Smart Grid Data Integrity Attacks

Annarita Giani, Eilyan Bitar, Manuel Garcia, Miles McQueen, Pramod Khargonekar, and Kameshwar Poolla

***Abstract*—Real power injections at loads and generators, and real power flows on selected lines in a transmission network are monitored and transmitted over a SCADA network to the system operator. These are used in state estimation algorithms to make dispatch, re-balance and other energy management system [EMS] decisions. Coordinated cyber attacks on power meter readings can be designed to be undetectable by any bad data detection algorithm. These unobservable attacks present a serious threat to grid operations. Of particular interest are *sparse* attacks that involve the compromise of a modest number of meter readings. An efficient algorithm to find all unobservable attacks [under standard DC load flow approximations] involving the compromise of *exactly two* power injection meters and an arbitrary number of power meters on lines is presented. This requires $O(n^2 m)$ flops for a power system with n buses and m line meters. If *all* lines are metered, there exist canonical forms that characterize all 3, 4, and 5-sparse unobservable attacks. These can be quickly detected with $O(n^2)$ flops using standard graph algorithms. *Known-secure* phasor measurement units [PMUs] can be used as countermeasures against a given collection of cyber attacks. Finding the minimum number of necessary PMUs is NP-hard. It is shown that $p+1$ PMUs at carefully chosen buses are sufficient to neutralize a collection of p cyber attacks.**

***Index Terms*—Cybersecurity, integrity attacks, observability, smart grid, synchro-phasors.**

I. Introduction

CYBERSECURITY of critical infrastructures in general, and the electricity grid in particular, is a subject of increasing research interest [8], [10]. The potential consequences of successful cyber attacks on the electricity grid are staggering. SCADA [Supervisory Control and Data Acquisition] hardware and software components are used to supervise, control, optimize, and manage electricity generation and transmission systems. As the grid evolves, legacy SCADA systems will co-exist and inter-operate with new components [ex: smart meters], networks [ex: NASPInet] [29], sensors [ex: phasor measurement units or PMUs] [37], and control devices [ex: intelligent relays] [30], [31]. Tomorrow's *Smart Grid* will incorporate increased sensing, communication, and distributed control to accommodate renewable generation, EV [Electric Vehicle] loads, storage, and many other technologies. These innovations increase the grid's vulnerability to cyber attacks, increasing the urgency and relevance of cyber security research.

State estimation is a major component of Energy Management Systems [1], [28]. This is the optimal estimation of the power system state [voltage magnitudes and phase angles at all buses] using [noisy] data from [real and reactive] power meters, voltage sensors, and system parameters. We consider data integrity cyber attacks that consist of a set of compromised power meters whose readings are altered by the attacker. Cyber-attacks whose compromised meter readings are consistent with the physical power flow constraints are called *unobservable*. Unobservable attacks require *coordination*—compromised meter readings must be carefully orchestrated to fall on a low dimensional manifold in order for the attack to be unobservable. Unobservable attacks will pass any bad data detection algorithm. Such attacks can cause significant errors in state estimation algorithms, which can mislead system operators into making potentially catastrophic decisions. Liu *et al.* [25] have recently shown that many power systems commonly admit unobservable attacks involving a *relatively small number* of power meters, and consequently the degree of coordination necessary is modest. This surprising result has led to a flurry of activity in the power system cybersecurity research community [6], [20], [34], [35].

A. Summary of Contributions

We focus on unobservable *low-sparsity cyber attacks* that require coordination of a small number of [≤ 5] meters. Indeed, we suggest that cyber attacks of large numbers of meters are improbable because of the degree of temporal coordination necessary across geographically separated attack points. We provide an efficient algorithm to find all unobservable attacks involving the compromise of *exactly two* power injection meters and an arbitrary number of power meters on lines. This requires $O(n^2 m)$ flops for a power system with n buses and m line meters. For the special case, where *all* lines are metered, we derive canonical forms for 3, 4, and 5-sparse unobservable attacks in terms of the graph of the power network. We further show that all k-sparse attacks for $k \leq 5$ can be found using graph-theoretic algorithms that require $O(n^2)$ flops to detect the presence of these canonical forms for power systems with bounded degree [i.e. max number of lines attached to a bus].

We next consider the problem of using *known-secure PMUs* to thwart an arbitrary collection [not necessarily sparse] of

Manuscript received May 30, 2012; revised October 03, 2012 and November 15, 2012; accepted January 18, 2013. Date of publication April 18, 2013; date of current version August 21, 2013. This work was supported in part by EPRI and CERTS under sub-award 09-206; PSERC S-52, in part by the NSF under Grants EECS-1129061/9001, CPS-1239178, and CNS-1239274/9467/9178, in part by the Republic of Singapores National Research Foundation through a grant to the Berkeley Education Alliance for Research in Singapore for the SinBerBEST Program, in part by the Florida Energy Systems Consortium, the Eckis Professor endowment at the University of Florida, in part by Robert Bosch LLC through its Bosch Energy Research Network funding program, and in part by the U.S. Department of Energy through the INL/LANL/LDRD/CNLSPrograms.

A. Giani is with the Center for Nonlinear Studies, Los Alamos National Laboratory, Los Alamos, NM 87545 USA.

E. Bitar is with the School of Electrical and Computer Engineering, Cornell University, Ithaca, NY 14850 USA.

M. Garcia is with the Department of Mechanical Engineering, University of California, Berkeley, CA 94720 USA.

M. McQueen is with the Idaho National Laboratory, Idaho Falls, ID 83401 USA.

P. Khargonekar is with the Department of Electrical Engineering, University of Florida, Gainesville, FL 32611 USA.

K. Poolla is with the Department of Electrical and Computer Engineering, University of California, Berkeley, CA 94720 USA.

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.2013.2245155

cyber attacks. We offer a characterization of buses at which these PMUs must be placed to mitigate the collection of attacks. Finding the minimum number of necessary PMUs is NP-hard [3]. We show that it is sufficient to place $p+1$ PMUs at carefully chosen buses to neutralize a collection of p cyber attacks. We offer an algorithm to determine this sufficient placement that requires $O(n^2 p)$ flops. We also offer countermeasures based on state estimation without additional hardware. We conclude with synthetic examples that illustrate our results.

We use the notion of *topological observability* for deriving our results. Unobservable attacks can be characterized topologically. As a result, they do not depend on power system line electrical parameters or operating points. Consequently, our results are not restricted to the linearized DC state estimation setting but also hold for general nonlinear power flow models. The complete development in the nonlinear setting is left for a future paper.

B. Related Work

Many recent papers have explored various aspects of cyber attacks on SCADA/EMS systems that impact the key function of state estimation [5], [6], [20], [34], [35]. It was shown in [20] that the attack strategy identified in [25] can be equivalently characterized by the property that the power system becomes unobservable by the removal of the compromised meters. Fault detection is intimately connected to, but distinct from, integrity attack detection. Recently, Gorinevski *et al.* [12] considered a fault detection problem in SCADA/EMS systems that is closely related to the problem formulation and approach of [20]. Phasor measurement units have recently attracted a great deal of interest for providing direct, low-latency state measurements. Emami and Abur [9] have shown that with the introduction of a few extra PMUs, the bad data detection capabilities of a given system can be dramatically improved. More relevant to our work is the recent paper of Bobba *et al.* [3] who have investigated the use of PMUs in mitigation of SCADA/EMS cyber attacks identified in [25] using heuristic algorithms. The recent paper by Kim and Poor [19] also investigates optimal PMU placement problems. Their approach is to use a greedy PMU placement algorithm which suggests in simulation studies that placing PMUs at ≈1/3 the number of nodes serves to protect the system. Both papers recognize that the underlying placement problem is NP-hard.

An early version without proofs of some of the results in this paper was presented at the 2011 IEEE SmartGridComm [11].

II. Problem Set-Up

The k^{th} entry in the vector v is v_k. The vector, every component of which is 1, is $\underline{1}$, and e^k denotes the k^{th} unit vector. For a matrix M, let $\mathcal{R}(M)$ and $\mathcal{N}(M)$ denote its range and null spaces respectively. The transpose of M is written M^*. Subspaces of $\mathbb{R}^n$ are written $\mathcal{S}, \mathcal{T}, \ldots$. Sets [of meters, buses, attacks] are designated $\mathbb{S}, \mathbb{V}, \mathbb{A}$. The number of elements in $\mathbb{S}$ is written $|\mathbb{S}|$, and $\mathbb{V} \setminus \mathbb{S}$ denotes the set of elements in $\mathbb{V}$ that are not in $\mathbb{S}$.

Consider a power system consisting of $n+1$ buses, connected by transmission lines. The power system can be represented as an undirected graph $\mathcal{G}$ whose vertices $\mathbb{V}$ are the buses, and with edge set $\mathbb{E}$ being the lines. Generators and loads are represented by arcs entering or leaving a vertex.

There are two types of buses: *injection buses* where loads or generators are connected, and *null buses* where no external power is supplied or extracted. Transmission lines connect pairs of buses. We combine all generation and loads at a bus into a single injection, and we assume there is no more than one line between any pair of buses. There are m real power flow meters on *selected* lines, and power injection meters to measure net injected real power from *all* generators, and net power supplied to *all* loads. As we will consider lossless DC load flow models, other measurements [ex: real power flows at both ends of a line, reactive power flows, etc.] are not immediately relevant to our problem formulation. These become important for general nonlinear load flow models. Today, real power meter data is acquired every 2–10 seconds and transmitted to the EMS control center over a legacy SCADA network. There is some consensus that this SCADA network is vulnerable to cyber-attacks [17]. A small fraction [∼10–15%] of lines have power flow meters, and while all generators and loads are metered [for settlement], only larger [>50 MW] units have meters connected to the SCADA network.

We consider a power system whose underlying graph $\mathcal{G}$ is simply connected. We make standard DC load flow assumptions: quasi-steady state operation, all bus voltages are = 1 p.u., the lines are lossless, and power angle differences $\delta_i - \delta_j$ are small. We remark that these assumptions are made to simplify our exposition. Indeed, some of the results of this paper [see Remark 15] are intimately connected to topological observability [18] and therefore apply to the general case of nonlinear load flow irrespective of operating condition. We designate an arbitrary slack bus from which voltage phases are referenced. Under these DC load flow assumptions, the power system state is simply the bus angles relative to the slack bus $x = \delta \in \mathbb{R}^n$. In standard practice, we disregard one of the injected power readings, as the sum of power injections is zero to account for power conservation. In our situation, we must depart from this practice to allow for the possibility that power readings at *any* bus might be compromised.

Let $y_1 \in \mathbb{R}^{n+1}$ be the vector of injected power measurements at the $n+1$ buses. We order the buses so the first subset consists of null buses, and the second subset consists of injection buses. Thus y_1 has the form $[0\ \xi^T]^T$. Let $y_2 \in \mathbb{R}^m$ be the vector of line power measurements. We can model the power system by the linear equations:

$$\begin{bmatrix} y_1 \\ y_2 \end{bmatrix} = y = Hx = \begin{bmatrix} H_1 \\ H_2 \end{bmatrix} x, \quad H \in \mathbb{R}^{(m+n+1)\times n} \tag{1}$$

Here, H is constructed from line susceptances. We assume that all susceptances are positive. With this assumption, we note that the DC power flow model (1) does not admit real power flow loops. The partition of y [and H] corresponds to buses [null and injection], and line meters respectively. We assume the system state x can be uniquely deduced [modulo translations] from the injected power observations y_1, or equivalently, $\operatorname{rank}(H_1) = n$.

A. Unobservable Attacks

Definition 1: An *attack* $\mathcal{A} = (\mathbb{S}, a)$ is a set of meters $\mathbb{S}$, and an attack vector $0 \neq a \in \mathbb{R}^{m+n+1}$. The nonzero components of a correspond to the *compromised* meters in $\mathbb{S}$, i.e. $k \in \mathbb{S} \iff a_k \neq 0$. Under the attack $\mathcal{A}$, the meter readings are changed by the attacker from their uncompromised values y to the compromised values $y + a$. We abuse language and say that a line is compromised when we mean that the meter on that line is compromised. The *sparsity* of the attack $\mathcal{A}$ is $|\mathbb{S}| =$ the number of compromised meters.

Definition 2: Consider a power system with the power flow model (1). Let x^o denote the current system state, and $y^o = Hx^o$ denote the uncompromised measurements. An attack $\mathcal{A}$ is called *unobservable* at operating point x^o with respect to the model (1) if there exists some system state consistent with the compromised observations, i.e.

$$\exists\, x^a : y^o + a = H(x^o + x^a) \tag{2}$$

Remark 3: Here x^a is the (unique) *perceived state perturbation* associated with attack $\mathcal{A}$. It is the fictitious change of system state necessary to produce the compromised meter readings $y^o + a$. As model (1) is linear, $\mathcal{A} = (\mathbb{S}, a)$ is unobservable if and only if $a \neq 0$, $a = Hx^a$ is solvable, and $\mathbb{S}$ indexes the nonzero elements of a. Unobservability of $\mathcal{A}$ under the model (1) does not depend on the current system state x^o. □

Remark 4: Consider an unobservable attack $\mathcal{A} = (\mathbb{S}, a)$. Let $\mathbb{M}$ denote set of all meters, indexed $\{1, \cdots, m+n+1\}$, and let $\mathbb{T} = \mathbb{M} \setminus \mathbb{S}$ be the complement of $\mathbb{S}$. We can conduct elementary row permutations (or re-index power meters) to write

$$a = Hx^a = \begin{bmatrix} L \\ K \end{bmatrix} x^a = \begin{bmatrix} q \\ 0 \end{bmatrix} \begin{matrix} \}\text{ compromised } \mathbb{S} \\ \}\text{uncompromised } \mathbb{T} \end{matrix} \tag{3}$$

Here the matrices K and L are formed from H by deleting the rows in $\mathbb{S}$ and by retaining the rows in $\mathbb{S}$ respectively. *Note that every element of the vector q is nonzero.* This representation will be useful in the sequel. □

The next result follows immediately from [20].

Theorem 5: Consider the DC power flow model (1). Consider an unobservable attack $\mathcal{A} = (\mathbb{S}, a)$. Construct the matrices K and L from H by deleting the rows in $\mathbb{S}$ and by retaining the rows in $\mathbb{S}$ respectively. Then

(a) $\operatorname{rank}(K) \leq n - 1$

(b) the attack vector a must belong to the subspace:

$$\mathcal{T} = \{a \in \mathbb{R}^{m+n+1} : a = Hx, \quad Kx = 0\}$$

Proof: Let $0 \neq x^a$ is the (unique) *perceived state perturbation* associated with attack $\mathcal{A}$. From Remark 4, we can permute the rows of H to write

$$a = Hx^a = \begin{bmatrix} L \\ K \end{bmatrix} x^a = \begin{bmatrix} q \\ 0 \end{bmatrix}$$

This establishes (b). Also, $Kx^a = 0$, which forces $\operatorname{rank}(K) \leq n-1$, proving (a). We note that while $a \in \mathcal{T}$, not every vector in $\mathcal{T}$ is an admissible attack vector. This is because we also require that every entry of $q = Lx^a$ be nonzero. ■

Unobservable attacks require a high degree of *coordination*. The attack vector must be carefully orchestrated across spatially separated meters, and the attacker must have access to the model. This necessary coordination suggests that low sparsity attacks are more probable as they involve compromising a small number of meters. Low sparsity attacks have been studied in [25], [35].

B. Observable Islands

With every unobservable attack, we can associate a set of *observable islands*. This graph-theoretic construct is central to the results in this paper. Observable islands are disjoint subsets of buses, which share the same perceived change of state [voltage phase] under the attack. More precisely:

Definition 6: Let $\mathcal{A} = (\mathbb{S}, a)$ be an unobservable attack, and let x^a be its associated *perceived* change of system state. Partition the set of buses $\mathbb{V}$ into the disjoint union

$$\mathbb{V} = \mathbb{V}_1 \cup \cdots \cup \mathbb{V}_s, \quad \mathbb{V}_i \cap \mathbb{V}_j = \phi \quad \text{for } i \neq j$$

defined by the equivalence classes

$$v_1, v_2 \in \mathbb{V}_i \iff x^a_{v_1} = x^a_{v_2}$$

The sets $\{\mathbb{V}_i\}_{i=1}^{s}$ are called the *observable islands* associated with the attack $\mathcal{A}$.

Remark 7: We can now offer a geometric picture of unobservable attacks. If an attack $\mathcal{A}$ is unobservable, it must be consistent with the underlying model, and thus corresponds to a *perceived perturbation* in power flow. All non-zero power flows in this perturbed power flow correspond either to compromised sensors or unmetered lines. This perturbation must satisfy power conservation at each bus. It is characterized by the perceived bus phase perturbations x^a. All buses within an observable island have the same perceived voltage angle perturbation, and therefore perceived power flow perturbations on lines *entirely within* any observable island are identically zero. *None* of meters on these lines could have been compromised. Conversely, any line connecting two *distinct observable islands* has a phase difference across it, and must therefore have non-zero perceived power flow perturbation. *All* such lines must either have compromised meters or be unmetered. This observable island characterization is central to our exposition. □

Theorem 8: Consider the unobservable attack $\mathcal{A} = (\mathbb{S}, a)$.

(a) Every compromised line in $\mathbb{S}$ connects distinct observable islands.

(b) Every line that connects distinct observable islands is either unmetered or compromised.

(c) No lines contained within an observable island are compromised.

Proof: Under attack $\mathcal{A}$, we will have perceived real power flow perturbations p_{ij} from bus i to bus j, and bus phase perturbations x^a_i at bus i.

(a) If the line connecting buses i and j is compromised, $p_{ij} \neq 0$ and this requires $x^a_i - x^a_j \neq 0$. Thus, buses i, j must fall in distinct observable islands.

(b) If a line connects buses i, j from distinct observable islands, we must have $x^a_i - x^a_j \neq 0$ which forces $p_{ij} \neq 0$. This implies that the meter on that line is compromised or that the line is unmetered.

(c) Any line connecting buses i, j within an observable island has $x_i^a - x_j^a = 0$ which implies $p_{ij} = 0$. As a result, this line cannot have been compromised.

■

Remark 9: Fix an unobservable attack $\mathcal{A} = (\mathbb{S}, a)$. Its associated observable islands can be found by solving $a = Hx^a$ for the state x^a, and placing buses into equivalence classes according to Definition 6. This requires $O(n^3)$ flops and is numerically sensitive. If all lines are metered, Theorem 8 suggests a robust graph-theoretic algorithm to calculate all connected components corresponding to the observable islands of $\mathcal{A}$: (a) Start with the power system graph $\mathcal{G}$, and delete all compromised lines indexed in $\mathbb{S}$. (b) The observable islands are the resulting connected components of the reduced graph. All connected components of a graph can be found in $O(n+m)$ time using standard breadth-first or depth-first search algorithms [14]. The observable islands of $\mathcal{A}$ *do not depend* on transmission line parameters. They are derived from the interconnection structure of the power system graph. We do not have a graph-theoretic method of constructing observable islands in the case that all lines are not metered. The easiest way appears to be linear algebraic. Solve $y = Hx^a$ for the state perturbation x^a and place buses accordingly in equivalent classes. This method is not robust and suffers from noise issues. Indeed, it may be worth while exploring other notions of islands to allow for small [non-zero] power flow within an island. This is a subject of further research and beyond the scope of this paper. □

III. Characterizations of Sparse Attacks

We now characterize irreducible attacks, and offer an algorithm to find all irreducible attacks that involve the compromise of exactly two power injection meters. We then derive canonical forms for all 3-, 4-, and 5-sparse attacks under the assumption that *all* lines are metered.

A. Irreducible Attacks

Definition 10: An attack $\mathcal{A} = (\mathbb{S}, a)$ is called *irreducible* if it is unobservable and there is no unobservable attack $\mathcal{A}' = (\mathbb{S}', a')$ with $\mathbb{S}' \subsetneq \mathbb{S}$.

We will need the following:

Lemma 11: Let $\mathcal{A} = (\mathbb{S}, a)$ be an irreducible attack. Construct the matrices K and L from H by deleting the rows in $\mathbb{S}$ and by retaining the rows in $\mathbb{S}$ respectively. Then,

$$0 \neq x, Kx = 0 \Longrightarrow all\ entries\ of\ Lx\ are\ nonzero$$

Proof: Assume $\mathcal{A} = (\mathbb{S}, a)$ is irreducible. Without loss of generality, we can permute the rows of H to write

$$H = \begin{bmatrix} L \\ K \end{bmatrix}$$

Suppose there exists $0 \neq x'$ such that $Kx' = 0$ with at least one entry of $p = Lx'$ being zero. Define $a' = Hx'$ and $\mathbb{S}' = \{k : p_k \neq 0\}$. Note that $\mathbb{S}' \subsetneq \mathbb{S}$ (strictly). Then, $\mathcal{A}' = (\mathbb{S}', a')$ is unobservable, contradicting irreducibility of $\mathcal{A}$. ■

We begin by characterizing irreducible attacks:

Theorem 12: Consider the DC power flow model (1). Fix $\mathbb{S}$. Construct the matrices K and L from H by deleting the rows in $\mathbb{S}$ and by retaining the rows in $\mathbb{S}$ respectively. Then, the attack $\mathcal{A} = (\mathbb{S}, a)$ is irreducible $\Longleftrightarrow$

(a) $\operatorname{rank}(K) = n - 1$

(b) For $k = 1, \cdots, |\mathbb{S}|$, $\operatorname{rank}\begin{bmatrix}(e^k)^* L \\ K\end{bmatrix} = n$

(c) $0 \neq a \in \mathcal{T} = \{a \in \mathbb{R}^{m+n+1} : a = Hx, Kx = 0\}$

Proof: Necessity. Suppose $\mathcal{A} = (\mathbb{S}, a)$ is irreducible. As $\mathcal{A}$ is in particular, unobservable, from Theorem 5 we have $\operatorname{rank}(K) \leq n-1$. Assume $\operatorname{rank}(K) \leq n-2$. Then, there exist independent vectors x, y such that $Kx = Ky = 0$. From Lemma 11, we conclude that all the entries of $p = Lx$ and $q = Ly$ are nonzero. Define $z = p_1 y - q_1 x$. As $\{x, y\}$ are independent and $p_1, q_1 \neq 0$, we have $z \neq 0$. Notice that $Kz = 0$. By construction, the first component of Lz is $p_1(Ly)_1 - q_1(Lx)_1 = 0$. Using Lemma 11, this contradicts irreducibility of $\mathcal{A}$, proving (a).

Next, suppose condition (b) is violated. Then, there exists k and $x' \neq 0$ such that

$$\begin{bmatrix}(e^k)^* L \\ K\end{bmatrix} x' = 0$$

Define $p = Lx'$, $a' = Hx'$ and $\mathbb{S}' = \{i : p_i \neq 0\}$. Since $p_k = 0$, we have $\mathbb{S}' \subsetneq \mathbb{S}$. Also, $\mathcal{A}' = (\mathbb{S}', a')$ is unobservable, contradicting irreducibility of $\mathcal{A}$.

From Theorem 5(b), we have that $a \in \mathcal{T}$, proving (c).

Sufficiency. Suppose conditions(a)–(c) hold. Select any $0 \neq a \in \mathcal{T}$. We show that $\mathcal{A} = (\mathbb{S}, a)$ is irreducible.

Since $a \in \mathcal{T}$, we can write $a = Hx, Kx = 0$. Define $q = Lx$. If $q_k = 0$, we have

$$\begin{bmatrix}(e^k)^* L \\ K\end{bmatrix} x = \begin{bmatrix} q_k \\ 0 \end{bmatrix} = 0$$

This violates condition (b). Thus, every entry of q is nonzero. Observe that

$$a = Hx = \begin{bmatrix} L \\ K \end{bmatrix} x = \begin{bmatrix} q \\ 0 \end{bmatrix} \begin{matrix} \}\mathbb{S} \\ \}\mathbb{T} \end{matrix}$$

with every entry of q being nonzero. From Remark 4, $\mathcal{A} = (\mathbb{S}, a)$ is unobservable.

We now show that $\mathcal{A}$ is irreducible. Suppose not. Then, there exists an unobservable attack $\mathcal{A}' = (\mathbb{S}', a')$ with $\mathbb{S}' \subsetneq \mathbb{S}$. Let x' be the corresponding perceived perturbation. Let $\mathbb{M} = \{1, \cdots, m+n+1\}$ denote the set of all meters, and define the complementary sensor sets $\mathbb{T} = \mathbb{M} \setminus \mathbb{S}$, $\mathbb{T}' = \mathbb{M} \setminus \mathbb{S}'$. Note that $\mathbb{T}' \supsetneq \mathbb{T}$. We have

$$a' = Hx' = \begin{bmatrix} L' \\ K' \end{bmatrix} x' = \begin{bmatrix} q' \\ 0 \end{bmatrix} \begin{matrix} \}\mathbb{S}' \\ \}\mathbb{T}' \end{matrix}$$

Since $\mathbb{T}' \supsetneq \mathbb{T}$, we have that K' contains the rows of K. This forces $Kx' = 0$. From (a), every vector in $\mathcal{N}(K)$ has the form αx. Thus $x' = \alpha x$ for some $\alpha \neq 0$. As a result, $a' = Hx' = \alpha Hx = \alpha a$. The nonzero entries of the attack vectors a, a' index compromised sensors, so $\mathbb{S} = \mathbb{S}'$, contradicting the strict containment, proving the claim. ■

```
1  Partition
   $H = \begin{bmatrix} G_2 \\ G_1 \end{bmatrix}$ where $G_2 \in \mathbb{R}^{n \times n}$
   $G_2$ is invertible because the system state can be
   deduced [modulo translations] from
   all injected power observations
2  Compute $Q = G_1 G_2^{-1} \in \mathbb{R}^{(m+1) \times n}$
3  Select any two injection nodes $i > j$
if $i \neq n+1$
4  Define $Q[e^i e^j] = [q^i q^j] \in \mathbb{R}^{(m+1) \times 2}$
   where $e^i, e^j \in \mathbb{R}^n$ are unit vectors
5  Define $\mathbb{I} = \{$row indices $k$ such that $q_k^i \neq q_k^j\}$
6  The only irreducible attacks that compromise
   meters $i$ and $j$ are $\mathcal{A} = (\mathbb{S},\ a)$ where
       $\mathbb{S} = \{i,\ j,\ n+1+\mathbb{I}\}$
       $a = \alpha \begin{bmatrix} (e^i - e^j) \\ (q^i - q^j) \end{bmatrix}, \qquad \neq \alpha \in \mathbb{R}$
if $i = n+1$
4  Define $Qe^j = q^j \in \mathbb{R}^{m+1}$
   where $e^j \in \mathbb{R}^n$ is the $j^{\text{th}}$ unit vector
   (it will happen that $q_1^j = -1$)
5  Define $\mathbb{I} = \{$row indices $k$ such that $q_k^j \neq \ \}$
6  The only irreducible attacks that compromise
   meters $i$ and $j$ are $\mathcal{A} = (\mathbb{S},\ a)$ where
       $\mathbb{S} = \{j,\ n+\mathbb{I}\}$
       $a = \alpha \begin{bmatrix} e^j \\ q^j \end{bmatrix}, \qquad \neq \alpha \in \mathbb{R}$
```

Fig. 1. Algorithm for finding all irreducible attacks involving the compromise of exactly two power injection meters and an arbitrary number of line meters.

B. Attacks Involving 2 Power Injection Meters

Finding all possible irreducible attacks is equivalent to finding *minimal* sets of rows of H whose deletion reduces $\mathrm{rank}(H)$ by one (see Theorem 12). This is a computationally intractable problem even for small power networks. Cyber-attacks involving large numbers of meters are improbable because of the degree of temporal coordination necessary across geographically separated attack points. We therefore focus on *low-sparsity cyber-attacks* that require coordination of a small number of meters.

We first consider irreducible attacks involving the compromise of exactly two power injection meters and an arbitrary number of power meters on lines. Theorem 12 immediately suggests an efficient algorithm offered in Fig. 1 to find all such attacks. Our algorithm uses certain linear algebraic manipulations that bear some resemblance to the procedure in [21] to find all p critical measurement sets in the context of power system observability.

The algorithm exploits the following observations. Consider the DC power flow model (1). As the system is assumed observable, $\mathrm{rank}(H_1) = n$. Using elementary column operations, we can write the power flow model as

$$\begin{array}{r} \text{injection and null buses}\{ \\ \text{line meters}\{ \end{array} \left[\begin{array}{c} y_1 \\ \hline y_2 \end{array}\right] = \left[\begin{array}{cccc} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \\ -1 & -1 & \cdots & -1 \\ \hline q_{11} & q_{12} & \cdots & q_{1n} \\ q_{21} & q_{22} & \cdots & q_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ q_{m1} & q_{m2} & \cdots & q_{mn} \end{array}\right] x$$

All entries of the $(n+1)^{\text{st}}$ row are -1, because the sum of injected powers is zero for all states x. We seek minimal sets of rows of H [two injection meters and an arbitrary number of lines] whose deletion reduces its rank by one. For example, deleting the first two rows of H leaves

$$\begin{bmatrix} 0 & 0 & I_{n-2} \\ -1 & -1 & * \\ q^1 & q^2 & * \end{bmatrix}$$

For this matrix to have rank $n-1$, we must further delete all line meter rows where $q_k^1 \neq q_k^2$. The complete algorithm is offered in Fig. 1.

This algorithm requires $O(n^2 m)$ flops for a power system with n buses and m line meters. For the CAISO 4000 bus system, this can be done in approximately 1 minute on a 3 Ghz PC. The technique can be recursively extended to irreducible attacks involving $k > 2$ power injection meters, but the algorithm complexity is $O(mn!/k!(n-k)!)$, which is disheartening. The attack vector a, which is also specified in the algorithm, must lie in a 1-dimensional subspace as identified in Theorem 12.

C. Canonical Forms

In some future reality, we can imagine that *all* lines on the transmission network are instrumented with power meters.

In this situation, we can offer a graph theoretic characterization of 3-, 4-, and 5-sparse attacks. A *bridge* is an edge whose deletion increases the number of connected components in a graph. We have the following:

Theorem 13: Assume all lines are metered. An irreducible attack $(\mathbb{S}, a)$ is 3-sparse if and only if

(a) $\mathbb{S}$ consists of two adjacent injection buses b_1, b_2 and the line ℓ connecting these buses, and

(b) The connecting line ℓ is a bridge of the power system graph $\mathcal{G}$.

Proof: Let $\mathcal{A}$ be a 3-sparse irreducible attack. This corresponds to some perceived perturbation in power flow (see Remark 7). As this power flow must have a source and a sink, two distinct injection buses b_1, b_2 must be compromised. These buses must be in distinct observable islands. There must exist some path from b_1 to b_2 along which the perceived power flows. As all lines are metered, every edge on that path must be compromised. Since $\mathcal{A}$ is 3-sparse, this path can contain only one edge, i.e. the third compromised sensor must be on a line ℓ connecting b_1, b_2. If there are other lines connecting these islands, they must also be compromised (see Theorem 8). As only three sensors are compromised, no such line can exist, which forces ℓ to be a bridge. Sufficiency is evident from construction. ■

Theorem 14: Assume all lines are metered. An irreducible attack $(\mathbb{S}, a)$ is 4-sparse if and only if

(a) $\mathbb{S}$ consists of two injection buses b_1, b_2 and two lines ℓ_1, ℓ_2.

(b) The injection buses b_1, b_2 are connected by the lines ℓ_1, ℓ_2 via an intermediate bus b_o.

(c) The connecting lines ℓ_1, ℓ_2 are bridges of the power system graph $\mathcal{G}$.

Proof: Let $\mathcal{A}$ be a 4-sparse irreducible attack. This corresponds to some perceived perturbation in power flow (see Remark 7). As this power flow must have a source and a sink, two injection buses b_1, b_2 must be compromised. Since perceived power flows from b_1 to b_2 [or vice-versa], these buses must be in distinct islands. Since the system graph is connected, there must be at least 1 line connecting these islands. This line must also be compromised as all lines are assumed metered. Since $\mathcal{A}$ is 4-sparse, exactly one other meter must be compromised. If this is an injection meter, it must be at a bus b_3 distinct from b_1, b_2 as we assume there is at most one injection meter at any bus. Since perceived power must flow from or to b_3, at least one other line meter must be compromised, making $\mathcal{A}$ have sparsity $\geq$5. Thus, exactly two distinct injection buses b_1, b_2 and two lines ℓ_1, ℓ_2 are compromised.

All paths that carry nonzero perceived power must connect b_1 and b_2 as these are the only compromised injection nodes. As all lines are metered, every edge on these paths must be compromised. Since $\mathcal{A}$ is 4-sparse, these paths contain exactly 2 edges in total. Thus at most two such paths exist. If there were two paths, these contain distinct singleton edges connecting b_1, b_2. This possibility is precluded by our assumption that there is no more than one line between any pair of buses. Thus the perceived power must flow from b_1 to b_2 on a *single* path containing exactly two compromised lines ℓ_1, ℓ_2. Label the intermediate bus b_0. This could be a null bus or an uncompromised injection bus.

Finally, the buses b_0, b_1, b_2 must fall in distinct observable islands as perceived power flows between these buses. Lines ℓ_1 or ℓ_2 connect these islands. If there are other lines connecting these islands, they must also be compromised (see Theorem 8). As only 4 sensors are compromised, no such lines can exist, which forces ℓ_1, ℓ_2 to be bridges. Sufficiency is evident from construction. ■

Theorems 13 and 14 essentially offer *canonical forms* for 3- and 4-sparse irreducible attacks. A more succinct representation of these canonical forms is shown in Fig. 2. Every 3- and 4-sparse irreducible attack must have the structure captured in these canonical forms. For 5-sparse attacks, there are three possible canonical forms, and these are shown in Fig. 3. Armed with these canonical forms, we can readily parse a power system graph to detect the presence of low sparsity unobservable attacks. This involves standard depth-first search methods [7] to find minimal cut-sets. For example, [33] offers a $O(n + m)$ algorithm to find all bridges in a graph. Finding cut-sets consisting of 2 edges [as found in two of the 5-sparse canonical forms] can be done by deleting edges and searching for bridges.

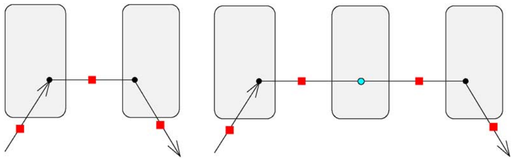

Fig. 2. Canonical forms: 3-sparse (left) & 4-sparse (right) irreducible attacks.

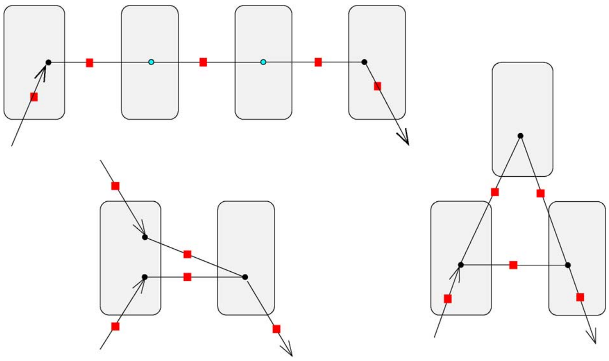

Fig. 3. Three canonical forms for 5-sparse irreducible attacks.

Remark 15: These canonical forms for sparse attacks depend only on the topological properties on the power system graph. Indeed, the current operating point and bus admittance parameters play no role. As a result, these canonical forms represent attacks that are irreducible with respect to a complete *nonlinear* power system model. The attack vector itself must lie on a one-dimensional manifold [as opposed to a *subspace* for the linear DC power flow model (1)]. □

IV. Countermeasures

A. Countermeasures Using Known-Secure PMUs

Consider an arbitrary [not necessarily sparse] collection $\mathbb{A}$ of unobservable attacks. We now consider countermeasures against attacks in $\mathbb{A}$ by placing *known-secure* phase measurement units [PMUs] at certain buses to render these attacks observable. A PMU placed at bus k offers direct measurement of the voltage phase x_k at that bus. PMU's are networked on the newer NASPInet architecture which has been designed for secure data transfer. As a result, attacks that compromise PMU data are much less likely than those that target power meters on the legacy SCADA network. This justifies our assumption of known-secure PMUs. We begin with the following:

Theorem 16: Consider an arbitrary collection of unobservable attacks $\mathbb{A} = \{\mathcal{A}_1, \cdots, \mathcal{A}_p\}$. Let

$$\mathbb{V}_1^k \quad \mathbb{V}_2^k \quad \cdots \quad \mathbb{V}_{s_k}^k$$

denote the observable islands associated with attack $\mathcal{A}_k$.

All attacks in $\mathbb{A}$ can be made observable by placing PMUs at buses $\mathbb{B}$

$$\iff \quad \forall\, k, \exists\, i_1 \neq i_2 : \mathbb{V}_{i_1}^k \cap \mathbb{B} \neq \phi, \mathbb{V}_{i_2}^k \cap \mathbb{B} \neq \phi$$

i.e. every attack has two distinct islands which contain PMUs.

Proof: Consider the observable islands $\mathbb{V}_1^k, \cdots, \mathbb{V}_{s_k}^k$ associated with attack $\mathcal{A}_k$. If attack $\mathcal{A}_k$ occurs, all observable islands must have pair-wise distinct phases. By placing PMUs at buses in *any two distinct islands*, we can monitor their voltage phase difference, rendering attack $\mathcal{A}_k$ observable. ■

Finding the minimal number of PMUs necessary to make the attacks in $\mathbb{A}$ observable is equivalent to the following set-theoretic problem: Given a collection $\mathbb{Q} = \{\mathbb{Q}^j : j = 1, \ldots, n\}$ of sets, find the minimal set $\mathbb{B}$, such that $\mathbb{Q}^j \cap \mathbb{B} \neq \phi$ for all $j = 1, \ldots, n$. This is known as the *hitting set problem* [see [36], p. 451], which is known to be NP-hard. We are able to offer a clean upper bound on the minimal number of PMUs required, and offer an algorithm to determine their placement:

Theorem 17: Consider *any* collection $\mathbb{A} = \{\mathcal{A}_1, \cdots, \mathcal{A}_p\}$ of p unobservable attacks. There exists a set $\mathbb{B}$ containing $p+1$ buses with the following property: if direct measurements of the voltage phase angles at all buses $b_i \in \mathbb{B}$ are available, then the collection of attacks $\mathbb{A}$ becomes observable.

Proof: We construct the set of buses $\mathbb{B}$ at which we place PMUs. Select any buses b_0, b_1 drawn from *distinct* observable islands $\mathbb{V}_i^1$ and $\mathbb{V}_j^1$ associated with $\mathcal{A}_1$ for inclusion in $\mathbb{B}$. This choice renders $\mathcal{A}_1$ observable from Theorem 16. Consider the observable islands associated with attack $\mathcal{A}_2$:

$$\mathbb{V}_1^2 \quad \mathbb{V}_2^2 \quad \cdots \quad \mathbb{V}_{s_2}^2$$

As the union of these islands contains *all* buses, we must have $b_0 \in \mathbb{V}_{k_2}^2$ for some index k_2. Select any bus $b_2 \in \mathbb{V}_k^2$, $k \neq k_2$ for inclusion in $\mathbb{B}$. By construction, we have placed PMUs in two distinct observable islands associated with $\mathcal{A}_2$. Next, consider the observable islands of attack $\mathcal{A}_3$. Again, we must have $b_0 \in \mathbb{V}_{k_3}^3$ for some index k_3. Select any bus $b_3 \in \mathbb{V}_k^3$, $k \neq k_3$ for inclusion in $\mathbb{B}$. PMUs at b_0 and b_3 render $\mathcal{A}_3$ observable. We continue in this fashion and select buses $b_0, b_1, \cdots, b_p$ for inclusion in $\mathbb{B}$. This collection of PMUs makes all the attacks in $\mathbb{A}$ observable, proving the claim. ■

Heuristic procedures can be used to reduce the number of PMUs necessaryto render $\mathbb{A}$ observable. A greedy algorithm for this was proposed in [3]. The placement algorithm of [19] suggests in simulation studies that it requires placing PMUs at about 1/3 the total number of buses to protect the system. We offer an alternative method that exploits the underlying observable island structure. The idea is to select buses at each iteration from the *smallest* observable island. Intuitively, this process is likely to place PMUs that are common to many islands. Our algorithm is detailed in Fig. 4.

```
Given unobservable attacks $\mathbb{A} = \{\mathcal{A}_1, \cdots, \mathcal{A}_p\}$
0   For $k = 1 : p$, find observable islands $\mathbb{V}_i^k$, $i = 1 : s_k$
1   Select an arbitrary bus $b$ for inclusion in $\mathbb{B}$
2   For each $k$, find $i : b \in \mathbb{V}_i^k$
3   Calculate the complement $\mathbb{X}^k = \mathbb{V} - \mathbb{V}_i^k$
    Define $\mathcal{X} = \{\mathbb{X}^1, \cdots, \mathbb{X}^p\}$
while $\mathcal{X} \neq \phi$
4   Find the smallest set $\mathbb{X}^k \in \mathcal{X}$
    Select an arbitrary bus $c \in \mathbb{X}^k$ for inclusion in $\mathbb{B}$
5   Remove all sets from $\mathcal{X}$ that contain $c$
end
```

Fig. 4. Heuristic algorithm for PMU placement.

B. Countermeasures Based on State-Estimation

We now offer a countermeasure strategy based on state-estimation that does not require any hardware investment. It is of use to detect large unobservable attacks where the measurements are compromised at a time scale much faster than the native rate at which loads and generation vary. The essential idea is as follows. Let $x(t)$ denote the trajectory of voltage phases. Under normal system operation $x(t)$ is a slowly varying signal. At the time-scales we are concerned with, we can write $x(t) \approx \text{constant}$. Suppose we have an unobservable attack $\mathcal{A}$, which commences at time t°. Let $\mathbb{V}_1, \cdots, \mathbb{V}_s$ denote the observable islands of $\mathcal{A}$. Define $x(t^\circ) = c$. Under normal operating conditions, $x(t) \approx c$ for a short time interval after the attack commences. Consider any island $\mathbb{V}_k$, and designate an arbitrary reference bus $b \in \mathbb{V}_k$. For all other buses $i \in \mathbb{V}_k$, the phase differences $x_b(t) - x_i(t) = 0$, $t \geq t^\circ$. Equivalently, the voltage angles at all buses within an island translate in unison after an attack. For example, suppose we have two observable islands $\mathbb{V}_1$ and $\mathbb{V}_2$. The voltage angles [prior to the attack] are roughly constant. After the attack, two groups of bus angles evolve together, i.e. for $t \geq t^\circ$ we have

$$x_i(t) = \begin{cases} c_i + a(t) & i \in \mathbb{V}_1 \\ c_i + b(t) & i \in \mathbb{V}_2 \end{cases}$$

We can declare an arbitrary slack bus k, which we place in $\mathbb{V}_1$. Therefore, we observe [equivalently] that for $t \geq t^\circ$,

$$x_i(t) = \begin{cases} d_i & i \in \mathbb{V}_1 \\ d_i + b(t) - a(t) & i \in \mathbb{V}_2 \end{cases}$$

where $d_i = c_i - c_k$. If $q = |\mathbb{V}_2|$ is large, this event of q bus angles *translating in unison is improbable* under normal system operation.

In the general case, we will have a collection of observable islands. After an attack, the voltage angles translate in unison for each island. We place the slack bus in the largest island. State estimation will reveal that collections of states in the other islands translate in union. Define $\gamma(\mathcal{A}) = \text{size}$ of the second largest island. If $\gamma(\mathcal{A}) = 1$, we would observe states of all other [singleton] islands translating, which will not raise any alarms. If however, $\gamma(\mathcal{A})$ is large, say 10, we would observe the states of ten buses translating in union. Thus, $\gamma(\mathcal{A})$ is a natural measure of detectability of the attack. Attacks with very large γ are easily detected. Further research based on change-point detection methods [2] is required to establish a connection between γ and the latency of detecting the attack.

V. Examples

A. 6-bus Illustrative Example

We begin with a synthetic 6-bus example to illustrate unobservable attacks, perceived power flows, the associated observable islands, and our counter measure strategy using known-secure PMUs. Buses 2 and 5 are generator buses, while buses 1, 3,

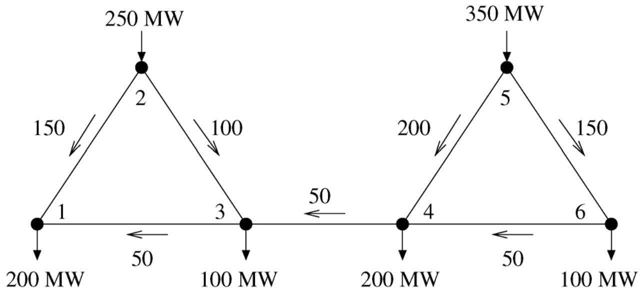

Fig. 5. Power system actual flows before the attack.

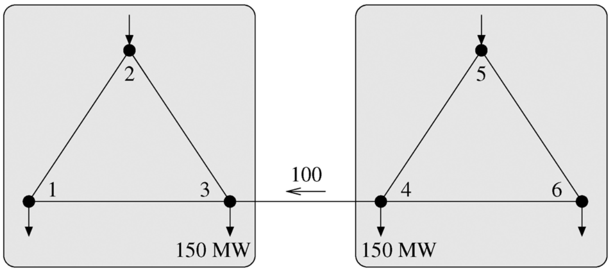

Fig. 6. Power system perceived flows after the attack.

TABLE I
SYNTHETIC 6-BUS EXAMPLE: VOLTAGE PHASE ANGLES

Bus	1	2	3	4	5	6
θ pre	0.01°	7.48°	2.50°	5.02°	15.03°	7.50°
θ post	−0.03°	7.49°	2.51°	7.50°	17.52°	10.01°
θ change	−0.04°	0.01°	0.01°	2.48°	2.49°	2.51°

TABLE II
IEEE TEST CASES WITH 20% OF LINES METERED

# of buses	2 sparse attacks	3 sparse attacks	4 sparse attacks	total attacks	PMUs needed
300	143	17	48	208	55
2383	582	66	37	685	232
2746	247	27	21	295	145

TABLE III
IEEE TEST CASES WITH ALL LINES METERED

# of buses	2 sparse attacks	3 sparse attacks	4 sparse attacks	total attacks	PMUs needed
300	-	51	58	109	55
2383	-	270	210	480	232
2746	-	144	62	206	145

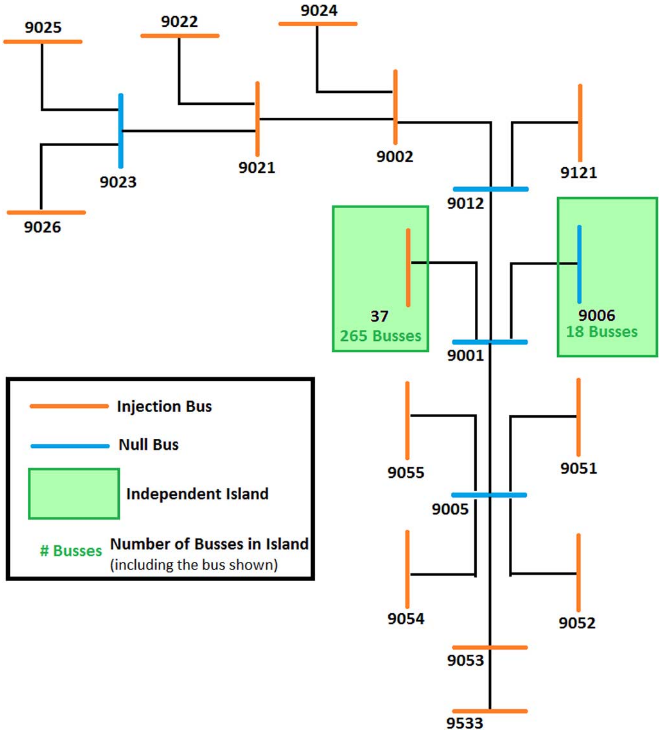

Fig. 7. IEEE 300 bus test case: 19 bus subsystem.

4, and 6 are loads. All line admittances are identical. The generation at bus 5 is less expensive. All power injections/extractions and all line flows are metered. The power flows before the attack are shown in Fig. 5. At a certain time, an attacker compromises the line meter reading on line (3, 4) and the power extraction readings at loads 3, 4. This is done in a *coordinated* fashion so the perceived flows are consistent with the DC power flow model. This consistency renders the attack unobservable. The perceived power flows after the attack are shown in Fig. 6 [only the values that change are shown]. The perceived power flow *perturbation* is a 50 MW flow *from bus 4 to bus 3 along the tie-line (3,4)*. There are two observable islands: $\mathbb{V}_1 = \{1, 2, 3\}$ and $\mathbb{V}_2 = \{4, 5, 6\}$. Notice that there is no perceived power flow *entirely within* any observable island. The system operator estimates the voltage phase angles at all buses before and after the attack. These are tabulated in Table I. Observe that the perceived angle changes are approximately constant within any island. Placing two secure PMUs at a pair of buses, one in each island, will serve as a countermeasure. The recorded phase difference between these PMUs in distinct islands will be ≈ zero which is in conflict with the state estimation results, alerting the system operator to this attack.

B. Irreducible Attacks

We have run our algorithm for finding all irreducible attacks involving *exactly two injection meters* [see Fig. 1] on the 300, 2383, and 2746 IEEE Bus Test Cases. We have done this in two cases: (a) all lines are metered, (b) 20% of the lines [chosen at random] are metered. In each case, we have found the number of 2, 3, and 4 sparse attacks, and an upper bound on the number of PMUs necessary to render these attacks observable. PMUs were placed using our heuristic algorithm [see Fig. 4]. Our results are tabulated below.

From these limited studies, we see that power systems are vulnerable to many sparse unobservable attacks. If only some lines are metered, the number of possible attacks can increase substantially. Sparse attacks can be found quickly, and countermeasures can be developed using known-secure PMUs. These examples suggest that $\approx p/2$ PMUs are needed to render the collection of attacks observable. This is approximately half the sufficient number of PMUs used in the placement algorithm of Theorem 17. For instance, in the 2383 test case with all lines metered, we have identified 480 unobservable attacks with sparsity ≤ 4. Our heuristic algorithm of Fig. 4 places PMUs at 232 select buses to render this collection of attacks observable, while

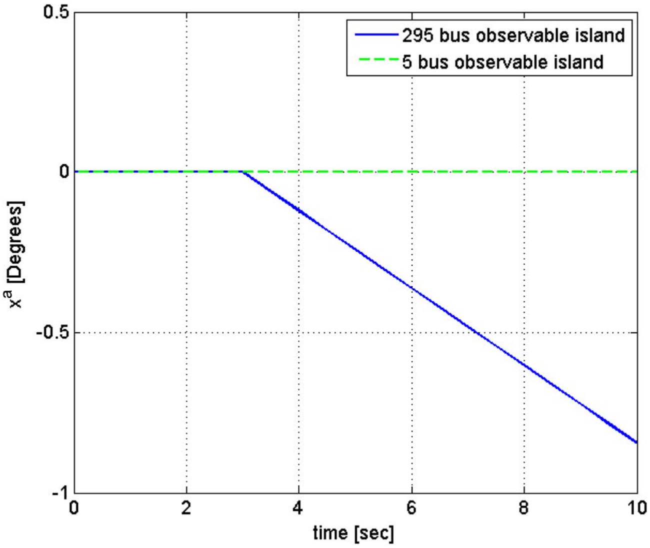

Fig. 8. 3-Sparse attack that compromises injection buses 9021 and 9002. The attack commences at $t = 3$ sec with amplitude increasing at 3 MW/sec.

Theorem 17 offers an upper bound of $p + 1 = 481$ PMUs for this purpose.

C. State Estimation Based Countermeasures

Fig. 7 shows a 19 bus portion of the IEEE 300 bus test case that is particularly prone to unobservable attacks. If all lines and all injection buses were metered then this 19 bus test case would be prone to six 5-sparse, twelve 4-sparse, and four 3-sparse attacks. In particular, we examine the 3-sparse attack that involves injection buses 9021 and 9002. This attack has two observable islands, one containing 5 buses and the other containing 295 buses. The attack begins at $t = 3$ sec, and the attacker gradually increases the amplitude of the attack at 3 MW/sec to evade detection. Fig. 8 shows the state evolution. Notice that two groups of voltage angles [corresponding to the observable islands] evolve in unison. The perceived angle perturbations in the 5 bus island are zero because the [arbitrary] slack bus is contained in this island. This event alerts the system operator of the attack without the investment of additional PMUs.

VI. Conclusions

In this paper, we have introduced and characterized irreducible cyberattacks. We have offered an efficient algorithm to find all irreducible attacks that involve the compromise of exactly two power injection meters. We have derived canonical forms for all 3-, 4-, and 5-sparse attacks under the assumption that all lines are metered. We have offered countermeasures against arbitrary unobservable attacks using known-secure PMUs, and shown that $p + 1$ PMUs are sufficient to disable p attacks.

A significant difficulty in state estimation is the *stale data problem*. Meter readings arrive asynchronously at the state estimator, and the worst case delay may be on the order of 5-10 minutes [including algorithm convergence time]. With such latencies, state estimation may be a poor vehicle to detect cyberattacks. The deeper issue with cybersecurity research relates to grid operations. An attack has consequences only when the grid operator is misled into taking harmful actions based on the compromised data. A comprehensive and realistic analysis of cybersecurity threats to electricity grids must therefore incorporate current operating practice, both under normal and contingency operations. These issues are worthy of future research.

References

[1] A. Abur and A. G. Exposito, *Power System State Estimation: Theory and Implementation*. Boca Raton, FL, USA: CRC Press, 2004.

[2] M. Basseville and I. V. Nikiforov, *Detection of Abrupt Changes: Theory and Application*. Englewood Cliffs, NJ, USA: Prentice-Hall, 1993.

[3] R. B. Bobba, K. M. Rogers, Q. Wang, H. Khurana, K. Nahrstedt, and T. J. Overbye, "Detecting false data injection attacks on DC state estimation," in *Proc. 1st Workshop Secure Control Systems, CPS Week 2010*, Stockholm, Sweden, Apr. 2010, pp. 1–9.

[4] J. Chen and A. Abur, "Placement of PMUs to enable bad data detection in state estimation," *IEEE Trans. Power Syst.*, vol. 21, no. 4, pp. 1608–1615, Apr. 2006.

[5] S. Cui, Z. Han, S. Kar, T. T. Kim, H. V. Poor, and A. Tajer, "Coordinated data injection attack and detection in smart grid," *IEEE Signal Process. Mag.*, vol. 29, no. 5, pp. 106–115, 2012.

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

[7] S. Dasgupta, C. Papadimitriou, and U. Vazirani, *Algorithms*. NewYork, NY, USA: McGrawHill, 2006.

[8] Department of Energy. [Online]. Available: http://www.oe.energy.gov/DocumentsandMedia/02-1-11_OE_Press_Release_Risk_Management.pdf

[9] R. Emami and A. Abur, "Robust measurement design by placing synchronized phasor measurements on network branches," *IEEE Trans. Power Syst.*, vol. 25, no. 1, pp. 38–43, Feb. 2010.

[10] T. Flick and J. Morehouse, "Securing the smart grid: Next generation power grid security," in *Proc. Syngress*, Amsterdam, The Netherlands, 2010.

[11] A. Giani, E. Bitar, M. Garcia, M. McQueen, P. Khargonekar, and K. Poolla, "Smart grid data integrity attacks: Characterizations and countermeasures," in *Proc. 2nd IEEE Int. Conf. Smart Grid Communications (SmartGridComm)*, 2010, pp. 232–237.

[12] D. Gorinevsky, S. Boyd, and S. Poll, "Estimation of faults in DC electrical power system," in *Proc. IEEE Conf. Decision Contr.*, Dec. 2009, pp. 4334–4339.

[13] G. P. Granelli and M. Montagna, "Identification of interacting bad data in the framework of the weighted least square method," *Electric Power Syst. Res.*, vol. 78, no. 5, pp. 806–814, 2008.

[14] J. Hopcroft and R. Tarjan, "Efficient algorithms for graph manipulation," *Commun. ACM*, vol. 16, no. 6, pp. 372–378, 1973.

[15] C.-H. Huang, C.-H. Lee, K.-R. Shih, and Y.-J. Wang, "Bad data analysis in power system measurement estimation," *Eur. Trans. Electr. Power*, vol. 20, pp. 1082–1100, 2010.

[16] H.-J. Koglin, T. Neisius, G. Beissler, and K. D. Schmitt, "Bad data detection and identification," *Int. J. Electric Power*, vol. 12, no. 2, pp. 94–103, 1990.

[17] V. Igure, S. Laughtera, and R. Williams, "Security issues in SCADA networks," *Comput. Security*, vol. 25, no. 7, pp. 498–506, 2006.

[18] G. N. Korres *et al.*, "Numerical observability analysis based on network graph theory," *IEEE Trans. Power Syst.*, vol. 18, no. 3, pp. 1035–1045, 2003.

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

[20] O. Kosut, L. Jia, R. Thomas, and L. Tong, "Malicious data attacks on smart grid state estimation: Attack strategies and counter measures," in *Proc. 1st IEEE Int. Conf. Smart Grid Commun. (SmartGridComm)*, 2010, pp. 220–225.

[21] J. London, J. B. A. L. Alberto, and N. Bretas, "Network observability: Identification of the measurements redundancy level," in *Proc. Power Syst. Technol. Conf.*, 2000, vol. 2, pp. 577–582.

[22] Q. Li, R. Negi, and M. D. Ilíc, "Phasor measurement units placement for power system state estimation: A greedy approach," in *Proc. IEEE Power Energy Soc. General Meeting*, 2011, pp. 1–8.

[23] K.-P. Lien *et al.*, "Transmission network fault location observability with minimal PMU placement," *IEEE Trans. Power Del.*, vol. 21, no. 3, pp. 1128–1136, 2006.

[24] J. Lin and H. Pan, "A static state estimation approach including bad data detection and identification in power systems," in *Proc. IEEE Power Energy Society General Meeting*, 2007, pp. 1–7.

[25] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," in *Proc. 16th ACM Conf. Comput. Commun. Security*, 2009, pp. 21–32.

[26] L. Mili, T. Van Cutsem, and M. Ribbens-Pavella, "Bad data identification methods in power systems state estimation," *IEEE Trans. Power Apparatus Syst.*, vol. 103, no. 11, pp. 3037–3049, 1985.

[27] N. M. Manousakis and G. N. Korres, "Observability Analysis for Power Systems Including Conventional and Phasor Measurements," in *Proc. 7th Mediterranean Conf. Power Generation, Transmission, Distribution Energy Conversion*, 2010, pp. 1–8.

[28] A. Monticelli*, State Estimation in Electric PowerSystems: A Generalized Approach*. New York, NY, USA: Springer, 1999.

[29] NIST Framework and Roadmap for Smart Grid Interoperability Standards, "NIST Special Publication 1108,", Jan. 2010.

[30] [Online]. Available: http://www.naspi.org/naspinet.stm

[31] T. J. Overbye and J. D. Weber, "The smart grid and PMUs: Operational challenges and opportunities," in *Proc. IEEE Power Energy Soc. General Meeting*, 2010, pp. 1–5.

[32] A. G. Phadke, J. S. Thorp, and K. Karimi, "State estimation with phasor measurements," *IEEE Trans. Power Syst.*, vol. 1, pp. 233–241, 1986.

[33] R. Tarjan, "A note on finding the bridges of a graph," in *Proc. Inf. Process. Lett.*, Apr. 1974, pp. 160–161.

[34] A. Teixeira, S. Amin, H. Sandberg, K. H. Johansson, and S. S. Sastry, "Cyber-security analysis of state estimators in electric power systems," in *Proc. IEEE Conf. Decision Contr.*, 2010, pp. 5991–5998.

[35] A. Teixeira, G. Dan, H. Sandberg, and K. H. Johansson, "A Cyber Security Study of a SCADA Energy Management System," ArXiv e-prints, 2010.

[36] D. P. Williamson, "The primal-dual method for approximation algorithms," *Math Programming Series B*, vol. 91, pp. 447–478, 2002.

[37] H. Wu, "PMU impact on state estimation reliability for improved grid security," in *Proc. IEEE Transm. Distrib. Conf. Exhibition, PES*, 2006, vol. 25, no. 1, pp. 1349–1351.

Annarita Giani received the M.S. degree in mathematics from the Universitá di Pisa, Pisa, Italy. She received a Ph.D from the Thayer School of Engineering at Dartmouth College, Hanover with a dissertation on computer security, anomaly tracking and cognitive attacks.

She then worked for the Italian Registration Authority and for the Instituto di Informatica e Telematicadel Consiglio Nazionale delle Ricerche di Pisa. After graduation she was a researcher at the Institute for Security Technology Studies. From 2007 she was a postdoctoral fellow at the Department of Electrical Engineering and Computer Science, University of California at Berkeley, CA, USA. She is currently a Director's Fellowship at Los Alamos National Laboratory, NM, USA, where she works on issues related to cyber security of smart grid. Her research interests include computer security, cyber physical systems and critical infrastructure protection.

Eilyan Bitar received the B.S. and Ph.D. degrees from the University of California, Berkeley, CA, USA, in 2006 and 2011, respectively.

He is currently an Assistant Professor and the David D. Croll Sesquicentennial Faculty Fellow in the School of Electrical and Computer Engineering at Cornell University, Ithaca, NY, USA. Prior to joining Cornell in the Fall 2012, he was engaged as a Postdoctoral Fellow in the department of Computing and Mathematical Science (CMS) at the California Institute of Technology and at the University of California, Berkeley, in Electrical Engineering and Computer Science during the 2011-12 academic year. His research interests include stochastic optimization and control theory and their applications to the economics, control, and protection of electric power systems.

Manuel Garcia is a second year graduate student in Mechanical Engineering at the University of California, Berkeley, CA, USA, working in the Berkeley Center for Control and Identification (BCCI).

His general research interests include optimization, nonlinear analysis and control, and uncertainty quantification. His power systems interests include cyber security, fast state estimation, and optimal resource scheduling.

Miles McQueen is a Chief Scientist in the Cyber Security RD department at Idaho National Laboratory (INL). Miles has held a variety of technical and programmatic leadership roles at INL, and has also been Director of the University of Idaho's Computer Science Program at the Idaho Falls Center for Higher Education.

With well over 40 peer reviewed scientific publications, he is currently leading research teams investigating various aspects of the security eco system related to critical infrastructure, and developing novel mitigations for currently unidentified vulnerabilities. Previously, he investigated novel, first of a kind, Zero-Day vulnerability estimation techniques.

Pramod Khargonekar received the B.Tech. degree in electrical engineering from the Indian Institute of Technology, Bombay, India, in 1977, the M.S. degree in mathematics, and the Ph.D. degree in electrical engineering from the University of Florida, Gainesville, FL, USA, in 1980 and 1981, respectively.

After holding faculty positions in Electrical Engineering at the University of Florida and University of Minnesota, he joined The University of Michigan in 1989 as Professor of Electrical Engineering and Computer Science. He became Chairman of the Department of Electrical Engineering and Computer Science in 1997 and also held the position of Claude E. Shannon Professor of Engineering Science. In July 2001, he rejoined the University of Florida and served as Dean of the College of Engineering from till July 2009. He is currently Eckis Professor Electrical and Computer Engineering at the University of Florida.

Kameshwar Poolla received the B.Tech. degree from the Indian Institute of Technology, Bombay, India, in 1980, and the Ph.D. degree from the University of Florida, Gainesville, FL, USA, in 1984, both in electrical engineering.

He has served on the faculty of the University of Illinois, Urbana, IL, USA, from 1984 to 1991. Since then, he has been at the University of California, Berkeley, CA, USA, where he is the Cadence Distinguished Professor of Mechanical Engineering and Electrical Engineering and Computer Sciences. He also serves as the Founding Director of the IMPACT Center for Integrated Circuit manufacturing at the University of California. He co-founded On Wafer Technologies which offers metrology based yield enhancement solutions for the semiconductor industry. On Wafer was acquired by KLA-Tencor in 2007.

Dr. Poolla has been awarded a 1988 NSF Presidential Young Investigator Award, the 1993 Hugo Schuck Best Paper Prize, the 1994 Donald P. Eckman Award, the 1998 Distinguished Teaching Award of the University of California, the 2005 and 2007 IEEE TRANSACTIONS ON SEMICONDUCTOR MANUFACTURING BEST PAPER PRIZES, and the 2009 IEEE CSS Transition to Practice Award. His current research interests covers many aspects of the Smart Grid: Renewable Integration, Demand Response, Cybersecurity, Experimental Economics, and Sensor Networks.