Strategic Protection Against Data Injection Attacks on Power Grids

Tùng T. Kim, *Member, IEEE*, and H. Vincent Poor, *Fellow, IEEE*

***Abstract*—Data injection attacks to manipulate system state estimators on power grids are considered. A unified formulation for the problem of constructing attacking vectors is developed for linearized measurement models. Based on this formulation, a new low-complexity attacking strategy is shown to significantly outperform naive ℓ_1 relaxation. It is demonstrated that it is possible to defend against malicious data injection if a small subset of measurements can be made immune to the attacks. However, selecting such subsets is a high-complexity combinatorial problem given the typically large size of electrical grids. To address the complexity issue, a fast greedy algorithm to select a subset of measurements to be protected is proposed. Another greedy algorithm that facilitates the placement of secure phasor measurement units (PMUs) to defend against data injection attacks is also developed. Simulations on the IEEE test systems demonstrate the benefits of the proposed algorithms.**

***Index Terms*—Bad data, cyberattack, phasor measurement units (PMUs), power grid security, sparse signal processing, system state estimation.**

I. Introduction

COORDINATED cyberattacks have been increasingly viewed as an imminent threat to modern electric grids. As supervisory control and data acquisition (SCADA) systems become more sophisticated and interconnected, the connection between the control networks and administrative ones as well as the Internet makes them more susceptible to intrusions. Hackers may have already infiltrated portions of the U.S. electric grids and have left malicious software behind, raising serious security concerns [1]. It was reported in August 2010 that a computer worm, the first known to specifically target SCADA systems, had been trying to infect thousands of computers worldwide [2]. Compromised control systems can cause very extensive damage not only to electric grids but also to other critical infrastructures.

At the heart of a monitoring and control system lies the critical task of state estimation. Keeping track of the current state of the system based on a set of measurements distributed over the power network is essential for maintaining stability and preventing disruption. Power system state estimation is a well established area of research. To determine gross errors that occasionally affect the measurements, statistical tests on the measurement residual are often used [3]. However, it is well known that if there are multiple bad measurements that are interacting and conforming, residual tests may not be able to identify the bad data [3].

It is not very likely for random phenomena such as measurement noises to cause simultaneous multiple bad data that can evade detection. However, the inability of conventional approaches to detect gross errors raises security concerns about intentional attacks on meters that can tamper with their measurements. The key observation from a recent work [4] is that under some mild conditions, synchronized data injection attacks on meters can successfully evade any detection schemes that are based on residual testing. Furthermore, the attacker may need to control only a few meters to launch a successful attack [4]. With the increasing deployment around the world of smart measurement devices, which may inherit some security issues of current computer networks, the vulnerability to malicious data injection attacks cannot be overstated.

In the present work, we develop a unified formulation for the problem of constructing an attacking vector under an optimization framework, taking into account constraints on the measurements and limited resources of the attacker. We also show that the proposed construction of attacking vectors in some previous work can be significantly improved. Built on the unified formulation, we develop a novel low-complexity attacking strategy, which is demonstrated to significantly outperform the naive ℓ_1 relaxation. This attacking strategy can be seen as the combination of analysis-based and synthesis-based ℓ_1 recovery problems [5], [6]. Our current work does not impose any additional assumptions on the underlying states, as required in some other work such as [7].

The sheer number of meters in electric grids makes it impractical to protect all of them. However, it is arguably plausible to protect a subset of the measurements, e.g., by a combination of encryption, continuous monitoring, separation from the Internet, etc. Given the typically very large size of electric grids, the complexity of selecting the key measurements to protect is a major issue. Even for a moderate-size network with a few hundred measurements, a brute force search over all possible small-size subsets is prohibitive.

In the current work, we propose a greedy algorithm that adds one measurement to the protected set at a time, which scales well with the network size. We also propose a fast algorithm that strategically places secure phasor measurement units (PMUs) at key buses in the network to defend against data injection attacks. The greedy nature of the proposed algorithms may facilitate

Manuscript received September 18, 2010; accepted February 14, 2011. Date of publication April 15, 2011; date of current version May 25, 2011. This research was supported in part by the National Science Foundation under Grant CNS-09-05398 and in part by DTRA under Grant HDTRA1-07-1-0037. Paper no. TSG-00133-2010.

The authors are with the Department of Electrical Engineering, Princeton University, Princeton, NJ 08544 (e-mail: thanhkim@princeton.edu; poor@princeton.edu).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TSG.2011.2119336

gradual upgrading of existing grids. Simulations on IEEE test systems illustrate the effectiveness of the proposed algorithms: Either protecting a small subset of existing measurements, or placing additional secure PMUs on a fraction of buses can force the attacker to seek control of significantly more meters to avoid being detected.

II. System Model and Formulation of the Attacking Problem

Consider the linearized measurement model of an electric network

$$\mathbf{z} = \mathbf{H}\boldsymbol{\theta} + \mathbf{n} \tag{1}$$

where $\mathbf{z} \in \mathbb{R}^M$ is the vector of measurements, $\mathbf{H}$ is the measurement Jacobian matrix of size $M \times N$, and $\mathbf{n}$ is the measurement noise [3]. The state vector $\boldsymbol{\theta}$ consists of the voltage phase angles at the buses. It is common to have $M > N$, so that the redundancy in the measurements provides some form of protection against bad data. No specific distribution on the state variables $\boldsymbol{\theta}$ is assumed.

It is assumed that an attacker having control over multiple meters can *inject* a vector $\mathbf{x}$ making the measurements become $\hat{\mathbf{z}} = \mathbf{z} + \mathbf{x}$ instead of the true measurements $\mathbf{z}$. It is shown in [4] that if there exists a $\mathbf{c} \in \mathbb{R}^N$ such that

$$\mathbf{x} = \mathbf{H}\mathbf{c}, \tag{2}$$

then this injection does not change the measurement residuals. In such cases, conventional statistical tests will not be able to detect the intruder. In the absence of measurement noise, the attacker would successfully trick the estimator into believing that the state vector is $\boldsymbol{\theta} + \mathbf{c}$. The attacking vector $\mathbf{x}$ can be quite sparse, and thus the attacker can be successful even with limited resources [4].

We assume that the system is able to securely protect a *subset* of measurements preventing any attacker from changing their values. For example, some of the measurements may be encrypted. The exact mechanism to protect the meters is beyond the scope of the present work. Due to cost and management difficulties, the number of measurements being protected is assumed to be limited. One of the main goals of this work is to develop fast methods to identify *which subset* of measurements needs protecting.

In [4] it is proposed to transform (2) by left-multiplying both sides of (2) with a projection matrix $\mathbf{P} = \mathbf{H}(\mathbf{H}^{\mathrm{T}}\mathbf{H})^{-1}\mathbf{H}^{\mathrm{T}}$, where $[\cdot]^{\mathrm{T}}$ denotes the transpose of a matrix, leading to

$$\mathbf{P}\mathbf{x} = \mathbf{x}. \tag{3}$$

Note that the projection matrix $\mathbf{P}$ is rank-deficient since the number of states N is in general (much) smaller than the number of measurements M. Therefore, for a *given* $\mathbf{c}$ the two equations (2) and (3) are not equivalent in general. For example, consider $\mathbf{P} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$. Then $\mathbf{P}\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \mathbf{P}\begin{bmatrix} y_1 \\ y_2 \end{bmatrix}$ does not imply $\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} y_1 \\ y_2 \end{bmatrix}$. Nevertheless, since it is only required that (2) holds for *some* $\mathbf{c}$, if (3) holds then one can *construct* $\mathbf{c} = (\mathbf{H}^{\mathrm{T}}\mathbf{H})^{-1}\mathbf{H}^{\mathrm{T}}\mathbf{x}$ that satisfies the detection-evading condition. In the current work, however, we will use (2) exclusively as it fits naturally into the unified formulation that we develop next.

In the following we develop a unified formulation of the problem faced by the attacker, taking into consideration both the limited resources of the attacker and the security constraints imposed by the system designer. We also introduce a new constraint to make the attack more "meaningful," which essentially requires that at least one element of the noiseless shift must be sufficiently large.

Let $\mathcal{S}$ denote the set of indices corresponding to the measurements that are protected, and let $\bar{\mathcal{S}}$ denote the complementary set of indices (i.e., those corresponding to the measurement that are unprotected). We define $N_{\mathrm{S}} = |\mathcal{S}|$, i.e., the cardinality of $\mathcal{S}$. The measurement constraint for the attacker can be expressed as

$$\mathbf{H}^{\mathcal{S}}\mathbf{c} = \mathbf{0}. \tag{4}$$

In the above we denote by $\mathbf{H}^{\mathcal{S}}$ the matrix formed by the N_{S} rows of $\mathbf{H}$ indicated by the indices in $\mathcal{S}$. Similarly we can define $\mathbf{H}^{\bar{\mathcal{S}}}$.

It is possible that this constraint makes the problem of choosing an attacking vector $\mathbf{c}$ *infeasible*. In particular, if we are able to protect a sufficiently large number of measurements $N_{\mathrm{S}} \geq N$ and furthermore $\mathrm{rank}\,(\mathbf{H}^{\mathcal{S}}) = N$ then the system of linear equations $\mathbf{H}^{\mathcal{S}}\mathbf{c} = \mathbf{0}$ is overdetermined and the only solution is $\mathbf{c} = \mathbf{0}$. In such cases, without having access to the protected meters, it is impossible for the attacker to find a nonzero $\mathbf{c}$ satisfying the condition (2). If the system is *observable*, then there exist N linearly independent measurements. By protecting these measurements, we are also guaranteed that the attacker cannot inject false data without affecting the residuals.

On the other hand, if $\mathrm{rank}\,(\mathbf{H}^{\mathcal{S}}) < N$ then there are infinitely many nonzero solutions $\mathbf{c}$ to $\mathbf{H}^{\mathcal{S}}\mathbf{c} = \mathbf{0}$. However, having a vector $\mathbf{c}$ at whose all elements are too small in magnitude is not of much interest for the attacker, as this would have an insignificant impact on the estimated state vector. Therefore, to make the attack "meaningful," the attacker further constrains that

$$\|\mathbf{c}\|_\infty \geq \tau \tag{5}$$

with some positive threshold τ. That is, the ℓ_∞ norm of the attacking vector $\mathbf{c}$ should be no smaller than τ. In other words, the noiseless shift caused by at least one of the elements of $\mathbf{c}$ must be larger than the threshold τ. Note that since the attacker can always scale a known solution of $\mathbf{H}^{\mathcal{S}}\mathbf{c} = \mathbf{0}$ by any constant to obtain another one, the condition (5) does *not* reduce the attacker's ability to find an attacking vector $\mathbf{c}$. It, however, makes the optimization framework that we develop next more rigorous.

To find the smallest number of meters it needs to tamper with and their corresponding indices, the attacker needs to solve the optimization problem

$$\begin{aligned} \min_{\mathbf{c}} \ & \|\mathbf{H}^{\bar{\mathcal{S}}}\mathbf{c}\|_0 \\ \text{s.t} \ & \mathbf{H}^{\mathcal{S}}\mathbf{c} = \mathbf{0}, \\ & \|\mathbf{c}\|_\infty \geq \tau \end{aligned} \tag{6}$$

for a given $\tau > 0$. In other words, the attacker wants to find the sparsest solution that satisfies all the constraints. We notice that without the extra constraint (5), the trivial optimizer to the

above optimization is $\mathbf{c}=\mathbf{0}$ and thus $\mathbf{x}^{\bar{\mathcal{S}}}=\mathbf{H}^{\bar{\mathcal{S}}}\mathbf{c}=\mathbf{0}$, i.e., the attacker should not attack the system!

Equivalently, the attacker can resort to solving a series of problems of the form

$$\min_{i\in\{1,\ldots,N\}}\ \min_{\mathbf{c}}\ \|\mathbf{H}^{\bar{\mathcal{S}}}\mathbf{c}\|_0 \quad \text{s.t}\quad \mathbf{H}^{\mathcal{S}}\mathbf{c}=\mathbf{0},\ |c_i|\geq\tau. \tag{7}$$

It needs to solve the inner minimization for each state $i=\{1,\ldots,N\}$ and then takes the minimum of the N solutions. Extension to the case in which the attacker wants to focus its attack on a subset of state variables can be obtained by performing the outer minimization over a subset of $\{1,\ldots,N\}$.

We now show that for all i, solving the inner minimization in (7) is equivalent to solving

$$\min_{\mathbf{c}}\ \|\mathbf{H}^{\bar{\mathcal{S}}}\mathbf{c}\|_0 \quad \text{s.t}\quad \mathbf{H}^{\mathcal{S}}\mathbf{c}=\mathbf{0},\ c_i=1. \tag{8}$$

First note that by a simple change of variables, the inner minimization in (7) becomes

$$\min_{\mathbf{c}}\ \|\mathbf{H}^{\bar{\mathcal{S}}}\mathbf{c}\|_0 \quad \text{s.t}\quad \mathbf{H}^{\mathcal{S}}\mathbf{c}=\mathbf{0},\ |c_i|\geq 1 \tag{9}$$

where we have used the fact that scaling by $\tau>0$ does not change the ℓ_0 norm. The last constraint of (9) is more relaxed than that of (8), so it suffices to show that the minimum of the objective function in (9) is not smaller than that of (8). If (9) is infeasible, then (8) is infeasible and there is nothing to prove. If (9) is feasible, let $\mathbf{c}^\star$ be the optimizer of (9). Since $|c_i^\star|\geq 1>0$, we can define $\bar{\mathbf{c}}^\star=(\mathbf{c}^\star)/(c_i^\star)$. Then $\bar{\mathbf{c}}^\star$ satisfies the constraints of (8) and furthermore $\|\mathbf{H}^{\bar{\mathcal{S}}}\mathbf{c}^\star\|_0=\|\mathbf{H}^{\bar{\mathcal{S}}}\bar{\mathbf{c}}^\star\|_0$, which concludes the proof of the claim.

Let $\mathbf{h}_i$ denote the ith column of $\mathbf{H}$ and $\mathbf{H}_i$ denote the $M\times(N-1)$ matrix formed by removing the ith column from $\mathbf{H}$. We further denote $\mathbf{c}_i\in\mathbb{R}^{N-1}$ as the vector formed by removing the ith component c_i of $\mathbf{c}$. We can rewrite (8) in the final form as

$$\min_{\mathbf{c}_i\in\mathbb{R}^{N-1}}\ \left\|\mathbf{H}_i^{\bar{\mathcal{S}}}\mathbf{c}_i+\mathbf{h}_i^{\bar{\mathcal{S}}}\right\|_0 \quad \text{s.t}\quad \mathbf{H}_i^{\mathcal{S}}\mathbf{c}_i+\mathbf{h}_i^{\mathcal{S}}=\mathbf{0}. \tag{10}$$

The attacker can also readily modify the above procedure to inject specific data into more than one state by introducing additional equality constraints on multiple c_i's. In particular, assume that the attacker wants to shift N_{T} specific states indicated by the set of indices $\mathcal{T}$ by the values $\mathbf{t}=[\,\tau_1\ \ \cdots\ \ \tau_{N_{\mathrm{T}}}\,]$. Let $\bar{\mathcal{T}}$ be the complementary set of indices, specifying the states in which the attacker has no interest. To find the least number of measurements to manipulate, the attacker needs to solve

$$\min_{\mathbf{c}\in\mathbb{R}^{N-N_{\mathrm{T}}}}\ \left\|\mathbf{H}_{\bar{\mathcal{T}}}^{\bar{\mathcal{S}}}\mathbf{c}+\mathbf{H}_{\mathcal{T}}^{\bar{\mathcal{S}}}\mathbf{t}\right\|_0 \quad \text{s.t}\quad \mathbf{H}_{\bar{\mathcal{T}}}^{\mathcal{S}}\mathbf{c}+\mathbf{H}_{\mathcal{T}}^{\mathcal{S}}\mathbf{t}=\mathbf{0}, \tag{11}$$

where $\mathbf{H}_{\mathcal{T}}^{\mathcal{S}}$ denotes the submatrix of $\mathbf{H}$ whose columns are indicated by $\mathcal{T}$ and rows are specified by $\mathcal{S}$, and other submatrices defined similarly. Clearly imposing additional constraints on specific attacking values leads to a less relaxed optimization (possibly even infeasible).

III. Attacker's Strategies

The major issue for the attacker is that finding sparse solutions is in general NP-hard [8]. It is well known, however, that optimizing the ℓ_1 norm helps promote sparsity, and thus a reasonable approach for the attacker is to find $\mathbf{c}_i$ that solves the convex relaxation of (10)

$$\min_{\mathbf{c}_i}\ \left\|\mathbf{H}_i^{\bar{\mathcal{S}}}\mathbf{c}_i+\mathbf{h}_i^{\bar{\mathcal{S}}}\right\|_1 \quad \text{s.t}\quad \mathbf{H}_i^{\mathcal{S}}\mathbf{c}_i+\mathbf{h}_i^{\mathcal{S}}=\mathbf{0}. \tag{12}$$

We refer to (12) as a naive ℓ_1-relaxation attack. It is worth pointing out that the relaxation from ℓ_0 to ℓ_1 does not change the constraints that make the attacker successfully evade detection: $\mathbf{H}_i^{\mathcal{S}}\mathbf{c}_i+\mathbf{h}_i^{\mathcal{S}}=\mathbf{0}$. The only suboptimality that the attacker may suffer is that the solution may not be the *sparsest*, i.e., there may exist other sets of indices to attack with smaller cardinality. The basis pursuit approach proposed in [4] is equivalent to the naive ℓ_1-relaxation (12).

The problem (12) is related to the *analysis-based* ℓ_1 recovery problem. In the case in which the rows of $\mathbf{H}_i^{\bar{\mathcal{S}}}$ do not form an orthonormal basis, a fact that holds in general, this problem has not been fully understood from an analytical viewpoint [5], [6].

Alternatively, one may expect that the shift vector $\mathbf{c}_i$ should also be sparse, as this implies few states being modified. As the matrix $\mathbf{H}$ is also very sparse in practice, a sparse $\mathbf{c}_i$ may also lead to a sparse $\mathbf{x}^{\bar{\mathcal{S}}}$. Thus the attacker can also try to find the sparsest $\mathbf{x}^{\bar{\mathcal{S}}}$ indirectly by solving

$$\min_{\mathbf{c}_i}\ \|\mathbf{c}_i\|_1 \quad \text{s.t}\quad \mathbf{H}_i^{\mathcal{S}}\mathbf{c}_i+\mathbf{h}_i^{\mathcal{S}}=\mathbf{0}. \tag{13}$$

This heuristic in fact is a form of *synthesis-based* ℓ_1 recovery, commonly encountered in the literature of compressed sensing [9]. The problem (13) is related but not equivalent to the original analysis-based problem [6].

Note that by introducing the variable $\mathbf{u}\geq\mathbf{0}$, where the vector inequality indicates *element-wise* inequalities, we can recast the optimization problem (12) as a linear program

$$\min_{\mathbf{c}_i,\mathbf{u}}\ \mathbf{1}^{\mathrm{T}}\mathbf{u} \quad \text{s.t}\quad \mathbf{H}_i^{\mathcal{S}}\mathbf{c}_i+\mathbf{h}_i^{\mathcal{S}}=\mathbf{0},\ \mathbf{u}\geq\mathbf{0},\quad \mathbf{u}\geq\mathbf{H}_i^{\bar{\mathcal{S}}}\mathbf{c}_i+\mathbf{h}_i^{\bar{\mathcal{S}}}\geq-\mathbf{u}, \tag{14}$$

where $\mathbf{1}$ is a vector of all ones. This linear program can then be solved efficiently, e.g., with interior point methods [10]. The same technique can be used in solving (13).

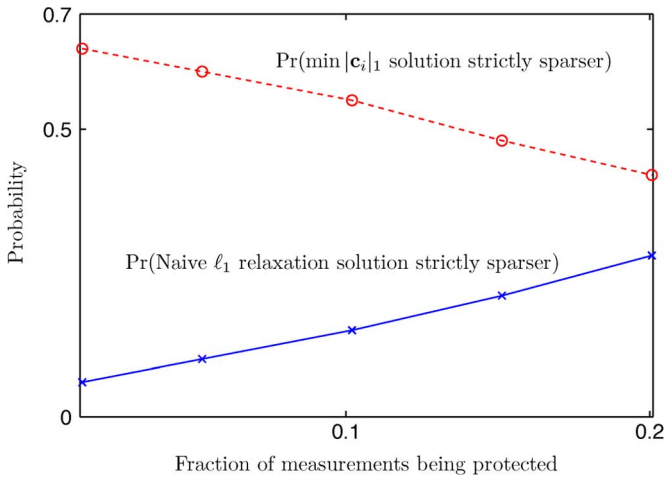

Fig. 1. Performance comparison of the naive ℓ_1 relaxation (12) and the synthesis-based heuristic (13) on the IEEE 118 bus system with different fractions of the meters being protected.

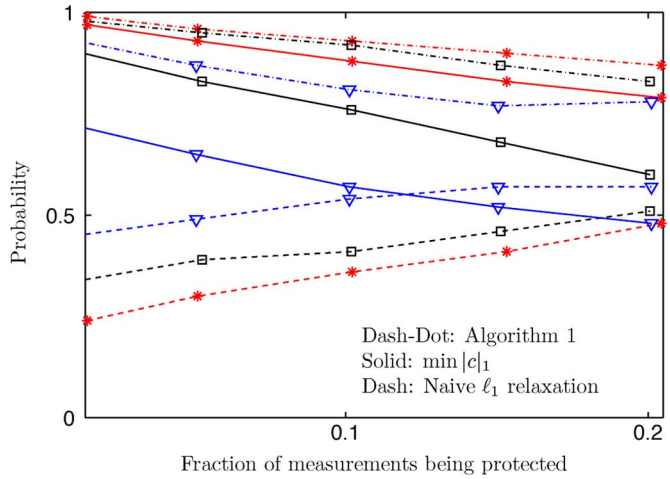

Fig. 2. Probabilities of finding the sparsest attacking vector among those obtained by three different attack schemes on three different IEEE test systems. Star: IEEE 57-bus, square: IEEE 118-bus, triangle: IEEE 300-bus.

Unfortunately analytical comparison of the analysis- and synthesis-based approaches is generally difficult to develop [5], [6]. Thus, *a priori* it is unclear which approaches are more beneficial for the attacker. To tentatively estimate the efficiency of (12) versus that of (13) in some relatively realistic scenarios, we simulated attacks on standard IEEE test systems, using 300 random sets $\mathcal{S}$ for each value of $|\mathcal{S}| = N_{\mathrm{S}}$ (further detail about numerical results will be provided in Section VI).

For example, in the IEEE 118-bus system plotted in Fig. 1, the attacking vector $\mathbf{x}$ obtained from (13) is *strictly* sparser than that obtained from (12) for 42%–64% of the time, while the vector obtained from (12) is strictly sparser for 6%–28% of the time only. Similar behavior is observed for other standard test systems. Thus despite its apparent suboptimality, using (13) does result in significant resource saving for the attacker, especially when the fraction of meters being protected $(N_{\mathrm{S}})/(N)$ is small.

These results motivate an attacking approach that combines *both* (12) and (13). The attacker first solves (13), to obtain an initial estimate of the sparse solution with superior performance. Then, it uses the *a priori* knowledge from the initial solution to solve a weighted optimization [6]

$$\begin{aligned} \min_{\mathbf{c}_i} \ & \left\| \mathrm{diag}\left(\mathbf{w}^i\right) \left(\mathbf{H}_i^{\bar{\mathcal{S}}} \mathbf{c}_i + \mathbf{h}_i^{\bar{\mathcal{S}}} \right) \right\|_1 \\ \text{s.t} \ & \mathbf{H}_i^{\mathcal{S}} \mathbf{c}_i + \mathbf{h}_i^{\mathcal{S}} = \mathbf{0}, \end{aligned} \tag{15}$$

where $\mathrm{diag}(\mathbf{w}^i)$ denotes a diagonal matrix whose diagonal entries are given by $\mathbf{w}^i \in \mathbb{R}^{M-N_{\mathrm{S}}}$. Note that with $\mathbf{w}^i = \mathbf{1}$, (15) reduces to (12). The attacker may incorporate *a priori* knowledge by the judicious choice of the weights $w_k^i = (1)/(|x_k^i| + \epsilon)$, $k = 1, \ldots, M - N_{\mathrm{S}}$, where the fixed $\epsilon > 0$ is to regularize division by (near) zero [6]. It can also try to improve the performance by repeating the process for multiple iterations. However, our numerical results suggest that there is little performance gain beyond a *single* inner iteration. The attacker's strategy is listed in Algorithm 1, where we omit the iteration index for readability.

Algorithm 1
An Attacker's Strategy

for $i = 1, \ldots, N$ **do**

Solve (13) to obtain the initial $\mathbf{c}_i$;

for a fixed number of iterations **do**

Compute $\mathbf{x}^i = \mathbf{H}_i^{\bar{\mathcal{S}}} \mathbf{c}_i + \mathbf{h}_i^{\bar{\mathcal{S}}}$;

Compute $w_k^i = (1)/(|x_k^i| + \epsilon)$, $k = 1, \ldots, M - N_{\mathrm{S}}$;

Solve the weighted problem (15) to obtain $\mathbf{c}_i$;

end for

end for

Instead of (13), the attacker can also try to use (12) to find the initial $\mathbf{c}_i$. Using (12) to initialize the algorithm is identical to the reweight approach in [6]. At least in the IEEE test systems, this provides very little improvement over using (12) alone. Intuitively, the re-weight algorithm depends on the initial solution (12), which, as demonstrated in Fig. 1, is generally not a very good estimate.

In Fig. 2, we numerically evaluate the performance of different attacking approaches on IEEE standard test systems. In particular, we apply three approaches: using (12) alone, using (13) alone, and using Algorithm 1. We plot in Fig. 2 the probability that each approach finds the sparsest solution *among* the three. Note that the truly sparsest solutions are unknown as they require solving the NP-hard problem (10). In all test systems, Algorithm 1 outperforms the naive ℓ_1 relaxation significantly. Even the simple heuristic (13) generally finds better solutions more frequently than does the naive approach (12), except for in the 300-bus system. When a large fraction of meters are protected, the performance of Algorithm 1 somewhat degrades and

it may be beneficial for the attacker to use *both* Algorithm 1 and the relaxation (12) and then to choose the resulting solution with smaller cardinality.

In any case, from the viewpoint of the attacker, finding the meters to inject bad data can be reduced to solving a series of linear programs. The attacker needs to know the matrix $\mathbf{H}$, which depends on the topology of the grid network, and the indices of the protected meters $\mathcal{S}$, which may simply reflect the measurements to which it does not have access.

On the other hand, from the point of view of a grid designer, the problem is much more complicated. If we want to implement some form of protection for $N_{\rm S}$ out of M measurements, the number of possible choices is $\binom{M}{N_{\rm S}}$. For example, in a moderate-size network with $M = 200$ measurements and with a small number of meters to be protected $N_{\rm S} = 20$, the number of all possible combinations is already more than 1.6×10^{27}. An exhaustive search for the optimal set of meters to be protected is clearly out of the question. In the next section, we present a systematic method with lower complexity to select the measurements to be protected.

IV. A Subset Selection Algorithm

It is very important to point out upfront that since we cannot emulate the optimal attack strategy (10), which is NP-hard, we need to *assume* the specific attacking strategies, e.g., the one described in Algorithm 1. This raises the possibility that the attacker may come up with some different schemes to find possibly sparser attacking vectors. The numerical results of any protection algorithm therefore should be interpreted with some care. Nevertheless, the algorithm described in this section can be readily modified if any better attacking strategies are discovered.

We first introduce some key notation. For $i = 1, \ldots, N$, let $\mathbf{c}_i^\star$ be the best *known* solution for the attack that modifies at least the ith state and $\mathbf{x}_i = \mathbf{H}_i^{\bar{\mathcal{S}}} \mathbf{c}_i^\star + \mathbf{h}_i^{\bar{\mathcal{S}}}$. Let $\mathbf{x}_i^\star \in \mathbb{R}^M$ be the vector whose elements indexed by $\bar{\mathcal{S}}$ are given by $\mathbf{x}_i$ and all other elements are zero, i.e., $\mathbf{x}_i^\star$ is the change in the measurements incurred by the attack. Let $N_{{\rm A}i} = \|\mathbf{x}_i^\star\|_0$, and $\mathcal{S}_i$ be the set of the indices of nonzero elements. We use the convention $N_{{\rm A}i} = \infty$ if the corresponding optimization problems are infeasible.

The goal of the system designer is to solve the subset selection problem

$$\min_{\mathcal{S}} |\mathcal{S}| \quad \text{s.t} \quad \min_{i \in \{1,\ldots,N\}} N_{{\rm A}i} \geq N_{\rm A} \tag{16}$$

where $N_{\rm A}$ is a positive integer. Recall that $|\mathcal{S}|$ denotes the cardinality of $\mathcal{S}$. Thus, an algorithm should search for the smallest number of measurements that need protecting so that the attacker will need to tamper with at least $N_{\rm A}$ meters to evade detection. This essentially prepares against the worst-case scenario, in which the attacker tries to influence the values of the most vulnerable state variables.

As observed above, a brute force search is clearly out of the question. Furthermore, beforehand we do not even know what the size of the set $\mathcal{S}$ is. We thus propose a greedy, suboptimal algorithm that adds one measurement into the set $\mathcal{S}$ at a time, until all the conditions $N_{{\rm A}i} \geq N_{\rm A}$ are met. The algorithm is presented as follows

Algorithm 2
Subset Selection

$\mathcal{S} = \emptyset$;
repeat
  $\text{MeasureArr}(\{1, \ldots, M\}) = 0$;
  for $i = 1$ to N **do**
    Find $\mathcal{S}_i$ and $N_{{\rm A}i}$;
    if $N_{{\rm A}i} < N_{\rm A}$ **then**
      $\text{MeasureArr}(\mathcal{S}_i) \Leftarrow \text{MeasureArr}(\mathcal{S}_i) + 1$;
    end if
  end for
  $k^\star = \arg\max_k \text{MeasureArr}(k)$;
  Add $k^\star$ to $\mathcal{S}$;
until $N_{{\rm A}i} \geq N_{\rm A}, \forall i$

At each iteration, the algorithm emulates attacks under the current security subset $\mathcal{S}$, which is initialized to be empty, assuming a specific attacking strategy. The key idea of the algorithm is that it maintains an array of counters, $MeasureArr$, counting the number of times that each measurement is manipulated by the attacker. We count only when $N_{{\rm A}i} < N_{\rm A}$, i.e., when the condition on the minimum number of measurements being attacked is not met. The algorithm then determines which measurement is modified the most and moves it to the protected set $\mathcal{S}$. The maximizer may not be unique. In such cases the algorithm chooses a random index among all the optimizers. Intuitively, the removal of this measurement forces the attacker to find other attacking solutions to the largest number of vulnerable states. The complexity order of the algorithm is equivalent to that of solving $N \times N_{\rm S}$ linear programs, as compared to solving $\binom{M}{N_{\rm S}}$ linear programs in the exhaustive search. Note that the proposed algorithm does not necessarily converge to a global optimum. In the numerical results, we run the algorithm several times for each $N_{\rm A}$ and choose the output $\mathcal{S}$ with the smallest cardinality.

V. A Secure PMU Placement Algorithm

In this section, as an alternative to providing protection for a subset of existing traditional measurements in power grids, we consider the placement of additional PMUs. By synchronizing to GPS time, PMUs have the capability of providing accurate synchronous phasor measurements for geographically dispersed nodes in power grids [11], [12]. The use of PMUs is considered to be one of the factors that can revolutionize future power systems. In the linearized measurement model that we consider, a PMU placed at a given bus can measure both the bus voltage angle and the power flows on several or all branches incident to that bus [13].

We assume that the measurements obtained by the PMUs are secure in the sense that they cannot be controlled by the attacker, a reasonable assumption since PMUs are sophisticated devices that can provide GPS time stamps on the measurement reports.

Again the exact mechanism to secure the PMUs is outside the scope of our current work. Since the high cost of PMUs is a major hindrance for large-scale deployment, the design problem is to find which buses on which to place the PMUs so that the number of PMUs is minimized, given a target N_{A}. Recall that N_{A} is the minimum number of conventional meters that the attacker needs to control to evade detection.

Under these assumptions, placing a PMU at a given bus is equivalent to moving all of the PMU measurements to the secure set $\mathcal{S}$. We notice that placing any PMU increases the number of rows of the Jacobian $\mathbf{H}$ as this provides additional secure measurements. Let $\mathbf{H}_k^{\mathrm{PMU}}$ be the Jacobian matrix corresponding to the measurements associated with a PMU placed at bus k, i.e., by placing a PMU at bus k we obtain the additional measurements $z_k^{\mathrm{PMU}} = \mathbf{H}_k^{\mathrm{PMU}}\boldsymbol{\theta}$ and thus the constraint (4) becomes

$$\begin{bmatrix} \mathbf{H}^{\mathcal{S}} \\ \mathbf{H}_k^{\mathrm{PMU}} \end{bmatrix} \mathbf{c} = \mathbf{0}. \tag{17}$$

As in the previous section, let $\mathbf{c}_i^\star$ be the best known solution to the attack that modifies at least the ith state and $\mathbf{x}_i^\star$ be the corresponding change in the measurements caused by this attack. If $\mathbf{H}_k^{\mathrm{PMU}}\mathbf{c}_i^\star = \mathbf{0}$ then adding a PMU at bus k does not provide any extra protection, since $\mathbf{c}_i^\star$ still satisfies (17). On the other hand, if $\mathbf{H}_k^{\mathrm{PMU}}\mathbf{c}_i^\star \neq \mathbf{0}$ then adding a PMU at the kth bus forces the attacker to find another solution. We are interested only in protecting the vulnerable states that have $N_{\mathrm{A}i} = \|\mathbf{x}_i^\star\|_0 < N_{\mathrm{A}}$, and thus we can count the immediate award of adding a PMU at bus k as

$$\sum_{i=1:N_{\mathrm{A}i}<N_{\mathrm{A}}}^{N} \mathbb{I}\left(\mathbf{H}_k^{\mathrm{PMU}}\mathbf{c}_i^\star \neq \mathbf{0}\right) \tag{18}$$

where $\mathbb{I}(\cdot)$ is the indicator function. We can then naturally develop a greedy algorithm that adds one PMU at a time, namely the one that can possibly help the most number of vulnerable states. The algorithm is listed as follows, where we omit the iteration index for the sake of brevity.

Algorithm 3
Secure PMU Placement

repeat

$\mathrm{PMUArr}(\{1,\ldots,N\}) = 0;$

for $i = 1$ to N **do**

Find $\mathbf{c}_i^\star$ and $N_{\mathrm{A}i}$;

if $N_{\mathrm{A}i} < N_{\mathrm{A}}$ **then**

$\mathrm{PMUArr}(k) \Leftarrow \mathrm{PMUArr}(k) + \mathbb{I}(\mathbf{H}_k^{\mathrm{PMU}}\mathbf{c}_i^\star \neq \mathbf{0})$, for $k = 1,\ldots,N$;

end if

end for

$k^\star = \arg\max_k \mathrm{PMUArr}(k);$

$\mathbf{H}^{\mathcal{S}} \Leftarrow \begin{bmatrix} \mathbf{H}^{\mathcal{S}} \\ \mathbf{H}_{k^\star}^{\mathrm{PMU}} \end{bmatrix};$

until $N_{\mathrm{A}i} \geq N_{\mathrm{A}}, \forall i$

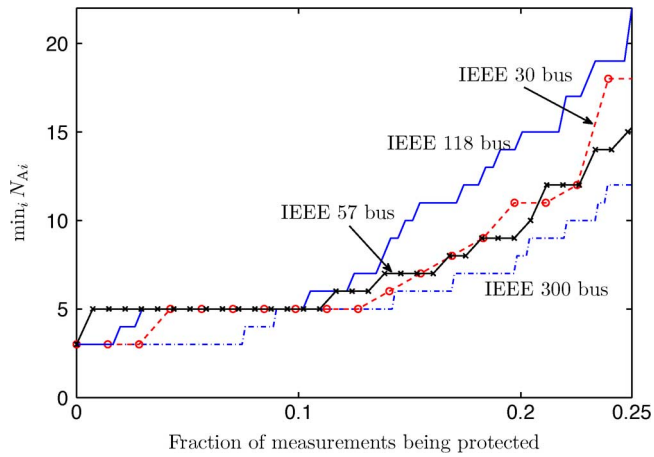

Fig. 3. The minimum number of measurements that the attacker needs to manipulate to evade detection as a function of the fraction of measurements being protected. The subsets to be protected are designed by Algorithm 2.

The idea behind this algorithm is in a way similar to that behind Algorithm 2. Instead of counting the number of times that an *existing* measurement is modified as in Algorithm 2, we count the number of times that adding a *new* set of secure measurements can help. Of course since we do not choose the PMUs jointly, there is no guarantee that the algorithm provides a globally optimal solution. The low complexity of the algorithm, which is on the order of that of solving $N \times N_{\mathrm{P}}$ linear programs with $N_{\mathrm{P}} \leq N$ being the total number of PMUs added, is again a major advantage.

VI. Numerical Results

To evaluate the design algorithms introduced above, we have performed simulations on the IEEE 30-bus, 57-bus, 118-bus and 300-bus test systems. The configuration data of the test systems is obtained from the MATPOWER package [14]. The measurements consist of the power injection measurements at all buses, and the real power flows at all branches. The purpose of using these configurations is to demonstrate the vulnerability of the networks even with high redundancy in the measurements. We use the CVX package [15] to solve the optimization problems in the design algorithms.

We first demonstrate the effectiveness of the subset selection Algorithm 2. In Fig. 3 we plot the minimum number of measurements that the attacker needs to manipulate in order to change at least one state variable without being detected as a function of the fraction of measurements being protected. The sets of protected measurements are designed by Algorithm 2. For each value of N_{A}, we run the algorithm three times.

As can be seen, all the test systems display a relatively similar behavior. At first it is fairly expensive to protect the systems, as the attacker needs to control only a few more meters to evade detection even if the designer can protect up to 10% of the measurements. Afterwards the cost of protection reduces significantly as indicated by the steeper slopes of the curves. For example by protecting 25% of the measurements on the IEEE 57-bus system, we can force the attacker to control at least 15 meters to succeed, a fivefold increase over not using any form of protection. The high cost of protection perhaps can be attributed to the fact that there typically is a large fraction of the states having very few associated measurements as illustrated in

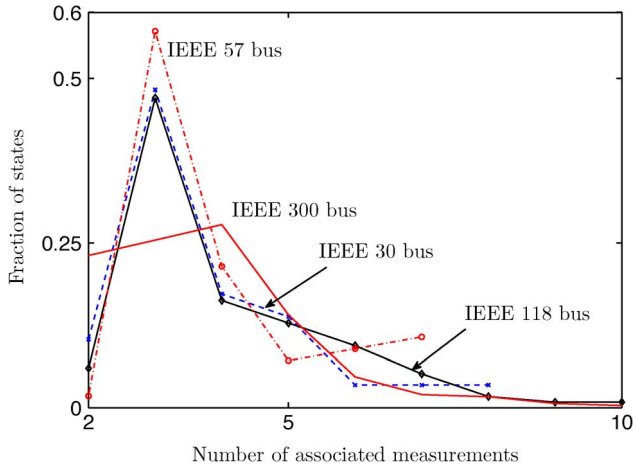

Fig. 4. The fraction of states as a function of the number of associated measurements for different test systems.

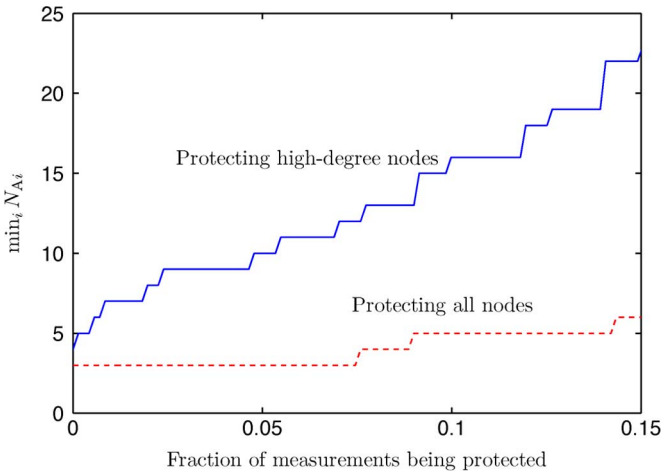

Fig. 5. Protection of buses with at least four incident branches in the IEEE 300-bus system.

Fig. 4. In other words, since electric grids are typically sparse, protecting one measurement can typically impact a few states only.

So far we can see that it is fairly expensive to provide even mild protection for *all* state variables. In some cases, however, the system operator may want to conserve the resources to protect important state variables. For example, the operator may want to focus on securing the states of the buses with high degrees, i.e., buses that have large numbers of incident branches, because the failure of one of those nodes has significant potential of causing cascading failure of the whole grid [16]. We demonstrate in Fig. 5 the selective protection of high-degree nodes on the IEEE 300 bus system. In particular we provide protection only for the buses that have at least four incident branches. As can be seen, it is much "cheaper" to protect these states: The attacker has to control significantly more meters even with a small fraction of the meters being protected. Thus, while the failure of high-degree nodes may have catastrophic consequences, the inherent redundancy in the measurements associated with such high-degree buses makes it difficult for data injection attacks on these buses to succeed.

In the next experiment, we consider the placement of secure PMUs by Algorithm 3. Before the placement of PMUs, none of the existing measurements in the grid is assumed to be secure.

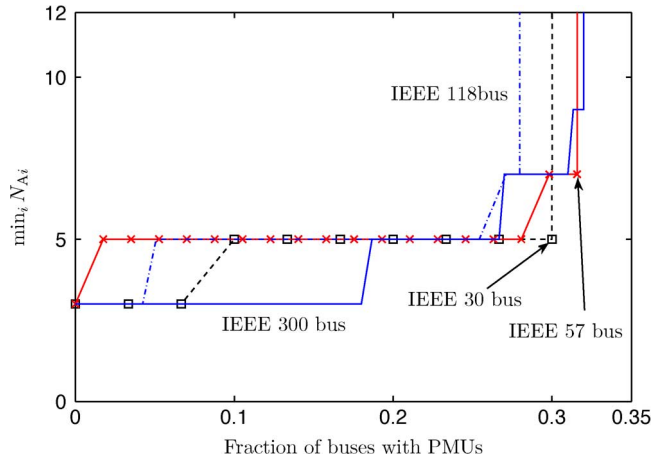

Fig. 6. The minimum number of meters that the attacker needs to manipulate to evade detection as a function of the fraction of buses having PMUs placed by Algorithm 3.

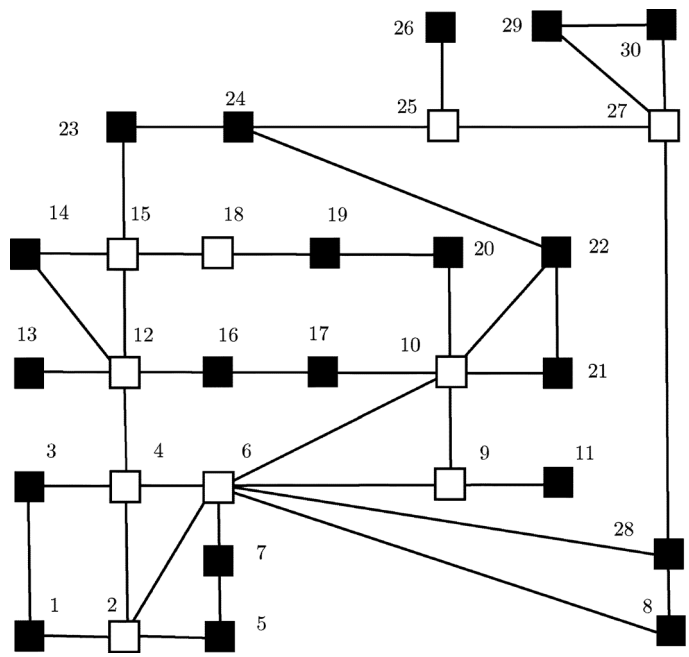

Fig. 7. The IEEE 30-bus test system as an undirected graph. The white nodes indicate the buses on which PMUs are placed by Algorithm 3 with any $N_A \geq 6$. The placement of these 10 secure PMUs make detection-evading data injection attacks infeasible.

In the simulations, we assume that a PMU placed at a given bus can provide the (secure) bus voltage angle as well as the power flow measurements of all branches incident to that bus. Note that our approach of using the matrices $\mathbf{H}_k^{\mathrm{PMU}}$ is very flexible and can handle any other measurement configurations.

In Fig. 6 we plot the minimum number of conventional measurements that the attacker needs to control to evade detection as a function of the fraction of buses having PMUs. Interestingly, the system behavior changes quite abruptly, in contrast with the gradual improvement obtained by protecting individual conventional measurements, cf. Fig. 3. At first placing PMUs on a small fraction of buses (i.e., setting a small target N_A in Algorithm 3) gives little improvement. However, when approximately $1/3$ of the buses have PMUs placed by Algorithm 3, it becomes infeasible for the attacker to inject data without changing the residual, i.e., $\min_i N_{Ai} = \infty$. Intuitively at this

threshold we have $\mathrm{rank}(\mathbf{H}^{\mathcal{S}}) = N$, and according to the observation in Section II the attacks become infeasible. Interestingly the threshold of 1/3 is consistent with earlier work on PMU placement that employed largely different techniques; see, e.g., [17]–[19].

As an example, in Fig. 7 we illustrate the IEEE 30-bus test system as an undirected graph in which nodes indicate buses and edges specify branches. Using any $N_{\mathrm{A}} \geq 6$ in Algorithm 3 gives the positions of the 10 secure PMUs indicated by the white nodes. The placement of these PMUs makes the grid completely secure from detection-evading data injection attacks.

VII. Conclusion

We have studied the problem of simultaneous attacks on multiple meters of electric grids to manipulate state estimation. We have formulated the attacking problem as a series of linear programs and introduced a constraint on the attacking vector to make the problem more meaningful. It has been demonstrated on the IEEE test systems that in many cases it is more economical for the attacker to use an indirect method that seeks to minimize the number of states affected than to use a direct ℓ_1 relaxation approach.

Assuming that a small subset of measurements can be made immune against these attacks, we have proposed a low-complexity algorithm to identify the key measurements to be protected. We have shown that by protecting these key measurements, which constitute a small fraction of the total measurements, we can make the minimum number of meters that the attacker has to control several times higher than that without protection. Finally, we have proposed a versatile algorithm that places secure PMUs on strategic buses in the network, which has low complexity and is capable of handling different types of PMU measurements.

Overall, the proposed algorithms allow system operators to focus their limited resources on a small part of a large-scale power grid, reducing costs and improving manageability. The greedy nature of these algorithms may also facilitate the *gradual* upgrades of existing networks. Possible future work includes finding explicit mechanisms to secure some of the measurements, developing possibly more efficient attacking strategies, and seeking computable upper bounds to better evaluate the performance of the design algorithms.

References

[1] S. Gorman, "Electricity grid in U.S. penetrated by spies," *Wall St. J.*, p. A1, Apr. 8, 2009.

[2] L. C. Baldor, "New threat: Hackers look to take over power plants," Aug. 3, 2010 [Online]. Available: http://abcnews.go.com/Business/wireStory?id=11316203

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

[4] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," in *Proc. ACM Conf. Comput. Commun. Security*, Chicago, IL, Nov. 2009, pp. 21–32.

[5] M. Elad, P. Milanfar, and R. Rubinstein, "Analysis versus synthesis in signal priors," *Inverse Probl.*, vol. 23, pp. 947–968, Jun. 2007.

[6] E. J. Candes, M. B. Wakin, and S. Boyd, "Enhancing sparsity by reweighted l1 minimization," *J. Fourier Anal. Appl.*, vol. 14, pp. 877–905, Dec. 2008.

[7] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Limiting false data attacks on power system state estimation," in *Proc. Conf. Inf. Sci. Syst.*, Princeton, NJ, Mar. 2010, pp. 1–7.

[8] E. J. Candes and T. Tao, "Decoding by linear programming," *IEEE Trans. Inf. Theory*, vol. 51, pp. 4203–4215, Dec. 2005.

[9] D. L. Donoho, "Compressed sensing," *IEEE Trans. Inf. Theory*, vol. 52, pp. 1289–1306, Apr. 2006.

[10] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge, U.K.: Cambridge Univ. Press, 2004.

[11] J. De La Ree, V. Centeno, J. S. Thorp, and A. G. Phadke, "Synchronized phasor measurement applications in power systems," *IEEE Trans. Smart Grid*, vol. 1, pp. 20–27, Jun. 2010.

[12] A. G. Phadke, "Synchronized phasor measurements in power systems," *IEEE Comput. Appl. Power*, vol. 6, pp. 10–15, Apr. 1993.

[13] J. Chen and A. Abur, "Placement of PMUs to enable bad data detection in state estimation," *IEEE Trans. Power Syst.*, vol. 21, pp. 1608–1615, Nov. 2006.

[14] R. D. Zimmerman, C. E. Murillo-Sánchez, and R. J. Thomas, "MATPOWER's extensible optimal power flow architecture," in *Proc. IEEE Power Energy Soc. Gen. Meet.*, Calgary, AB, Jul. 2009, pp. 1–7.

[15] M. Grant and S. Boyd, "CVX: Matlab software for disciplined convex programming, version 1.21," Aug. 2010 [Online]. Available: http://cvxr.com/cvx

[16] A. E. Motter and Y.-C. Lai, "Cascade-based attacks on complex networks," *Phys. Rev. E*, vol. 66, p. 065102, Dec. 2002.

[17] T. Baldwin, L. Mili, M. Boisen, Jr., and R. Adapa, "Power system observability with minimal phasor measurement placement," *IEEE Trans. Power Syst.*, vol. 8, pp. 707–715, May 1993.

[18] R. F. Nuqui and A. G. Phadke, "Phasor measurement unit placement techniques for complete and incomplete observability," *IEEE Trans. Power Del.*, vol. 20, pp. 2381–2388, Oct. 2005.

[19] B. Xu and A. Abur, "Observability analysis and measurement placement for systems with PMUs," in *Proc. IEEE Power Eng. Soc. Power Syst. Conf. Expo.*, New York, Oct. 2004, pp. 943–946.

Tùng T. Kim (S'04–M'08) received the B.Eng. degree in electronics and telecommunications from Hanoi University of Technology, Hanoi, Vietnam, in 2001, and the M.S. and Ph.D. degrees in electrical engineering from the Royal Institute of Technology (KTH), Stockholm, Sweden, in 2004 and 2008, respectively.

He held visiting positions at the University of Southern California, Los Angeles, CA in 2007, and at the University of Cambridge, Cambridge, U.K., in 2008. He is currently a Postdoctoral Research Associate with the Department of Electrical Engineering, Princeton University, Princeton, NJ. His research interests include information theory and signal processing with applications in wireless communications and smart grid systems.

H. Vincent Poor (S'72–M'77–SM'82–F'87) received the Ph.D. degree in EECS from Princeton University, Princeton, NJ, in 1977.

From 1977 to 1990, he was on the faculty of the University of Illinois at Urbana-Champaign. Since 1990 he has been on the faculty at Princeton, where he is the Michael Henry Strater University Professor of Electrical Engineering and Dean of the School of Engineering and Applied Science. His research interests are in the areas of stochastic analysis, statistical signal processing, and information theory, and their applications in several fields. Among his recent publications in these areas are *Quickest Detection* (Cambridge University Press, 2009) and *Information Theoretic Security* (NOW, 2009).

Dr. Poor is a member of the National Academy of Engineering, a Fellow of the American Academy of Arts and Sciences, and an International Fellow of the Royal Academy of Engineering (U.K.). He is also a Fellow of the Institute of Mathematical Statistics, the Optical Society of America, and other organizations. In 1990, he served as President of the IEEE Information Theory Society, and in 2004–07 he served as the Editor-in-Chief of the *IEEE Transactions on Information Theory*. He received a Guggenheim Fellowship in 2002 and the IEEE Education Medal in 2005. Recent recognition of his work includes the 2007 Technical Achievement Award of the IEEE Signal Processing Society, the 2009 Edwin Howard Armstrong Award of the IEEE Communications Society, the 2010 IET Ambrose Fleming Medal, and the 2011 IEEE Eric E. Sumner Award.