b, and 3c show the the singular values of the

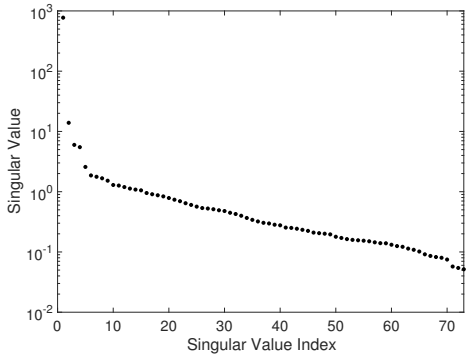
matrix $\mathbf{V}$ defined in (6) for the RTS-96 system, the 2869-bus PEGASE system, and the 1354-bus PEGASE system, respectively. With all non-zero singular values, $\mathbf{V}$ for the RTS-96 system has full row rank, and hence all attacks will be detected by Algorithm 1 without need for augmenting the historical data using (8). In contrast, the left nullspaces for the 2869-bus and 1354-bus PEGASE systems are not empty, with 8.4% and 2.2%, respectively, of the singular values being less than 1×10^{-6}. Ensuring the detectability of all attacks for these systems can be achieved by augmenting the historical data with sets of basis vectors for the left nullspaces as discussed in Section IV-B. Note that the small dimensions of the left nullspaces significantly restricts an attacker's ability to remain undetected for these test cases even without this augmentation.

The computational experiments were conducted with MATLAB version 2016a using a laptop computer with a quad-core 2.70 GHz Intel i7 processor and 16 GB of RAM running Windows 7.

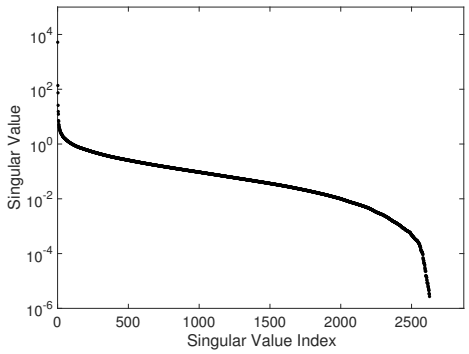
B. RTS-96 System: Combined Cyber/Physical Attack

The first scenario is a combined cyber and physical attack on the RTS-96 system operating at peak loading. The attacker modifies the shunt susceptances associated with three lines in the RTS-96 system. (See Table I for the attack details.) The system operator solves an AC OPF using the attacked line parameter values. The OPF solution is feasible (all lines within their normal flow limits) in the problem using the attacked system parameters. However, as determined by a power flow solution using the unattacked network parameters with power injections dictated by the OPF solution, the actual flows on the three attacked lines are approximately 30% greater than their emergency ratings. This would result in failure of these lines, which places the system in an insecure operating state. If the attacker followed the cyberattack with a physical attack that tripped one additional line (see Table I), the OPF problem becomes infeasible even considering the emergency line flow limits and allowing for redispatch of all generators over their entire operating ranges. (The infeasibility of the OPF problem is verified using a semidefinite programming relaxation [49], [50].) The system operator would be required to resort to unplanned load shedding or a blackout would ensue. This scenario thus illustrates the potential damage that may be inflicted by malicious modifications to the network parameter values, even for relatively robust systems such as the RTS-96 system. This scenario also demonstrates how a cyberattack can place the system in a vulnerable state. An attacker who has limited ability to destroy physical infrastructure can thus leverage the cyberattack to cause a more significant blackout than may be possible with either a cyberattack or a physical attack separately.

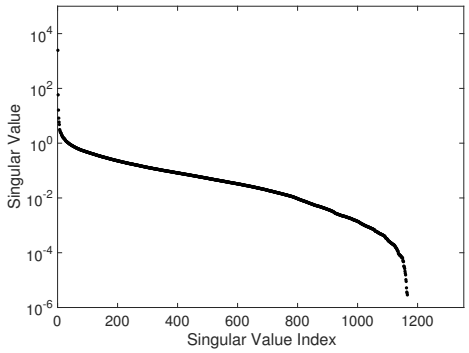
The proposed algorithm quickly identifies and characterizes this cyberattack (100% detection rate and no false positives) in order to avoid the insecure dispatch resulting from the attacked parameter values. Applying Algorithm 1 using one year of historical operational data with $\epsilon = 0.05$ per unit detects the attack ($||r(t)||_\infty = 0.68$ per unit) and correctly characterizes the three attacked lines: the terminal buses of the three attacked lines had maximum residual values $|r(t)|$, $t = 1, \ldots, t$, greater than 0.64 per unit, while all other buses had maximum residual values less than 2×10^{-5} per unit. The computation time was less than 0.05 seconds. Fig. 4 shows how Algorithm 1 characterizes the attack.



(a) RTS-96 System



(b) 2869-Bus PEGASE System



(c) 1354-Bus PEGASE System

Fig. 3. Singular values from the matrix of voltage phasors, $\mathbf{V}$, for one year of hourly data. For the RTS-96 system, the fact that all singular values are non-zero (i.e., the left nullspace is empty) indicates that a cyberattack to the network parameter data would be detected by the proposed algorithm without the need to augment the historical operational data. For the 2869-bus and 1354-bus PEGASE systems, the left nullspaces are non-empty but low-dimensional (8.4% and 2.2%, respectively, of the singular values are smaller than 1×10^{-6}). Thus, the historical data alone highly restricts the ability of an attacker to remain undetected, and only a small number of singular vectors need be added to the historical data as discussed in Section IV-B in order to guarantee the ability to detect all attacks.

C. PEGASE 2869-Bus System: Targeted Cyberattack

The second scenario considers a targeted attack to cause economic losses that primarily affect a specific generator in the 2869-bus PEGASE system. This attack increases the resistance of a single line (see Table II), which results in the generator at

TABLE I
RTS-96 ATTACK DETAILS

Line Index	From Bus	To Bus	Parameter	Actual Value	Attacked Value
10	106	110	Shunt Susceptance	2.4590	1.2295
51	206	210	Shunt Susceptance	2.4590	1.2295
89	306	310	Shunt Susceptance	2.4590	1.2295
42	201	202	Physical attack	Line trip	

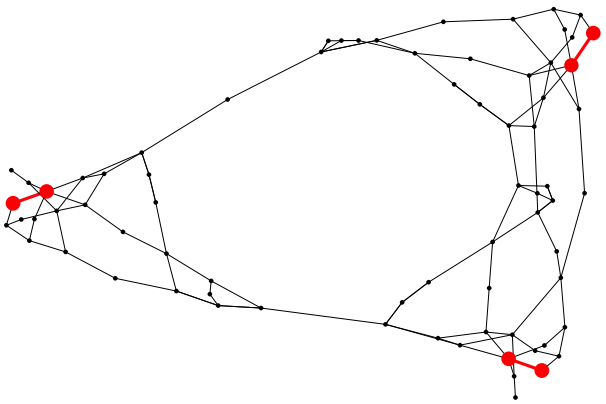


Fig. 4. One-line diagram for the RTS-96 system. Algorithm 1 correctly characterizes the cyberattack as occurring at the red lines via the large residuals $|r(t)|$ at the red terminal buses.

the bus numbered 6329 being less economically competitive. While the overall system costs only undergo a negligible change (less than 0.001%), this specific generator is dispatched significantly less frequently (35% lower total output when aggregated over a year).

Algorithm 1 successfully detects this cyberattack (100% detection rate and no false positives). Using one year of historical data and choosing $\epsilon = 0.05$ per unit, the algorithm detects the cyberattack via a maximum residual of $||r(t)||_\infty = 1.89$ per unit. No buses had residuals larger than 0.0002 per unit except for buses 8789 and 6329, which both had residuals of 1.89 per unit. The line connecting these buses (line index 3800) had its resistance modified in the cyberattack. Thus, Algorithm 1 correctly characterizes this attack. The total computation time for Algorithm 1 to detect and characterize the attack is less than one second.

D. PEGASE 1354-Bus System: Random Cyberattack

The third scenario considers an attack on the 1354-bus PEGASE system that modifies the series reactances of thirty randomly chosen lines. The reactances are modified relative to their actual values by multiplicative factors that are uniformly distributed over the range $[75\%, 125\%]$. The specific modifications are given in Table III.

TABLE II
PEGASE 2869-BUS TARGETED ATTACK DETAILS

Line Index	From Bus	To Bus	Parameter	Actual Value	Attacked Value
3800	8789	6329	Series Resistance	0.0016	0.0161

TABLE III
PEGASE 2869-BUS RANDOM ATTACK DETAILS

Line Index	From Bus	To Bus	Parameter	Actual Value	Attacked Value
33	1264	591	Series Reactance	0.00074	0.00067
88	1060	834	Series Reactance	0.01509	0.01402
169	718	663	Series Reactance	0.00047	0.00053
247	194	1063	Series Reactance	0.02924	0.02652
258	861	493	Series Reactance	0.04190	0.05032
352	70	1152	Series Reactance	0.04708	0.04846
378	145	524	Series Reactance	0.00020	0.00018
661	102	458	Series Reactance	0.03096	0.02654
741	704	1190	Series Reactance	0.00354	0.00364
757	740	1177	Series Reactance	0.01552	0.01526
763	341	1048	Series Reactance	0.00500	0.00383
795	567	328	Series Reactance	0.03401	0.03284
871	218	390	Series Reactance	0.06672	0.08104
877	1246	957	Series Reactance	0.00783	0.00862
1027	1085	822	Series Reactance	0.00064	0.00071
1085	371	524	Series Reactance	0.02677	0.02200
1208	303	873	Series Reactance	0.02591	0.03072
1271	983	1110	Series Reactance	0.00058	0.00051
1368	61	538	Series Reactance	0.00285	0.00283
1461	182	68	Series Reactance	0.01117	0.00981
1462	182	448	Series Reactance	0.00777	0.00855
1515	882	23	Series Reactance	0.01663	0.01316
1627	515	321	Series Reactance	0.00285	0.00236
1635	731	448	Series Reactance	0.00285	0.00341
1649	283	1215	Series Reactance	0.00269	0.00316
1672	387	312	Series Reactance	0.00080	0.00087
1703	15	35	Series Reactance	0.00387	0.00380
1752	1349	356	Series Reactance	0.04910	0.04712
1784	428	944	Series Reactance	0.02437	0.02326
1951	54	351	Series Reactance	0.01247	0.01094

The attacked system has a negligible change in the total operating cost. However, aggregating the magnitudes of the hourly differences between the active power generation resulting from the attacked parameters and the actual parameters yields an average deviation per generator of 6.4%, and one generator had a yearly aggregate deviation of 72.6%. This shows that even an unsophisticated attack can have a non-negligible impact on the dispatch.

Using a year of historical data and selecting $\epsilon = 0.05$ per unit, Algorithm 1 detects the attack via a maximum residual of $||r\,(t)||_\infty = 86.6$ per unit. Fig. 5 illustrates how Algorithm 1 characterizes the attack. In particular, with a single exception, all lines shown in Table III are identified as possible targets of the cyberattack (96.7% detection rate). The exception is line index 1368, which is not detected due to a very small modification in the associated line reactance (a 0.70% reduction) leading to a maximum residual of 0.0032 per unit at the line's terminal buses. This residual is less than the threshold of 0.05 per unit, so this attack is too small to be detected.

Further, in contrast to the other test cases, Algorithm 1 spuriously characterizes other lines as possible targets of the cyberattack. In particular, Algorithm 1 also identifies twenty other lines (line indices 89, 742, 756, 876, 1514, 1753, 1785, 431, 432, 754, 1458, 1459, 1632, 1633, 1634, 1770, 1771, 1772, 1924, and 1925). These false positive characterizations are explained by the fact that these lines share terminal buses with other lines which are attacked. (Note that the first seven

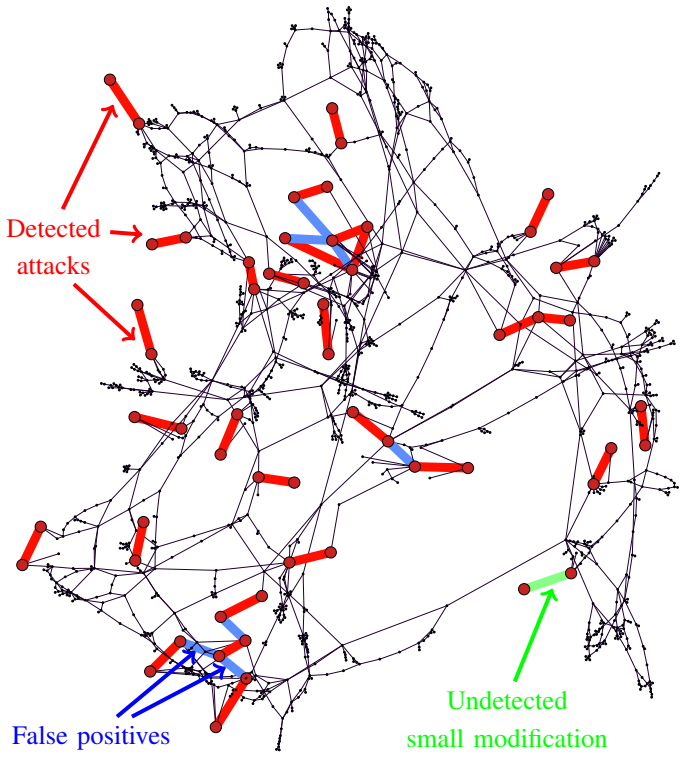


Fig. 5. One-line diagram for the 1354-bus PEGASE system. Algorithm 1 correctly characterizes the cyberattack as occurring at the red lines via the large residuals $|r(t)|$ at the red terminal buses. The lines shown in blue denote "false positive" characterizations of possible attacked lines. Both terminal buses for these "false positive" lines are shared with attacked lines. The line in green is attacked with a small modification (0.70% reduction) to the line reactance. The attack to this line is not detected by Algorithm 1 because the small modification results in residuals at the terminal buses that are below the specified threshold.

of these lines are in parallel with an attacked line.) Regardless of these spurious characterizations, Algorithm 1 identifies a superset of the attacked lines with a limited number of false positives (20 false positives versus 30 attacked lines). The total computation time for Algorithm 1 to detect and characterize the attack is less than 0.5 seconds.

VI. Conclusions and Future Work

This paper has proposed an algorithm for detecting and characterizing cyberattacks to network parameter data. In this class of cyberattacks, the optimization and control algorithms at a control center are applied to maliciously modified network data, potentially harming power system reliability and economic efficiency. The proposed algorithm uses inconsistencies between historical operational data and the specified network parameters to detect and characterize the cyberattack. These inconsistencies are measured via the residual of the relationship between the voltage and current phasors implied by the network parameters.

This paper demonstrates the capabilities of the proposed algorithm using attack scenarios that were developed via ad hoc methods. As discussed in Section III, a direction for future work is the study of more systematic approaches for constructing potential attacks. Another direction for future work is further analysis of the variation inherent to the historical voltage phasors. As discussed in Section IV, the detection and characterization capabilities of Algorithm 1 are improved via access to a richer range of variation in the historical operational data. More accurately simulating typical operational practices (e.g., considering unit commitment problems, including security constraints, etc.) would better demonstrate the capabilities of the proposed approach. Evaluation using actual operational data for a real system would be even more valuable.

References

[1] G. Burke and J. Fahey, "US Power Grid Vulnerable to Foeign Hacks," *Associated Press Investigation*, Dec. 21, 2015. [Online]. Available: http://bigstory.ap.org/article/c8d531ec05e0403a90e9d3ec0b8f83c2/ap-investigation-us-power-grid-vulnerable-foreign-hacks

[2] T. Koppel, *Lights Out: A Cyberattack, A Nation Unprepared, Surviving the Aftermath*. Crown, 2015.

[3] The Smart Grid Interoperability Panel Cyber Security Working Group, "Introduction to NISTIR 7628 Guidelines for Smart Grid Cyber Security," Sept. 2010.

[4] Energy Sector Control Systems Working Group, "Roadmap to Achieve Energy Delivery Systems Cybersecurity," Sept. 2011.

[5] D. Dolezilek and L. Hussey, "Requirements or Recommendations? Sorting out NERC CIP, NIST, and DOE Cybersecurity," *64th Ann. Conf. Protective Relay Eng.*, pp. 328–333, Apr. 2011.

[6] Y. Liu, P. Ning, and M. Reiter, "False Data Injection Attacks Against State Estimation in Electric Power Grids," *ACM Trans. Infor. Syst. Secur. (TISSEC)*, vol. 14, no. 1, p. 13, 2011.

[7] R. Bobba, K. Rogers, Q. Wang, H. Khurana, K. Nahrstedt, and T. Overbye, "Detecting False Data Injection Attacks on DC State Estimation," *Proc. First Workshop Secure Contr. Syst. (SCS)*, 2010.

[8] G. Dán and H. Sandberg, "Stealth Attacks and Protection Schemes for State Estimators in Power Systems," *IEEE Int. Conf. Smart Grid Comm. (SmartGridComm)*, pp. 214–219, Oct. 2010.

[9] O. Kosut, L. Jia, R. Thomas, and L. Tong, "Malicious Data Attacks on the Smart Grid," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 645–658, 2011.

[10] T. Kim and H. Poor, "Strategic Protection Against Data Injection Attacks on Power Grids," *IEEE Trans. Smart Grid*, vol. 2, no. 2, pp. 326–333, June 2011.

[11] A. Giani, E. Bitar, M. Garcia, M. McQueen, P. Khargonekar, and K. Poolla, "Smart Grid Data Integrity Attacks: Characterizations and Countermeasures," *IEEE Int. Conf. Smart Grid Comm. (SmartGridComm)*, pp. 232–237, 2011.

[12] G. Hug and J. Giampapa, "Vulnerability Assessment of AC State Estimation with Respect to False Data Injection Cyber-Attacks," *IEEE Trans. Smart Grid*, vol. 3, no. 3, pp. 1362–1370, 2012.

[13] L. Liu, M. Esmalifalak, Q. Ding, V. Emesih, and Z. Han, "Detecting False Data Injection Attacks on Power Grid by Sparse Optimization," *IEEE Trans. Smart Grid*, vol. 5, no. 2, pp. 612–621, 2014.

[14] Q. Yang, J. Yang, W. Yu, D. An, N. Zhang, and W. Zhao, "On False Data-Injection Attacks against Power System State Estimation: Modeling and Countermeasures," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 3, pp. 717–729, Mar. 2014.

[15] S. Gao, L. Xie, A. Solar-Lezama, D. Serpanos, and H. Shrobe, "Automated Vulnerability Analysis of AC State Estimation under Constrained False Data Injection in Electric Power Systems," *IEEE 54th Ann. Conf. Decis. Contr. (CDC)*, pp. 2613–2620, Dec. 2015.

[16] J. Zhao, G. Zhang, M. La Scala, Z. Dong, C. Chen, and J. Wang, "Short-Term State Forecasting-Aided Method for Detection of Smart Grid General False Data Injection Attacks," *IEEE Trans. Smart Grid*, vol. 8, no. 4, pp. 1580–1590, July 2017.

[17] M. Kallitsis, S. Bhattacharya, S. Stoev, and G. Michailidis, "Adaptive Statistical Detection of False Data Injection Attacks in Smart Grids," *IEEE Global Conf. Signal Inf. Process. (GlobalSIP)*, Dec. 2016.

[18] L. Xie, Y. Mo, and B. Sinopoli, "Integrity Data Attacks in Power Market Operations," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 659–666, Dec. 2011.

[19] L. Jia, J. Kim, R. J. Thomas, and L. Tong, "Impact of Data Quality on Real-Time Locational Marginal Price," *IEEE Trans. Power Syst.*, vol. 29, no. 2, pp. 627–636, Mar. 2014.

[20] M. Wang, P. Gao, S. Ghiocel, J. Chow, B. Fardanesh, G. Stefopoulos, and M. P. Razanousky, "Identification of "Unobservable" Cyber Data Attacks on Power Grids," *IEEE Int. Conf. Smart Grid Comm. (SmartGridComm)*, pp. 830–835, Nov. 2014.

[21] S. Mousavian, J. Valenzuela, and J. Wang, "A Probabilistic Risk Mitigation Model for Cyber-Attacks to PMU Networks," *IEEE Trans. Power Syst.*, vol. 30, no. 1, pp. 156–165, 2015.

[22] Y. Hao, M. Wang, and J. Chow, "Likelihood Analysis of Cyber Data Injection Attacks to Power Systems," *IEEE Global Conf. Signal Inf. Process. (GlobalSIP)*, Dec. 2015.

[23] C. Barrento and A. Cárdenas, "Detecting Fraud in Demand Response Programs," *IEEE 54th Ann. Conf. Decis. Contr. (CDC)*, pp. 5209–5214, Dec. 2015.

[24] C. Lassetter, E. Cotilla-Sanchez, and J. Kim, "Load Oscillating Smart Meter Attack," *IEEE Global Conf. Signal Inf. Process. (GlobalSIP)*, Dec. 2016.

[25] S. Sridhar and M. Govindarasu, "Model-Based Attack Detection and Mitigation for Automatic Generation Control," *IEEE Trans. Smart Grid*, vol. 5, no. 2, pp. 580–591, Mar. 2014.

[26] S. Nabavi and A. Chakrabortty, "An Intrusion-Resilient Distributed Optimization Algorithm for Modal Estimation in Power Systems," *IEEE 54th Ann. Conf. Decis. Contr. (CDC)*, pp. 39–44, Dec. 2015.

[27] J. Valenzuela, J. Wang, and N. Bissinger, "Real-Time Intrusion Detection in Power System Operations," *IEEE Trans. Power Syst.*, vol. 28, no. 2, pp. 1052–1062, May 2013.

[28] S. Mousavian, J. Valenzuela, and J. Wang, "Real-Time Data Reassurance in Electrical Power Systems based on Artificial Neural Networks," *Electr. Power Syst. Res.*, vol. 96, pp. 285–295, 2013.

[29] A. Anwar, A. N. Mahmood, and Z. Tari, "Ensuring Data Integrity of OPF Module and Energy Database by Detecting Changes in Power Flow Patterns in Smart Grids," to appear in *IEEE Trans. Ind. Informat.*, 2017.

[30] H. Sedghi and E. Jonckheere, "Statistical Structure Learning to Ensure Data Integrity in Smart Grid," *IEEE Trans. Smart Grid*, vol. 6, no. 4, pp. 1924–1933, July 2015.

[31] R. Moslemi, A. Mesbahi, and J. M. Velni, "A Fast, Decentralized Covariance Selection-based Approach to Detect Cyber Attacks in Smart Grids," to appear in *IEEE Trans. Smart Grid*, 2018.

[32] D. Deka, S. Talukdar, M. Chertkov, and M. Salapaka, "Topology Estimation in Bulk Power Grids: Guarantees on Exact Recovery," *arXiv:1707.01596*, July 2017.

[33] A. Anwar and A. N. Mahmood, "Anomaly Detection in Electric Network Database of Smart Grid: Graph Matching Approach," *Electric Power Syst. Res.*, vol. 133, no. Supplement C, pp. 51 – 62, 2016.

[34] M. Aldeen and F. Crusca, "Observer-Based Fault Detection and Identification Scheme for Power Systems," *IEE Proc. - Generation, Transmission, Distribution*, vol. 153, no. 1, pp. 71–79, Jan. 2006.

[35] D. Dustegor, S. V. Poroseva, M. Y. Hussaini, and S. Woodruff, "Automated Graph-Based Methodology for Fault Detection and Location in Power Systems," *IEEE Trans. Power Del.*, vol. 25, no. 2, pp. 638–646, Apr. 2010.

[36] R. J. Patton, P. M. Frank, and R. N. Clark, *Issues of Fault Diagnosis for Dynamic Systems*. Springer Science & Business Media, 2013.

[37] J. A. Momoh, *Electric Power System Applications of Optimization*. CRC Press, 2008.

[38] K. Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*. Crown, 2014.

[39] "Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies," *National Cybersecurity and Communications Integration Center (NCCIC) and Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)*, Sept. 2016.

[40] IEEE PES CAMS Task Force on Cascading Failure, "Initial Review of Methods for Cascading Failure Analysis in Electric Power Transmission Systems," in *IEEE PES General Meeting*, July 2008, pp. 1–8.

[41] R. Zimmerman, C. Murillo-Sánchez, and R. Thomas, "MATPOWER: Steady-State Operations, Planning, and Analysis Tools for Power Systems Research and Education," *IEEE Trans. Power Syst.*, no. 99, pp. 1–8, 2011.

[42] V. Cecchi, A. S. Leger, K. Miu, and C. O. Nwankpa, "Incorporating Temperature Variations Into Transmission-Line Models," *IEEE Trans. Power Del.*, vol. 26, no. 4, pp. 2189–2196, Oct. 2011.

[43] V. Cecchi, M. Knudson, and K. Miu, "System Impacts of Temperature-Dependent Transmission Line Models," *IEEE Trans. Power Del.*, vol. 28, no. 4, pp. 2300–2308, Oct. 2013.

[44] D. Bienstock, J. Blanchet, and J. Li, "Stochastic Models and Control for Electrical Power Line Temperature," *Energy Syst.*, vol. 7, no. 1, pp. 173–192, Feb. 2016.

[45] D. Kalman, "A Singularly Valuable Decomposition: The SVD of a Matrix," *The College Mathematics Journal*, vol. 27, no. 1, pp. 2–23, 1996.

[46] C. Grigg, P. Wong, P. Albrecht, R. Allan, M. Bhavaraju, R. Billinton, Q. Chen, C. Fong, S. Haddad, S. Kuruganty, W. Li, R. Mukerji, D. Patton, N. Rau, D. Reppen, A. Schneider, M. Shahidehpour, and C. Singh, "The IEEE Reliability Test System-1996. A Report Prepared by the Reliability Test System Task Force of the Application of Probability Methods Subcommittee," *IEEE Trans. Power Syst.*, vol. 14, no. 3, pp. 1010–1020, Aug. 1999.

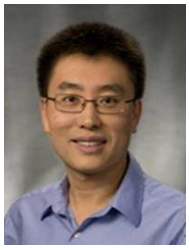
[47] Power Systems Test Case Archive. University of Washington Department of Electrical Engineering. [Online]. Available: http://www.ee.washington.edu/research/pstca/

[48] C. Josz, S. Fliscounakis, J. Maeght, and P. Panciatici, "AC Power Flow Data in MATPOWER and QCQP Format: iTesla, RTE Snapshots, and PEGASE ," *arXiv:1603.01533*, Mar. 2016.

[49] J. Lavaei and S. Low, "Zero Duality Gap in Optimal Power Flow Problem," *IEEE Trans. Power Syst.*, vol. 27, no. 1, pp. 92–107, Feb. 2012.

[50] D. K. Molzahn, J. T. Holzer, B. C. Lesieutre, and C. L. DeMarco, "Implementation of a Large-Scale Optimal Power Flow Solver Based on Semidefinite Programming," *IEEE Trans. Power Syst.*, vol. 28, no. 4, pp. 3987–3998, 2013.

Daniel K. Molzahn (S'09-M'13) is a Computational Engineer at Argonne National Laboratory. He was a Dow Postdoctoral Fellow in Sustainability at the University of Michigan, Ann Arbor and received the B.S., M.S., and Ph.D. degrees in electrical engineering and the Masters of Public Affairs degree from the University of Wisconsin–Madison, where he was a National Science Foundation Graduate Research Fellow. His research focuses on optimization and control of electric power systems.



Jianhui Wang (M'07-SM'12) received the Ph.D. degree in electrical engineering from the Illinois Institute of Technology, Chicago, IL, USA, in 2007. Presently, he is an Associate Professor with the Department of Electrical Engineering at Southern Methodist University in Dallas Texas, USA. Dr. Wang is the secretary of the IEEE Power & Energy Society (PES) Power System Operations, Planning, & Economics Committee. He is an associate editor of Journal of Energy Engineering and an editorial board member of Applied Energy. He has held visiting positions in Europe, Australia, and Hong Kong, including a VELUX Visiting Professorship at the Technical University of Denmark (DTU). Dr. Wang is the Editor-in-Chief of the IEEE Transactions on Smart Grid and an IEEE PES Distinguished Lecturer. He is also the recipient of the IEEE PES Power System Operation Committee Prize Paper Award in 2015.