Detecting Stealthy False Data Injection Using Machine Learning in Smart Grid

Mohammad Esmalifalak, *Student Member, IEEE*, Lanchao Liu, *Student Member, IEEE*, Nam Nguyen, *Student Member, IEEE*, Rong Zheng, *Senior Member, IEEE*, and Zhu Han, *Fellow, IEEE*

***Abstract*—Aging power industries, together with the increase in demand from industrial and residential customers, are the main incentive for policy makers to define a road map to the next-generation power system called the smart grid. In the smart grid, the overall monitoring costs will be decreased, but at the same time, the risk of cyber attacks might be increased. Recently, a new type of attacks (called the stealth attack) has been introduced, which cannot be detected by the traditional bad data detection using state estimation. In this paper, we show how normal operations of power networks can be statistically distinguished from the case under stealthy attacks. We propose two machine-learning-based techniques for stealthy attack detection. The first method utilizes supervised learning over labeled data and trains a distributed support vector machine (SVM). The design of the distributed SVM is based on the alternating direction method of multipliers, which offers provable optimality and convergence rate. The second method requires no training data and detects the deviation in measurements. In both methods, principal component analysis is used to reduce the dimensionality of the data to be processed, which leads to lower computation complexities. The results of the proposed detection methods on IEEE standard test systems demonstrate the effectiveness of both schemes.**

***Index Terms*—Anomaly detection, bad data detection (BDD), power system state estimation, support vector machines (SVMs).**

I. Introduction

RECENTLY, the population growth on one hand and the increasing consumerism in many societies on the other hand have created major challenges for many industries such as the electric industry. Facing these challenges needs profound changes in traditional power systems and should consider the improvement in operational efficiencies and environmental compliance. Transition to smart grids opens enormous research opportunities such as improving the quality of monitoring with utilizing advanced communication infrastructure [1]–[3] and the integration of new types of energy resources such as wind energy and solar energy [4]–[6].

Conventionally, electricity is not storable in vast quantity, and as a result, the generation should follow the consumption of electricity closely. Any mismatch of generation and consumption will deviate the electrical quantities, such as the frequency and voltage levels in a power grid. Thus, control centers need to closely monitor the power network to make sure that the operation of the power system is safe and reliable. State estimation is an efficient way of online monitoring of states in power networks. To estimate the states of a network, the measured values of active power should be distributedly collected to a central state estimator using communication links. These measurements are collected via sensors installed in the transmission network (mainly on substations) and consist of transmitted active power and injected active power measurements. The estimated states will be the basis of corrective actions that the control center considers to keep the operation of the power grid in a safe mode.

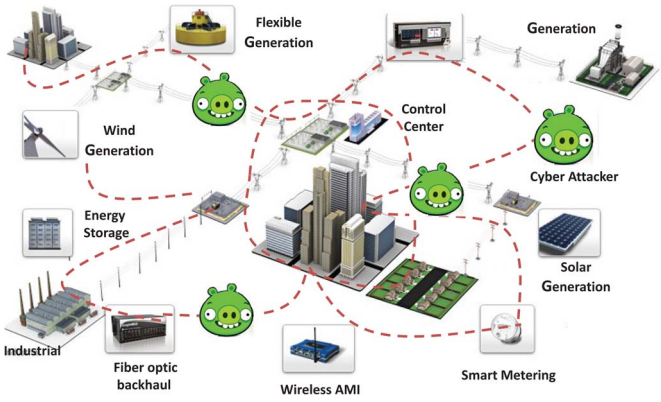


Fig. 1. Cyber threat in the smart grid.

Communication infrastructure links the critical power facilities together, but at the same time, it increases cyber security challenges (see Fig. 1 for cyber threats in the smart grid). The communication links used in state estimation can have potential cyber-attack risk. Different incentives may initiate a cyber attack in state estimators such as: 1) making financial benefits; 2) creating technical problems, such as blackouts, to the grid; and 3) a combination of financial benefits and technical problems. Analyzing the vulnerabilities in the state estimation (and, more generally, in the smart grid) gives the chance to control centers to improve the safety of operation through considering suitable countermeasures.

Unlike other communication networks, practically, the information exchange in the smart grid is more likely in one direction. For example, sending the information from measurements to the control center is usually in one direction (from the measurements to the control center). This characteristic gives

Manuscript received March 23, 2014; revised May 24, 2014 and June 29, 2014; accepted July 5, 2014. Date of publication August 20, 2014; date of current version September 27, 2017.

M. Esmalifalak, L. Liu, and Z. Han are with the Department of Electrical and Computer Engineering, Cullen College of Engineering, University of Houston, Houston, TX 77004 USA.

N. Nguyen is with Schlumberger Information Solutions, Houston, TX 77056 USA (e-mail: nnguyen8@slb.com).

R. Zheng is with the Department of Computing and Software and the Department of Electrical and Computer Engineering, Faculty of Engineering, McMaster University, Hamilton, ON L8S 4K1, Canada.

Digital Object Identifier 10.1109/JSYST.2014.2341597

priority to studying malicious user behaviors [7]–[12] versus studying the selfish behaviors [14]–[16] of users in the smart grid. A stealth attack is an example of a malicious behavior, and in this paper, we formulate and solve its detection based on signal processing and machine learning techniques. This type of attack bypasses the conventional bad data detection (BDD) methods and can create serious problems such as power system outages.[1] Although different methods have been used for BDD in power systems [7]–[13], to the best knowledge of the authors, this is the first paper that uses machine learning methods to detect stealthy false data injection. We devise two machine-learning-based techniques for stealthy attack detection. The first method utilizes supervised learning over labeled data and trains a support vector machine (SVM). The second method requires no training data and detects the deviation in measurements. In both methods, we first use principal component analysis (PCA) to project the data to a low-dimensional space. The key observation that motivates our solution approach is that normal data and tampered data (due to attacks) tend to be separated in the projected space. This is because the normal data are governed by physical laws, such as Kirchhoff's law, whereas the tampered data are not. Using the PCA also reduces the dimensionality of the data to be processed and thus leads to lower computation complexities. Simulation results demonstrate the effectiveness of the machine learning methods in the separation of the attacked and safe operation modes.

II. Literature Survey

The security of the smart grid is surveyed in [18] and [19]. The work in [18] reviews the cyber security for different parts of the smart grid, such as the process control system, the smart meter, the power system state estimation, and the smart-grid communication protocol. The work in [19] surveys malicious attacks in three different categories based on the smart-grid security objectives.

1) *Attacks targeting availability*. Attackers try to delay, block, or corrupt the communication in the smart grid (also called as denial-of-service attacks) [20], [21].
2) *Attacks targeting integrity*. An attacker attempts to illegally disrupt the data exchange [7]–[12].
3) *Attacks targeting confidentiality*. An attacker tries to get unauthorized information from network resources [22]–[24].

The challenges and opportunities of utilizing power networks with communication networks are described in [1]–[3]. False data may be due to unintended measurement abnormalities, topology errors, or injection by malicious attacks. An undetectable attack (a stealth attack) is introduced in [7], where it is shown how this type of false data pass the BDD in the control center. The works in [8] and [9] analyze the economical effect of false data injection on the transmission line congestion. The work in [10] shows that, although the structure of the power network is unknown, the attacker can first infer the structure and then use independent component analysis to launch a stealth attack. The work in [12] defines a security measure to quantify the hardness of performing attacks and describes an algorithm to compute this hardness. Liu *et al.* [13] used the low-rank structure of a power grid and the sparse nature of observable malicious attacks and formulated the false data detection problem as a low-rank matrix recovery and completion problem.

[1]This is indeed because of the inaccurate reactions of the control center in response to the faulty feedback through the faulty state estimation that it receives.

TABLE I
NOTATIONS

P_{ij}	Transmitted power from bus i to bus j
$\boldsymbol{\theta}$	$n \times 1$ vector of voltage angles
X_{ij}	Line reactance between bus i and bus j
$\mathbf{H}$	$m \times n$ Jacobian matrix
m	Number of measurements
n	Number of states (number of buses here)
$\mathbf{r}$	$m \times 1$ residue vector for BDD
γ	Residue threshold in BDD
$\boldsymbol{\Sigma}_e$	$m \times n$ covariance matrix of measurements' errors
$\mathbf{z}'$	$m \times 1$ attacked measurement vector
$\mathbf{Z_t}$	Measurement sets over m different time steps
$\mathbf{Z_{tr}}$	$m \times k$ reduced measurement matrix
$\boldsymbol{\omega}$	Support Vector Machine optimization parameter
$\mathbf{f^{(i)}}$	Similarity function for i^{th} sample
F_1	Metric for evaluating the performance of clustering algorithms
$\boldsymbol{\xi}$	Support Vector Machine optimization parameter
δ	Threshold for Anomaly Detection algorithm

The remainder of this paper is organized as follows. The system model is given in Section III. The false data injection and the stealthy false data injection are studied in Section III. The proposed machine learning techniques for false data detection are described in Section IV. Numerical results are given in Section V, and Section VI concludes this paper. Some important notations are listed in Table I.

III. System Model

In power systems, transmission lines are used to transfer generated power to consumers [25]. Theoretically, the transmitted complex power between bus i and bus j depends on the voltage difference between these two buses, and it is also a function of the impedance between these buses. In general, transmission lines have high reactance over resistance (i.e., the X/R ratio), and one can approximate the impedance of a transmission line with its reactance. The transmitted active power from bus i to bus j can be written as [26]

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

where V_i is the voltage magnitude, θ_i is the voltage phase angle in bus i, and X_{ij} is the reactance of the transmission line between bus i and bus j. In direct-current power flow studies, it is usually assumed that the voltage phase difference between two buses is small, and the amplitudes of voltages in buses are near to the unity. Therefore, further simplification gives a linear relation between the voltage phase angles and the lines' reactance as [27]

$$P_{ij} = \frac{\theta_i - \theta_j}{X_{ij}}. \tag{2}$$

The state-estimation problem is to estimate n phase angles θ_i by observing m real-time measurements. In power flow studies, the voltage phase angle θ_i of the reference bus is fixed and known; thus, only $n-1$ angles need to be estimated. We define the state vector as $\boldsymbol{\theta} = [\theta_1, \ldots, \theta_n]^T$.

The control center observes vector $\mathbf{z}$ for m active power measurements. These measurements could be either transmitted active power from bus i to bus $j(P_{ij})$ or injected active power to bus $i(\sum P_{ij})$. The observation can be described as follows:

$$\mathbf{z} = \mathbf{P}(\boldsymbol{\theta}) + \mathbf{e} \tag{3}$$

where $\mathbf{z} = [z_1, \ldots, z_m]^T$ is the vector of the measured active power in transmission lines, $\mathbf{P}(\boldsymbol{\theta})$ is the nonlinear relation between measurement $\mathbf{z}$ and state $\boldsymbol{\theta}$ that is the vector of n bus phase angles θ_i, and $\mathbf{e} = [e_1, \ldots, e_m]^T$ is the Gaussian measurement noise vector with covariant matrix $\boldsymbol{\Sigma}_e$.

Without loss of generality, the Jacobian matrix $\mathbf{H} \in \mathbb{R}^m$ at $\theta = 0$ is

$$\mathbf{H} = \left.\frac{\partial \mathbf{P}(\boldsymbol{\theta})}{\partial \boldsymbol{\theta}}\right|_{\boldsymbol{\theta}=\mathbf{0}}. \tag{4}$$

If the phase differences $(\theta_i - \theta_j)$ in (2) are small, the linear approximation model of (3) can be described as

$$\mathbf{z} = \mathbf{H}\boldsymbol{\theta} + \mathbf{e}. \tag{5}$$

We focus on the problems of identifying and mitigating the impact of malicious cyber attacks on the state estimation, as the state estimation plays a key role in connecting the measurements collected via the communication network and in controlling the physical operations in the smart grid. Next, we first study how to detect false data injection, and then, we explain the concept of stealth attacks.

A. Conventional BDD

Given power flow measurements $\mathbf{z}$, the estimated state vector $\hat{\boldsymbol{\theta}}$ can be computed as

$$\hat{\boldsymbol{\theta}} = \left(\mathbf{H}^T\boldsymbol{\Sigma}_e^{-1}\mathbf{H}\right)^{-1}\mathbf{H}^T\boldsymbol{\Sigma}_e^{-1}\mathbf{z} = \mathbf{M}\mathbf{z} \tag{6}$$

where $\mathbf{M} = \mathbf{H}(\mathbf{H}^T\boldsymbol{\Sigma}_e^{-1}\mathbf{H})^{-1}\mathbf{H}^T\boldsymbol{\Sigma}_e^{-1}$. Thus, residue vector $\mathbf{r}$ can be computed as the difference between the measured quality and the calculated value from the estimated state as $\mathbf{r} = \mathbf{z} - \mathbf{H}\hat{\boldsymbol{\theta}}$. Therefore, the expected value and the covariance of the residual are

$$E(\mathbf{r}) = \mathbf{0} \qquad \text{cov}(\mathbf{r}) = (\mathbf{I} - \mathbf{M})\boldsymbol{\Sigma}_e. \tag{7}$$

The false data detection due to faulty sensors and topological errors can be performed using a BDD, such as the threshold test proposed in [30]. Therefore, the hypothesis of not being attacked is accepted if we have

$$\max_i |r_i| \leq \gamma \tag{8}$$

where γ is the threshold, and r_i is the component of $\mathbf{r}$.

B. Stealth (Unobservable) Attack

From the discussion of the BDD, we observe that if the attacker has knowledge on topology $\mathbf{H}$, it can add $\delta\boldsymbol{\theta}$ to $\hat{\boldsymbol{\theta}}$ by changing the value of the measurement data as

$$\mathbf{z}' = \mathbf{H}(\boldsymbol{\theta} + \delta\boldsymbol{\theta}) + e. \tag{9}$$

In this case, the hypothesis test fails in detecting the attacker since $\max_i |r_i| \leq \gamma$ does not change, and indeed, the control center believes that the true state is $\boldsymbol{\theta} + \delta\boldsymbol{\theta}$. This is called the *stealthy false data injection* [7].

IV. Machine-Learning-Based BDD

In the previous section, we have showed that stealthy bad data can pass the traditional BDD. In this section, we devise two machine-learning-based techniques to detect stealthy attacks. The main motivation for this approach is that the normal data and the tampered data (due to attacks) tend to be separated in a certain projected space. When the class labels (normal versus tampered) are given in the historical data, we can train a classifier to identify attacks. On the other hand, when labels are not given, we will apply anomaly detection to identify the outliers as potential attacks. In both schemes, one main challenge is the curse of dimensionality, i.e., as the size of the power grid grows, the dimension of the measurement data grows, rendering a high computation complexity. We use the PCA to first reduce the dimension of measurements, and then, we apply the proposed classification/detection techniques. The PCA maps the data from the original domain to a new domain. The attacked data in the new domain are more handleable than those in the original domain because the data are not correlated anymore.

A. Preprocessing PCA

Most of the practical systems, such as power networks, have a complex structure; thus, understanding their behavior is very challenging in some cases. One interesting way of analyzing this behavior is to first use redundant measurements in the network and then use the PCA to extract the interest dynamics of the system. The PCA is a well-known method; therefore, we just briefly bring the concept and the formulation here. Mathematically, the PCA maps the data from an n-dimensional space to an r-dimensional space [see (12)], where $r \leqslant n$. The data in the new domain have two important properties: 1) the different dimensions of the data have no correlation anymore; and 2) the dimensions are ordered based on the importance of their information. The following equations are used to map the $m \times n$ measurement matrix $\mathbf{Z}_t$ to an $m \times r$ dimension matrix $\mathbf{Z}_{tr}$ [31]:

$$\eth = \frac{1}{m} \times \mathbf{Z_t^T} \times \mathbf{Z_t} \tag{10}$$

$$[\mathbf{U}, \mathbf{S}, \mathbf{V}] = \text{svd}(G) \tag{11}$$

$$\mathbf{Z_{tr}} = \mathbf{U}(:, 1:r)^T \times \mathbf{Z_t} \tag{12}$$

where $\mathbf{Z}_t = [\mathbf{z}^{(1)}, \ldots, \mathbf{z}^{(m)}]^T$ is the matrix containing the measurement sets over m different time steps. $\mathbf{S}$ is a diagonal matrix with nonnegative diagonal elements in a decreasing order. Matrices $\mathbf{U}$ and $\mathbf{V}$ are unitary matrices that satisfy

$\eth = \mathbf{USV}^T$. svd is a function for computing the singular value decomposition. S_{ii} is the eigenvalue of the ith feature, where the bigger S_{ii} is, the more information the ith feature has.[2] Indeed, in many correlated systems (such as power grids), only the first few components of S are significant. It is common to select the smallest value of r such that the following condition holds:

$$\frac{\sum_{i=1}^{r} S_{ii}}{\sum_{i=1}^{m} S_{ii}} \times 100 \geq \varepsilon \tag{13}$$

i.e., $\varepsilon\%$ of the variance is retained. After mapping the features to the low-dimensional space in (12), the control center can use efficient machine learning techniques to determine the boundary between the normal and tampered data.

To this end, we can observe that the PCA chooses the principal components that maximize the variance. This is a very important feature, which explains why with much less information (or number of dimensions) of the observations, the anomaly detection still performs well. The PCA not only retains all the signal variations but also maximizes the separation between the normal and anomaly operation points. This property is precious since it helps increase the attack detection property and explains why we choose the PCA to reduce the number of observation dimensions.

B. Detection Method 1: Anomaly Detection

In data mining, the data sets that are considerably different from the remainder of the data are called outliers or anomalies. Different types of anomaly detection methods have been proposed, such as the distance-based, model-based, and statistical-based methods [29]. In this paper, we use the statistical-based methods. We use metric $P(\mathbf{z})$ and a threshold δ, where $P(\mathbf{z})$ represents the statistical characteristics of the historical data. If $P(\mathbf{z}) \leq \delta$, then $\mathbf{z}$ statistically has low similarity to the remaining data. In this method, the hypothesis of anomaly is confirmed if $P(\mathbf{z}) \leq \delta$, and it is rejected if $P(\mathbf{z}) > \delta$. Threshold δ will be learnt by the historical data (Step 3 in Algorithm 1). Because of using the historical data to learn δ, this method, in some literature, is called the semisupervised learning method. We use the multivariate Gaussian distribution probability density function (pdf) as metric $P(\mathbf{z})$ as follows:

$$\begin{aligned}\mathbf{P}(\mathbf{Z};\boldsymbol{\mu},\boldsymbol{\Sigma}) &= \frac{1}{(2\pi)^{\frac{n}{2}}|\boldsymbol{\Sigma}|^{0.5}} \exp\left[-\frac{1}{2}(\mathbf{Z}-\boldsymbol{\mu})^T\boldsymbol{\Sigma}^{-1}(\mathbf{Z}-\boldsymbol{\mu})\right] \\ \boldsymbol{\mu} &= \frac{1}{m}\sum_{i=1}^{m}\mathbf{Z}^{(i)}; \\ \boldsymbol{\Sigma} &= \frac{1}{m}\sum_{i=1}^{m}\left(\mathbf{Z}^{(i)}-\boldsymbol{\mu}\right)\left(\mathbf{Z}^{(i)}-\boldsymbol{\mu}\right)^T\end{aligned} \tag{14}$$

where n is the number of features, m is the number of samples, and $P_i(z_i)$ is the pdf of feature i. Each feature z_i follows a certain distribution that should be fitted based on the historical data. It is worth mentioning that the assumption of independence for $\mathbf{Z}$ holds for the Gaussian distributed features because of using the PCA.[3] Algorithm 1 shows the basic procedure of the anomaly detection method.

In Step 1, the historical data will be collected. These data will be gathered from the supervisory control and data acquisition (SCADA) information in the control center. The collected historical data will be preprocessed and will be mapped to a low-dimensional space in Step 2. This will decrease the computational complexity without sacrificing accuracy [31]. In Step 3, a Gaussian density function will be fitted to the preprocessed data ($\mathbf{P}(\mathbf{Z})$). If the new operational points (the validation data set that has not been used in Step 3) are statistically not similar to the historical data, the value of $\mathbf{P}(\mathbf{Z}_{\text{val}})$ will be less than threshold δ. Step 4 defines the best possible δ using the labeled historical data. The new operating point will be tested in Step 5 to see how similar it is to the normal data.

Algorithm 1: Stealth false data detection using anomaly detection

1 Collect historical data from state estimator
$\mathbf{Z_t} = [\mathbf{z}^{(1)}, \ldots, \mathbf{z}^{(m)}]^T$,
2 Use PCA:
$\eth = \frac{1}{m} \times \mathbf{Z_t^T} \times \mathbf{Z_t}$;
$[\mathbf{U}, \mathbf{S}, \mathbf{V}] = svd(\eth)$;
$\mathbf{Z_{tr}} = \mathbf{U}(:, 1:k)^T \times \mathbf{Z_t}$;
3 Fit density function $\mathbf{P}(\mathbf{Z}; \boldsymbol{\mu}, \boldsymbol{\Sigma})$ to the historical data $\mathbf{Z_t}$ using (14);
4 Choose the best δ;
$\delta^{best} = 0,\ F_1^{best} = 0$,
for $\delta = min\mathbf{P}(\mathbf{Z_{val}}) : St : max\mathbf{P}(\mathbf{Z_{val}})$ **do**

$$\mathbf{Y_{pred}} = \begin{cases} \mathbf{Y_{pred}}(i) = 1, & \forall i, \quad P(Z_{val})(i) \leq \delta, \\ \mathbf{Y_{pred}}(i) = 0, & \forall i, \quad P(Z_{val})(i) > \delta, \end{cases}$$

$f_p = sum(\mathbf{Y_{pred}} == 1\ \&\ \mathbf{Y} == 0)$,
$t_p = sum(\mathbf{Y_{pred}} == 1\ \&\ \mathbf{Y} == 1)$,
$f_n = sum(\mathbf{Y_{pred}} == 0\ \&\ \mathbf{Y} == 1)$,
$t_n = sum(\mathbf{Y_{pred}} == 0\ \&\ \mathbf{Y} == 0)$,

$$F_1 = 2\frac{P_r \times R_e}{P_r + R_e}, \text{ where } \begin{cases} P_r = t_p/(t_p + f_p), \\ R_e = t_p/(t_p + f_n), \end{cases}$$

if $F_1 > F_1^{best}$ **then**
$F_1^{best} \leftarrow F_1\ \ \delta^{best} \leftarrow \delta$ exit
end
5 For the new operating point $\mathbf{Z^{new}}$

$$\text{If } P(\mathbf{Z^{new}}; \mu, \boldsymbol{\Sigma}) = \begin{cases} \leq \delta^{best} \dashrightarrow \mathbf{Z^{new}} & \text{is corrupted,} \\ > \delta^{best} \dashrightarrow \mathbf{Z^{new}} & \text{is normal.} \end{cases}$$

C. Detection Method 2: SVMs

In this section, a distributed SVM is proposed to detect stealthy false data injections. Generally, an SVM constructs a hyperplane or a set of hyperplanes used for classification and regression. Given a labeled training set $\mathcal{S} = (\mathbf{x}_l, y_l)$,

[2]Statistically, the direction with the highest variation is the most important direction because it can represent the best approximation of the data in lower dimensions (the direction with highest variation has the most important information among other directions inside the data).

[3]The PCA transforms a set of (possibly) correlated data into linearly uncorrelated data.

$l = 1, \ldots, L$ of size L, with $y_l \in \{1, -1\}$, the SVM can be obtained by solving

$$\min_{\boldsymbol{\omega}, \xi, b} \quad \frac{1}{2}\boldsymbol{\omega}^\top \boldsymbol{\omega} + C\sum_{i=l}^{L} \xi_l \tag{15}$$

$$\text{subject to} \quad y_i \left(\boldsymbol{\omega}^\top \phi(\mathbf{x}_l) + b\right) \geq 1 - \xi_l \tag{16}$$

$$\xi_l \geq 0, l = 1, \ldots, L \tag{17}$$

where $\phi(\mathbf{x}_l)$ is a nonlinear transformation that maps $\mathbf{x}_l$ in a higher dimensional space. The slack variable ξ_l accounts for nonlinearly separable training sets, and C is a tunable positive regularization parameter.

In order to obtain a distributed SVM, (15) can be rewritten as

$$\min_{\boldsymbol{\omega}_i, \xi_i, b_i} \quad \frac{1}{2}\sum_{i=1}^{N} \boldsymbol{\omega}_i^\top \boldsymbol{\omega}_i + C\sum_{i=1}^{N}\sum_{l=1}^{L} \xi_{il} \tag{18}$$

$$\text{subject to} \quad y_{il} \left(\boldsymbol{\omega}_i^\top \phi(\mathbf{x}_{il}) + b_i\right) \geq 1 - \xi_{il} \tag{19}$$

$$\xi_{il} \geq 0, \quad i = 1, \ldots, N; l = 1, \ldots, L \tag{20}$$

where N is the number of groups that work together to train the SVM, and $\boldsymbol{\omega}_i$ is the local optimization parameter for each group. By introducing a global variable $\mathbf{z}$, (18) can be reformulated as

$$\min_{\mathbf{z}, \boldsymbol{\omega}_i, \xi_i, b_i} \quad \frac{1}{2}\mathbf{z}^\top \mathbf{z} + C\sum_{i=1}^{N}\sum_{l=1}^{L} \xi_{il} \tag{21}$$

$$\text{subject to} \quad y_{il} \left(\boldsymbol{\omega}_i^\top \phi(\mathbf{x}_{il}) + b_i\right) \geq 1 - \xi_{il} \tag{22}$$

$$\xi_{il} \geq 0, \ \mathbf{z} = \boldsymbol{\omega}_i \tag{23}$$

$$i = 1, \ldots, N; \ l = 1, \ldots, L. \tag{24}$$

In order to solve (21) distributively, variables $\{\mathbf{z}, \boldsymbol{\omega}_i\}$, $i = 1, \ldots, N$ can be partitioned into two groups $\{\mathbf{z}\}$ and $\{\boldsymbol{\omega}_i\}$, $i = 1, \ldots, N$, and the alternating direction method of multipliers can be applied to solve it. Specifically, the scaled augmented Lagrangian function is expressed as

$$\mathcal{L}\{\mathbf{z}, \boldsymbol{\omega}_i, \xi_i, \rho, \boldsymbol{\mu}_i\} = \frac{1}{2}\mathbf{z}^\top \mathbf{z} + C\sum_{i=1}^{N}\sum_{l=1}^{L} \xi_{il} + \frac{\rho}{2}\|\boldsymbol{\omega}_i - \mathbf{z} + \boldsymbol{\mu}_i\|_2^2 \tag{25}$$

where ρ is the step size, and $\boldsymbol{\mu}_i$ is the scaled dual variable. At each iteration k, $\{\boldsymbol{\omega}_i\}$, $\{\mathbf{z}\}$, and $\boldsymbol{\mu}_i$ are updated as follows:

$$\boldsymbol{\omega}_i[k+1] = \arg\min_{\boldsymbol{\omega}_i, \xi_i, b_i} C\sum_{l=1}^{L} \xi_{il} + \frac{\rho}{2}\|\boldsymbol{\omega}_i - \mathbf{z}[k] + \boldsymbol{\mu}_i[k]\|_2^2 \tag{26}$$

$$\text{subject to} \quad y_{il} \left(\boldsymbol{\omega}_i^\top \phi(\mathbf{x}_{il}) + b_i\right) \geq 1 - \xi_{il} \tag{27}$$

$$\xi_{il} \geq 0, \quad l = 1, \ldots, L. \tag{28}$$

Note that the update process of $\boldsymbol{\omega}_i$ can be locally done at the ith group. Furthermore, it involves fitting an SVM to the local data with an offset in the quadratic regularization term, which can be easily solved with existing software such as LIBSVM [17]. Vector $\{\mathbf{z}\}$ is expressed as

$$\mathbf{z}[k+1] = \arg\min_{\mathbf{z}} \frac{1}{2}\mathbf{z}^\top \mathbf{z} + \frac{\rho}{2}\|\boldsymbol{\omega}_i[k+1] - \mathbf{z} + \boldsymbol{\mu}_i[k]\|_2^2 \tag{29}$$

which can be analytically solved as

$$z = \frac{N\rho}{\frac{1}{C} + N\rho}\left(\bar{\boldsymbol{\omega}}[k+1] + \bar{\boldsymbol{\mu}}[k]\right) \tag{30}$$

where $\bar{\boldsymbol{\omega}} = (1/N)\sum_{i=1}^{N} \boldsymbol{\omega}_i$, and $\bar{\boldsymbol{\mu}} = (1/N)\sum_{i=1}^{N} \boldsymbol{\mu}_i$. Finally, we update scaled dual variable $\boldsymbol{\mu}_i$ by

$$\boldsymbol{\mu}_i[k+1] = \boldsymbol{\mu}_i[k] + \boldsymbol{\omega}_i[k+1] - \mathbf{z}[k+1]. \tag{31}$$

Algorithm 2 describes the procedure to detect stealthy false data injection using the distributed SVM method. In Step 1, the historical data are prepared at each group. These data can be obtained from the control center or can be locally collected by each group. The local and global optimization parameters are initialized in Step 2. Step 3 consists of two parts, i.e., the local parameter update and the global parameter update. Local optimization parameter ω_i is obtained by solving optimization problem (26) under constraints (27) and (28). This can be implemented by existing software such as LIBSVM [17]. The global optimization parameter is optimized by (30), in which $\bar{\boldsymbol{\omega}}$ and $\bar{\boldsymbol{\mu}}$ can be obtained by in-network processing through messages that were only exchanged among neighboring groups. After the problem is solved and each group achieved the converged ω_i, the local and global optimization parameters, i.e., ω_i and z, respectively, are returned in Step 4.

Algorithm 2: Stealthy false data detection using the distributed SVM

1 Input: Historical data from the state estimator;
2 Initialize: $\{\mathbf{z}\}$, $\{\boldsymbol{\omega}_i\}$, $\boldsymbol{\mu}_i$, ρ, $k = 0$;
3 while not converged do
  $\{\boldsymbol{\omega}_i\}$-update, distributively at each computing node:
  $\boldsymbol{\omega}_i[k+1] = \arg\min_{\boldsymbol{\omega}_i, \xi_i, b_i} C\sum_{l=1}^{L} \xi_{il}$
  $+(\rho/2)\|\boldsymbol{\omega}_i - \mathbf{z}[k] + \boldsymbol{\mu}_i[k]\|_2^2$,
  subject to Constraints (27) and (28).

  $\{\mathbf{z}\}$-update:
  $z = (N\rho/((1/C) + N\rho))(\bar{\boldsymbol{\omega}}[k+1] + \bar{\boldsymbol{\mu}}[k])$
  $\boldsymbol{\mu}_i[k+1] = \boldsymbol{\mu}_i[k] + \boldsymbol{\omega}_i[k+1] - \mathbf{z}[k+1]$.
  Adjust penalty parameter ρ_i is necessary;
  $k = k + 1$;
  end while
4 return $\{\mathbf{z}\}, \{\boldsymbol{\omega}_i\}$;
  Output $\{\mathbf{z}\}, \{\boldsymbol{\omega}_i\}$;

V. Experimental Results

In this section, we evaluate the effect of machine-learning-based techniques on detecting a stealthy attack in the state estimation. We use the IEEE 118-bus test system. In order

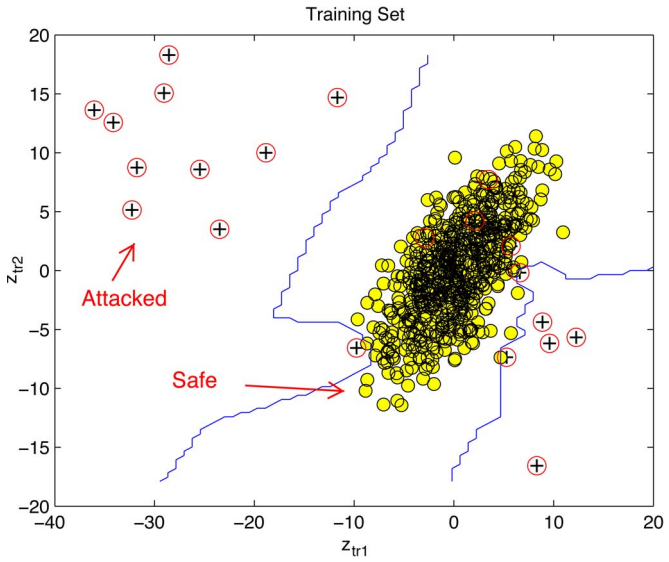


Fig. 2. Attacked and safe operating modes in the $\mathbb{R}^2$ space.

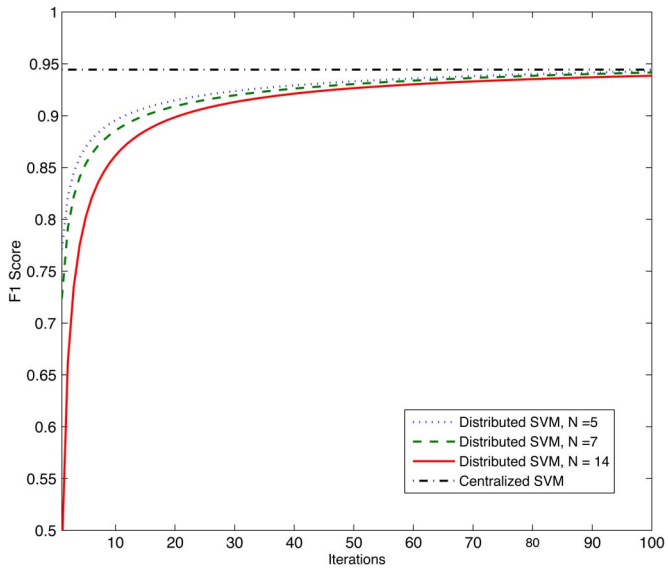


Fig. 3. Distributed SVM convergence.

to simulate a more realistic operation of the power system, we will use the stochastic loads in the network. Without loss of generality, these loads are considered to follow a uniform distribution in the range of $[0.9 \times L_0 - 1.1 \times L_0]$, where L_0 is the base load. The mean value of the load in a specific period of time is often considered L_0. Here, we use MATPOWER [32] to simulate the operation of the power network. In these simulations, active power measurements are collected from each transmission line. Thus, in the 118-bus case study, there are 304 measurement features (one feature per transmission line). These measurements will be considered inputs to the proposed algorithms. Due to the random nature of the load, the measurement vector varies over time. Using the Monte Carlo simulation, we have recorded the measurement vector in 1000 different instances.[4] As previously discussed, the measurement data are highly correlated; thus, the PCA is applied for dimension reduction. In the simulated data set, with only two principal components $(k = 2)$, 99% of the variance will be retained. Fig. 2 shows a 2-D plot of the principal components, where the circles represent the normal state, and the plus signs represent the attacked state. This figure demonstrates that a stealthy attack is separable in the control center.

A. SVM

In this paper, we use the Gaussian kernel for the following similarity function:

$$f_m^{(i)} = \exp\left(-\frac{\left\|\mathbf{z}_{tr}^{(i)} - \mathbf{l}^{(m)}\right\|^2}{2\sigma^2}\right) \tag{32}$$

where $\mathbf{l}^{(m)}$ is the mth landmark. The landmarks can be randomly placed in the historical data-set space. σ is another parameter that can be used for changing the complexity of the decision boundary. The optimal choice for σ in (32) and regularization parameter C in (15) can improve the efficiency of the SVM in detecting the attacked mode for the cross-validation set. In this paper, we have used 70% of the historical data as a learning data set and tested the accuracy of the fitted decision boundary on 30% of the remaining data sets called the cross-validation data sets. In order to define the optimal choice for σ and C, we vary both and choose the best σ and C, which correspond to the largest accuracy. In this paper, we use the F_1 score as the measure of accuracy, i.e.,

$$F_1 = 2\frac{P_r \times R_e}{P_r + R_e} \tag{33}$$

where P_r and R_e are called the precision and the recall, respectively, and they are calculated using the following equations:

$$P_r = \frac{\text{True Positive}}{\text{Predicted Positive}} \qquad R_e = \frac{\text{True Positive}}{\text{Actual Positive}}$$

where true positive corresponds to the points that the algorithm detects as positive samples, and they are indeed positive points. Predictive positives are the points that the algorithm detects as positive points, but they may have errors. Actual positives are all the positive points in the data sets. The F_1 score is no greater than 1, and the bigger the value of F_1, the more accurate the classifier is in general.

The convergence performance is shown in Fig. 3. It is shown that after a moderate number of iterations, the proposed distributed algorithm converges to the optimal values in different cases. In Fig. 3, we can see that, when the number of groups $N = 5$, the convergence rate is fastest. As the number of groups increases, the convergence rate slows down. This is mainly due to the increase in the communication overhead. Note that after very few iterations, the optimization result is very close to the optimal value, which means that the proposed algorithm is able to yield a good approximation to the optimal value in a short period of time.

[4]In the Pennsylvania, New Jersey, and Maryland (PJM) market, the control center collects the measured data in 1-min time intervals and runs the Siemens state-estimation program [33].

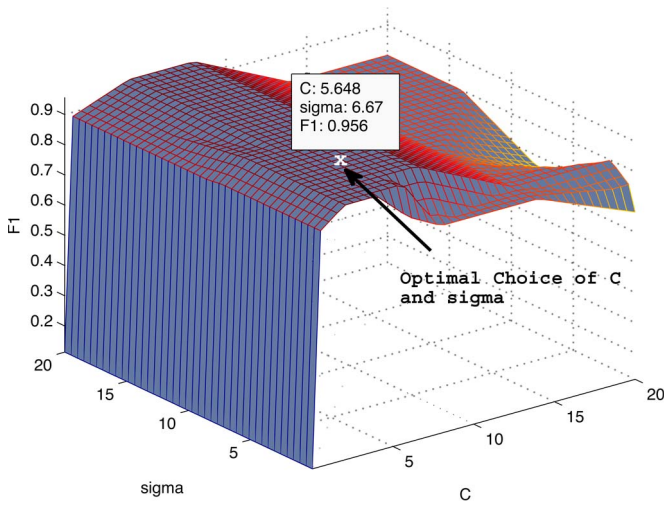


Fig. 4. Optimal Choice for C and σ.

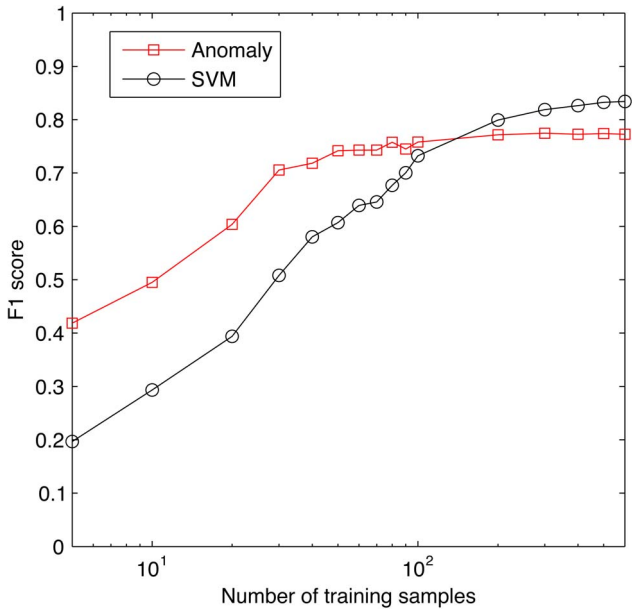


Fig. 5. Learning curve of the SVM and the anomaly detection.

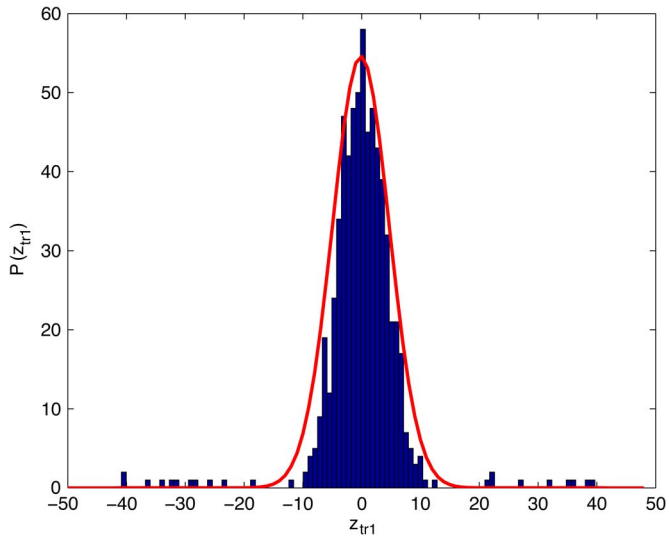


Fig. 6. Histogram representation of $\mathbf{z_{tr1}}$.

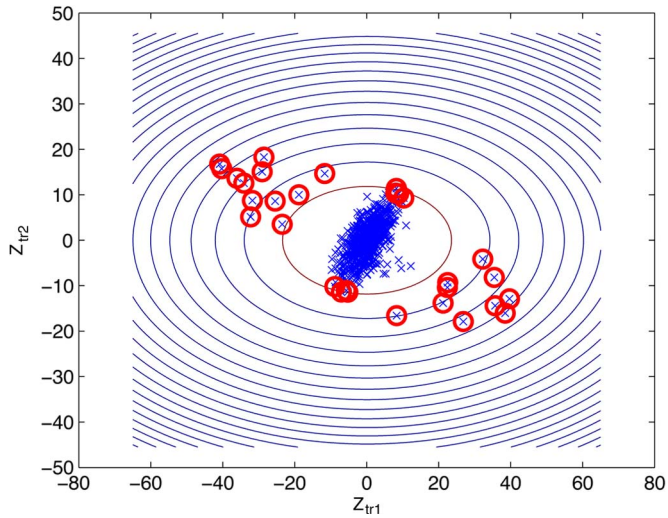


Fig. 7. Unsupervised anomaly detection with a large threshold $\delta(P(\mathbf{z}) < 2e-4)$.

To define the attacked and safe modes' boundary, we use a nonlinear classifier with a Gaussian kernel. Different values of C and σ have different effects on the clustering efficiency; hence, we train the SVM with different C and σ, and we compute F_1 for the cross-validation set. Following Algorithm 2, we define the best choice for C and σ. Fig. 4 shows the F_1 score for different values of C and σ. The efficiency of the learning algorithm can be improved by increasing the number of learning data. In order to analyze the effect of increasing the number of learning data on the detection performance, it is often useful to plot a learning curve. Fig. 5 compares the performance of the anomaly and SVM methods. This figure shows that, for fewer training data sets, the anomaly detection performs better than the SVM, but with a sufficient training data set, the SVM outperforms the anomaly detection. The plotted F_1 score is the average of F_1, which is obtained from 100 different data sets.

B. Anomaly Detection

After applying the PCA, the measurement data are mapped to points in 2-D. Fig. 6 shows the histogram of the first feature. We fit a Gaussian pdf to the features. The results of the anomaly detection on practical problems show that fitting the Gaussian density function for other data sets (which does not follow the Gaussian distribution) does not change the clustering efficiency drastically. Following the procedure given in Algorithm 1, the anomaly points can be detected by applying a threshold δ. The sensitivity of detecting a point as an anomaly depends on the magnitude of threshold δ. For larger values of δ, the algorithm is more sensitive and flags an anomaly for most of the operating points (see Fig. 7). For smaller values of δ, the algorithm is less sensitive and may lose detection of some of attacked points (see Fig. 8). In the semisupervised method, the output labels are used to learn the best threshold (see Fig. 9).

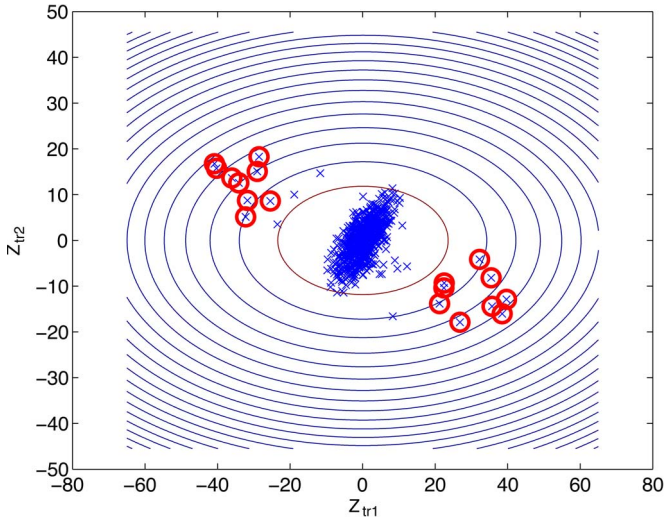


Fig. 8. Unsupervised anomaly detection with a small threshold $\delta(P(\mathbf{z}) < 2e-6)$.

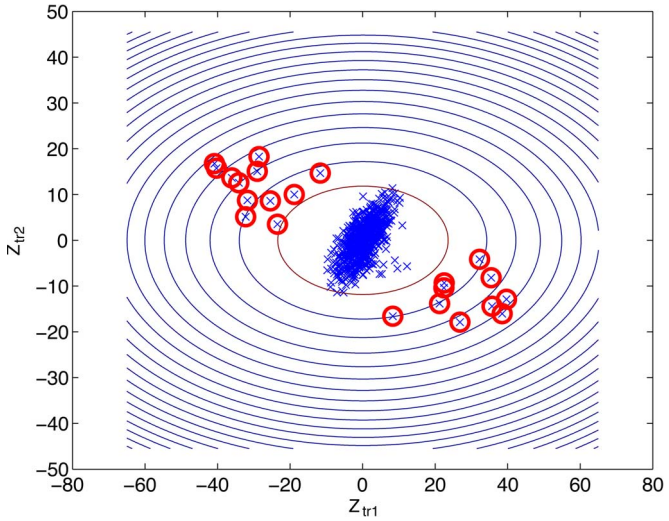


Fig. 9. Semisupervised anomaly detection with optimal threshold $(P(\mathbf{z}) < 2.98e-5)$

VI. Conclusion and Future Work

In this paper, first, we have collected the normal and stealthy attacked operating points in the state estimator. We use the collected data from the active power flow measurements in the network as the learning (historical) data. Projecting the historical data into a low-dimensional space shows that normal measurement data are well separated from the data under attack. This fact shows that the machine learning algorithms can be applied to detect the stealthy false data injection in the state estimator. We use both supervised and unsupervised learning methods to distinguish the attacked and safe operating modes. Numerical results show the effectiveness of the proposed algorithms in detecting the stealthy false data injection. Although we addressed stealthy bad data injection in this paper, there are several other failures that are not due to cyber attacks, such as transmission line and generator outages. This paper can be expanded in this direction to use other advanced machine learning and data mining methods to detect different types of anomalies in a power network.

References

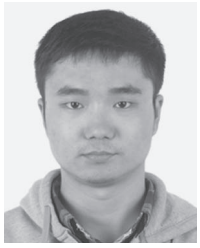
[1] V. C. Gungor and F. C. Lambert, "A survey on communication networks for electric system automation," *Comput. Netw., Int. J. Comput. Telecommun. Netw.*, vol. 50, no. 7, pp. 877–897, May 2006.
[2] W. Wang, Y. Xu, and M. Khanna, "A survey on the communication architectures in smart grid," *Comput. Netw.*, vol. 55, no. 15, pp. 3604–3629, Oct. 2011.
[3] T.-I. Choi, K. Y. Lee, D. R. Lee, and J. K. Ahn, "Communication system for distribution automation using CDMA," *IEEE Trans. Power Del.*, vol. 23, no. 2, pp. 650–656, Apr. 2008.
[4] C. W. Potter, A. Archambault, and K. Westrick, "Building a smarter smart grid through better renewable energy information," in *Proc. IEEE/PES PSCE*, Seatle, WA, USA, Mar. 2009, pp. 1–5.
[5] T. J. Hammons, "Integrating renewable energy sources into European grids," *Int. J. Elect. Power Energy Syst.*, vol. 30, no. 8, pp. 462–475, Oct. 2008.
[6] H. Farhangi, "The path of the smart grid," *IEEE Power Energy Mag.*, vol. 8, no. 1, pp. 18–28, Feb. 2010.
[7] Y. Liu, M. K. Reiter, and P. Ning, "False data injection attacks against state estimation in electric power grids," in *Proc. 16th ACM Conf. Comput. Commun. Security*, Chicago, IL, USA, Nov. 2009, pp. 21–32.
[8] 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.
[9] M. Esmalifalak, Z. Han, and L. Song, "Effect of stealthy bad data injection on network congestion in market based power system," in *Proc. IEEE WCNC*, Paris, France, Apr. 2010, pp. 2468–2472.
[10] M. Esmalifalak, H. Nguyen, R. Zheng, and Z. Han, "Stealth false data injection using independent component analysis in smart grid," in *Proc. IEEE 2nd Conf. Smart Grid Commun.*, Brussels, Belgium, Oct. 2011, pp. 244–248.
[11] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Malicious data attacks on smart grid state estimation: Attack strategies and countermeasures," in *Proc. 1st IEEE Int. Conf. SmartGridComm*, Nov. 2010, pp. 220–225.
[12] G. Dán and H. Sandberg, "Stealth attacks and protection schemes for state estimators in power systems," in *Proc. 1st IEEE Int. Conf. SmartGridComm*, Oct. 2010, pp. 214–219.
[13] L. Liu, M. Esmalifalak, Q. Ding, V. A. Emesih, and Z. Han, "Protection against false data injection attacks in power grids via sparsity and low rank," *IEEE Trans. Smart Grid*, vol. 5, no. 2, pp. 612–621, Mar. 2014.
[14] M. Cagalj, S. Ganeriwal, I. Aad, and J.-P. Hubaux, "On selfish behavior in CSMA/CA networks," in *Proc. 24th Annu. Joint Conf. IEEE Comput. Commun. Soc., INFOCOM*, Miami, FL, Mar. 2005.
[15] A. A. Cardenas, S. Radosavac, and J. S. Baras, "Performance comparison of detection schemes for MAC layer misbehavior," in *Proc. 26th IEEE INFOCOM*, Anchorage, AK, USA, May 2007, pp. 1496–1504.
[16] K. Pelechrinis, G. Yan, and S. Eidenbenz, "Detecting selfish exploitation of carrier sensing in 802.11 networks," in *Proc. 28th Annu. IEEE INFOCOM*, Rio de Janeiro, Brazil, Apr. 2009, pp. 857–665.
[17] C. C. Chang and C. J. Lin, LIBSVM: A library for support vector machines 2001, Software.
[18] T. Baumeister, "Literature Review on Smart Grid Cyber Security," Dec. 2010, Tech. Rep.
[19] W. Wang and Z. Lu, "Cyber security in the smart grid: Survey and challenges," *Comput. Netw.*, vol. 57, no. 5, pp. 1344–1371, Apr. 2013.
[20] D. Jin, D. M. Nicol, and G. Yan, "An event buffer flooding attack in DNP3 controlled SCADA systems," in *Proc. Winter Simul. Conf.*, Phoenix, AZ, USA, Dec. 2011, pp. 2614–2626.
[21] C. Popper, M. Strasser, and S. Capkun, "Jamming-resistant broadcast communication without shared keys," in *Proc. 18th USENIX Security Symp.*, Montreal, QC, Canada, Aug. 2009, pp. 231–248.
[22] K. Jain, "Security based on network topology against the wiretapping attack," *IEEE Wireless Commun.*, vol. 11, no. 1, pp. 68–71, Feb. 2004.
[23] H. Li, L. Lai, and W. Zhang, "Communication requirement for reliable and secure state estimation and control in smart grid," *IEEE Trans. Smart Grid*, vol. 2, no. 3, pp. 476–486, Sep. 2011.
[24] L. Sankar, S. Kar, R. Tandon, and H. V. Poor, "Competitive privacy in the smart grid: An information-theoretic approach," in *Proc. Conf. Smart Grid Commun.*, Brussels, Belgium, Oct. 2011, pp. 220–225.
[25] J. Casazza and F. Delea, *Understanding Electric Power Systems*. Hoboken, NJ, USA: Wiley, 2010, ser. IEEE Press Understanding Science and Technology Series.
[26] J. J. Grainger and W. D. Stevenson, Jr., *Power System Analysis*, vol. 621. New York, NY, USA: McGraw-Hill, 1994.
[27] A. J. Wood and B. F. Wollenberg, *Power Generation, Operation, Control*. New York, NY, USA: Wiley, 1996.

[28] N. Cristianini and J. S. Taylor, *An Introduction to Support Vector Machines and Other Kernel-Based Learning Methods*. Cambridge, U.K.: Cambridge Univ. Press.
[29] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection: A survey," *ACM Comput. Surveys*, vol. 41, no. 3, pp. 137–195, Jul. 2009.
[30] 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.
[31] I. T. Jolliffe, *Principal Component Analysis*. Hoboken, NJ, USA: Wiley, 2002.
[32] 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.
[33] A. L. Ott, "Experience with PJM market operation, system design, implementation," *IEEE Trans. Power Syst.*, vol. 18, no. 2, pp. 528–534, May 2003.

Mohammad Esmalifalak (S'12) received the M.S. degree in power system engineering from Shahrood University of Technology, Shahrood, Iran, in 2007 and the Ph.D. degree from the University of Houston, Houston, TX, USA, in 2010.

He is currently with the Department of Electrical and Computer Engineering, Cullen College of Engineering, University of Houston. His main research interests include the application of data mining, machine learning, and signal processing in the operation and expansion of smart grids.

Dr. Esmalifalak was the recipient of the Best Paper Award in the IEEE Wireless Communications and Networking Conference, Paris, France, in 2012.



Lanchao Liu (S'11) received the B.S. degree in electrical engineering from Huazhong University of Science and Technology, Wuhan, China, in 2010. He is currently working toward the Ph.D. degree in the Department of Electrical and Computer Engineering, Cullen College of Engineering, University of Houston, Houston, TX, USA.

His research interests include the theoretical and algorithmic studies in signal processing and mathematical optimization, distributed and parallel computing algorithms, compressive sensing theory, statistical learning and inference, and their applications in communications, networks, smart grids, and hyperspectral imaging.

Nam Nguyen (S'10) received the Bachelor of Science degree from the Hanoi University of Technology, Hanoi, Vietnam, in 2002; the Master of Science degree from the Southern Illinois University Edwardsville, Edwardsville, IL, USA, in 2008; and the Ph.D. degree in electrical and computer engineering from the University of Houston, Houston, TX, USA, on December 20, 2013.

Since February 2014, he has been a Data Analytics Scientist with Schlumberger Information Solutions, Houston, TX, USA. He is an expert in machine learning and statistics, particularly in nonparametric Bayesian classification techniques, Markov models, Dirichlet processes, and deep learning. His major interests include indoor localization, mobile users' behavior learning, location-based service, Long Term Evolution Direct, and wireless security.

Rong Zheng (S'03–M'04–SM'10) received the Ph.D. degree from the University of Illinois at Urbana–Champaign, Urbana, IL, USA, and the M.E. and B.E. degrees in electrical engineering from Tsinghua University, Beijing, China.

From 2004 to 2012, she was with the faculty of the Department of Computer Science, College of Natural Sciences and Mathematics, University of Houston, Houston, TX, USA. From August 2011 to January 2012, she was a Visiting Associate Professor with the Hong Kong Polytechnic University, Hung Hom, Hong Kong, and from February 2012 to May 2012, she was a Visiting Research Scientist with the Sensing and Energy Research Group, Microsoft Research, Redmond, WA, USA. She is currently with the Faculty of Engineering, McMaster University, Hamilton, ON, Canada, where she is currently a tenured Associate Professor with the Department of Computing and Software and an Associate Member of the Department of Electrical and Computer Engineering. Her research interests include network monitoring and diagnosis, cyber physical systems, and mobile computing.

Dr. R. Zheng serves on the technical program committees of leading networking conferences, including the IEEE Conference on Computer Communications (INFOCOM), the International Conference on Distributed Computing Systems, the IEEE International Conference on Network Protocols, etc. She served as a Guest Editor for the European Association for Signal Processing (EURASIP) *Journal on Advances in Signal Processing* Special Issue on wireless location estimation and tracking and for Elsevier *Computer Communications* Special Issue on Cyber–Physical Systems. She was a Program Cochair of the 2012 Wireless Algorithms, Systems, and Applications; the 2012 IEEE International Conference on Cyber, Physical and Social Computing (CPSComs); and MobileHealth 2014. She was the recipient of the National Science Foundation Faculty Early Career Development (CAREER) Award in 2006.

Zhu Han (S'01–M'04–SM'09–F'14) received the B.S. degree in electronic engineering from Tsinghua University, Beijing, China, in 1997 and the M.S. and Ph.D. degrees in electrical engineering from the University of Maryland, College Park, MD, USA, in 1999 and 2003, respectively.

From 2000 to 2002, he was a Research and Development Engineer with JDS Uniphase Corporation, Germantown, MD, USA. From 2003 to 2006, he was a Research Associate with the University of Maryland. From 2006 to 2008, he was an Assistant Professor with Boise State University, Boise, ID, USA. Currently, he is an Associate Professor with the Department of Electrical and Computer Engineering, Cullen College of Engineering, University of Houston, Houston, TX, USA. His research interests include wireless resource allocation and management, wireless communications and networking, game theory, wireless multimedia, security, and smart-grid communication.

Dr. Han has been an Associate Editor of the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS since 2010. He was the recipient of the IEEE Fred W. Ellersick Prize in 2011 and the National Science Foundation Faculty Early Career Development (CAREER) Award in 2010.