A Polynomial-Time Method to Find the Sparsest Unobservable Attacks in Power Networks

Yue Zhao, Andrea Goldsmith, and H. Vincent Poor

***Abstract*— Power injection attacks that alter generation and loads at buses in power networks are studied. The system operator employs Phasor Measurement Units (PMUs) to detect such physical attacks, while attackers devise attacks that are unobservable by such PMU networks. "Unalterable buses", whose power injections cannot be changed, are also considered in our model. It is shown that, given the PMU locations, the minimum sparsity of unobservable attacks has a simple form with probability one, namely, $\bar{\kappa}(\mathcal{G}^{\mathcal{M}})+1$, where $\bar{\kappa}(\mathcal{G}^{\mathcal{M}})$ is defined as the vulnerable vertex connectivity of an augmented graph. The constructive proof allows one to find the entire set of the sparsest unobservable attacks in polynomial time.**

I. Introduction

The power grid is a critical infrastructure whose security is of paramount importance to national security. While application of information technology is increasingly being used to make the power grid more robust, flexible and dynamic, this change also makes the grid more vulnerable to cyber attacks. Data injection attacks that alter power system measurements can disrupt a power system operator's situational awareness [1]. Control signals of power grid components, including generation and loads, can also be hacked, leading to instability and failures of power systems [2].

The feasibility of constructing *unobservable* data injection attacks that can alter the system operator's state estimates and pass any bad data detection mechanisms in place was first shown in [1]. A central issue that arises for such attacks is characterizing the *sparsest unobservable* data injection attack, as attackers often have limited resources and would like to achieve the minimum attack implementation complexity while maintaining unobservability. However, this problem requires solving an NP-hard l_0 minimization problem. While efficiently finding the set of sparsest unobservable attacks in general remains an open problem, exact solutions under some special problem settings have been developed [3] [4] [5]. Another important aspect of data injection attacks is their impact on the power system. As state estimates are used to guide system and market operation of the grid, several studies have investigated the impact of data attacks on optimal power flow recommendations [6] and locational marginal prices in a deregulated power market [7] [8].

This research was supported in part by the DTRA under Grant HDTRA1-08-1-0010, and in part by the National Science Foundation under Grants CCF-1420575 and CMMI-1435778.

Y. Zhao is with the Dept. of Electrical and Computer Engineering, Stony Brook University, Stony Brook, NY, 11794 USA (e-mail: yue.zhao.2@stonybrook.edu).

A. Goldsmith is with the Dept. of Electrical Engineering, Stanford University, Stanford, CA 94305 USA (e-mail: andrea@ee.stanford.edu).

H. V. Poor is with the Dept. of Electrical Engineering, Princeton University, Princeton, NJ 08544 USA (e-mail: poor@princeton.edu).

On the other hand, physical attacks that directly alter the power network's physical processes also pose significant threats to our power system. Power injection attacks that change generation and loads can be implemented via hacking control signals of generators as well as Internet-based message attacks [2]. Topological attacks have been considered in [9], representing another type of physical attack. In addition, dynamic power injection attacks have been analyzed in several studies. For example, in [10], conditions for the existence of undetectable and unidentifiable attacks were provided, and the sizes of the sets of such attacks were shown to be bounded by graph-theoretic quantities. Alternatively, in [11] and [12], state estimation is considered in the presence of both data injection attacks and power injection attacks.

In this paper, we investigate power injection attacks that alter generation and loads in power networks. Furthermore, our model allows for the power injections at some buses to be "unalterable". This captures the cases of "zero injection buses" with no generation or load, and buses that are protected by the system operator. As such, this paper generalizes our prior work [13] that assumes all buses are alterable. We consider a grid operator that employs PMUs to monitor the network. We study the open l_0 minimization problem of finding the *sparsest unobservable attacks* given any sets of PMU locations and alterable buses.

We first study the condition under which unobervable attacks are feasible. We prove that, with generic grid parameters, the existence of an unobservable power injection attack restricted to any set of buses can be determined with probability one by computing a quantity called the structural rank. Next, we prove that, with generic grid parameters, the NP-hard problem of finding the minimum sparsity of unobservable attacks can be solved in polynomial time with probability one. Specifically, the sparsity of the optimal solution is $\bar{\kappa}(\mathcal{G}^{\mathcal{M}})+1$, where $\bar{\kappa}(\mathcal{G}^{\mathcal{M}})$ is the "vulnerable vertex connectivity" that we define for an augmented graph of the original power network. Thus we show that the entire set of globally optimal solutions to the sparsest unobservable attack problem can be found in polynomial time, with probability one.

The remainder of the paper is organized as follows. In Section II, models of the power network, power injection attacks, PMUs and unalterable buses are established. In addition, the minimum sparsity problem of unobservable attacks is formulated. In Section III we provide the feasibility condition for unobservable attacks restricted to any subset of the buses. In Section IV we prove that the minimum sparsity of unobservable attacks has a simple form with probability

one, which can be computed in polynomial time. Conclusions are drawn in Section V.

II. Problem formulation

A. Power network model

We consider a power network with N buses, and denote the set of buses and the set of transmission lines by $\mathcal{N} = \{1, 2, \ldots, N\}$ and $\mathcal{L} = \{1, 2, \ldots, L\}$ respectively. For a line $l \in \mathcal{L}$ that connects buses n and m, denote its reactance by x_l as well as x_{nm}, and define its incidence vector $\boldsymbol{m}_l \in \mathbb{R}^N$ as follows:

$$\boldsymbol{m}_l(i) = \begin{cases} 1, & \text{if } i = n, \\ -1, & \text{if } i = m, \\ 0, & \text{otherwise.} \end{cases}$$

Based on the power network topology and line reactances, we construct a weighted graph $\mathcal{G} = \{\mathcal{N}, \mathcal{L}, \boldsymbol{w}\}$ where the edge weight $w_l \triangleq \frac{1}{x_l}, \forall l = 1, \ldots, L$. Under a DC power flow model, the real power injections $\boldsymbol{P} \in \mathbb{R}^N$ and the voltage phase angles $\boldsymbol{\theta} \in \mathbb{R}^N$ satisfy $\boldsymbol{P} = \boldsymbol{B}\boldsymbol{\theta}$, where $\boldsymbol{B} = \sum_{l=1}^{L} \frac{1}{x_l} \boldsymbol{m}_l \boldsymbol{m}_l^T \in \mathbb{R}^{N \times N}$ is the Laplacian of the weighted graph $\mathcal{G}$. We consider attackers inflicting power injection attacks that alter the generation and loads in the power network. We denote the power injections under normal conditions by $\boldsymbol{P}$, and denote a power injection attack by $\Delta\boldsymbol{P} \in \mathbb{R}^N$. Thus the post-attack power injections are $\boldsymbol{P} + \Delta\boldsymbol{P}$.

Furthermore, we generalize our model to allow a subset of buses to be "unalterable buses", meaning that their nodal power injection cannot be changed by attackers. This allows us to model the following scenarios:

- A "zero injection" bus that simply connects multiple lines without nodal generation or load, and hence its power injection is always zero and cannot be changed.
- A bus "protected" by the system operator, so that its power injection is not accessible by the attacker.

We denote the set of unalterable buses by $\mathcal{U}$. The other buses $\mathcal{U}^c$ are termed "alterable" buses.

B. Sensor model and unobservable attacks

We consider the use of PMUs by the system operator for monitoring the power network in order to detect power injection attacks. With PMUs installed at the buses, we consider the following two different sensor models:

1) A PMU securely measures the voltage phasor of the bus at which it is installed.
2) A PMU securely measures the voltage phasor of the bus at which it is installed, as well as the current phasors on all the lines connected to this bus[1].

We denote the set of buses with PMUs by $\mathcal{M}$ ($\subseteq \mathcal{N}$), and let $M \triangleq |\mathcal{M}|$ be the total number of PMUs, where $|\cdot|$ denotes the cardinality of a set. Without loss of generality (WLOG), we choose one of the buses in $\mathcal{M}$ to be the angle reference bus. We say that a power injection attack $\Delta\boldsymbol{P}$ is *unobservable* if it leads to *zero* changes in all the quantities measured by the PMUs. With the first PMU model described above, we have the following definition:

Definition 1 (Unobservability condition)**.** *An attack $\Delta\boldsymbol{P}$ is unobservable if and only if*

$$\exists \Delta\boldsymbol{\theta}, \text{ such that } \Delta\boldsymbol{P} = \boldsymbol{B}\Delta\boldsymbol{\theta} \text{ and } \Delta\boldsymbol{\theta}_{\mathcal{M}} = \boldsymbol{0}, \quad (1)$$

where $\Delta\boldsymbol{\theta}_{\mathcal{M}}$ denotes the $M \times 1$ sub-vector of $\Delta\boldsymbol{\theta}$ obtained by keeping its M entries that have indices in $\mathcal{M}$.

With the second PMU model described above, for any bus $n \in \mathcal{N}$, it is immediate to verify that the following three conditions are equivalent:

1) There are no changes of the voltage phasor at n and of the current phasors on all the lines connected to n.
2) There are no changes of the voltage phasor at n and of the power flows on all the lines connected to n.
3) $\forall n' \in N[n]$, there is no change of the voltage phasor at n', where $N[n]$ is the closed neighborhood of n which includes n and its neighboring buses $N(n)$.

Thus, for forming unobservable attacks, the following two situations are equivalent to the attacker:

- The system operator monitors the set of buses $\mathcal{M}$ with the second PMU model;
- The system operator monitors the set of buses $N[\mathcal{M}]$ with the first PMU model,

where $N[\mathcal{M}]$ is the closed neighborhood of $\mathcal{M}$ which includes all the buses in $\mathcal{M}$ and their neighboring buses $N(\mathcal{M})$. Thus, the unobservability condition with the second PMU model is obtained by replacing $\mathcal{M}$ with $N[\mathcal{M}]$ in (1). WLOG, we employ the first PMU model in the following analysis, and based on the discussion above all the results can be directly translated to the second PMU model.

C. Sparsest unobservable attacks

Since attackers are typically resource-constrained, they can choose only a limited number of buses to implement attacks. Thus, for an attack vector $\Delta\boldsymbol{P}$, we use its cardinality $\|\Delta\boldsymbol{P}\|_0$ to model its execution complexity. For minimizing attack complexity, an attacker is interested in finding the set of sparsest attacks that satisfy the unobservability condition (1):

$$\min_{\Delta\boldsymbol{\theta}} \ \|\Delta\boldsymbol{P}\|_0 \quad (2)$$
$$s.t.\ \Delta\boldsymbol{P} = \boldsymbol{B}\Delta\boldsymbol{\theta},\ \Delta\boldsymbol{\theta}_{\mathcal{M}} = \boldsymbol{0},\ \Delta\boldsymbol{P}_{\mathcal{U}} = \boldsymbol{0},\ \Delta\boldsymbol{\theta} \neq \boldsymbol{0}.$$

Since $\Delta\boldsymbol{\theta}_{\mathcal{M}} = \boldsymbol{0},\ \Delta\boldsymbol{\theta} \neq \boldsymbol{0} \Rightarrow \boldsymbol{B}\Delta\boldsymbol{\theta} = \boldsymbol{B}_{\mathcal{N}\mathcal{M}^c}\Delta\boldsymbol{\theta}_{\mathcal{M}^c},\ \Delta\boldsymbol{\theta}_{\mathcal{M}^c} \neq \boldsymbol{0}$, a more compact form of (2) is as follows:

$$(2) \Leftrightarrow \min_{\substack{\Delta\boldsymbol{\theta}_{\mathcal{M}^c} \neq \boldsymbol{0}, \\ (\boldsymbol{B}_{\mathcal{N}\mathcal{M}^c}\Delta\boldsymbol{\theta}_{\mathcal{M}^c})_{\mathcal{U}} = 0}} \|\boldsymbol{B}_{\mathcal{N}\mathcal{M}^c}\Delta\boldsymbol{\theta}_{\mathcal{M}^c}\|_0, \quad (3)$$

where $\mathcal{M}^c = \mathcal{N} \backslash \mathcal{M}$ denotes the complement of M, and $\boldsymbol{B}_{\mathcal{N}\mathcal{M}^c}$ is the submatrix of $\boldsymbol{B}$ formed by choosing all its rows and a set of columns $\mathcal{M}^c$.

We now note that problem (3) is NP-hard: Specifically, as a special case of the cospark problem of a matrix [14], problem (3) resembles the security index problem discussed in [5], which has been proven to be NP-hard. For data

[1]In practice, the second PMU measurement model is achieved by installing PMUs on all the lines connected to a bus.

injection attacks, problems of this type have been shown to be solvable exactly in polynomial time under some special problem settings [3] [4] [5]. In general, low complexity heuristics have been developed for solving l_0 minimization problems (e.g., l_1 relaxation).

D. Graph augmentation

Given the locations of the sensors $\mathcal{M}$, we now introduce an augmentation of the graph $\mathcal{G}$ that will prove key to developing the main results later. In particular, we will show that a vertex cut of the augmented graph can never disconnect those buses with PMUs from each other.

Definition 2. *Given a set of buses $\mathcal{M} \subseteq \mathcal{N}$, $\mathcal{G}^{\mathcal{M}}$ is defined to be the following augmented graph based on $\mathcal{G}$:*

1) *$\mathcal{G}^{\mathcal{M}}$ includes all the buses in $\mathcal{G}$, and has one additional unalterable dummy bus.*
2) *Define an augmented set $\bar{\mathcal{M}}$ that contains $\mathcal{M}$ and the unalterable dummy bus.*
3) *$\mathcal{G}^{\mathcal{M}}$ includes all the edges of $\mathcal{G}$, and an edge is added between every pair of buses in $\bar{\mathcal{M}}$. The weight for each of these added edges can be chosen arbitrarily as any positive number.*

We note that the dummy bus is only connected to the set of sensors $\mathcal{M}$. We observe the following key facts. First, an unobservable attack in the original graph $\mathcal{G}$ leads to zero changes in all the voltage phase angles in $\mathcal{M}$. Thus, any line between a pair of buses in $\mathcal{M}$ would see a zero change of the power flow on it. It is then clear that the added dummy bus and the added lines in $\mathcal{G}^{\mathcal{M}}$ do not lead to any power flow changes in the network under any unobservable attack. We thus have the following lemma:

Lemma 1. *An attack is unobservable by $\mathcal{M}$ in $\mathcal{G}$ if and only if it is unobservable by $\mathcal{M}$ in $\mathcal{G}^{\mathcal{M}}$.*

This allows us to work with the augmented graph $\mathcal{G}^{\mathcal{M}}$ instead of $\mathcal{G}$. It is clear that the weights of the added edges in $\mathcal{G}^{\mathcal{M}}$ do not matter for Lemma 1 to hold.

III. Feasibility condition of unobservable attacks

In this section, we address the following question whose solutions will be useful in solving the minimum sparsity problem (3): Assuming that the attacker can only alter the power injections at a subset of the buses, denoted by $\mathcal{A} \subseteq \mathcal{U}^c$, does there *exist* an attack that is unobservable by a set of PMUs $\mathcal{M}$? For any given $\mathcal{A}$, a feasible non-zero attack $\Delta \boldsymbol{P}$ $(\neq \boldsymbol{0})$ must satisfy $\Delta \boldsymbol{P}_{\mathcal{A}^c} = \boldsymbol{0}$. In other words, it must not alter the power injections at the buses in $\mathcal{A}^c$.

From (1), there exists an unobservable non-zero attack if and only if

$$\exists \Delta \boldsymbol{P}, \Delta \boldsymbol{\theta} \neq \boldsymbol{0},\ s.t.$$
$$\Delta \boldsymbol{P} = \boldsymbol{B} \Delta \boldsymbol{\theta},\ \Delta \boldsymbol{P}_{\mathcal{A}^c} = \boldsymbol{0},\ \Delta \boldsymbol{\theta}_{\mathcal{M}} = \boldsymbol{0}. \tag{4}$$

Since $\begin{cases} \Delta \boldsymbol{\theta}_{\mathcal{M}} = \boldsymbol{0} \\ \Delta \boldsymbol{\theta} \neq \boldsymbol{0} \end{cases} \Rightarrow \Delta \boldsymbol{\theta}_{\mathcal{M}^c} \neq \boldsymbol{0}, \Delta \boldsymbol{P} \neq \boldsymbol{0}$, we have that (4) is equivalent to

$$\exists \Delta \boldsymbol{\theta}_{\mathcal{M}^c} \neq \boldsymbol{0},\ s.t.\ (\Delta \boldsymbol{P}_{\mathcal{A}^c} =)\ \boldsymbol{B}_{\mathcal{A}^c \mathcal{M}^c} \Delta \boldsymbol{\theta}_{\mathcal{M}^c} = \boldsymbol{0}, \tag{5}$$

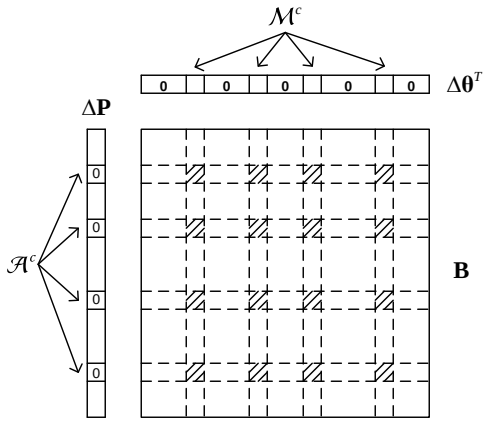


Fig. 1. An illustration of (5) where the submatrix formed by the shaded blocks represents $\boldsymbol{B}_{\mathcal{A}^c \mathcal{M}^c}$.

where $\boldsymbol{B}_{\mathcal{A}^c \mathcal{M}^c}$ is the submatrix of $\boldsymbol{B}$ formed by its rows $\mathcal{A}^c$ and columns $\mathcal{M}^c$. An illustration of (5) is depicted in Figure 1, where the submatrix formed by the shaded blocks represents $\boldsymbol{B}_{\mathcal{A}^c \mathcal{M}^c}$. From (5), we have the following lemma on the feasibility condition of unobservable attacks.

Lemma 2. *Given $\mathcal{A}$ and $\mathcal{M}$, there exists an unobservable non-zero attack if and only if $\boldsymbol{B}_{\mathcal{A}^c \mathcal{M}^c}$ is column rank deficient.*

To analyze when this column rank deficiency condition, $\mathrm{rank}\,(\boldsymbol{B}_{\mathcal{A}^c \mathcal{M}^c}) < |\mathcal{M}^c|$, is satisfied, we start with the following observations based on the fact that $\boldsymbol{B}$ is the Laplacian of the weighted graph $\mathcal{G}$.

1) The *signs* $(+1, -1, \text{or } 0)$ of the entries of $\boldsymbol{B}$ are fully determined by the *network topology*:

   $\boldsymbol{B}_{ij} > 0$, if $i = j$,
   $\boldsymbol{B}_{ij} < 0$, if node (bus) i and node j $(i \neq j)$ are connected by an edge (transmission line),
   $\boldsymbol{B}_{ij} = 0$, if node (bus) i and node j $(i \neq j)$ are not connected.

2) The *values* of the non-zero entries of $\boldsymbol{B}$ are determined by the *line reactances* $\{x_{ij}\}$:

$$\boldsymbol{B}_{ii} = \sum_{j \neq i} w_{ij} = \sum_{j \neq i} \frac{1}{x_{ij}},$$
$$\boldsymbol{B}_{ij} = -w_{ij} = -\frac{1}{x_{ij}},\ \text{if } i \neq j \text{ and } \boldsymbol{B}_{ij} \neq 0.$$

When all the line reactances in the power network are known, so are the entries of the submatrix $\boldsymbol{B}_{\mathcal{A}^c \mathcal{M}^c}$, and it is immediate to compute whether $\mathrm{rank}\,(\boldsymbol{B}_{\mathcal{A}^c \mathcal{M}^c}) < |\mathcal{M}^c|$. *Without* knowing the exact values of any line reactances, we will show that it can be determined almost surely if $\mathrm{rank}\,(\boldsymbol{B}_{\mathcal{A}^c \mathcal{M}^c}) < |\mathcal{M}^c|$ by computing the *structural rank* of $\boldsymbol{B}_{\mathcal{A}^c \mathcal{M}^c}$, defined as follows [15].

Definition 3 (Set of independent entries)**.** *A set of independent entries of a matrix $\boldsymbol{H}$ is a set of nonzero entries, no two of which lie on the same line (row or column).*

Definition 4 (Structural rank)**.** *The structural rank of a matrix $\boldsymbol{H}$, denoted by* $\mathrm{sprank}(\boldsymbol{H})$*, is the maximum number of elements contained in at least one set of independent entries.*

A basic relation between the structural rank and the rank of a matrix is the following [15]:

$$\mathrm{sprank}(\boldsymbol{B}_{\mathcal{A}^c\mathcal{M}^c}) \geq \mathrm{rank}(\boldsymbol{B}_{\mathcal{A}^c\mathcal{M}^c}). \tag{6}$$

In the literature, structural rank is also termed "generic rank" [16].

Returning to the problem of unobservable attacks, we assume that we have *generic* power grid parameters, i.e., we assume that the line reactances x_l $(l = 1, 2, \ldots, L)$ are independent, but not necessarily identical, random variables drawn from continuous probability distributions. We assume that the reactances are bounded away from zero from below (as lines do not have zero reactances in practice). Accordingly, the analysis in this work has a similar flavor to that of *structural properties* as in [15] and [16], and we will develop results that hold *with probability one*. We believe the independence (but not identically distributed) assumption is sufficiently general in practice. In particular, there are uncertainties in factors that influence the reactance of a line (e.g. the distance that a line travels, the degradation of a line over time). These uncertainties can be modeled as independent (but not identically distributed) random variables, leading to the model employed in this paper.

Clearly, $\boldsymbol{B}_{\mathcal{A}^c\mathcal{M}^c}$ is always column rank deficient when $|\mathcal{A}^c| < |\mathcal{M}^c|$. We next discuss the case of $|\mathcal{A}^c| \geq |\mathcal{M}^c|$. We begin with the special case $\mathcal{A} = \mathcal{M}$ for which we have the following lemma, whose proof is provided in [17]:

Lemma 3. *Let $\boldsymbol{B} \in \mathbb{R}^{N\times N}$ be the Laplacian of a connected graph $\mathcal{G}$ with strictly positive edge weights. For any set of node indices $\mathcal{I} \subset \{1, 2, \ldots, N\}$, denote by $\boldsymbol{B}_{\mathcal{I}\mathcal{I}}$ the submatrix of $\boldsymbol{B}$ formed by $\boldsymbol{B}$'s components that have row and column indices in $\mathcal{I}$. Then $\forall \mathcal{I}, |\mathcal{I}| \leq N-1$, $\boldsymbol{B}_{\mathcal{I}\mathcal{I}}$ is of full rank.*

Note that Lemma 3 holds deterministically without assuming generic edge weights of the graph. For the case of $\mathcal{A} = \mathcal{M}$, we let $\mathcal{I} = \mathcal{A}^c = \mathcal{M}^c$, and Lemma 3 proves that $\mathrm{rank}\,(\boldsymbol{B}_{\mathcal{A}^c\mathcal{M}^c}) = |\mathcal{M}^c|$. This implies the intuitive fact that there exists no attack restricted to $\mathcal{A}$ that is unobservable by a set of PMUs $\mathcal{M} = \mathcal{A}$.

Now, we address the general case of arbitrary $\mathcal{A}$ and $\mathcal{M}$. We have the following theorem demonstrating that having $\mathrm{sprank}(\boldsymbol{B}_{\mathcal{A}^c\mathcal{M}^c}) = |\mathcal{M}^c|$ *almost surely guarantees* $\mathrm{rank}(\boldsymbol{B}_{\mathcal{A}^c\mathcal{M}^c}) = |\mathcal{M}^c|$. The proof is provided in [17].

Theorem 1. *For a connected weighted graph $\mathcal{G} = \{\mathcal{N}, \mathcal{L}, \boldsymbol{w}\}$, assume that the edge weights are independent continuous random variables strictly bounded away from zero from below, and denote the Laplacian of $\mathcal{G}$ by $\boldsymbol{B} \in \mathbb{R}^{N\times N}$. Then, any $N' \times N''$ submatrix of $\boldsymbol{B}$, with $\min(N', N'') \leq N-1$, has a rank of $\min(N', N'')$ with probability one if it has a structural rank of $\min(N', N'')$.*

From Theorem 1, with $|\mathcal{A}^c| \geq |\mathcal{M}^c|$, if $\mathrm{sprank}(\boldsymbol{B}_{\mathcal{A}^c\mathcal{M}^c}) = |\mathcal{M}^c| \leq N-1$, we have with probability one that $\mathrm{rank}(\boldsymbol{B}_{\mathcal{A}^c\mathcal{M}^c}) = |\mathcal{M}^c|$, and there exists no attack restricted to $\mathcal{A}$ that is unobservable by a set of PMUs $\mathcal{M}$. On the other hand, if $\mathrm{sprank}(\boldsymbol{B}_{\mathcal{A}^c\mathcal{M}^c}) < |\mathcal{M}^c|$, from (6), $\mathrm{rank}(\boldsymbol{B}_{\mathcal{A}^c\mathcal{M}^c}) < |\mathcal{M}^c|$ as well, and there exists at least one unobservable attack.

Remark 1. *It has been previously known in the literature (see e.g., [15]) that a full structural rank of a matrix leads to a full rank matrix with probability one, as long as the nonzero entries in the matrix are drawn independently from continuous probability distributions. However, it is worth noting that this is not sufficient for proving Theorem 1. This is because, in Theorem 1, we are interested in matrices that are* submatrices of a graph Laplacian*: even with the edge weights of the graph drawn independently, the entries in these submatrices are* correlated *due to the special structure of a graph Laplacian.*

We note that the structural rank of a matrix can be computed in polynomial time via finding the maximum bipartite matching in a graph [15]. Since whether an entry of $\boldsymbol{B}$ is non-zero is solely determined by the topology of the network, we have the following corollary.

Corollary 1. *Given $\mathcal{A}$ and $\mathcal{M}$, whether a non-zero unobservable attack exists can be determined with probability one based solely on the knowledge of the grid topology.*

IV. Solving the sparsest unobservable attacks

In this section, we study the problem of finding the set of sparsest unobservable attacks given any set of PMUs $\mathcal{M}$ (cf. (3)). As remarked in Section II-C, the general problem of l_0 minimization such as (3) is NP-hard. However, due to the particular structure of our problem, we will show that the minimum sparsity of unobservable attacks can in fact be found in *polynomial time with probability one*. We first introduce a key concept — a *vulnerable vertex cut*. We then state our main theorem that yields an explicit solution for (3), the minimum sparsity of unobservable attacks. We prove that this solution both upper and lower bounds the minimization problem of (3), hence proving the theorem.

A. Vulnerable vertex cut and vulnerable vertex connectivity

We start with the following basic definitions:

Definition 5 (Vertex cut)**.** *A vertex cut of a connected graph $\mathcal{G}$ is a set of vertices whose removal renders $\mathcal{G}$ disconnected.*

Definition 6 (Vertex connectivity)**.** *The vertex connectivity of a graph $\mathcal{G}$, denoted by $\kappa(\mathcal{G})$, is the size of the minimum vertex cut of $\mathcal{G}$, i.e., it is the minimum number of vertices that need to be removed to make the remaining graph disconnected.*

From the definition of the augmented graph $\mathcal{G}^{\mathcal{M}}$ in Section II-D, since all the buses in $\bar{\mathcal{M}}$ (containing $\mathcal{M}$ and the dummy bus) are pair-wise connected, we have the following lemma:

Lemma 4. *For any vertex cut of the augmented graph $\mathcal{G}^{\mathcal{M}}$, there is no pair of the buses in $\bar{\mathcal{M}}$ that are disconnected by this cut.*

Accordingly, we introduce the following notations which will be used later on:

Notation 1. *Given a vertex cut of $\mathcal{G}^{\mathcal{M}}$, we denote the set of buses disconnected from $\bar{\mathcal{M}}$ after removing the cut set by $\mathcal{S}$. The cut set itself is thus $N(\mathcal{S})$.*

With the vertex cut $N(\mathcal{S})$, $\mathcal{G}^{\mathcal{M}}$ is partitioned into three subgraphs:

1) $\mathcal{S}$, which does not contain any bus in $\bar{\mathcal{M}}$, i.e., $\mathcal{S} \subseteq \bar{\mathcal{M}}^c$.
2) $N(\mathcal{S})$, which is the vertex cut set itself, and may contain buses in $\bar{\mathcal{M}}$.
3) $\mathcal{N}\backslash N[\mathcal{S}]$, which contains (not necessarily exclusively) all the remaining buses in $\bar{\mathcal{M}}$ after removing the cut set.

An illustrative example with a cut $N(\mathcal{S})$ of size 2 is depicted in Figure 2(b) in Section IV-C.

Leveraging the above notation, we now introduce a key type of vertex cut on $\mathcal{G}^{\mathcal{M}}$.

Definition 7 (Vulnerable vertex cut)**.** *A vulnerable vertex cut of a connected augmented graph $\mathcal{G}^{\mathcal{M}}$ is a vertex cut $N(\mathcal{S})$ for which $|\mathcal{U}^c \cap N[\mathcal{S}]| \geq |N(\mathcal{S})| + 1$.*

In other words, the number of *alterable* buses in $N[\mathcal{S}]$ is no less than the cut size plus one. The reason for calling such a vertex cut "vulnerable" will be made exact later in Section IV-C however the basic intuition is the following. In order to have $\Delta\boldsymbol{\theta}_{\mathcal{M}} = 0$ (unobservability), we must have the phase angle changes on the cut $N(\mathcal{S})$ be zero, with power injection changes (which can only happen on the alterable buses) restricted in $N[\mathcal{S}]$. As will be shown later, this can be achieved if a cut $N(\mathcal{S})$ is "vulnerable" as defined above. We note that it is possible that no vulnerable vertex cut exists (e.g., in the extreme case that all buses are unalterable).

Accordingly, we define the following variation on the vertex connectivity.

Definition 8 (Vulnerable vertex connectivity)**.** *The vulnerable vertex connectivity of an augmented graph $\mathcal{G}^{\mathcal{M}}$, denoted by $\bar{\kappa}(\mathcal{G}^{\mathcal{M}})$, is the size of the minimum vulnerable vertex cut of $\mathcal{G}^{\mathcal{M}}$. If no vulnerable vertex cut exists, $\bar{\kappa}(\mathcal{G}^{\mathcal{M}})$ is defined to be infinity.*

We note that the concepts of vulnerable vertex cut and vulnerable vertex connectivity do not apply to the original graph $\mathcal{G}$. We immediately have the following lemma:

Lemma 5. *If a vulnerable vertex cut exists, then $\bar{\kappa}(\mathcal{G}^{\mathcal{M}}) \leq M = |\mathcal{M}|$.*

Proof. Suppose a vulnerable vertex cut exists, and $\bar{\kappa}(\mathcal{G}^{\mathcal{M}}) \geq M+1$. Denote the minimum vulnerable vertex cut by $N(\mathcal{S})$ (cf. Notation 1). Now consider the set $\mathcal{M}$: it is a vertex cut of $\mathcal{G}^{\mathcal{M}}$ that separates the dummy bus and $\bar{\mathcal{M}}^c$. Because there are at least $\bar{\kappa}(\mathcal{G}^{\mathcal{M}}) + 1 \geq M + 2$ alterable buses in $N[\mathcal{S}] \subseteq N[\bar{M}^c]$, $\mathcal{M}$ is also a *vulnerable vertex cut*. This contradicts the minimum vulnerable vertex cut having size at least $M + 1$. □

B. Main result

We now state the following theorem which gives an explicit solution to (3), the minimum sparsity of unobservable attacks, in terms of the vulnerable vertex connectivity $\bar{\kappa}(\mathcal{G}^{\mathcal{M}})$.

Theorem 2. *For a connected grid $\mathcal{G} = \{\mathcal{N}, \mathcal{L}, \boldsymbol{w}\}$, assume that the line reactances x_l ($l \in \mathcal{L}$) are independent continuous random variables strictly bounded away from zero from below. Given any $\mathcal{M}$ and $\mathcal{U}$, the minimum sparsity of unobservable attacks, i.e., the global optimum of* (3)*, equals $\bar{\kappa}(\mathcal{G}^{\mathcal{M}}) + 1$ with probability one.*

We note that finding the vulnerable vertex connectivity of a graph is computationally efficient. For polynomial time algorithms we refer the reader to [18]. We now prove this theorem by upper and lower bounding the minimum sparsity of unobservable attacks in the following two subsections.

C. Upper bounding the minimum sparsity of unobservable attacks

We show that *any* vulnerable vertex cut $N(\mathcal{S})$ provides an upper bound on the optimum of (3) as follows.

Theorem 3. *For a connected grid $\mathcal{G}$ and a set of PMUs $\mathcal{M}$, for any vulnerable vertex cut of $\mathcal{G}^{\mathcal{M}}$ denoted by $N(\mathcal{S})$ (cf. Notation 1), there exists an unobservable attack of sparsity no higher than $|N(\mathcal{S})| + 1$.*

Proof. A vulnerable vertex cut $N(\mathcal{S})$ partitions $\mathcal{G}^{\mathcal{M}}$ into $\mathcal{S}$, $N(\mathcal{S})$ and $\mathcal{N}\backslash\mathcal{N}[\mathcal{S}]$, with $\mathcal{S} \subseteq \mathcal{M}^c$. Similarly to the range space interpretation of the problem defined by (3), it is sufficient to show that there exists a non-zero vector in the range space of $\boldsymbol{B}_{\mathcal{N}\mathcal{S}}$ such that i) it has a sparsity no higher than $|N(\mathcal{S})| + 1$, and ii) non-zero power injections occur only at the alterable buses.

By re-indexing the buses, WLOG, i) let $\mathcal{S} = \{1, 2, \ldots, |\mathcal{S}|\}$, and ii) let $\boldsymbol{B}_{\mathcal{N}\mathcal{S}}$ have the following partition as depicted in Figure 2(a):

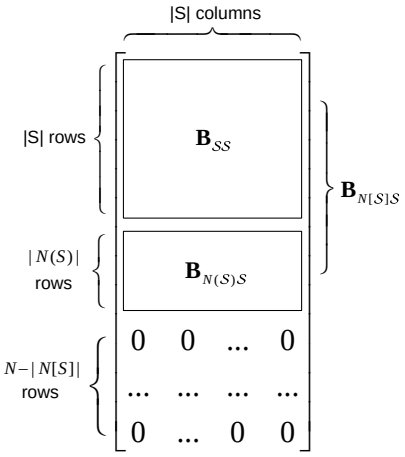
1) The top submatrix $\boldsymbol{B}_{\mathcal{S}\mathcal{S}}$ is an $|\mathcal{S}| \times |\mathcal{S}|$ matrix.
2) The middle submatrix (which will be shown to be $\boldsymbol{B}_{N(\mathcal{S})\mathcal{S}}$) consists of all the remaining rows, each of which has at least one *non-zero* entry.
3) The bottom submatrix is an *all-zero* matrix.

In particular, from the definition of the Laplacian, the middle submatrix of $\boldsymbol{B}_{\mathcal{N}\mathcal{S}}$, as described above, is exactly $\boldsymbol{B}_{N(\mathcal{S})\mathcal{S}}$ because its row indices correspond to those buses not in $\mathcal{S}$ but connected to at least one bus in $\mathcal{S}$.

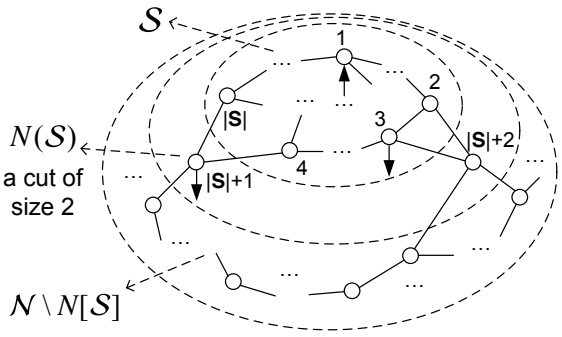
From the definition of the vulnerable vertex cut, $|\mathcal{U}^c \cap N[\mathcal{S}]| \geq |N(\mathcal{S})| + 1$. Now, pick any set of $|N(\mathcal{S})| + 1$ alterable buses in $\mathcal{U}^c \cap N[\mathcal{S}]$, denote this set by $\mathcal{A}$, and denote the other buses in $N[\mathcal{S}]$ by $\tilde{U} \triangleq N[\mathcal{S}]\backslash\mathcal{A}$. Clearly, $|\tilde{U}| = |S| - 1$. Therefore, $\boldsymbol{B}_{\tilde{\mathcal{U}}\mathcal{S}}$ (which is a submatrix of $\boldsymbol{B}_{N[\mathcal{S}]\mathcal{S}}$) has $|S|$ columns but only $|S|-1$ rows, and is hence column rank deficient.

Now let $\Delta\boldsymbol{\theta}_{\mathcal{S}}$ be a non-zero vector in the null space of $\boldsymbol{B}_{\tilde{\mathcal{U}}\mathcal{S}}$:

$$\boldsymbol{B}_{\tilde{\mathcal{U}}\mathcal{S}}\Delta\boldsymbol{\theta}_{\mathcal{S}} = \boldsymbol{0}. \tag{7}$$



(a) Block representation of $\boldsymbol{B}_{\mathcal{N}\mathcal{S}}$.



(b) A 3-sparse unobservable power injection attack.

Fig. 2. Sparse attacks with voltage phase angle changes restricted to buses $1, 2, \ldots |\mathcal{S}|$.

Then, we can construct an attack vector $\Delta \boldsymbol{P} = \boldsymbol{B}_{\mathcal{N}\mathcal{S}} \Delta \boldsymbol{\theta}_{\mathcal{S}}$ that has some possibly non-zero values at the indices that correspond to $\mathcal{A}$, and has *zero values at all other indices.* Thus,

$$\|\Delta \boldsymbol{P}\|_0 \leq |\mathcal{A}| = |N(\mathcal{S})| + 1. \tag{8}$$

□

Theorem 3 explains our terminology of a "vulnerable vertex cut" since, if a vertex cut is vulnerable, it leads to an unobservable attack. If a vulnerable vertex cut of $\mathcal{G}^{\mathcal{M}}$ exists, applying Theorem 3 to the *minimum* one, we have that the optimum of (3) is upper bounded by $\bar{\kappa}(\mathcal{G}^{\mathcal{M}}) + 1$. If no vulnerable vertex cut exists, $\bar{\kappa}(\mathcal{G}^{\mathcal{M}}) + 1 = \infty$ is a trivial upper bound.

We now provide a graph-theoretic interpretation of Theorem 3. As shown in Figure 2(a) and 2(b), all the buses can be partitioned into three subsets $\mathcal{S}, N(\mathcal{S})$ and $\mathcal{N} \backslash N[\mathcal{S}]$, corresponding to the row indices of the top, middle and bottom submatrices of $\boldsymbol{B}_{\mathcal{N}\mathcal{S}}$, respectively. $N(\mathcal{S})$ is a vulnerable vertex cut of $\mathcal{G}^{\mathcal{M}}$ that separates $\mathcal{S}$ from $\mathcal{N} \backslash N[\mathcal{S}]$. The sparse attack $\Delta \boldsymbol{P}$ (cf. (8)) is formed by injecting/extracting power at $|N(\mathcal{S})| + 1$ alterable buses in $N[\mathcal{S}]$, such that the phase angle changes at $\mathcal{N} \backslash \mathcal{S}$ are all zero. Note that $(\mathcal{N} \backslash \mathcal{S}) \supseteq \mathcal{M}$. The example with $|N(\mathcal{S})| = 2$ in Figure 2(b) illustrates a 3-sparse attack with power injection/extractions at (assumed alterable) buses $1, 3$ and $|\mathcal{S}| + 1$, such that the phase angle changes at $\mathcal{N} \backslash \mathcal{S}$ are all zero.

D. Lower bounding the sparsity of unobservable attacks

We first define the following property of a matrix $\boldsymbol{H} \in \mathbb{R}^{N \times N}$, which will be shown to be equivalent to having $\text{sprank}(\boldsymbol{H}) = N$.

Property 1 (An equivalent condition for having a full structural rank)**.**

$\forall n = 1, 2, \ldots, N$, *and for any* $n \times N$ *submatrix of* $\boldsymbol{H}$, *the submatrix has at least* n *columns each with at least one non-zero entry.*

We have the following lemma whose proof is provided in [17]:

Lemma 6. *Property 1 is equivalent to* $\text{sprank}(\boldsymbol{H}) = N$.

We now prove the lower bounding part of Theorem 2, namely, with probability one, all unobservable power injection attacks $\Delta \boldsymbol{P}$ must have $\|\Delta \boldsymbol{P}\|_0 \geq \bar{\kappa}(\mathcal{G}^{\mathcal{M}}) + 1$. The key idea is in showing that the equivalence between Property 1 and a full structural rank (cf. Lemma 6) implies a connection between the vulnerable vertex connectivity and the feasibility condition of unobservable attacks (cf. Lemma 2).

Proof of $\|\Delta \boldsymbol{P}\|_0 \geq \bar{\kappa}(\mathcal{G}^{\mathcal{M}}) + 1$ *for unobservable* $\Delta \boldsymbol{P}$*, w.p.1.* We focus on $\mathcal{G}^{\mathcal{M}}$ and consider its corresponding Laplacian $\boldsymbol{B}$. Suppose there exists a power injection attack $\Delta \boldsymbol{P} \neq \boldsymbol{0}$ such that

$$\Delta \boldsymbol{\theta}_{\mathcal{M}} = \boldsymbol{0} \text{ and } \|\Delta \boldsymbol{P}\|_0 \leq \bar{\kappa}(\mathcal{G}^{\mathcal{M}}). \tag{9}$$

Denote the buses with non-zero power injection changes by $\mathcal{A} \subseteq \mathcal{U}^c$, and hence $\Delta \boldsymbol{P}_{\mathcal{A}^c} = \boldsymbol{0}$. From (9), $|\mathcal{A}| \leq \bar{\kappa}(\mathcal{G}^{\mathcal{M}}), \Delta \boldsymbol{\theta}_{\mathcal{M}^c} \neq \boldsymbol{0}$, and $\boldsymbol{0} = \Delta \boldsymbol{P}_{\mathcal{A}^c} = \boldsymbol{B}_{\mathcal{A}^c \mathcal{M}^c} \Delta \boldsymbol{\theta}_{\mathcal{M}^c}$, implying that $\boldsymbol{B}_{\mathcal{A}^c \mathcal{M}^c}$ is column rank deficient. We first consider the case that a vulnerable vertex cut exists, i.e., $\bar{\kappa}(\mathcal{G}^{\mathcal{M}}) < \infty$. The proof for the case of $\bar{\kappa}(\mathcal{G}^{\mathcal{M}}) = \infty$ follows similarly. For notational simplicity, we will use $\bar{\kappa}$ instead of $\bar{\kappa}(\mathcal{G}^{\mathcal{M}})$ in the remainder of the proof.

a) If a vulnerable vertex cut exists, i.e., $\bar{\kappa} < \infty$*:*

We will prove that, for all $\mathcal{A} \subseteq \mathcal{U}^c$ with $|\mathcal{A}| \leq \bar{\kappa}$, $\boldsymbol{B}_{\mathcal{A}^c \mathcal{M}^c}$ *is of full column rank with probability one*, i.e., (9) can only happen with probability zero. From Lemma 5, $\bar{\kappa} \leq M$. It is then sufficient to prove for the "worst cases" with $|\mathcal{A}| = \bar{\kappa} = M$, i.e., $|\mathcal{A}^c| = |\mathcal{M}^c| = N - \bar{\kappa}$ and $\boldsymbol{B}_{\mathcal{A}^c \mathcal{M}^c}$ is a square matrix. From Theorem 1 and Lemma 6, it is sufficient to show that $\boldsymbol{B}_{\mathcal{A}^c \mathcal{M}^c}$ *satisfies Property 1*, and hence is of full rank with probability one. Recall from the definition of the Laplacian $\boldsymbol{B}$ that, for any column (or row) of $\boldsymbol{B}$, $\boldsymbol{b}_i, i = 1, \ldots, N$, its non-zero entries correspond to bus i and those buses that are connected to bus i. With this, we now prove that $\boldsymbol{B}_{\mathcal{A}^c \mathcal{M}^c}$ satisfies Property 1.

Consider any set of n ($\leq N - \bar{\kappa}$) buses in $\mathcal{A}^c$, denoted by $\tilde{\mathcal{N}}$.

i) If $\tilde{\mathcal{N}} \subseteq \mathcal{M}^c$: Based on the definition of the Laplacian $\boldsymbol{B}$, the n columns of $\boldsymbol{B}_{\tilde{\mathcal{N}} \mathcal{M}^c}$ *that correspond to the buses* $\tilde{\mathcal{N}}$ *themselves* each has at least one non-zero entry.

ii) If $\tilde{\mathcal{N}} \cap \mathcal{M} \neq \emptyset$: We prove that $N(\tilde{\mathcal{N}})$ must contain at least $\bar{\kappa}$ buses. This is because, otherwise, $|N(\tilde{\mathcal{N}})| \leq \bar{\kappa} - 1$, contradicting that $\bar{\kappa}$ is the minimum size of vulnerable vertex cuts for the following reasons:

1) $\mathcal{A} \subseteq \tilde{\mathcal{N}}^c$, and thus $\tilde{\mathcal{N}}^c$ has at least $|\mathcal{A}| = \bar{\kappa}$ alterable buses.
2) $|N(\tilde{\mathcal{N}})| \leq \bar{\kappa} - 1$ implies that $\tilde{\mathcal{N}}^c \backslash N(\tilde{\mathcal{N}}) \neq \emptyset$, and thus $N(\tilde{\mathcal{N}})$ is a vertex cut that separates $\tilde{\mathcal{N}}$ and $\tilde{\mathcal{N}}^c \backslash N(\tilde{\mathcal{N}})$.
3) Because $\tilde{\mathcal{N}} \cap \mathcal{M} \neq \emptyset$ and $\mathcal{M}$ are pairwise connected in $\mathcal{G}^{\mathcal{M}}$, $\mathcal{M} \subseteq N[\tilde{\mathcal{N}}]$. Thus, $\tilde{\mathcal{N}}^c \backslash N(\tilde{\mathcal{N}})$ and $\mathcal{M}$ are disjoint.

From 1), 3), and the fact that $|N(\tilde{\mathcal{N}})| \leq \bar{\kappa} - 1$, we observe that $N(\tilde{\mathcal{N}})$ is a *vulnerable vertex cut* of size $\bar{\kappa} - 1$, contradicting $\bar{\kappa}$ being the vulnerable vertex connectivity.

Now, based on the definition of the Laplacian $\boldsymbol{B}$, the $n \times N$ submatrix $\boldsymbol{B}_{\tilde{\mathcal{N}}\mathcal{N}}$ *must have at least* $n + \bar{\kappa}$ *columns each of which has at least one non-zero entry for the following reasons:*

- The n columns of $\boldsymbol{B}_{\tilde{\mathcal{N}}\mathcal{N}}$ that correspond to the buses $\tilde{\mathcal{N}}$ themselves each has at least one non-zero entry.
- As $\tilde{\mathcal{N}}$ are connected to at least $\bar{\kappa}$ other buses, each one of these $\bar{\kappa}$ neighbors of $\tilde{\mathcal{N}}$ corresponds to one column of $\boldsymbol{B}_{\tilde{\mathcal{N}}\mathcal{N}}$ that has at least one non-zero entry.

Accordingly, the $n \times (N - \bar{\kappa})$ submatrix $\boldsymbol{B}_{\tilde{\mathcal{N}}\mathcal{M}^c}$ has at least n columns each of which has at least one non-zero entry.

Summarizing i) and ii), $\boldsymbol{B}_{\mathcal{A}^c\mathcal{M}^c}$ satisfies Property 1, and is thus of full column rank with probability one. Therefore, (9) can only happen with probability zero.

b) If no vulnerable vertex cut exists, i.e., $\bar{\kappa} = \infty$*:* If $\mathcal{M} = \mathcal{N}$, i.e., all buses have PMUs, no unobservable attack exists. If $M \leq N - 1$. Suppose $|\mathcal{A}| \geq M + 1$. Consider the set $\bar{M}$ containing $\mathcal{M}$ and the dummy bus. $\Delta\boldsymbol{\theta}_{\mathcal{M}} = \mathbf{0}$ (cf. (9)) implies that $\mathcal{A} \subseteq N[\bar{\mathcal{M}}^c]$, and thus $N[\bar{\mathcal{M}}^c]$ has at least $|\mathcal{A}| \geq M + 1$ alterable buses. Since $\mathcal{M}$ $(= N(\bar{\mathcal{M}}^c))$ separates the dummy node and $\mathcal{N} \backslash \mathcal{M}$, $\mathcal{M}$ is a *vulnerable vertex cut*. This contradicts the nonexistence of a vulnerable vertex cut. Therefore, $|\mathcal{A}| \leq M$. In this case, the same proof as in the above case i) when a vulnerable vertex cut exists applies, and (9) can only happen with probability zero. □

With the proofs of these upper and lower bounds, we have now proved Theorem 2. In addition, from the proof of Theorem 3, we have a *constructive solution* of the set of sparsest unobservable attack in polynomial time. We highlight the following fact similar to that in Section III: the minimum sparsity of unobservable attacks is fully determined with probability one by the *network topology, the locations of the alterable buses, and the locations of the PMUs*. Further studies on the impact of sparsest unobservable attacks and countermeasures by system operators can be found in [17].

V. Conclusion

We have studied power injection attacks that alter power generation and loads in power networks while remaining unobservable by PMUs of the system operator. Given the PMU locations, we have first shown that the existence of an unobservable attack restricted to any subset of the buses can be determined with probability one by computing the structural rank of a submatrix of the network Laplacian $\boldsymbol{B}$. Next, we have provided an explicit solution to the open problem of finding the set of sparsest unobservable attacks: the minimum sparsity among all unobservable attacks equals $\bar{\kappa}(\mathcal{G}^{\mathcal{M}}) + 1$ with probability one, where $\bar{\kappa}(\mathcal{G}^{\mathcal{M}})$ is the vulnerable vertex connectivity of an augmented graph. The constructive solution allows us to find all the sparsest unobservable attacks in polynomial time.

References

[1] Y. Liu, P. Ning, and M. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Transactions on Information and System Security*, vol. 14, no. 1, Article 13, May 2011.

[2] A.-H. Mohsenian-Rad and A. Leon-Garcia, "Distributed internet-based load altering attacks against smart power grids," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 667–674, December 2011.

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

[4] K. C. Sou, H. Sandberg, and K. H. Johansson, "On the Exact Solution to a Smart Grid Cyber-Security Analysis Problem," *IEEE Transactions on Smart Grid*, vol. 4, no. 2, pp. 856 – 865, Jun. 2013.

[5] J. Hendrickx, K. H. Johansson, R. Jungers, H. Sandberg, and K. C. Sou, "Efficient computations of a security index for false data attacks in power networks," *IEEE Transactions on Automatic Control*, vol. 59, no. 12, pp. 3194–3208, December 2014.

[6] A. Teixeira, H. Sandberg, G. Dan, and K. H. Johansson, "Optimal power flow: closing the loop over corrupted data," *Proc. American Control Conference*, pp. 3534 – 3540, Jun. 2012.

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

[8] J. Kim and L. Tong, "On Topology Attack of a Smart Grid: Undetectable Attacks and Countermeasures," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 7, pp. 1294 – 1305, Jul. 2013.

[9] J. Weimer, S. Kar, and K. H. Johansson, "Distributed detection and isolation of topology attacks in power networks," *Proc. 1st International Conference on High Confidence Networked Systems*, pp. 65–72, July 2012.

[10] F. Pasqualetti, F. Dorfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," *IEEE Transactions on Automatic Control*, vol. vol.58, no.11, pp. 2715–2729, Nov. 2013.

[11] H. Fawzi, P. Tabuada, and S. Diggavi, "Secure estimation and control for cyber-physical systems under adversarial attacks," *IEEE Transactions on Automatic Control*, vol. 59, no.6, pp. 1454–1467, June 2014.

[12] ——, "Security for control systems under sensor and actuator attacks," *Proc. IEEE 51st Annual Conference on Decision and Control (CDC)*, pp. 3412–3417, December 2012.

[13] Y. Zhao, A. Goldsmith, and H. V. Poor, "Fundamental limits of cyber-physical security in smart power grids," *Proc. IEEE 52nd Annual Conference on Decision and Control (CDC)*, pp. 200–205, Dec. 2013.

[14] E. J. Candes and T. Tao, "Decoding by linear programming," *IEEE Transactions on Information Theory*, vol. 51, no. 12, pp. 4203 – 4215, Dec. 2005.

[15] K. Reinschke, *Multivariable Control - A Graph-Theoretic Approach*. New York: Springer-Verlag, Lecture Notes in Control and Information Sciences, vol. 108, 1988.

[16] R. Johnston, G. Barton, and M. Brisk, "Determination of the generic rank of structural matrices," *Int. J. Control*, vol. 40, pp. 257 – 264, 1984.

[17] Y. Zhao, A. Goldsmith, and H. V. Poor, "Minimum sparsity of unobservable power network attacks," *IEEE Transactions on Automatic Control, in revision*.

[18] M. R. Henzingera, S. Raob, and H. N. Gabow, "Computing vertex connectivity: new bounds from old techniques," *Journal of Algorithms*, vol. 34, no. 2, pp. 222 – 250, February 2000.