Blind False Data Injection Attack Using PCA Approximation Method in Smart Grid

Zong-Han Yu and Wen-Long Chin

***Abstract*—Accurate state estimation is of paramount importance to maintain normal operations of smart power grids. However, recent research shows that carefully produced attacks with the knowledge of the grid topology, i.e., Jacobian matrix, can bypass the bad data detection (BDD) system. The BDD is used to ensure the integrity of state estimation to filter faulty measurements introduced by device malfunctions or malicious attacks. However, to construct the false data injection attack vectors, a common assumption in most prior works on false data injection attacks is that the attacker has complete knowledge about the power grid topology and transmission-line admittances. By contrast, this paper studies the general problem of blind false data injection attacks using the principal component analysis approximation method without the knowledge of Jacobian matrix and the assumption regarding the distribution of state variables. The proposed attack is proven to be approximately stealthy.[1] The performance of the proposed attack is analyzed. Simulations confirm the performance of the proposed method.**

***Index Terms*—Bad data detection (BDD), blind and stealthy attack, Jacobian matrix, principal component analysis (PCA), smart power grid, state estimation.**

I. Introduction

ELECTRICITY is the lifeline of civilization. Recent advances in smart grid can significantly enhance efficiency and reliability of power grids [1]. The smart grid [2], [3] envisions an interconnected power distribution network that streamlines transmission, distribution, monitoring, and control of electricity by allowing two-way communication and flow of power [4]. Smart grid security encompasses protection of both the communication network and the power grid, because these two systems need to ensure availability of access as well as survivability under threats [5], [6]. If the state information of the grid were maliciously altered, the grid could destabilize with potential for physical damage [7]. Therefore, state estimation [8]–[13] is a key function in building real-time models of electricity networks in energy management centers.

Based on the integrated infrastructure and two-way communication, the risk and vulnerability in the power grid have increased [8]–[10]. The strong coupling between cyber and physical operations makes power systems vulnerable to cyber attacks. For example, information of the electric power system will be transmitted on the network, and the information may interest parties who want to harm the utility or its customers. Current power systems are continuously monitored and controlled by energy management system and supervisory control and data acquisition (SCADA) systems in order to maintain the operating conditions in a normal and secure state [14].

To ensure the integrity of state estimation, current power grid systems employ the bad data detection (BDD) to filter faulty measurements caused by device malfunctions or malicious attacks. The threat of false data injection attack is an important issue for the success of smart grid [10], [15]. The power system uses the BDD system to detect the random errors caused by device malfunctions, telemetry failure, and communication noise. As the power grid becomes more complicated than before, there will be plenty of ways through the integrated communication network to attack the power system. Owing to arising new vulnerability in the system, the BDD system may not be able to protect the system thoroughly.

To construct the false data injection attack vectors, a common assumption in most prior works on false data injection attacks is that the attacker has complete knowledge about the power grid topology and transmission-line admittances. However, it is more practical than prior works by the case of knowing limited information regarding the power network topology or admittance for some transmission lines [16]. In [16], a successful false data attack with limited information is described. By contrast, this paper studies the problem of blind false data injection attacks without explicit knowledge of the power grid topology and makes inferences from the correlations of the line measurements, while the countermeasures for the proposed attacks are outside the scope of this paper. The dc power flow model [17], which considers the voltage angles of all buses as state variables, is utilized in this paper. In practice, a nonlinear state estimator is often used. We demonstrate that, under the nonlinear ac power flow model, effective attack vectors can still be generated by the proposed method. Though distributed implementation is possible, we focus on centralized attack carried out by breaking into the SCADA system in the utility control center.

The proposed method utilizes the principal component analysis (PCA) [18] approximation method to transform the observation vector into a linear combination of a vector with uncorrelated components, which can be regarded as the product of the PCA matrix and observation vector. The PCA matrix obtained by the PCA can be also viewed as the product of the

Manuscript received May 29, 2014; revised October 21, 2014; accepted December 13, 2014. Date of publication January 6, 2015; date of current version April 17, 2015. This work was supported by Taiwan under Grant MOST-103-2221-E-006-082. Paper no. TSG-00522-2014.

The authors are with National Cheng Kung University, Tainan 701, Taiwan (e-mail: johnsonchin@pchome.com.tw).

Digital Object Identifier 10.1109/TSG.2014.2382714

[1] Approximation is introduced by the dimensionality reduction of PCA to conform to the dimension of the original Jacobian matrix.

Jacobian matrix of the power grid with a projection matrix. The attack vector generated by the PCA matrix is proven to be approximately stealthy. Approximation of the PCA matrix is introduced by the dimensionality reduction of PCA to conform to the dimension of the original Jacobian matrix. Because it is arguable to make any assumption about the distribution of state variables, the state variables of the electrical grids for the proposed attack can be any random variables with unknown distributions, including both Gaussian and non-Gaussian distributed random variables. For fixed or real state variables, the proposed method can also function very well. The performance of the proposed attack is analyzed using the extreme value theory [19]. Simulation results confirm the advantages of the proposed blind and stealthy attack.

The rest of this paper is organized as follows. Section II presents related works. Section III introduces the system model, state estimation, and BDD. Section IV then describes the conventional false data injection attack. Next, Section V gives the basic principles of PCA and the proposed blind false data injection attack. Section VI analyzes the performance of BDD against the proposed attack. Section VII summarizes the simulation results. The conclusion and future works are finally drawn in Section VIII.

II. Related Works

Complete surveys of existing attacks and detection methods for false data injection attacks are given in [20] and [21]. Interested readers can refer to them, and the references therein. Some works are described briefly as follows. The effects of random and structured bad data on the state estimation are analyzed in [22]. Because the stability and synchronization of the grid depend strongly on the data in the grid, data poisoning and false injection attacks remain major concerns of smart grid security [15]. False data may be due to unintended measurement abnormalities or topology errors, or injection by malicious attacks. Many authors show how an attacker can exploit the configuration of a power system to introduce arbitrary errors in the state estimation while successfully passing existing techniques for bad measurement detection [15]–[25]. Liu *et al.* [15] showed that an attacker can carry out attacks by corrupting the power flow measurements through attacking the remote terminal units, tampering with the heterogeneous communication network or breaking into the SCADA system through the local area network of control center office. Two specific cases are investigated: 1) attacker constrained to a set of meters due to the physical protection of the meters; and 2) attacker has limited resources to launch the attack on the meters. Simulation results show that, despite the limitations, attackers will be able to compromise the state estimation in both scenarios. Two regimes of attacks are considered in [23], i.e., strong and weak attacks. In strong attack regime, the smallest set of attacked meters capable of causing network unobservability is characterized. In weak attack regime, an optimal attack based on minimum energy leakage is proposed.

Vuković and Dán [8] considered the security of fully distributed power system state estimation. It shows that an attacker that compromises the communication infrastructure of a single control center can successfully perform a denial-of-service attack. A new mechanism, named data framing attack, aimed at misleading a power system control center about the source of a data attack is proposed [9]. The proposed attack frames meters that are providing correct data as sources of bad data such that the control center will remove useful measurements that would otherwise be used by the state estimator.

Defending mechanisms against false data injection attacks by protecting a few carefully selected measurements are studied [15], [26], [27]. They show both optimum and reduced-complexity algorithms for protecting the data integrity and demonstrate it by physical experiments. Huang *et al.* [26] presented an adaptive cumulative sum algorithm to address the quick detection against the false data issue. The vulnerability of ac state estimation is assessed in [28] and [29] with respect to false data injection cyber-attacks. Bi and Zhang [10] provided an approach to defend against false data injection attacks using covert power network topological information.

III. System Model, State Estimation, and BDD

A. System Model

Consider a power system with $n+1$ buses. Assuming the resistance in the transmission line connecting buses i and j is small compared to its reactance, the active power-flow model from bus i to bus j can be expressed as [30]

$$P_{ij} = \frac{V_i V_j}{X_{ij}} \sin\left(\theta_i - \theta_j\right) \tag{1}$$

where V_i and θ_i denote the voltage magnitude and phase angle at bus i, respectively, and X_{ij} denotes the reactance between bus i and bus j. Consider the active power P_i injected into bus i, the conservation of energy yields that for all buses

$$P_i = \sum_{j \in \mathcal{A}_i} P_{ij} \tag{2}$$

where $\mathcal{A}_i$ denotes the set of buses directly connected to bus i. A negative P_i represents the power load. Even though (1) is nonlinear, the state estimate is obtained by iterations of weighted linear least square estimation with the locally linearized model. Hence, around the system operating point, it is reasonable to analyze the state estimation using the locally linearized model [9]. In dc power flow studies [17], it is usually assumed that the difference of phase angles, $\theta_i - \theta_j$, is small between any pair of buses, and the voltage magnitudes are close to unity. Therefore, by inserting (1) into (2), one has

$$P_i \approx \sum_{j \in \mathcal{A}_i} \frac{\theta_i - \theta_j}{X_{ij}}. \tag{3}$$

B. State Estimation

Let $x_i \equiv \theta_i$ denote the phase angle. The state estimation problem is to estimate the system state $\mathbf{x} = (x_1, x_2, \ldots, x_n)^T$, where $(\cdot)^T$ denotes the transpose operation. A bus is treated as the reference bus; therefore, only n phase angles need to be estimated. The control center observes a vector

$\mathbf{z} = (z_1, z_2, \ldots, z_m)^T$ of measurements from m active power-flow branches, $m \geq n$. Hence, the measurements can be generally described as

$$\mathbf{z} = P(\mathbf{x}) + \mathbf{v} \tag{4}$$

where $P(\cdot)$ denotes the nonlinear relation between measurement $\mathbf{z}$ and state $\mathbf{x}$, $\mathbf{v} = (v_1, v_2, \ldots, v_m)^T \sim N(\mathbf{0}_{m\times 1}, \Sigma_v)$ denotes the Gaussian measurement noise vector with zero mean $\mathbf{0}_{m\times 1}$, which denotes an $m \times 1$ vector with all-zero elements and $\times$ denotes the multiplication, and covariance matrix $\Sigma_v = \mathrm{diag}(\sigma_1^2, \sigma_2^2, \ldots, \sigma_m^2) = \mathbf{I}_{m\times m}\sigma_v^2$, where $\sigma_1^2 = \sigma_2^2 = \cdots = \sigma_m^2 = \sigma_v^2$, $\mathrm{diag}(\cdot)$ denotes the diagonal matrix and $\mathbf{I}_{m\times m}$ denotes the $m \times m$ identity matrix. In dc power flow model, with the Jacobian or topology matrix

$$\mathbf{H} \equiv \left.\frac{\partial P(\mathbf{x})}{\partial \mathbf{x}}\right|_{\mathbf{x}=\mathbf{0}} \tag{5}$$

the linear approximation model of (4) can be represented as

$$\mathbf{z} = \mathbf{H}\mathbf{x} + \mathbf{v}. \tag{6}$$

Here, $\mathbf{H}$ is an $m \times n$ matrix. The matrix $\mathbf{H}$ is a full rank matrix to allow the estimation of $\mathbf{x}$ from $\mathbf{z}$ [31]. Without loss of generality, we further assume $m \geq n$. Thus, $\mathrm{rank}\,(\mathbf{H}) = n$. According to (6), the maximum-likelihood estimation of $\mathbf{x}$ can be determined by [31]

$$\hat{\mathbf{x}} = \left(\mathbf{H}^T\mathbf{W}\mathbf{H}\right)^{-1}\mathbf{H}^T\mathbf{W}\mathbf{z} \tag{7}$$

where $\hat{\mathbf{x}}$ is a $n \times 1$ vector, and $\mathbf{W} = \Sigma_v^{-1}$ is an $m \times m$ matrix and denotes the inverse matrix of Σ_v.

C. BDD

Based on $\hat{\mathbf{x}}$, the residue vector $\mathbf{r}$, which is an $m \times 1$ vector, can be calculated as the difference between the measurement vector $\mathbf{z}$ and the estimated measurement vector $\mathbf{H}\hat{\mathbf{x}}$, that is

$$\mathbf{r} = \mathbf{z} - \mathbf{H}\hat{\mathbf{x}}. \tag{8}$$

It can be shown that $E[\mathbf{r}] = \mathbf{0}_{m\times 1}$, where $E[\,\cdot\,]$ denotes the expectation, and $\mathrm{Cov}(\mathbf{r}) = (\mathbf{I}_{m\times m} - \mathbf{G})\Sigma_v(\mathbf{I}_{m\times m} - \mathbf{G})^T$, where $\mathrm{Cov}(\mathbf{r})$ denotes the covariance matrix of $\mathbf{r}$, and $\mathbf{G} = \mathbf{H}(\mathbf{H}^T\mathbf{W}\mathbf{H})^{-1}\mathbf{H}^T\mathbf{W}$ is an $m \times m$ matrix. The threshold test [32] can be used to detect the false data due to attacks, faulty sensors, and topological errors, and can be expressed as

$$\max_{i=1}^{m} |r_i| \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} \gamma \tag{9}$$

where $|\cdot|$ denotes the magnitude, $\mathcal{H}_0$ and $\mathcal{H}_1$ denote the hypotheses without and with the false data injection, respectively, γ is the decision threshold, and r_i, $i = 1, 2, \ldots, m$, denotes the elements of $\mathbf{r}$.

IV. Conventional False Data Injection Attack

Under the condition of perfect knowledge of the Jacobian matrix, an attacker can inject a vector $\mathbf{a}$ resulting in the new measurements $\mathbf{z}_a = \mathbf{z} + \mathbf{a}$, where $\mathbf{a}$ and $\mathbf{z}_a$ are $m \times 1$ vectors, to masquerade as the original measurements $\mathbf{z} = \mathbf{H}\mathbf{x} + \mathbf{v}$. According to [15], an attack can be achieved with

$$\mathbf{a} = \mathbf{H}\mathbf{c} \tag{10}$$

where $\mathbf{c} = (c_1, c_2, \ldots, c_n)^T$ is an arbitrary $n \times 1$ nonzero vector. Doing so makes the residue

$$\begin{aligned}\mathbf{r}_a &= \mathbf{z}_a - \mathbf{H}\hat{\mathbf{x}}_a = \mathbf{z} + \mathbf{a} - \mathbf{H}\left(\hat{\mathbf{x}} + \mathbf{c}\right)\\ &= \mathbf{z} - \mathbf{H}\hat{\mathbf{x}} + (\mathbf{a} - \mathbf{H}\mathbf{c}) = \mathbf{z} - \mathbf{H}\hat{\mathbf{x}}\end{aligned} \tag{11}$$

where $\hat{\mathbf{x}}_a = (\mathbf{H}^T\mathbf{W}\mathbf{H})^{-1}\mathbf{H}^T\mathbf{W}\mathbf{z}_a = \hat{\mathbf{x}} + \mathbf{c}$ is a $n \times 1$ vector and represents the state estimate from the new measurement (under attack) $\mathbf{z}_a$, and $\hat{\mathbf{x}}$ denotes the state estimate from the original measurement (without attack) $\mathbf{z}$. As indicated by (8) and (11), the attack has the same residue as that without attack. Therefore, the attack is stealthy and expected to have the same probability of missed detection as that without attack, whose performance is mainly influenced by the statistical properties of the measurement noise vector $\mathbf{v}$.

V. Proposed Blind False Data Injection Attack

A. Basic Principles of PCA

Before delving into the proposed method, the basic principles of PCA are introduced. The PCA is a statistical analysis of data in an effective way by reducing the dimensions of a given unlabeled high-dimensional dataset while keeping its spatial characteristics as much as possible. More specifically, the PCA transforms the dataset into a new coordinate system such that the projection onto it has the greatest variance among all possible projections. By finding the successive coordinates (or principal components), we can visualize the distribution of the original dataset after projecting it onto a low-dimensional space [18].

Based on the original dataset (or random vector) $\mathbf{z}$ and its realization (or observed vector) $\mathbf{z}_i$, $i = 1, 2, \ldots, d$, where d denotes the number of observed vectors and $\mathbf{z}_i$ is an $m \times 1$ vector. The sample mean vector of $\mathbf{z}$ is $\mu_z = 1/d\sum_{i=1}^{d}\mathbf{z}_i$. The goal of PCA is to find a unity vector $\tilde{\mathbf{p}}_1 = (\tilde{p}_{11}, \tilde{p}_{12}, \ldots, \tilde{p}_{1m})^T$ such that the squared sum of the projection onto this direction is the maximum. Let the dataset $\mathbf{z}' = \mathbf{z} - \mu_z$, which has a zero mean vector $\mu_{z'} = \mathbf{0}_{m\times 1}$. Let $\mathbf{Z}'_{m\times d} = (\mathbf{z}'_1, \mathbf{z}'_2, \ldots, \mathbf{z}'_d)$, the projection of each column of $\mathbf{Z}'$ onto $\tilde{\mathbf{p}}_1$ can be written as

$$\mathbf{p}_{d\times 1} = \begin{bmatrix}\mathbf{z}'^T_1\tilde{\mathbf{p}}_1\\ \vdots\\ \mathbf{z}'^T_d\tilde{\mathbf{p}}_1\end{bmatrix} = \mathbf{Z}'^T\tilde{\mathbf{p}}_1 \tag{12}$$

where $\mathbf{z}'^T_i\tilde{\mathbf{p}}_1$ represents the projection of $\mathbf{z}'_i$ onto $\tilde{\mathbf{p}}_1$. Normalized by d, the square sum of the projection is a function of $\tilde{\mathbf{p}}_1$ and can be denoted by

$$J(\mathbf{p}) = \frac{1}{d}|\mathbf{p}|^2 = \frac{1}{d}\mathbf{p}^T\mathbf{p} = \frac{1}{d}\tilde{\mathbf{p}}_1^T\mathbf{Z}'\mathbf{Z}'^T\tilde{\mathbf{p}}_1 = \tilde{\mathbf{p}}_1^T\Sigma_{z'}\tilde{\mathbf{p}}_1 \tag{13}$$

where the sample covariance matrix $\Sigma_{z'} = 1/d\sum_{i=1}^{d}(\mathbf{z}'_i - \mu_{z'})(\mathbf{z}'_i - \mu_{z'})^T = 1/d\mathbf{Z}'\mathbf{Z}'^T$ is an $m \times m$ matrix. Notably, the sample covariance matrix of $\mathbf{z}$, Σ_z, is the same as $\Sigma_{z'}$. To maximize $J(\mathbf{p})$ under the constraint $|\tilde{\mathbf{p}}_1| = 1$, one can use the Lagrange multiplier to form a new objective function

$$\tilde{J}\,(\mathbf{p}, \lambda_1) = \tilde{\mathbf{p}}_1^T\Sigma_{z'}\tilde{\mathbf{p}}_1 + \lambda_1\left(1 - \tilde{\mathbf{p}}_1^T\tilde{\mathbf{p}}_1\right). \tag{14}$$

Differentiate $\tilde{J}(\mathbf{p}, \lambda_1)$ with respect to $\tilde{\mathbf{p}}_1$ and set it to zero, one has

$$\Sigma_{z'}\tilde{\mathbf{p}}_1 = \lambda_1\tilde{\mathbf{p}}_1. \tag{15}$$

It is obvious that the solution $\tilde{\mathbf{p}}_1$ of (15) is an eigenvector of $\Sigma_{z'}$ with eigenvalue λ_1. Under this condition

$$J(\mathbf{p}) = \lambda_1. \tag{16}$$

Without loss of generality, one can arrange the eigenvalues of $\Sigma_{z'}$ into a descending order

$$\lambda_1 > \lambda_2 > \cdots > \lambda_m \tag{17}$$

with the corresponding eigenvectors $\tilde{\mathbf{p}}_1, \tilde{\mathbf{p}}_2, \ldots, \tilde{\mathbf{p}}_m$. Then, the maximum value of $J(\mathbf{p})$ is λ_1, which occurs at $\tilde{\mathbf{p}}_1$, while the second maximum is λ_2, which occurs at $\tilde{\mathbf{p}}_2$, and so on.

Once we have found the first principal component $\tilde{x}_1 = \tilde{\mathbf{p}}_1^T\mathbf{z}$ as the projection onto the unity eigenvector corresponding to the maximum eigenvalue of $\Sigma_{z'}$, we can continue to find the second principal component $\tilde{x}_2 = \tilde{\mathbf{p}}_2^T\mathbf{z}$ that achieves the maximum projection onto $\tilde{\mathbf{p}}_2$ with the constraint that $\tilde{\mathbf{p}}_2$ is orthogonal to $\tilde{\mathbf{p}}_1$. To this end, the objective function

$$\tilde{J}_1(\mathbf{p}, \rho_1, \rho_2) = \tilde{\mathbf{p}}_2^T\Sigma_{z'}\tilde{\mathbf{p}}_2 + \rho_1\left(1 - \tilde{\mathbf{p}}_2^T\tilde{\mathbf{p}}_2\right) + \rho_2\left(\tilde{\mathbf{p}}_2^T\tilde{\mathbf{p}}_1\right) \tag{18}$$

is maximized by differentiating it respect to $\tilde{\mathbf{p}}_2$, which can be found that the solution $\tilde{\mathbf{p}}_2$ is also an eigenvector of $\Sigma_{z'}$ with eigenvalue λ_2. By repeating this process, one can obtain the successive principal components as the projection onto orthogonal eigenvectors $\tilde{\mathbf{p}}_1, \tilde{\mathbf{p}}_2, \ldots, \tilde{\mathbf{p}}_m$ of $\Sigma_{z'}$. Notable, since $\Sigma_{z'}$ is symmetric, its eigenvectors form an orthonormal basis with $\tilde{\mathbf{p}}_i^T\tilde{\mathbf{p}}_j = 0$, $\forall i \neq j$.

The steps for the PCA operation are summarized here. First, the sample mean vector, μ_z, of the dataset $\mathbf{z}$ is obtained. Second, since $\Sigma_{z'} = \Sigma_z$, the sample covariance matrix Σ_z is calculated. Third, find the eigenvalues of Σ_z and arrange them into descending order $(\lambda_1, \lambda_2, \ldots, \lambda_m)$, with eigenvectors $(\tilde{\mathbf{p}}_1, \tilde{\mathbf{p}}_2, \ldots, \tilde{\mathbf{p}}_m)$. Finally, the transformation matrix

$$\tilde{\mathbf{P}}^T = \begin{bmatrix} \tilde{\mathbf{p}}_1^T \\ \tilde{\mathbf{p}}_2^T \\ \vdots \\ \tilde{\mathbf{p}}_m^T \end{bmatrix} \tag{19}$$

is an $m \times m$ matrix and used to transform $\mathbf{z}$ into $\tilde{\mathbf{x}}$ as

$$\tilde{\mathbf{P}}^T\mathbf{z} = \tilde{\mathbf{x}} \tag{20}$$

where the vector of principal components $\tilde{\mathbf{x}} = (\tilde{x}_1, \tilde{x}_2, \ldots, \tilde{x}_m)^T$. The elements of $\tilde{\mathbf{x}}$ are mutually orthogonal, and $\Sigma_{\tilde{x}} = 1/d\sum_{i=1}^{d}(\tilde{\mathbf{x}}_i - \mu_{\tilde{x}})(\tilde{\mathbf{x}}_i - \mu_{\tilde{x}})^T = \mathrm{diag}(\lambda_1, \lambda_2, \ldots, \lambda_m)$. If one only wants to keep n dimensions, $n \leq m$, then simply put n eigenvectors into $\tilde{\mathbf{P}}$.

B. Blind Derivation of the PCA Matrix Using PCA

This paper studies the problem of blind false data injection attacks without prior knowledge of the power grid topology and makes inferences from the correlations of the line measurements. We focus on the problems of identifying the impact of malicious cyber attacks on state estimation, by recognizing the key role of state estimation as the interface between cyber and physical operations in a smart grid.

The PCA is a mathematical procedure that uses orthogonal transformation to convert a set of observations of possibly correlated variables $\mathbf{z}$ into a set of linearly uncorrelated variables, $\tilde{\mathbf{x}}$, called principal components. Or, equivalently, (20) can be written as

$$\mathbf{z} = \left(\tilde{\mathbf{P}}^T\right)^{-1}\tilde{\mathbf{x}} = \tilde{\mathbf{P}}\tilde{\mathbf{x}} \tag{21}$$

because eigenvectors form an orthonormal basis.

The PCA algorithm maximizes the variance of principal components to reduce the dimension of a data set, which indicates that the first principal component has the largest eigenvalue λ_1. The sample variance of $\tilde{x}_i = \tilde{\mathbf{p}}_i^T\mathbf{z}$ can be shown to be

$$\mathrm{var}(\tilde{x}_i) = \tilde{\mathbf{p}}_i^T\Sigma_z\tilde{\mathbf{p}}_i = \tilde{\mathbf{p}}_i^T\Sigma_{z'}\tilde{\mathbf{p}}_i = \lambda_i\tilde{\mathbf{p}}_i^T\tilde{\mathbf{p}}_i = \lambda_i \tag{22}$$

where the third equality holds because of (15). Hence, this transformation is defined in such a way that the first principal component has the largest variance, the second principal component has the second largest variance, and so on.

Generally, the ith principal component can be given as

$$\tilde{x}_i = \tilde{\mathbf{p}}_i^T\mathbf{z}. \tag{23}$$

By the PCA, the number of principal components can be less than the number of original variables, which is named the dimensionality reduction. In smart grid, owing to the dimension of the Jacobian matrix, we propose to use the number of state variables, n, as the number of principal components. Hence, dropping those nonprincipal components, $\tilde{x}_i$ for $n < i \leq m$, with small variances or eigenvalues of Σ_z, and according to (21), $\mathbf{z}$ can be approximated by

$$\begin{aligned}\mathbf{z} &\approx \begin{bmatrix}\tilde{\mathbf{p}}_1 \ldots \tilde{\mathbf{p}}_m\end{bmatrix}\begin{bmatrix}\tilde{x}_1 \\ \vdots \\ \tilde{x}_n \\ 0 \\ \vdots \\ 0\end{bmatrix} \\ &= \underbrace{\begin{bmatrix}\tilde{\mathbf{p}}_1 \ldots \tilde{\mathbf{p}}_n\end{bmatrix}}_{\equiv\mathbf{H}_{\mathrm{PCA}}}\underbrace{\begin{bmatrix}\tilde{x}_1 \\ \vdots \\ \tilde{x}_n\end{bmatrix}}_{\equiv\mathbf{x}_{\mathrm{PCA}}} \\ &= \mathbf{H}_{\mathrm{PCA}}\mathbf{x}_{\mathrm{PCA}}\end{aligned} \tag{24}$$

where the dimensionality reduction version of $\tilde{\mathbf{P}}$, i.e., the PCA matrix $\mathbf{H}_{\mathrm{PCA}}$, is an $m \times n$ matrix and will be used for the new topology matrix, and $\mathbf{x}_{\mathrm{PCA}}$ is a $n \times 1$ vector.

Next, the relation between $\mathbf{x}$ and $\mathbf{x}_{\mathrm{PCA}}$ is obtained.

Proposition 1:

$$\mathbf{x} \approx \mathbf{P}_x\mathbf{x}_{\mathrm{PCA}} \tag{25}$$

where $\mathbf{P}_x = \mathbf{H}^{+}\mathbf{H}_{\mathrm{PCA}}$ is a $n \times n$ projection matrix of principal components $\mathbf{x}_{\mathrm{PCA}}$ to original state variables $\mathbf{x}$, and $\mathbf{H}^{+}$ is a $n \times m$ matrix and denotes the pseudoinverse of $\mathbf{H}$ (see the Appendix A). Notably, $\mathbf{x} \approx \mathbf{P}_x\mathbf{x}_{\mathrm{PCA}} \neq \mathbf{x}_{\mathrm{PCA}}$. The relation between $\mathbf{x}$, $\mathbf{x}_{\mathrm{PCA}}$, and $\mathbf{z}$ can be described using the vector projection in Fig. 1.

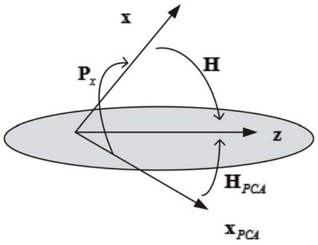

Fig. 1. Relation between $\mathbf{x}$, $\mathbf{x}_{\text{PCA}}$, and $\mathbf{z}$ described using the vector projection.

Algorithm 1 Blind Stealthy Attack

```
input : original dataset $\mathbf{z}$
[$\mathbf{H}_{\text{PCA}}$,$\tilde{\mathbf{x}}$]=PCA($\mathbf{z}$,$n$); % The dimension of $\mathbf{H}_{\text{PCA}}$ is $m \times n$.
                               % Transformed dataset $\tilde{\mathbf{x}}$ is not needed
                               % by the proposed attack.
Generate a nonzero vector $\mathbf{c} = (c_1, c_2, \ldots, c_n)^T$,
  $c_i \sim N(0, \sigma_c^2)$;   % $\sigma_c^2$ denotes the variance of $c_i$, $\forall i$.
$\mathbf{a}_{\text{PCA}} = \mathbf{H}_{\text{PCA}}\mathbf{c}$;
$\mathbf{z}_{a,\text{PCA}} = \mathbf{z} + \mathbf{a}_{\text{PCA}}$;
output : false dataset $\mathbf{z}_{a,\text{PCA}}$
```

C. Blind Stealthy Attack

Ignore measurement noise, the measurements can be represented as

$$\mathbf{z} = \mathbf{H}\mathbf{x} \approx \mathbf{H}\mathbf{P}_x\mathbf{x}_{\text{PCA}}. \tag{26}$$

Comparing (24) with (26), the PCA matrix

$$\mathbf{H}_{\text{PCA}} \approx \mathbf{H}\mathbf{P}_x \tag{27}$$

which indicates that $\mathbf{H}_{\text{PCA}}$ can be approximately expressed as the product of the original topology matrix $\mathbf{H}$ and $\mathbf{P}_x$. Based on $\mathbf{H}_{\text{PCA}}$, the proposed attack is formulated. Before that, the following theorem is introduced.

Theorem 1: The proposed attack using the $m \times 1$ attack vector

$$\mathbf{a}_{\text{PCA}} = \mathbf{H}_{\text{PCA}}\mathbf{c} \tag{28}$$

where $\mathbf{c}$ is an arbitrary $n \times 1$ nonzero vector, is almost stealthy when the PCA matrix $\mathbf{H}_{\text{PCA}}$ can be approximately written as the product of the original Jacobian matrix and another matrix, say $\mathbf{P}_x$, i.e., $\mathbf{H}_{\text{PCA}} \approx \mathbf{H}\mathbf{P}_x$ (see the Appendix B).

The phrase "almost stealthy" is used to emphasize that the residue is approximately the same as that without attack, which occurs because of (27), i.e., owing to the dimensionality reduction used to conform to the dimension of the original Jacobian matrix $\mathbf{H}$. The PCA matrix $\mathbf{H}_{\text{PCA}}$ is merely an approximation of $\tilde{\mathbf{P}}$.

The proposed algorithm is displayed in Algorithm 1. Based on $\mathbf{H}_{\text{PCA}}$ obtained using the PCA algorithm, the stealthy attack vector $\mathbf{z}_{a,\text{PCA}}$ is generated for the blind false data injection attack. One may ask whether an arbitrary $m \times n$ matrix, for example, $\mathbf{H}'$, can be expressed as the product of the Jacobian matrix $\mathbf{H}$ and another $n \times n$ matrix $\mathbf{P}'$, i.e., $\mathbf{H}' = \mathbf{H}\mathbf{P}'$. The answer is *no*, because $\mathbf{H}$ has the full column rank. On the contrary, if $\mathbf{H}$ has the full row rank, since $\mathbf{H}\mathbf{H}^+ = \mathbf{I}_{m\times m}$, $\mathbf{H}' = \mathbf{H}\mathbf{H}^+\mathbf{H}' = \mathbf{H}\mathbf{P}'$, where $\mathbf{P}' = \mathbf{H}^+\mathbf{H}'$. Hence, in this case, an arbitrary matrix can be expressed as the product of $\mathbf{H}$ and another matrix $\mathbf{P}'$, and can be used to generate undetectable attacks, which is certainly not the case in the considered scenario.

It should be noted that the expectation of residue $E[\mathbf{r}_{a,\text{PCA}}] = (\mathbf{H}_{\text{PCA}} - \mathbf{H}\mathbf{P}_x)\mathbf{c} \neq \mathbf{0}_{m\times 1}$, which depends on the value of $\mathbf{c}$ and the difference between $\mathbf{H}_{\text{PCA}}$ and $\mathbf{H}\mathbf{P}_x$. If $\mathbf{c}$ is an arbitrary vector, the smaller $(\mathbf{H}_{\text{PCA}} - \mathbf{H}\mathbf{P}_x)$, the more stealthy for the proposed attack. Additionally, the covariance matrix $\text{Cov}(\mathbf{r}_{a,\text{PCA}}) = (\mathbf{I} - \mathbf{G})\Sigma_v(\mathbf{I} - \mathbf{G})^T$, which is the same as the covariance of residue without any attack.

VI. Performance Analysis

The asymptotic cumulative distribution function (cdf) of the extreme value (9) of the residue $\mathbf{r}$, that is

$$r_{\max} = \max\{|r_1|, |r_2|, \ldots, |r_m|\} \tag{29}$$

has a function of the type [19]

$$F_{r_{\max}}(\gamma) = e^{-e^{-\alpha(\gamma-\beta)}} \tag{30}$$

where $F_{r_{\max}}(\gamma) = P(r_{\max} \leq \gamma)$ denotes the cdf of $r_{\max}$, $P(\cdot)$ denotes the probability, $e^{(\cdot)}$ denotes the exponential function, and α and β are parameters of the cdf. If statistical samples of $r_{\max}$ are available, then these parameters may be estimated so that the theoretical mean value and variance of the distribution match the sample mean and sample variance. To use this moment-matching method of parameter estimation, one needs expressions for the mean μ and variance σ^2 in terms of the parameters as

$$\begin{cases} \mu = \beta + \frac{0.577}{\alpha} \\ \sigma^2 = \frac{1.645}{\alpha^2}. \end{cases} \tag{31}$$

Based on μ and σ^2, α and β can be determined. Notably, the above cdf of the extreme value of the residue can be used for other unknown distributions of $\mathbf{v}$ supposed that the probability density of $\mathbf{v}$ decays in the upper tail as an exponential function. The upper tail of the Rayleigh distribution of $|r_i|$ actually decays as an exponential function.

Finally, based on the cdf, the probability of missed detection, $P_{\text{miss}} \equiv P(\max_i |r_i| < \gamma|\mathcal{H}_1)$, can be expressed as

$$P_{\text{miss}} = F_{r_{\max}}(\gamma) \tag{32}$$

where $P(\cdot|\mathcal{H}_1)$ denotes the probability of a random variable conditioned on $\mathcal{H}_1$.

VII. Performance Evaluation

Monte Carlo simulations are conducted to assess the performance of the proposed attack using different network topologies, which are obtained using MATPOWER [33]. The measurements consist of the power injection measurements at all buses and the power flows at all branches. First, the simulation results are conducted on the IEEE 14-Bus electrical grid model [34], as shown in Fig. 2. There are 54 measurements in the IEEE 14-Bus model. The impacts of measurement noise with zero mean Gaussian distribution are

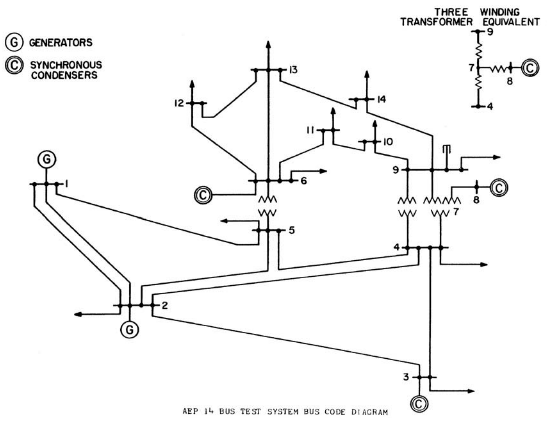
THREE WINDING TRANSFORMER EQUIVALENT
G GENERATORS
C SYNCHRONOUS CONDENSERS
1
2
3
4
5
6
7
8
9
10
11
12
13
14
AEP 14 BUS TEST SYSTEM BUS CODE DIAGRAM

Fig. 2. IEEE 14-Bus grid model [34].

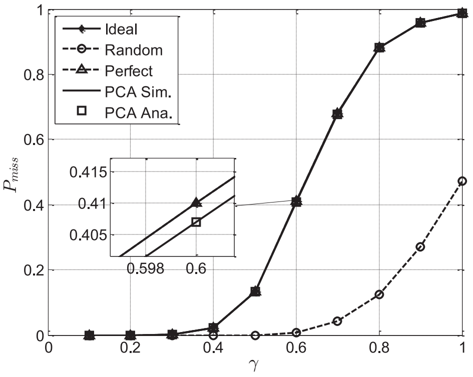

Fig. 3. Probability of missed detection P_{miss} versus the decision threshold γ for the ideal, perfect, random, and proposed PCA attacks (PCA Sim.) over IEEE 14-Bus grid model under the condition of uniform state variables. The analytical result (PCA Ana.) of the proposed PCA attack is also displayed.

also evaluated. The signal-to-measurement noise ratio is 10 dB. For the conventional false data injection attack, the state vector becomes $\mathbf{x}_a = \mathbf{x} + \mathbf{c}$, where the elements of $\mathbf{c}$ are randomly generated by a Gaussian random variable with variance σ_c^2. In this case, the signal-to-measurement noise ratio is defined as $10\log(\sigma_{x_a}^2/\sigma_v^2)$, where $\sigma_{x_a}^2 = \sigma_x^2 + \sigma_c^2$, $\sigma_{x_a}^2$ and σ_x^2 denote the variances of the elements of $\mathbf{x}_a$ and $\mathbf{x}$, respectively, and $10\log(\sigma_c^2/\sigma_x^2) = 3$ dB, i.e., the variance of the state vector contributed by the injected vector is assumed to be 3 dB higher than that contributed by the original measurement data. For other attacks, the signal-to-measurement noise ratio is similarly defined. If there is no false data, $\mathbf{c} = \mathbf{0}_{n\times 1}$ and $\sigma_c^2 = 0$; hence, the signal-to-measurement noise ratio $10\log(\sigma_{x_a}^2/\sigma_v^2) = 10\log(\sigma_x^2/\sigma_v^2)$. Because it is arguable to make any assumption about the distribution of state variables, the state variables of the electrical grids for the proposed attack can be any random variables with unknown distributions, including both independent Gaussian and non-Gaussian distributed random variables. Three kinds of state variable distribution are considered for the IEEE 14-Bus: 1) all are non-Gaussian; 2) all are Gaussian; and 3) mixing Gaussian and non-Gaussian. For fixed state variables during a period of time, the proposed method can also function very well, and hence, its simulation results are omitted here.

Fig. 3 plots the probability of missed detection, P_{miss}, over the IEEE 14-Bus grid model versus the decision threshold γ for the measurement without attacks (ideal), conventional attack with perfect knowledge of Jacobian matrix (perfect), random attack (random), and the proposed attack using the PCA approximation method (PCA Sim.). The state variables are all non-Gaussian and uniformly distributed. For other non-Gaussian random variables, similar results can be observed; therefore, they are omitted here for clarity. As shown, the random attack without taking the Jacobian matrix into consideration has the lowest P_{miss}; hence, it is not stealthy. As expected, the performance of the perfect attack coincides with that of the ideal condition; therefore, the perfect attack is indeed a stealthy and perfect attack. In addition, the performance of the proposed PCA attack can approach those of the ideal condition and perfect attack with perfect knowledge of Jacobian matrix, and has a much better performance than that of the random attack. Hence, the proposed attack is considered to be almost stealthy. Moreover, the theoretical result (PCA Ana.) matches the simulation result of the proposed method very well, which further confirms the advantages of the proposed attack.

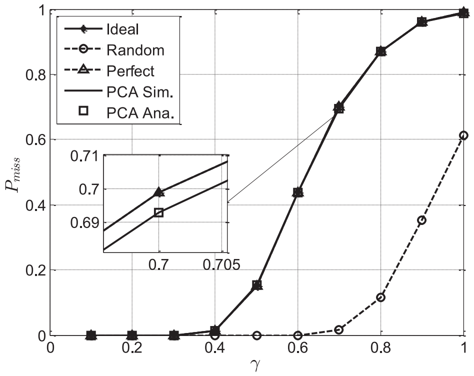

Fig. 4. Probability of missed detection P_{miss} versus the decision threshold γ for the ideal, perfect, random, and proposed PCA attacks (PCA Sim.) over IEEE 14-Bus grid model under the condition of all Gaussian state variables. The PCA Ana. is also displayed.

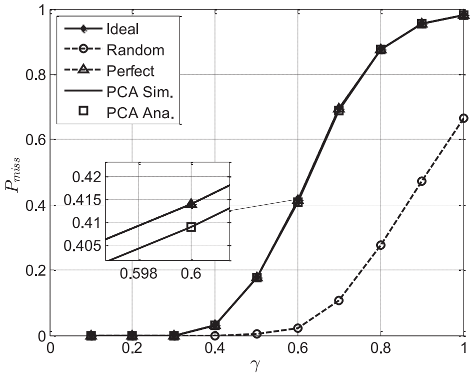

Fig. 5. Probability of missed detection P_{miss} versus the decision threshold γ for the ideal, perfect, random, and proposed PCA attacks (PCA Sim.) over IEEE 14-Bus grid model under the condition of mixing 50% Gaussian and 50% non-Gaussian state variables. The PCA Ana. is also displayed.

Fig. 4 plots the probability of missed detection, P_{miss}, versus the decision threshold γ for the ideal, perfect, random, and proposed PCA attacks over the IEEE 14-Bus grid model under the conditions of all Gaussian state variables, while the

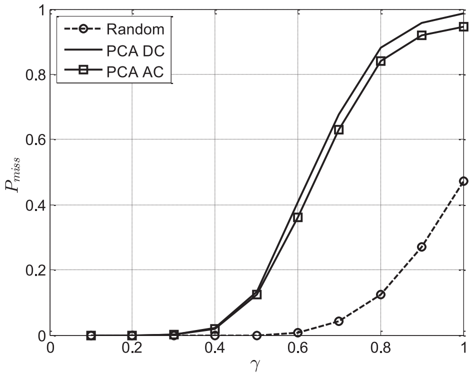

Fig. 6. Probability of missed detection P_{miss} versus the decision threshold γ for the random, proposed PCA attack using dc power flow model (PCA dc), and proposed PCA attack using ac power flow model (PCA ac) over IEEE 14-Bus grid model.

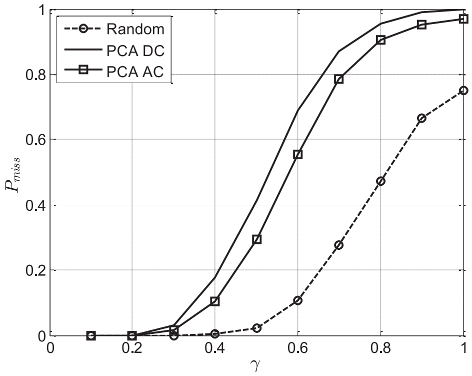

Fig. 7. Probability of missed detection P_{miss} versus the decision threshold γ for the random, PCA dc, and PCA ac over IEEE 300-Bus grid model.

state variable in Fig. 5 is mixing 50% Gaussian and 50% non-Gaussian random variables. As presented, the proposed PCA attack is robust to various distributions of state variables and its performance can still approach that of the ideal condition and perfect attack with perfect knowledge of Jacobian matrix. Besides, comparing Figs. 3–5, the performance of the proposed PCA attack is only slightly affected by the distributions of state variables.

Next, the simulation results are conducted on the IEEE 14-Bus and 300-Bus electrical grid models [34], as shown in Figs. 6 and 7, respectively. The IEEE 300-Bus model has 1122 meters. The state vector is typically correlated in power grids. Therefore, we use the data generated by MATPOWER which reflects a more realistic simulation environment. The attack vector is constructed based on the dc power flow model. Once constructed, the attack vector is added to the noisy measurements. Notice that the attack vector is designed based on the dc power flow model, which has only the real part of the measurements. As shown in these figures, the proposed method is also effective for the real data in large and small electric grids. To evaluate the effects of the nonlinearity of the PCA ac, as shown in Figs. 6 and 7, the performance of the PCA ac degrades owing to the introduced nonlinearity, but its performance is still better than that of the random attack. Compared to PCA dc, the performance of the PCA ac degrades more for a large system than a smaller one. However, to the best of our knowledge, the perfect attack for the ac power flow model has still not been developed in literature. In the case of correlated state vectors, the correlated state vector $\mathbf{x}$ can be projected to an independent vector $\mathbf{y}$ with $\mathbf{x} = \mathbf{D}\mathbf{y}$, where $\mathbf{D}$ is an $n \times n$ matrix and the eigenvectors of $\mathbf{x}$. Thus, the model becomes $\mathbf{z} = \mathbf{H}\mathbf{x} = \mathbf{H}\mathbf{D}\mathbf{y} = \mathbf{H}'\mathbf{y}$, where $\mathbf{H}' = \mathbf{H}\mathbf{D}$ denotes the Jacobian matrix used for the case of independent vectors. The PCA matrix becomes $\mathbf{H}_{\text{PCA}} \approx \mathbf{H}'\mathbf{P}_x$. Therefore, the proposed method can generally be applied for correlated state vectors.

VIII. Conclusion

Conventional false data injection attack assumes the explicit knowledge of the Jacobian topology matrix. Besides, it is arguable that the distribution of the state variables is Gaussian or not; therefore, this paper proposes a stealthy and blind attack without the knowledge of the Jacobian matrix and any assumption about the distribution of state variables. Additionally, the proposed method can also be applied for the real and fixed state variables. The performance of the proposed attack approaches those without attack and attack with perfect knowledge of Jacobian matrix. This type of new blind attacks opens a potential research direction, and deserves much attention to prevent the power grids from being masqueraded. Our future research direction will focus on the attacks constrained to a set of meters, limited resources, and specific states.

Appendix A
Proof of (25)

Ignoring measurement noise in (6) and equating it with (24) yield

$$\mathbf{z} = \mathbf{H}\mathbf{x} \approx \mathbf{H}_{\text{PCA}}\mathbf{x}_{\text{PCA}}. \tag{33}$$

Since, $\mathbf{H}$ has the full column rank

$$\mathbf{x} \approx \mathbf{H}^{+}\mathbf{H}_{\text{PCA}}\mathbf{x}_{\text{PCA}} \tag{34}$$

hence, $\mathbf{P}_x = \mathbf{H}^{+}\mathbf{H}_{\text{PCA}}$. The proof follows.

Appendix B
Proof of Theorem 2

Under the proposed attack, the new $m \times 1$ measurement vector $\mathbf{z}_{a,\text{PCA}} = \mathbf{z} + \mathbf{a}_{\text{PCA}}$ gives the state estimate $\hat{\mathbf{x}}_{a,\text{PCA}} = (\mathbf{H}^T\mathbf{W}\mathbf{H})^{-1}\mathbf{H}^T\mathbf{W}\mathbf{z}_{a,\text{PCA}} = \hat{\mathbf{x}} + \mathbf{P}_x\mathbf{c}$, where $\hat{\mathbf{x}}_{a,\text{PCA}}$ is a $n \times 1$ vector. Therefore, the residue of the proposed blind attack under the attack vector $\mathbf{z}_{a,\text{PCA}}$ is written as

$$\begin{aligned}\mathbf{r}_{a,\text{PCA}} &= \mathbf{z}_{a,\text{PCA}} - \mathbf{H}\hat{\mathbf{x}}_{a,\text{PCA}}\\ &= \mathbf{z} + \mathbf{a}_{\text{PCA}} - \mathbf{H}\left(\hat{\mathbf{x}} + \mathbf{P}_x\mathbf{c}\right)\\ &= \mathbf{z} - \mathbf{H}\hat{\mathbf{x}} + (\mathbf{a}_{\text{PCA}} - \mathbf{H}\mathbf{P}_x\mathbf{c})\\ &\approx \mathbf{z} - \mathbf{H}\hat{\mathbf{x}} + (\mathbf{a}_{\text{PCA}} - \mathbf{H}_{\text{PCA}}\mathbf{c})\\ &= \mathbf{z} - \mathbf{H}\hat{\mathbf{x}}.\end{aligned} \tag{35}$$

Therefore, the new attack is almost stealthy, because its residue is approximately the same as that without attack. The proof follows. ■

References

[1] A. Ipakchi and F. Albuyeh, "Grid of the future," *IEEE Power Energy Mag.*, vol. 7, no. 2, pp. 52–62, Mar. 2009.

[2] S. M. Amin and B. F. Wollenberg, "Toward a smart grid: Power delivery for the 21st century," *IEEE Power Energy Mag.*, vol. 3, no. 5, pp. 34–41, Sep. 2005.

[3] P. E. Marken *et al.*, "VFT—A smart transmission technology that is compatible with the existing and future grid," in *Proc. IEEE Power Syst. Conf. Expo. (PSCE)*, Seattle, WA, USA, Mar. 2009, pp. 1–7.

[4] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A survey on smart grid communication infrastructures: Motivations, requirements and challenges," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 1, pp. 5–20, Apr. 2013.

[5] K. Vu, M. M. Begouic, and D. Novosel, "Grids get smart protection and control," *IEEE Comput. Appl. Power,* vol. 10, no. 4, pp. 40–44, Oct. 1997.

[6] R. Ma, H. H. Chen, Y. R. Huang, and W. Meng, "Smart grid communication: Its challenges and opportunities," *IEEE Trans. Smart Grid,* vol. 4, no. 1, pp. 36–46, Mar. 2013.

[7] A. Bose and K. A. Clements, "Real-time modeling of power networks," *Proc. IEEE*, vol. 75, no. 12, pp. 1607–1622, Dec. 1987.

[8] O. Vuković and G. Dán, "Security of fully distributed power system state estimation: Detection and mitigation of data integrity attacks," *IEEE J. Sel. Areas Commun.,* vol. 32, no. 7, pp. 1500–1508, Jul. 2014.

[9] J. Kim, L. Tong, and R. J. Thomas, "Data framing attack on state estimation," *IEEE J. Sel. Areas Commun.,* vol. 32, no. 7, pp. 1460–1470, Jul. 2014.

[10] S. Bi and Y. J. Zhang, "Using covert topological information for defense against malicious attacks on DC state estimation," *IEEE J. Sel. Areas Commun.,* vol. 32, no. 7, pp. 1471–1485, Jul. 2014.

[11] A. Monticelli, "Electric power system state estimation," *Proc. IEEE*, vol. 88, no. 2, pp. 262–282, Feb. 2000.

[12] F. F. Wu, "Power system state estimation: A survey," *Int. J. Elect. Power Energy Syst.*, vol. 12, no. 2, pp. 80–87, Jan. 1990.

[13] L. Holten, A. Gjelsvik, S. Aam, and F. F. Wu, "Comparison of different methods for state estimation," *IEEE Trans. Power Syst.*, vol. 3, no. 4, pp. 1798–1806, Nov. 1988.

[14] B. Zhu, A. Joseph, and S. Sastry, "A taxonomy of cyber attacks on SCADA systems," in *Proc. IEEE Int. Conf. Internet Things, 4th Int. Conf. Cyber Phys. Social Comput. (iThings/CPSCom)*, Dalian, China, Oct. 2011, pp. 380–388.

[15] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," in *Proc. ACM Trans. Inf. Syst. Security*, vol. 14, no 1, pp. 1–12, Nov. 2009.

[16] M. A. Rahman and H. Mohsenian-Rad, "False data injection attacks with incomplete information against smart power grids," in *Proc. IEEE Glob. Commun. Conf.*, Anaheim, CA, USA, Dec. 2012, pp. 3153–3158.

[17] B. Stott and O. Alsac, "Fast decoupled load flow," *IEEE Trans. Power App. Syst.*, vol. PAS-93, no. 3, pp. 859–869, May 1974.

[18] P. D. P. Bickel *et al.*, *Principle Component Analysis: Springer Series in Statistics,* I. T. Jollifle, Ed. New York, NY, USA: Springer, 2002.

[19] E. Castillo, *Extreme Value Theory in Engineering*. New York, NY, USA: Academic Press, 1988.

[20] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A survey on cyber security for smart grid communications," *IEEE Commun. Surveys Tuts.,* vol. 14, no. 4, pp. 998–1010, Apr. 2012.

[21] S. Cui *et al*, "Coordinated data-injection attack and detection in the smart grid: A detailed look at enriching detection solutions," *IEEE Signal Process. Mag.*, vol. 29, no. 5, pp. 106–115, Sep. 2012.

[22] A. Tajer, "Energy grid state estimation under random and structured bad data," in *Proc. IEEE Sensor Array Multichannel Signal Process. Workshop (SAM)*, A Coruna, Spain, Jun. 2014, pp. 65–68.

[23] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Malicious data attacks on the smart grid," *IEEE Trans. Smart Grid,* vol. 2, no. 4, pp. 645–658, Dec. 2011.

[24] Q. Yang, J. Yang, W. Yu, N. Zhang, and W. Zhao, "On a hierarchical false data injection attack on power system state estimation," in *Proc. IEEE Glob. Commun. Conf. (Globecom)*, Houston, TX, USA, Dec. 2011, pp. 1–5.

[25] R. B. Bobba *et al.*, "Detecting false data injection attacks on DC state estimation," in *Proc. 1st IEEE Workshop Secure Control Syst. (CPSWEEK)*, Stockholm, Sweden, Apr. 2010, pp. 1–9.

[26] Y. Huang, H. Li, K. A. Campbell, and Z. Han, "Defending false data injection attack on smart grid network using adaptive CUSUM test," in *Proc. 45th IEEE Annu. Conf. Inf. Sci. Syst. (CISS)*, Baltimore, MD, USA, Mar. 2011, pp. 1–6.

[27] S. Bi and Y. J. Zhang, "Defending mechanisms against false-data injection attacks in the power system state estimation," in *Proc. IEEE GLOBECOM Workshops (GC Wkshps),* Houston, TX, USA, Dec. 2011, pp. 1162–1167.

[28] G. Hug and J. A. 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, Sep. 2012.

[29] K. R. Davis, K. L. Morrow, R. Bobba, and E. Heine, "Power flow cyber attacks and perturbation-based defense," in *Proc. IEEE Smart Grid Commun. (SmartGridCommun)*, Tainan, Taiwan, Nov. 2012, pp. 342–347.

[30] J. Casazza and F. Delea, *Understanding Electric Power Systems*. Hoboken, NJ, USA: Wiley, Feb. 2010.

[31] A. Wood and B. Wollenberg, *Power Generation, Operation, and Control,* 2nd ed. Hoboken, NJ, USA: Wiley, 1996.

[32] F. F. Wu and W. E. Liu, "Detection of topology errors by state estimation," *IEEE Trans. Power Syst.*, vol. 4, no. 1, pp. 176–183, Feb. 1989.

[33] R. D. Zimmerman, C. E. Murillo-Snchez, 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.

[34] (Feb. 17). *Power Systems Test Case Archive*. [Online]. Available: http://www.ee.washington.edu/research/pstca/

Zong-Han Yu, photograph and biography not available at the time of publication.

Wen-Long Chin received the B.S. degree in electronics engineering from National Chiao Tung University, Hsinchu, Taiwan, in 1994; the M.S. degree in electrical engineering from National Taiwan University, Taipei, Taiwan, in 1996; and the Ph.D. degree in electronics engineering from National Chiao Tung University, in 2008.

He was with Hsinchu Science Park, Hsinchu, for over 11 years, where he was in charge of communication and network integrated circuits designs. He is currently an Associate Professor with National Cheng Kung University, Tainan, Taiwan. His current research interests include application-specified integrated circuit design, and digital signal processing for communications and networking.