Real-Time Intrusion Detection in Power System Operations

Jorge Valenzuela, Jianhui Wang, *Member, IEEE*, and Nancy Bissinger, *Student Member, IEEE*

***Abstract*—Increasing power system security is crucial to the future of the electric power grid. In this paper, we define a new class of cyberattacks to power systems-malicious modification of network data stored in an accessible database. Grounded in multivariate statistical process control, our approach to intrusion detection ensures data integrity in power system operations. We develop an algorithm that monitors power flow results and detects anomalies in the input values that could have been modified by cyberattacks. Our algorithm uses principal component analysis to separate power flow variability into regular and irregular subspaces. Analysis of the information in the irregular subspace determines whether the power system data has been compromised. We verify the efficacy of the algorithm using both the IEEE 24-bus and 118-bus reliability test systems. The results show that the developed algorithm is a promising enhancement to data security procedures in a control center.**

***Index Terms*—Cybersecurity, intrusion detection, power system security, principal component analysis.**

NOMENCLATURE

J	Number of branches.
T	Number of time intervals.
$\mathbf{F}$ $T \times J$	Matrix of real power flows.
$\mathbf{Z}$ $T \times J$	Matrix of standardized real power flows.
$\mathbf{Y}$ $T \times J$	Matrix of principal component scores.
$\mathbf{f}_j$	Vector of real power flows through each branch, j.
$\bar{\mathbf{f}}_j$	Vector of sample mean of real power flows through each branch, j.
$\mathbf{f}^{\max}$	Vector of maximum flow through each branch.
$\mathbf{s}_j$	Vector of sample standard deviation of real power flows through each branch, j.
$\mathbf{z}_j$	Vector of standardized real power flows through each branch, j.
P	Number of principal components in the regular subspace.
K	Number of principal components in the irregular subspace.
$\mathbf{A}$ $J \times J$	Matrix of principal component coefficients.
$\mathbf{a}_j$	Column vectors of $\mathbf{A}$.
$\mathbf{A_i}$ $K \times J$	Irregular subspace of $\mathbf{A}$.
$\mathbf{A_r}$ $P \times J$	Regular subspace of $\mathbf{A}$.
$\mathbf{y}_i$	Vector of principal component scores at time, t.
$\mathbf{b}$	Vector of sum of squared terms at time, t.
τ	Detection threshold.
β	Line characteristic change factor.
N^b	Number of buses.
N^g	Number of generators.
$\boldsymbol{\theta}$ $N^b \times 1$	Vector of voltage angles.
$\mathbf{v}$ $N^b \times 1$	Vector of voltage magnitudes.
$\mathbf{p}^g$ $N^g \times 1$	Vector of generator real power injections.
$\mathbf{q}^g$ $N^g \times 1$	Vector of generator reactive power injections.
$\mathbf{p}^d$ $N^b \times 1$	Vector of real load.
$\mathbf{q}^d$ $N^b \times 1$	Vector of reactive load.
$\mathbf{C}$ $N^b \times N^g$	Generator connection matrix whose (i,j)th element is 1 if generator j is located at bus i and 0 otherwise.
$\mathbf{p}^{\text{bus}}(\boldsymbol{\theta}, \mathbf{v})$ $N^b \times 1$	Vector of nodal real power injected at buses.
$\mathbf{q}^{\text{bus}}(\boldsymbol{\theta}, \mathbf{v}))N^b \times 1$	Vector of nodal reactive power injected at buses.

Manuscript received December 27, 2011; revised May 29, 2012, August 20, 2012, and October 05, 2012; accepted October 06, 2012. Date of publication November 27, 2012; date of current version April 18, 2013. This work was supported by UChicago Argonne, LLC, Operator of Argonne National Laboratory (Argonne). Argonne, a U.S. Department of Energy Office of Science laboratory, is operated under Contract No. DE-AC02-06CH11357. Paper no. TPWRS-01246-2011.

J. Valenzuela and N. Bissinger are with the Department of Industrial and Systems Engineering, Auburn University, Auburn, AL 36849 USA (e-mail: valenjo@auburn.edu; npb0004@auburn.edu).

J. Wang is with Argonne National Laboratory, Argonne, IL 60439 USA (e-mail: jianhui.wang@anl.gov).

Digital Object Identifier 10.1109/TPWRS.2012.2224144

I. INTRODUCTION

AS POWER systems transition to the smart grid, upgrading hardware, software and infrastructure increases the threat of cyberattack on critical resources. The Government

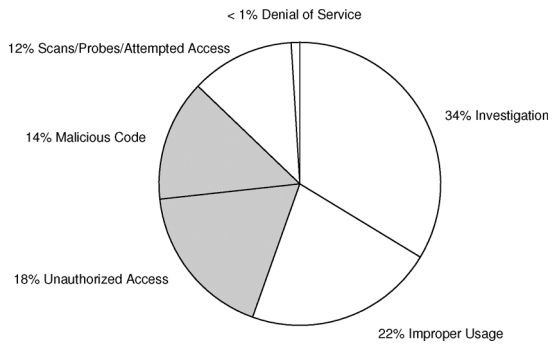


Fig. 1. Percentage of incidents reported to US-CERT in 2006–2008 by category [1].

Accountability Office (GAO) reported in 2009 that cyberthreats to critical infrastructure like the power grid are increasing and evolving. The sources of these threats—hackers, foreign nations, disgruntled employees and terrorists—coupled with the sophistication of technology and widespread documentation of intrusion techniques on the Internet have led the government to become increasingly concerned about the potential for cyberattack. Fig. 1, from the United States Computer Emergency Readiness Team (US CERT), illustrates that threats categorized as unauthorized access and malicious code made up 32% of cyberthreats to federal information systems and cyberbased critical infrastructures in the three year timespan beginning in 2006 [1]. Unauthorized access is considered logical (or physical) access to data without permission. And, malicious code is the successful installation of a virus, worm or other code-based entity that infects a system and is not quarantined by anti-virus software. The successful enactment of either of these threats could disrupt operation of the power grid.

While the threat is real, cyberattacks have not disrupted power delivery in the United States [2]. However, advanced intruders can circumvent computer and network security. The Stuxnet worm is one recent example of malicious code that gained access to and damaged critical control systems in Iran's nuclear program [3].

Our research defines a new class of cyberattacks to power systems—malicious modification of network data stored in an accessible database. We posit that data anomalies could be the result of unauthorized access to and modification of data by an intruder or by malicious code that is not quarantined by preventive software. Since modern control centers use state-of-the-art security to prevent cyberintrusion based on recommendations, regulations and requirements from agencies like NERC, NIST and DOE [4], operators expect the data stored in protected databases to be secure. A cybercriminal could manage to get around security measures and modify data in a database without the system operator's knowledge.

The trustworthiness of the data passed among supervisory control and data acquisition (SCADA), Energy Management System (EMS) and Business Management System (BMS) [5] program modules is extremely important for the proper operation of the power grid. In addition, integrated topology processing, such as in the PowerWorld software [6] provides for information exchanges across operations and planning modules. Output data from an operations module is often used as input data to a planning module and vice versa. At any point in the process of data collection and decision making, data errors could lead to unnecessary and costly outages if not recognized in a timely manner. The data could be compromised not only through equipment or human errors but also by the intervention of an intruder who tampers with the data stored in a database or interferes with the module that processes real time network topology.

The optimal power flow (OPF) program solves a set of nonlinear equations using stored data to compute a steady state operation point with the objective function varying according to the target of the optimization. OPF is widely used in power system control and since it runs often, sometimes every 30 seconds [7], an undetected cyberattack on data supplied to the OPF program could cause power to be dispatched erroneously. Network configuration, generator capacity and system loads are some of the data input to the OPF program that could be maliciously modified by an adversary through unauthorized access or the introduction of malicious code.

In this paper we develop an algorithm that uses principal component analysis (PCA) to determine whether input data passed to the OPF software module has been contaminated by cyberterrorists. The algorithm computes an orthogonal linear transformation of output data and splits the resulting space into two subspaces—regular and irregular, separating the output data's variability into normal and anomalous variability. Normal variability is described as naturally occurring and inherent to the process while anomalous variability is unnatural and due to a shock or disruption to the process. An anomaly is detected if the summed square of the data mapped onto the irregular subspace exceeds a statistical threshold. PCA has been used in the detection of anomalies in security considerations in communication networks [8], [9], but to our knowledge, not for detecting data anomalies in the power industry.

The PCA-based algorithm presented in this paper is customized to determine if input data related to transmission lines has been compromised. In doing so, the algorithm monitors the real power flow output from OPF. The orthogonal linear transformation model is obtained from historical OPF outputs (real power flows), which are computed under normal operating conditions. While our algorithm analyzes real power flows and detects anomalies in transmission line parameters, it is possible to monitor a different OPF output and detect cyberintrusion in different input data. In this case, a different customization of the algorithm is necessary.

The remainder of this paper is organized as follows: Section III documents recent research in intrusion detection in power system operations; Section IV describes the power system model; Section V explains the anomaly detection model and assumptions; Section VI provides numerical results for two test power systems; and Section VII reports our conclusions.

II. Related Work

Recent research in power system security has focused entirely on cyberintrusion related to intelligent electronic devices (IEDs) like remote terminal units (RTUs), phasor measurement units (PMUs) and meters. These attacks are referred to as malicious data injection attacks. Our research defines a new class of cyberattacks to power systems—malicious modification of network

data stored in an accessible database—which is different from the research on malicious data injection attacks.

An important module in the modern power control system, the state estimation program uses the measurements from IEDs to estimate state variables like voltage angles and magnitudes at each bus in a power system. Statistical techniques successfully identify and remove obvious bad data from state estimation procedures. And, since state estimation cleans the data, this process also prevents the bad data from being stored in databases for future use.

Bad data detection methods were included in the first state estimation programs in the late 1960s and were designed to detect large errors that were the result of equipment malfunction [10]. The methods have been enhanced over the years [11], [12], but remain much the same as when first implemented in the latter half of the twentieth century.

Recently, more consideration has been placed on detecting data errors intentionally injected into the power system through telemetered data. These errors will likely not be detectable through state estimation by commonly used methods like least normalized residuals (LNR). The false data are designed to be undetectable. An intruder could craftily design an attack to inject bad data in a way that would optimize damage to the power system while minimizing detection.

Liu *et al.*, in [13], described a new class of cyberattacks called false data injection attacks. Results of their research indicate that it is possible by compromising meter measurements to construct an attack vector that changes the results of state estimation and is undetectable by commonly used methods of bad data detection like LNR. Sensor measurement protection through the use of network observability rules as a solution to detecting false data injection attacks was the focus of research in [14]. To measure the vulnerability of a network, the research in [15] defined a security index as the minimum number of meters necessary to perform an unobservable attack. An algorithm for such an index that helps to locate power flows whose measurements are potentially easy to manipulate can be found in [16] where the authors urge the incremental deployment of protected measurements to increase grid security. In an expansion on the research by Liu *et al.*, Kosut *et al.* proposed a detector based on the generalized likelihood ratio test (GLRT) to detect attacks where the adversary does not have access to a sufficient number of meters to launch an unobservable attack. They posit that the key to defending against such malicious data attacks is the introduction of redundant and trustworthy measurements that ensure network observability [17]. The financial effects of the aforementioned false data injection attacks on electric power market operations is studied in [18]. The most recent research on smart grid data integrity attacks with the goal of biasing state estimation results, focuses on strategic methods of identifying, foiling and counteracting attacks on IEDs. In [19] unobservable, coordinated attacks are described and strategic placement of secure PMUs are shown to be an effective defense. The research by Kim *et al.* develops an algorithm to optimize the choice of PMUs to secure and a separate algorithm to optimize their placement [20].

Implementation of the results from the recent research is necessary to protect the power grid; however, it is not sufficient. Network data stored in databases is also vulnerable to cyberattack. These cyberattacks are different from previously researched data integrity attacks in the sense that these physical transmission line data do not depend on the measurements from IEDs. If a cyberattack which changed network parameters stored in a database were to significantly alter the system state estimate, then the alarm raised to the operator during bad data detection would likely discover the parameter change. However, situations could arise where the state estimation bad data detection schemes would not detect malicious modification of network data in an accessible database. For example inadequate measurement redundancy could cause the parameter to be undetectable [21] or the network database could be modified by cyberattackers after the most recent state estimation program has run and before an instance of the OPF module has run. Our proposed method, implemented in the network topology processing portion of the OPF module, provides an additional security measure to protect the power grid.

III. OPF Model

The modern control center uses multiple instances of the OPF module, often in real-time, to operate the power system as economically as possible while ensuring its reliability despite changes in load requirements and available resources. The OPF module provides an optimal solution of flows, voltages, and power injections either to the operator or as input to automated generation control (AGC) programs and is commonly executed every 3 minutes with an updated set of values for input parameters [7]. Some of the input values, such as line characteristics and network configuration, typically do not change over a short period of time while others, such as load and the set of available generators, vary more often. Therefore, the solution vector of the OPF module changes over time based on the natural variability in the module's input data.

We use MatPower's default primal-dual interior point solver (MIPS) to compute AC power flows. In the standard AC OPF model from the MatPower manual that follows [22] N^b is the number of buses and N^g is the number of generators in the network.

A. General Model

$$\min_{\mathbf{x}} f(\mathbf{x})$$

subject to

$$\mathbf{G}(\mathbf{x}) = 0 \tag{1}$$

$$\mathbf{H}(\mathbf{x}) \leq 0 \tag{2}$$

$$\mathbf{x}^{\min} \leq \mathbf{x} \leq \mathbf{x}^{\max} \tag{3}$$

where the equality constraints are the power balance equations and the inequality constraints are the branch flow limits.

B. Decision Variables

$$\mathbf{x} = \begin{bmatrix} \boldsymbol{\theta} \\ \mathbf{v} \\ \mathbf{p}^g \\ \mathbf{q}^g \end{bmatrix}. \tag{4}$$

$\boldsymbol{\theta}$ and $\mathbf{v}$ are $N^b \times 1$ vectors of voltage angles and magnitudes, respectively. $\mathbf{p}^g$ and $\mathbf{q}^g$ are $N^g \times 1$ vectors of generator real and reactive power injections.

C. Objective Function

$$\min_{\boldsymbol{\theta},\mathbf{v},\mathbf{p}^g,\mathbf{q}^g} \sum_{i=1}^{N^g} P_i\left(p_i^g\right) + Q_i\left(q_i^g\right). \tag{5}$$

The objective function sums the polynomial cost functions, P_i and Q_i of real and reactive power injections, respectively, for each generator. We particularly focus on the OPF instance whose objective is to find a steady state operation point which minimizes generation cost while enforcing system performance through limits on real and reactive power generator outputs, bus voltage angles and magnitudes, and transmission line flows.

D. Constraints

1) Power Balance Equations:

$$\mathbf{G}^p(\boldsymbol{\theta},\mathbf{v},\mathbf{p}^g) = \mathbf{p}^{\text{bus}}(\boldsymbol{\theta},\mathbf{v}) + \mathbf{p}^d - \mathbf{C}\mathbf{p}^g = \mathbf{0} \tag{6}$$

$$\mathbf{G}^q(\boldsymbol{\theta},\mathbf{v},\mathbf{q}^g) = \mathbf{q}^{\text{bus}}(\boldsymbol{\theta},\mathbf{v}) + \mathbf{q}^d - \mathbf{C}\mathbf{q}^g = \mathbf{0} \tag{7}$$

so that

$$\mathbf{G}(\boldsymbol{\theta},\mathbf{v},\mathbf{p}^g,\mathbf{q}^g) \text{ from Equation (1)} = \begin{bmatrix} \mathbf{G}^p(\boldsymbol{\theta},\mathbf{v},\mathbf{p}^g) \\ \mathbf{G}^q(\boldsymbol{\theta},\mathbf{v},\mathbf{q}^g) \end{bmatrix}. \tag{8}$$

2) Branch Flow Limits:

$$\mathbf{H}^f(\boldsymbol{\theta},\mathbf{v}) - \mathbf{f}^{\max} \le \mathbf{0} \tag{9}$$

$$-\mathbf{H}^f(\boldsymbol{\theta},\mathbf{v}) - \mathbf{f}^{\max} \le \mathbf{0} \tag{10}$$

so that

$$\mathbf{H}(\boldsymbol{\theta},\mathbf{v}) \text{ from Equation (2)} = \begin{bmatrix} \mathbf{H}^f(\boldsymbol{\theta},\mathbf{v}) - \mathbf{f}^{\max} \\ -\mathbf{H}^f(\boldsymbol{\theta},\mathbf{v}) - \mathbf{f}^{\max} \end{bmatrix}. \tag{11}$$

3) Variable Limits:

$$-\theta_i^{\text{ref}} \le \theta_i \le \theta_i^{\text{ref}}, \quad i \in \mathcal{I}_{\text{ref}} \tag{12}$$

$$v_i^{\min} \le v_i \le v_i^{\max}, \quad i = 1 \ldots N^b \tag{13}$$

$$p_i^{g,\min} \le p_i^g \le p_i{}^{g,\max}, \quad i = 1 \ldots N^g \tag{14}$$

$$q_i^{g,\min} \le q_i^g \le q_i{}^{g,\max}, \quad i = 1 \ldots N^g. \tag{15}$$

In this paper we assume that a cyberterrorist has compromised the integrity of network data stored in an accessible database and, unknown to the operator, input to the OPF module affecting the real power flows is erroneous. The real power flow through branch i (connecting buses $\text{from}(i)$ and $\text{to}(i)$) can be calculated according to the following equation [21]:

$$f_i = v_{\text{from}(i)}^2\left(g_{\text{from}(i)}^s + g_i\right) - v_{\text{from}(i)}v_{\text{to}(i)}(g_i\cos\theta_i + b_i\sin\theta_i) \tag{16}$$

where

$$\theta_i = \theta_{\text{from}(i)} - \theta_{\text{to}(i)}, g_{\text{from}(i)}^s + jb_{\text{from}(i)}^s$$

is the admittance of the shunt branch connected at bus $\text{from}(i)$, $g_i + jb_i$ is the admittance of the series branch.

Optimal power flow problems have been studied and improved upon since first discussed by Carpentier in 1962 [23]. For a better understanding of OPF formulations the reader is directed to [24]–[26] and for this specific implementation, the MatPower Manual [22].

IV. Anomaly Detection

We generate historical flow data by coding a Monte Carlo simulation of the power system since actual line flows are difficult to obtain. In the simulation, we use MatPower to compute the optimal real power flow through each branch, j, $\mathbf{f}_j = (f_j(1), \ldots, f_j(T))$, $j \in [1, J]$ for T intervals under normal operating conditions as defined in (16).

We use PCA to transform the power flow data to a new set of axes called principal components. In the transformation, the resulting principal components are ordered so that the first one accounts for as much of the variability in the original data as possible. Each subsequent principal component accounts for as much of the remaining variability as possible. The Jth principal component accounts for the least amount of variability.

Using this property of principal components, we separate the results into two subspaces—regular and irregular. We map the output to be analyzed onto the irregular subspace to discover the time at which a cyberattack led to abnormal power flows.

In the remainder of this section we define the principal components and explain the process of separating the anomalous flows from the normal flows through the use of subspaces.

A. Principal Component Analysis

PCA is a powerful multivariate analysis technique used extensively in the social sciences to reduce the dimensionality of data and more recently in such fields as facial recognition and image compression. It was first documented by Pearson in 1901 [27] and developed independently by Hotelling in 1933 [28]. While its use as a dimension reduction tool is well documented, PCA is also one of the best-known statistical methods for identifying anomalies in communication network traffic [29]. This type of anomaly identification application is also known as outlier detection. PCA transforms a (typically) large set of correlated variables into a set of uncorrelated variables on a new coordinate system. These uncorrelated variables, called principal components, are then ordered so that the first few principal components contain most of the variability in all of the original set of variables while maintaining as much information as possible from the original data.

1) Definition of Principal Components: Principal components are the orthogonal axes formed when PCA is applied to a set of data. Each of the principal components points in the direction of maximum variance remaining in the data, given the variance already accounted for by the previous principal components.

We start by standardizing the real power flow vectors $\mathbf{f}_j$:

$$\mathbf{z}_j = (\mathbf{f}_j - \bar{\mathbf{f}}_j)/\mathbf{s}_j \tag{17}$$

where $\bar{\mathbf{f}}_j$ is the sample mean of the real power flow through transmission line j and $\mathbf{s}_j$ is the sample standard deviation of the same flow. We apply PCA to the standardized power flow matrix, $\mathbf{Z}$, which is made up of J column vectors, $\mathbf{z}$, of T real power flow measurements. We are interested in the variances and structure of covariances among the J flows in the time series.

PCA is an iterative process that in step 1 looks for a linear function of the elements of $\mathbf{Z}$

$$\mathbf{a}_1^T\mathbf{z} = a_{11}\mathbf{z}_1 + a_{12}\mathbf{z}_2 + \cdots + a_{1J}\mathbf{z}_J = \sum_{i=1}^{J} a_{1i}\mathbf{z}_i \qquad (18)$$

where $\mathbf{a}_1^T\mathbf{z}$ accounts for the maximum variance among the J flows and is called the first principal component. In the next iteration, $\mathbf{a}_2^T\mathbf{z} = \sum_{i=1}^{J} a_{2i}\mathbf{z}_i$ is orthogonal to $\mathbf{a}_1^T\mathbf{z}$, accounts for the next highest variance and is called the second principal component, etc. until the Jth linear function, $\mathbf{a}_J^T\mathbf{z} = \sum_{i=1}^{J} a_{Ji}\mathbf{z}_i$, which is orthogonal to $\mathbf{a}_1^T\mathbf{z}, \mathbf{a}_2^T\mathbf{z}, \ldots, \mathbf{a}_{J-1}^T\mathbf{z}$ and accounts for the least amount of variance. The J principal components are uncorrelated and mutually orthogonal.

$\mathbf{A}$ is the $J \times J$ orthogonal basis set of principal component coefficients. Each column of $\mathbf{A}$ is an eigenvector of the sample covariance matrix, $\mathbf{Z}^T\mathbf{Z}$, corresponding to its jth largest eigenvalue λ_j and contains the coefficients for one principal component. Since $\mathbf{a}_j\mathbf{a}_j^T = 1$ for each column of $\mathbf{A}$, λ_j is the variance of the jth column of $\mathbf{Z}^T\mathbf{Z}$.

The coefficients, a_{ji}, are referred to as loadings since they are the weights by which the original data elements are multiplied when calculating the principal components. Each $a_{ji}\mathbf{z}_i$ in (18) is a score and a principal component is the sum of all of the scores for one column of loadings.

2) Derivation of Principal Components: Derivation of the principal components can be accomplished in different ways. We include here the derivation using singular value decomposition (SVD) since it gives an efficient practical method of computation.

Given a $T \times J$ matrix $\mathbf{Z}$ of T observations on J real power flows measured about their means and using a key result of matrix algebra, SVD, $\mathbf{Z}$ can be written as

$$\mathbf{Z} = \mathbf{ULA}^{\mathbf{T}} \qquad (19)$$

where

1) $\mathbf{U}$ is a $T \times R$ matrix with orthonormal columns so that $\mathbf{U}^{\mathrm{T}}\mathbf{U} = \mathbf{I}_{\mathrm{R}}$;
2) $\mathbf{A}$ is a $J \times R$ matrix with orthonormal columns so that $\mathbf{A}^{\mathrm{T}}\mathbf{A} = \mathbf{I}_{\mathrm{R}}$;
3) $\mathbf{L}$ is an $R \times R$ diagonal matrix;
4) R is the rank of $\mathbf{Z}$.

The result of SVD follows:

1) $\mathbf{A}$ contains the eigenvectors, $\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_k$, of $\mathbf{Z}^{\mathrm{T}}\mathbf{Z}$;
2) $\mathbf{L}$ contains the square roots of the eigenvalues of the population covariance matrix;
3) The principal component scores can be calculated by $\mathbf{Y} = \mathbf{UL}$ or $\mathbf{Y} = \mathbf{ZA}$.

A complete discussion of PCA and the derivation of the principal components can be found in [30].

B. Tunable Parameters

In many applications of PCA, the first few components are used for analysis since the majority of variability in the entire original dataset is often concentrated in these first few (principal) components. Our solution uses the set of components containing the least amount of variability which we refer to as the minor components and two tunable parameters are key to successful analysis: K is the number of minor components used to determine the size of the irregular subspace and τ is the detection threshold used to detect anomalies. Since the value of these parameters is network sensitive, the trial and error approach we use for determination is only necessary once for a particular network configuration and can be accomplished offline. The operator may choose to adjust the threshold, τ, if the number of false alarms changes significantly over time.

1) Choosing K: Recent research on the use of subspaces in the analysis of traffic anomalies in communication network data documented three methods of choosing the size of the regular subspace: sighting the knee of a scree plot of cumulative variance accounted for by principal components, specifying a percentage of the same cumulative variance, and using 3σ from the mean [9]. These methods are often used when reducing dimensionality, but the authors in [29] concluded that none of them was a failsafe method for anomaly detection. In [30], Jolliffe discussed some of the same methods and also stressed the value of the minor components in certain types of outlier detection. Outliers which are not obvious from analysis of the original variables individually may be detected using the minor components. Because of the relationships among the power flows in transmission lines, we focus on the minor components and experimentally choose the value of K that in combination with τ results in the most detected anomalies with the least number of false alarms.

2) Choosing τ: The second tunable parameter τ, the detection threshold, is used to detect anomalies. Through experimentation we increase and decrease τ for various values of K until the percentage of true anomalies detected is high and the number of false anomalies detected is low.

C. Subspace Construction

After carefully choosing K, we separate the $\mathbf{A}$ matrix into two sub-spaces, regular and irregular. The K coefficient vectors associated with the *minor* components (which capture the least variability) form $\mathbf{A}_i$, the irregular subspace. The $P = J - K$ coefficient vectors associated with the *principal* components (which capture the most variability) form $\mathbf{A}_r$, the regular subspace. Since we use historical data under normal operating conditions as input to PCA the majority of the variability in the output from PCA can be attributed to naturally occurring phenomena like time of day and weather. Consequently, we define variability associated with the $\mathbf{A}_r$ subspace as normal variability and variability associated with the $\mathbf{A}_i$ subspace as anomalous variability. Note that the use of PCA subspaces for detecting anomalies is well-documented and we refer the reader to Jolliffe's text [30] for the related mathematical proofs.

D. Detection Model

To analyze the power flows in the new coordinate space, we create the scores vectors, $\mathbf{y}_i(t)$, by multiplying the original standardized data by the loadings in the irregular subspace

$$\mathbf{y}_i(t) = \mathbf{z}(t) \times \mathbf{A}_i. \tag{20}$$

In this process we ignore the normal variability and analyze $\mathbf{y_i}$ to discover any anomalous variability which may be related to maliciously modified input data.

To detect anomalies, we compute the sum of the squared terms of the scores of the minor components:

$$\mathbf{b}(t) = \mathbf{y}_i(t) \times \mathbf{y}_i(t)^T. \tag{21}$$

Because $\mathbf{b}(t)$ should be small given most of the variability has been removed from this subspace, we conclude that no evidence of anomalous variability exists if $\mathbf{b}(t) \leq \tau$, and therefore the power system is considered to be in control. If an anomaly is found, we regenerate the historical flows over the interval from $t_{\text{current}} - 168\,(\text{one week}) + 1$ to t_{current} and repeat the analysis.

This periodic regeneration of the historical flows re-calibrates the model to a relatively current time period. In a real-time implementation the algorithm would run in conjunction with an OPF module and use the latest power flow data as historical data on which to base the PCA. The regeneration of the historical data in our case studies emulates the real-time implementation by using the 168 hours of historical data immediately prior to the last anomaly encountered.

E. Pseudo-Code

Below we describe the developed model using pseudo code.

1) Generating historical power flows:

$T_0 = 0$

for $t = T_0 + 1$ to $T_0 + 168$ **do**

Sample generator status (on-off) from a continuous-time Markov chain [31]

Solve the OPF using the real and reactive loads at time t

Compute the tth row of the real power flow matrix $\mathbf{F}$

end for

Output $\mathbf{F}$ as the matrix of historical real power flows

2) Computing matrix $\mathbf{A}_i$:

Compute the mean of each column of $\mathbf{F}$

Compute the standard deviation of each column of $\mathbf{F}$

Compute the standardized line flow matrix $\mathbf{Z}$

Create $\mathbf{A}$

Form the irregular subspace matrix $\mathbf{A}_i$ where the columns are the eigenvectors $\mathbf{a}_j, (j = P + 1, \ldots, J)$

Map $\mathbf{Z}$ onto the irregular subspace, $\mathbf{A}_i$

Output $\mathbf{y}_i$

3) Detecting anomalies:

for $t = T_0 + 168 + 1$ to T **do**

Sample generator status (on-off) from a continuous-time Markov chain

Solve the OPF using the load at time t

Standardize the tth power flow observation

Map the tth power flow observation onto the irregular subspace

Compute $\mathbf{b}(t) = \mathbf{y}_i(t) \times \mathbf{y}_i(t)^T$

if $\mathbf{b}(t) > \tau$ **then**

An anomaly exists. Check the input data

if Anomaly is a false alarm **then**

Update historical real power flow matrix $\mathbf{F}$

Go to Step 2) to recompute matrix $\mathbf{A}_i$

else

Stop the process and alert the operator

end if

else

System is in control

end if

end for

V. Case Studies

To test the effectiveness of our detection algorithm, we introduce anomalies into a transmission system at a point in time and analyze the results. For our case studies, we use data from the IEEE Reliability Test System [31]. We run our simulation on both the 24-bus system and the 118-bus system. The 24-bus system consists of 38 transmission lines, 24 buses of which 17 have loads, and 33 generators. The 118-bus system has 186 transmission lines, 118 buses of which 99 have loads, and 54 generators. Because of the large amount of data related to these systems, we refer the reader to [22] and [31] for additional details.

As documented earlier in this paper, no known cyberattacks have been carried out on the U.S. transmission network so it is difficult to identify a *typical* attack. We choose line characteristics to change in the cases described below because this data is accessible, affects the calculation of optimal power flows and changes to line characteristics may not be detected by a system operator. In three of the five cases, the attacks are defined randomly. In lieu of a typical attack, this use of randomness in selecting the parameters to change, the amount of change, and the lines to change provides a range of scenarios and tests the effectiveness of the algorithm at various levels of severity.

For each system we run five cases, A-E. In Case A, we run the experiment with each line (one at a time) removed from service. In the rest of the experiments we change the values of line characteristics using a randomly generated factor, β, between .1

TABLE I
CASE DESCRIPTIONS

Line	Case				
	A	B	C	D	E
1st	Remove	Modify two factors	Modify reactance	Modify reactance	Modify reactance
2nd	—	—	Modify line rating	Modify line rating	Modify line rating
3rd	—	—	—	Modify resistance	Modify resistance
4th	—	—	—	—	Modify line rating or Remove

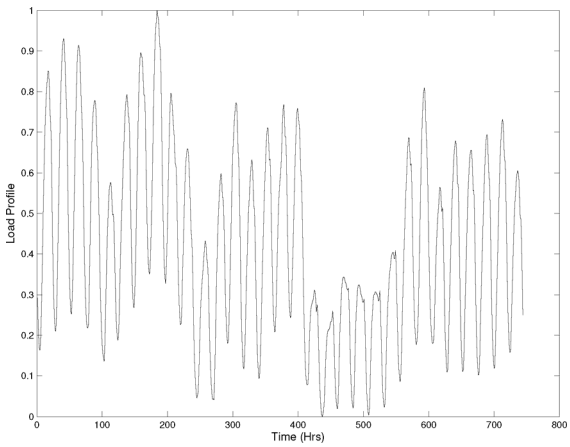


Fig. 2. Standardized load.

and 1.9, excluding the value 1. For each modification, a new β is generated. To test multiple attacks on a single line, in Case B we randomly choose two characteristics on the same line—resistance, reactance, line charging susceptance or MVA rating and modify the value of each characteristic by β. Line characteristic values are independent since our algorithm modifies the value stored in the database and the OPF module performs its calculations directly from the data in the database. Cases C, D and E are designed to test attacks on multiple lines at the same time. In Case C we randomly select two lines, change reactance on the first line and MVA rating on the second line. Case D tests a three line attack. We randomly select three lines, change reactance on the first line, MVA rating on the second line and resistance on the third line. And finally, Case E tests a four line attack. Four lines are randomly selected, reactance is changed on the first line, MVA rating on the second line, resistance on the third line and on the fourth line, either the MVA rating is changed or the line is removed from service. Table I summarizes the case descriptions.

Using actual data from the PJM [32], a standardized load profile of 744 hours is created by scaling down the load data so the value 1.0 corresponds to the peak load in the data. Fig. 2 is a plot of the standardized load. The load at each hour is calculated by applying the load profile to the load supplied by the IEEE test systems at each bus (where there is load). Although the load at each bus follows the same-time variability pattern, the actual values are distinct at different buses.

The design parameters, K and τ, are dependent on the data being analyzed. For each of the test systems we carefully choose

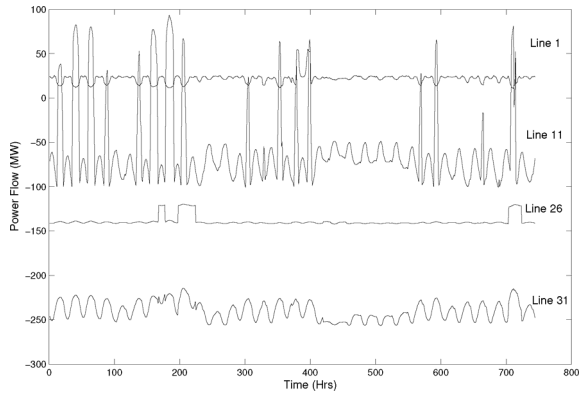


Fig. 3. Real power flow based on standardized load.

the parameters to ensure that cyberattacks of all severity are discovered and false alarms are not a problem for the operator.

We run the Monte Carlo simulation for 168 hours (1/4 of the total profile) to generate historical power flows. We refresh the historical data dynamically with $T_0 = t_{\text{current}} - 168$ for 168 hours when an anomaly is detected throughout each of the case studies. In the simulation, generator failures are sampled according to a continuous-time two-state Markov chain [31]. In Fig. 3 notice the variations in the plotted power flows on four of the lines in the 24-bus system.

In all cases we use PCA to derive an orthogonal basis set and form two subspaces, $\mathbf{A}_r$ and $\mathbf{A}_i$. $\mathbf{A}_r$ is the $J \times P$ subspace which contains most of the system's variability. We perform our analysis with the $J \times K$ subspace $\mathbf{A}_i$ where the least amount of system variability is captured. We map the flow observations, $\mathbf{z}(t)$ into the subspace, $\mathbf{A}_i$ using (20) and simulate the system.

To study the performance of the detection approach for each case study we run our simulation for 576 hours under regular operating conditions that include load variability and generator outages. At hour 577 we represent a cyberattack by introducing an anomaly prior to running the OPF module.

We define the severity of an attack as the overall amount of change that is introduced to the system by the anomaly. The severity level of each change is based on the factor, β, that is applied to the line characteristic. A low severity level 1 corresponds to a factor of .9 (reduce the value of the line characteristic by 10%) or 1.1 (increase the value of the line characteristic by 10%) and a high severity level 9 corresponds to a factor of .1 (reduce the value of the line characteristic by 90%) or 1.9 (increase the value of the line characteristic by 90%). Other severity levels relate in the same way. The severity level of an attack is the sum of the severity levels for each change in the attack.

Because we sum the severity levels when multiple lines are attacked and in each case a different number of lines are attacked, we define severity classes to better aggregate the large amount of data. In Table II we introduce five severity classes and show how the severity levels are aggregated among them.

A. 24-Bus Reliability Test System

1) Design Parameters K and τ: To choose design parameters we run a full experiment for several combinations of K and τ. In the experiment we change the reactance for each line, one at a time, by β. Table III shows results at three different values

TABLE II
SEVERITY CLASSES

Severity Class	Total Severity Level		
	Case C	Case D	Case E
1	2-3	3-5	4-8
2	4-7	6-10	9-14
3	8-12	11-18	15-23
4	13-16	19-23	24-29
5	17-18	24-27	30-36

TABLE III
PARAMETER (K AND τ) SELECTION FOR 24-BUS SYSTEM

K	τ	False Anomalies	Detections at β			Total Detections (%)
			.2	.8	1.5	
11	0.00009	5	37	36	37	98.35
11	0.0001	4	37	36	37	98.35
11	0.00011	3	37	35	37	97.9
10	0.00002	6	37	36	37	98.8
10	0.00003	3	37	35	37	98.2
10	0.00004	3	37	35	37	97.45
9	0.00001	5	37	35	37	98.5
9	0.00002	4	37	35	36	96.1
9	0.00003	2	37	35	35	95.35

of β. In every experiment using this test system, no anomalies are detected on line 11. To further investigate line 11, we calculate the line outage distribution factor (LODF) [25] matrix in MatPower for the 24-bus system. Line 11 is the only line with a factor of 0 for every line to line relationship. The LODF sensitivity analysis is an indication that line 11 is unaffected by changes to and outages in other lines in the system. Line 11 is a radial line connecting generator bus 7 (three generators and customer load) to load bus 8. Because line 11 provides the only source of power to the substation serving customers at bus 7, its power flow will be unaffected by changes in other lines and all results using this system are calculated with line 11 eliminated from the calculations.

The best results occur with $K = 10$ and $\tau = 0.00003$ where we detect 37 of 37 introduced anomalies when the reactance is decreased by 80% ($\beta = .2$), 35 of 37 introduced anomalies when the reactance is decreased by 20% ($\beta = .8$), and 37 of 37 introduced anomalies when the reactance is increased by 50% ($\beta = 1.5$) with only 3 false alarms. Increasing τ to .00004 and keeping $K = 10$ detects fewer introduced anomalies overall and results in the same number of false alarms while decreasing τ to .00002 and keeping $K = 10$ detects more introduced anomalies, but results in 6 false alarms.

The scree plot in Fig. 4 shows the cumulative variance captured by each principal component. The first 9 components, where $K = 38-9 = 29$, contain 99.996% of the variance in the power flow data so any choice of $K \leq 29$ will concentrate very close to 100% of the normal variability in the principal components formed by the regular subspace, A_r. Since our algorithm detects anomalies (outliers) in the power flow data, we focus on the minor components that contain the least amount of variance. Choosing $K = 10$ we capture 100% of the normal variability in the principal components formed by subspace, A_r. Hence,

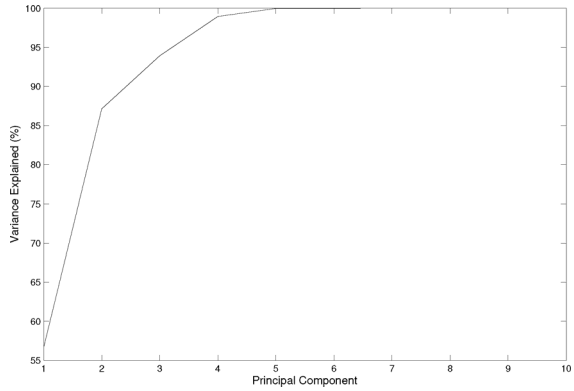


Fig. 4. Scree plot of cumulative variance.

TABLE IV
ANOMALY DETECTION IN A SINGLE LINE FOR 24-BUS SYSTEM

Case	Lines Not Detected	OPF Did Not Converge
A	None	10, 11
B	1, 8, 10, 11, 17, 19, 23	None

TABLE V
ANOMALY DETECTION BY SEVERITY CLASS FOR 24-BUS SYSTEM

Severity	Case C (%)	Case D (%)	Case E (%)
1	89	93	100
2	95	98	99
3	98	99	100
4	99	100	100
5	100	100	100
Overall	97	99	100

we perform our analysis with $K = 10$ and use the threshold, $\tau = 0.00003$.

2) Experimental Results: Results from Cases A and B are summarized in Table IV and results from Cases C, D, and E in Table V. The last row of Table V reports the overall percentage of anomaly detections for Cases C, D, and E.

In Case A the experiment is run a total of 38 times, once with each line (one at a time) removed from service. When either line 10 or line 11 is removed from service the OPF does not converge. Line 10 connects bus 6 to bus 10. Line 11 connects bus 7 to bus 8 and is a radial line, providing the only source of power to bus 7. For reporting purposes the situation where the OPF does not converge is considered a detection since the operator would be alerted. The introduced anomalies in Case A are detected 100% of the time.

In Case B where we test two changes on a single line, we again run the experiment once for each line for a total of 38 times. We detect the introduced anomaly on all but seven lines or 84% of the time. Detection is influenced both by the size of the change factor, β, and the characteristic that is modified. For example changes to line 1 are not detected when resistance is increased by 70% and line charging susceptance is increased by 50% (note that the value of resistance is independent from the value of line charging susceptance here since the OPF module reads the changed values from the database directly).

But changes to line 4, when MVA rating is decreased by 30% and reactance is increased by 20%, are detected.

To further test our algorithm, we perform three additional experiments in Cases C, D and E and run each experiment 1000 times. The severity class of each anomaly is measured as described previously.

In Case C we randomly modify two lines at one time. In the 1000 repetitions 97% of the anomalies are detected and all of the anomalies representing the severest attacks are detected. Among the anomalies not detected are one where in line 8 the MVA rating is reduced by 70% (severity 3) and in line 4 the reactance is reduced by 10% (severity 1). We sum the severity levels $(3 + 1 = 4)$ and from Table II we consider the anomaly to be in severity class 2. We note that in 17 of the 18 experimental runs where the reactance is changed on line 11 (65% of the undetected anomalies) the combined anomaly is not detected regardless of the amount of change introduced to the reactance. The OPF does not converge in the 18th experiment.

In Case D we randomly modify three lines at one time. 99% of the anomalies are detected in the 1000 repetitions and once again all of the anomalies representing the severest attacks are detected. Among the anomalies not detected are one repetition where in line 8 the MVA rating is increased by 20% (severity 2), in line 18 the reactance is increased by 20% (severity 2), and in line 22 the resistance is reduced by 10% (severity 1) Summing the three severities $(2 + 2 + 1 = 5)$ in Table II we consider the anomaly to be in severity class 1. Line 11 is one of the three lines in 73% of the undetected anomalies.

And, in Case E we randomly modify four lines at one time and detect anomalies 99.5% of the time. In the two highest overall severity levels, we detected 100% of the anomalies. Two of the five anomalies not detected include line 11 as one of the four lines. One of the anomalies not detected in severity class 3 was the repetition where in line 32 the line rating was increased by 70% (severity 7), in line 1 the reactance was increased by 20% (severity 2), in line 3 the resistance was increased by 20% (severity 2), and in line 2 the MVA rating was reduced by 60% (severity 6). The sum $(7+2+2+6 = 17)$ classifies the severity as class 3.

B. 118-Bus Reliability Test System

1) Design Parameters K and τ: Again we run a full experiment, changing line reactance by a factor, β, ranging from -10% to $+90\%$ on each line repeatedly for several combinations of K and τ. The choice of K is informed by a scree plot of cumulative variance by principal component similar to Fig. 4. Representative results from the experiment are documented in Table VI and we choose $K = 86$ and $\tau = .01727$. The number of false anomalies with this parameter selection is 10 and the overall rate of detection is 72.8%. With $K = 86$ we capture 100% of the normal variability in the subspace, A_r. We perform the remainder of our analysis with $K = 86$ and threshold, $\tau = .01727$.

2) Experimental Results: Experimental Cases A, B, C, D, and E are run in exactly the same manner as in the previous section with results from Cases A and B summarized in Table VII and results from Cases C, D, and E summarized in Table VIII. The last row of Table VIII is the overall percentage of anomaly detections for Cases C, D, and E.

TABLE VI
PARAMETER (K AND τ) SELECTION FOR 118-BUS SYSTEM

K	τ	False Anomalies	Detections at β .2	.8	1.5	Total Detections (%)
87	0.02072	9	156	112	138	71.6
87	0.02037	10	156	112	138	71.7
87	0.01379	11	158	120	147	74.8
86	0.02029	9	156	112	138	71.5
86	0.01727	10	157	113	140	72.8
86	0.01527	11	158	115	145	73.7
85	0.02014	9	155	111	137	71.3
85	0.01714	10	157	113	139	72.4
85	0.01371	11	158	120	145	74.3

TABLE VII
ANOMALY DETECTION IN A SINGLE LINE FOR 118-BUS SYSTEM

Case	Anomalies	Detected	OPF Did Not Converge	Not Detected
A	186	172	10	4
B	186	93	0	93

TABLE VIII
ANOMALY DETECTION BY SEVERITY CLASS FOR 118-BUS SYSTEM

Severity	Case C (%)	Case D (%)	Case E (%)
1	57	36	100
2	65	72	99
3	74	83	100
4	83	89	100
5	88	94	100
Overall	74	82	100

In Case A we remove a line from service, one at a time and the system detects the removal of 97.8% of the lines. In Case B we randomly choose two line characteristics to modify on one line at a time. The system detects the line changes on 50% of the lines. In Case C we randomly modify two lines. In the 1000 repetitions 74% of the anomalies are detected. The percentage of anomalies detected increases with increasing attack severity. Among the anomalies not detected is one repetition where in line 18 the reactance is reduced by 90% (severity 9) and in line 184 the MVA rating is reduced by 60% (severity 6). Summed $(9 + 6 = 15)$ severities put this anomaly in severity class 4.

In Case D we randomly modify three lines and 82% of the anomalies are detected in the 1000 repetitions. In the one anomaly not detected in the highest overall severity level of 5 the MVA rating in line 74 is increased by 80%, in line 79 the reactance is increased by 90%, and in line 171 the resistance is increased by 90%.

And, in Case E we randomly modify four lines and detect anomalies 99.6% of the time. The two anomalies not detected in this experiment are both in severity class 2. In the first one, the MVA rating in line 42 is increased by 50%, in line 12 the reactance is increased by 20%, in line 143 the resistance is increased by 20%, and in line 152 the MVA rating is reduced by 40%. In the second one, the MVA rating in line 148 is increased by 30%, in line 50 the reactance is reduced by 40%, in line 7 the resistance is reduced by 40%, and in line 6 the MVA rating is reduced by 10%.

VI. Conclusion

Sophisticated cyberterrorists will have sufficient technical computer and power system knowledge to devise an attack through the Internet which could compromise the power grid. In this paper we described a new class of cyberattacks to power systems—malicious modification of network data stored in an accessible database. We developed an algorithm that uses the results of principal component analysis to detect data anomalies resulting from this new class of attack.

We evaluated our algorithm by changing parameters associated with transmission lines in the power system and analyzing the resulting optimal power flows across two test systems. In our experiments we emulated an intruder and changed multiple parameters for a single transmission line as well as parameters for two, three, and four transmission lines. The algorithm was successful in detecting introduced anomalies at various severity levels with a small number of false alarms. While the algorithm was more successful in the 24-bus system than in the larger 118 bus system, in both systems the most severe anomalies were detectable over 88% of the time.

Engineers, system operators and government officials know that cybercrime prevention is not sufficient to protect the power grid and just as BDD in state estimation focuses on detection, additional detection algorithms strategically placed in the systems that manage the grid will certainly increase its reliability. Encouraged by the results from testing our algorithm, we believe that additional testing on larger systems using industry-provided data will demonstrate the value of implementing it in the network topology processing portion of the OPF module to improve database security in the power grid. Our new algorithm adds a dimension of protection for power systems that has not previously been addressed in the literature.

References

[1] G. C. Wilshusen, Cyber Threats and Vulnerabilities Place Federal Systems at Risk, May 2009. [Online]. Available: http://www.gao.gov/new.items/d09661t.pdf.

[2] B. Wingfield, Power-Grid Cyber Attack Seen Leaving Millions in Dark for Months, Jan. 2012. [Online]. Available: http://www.bloomberg.com/news/2012-02-01/cyber-attack-on-u-s-power-grid-seen-leaving-millions-in-dark-for-months.html.

[3] R. McMillan, "Siemens: Stuxnet worm hit industrial systems," *PC-World*, 2010.

[4] D. Dolezilek and L. Hussey, "Requirements or recommendations? sorting out NERC CIP, NIST, and DOE cybersecurity," in *Proc. 2011 64th Annu. Conf. Protective Relay Engineers*, 2011.

[5] F. F. Wu, K. Moslehi, and A. Bose, "Power system control centers: Past, present, and future," *Proc. IEEE*, vol. 93, pp. 1890–1907, 2005.

[6] Integrated Topology Processing: A Breakthrough in Power System Software Unification. [Online]. Available: http://www.power-world.com/products/IntegratedTP.asp.

[7] J. A. Momoh, R. J. Koessler, M. S. Bond, B. Stott, D. Sun, A. Papalexopoulos, and P. Ristanovic, "Challenges to optimal power flow," *IEEE Trans. Power Syst.*, vol. 12, pp. 444–447, 1997.

[8] L. Huang, X. Nguyen, M. Garofalakis, M. Jordan, A. Joseph, and N. Taft, In-Network PCA and Anomaly Detection, UC Berkeley, Tech. Rep., Jan. 2007.

[9] A. Lakhina, M. Crovella, and C. Diot, "Diagnosing network-wide traffic anomalies," in *Proc. ACM Conf. Special Interest Group on Data Communications (SIGCOMM)*, 2004.

[10] F. C. Schweppe, J. Wildes, and D. B. Rom, "Power system static state estimation, Parts, I, II, and III," *IEEE Trans. Power App. Syst.*, vol. PAS-89, pp. 120–135, 1970.

[11] E. Handschin, F. C. Schweppe, J. Kohlas, and A. Fechter, "Bad data analysis for power system state estimation," *IEEE Trans. Power App. Syst.*, vol. PAS-94, pp. 329–337, 1975.

[12] V. H. Quintana, A. Simoes-Costa, and M. Mier, "Bad data detection and identification techniques using estimation orthogonal methods," *IEEE Trans. Power App. Syst.*, vol. PAS-101, pp. 3355–3364, 1982.

[13] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," in *Proc. ACM Conf. Computer and Communications Security*, 2009, pp. 21–32, Associated Computer Machinery.

[14] R. B. Bobba, K. M. Rogers, Q. Wang, H. Khurana, K. Nahrstedt, and T. J. Overbye, "Detecting false data injection attacks on DC state estimation," in *Proc. Workshop Secure Control Systems*, 2010.

[15] H. Sandberg, A. Teixeira, and K. H. Johansson, "Stealth attacks and protection schemes for state estimators in power networks," in *Proc. 1st Workshop Secure Control Systems (CPSWEEK)*, 2010.

[16] G. Dan and H. Sandberg, "Stealth attacks and protection schemes for state estimators in power systems," in *Proc. 2010 1st IEEE Int. Conf. Smart Grid Communications (SmartGridComm)*, Oct. 2010, pp. 214–219.

[17] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Malicious data attacks on the smart grid," *IEEE Trans. Smart Grid*, vol. 2, pp. 645–658, 2011.

[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] A. Giani, E. Bitar, M. Garcia, M. McQueen, P. Khargonekar, and K. Poolla, "Smart grid data integrity attacks: Characterizations and countermeasures," in *Proc. IEEE SmartGridComm*, 2011.

[20] T. T. Kim and H. V. Poor, "Strategic protection against data injection attacks on power grids," *IEEE Trans. Smart Grid*, vol. 2, no. 2, pp. 326–333, Jun. 2011.

[21] A. Abur and A. G. Exposito, *Power System State Estimation: Theory and Implementation*. New York: Marcel Dekker, 2004.

[22] R. D. Zimmerman, C. E. Murillo-Sanchez, and R. J. Thomas, "Matpower: Steady-state operations, planning and analysis tools for power systems research and education," *IEEE Trans. Power Syst.*, vol. 26, no. 1, pp. 12–19, Feb. 2011.

[23] J. Carpentier, "Contribution e l'etude do dispatching economique," in *Bulletin Society Francaise Electriciens*, 1962, vol. 3.

[24] H. W. Dommel and W. F. Tinney, "Optimal power flow solutions," *IEEE Trans. Power App. Syst.*, vol. PAS-87, pp. 1866–1876, 1968.

[25] A. J. Wood and B. F. Wollenberg, *Power Generation, Operations, and Control*, 2nd ed. New York: Wiley, 1996.

[26] M. L. Crow, *Computational Methods for Electric Power Systems*, 2nd ed. Boca Raton, FL: CRC, 2009.

[27] K. Pearson, "On lines and planes of closest fit to systems of points in space," *Philosoph. Mag.*, vol. 2, no. 11, pp. 559–571, 1901.

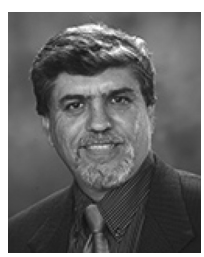
[28] H. Hotelling, "Analysis of a complex of statistical variables into principal components," *J. Educ. Psychol.*, vol. 24, pp. 417–441 and 498–520, 1933.

[29] H. Ringberg, J. Rexford, A. Soule, and C. Diot, "Sensitivity of PCA for traffic anomaly detection," *Signetrics 2007*, 2007.

[30] I. T. Jolliffe, *Principal Component Analysis*, ser. Springer Series in Statistics, 2nd ed. New York: Springer, 2002.

[31] IEEE RTS Task Force of APM Subcommittee, "IEEE reliability test system," *IEEE Trans. Power App. Syst.*, vol. PAS-98, no. 6, pp. 2047–2054, 1979.

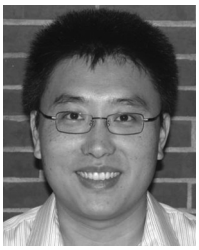
[32] PJM Operational Data. [Online]. Available: http://www.pjm.com.



Jorge Valenzuela received the Ph.D. degree in industrial engineering at the University of Pittsburgh, Pittsburgh, PA, in 2000.

His research interests are applied and theoretical stochastic modeling and optimization. His recent research involves stochastic models for the economics of wind power, optimization of electric power generation, and cybersecurity. He is Professor and Chair in the Department of Industrial and Systems Engineering at Auburn University, Auburn, AL, and teaches courses on stochastic operations research and information technology.

Dr. Valenzuela is member of INFORMS and IIE.



Jianhui Wang (M'07) received the Ph.D. degree in electrical engineering from Illinois Institute of Technology, Chicago, in 2007.

Presently, he is a Computational Engineer with the Decision and Information Sciences Division at Argonne National Laboratory, Argonne, IL.

Dr. Wang is the chair of the IEEE Power & Energy Society (PES) power system operation methods subcommittee and co-chair of an IEEE task force on the integration of wind and solar power into power system operations. He is an editor of the IEEE TRANSACTIONS ON SMART GRID, an editor of *Applied Energy*, and an associated editor of the *Journal of Energy Engineering*. He is the technical program chair of the IEEE Innovative Smart Grid Technologies conference 2012.

Nancy Bissinger (S'10) received the B.S. degree in mathematics and M.S. degree in industrial and systems engineering degree from Auburn University, Auburn, AL, in 1973 and 2010, respectively, where she is presently pursuing her Ph.D. degree in industrial and systems engineering.

She worked for eight years as a project manager for Entergy Corporation in New Orleans, LA.