Towards a Unified Resilience Analysis: State Estimation against Integrity Attacks

Duo Han¹, Yilin Mo³, Lihua Xie³
1. Nanyang Technological University, Singapore
E-mail: {dhanaa, ylmo, elhxie}@ntu.edu.sg

Abstract: We consider the problem of resilient state estimation in the presence of integrity attacks. There are m sensors monitoring the state and p of them are under attack. The sensory data collected by the compromised sensors can be manipulated arbitrarily by the attacker. The classical estimators such as the least squares estimator may not provide a reliable estimate under the so-called (p, m)-sparse attack. In this work, we are not restricting our efforts in studying whether any specific estimator is resilient to the attack or not, but instead we aim to present the generic sufficient and necessary conditions for resilience by considering a general class of convex optimization based estimators. The sufficient and necessary conditions are shown to be tight, with a trivial gap. We further specialize our result to scalar sensor measurements case and present some conservative but verifiable results for practical use. Experimental simulations tested on the IEEE 14-bus test system validate the theoretical analysis.

Key Words: Cyber-physical security; resilient estimation; integrity attack; convex optimization

1 Introduction

Cyber-physical systems [1–3] have been widely employed in various areas such as manufacturing processes, civil transportation or military infrastructures. Security is always a paramount issue for real applications. Therefore, cyber-physical security has been a hot research topic in last decades [4–9] since the first Supervisory Control And Data Acquisition (SCADA) system malware (called Stuxnet) was discovered. This article is concerned with the integrity attacks in sensor networks which are widely embedded in various industrial systems such as smart grid or SCADA systems [1]. During the integrity attack, the adversary can take full control of a subset of sensors and arbitrarily manipulate their measurements. The motivations for launching such an attack in industrial systems include creating arbitrage opportunities in electricity market, stealing gas or oil without being noticed, posing potential threat to national defense, etc.

We focus on the problem of resilient estimation against compromised sensory data in order to mitigate the damage caused by the integrity attack. Resilience for an estimator is urgently needed since quite a number of the commonly used estimators under attack fail to give a reliable estimate and thus lead to poor system performance. For instance, a linear estimator is not resilient since one bad measurement is enough to ruin the final estimate. A better estimator may be the geometric median of all measurements [10]. To be concrete, we consider the problem of estimating a vector state \( x \in \mathbb{R}^n \) from measurements collected by m sensors, where the measurements are subject to any random noise. For practical reasons, the spatially distributed sensors cannot be fully guaranteed to be secure. Some of them may be controlled by the attacker and due to the resource limitation the attacker can only attack up to \( p < m \) sensors. Without posing any restrictions on the attacker, we assume that the compromised sensory data can be arbitrarily changed.

Related Work: A quite similar problem in the context of power systems is bad data detection, which has been studied over the past decades [11, 12]. The method of checking the magnitude of residue is useful for identifying random bad data or outliers but may not work for intentional integrity attacks [4, 13]. For example, Liu et al. [14] successfully showed that a stealthy attack changing the state while not being detected is possible. Kim et al. [15] studied a so-called framing attack. Under such a attack, the bad data detector is misled to delete those critical measurements, without which the network is unobservable and a convert attack may be launched. Mo and Sinopoli [7] studied a scalar state estimation problem with integrity attacks. The result that the estimator should discard all measurements if less than half the sensors are secure is actually a special case of our work as we will see later.

For dynamical systems, resilient or robust estimation often refers to dealing with system modelling uncertainties [16–18]. Detecting malicious components via fault detection and isolation based methods has also been extensively studied in [2, 19, 20]. However, in the closely related work [19], the system is assumed to be noiseless, which greatly favors the fault detector. Pajic et al. [21] improved the work by considering the systems with bounded noise. On the top of sufficient conditions for exact recovery in noiseless case, they showed that the worst error is still bounded even under attack. However, their estimator is based on a combinatorial optimization problem, which in general is computational hard to solve and may not be applicable for large scale systems.

Motivated by different behaviours of various estimators under the integrity attacks, we target for proposing a unified resilience analysis framework integrating most commonly used estimators. In this work we consider static state estimation which has wide applications such as power systems and smart grid. Moreover, the main results introduced later provide fundamental insights on the counterpart for the dynamical systems which we are still investigating. We now summarize our main contributions as follows.

1) We integrate most commonly used estimators in a generic form of convex optimization based estimators and conduct the resilience analysis over a large class of estimators. To the best of our knowledge, this is the
first time to study the cyber-physical security problem in a unified approach rather than focus on a concrete estimator.

2) By formally defining the resilience of an estimator, we derive the tight necessary and sufficient conditions (with a trivial gap) on the resilience of such a general estimator. The paramount significance of this work is that the novel analytical methodology presented in this manuscript can be used for characterizing and designing a specific resilient estimator in the presence of compromised sensory data.

3) From a practical point of view, we also provide some conservative but verifiable sufficient and necessary conditions for the resilience of the estimator in the scalar measurement case.

4) Besides the theoretical contributions, we also demonstrate numerical experiments on the IEEE 14-bus test system and validate the analytical results.

The rest of the paper is organized as follows. In Section 2 we formulate the resilient estimation problem. Our main results on the resilience of a general convex optimization based estimator is presented in Section 3. We specialize our results for scalar sensor case in Section 4. The simulation results and concluding remarks are given in Section 5 and 6.

2 Problem Setup

2.1 System Model

Assume that $m$ sensors are measuring the state $x$ and the measurement equation for the $i$th sensor is given by

$$z_i = H_i x + w_i,$$  \hspace{1cm} (1)

where $x \in \mathbb{R}^n$ is the state of interest, $z_i \in \mathbb{R}^{m_i}$ is the “true” measurement collected by the $i$th sensor, and $w_i \in \mathbb{R}^{m_i}$ is the measurement noise for the $i$th sensor. The measurement matrix $H \triangleq [H_1^T, H_2^T, \ldots, H_m^T]^T \in \mathbb{R}^{(\sum_i m_i) \times n}$ is assumed to be observable, i.e., $H$ is full column rank.

Remark 1. Though we consider static state estimation here, the proposed methodology and the derived analytical results in the sequel provide quite a fundamental understanding of the resilience of estimators. They can be extended to the case of dynamical systems in some elegant way like \cite{19}, i.e., by setting a finite (not necessarily large) window for the filter such that the stacked observation matrix is observable and then transforming the resilient filtering problem into the framework here. Thus dynamical state estimation is beyond the scope of this paper. Interested readers can refer to \cite{22} for our preliminary work on the dynamical state estimation.

In the presence of attacks, the measurement equation can be written as

$$y_i = z_i + a_i = H_i x + w_i + a_i,$$  \hspace{1cm} (2)

where $y_i \in \mathbb{R}^{m_i}$ is the “manipulated” measurement and $a_i \in \mathbb{R}^{m_i}$ is the attack vector. In other words, the attacker can change the measurement of the $i$th sensor by $a_i$. Denote $z = [z_1^T, z_2^T, \ldots, z_m^T]^T$, $y = [y_1^T, y_2^T, \ldots, y_m^T]^T$, $w = [w_1^T, w_2^T, \ldots, w_m^T]^T$, $a = [a_1^T, a_2^T, \ldots, a_m^T]^T$.

Denote the index set of all sensors as $\mathcal{S} \triangleq \{1, 2, \ldots, m\}$. For any index set $\mathcal{I} \subseteq \mathcal{S}$, define the complement set to be $\mathcal{I}^c \triangleq \mathcal{S} \setminus \mathcal{I}$. In our attack model, we assume that the attacker can only compromise at most $p$ sensors but can arbitrarily choose $a_i$. With no assumptions on any attack patterns or any fault detection mechanisms, we are keen on the fundamentals of inherent resilience of the state estimators.

Formally, a $(p, m)$-sparse attack can be defined as follows:

Definition 1 ($(p, m)$-sparse attack). A vector $a$ is called a $(p, m)$-sparse attack if there exists an index set $\mathcal{I} \subset \mathcal{S}$, such that:

(i) $\|a_i\| = 0$, $\forall i \in \mathcal{I}$;

(ii) $|\mathcal{I}| \leq p$.

Define the collection of all possible index sets of malicious sensors as $\mathcal{C} \triangleq \{\mathcal{I} : \mathcal{I} \subset \mathcal{S}, |\mathcal{I}| = p\}$. The set of all possible $(p, m)$-sparse attacks is denoted as $\mathcal{A} \triangleq \bigcup_{\mathcal{I} \in \mathcal{C}} \{a : \|a_i\| = 0, i \in \mathcal{I}^c\}$.

The main task of this work is to investigate the sufficient and necessary conditions for an estimator to be resilient to $(p, m)$-sparse attacks. To this end, we first formally define the resilience of an estimator.

Definition 2 (Resilience). An estimator $g : \mathbb{R}^{\sum_i m_i} \mapsto \mathbb{R}^n$ which maps the measurements $y$ to a state estimate $\hat{x}$ is said to be resilient to the $(p, m)$-sparse attack if it satisfies the following condition:

$$\|g(z) - g(z + a)\| \leq \mu(z), \forall a \in \mathcal{A},$$  \hspace{1cm} (3)

where $\mu : \mathbb{R}^{\sum_i m_i} \mapsto \mathbb{R}$ is a real-valued mapping on $z$.

The resilience implies that the disturbance on the state estimate caused by an arbitrary attack is bounded. It is worthwhile to notice that a trivial resilient estimator is $g(y) = 0$ which provides very poor estimate. Therefore, another desirable property for an estimator is translation invariance, which is defined as follows:

Definition 3 (Translation invariance). An estimator $g$ is translation invariant if $g(y + Hu) = u + g(y)$, $\forall u \in \mathbb{R}^n$.

Remark 2. Notice that if an estimator is resilient and translation invariant, then

$$\|g(z) - g(z + a)\| = \|x + g(w) - x - g(w + a)\| = \|g(w) - g(w + a)\| \leq \mu(w).$$

Therefore, the maximum bias that can be injected by an adversary is only a function of the noise $w$.

In the next subsection, we propose a generic convex optimization based estimator which is translation invariant.

2.2 A Generic Convex Estimator

A large variety of estimators are developed by the research community to solve the state estimation problem. In order to achieve greater generality, we first propose a general convex optimization based estimator. We then show that many estimators can be rewritten in this general framework.

The generic estimator that we study in this paper is assumed to have the following form:

$$\hat{x} = g(y) = \arg\min_{\hat{x}} \sum_{i \in \mathcal{I}} f_i(y_i - H_i \hat{x}),$$  \hspace{1cm} (4)

where the following properties of function $f_i : \mathbb{R}^{m_i} \mapsto \mathbb{R}$ are assumed:
(i) $f_i$ is convex.
(ii) $f_i$ is symmetric, i.e., $f_i(u) = f_i(-u)$.
(iii) $f_i$ is non-negative and $f_i(0) = 0$.

**Remark 3.** One can view $y_i - H_i \hat{x}$ as the residue for the $i$th sensor and $f_i$ as a cost function. The convex constraints on $f_i$ ensure that the minimization problem can be solved in an efficient (possibly also distributed) fashion. The symmetric assumption on $f_i$ is typically true for many practically used estimator and can actually be relaxed. By the first two assumptions, the function $f_i$ will achieve minimum at 0. Therefore, without loss of generality, we can assume that the last assumption holds by adding a constant to $f_i$ to ensure $f_i(0) = 0$ and $f_i(x) \geq 0$.

It is easy to check that the estimation (4) is translation invariant. In fact, if $\hat{x}^* = g(y)$, then
\[ g(y + Hu) = \arg \min_{\hat{x}} \sum_{i \in S} f_i [y_i - H_i(\hat{x} - u)], \]
which implies that $g(y + Hu) - u = \hat{x}^*$.

We now take several commonly used estimators as examples and show that they can be written as (4).

(a) Least Square Estimator (LSE):
\[ \hat{x} = \arg \min_{\hat{x}} \sum_{i \in S} \| y_i - H_i \hat{x} \|_2, \]  
(5)

(b) The following is designed to minimize the sum of the $l_p$ norm of the residue, with a little abuse of the notation $p$:
\[ \hat{x} = \arg \min_{\hat{x}} \sum_{i \in S} \| y_i - H_i \hat{x} \|_p. \]  
(6)

The optimal estimate in the case where $p = 2$, $m_i = n$ and $H_i = 1_{n_i}$, $\forall i$ is the geometric median of all $y_i$’s, which is called an $L_1$ estimator in [10]. In other words, $\hat{x}$ is the point in $\mathbb{R}^n$ that minimizes the sum of Euclidean distances from $y_i$ to that point.

(c) Pajic et al. [21, 23] proposed the following resilient estimator in the presence of integrity attack:
\[ \text{minimize} \quad \| [\| a_1 \|_2 \cdots \| a_m \|_2 ] ^\top \|_0 \]
\[ \text{subject to} \quad y_i = H_i \hat{x} + w_i + a_i, \quad w \in \Omega, \]
where $w = [w_1^\top, \ldots, w_m^\top]^\top$ and the authors assume that the noise is bounded and lies in a convex set $\Omega$. However, this minimization problem involves zero-norm, and thus is difficult to solve in general. A commonly adopted approach is to use $L_1$ relaxation to approximate zero-norm, which leads to the following minimization problem:
\[ \text{minimize} \quad \sum_{i \in S} \| a_i \|_2 \]
\[ \text{subject to} \quad y_i = H_i \hat{x} + w_i + a_i, \quad w \in \Omega. \]  
(7)

Assuming that $\Omega$ can be written as a product set $\Omega = \Omega_1 \times \cdots \times \Omega_m$, then the constraint on $w$ can be decoupled as $w \in \Omega \iff w_i \in \Omega_i, \forall i$.

By the convexity of $\Omega$, each $\Omega_i$ must also be convex. We can define the following function
\[ f_i(r) \triangleq \min_{r - a_i \in \Omega_i} \| a_i \|_2. \]  
(8)

As a result, the relaxed minimization problem can be written as
\[ \hat{x} = \arg \min_{\hat{x}} \sum_{i \in S} f_i(y_i - H_i \hat{x}). \]  
(9)

(d) Similarly to the previous example, we can consider the following LASSO [24] estimator:
\[ \text{minimize} \quad \| u \|_2 + \lambda \| a \|_1 \]  
subject to \[ y = H \hat{x} + w + a. \]  

If we define the following function:
\[ f(r) \triangleq \min_{a_i} \| r - a_i \|_2^2 + \lambda \| a \|_1 \]  
(10)

Then one can easily prove that the optimization problem (10) can be rewritten as
\[ \hat{x} = \arg \min_{\hat{x}} \sum_{i \in S} f_i(y_i - H_i \hat{x}). \]  
(12)

In the next section, we shall present sufficient and necessary conditions for the resilience of the general estimator (4). Since (5), (6), (7) and (10) are all special cases of (4), we can easily analyze their individual resilience.

### 3 Resilience Analysis for a Generic Estimator

This section is devoted to the derivation of necessary and sufficient conditions for the resilience of the general estimator. Denote the compact set $\mathcal{U} \triangleq \{ u \in \mathbb{R}^n : \| u \| = 1 \}$. Before proceeding to the main results, we need the following lemma. The proof is omitted here.

**Lemma 1.** Let $q : \mathbb{R} \to \mathbb{R}$ be a convex function and $q(0) = 0$, then $q(t)/t$ is monotonically non-decreasing on $t \in \mathbb{R}^+$. Moreover,
\[ q(t + 1) - q(t) \geq q(t)/t. \]  
(13)

As a consequence of the convexity of $f_i(tH_iu)$ in terms of $t$ and Lemma 1, we know that $f_i(tH_iu)/t$ is monotonically non-decreasing on $t \in \mathbb{R}^+$. As a result, there are only two possibilities:
(i) $f_i(tH_iu)/t$ is bounded for all $i$ and for all $u$, which implies that the limit $\lim_{t \to \infty} f_i(tH_iu)/t$ exists.
(ii) $f_i(tH_iu)/t$ is unbounded for some $i$ and $u$.

The next lemma provides several important properties for the case where $\lim_{t \to \infty} f_i(tH_iu)/t$ exists, whose proof is reported in the appendix:

**Lemma 2.** If the following limit is well defined, i.e., finite, for all $u \in \mathbb{R}^n$:
\[ \lim_{t \to \infty} f_i(tH_iu)/t = C_i(u), \]  
(14)

then the following statements are true:
\( C_i(\alpha u) = |\alpha| C_i(u) \) and \( C_i(u_1 + u_2) \leq C_i(u_1) + C_i(u_2) \).

(ii) Define the function \( h_i(u, v, t) : \mathbb{R}^n \times \mathbb{R}^{m_i} \times \mathbb{R} \mapsto \mathbb{R} \),

\[
h_i(u, v, t) \triangleq \frac{1}{t} \left[ f_i(v + tH_i u) - f_i(v) \right].
\]

Then the following pointwise limits hold:

\[
\lim_{t \to \infty} h_i(u, v, t) = C_i(u).
\]

Moreover, the convergence is uniform on any compact set of \((u, v)\).

(iii) For any \( v \) and \( u \), we have that

\[
f_i(v + H_i u) - f_i(v) \leq C_i(u).
\]

Remark 4. Intuitively speaking, one can interpret \( f_i \) as a potential function and the derivative of \( f_i \) as the force generated by sensor \( i \) (if it is differentiable). By (17), we know that the force from the potential function \( f_i \) along the direction cannot exceed \( C_i(u) \) or \( C_i(u)/\|u\| \) to normalize. On the other hand, Equation (16) implies that this bound is tight.

Before we present our main results, we give a simple example to provide some insights.

Example 1. Suppose that three sensors are measuring a scalar \( x \) and each measurement is also a scalar. We use the estimator in (6) with \( l_1 \) norm. The optimal estimate is the minimizer of \( \sum_{i=1}^{3} |yi - \hat{x}| \). It is straightforward to see the optimal estimate is the median of \( \{y_1, y_2, y_3\} \) if \( H = [1 \ 1 \ 1]^T \). No matter which single measurement is manipulated, the estimate equals to the second measurement and cannot be arbitrarily driven. If \( H = [3 \ 1 \ 1]^T \), the optimal estimate \( \hat{x} \) is \( y_1/3 \). The estimate may be arbitrarily large when the first sensor corresponding to \( H_1 \) is 3 is manipulated. Under the force analogy, the force of the first sensor is \( 3 > 1 + 1 \) and that means the estimate can be dominated by the first sensor measurement. Thus it is not resilient to \((1,3)\)-sparse attacks.

Furthermore, it is not hard to show that the estimator in (6) is not resilient to \((2,3)\)-sparse attacks for any \( H \).

We now give the sufficient condition for the resilience of the estimator.

Theorem 1 (Sufficient condition). If the following conditions hold:

1) \( C_i(u) \) is well defined for all \( u \in \mathbb{R}^n \) and all \( i \in S \);
2) the following inequality holds for all non-zero \( u \):

\[
\sum_{i \in I} C_i(u) < \sum_{i \in I} C_i(u), \quad \forall I \in \mathcal{C},
\]

then the estimator \( g \) is resilient.

Proof. Our goal is to prove that there exists a \( \beta(z) \) where \( \beta : \mathbb{R} \to \mathbb{R} \), such that for any \( t \geq \beta(z), \|u\| = 1, a \in A \), the following inequality holds:

\[
\sum_{i \in S} f_i(y_i - H_i \times t u) \leq \sum_{i \in S} f_i(y_i - (t + 1) H_i u).
\]

As a result, any point \( \|\hat{x}\| \geq \beta(z) + 1 \) cannot be the solution of the optimization problem since there exists a better point \( (\|\hat{x}\| - 1)\hat{x}/\|\hat{x}\| \). Therefore, we must have \( \|g(y)\| \leq \beta(z) + 1 \) and hence the estimator is resilient.

Suppose the set of malicious sensors is \( I \), to prove (19), we will first look at benign sensors. Due to the uniform convergence of \( h_i(u, v, t) \) to \( C_i(u) \) on \( U \times \{-1, 1\} \) shown in Lemma 2, given any \( \delta > 0 \) we can always find a finite constant \( N_i(z, \delta) \) where \( N_i : \mathbb{R}^{m_i} \times \mathbb{R} \to \mathbb{R} \) such that for all \( t \geq N_i(z, \delta) \), the following inequality holds:

\[
h_i(-z_i, u, t) = \frac{1}{t} \left[ f_i(tH_i u - z_i) - f_i(-z_i) \right] \geq C_i(u) - \delta.
\]

for any \( \|u\| = 1 \). By (13), we can derive that

\[
f_i((t + 1)H_i u - z_i) - f_i(tH_i u - z_i) \geq C_i(u) - \delta.
\]

We fix \( \delta \) to be

\[
\delta = \frac{1}{m} \min_{\|u\|=1} \min_{I \in \mathcal{C}} \left( \sum_{i \in I} C_i(u) - \sum_{i \in I} C_i(u) \right).
\]

and take \( \beta(z) \) in the form: \( \beta(z) = \max_{1 \leq i \leq m} N_i(\delta, z_i) \). Notice that we write \( \min_{\|u\|=1} \) instead of \( \inf_{\|u\|=1} \) since \( C_i(u) \) is continuous and the set \( \{u : \|u\|=1\} \) is compact. Hence, the infimum is achievable, which further proves that \( \delta > 0 \) is strictly positive. Hence, for \( i = 1, \ldots, m \), if \( t > \beta(z) \) we have

\[
f_i((t + 1)H_i u - z_i) - f_i(tH_i u - z_i) \geq C_i(u) - \delta, \forall \|u\| = 1.
\]

Since for good sensors, \( z_i = y_i \), we know that

\[
\sum_{i \in I} \left[ f_i((t + 1)H_i u - z_i) - f_i(tH_i u - z_i) \right] \geq \sum_{i \in I} C_i(u) - (m - p) \delta, \forall \|u\| = 1.
\]

We now consider malicious sensors. By Lemma 2 (iii), we know that for \( i \in \mathcal{I} \), and any \( u \)

\[
\sum_{i \in \mathcal{I}} f_i(y_i - tH_i u) - \sum_{i \in \mathcal{I}} f_i(y_i - (t + 1) H_i u)
\]

\[
\leq \sum_{i \in \mathcal{I}} C_i(-u).
\]

Hence from (21), (23) and (22), we know that

\[
\sum_{i \in \mathcal{I}} f_i(y_i - (t + 1) H_i u) - \sum_{i \in \mathcal{I}} f_i(y_i - H_i u)
\]

\[
\geq \sum_{i \in \mathcal{I}} C_i(u) - \sum_{i \in \mathcal{I}} C_i(u) - (m - p) \delta > 0,
\]

which proves (19).

\[\square\]

Remark 5. Assuming that \( y_i \) is a scalar and \( w = 0 \), Fawzi et al. [19] proved that the state can be exactly recovered under the integrity attack if and only if for all \( u \neq 0 \), there are at least \( 2p + 1 \) non-zero \( H_i u \). Notice that if for some \( u \neq 0 \), there are less than \( 2p + 1 \) non-zero \( H_i u \), then we can choose \( I \) to contain the largest \( p H_i u \) and thus violate (18). As a result, our sufficient condition is stronger than the
ones proposed in [19]. The main reason is that we seek to use convex optimization to solve the state estimation problem, while in [19], a combinatorial optimization problem is needed to recover the state.

**Remark 6.** A natural question after proving the resilience of an estimator is to quantify the resilience, i.e., by knowing \( \mu(z) \) in (3). The constructive proof of Theorem 1 also sheds light on the derivation of a tight \( \mu(z) \). From the proof, we know that \( \mu(z) = \beta(z) + 1 \) where \( \beta(z) \) is dependent on the specific form of \( f_i \) in (4).

We next give necessary conditions for the resilience of the estimator.

**Theorem 2** (Necessary Condition I). If there exist \( u_0 \in \mathbb{R}^n \) and \( i \in I \) such that
\[
\lim_{t \to \infty} f_i(tH_i u_0)/t \to +\infty,
\]
then the estimator is not resilient to the \((p, m)\)-sparse attack for any \( p \).

Before proving Theorem 2, we need the following lemma whose proof is reported in the appendix.

**Lemma 3.** If the condition (24) holds, for any \( M > 0 \) and for all \( v \) in a compact set \( V \subset \mathbb{R}^n \), there exists \( N \) (depending on \( M \) and the set \( V \)) such that the following inequality holds:
\[
h_j(u_0, v, t) > M, \forall v \in V, \ t \geq N.
\]

Now we are ready to prove the theorem.

**Proof.** We will prove that for any \( r > 0 \), there exists a \( \hat{z} \) such that any \( \hat{x} \) that satisfies \( \|\hat{x}\| \leq r \) cannot be the optimal solution of (4).

We first look at any sensor \( i \), where \( i \neq j \). Since a continuous function achieves its supremum on a compact set, we know that the following supremum is well defined (not infinite)
\[
\sup_{\|\hat{z}\| \leq r} \left[ f(z_i - H_i(\hat{x} + u_0)) - f(z_i - H_i\hat{x}) \right] = M_i,
\]
which implies that for all \( \|\hat{x}\| \leq r \), we can find \( M > 0 \), such that
\[
\sum_{i \neq j} f(z_i - H_j(\hat{x} + u_0)) - \sum_{i \neq j} f(z_i - H_i\hat{x}) \leq M.
\]

Now let us consider sensor \( j \). Due to Lemma 3, we can find a \( t \), such that for all \( \|\hat{x}\| \leq r \), the inequality \( h_j(u_0, -H_j(\hat{x} + u_0), t) > M \) holds.

Using Lemma 1, we have
\[
f((t + 1)H_j u_0 - H_j(\hat{x} + u_0)) - f(tH_j u_0 - H_j(\hat{x} + u_0))
\geq h_j(u_0, -H_j(\hat{x} + u_0), t) > M.
\]

Now consider the following \( y \)
\[
y_i = \begin{cases} 
    z_i, & \text{if } i \neq j \\
    tH_j u_0, & \text{if } i = j,
\end{cases}
\]

Combining (26) and (27), we know that for all \( \|\hat{x}\| \leq r \), the following inequality holds
\[
\sum_{i \in I} f(y_i - H_i(\hat{x} + u_0)) - \sum_{i \in I} f(y_i - H_i\hat{x}) < 0,
\]
which implies that the optimal solution of (4) cannot be inside the ball \( \{ x : \|x\| \leq r \} \). Now since \( r > 0 \) is arbitrary, we know the estimator is not resilient.

Next we provide another necessary condition when the limit \( C_i(u) \) is well defined.

**Theorem 3** (Necessary Condition II). If \( C_i(u) \) is well defined for all \( u \in \mathbb{R}^n \) and all \( i \in S \) but there exist a unit vector \( u_0 \) and an index set \( I_0 \subset C \) such that
\[
\sum_{i \in I_0} C_i(u_0) > \sum_{i \in I_0} C_i(u_0),
\]
then the estimator is not resilient to the attack.

**Proof.** For the sake of space saving, we just outline the proof which is similar to Theorem 2. The resilience of the estimator is equivalent to that the optimal estimate \( \hat{x} \) satisfies \( \|\hat{x}\| \leq \mu(z) \) for all \( a \in A \), where \( \mu \) is a real-valued function. To this end, we can prove that for any \( r > 0 \), there exists an attack \( a \) such that all \( \hat{x} \) that satisfies \( \|\hat{x}\| \leq r \) cannot be the optimal solution of (4).

With some derivations, we can show that for a \( y \) satisfying \( y_i = \begin{cases} 
    z_i, & \text{if } i \in I_0 \\
    tH_j u_0, & \text{if } i \in I_0,
\end{cases} \)
\begin{align*}
\|\hat{x}\| & \leq r \\
\end{align*}
the vector \( \hat{x} + u_0 \) is a better estimate than all \( \hat{x} \) satisfying \( \|\hat{x}\| \leq r \). Since \( r \) is an arbitrary positive real number, we can conclude that the estimator is not resilient.

Before continuing on, we would like to provide some remarks on the main result. First, it is worth noticing that the existence of a well defined limit of \( f_i(tH_i u)/t \) is crucial for the resilience of \( g \) as Theorem 2 suggested. This implies that the least square estimator cannot be resilient since \( f_i \) is in quadratic form. Using the potential function and force analogies in Remark 4, one can interpret the results presented in this section as: the estimator \( g \) is resilient if the force generated by any sensor is bounded and if the combined force of any collection of \( p \) sensors is strictly less than the combined force of the remaining \( m - p \) sensors.

It is worthwhile to notice that the conditions proved in Theorem 1, 2 and 3 are very tight, with only a trivial gap where the LHS of (28) equals the RHS.

Finally, we want to point out that the condition (18) is non-trivial to check since it requires us to verify against all possible \( u \). In the next subsection, we consider a special case where each \( g_i \) is a scalar and provide a conservative but verifiable sufficient condition for the resilience of the estimator.

**4 Scalar Measurement Case: More Analysis**

In this section, we specialize our results to the scalar measurement case, i.e., \( m_i = 1, \forall i \in S \). More practical and verifiable sufficient and necessary conditions can be derived. Throughout this section, we assume that the limit \( \alpha_i \equiv \lim_{t \to \infty} f_i(t)/t \) is well-defined (otherwise by Theorem 2, the estimator cannot be resilient). It is not difficult to prove that \( C_i(u) = |\alpha_i H_i u| \). With slight abuse of notation,
define $C_i = \alpha_i H_i$, then $C_i(u) = |C_i| u$. For any index set $\mathcal{I} = \{i_1, \ldots, i_l\} \subset \mathcal{S}$, define $C_\mathcal{I} = [C_{i_1}^T \cdots C_{i_l}^T]^T$. From Theorem 1 and Theorem 3, we have the following sufficient and necessary conditions for resilience of $g$.

**Proposition 1.** (a) If for all possible index set $\mathcal{I}$ and all non-zero $u \in \mathbb{R}^n$, the following inequality holds:

$$\|C_\mathcal{I} u\|_1 = \sum_{i \in \mathcal{I}} |C_i| u < \sum_{i \in \mathcal{I}^c} |C_i| u = \|C_{\mathcal{I}^c} u\|_1, \quad (29)$$

then the estimator $g$ is resilient.

(b) If there exists an index set $\mathcal{I}$ and a $u \in \mathbb{R}^n$ such that the following inequality holds:

$$\|C_\mathcal{I} u\|_1 > \|C_{\mathcal{I}^c} u\|_1, \quad (30)$$

then the estimator $g$ is not resilient.

**Remark 7.** Note that in this special case of scalar measurements, the sufficient and necessary conditions resemble the well-known nullspace property in compressed sensing and sparse signal recovery [25]. A similar result [19, Proposition 6] is also given for the decoding condition without any noise. This reveals Theorem 1 and Theorem 3 have the greater generality than the existing results.

The main difficulty in Proposition 1 is to validate (29) or falsify (30) over all non-zero $u$’s. We next show Proposition 1 in a conservative but more practically useful fashion.

**Theorem 4.** If for any index set $\mathcal{I} \subset \mathcal{S}$ with cardinality $p$, the optimal value of the following optimization problem is strictly less than $1$:

$$\min_{K \in \mathbb{R}^{n \times (m-p)}} \|C_\mathcal{I} K\|_1 \quad \text{subject to} \quad KC_\mathcal{I} = I_n, \quad (31)$$

then the estimator $g$ is resilient.

**Proof.** Let $K \in \mathbb{R}^{n \times (m-p)}$ such that $KC_\mathcal{I} = I_n$. Denote $\xi = C_\mathcal{I} u$. We have $C_{\mathcal{I}^c} K \xi$. Therefore, if for all $\xi \neq 0$, $\|C_{\mathcal{I}^c} K \xi\|_1 < \|\xi\|_1$, i.e., $\|C_{\mathcal{I}^c} K\|_1 < 1$, then we have $\|C_\mathcal{I} u\|_1 < \|C_{\mathcal{I}^c} u\|_1$. By enumerating all possible $\mathcal{I}$, we conclude the proof.

Notice that (31) is not necessary. Since $\xi = C_\mathcal{I} u$, $\xi$ may not be able to take all possible value in $\mathbb{R}^{m-p}$.

Similarly, we can find a more practically useful version for the necessary condition implied by Proposition 1(b). By enumerating all $(C_\mathcal{I} ^\perp, C_{\mathcal{I}^c})$ and utilizing the following result, we can identify whether $g$ is resilient for a given $H$ or not.

**Theorem 5.** If there exists an index set $\mathcal{I}$ such that the following inequality holds:

$$\|C_\mathcal{I} C_{\mathcal{I}^c}^+\|_1 > (\sqrt{m} - \sqrt{p} + 1)/2, \quad (32)$$

where $C_{\mathcal{I}^c}^+$ is the Moore-Penrose pseudo inverse of $C_{\mathcal{I}^c}$, then the estimator $g$ is not resilient.

The following lemma, whose proof is given in the appendix, is needed for the proof of Theorem 5:

**Lemma 4.** Let $\xi \in \mathbb{R}^m$ such that $\xi = \xi || + \xi \perp$, where $\xi ||$ and $\xi \perp$ are perpendicular to each other. Then the inequality holds: $\|\xi ||\| \leq (\sqrt{\sqrt{m} + 1}/2) \|\xi\|_1$.

| $BP_1$ | $BP_6$ | $BP_7$ | $BP_{16}$ | $B1_1$ | $B1_2$ | $B1_7$ | $B1_{12}$ | $B1_{13}$ |
|-------|-------|-------|----------|-------|-------|-------|-------|-------|
| $B1_1$ | $B1_3$ | $B1_5$ | $B1_4$ | $B1_2$ | $B1_4$ | $B1_9$ | $B1_6$ | $B1_3$ |

Table 1: Examples of 8 critical pairs of sensors. When any pair is under attack, the estimator will be not resilient.

We are now ready to prove Theorem 5:

**Proof.** To prove $g$ is not resilient, from Proposition 1 we only need to show there exists a $u$ such that $\|C_\mathcal{I} u\|_1 < \|C_{\mathcal{I}^c} u\|_1$ if (32) holds. Since $\|C_\mathcal{I} C_{\mathcal{I}^c} C_{\mathcal{I}^c}^+\|_1 > (\sqrt{m} - \sqrt{p} + 1)/2$, we can find $\xi \in \mathbb{R}^{m-p}$, such that $\|C_\mathcal{I} C_{\mathcal{I}^c}^+ \xi\|_1 > ((\sqrt{m} - \sqrt{p} + 1)/2) \|\xi\|_1$.

Now we can decompose $\xi = \xi || + \xi \perp$, where $\xi ||$ belongs to the column space of $C_\mathcal{I}^\perp$ and $\xi \perp$ is perpendicular to the column space of $C_\mathcal{I}$. By the property of Moore-Penrose inverse, $C_{\mathcal{I}^c}^+ \xi \perp = 0$. Therefore, we have $\|C_{\mathcal{I}^c}^+ \xi\|_1 = \|C_\mathcal{I} C_{\mathcal{I}^c}^+ \xi\|_1$. On the other hand, since $\xi \in \mathbb{R}^{m-p}$, by Lemma 4, we have $((\sqrt{m} - \sqrt{p} + 1)/2) \|\xi\|_1 \geq \|\xi \perp\|_1$, which implies that $\|C_\mathcal{I} C_{\mathcal{I}^c}^+ \xi\|_1 > \|\xi \perp\|_1$. Since $\xi \perp$ belongs to the column space of $C_\mathcal{I}^\perp$, there exists a $u$, such that $C_\mathcal{I} u = \xi ||$. Therefore, we can find a $u$, such that $\|C_\mathcal{I} u\|_1 > \|C_{\mathcal{I}^c} u\|_1$, which completes the proof.

5 Simulations on the IEEE 14-bus Test System

In this section we validate our main results on the IEEE 14-bus test system [26]. We simulate the state estimation against the $(p, m)$-sparse attacks under the DC power flow model. We extract the observation matrix $H \in \mathbb{R}^{34 \times 13}$ of the tested system from MATPOWER [27]. The state variables are voltage angles of all buses (excluding the slack Bus 1), and the scalar meter measurements are real power flows of all branches and real power injections of all buses. For the sake of space saving, we do not include $H$ here and we recommend interested readers to see [14, 26, 27] for details. Moreover, we assume the measurement noise is Gaussian distributed with zero mean and unit variance.

We use the estimator $g$ described in (10). With some computation, we know that $f$ in (11) can be explicitly written as:

$$f(u) = \left\{ \begin{array}{ll}
u^2, & |u| \leq \frac{1}{\lambda}, \\
\lambda |u| - \frac{1}{2} \lambda^2, & |u| > \frac{1}{2} \lambda.\end{array} \right. \quad (33)$$

Then we have $C_i(u) = |H_i| u$. Numerically, we find that $g$ is not resilient when $p \geq 2$. For instance, when $p = 2$, the experiments show that there are 29 critical pairs of sensors, out of all 561 possible pairs. The “critical pairs” mean that if the sensor pair is simultaneously attacked the estimator is no longer resilient. Due to the limited space, we list 8 pairs in Table 1, where $BP_i$ stands for the sensor measuring the real power flow of $i$-th branch\(^1\) and $B1_i$ means the sensor measuring the real power injection of $i$-th bus.

We can check the tightness of Theorem 4 and Theorem 5. Based on Theorem 4, the experimental result shows that only when $p = 1$, the estimator $g$ is resilient. On the other hand, when $p \geq 3$, the estimator $g$ is not resilient from Theorem 5. The only case that Theorem 4 and 5 cannot verify is when $p = 2$.

\(^1\)The branch indices follow MATPOWER [27]
Tradeoff between mean square optimality and resilience

Next we conduct experiments to compare the performance of the resilient estimator \( g \) in (12) with different tuning factors \( \lambda \)'s under different attack scenarios. By tuning which we can achieve a desirable tradeoff between mean square optimality and resilience. If attacked, the sensor monitoring the power injection of the 4-th bus is assumed to be manipulated.

For comparison, we also plot the tradeoff of the resilient estimator in (7), denoted as \( \phi \), proposed by Pajic et al. [21]. In Fig.1 we plot the mean square error (MSE) characteristic curve in blue illustrating the performance of \( g \) in two scenarios by varying \( \lambda \). The y-axis represents the normalized MSE of an estimator in the presence of attacks, i.e., the quotient of MSE of \( g \) over MSE of the oracle LSE\(^2\). The x-axis represents the normalized MSE when there is no attack, by normalizing MSE of \( g \) over MSE of LSE.

The estimator \( \phi \) assumes the noise is bounded and lies in a convex set. Thus we let \( |w_i| \leq \epsilon \), \( \forall i \). Similarly, we plot the MSE characteristic curve in red illustrating the performance of \( \phi \) in two scenarios by varying \( \epsilon \). It is easy to see that \( g \) outperforms \( \phi \) in terms of the tradeoff. Especially when there is no attack, the MSE of \( \phi \) deviates too much from that of LSE.

6 Concluding Remarks

We have studied the resilient estimation problem where sensor networks are exposed to \((p, m)\)-sparse integrity attacks. No assumption on the attack patterns and fault detection mechanism makes us more focused on the properties of the inherent resilience of any estimator.

Our interest is not to study any concrete estimator in the presence of attacks. Instead, we have considered a general class of estimators which integrates a large number of important estimators as special cases and given sufficient and necessary conditions for the resilience of the estimator. To the best of our knowledge, this is the first time to conduct generic resilience analysis for cyber-physical systems. Moreover, we have presented more analytical results in the scalar measurement case to render the sufficient and necessary conditions more ready to use. The experimental results on the IEEE 14-bus test system have validated our theoretical results and illustrated how to apply the theories to real applications.

Acknowledgement

This research is partially funded by the Republic of Singapore National Research Foundation (NRF) through a grant to the Berkeley Education Alliance for Research in Singapore (BEARS) for the Singapore-Berkeley Building Efficiency and Sustainability in the Tropics (SinBerBEST) Program. BEARS has been established by the University of California, Berkeley as a center for intellectual excellence in research and education in Singapore.

Thank Dr. Yang Zai for the insightful discussion.

7 Appendix

Proof of Lemma 2:

(i) It is easy to prove the first statement. Due to the scaling property of \( C_i(u) \) and the convexity of \( f_i \), we have

\[
C_i(u_1 + u_2) = 2C_i \left( \frac{u_1 + u_2}{2} \right) \leq C_i(u_1) + C_i(u_2).
\]

Hence we know that \( C_i \) is indeed a semi-norm on \( \mathbb{R}^n \).

(ii) Based on the convexity of \( f_i \), we obtain

\[
2f_i(\frac{H_1u}{2}) \leq f_i(v + H_1u) + f_i(-v), \quad (34)
\]

\[
f_i(tH_1u) \geq 2f_i(\frac{t^2v + H_1u}{2}) - f(2v). \quad (35)
\]

Dividing both sides of (34) and (35) by \( t \) and taking limit over \( t \), we have

\[
C_i(u) \leq \liminf_{t \to \infty} \frac{1}{t} f_i(v + H_1u) + \lim_{t \to \infty} \frac{1}{t} f_i(-v),
\]

\[
C_i(u) \geq \limsup_{t \to \infty} \frac{1}{t} f_i(v + \frac{H_1u}{2}) - \lim_{t \to \infty} \frac{1}{t} f_i(2v).
\]

Since \( \lim_{t \to \infty} f_i(-v)/t = \lim_{t \to \infty} f_i(2v)/t = 0 \), we have the pointwise limit \( \lim_{t \to \infty} h_i(u, v, t) = C_i(u) \). Notice that for a fixed \((u, v)\), by Lemma 1, \( h_i(u, v, t) \) is monotonically non-decreasing with respect to \( t \). Furthermore, \( C_i(u) \) is continuous since it is a semi-norm. Therefore, by Dini’s theorem [28], \( h_i(u, v, t) \) converges uniformly to \( C_i(u) \) on a compact set of \((u, v)\).

(iii) By the convexity of \( f_i \), for any integer \( k \) we know that

\[
f_i(v + kH_1u) - f_i(v + (k - 1)H_1u) \\
\leq f_i(v + (k + 1)H_1u) - f_i(v + kH_1u).
\]

---

\(^2\)The oracle LSE refers to the LSE which can ideally identify and discard the malicious measurement and give an estimate based on only the benign sensors. The oracle LSE is practically impossible but from a theoretical point of view it provides a lower bound on the MSE of any estimator under attack.
Hence we can conclude that $f_i(v + H_i u) - f_i(v) \leq \lim_{N \to \infty} \sum_{k=1}^{N} (f_i(v + k H_i u) - f_i(v + (k - 1) H_i u))/N = \lim_{N \to \infty} (f_i(v + N H_i u) - f_i(v))/N = C_i(u)$. □

Proof of Lemma 3:

From (24) and (34), it is easy to see that $h_j(u_0, v, t)$ diverges to infinity for all $v$, i.e., $h_j(u_0, v, t) \to +\infty$. Next we will show this divergence is also uniform. Denote $\mathcal{W}_t = \{ v : h_j(u_0, v, t) > M \}$. Since $h_j(u_0, v, t)$ is continuous ($f_i$ is continuous due to convexity), each $\mathcal{W}_t$ is open. By Lemma 1, $h_j(u_0, v, t)$ is monotonically non-decreasing in $t$.

Therefore, $\mathcal{W}_t \subseteq \mathcal{W}_t'$ if $t \leq t'$. Thus for each $v$ there exists $t$ such that $h_j(u_0, v, t) > M$, we have $\bigcup_{k \geq 0} \mathcal{W}_k = \mathbb{R}^{m_i}$. Therefore, the collection $\{ \mathcal{W}_t \}$ is an open cover for the compact subset $\mathcal{V}$. Thus, we can find a finite cover $\mathcal{W}_{t_1}, \ldots, \mathcal{W}_{t_M}$ that covers $\mathcal{V}$, i.e., $\mathcal{V} \subseteq \mathcal{W}_{t_1} \cup \mathcal{W}_{t_2} \cup \cdots \cup \mathcal{W}_{t_M}$. Now we can define $N = \max(t_1, \ldots, t_M)$. Since $\mathcal{W}_t$ is non-decreasing with respect to $t$, we have $\mathcal{W}_{t_1} \cup \mathcal{W}_{t_2} \cup \cdots \cup \mathcal{W}_{t_M} = \mathcal{W}_N$. For any $t \geq N$, we have $\mathcal{V} \subseteq \mathcal{W}_N \subseteq \mathcal{W}_t$, which combined with the definition of $\mathcal{W}_t$ completes the proof.

Proof of Lemma 4:

Geometrically, $\xi_r$ can be written as $\xi_r = \xi_2 + r$, where $r \in \{ r \cap \| \xi_2 \|_2 = \| \xi_1 \|_2 /2 \}$. As a result, we have

$$\| \xi_1 \|_1 \leq \frac{1}{2} \| \xi_2 \|_1 + \| r \|_1 \leq \frac{1}{2} \| \xi_1 \|_1 + \sqrt{m} \| r \|_2$$

$$\leq \frac{1}{2} \| \xi_1 \|_1 + \sqrt{m} \| \xi_2 \|_2 \leq \frac{1}{2} \| \xi_2 \|_1 + \sqrt{m} \| \xi_2 \|_1 .$$

The first inequality is due to the triangle inequality of any norm. The second and third inequalities are due to the fact that for an $m$ dimensional vector $\xi$, $\| \xi \|_2 \leq \| \xi \|_1 \leq \sqrt{m} \| \xi \|_1$ holds. □

References

[1] S. A. Boyer, “SCADA: supervisory control and data acquisition,” Instrument Engineers’ Handbook, Volume Three: Process Software and Digital Networks, p. 357, 2002.

[2] F. Pasqualetti, A. Bicchi, and F. Bullo, “Consensus computation in unreliable networks: a system theoretic approach,” IEEE Trans. Autom. Control, vol. 57, no. 1, pp. 90–104, Jan 2010.

[3] D. Han, Y. Mo, J. Wu, S. Weerakkody, B. Sinopoli, and L. Shi, “Stochastic event-triggered sensor schedule for remote state estimation,” IEEE Trans. Autom. Control, vol. 60, no. 10, pp. 2661–2675, 2015.

[4] J. M. Hendrickx, K. H. Johansson, R. M. Jungers, H. Sandberg, and K. C. Sou, “Efficient computations of a security index for false data attacks in power networks,” IEEE Trans. Autom. Control, vol. 59, no. 12, pp. 3194–3208, 2014.

[5] H. Zhang, P. Cheng, L. Shi, and J. Chen, “Optimal DoS attack scheduling in wireless networked control system,” IEEE Trans. Control Systems Technology, to be published, 2015.

[6] Y. Li, L. Shi, P. Cheng, J. Chen, and D. Quevedo, “Jamming attacks on remote state estimation in cyber-physical systems: A game-theoretic approach,” IEEE Trans. Autom. Control, vol. 60, no. 10, pp. 2831–2836, 2015.

[7] Y. Mo and B. Sinopoli, “Secure estimation in the presence of integrity attacks,” IEEE Trans. Autom. Control, vol. 60, no. 4, pp. 1145–1151, 2015.

[8] ——, “On the performance degradation of cyber-physical systems under stealthy integrity attacks,” IEEE Trans. Autom. Control, to be published, 2015.

[9] Y. Li, D. E. Quevedo, S. Dey, and L. Shi, “SINR-based dos attack on remote state estimation: A game-theoretic approach,” IEEE Trans. Control of Network Systems, to be published, 2016.

[10] H. P. Lopuhaa and P. J. Rousseuw, “Breakdown points of affine equivariant estimators of multivariate location and covariance matrices,” The Annals of Statistics, vol. 19, no. 1, pp. 229–248, 1991.

[11] E. Handschin, F. Schweppe, J. Kohlas, and A. Fiechter, “Bad data analysis for power system state estimation,” IEEE Trans. Power Apparatus and Systems, vol. 94, no. 2, pp. 329–337, Mar. 1975.

[12] L. Mili, T. Van Cutsem, and M. Ribbens-Pavella, “Bad data identification methods in power system state estimation - a comparative study,” IEEE Power Engineering Review, vol. PER-5, no. 11, pp. 27–28, Nov. 1985.

[13] L. Xie, Y. Mo, and B. Sinopoli, “Integrity data attacks in power market operations,” IEEE Trans. Smart Grid, vol. 2, no. 4, pp. 659–666, 2011.

[14] Y. Liu, P. Ning, and M. K. Reiter, “False data injection attacks against state estimation in electric power grids,” ACM Trans. Information and System Security, vol. 14, no. 1, p. 13, 2011.

[15] J. Kim, L. Tong, and R. J. Thomas, “Data framing attack on state estimation,” IEEE J. Selected Areas in Commun., vol. 32, no. 7, pp. 1460–1470, Jul. 2014.

[16] X. Lu, L. Xie, H. Zhang, and W. Wang, “Robust Kalman filtering for discrete-time systems with measurement delay,” IEEE Trans. Circuits and Systems II: Express Briefs, vol. 54, no. 6, pp. 522–526, 2007.

[17] T. Zhou, “On the convergence and stability of a robust state estimator,” IEEE Trans. Autom. Control, vol. 55, no. 3, pp. 708–714, 2010.

[18] ——, “Sensitivity penalization based robust state estimation for uncertain linear systems,” IEEE Trans. Autom. Control, vol. 55, no. 4, pp. 1018–1024, 2010.

[19] H. Fawzi, P. Tabuada, and S. Diggavi, “Secure estimation and control for cyber-physical systems under adversarial attacks,” IEEE Trans. Autom. Control, vol. 59, no. 6, pp. 1454–1467, 2014.

[20] M. S. Chong, M. Wakaiki, and J. P. Hespanha, “Observability of linear systems under adversarial attacks,” in Proc. IEEE Amer. Control Conf., 2015.

[21] M. Pajic, J. Weimer, N. Bezzo, P. Tabuada, O. Sokolsky, I. Lee, and G. J. Pappas, “Robustness of attack-resilient state estimators,” in Proc. ACM/IEEE Int. Conf. Cyber-Physical Systems, Apr. 2014, pp. 163–174.

[22] D. Han, Y. Mo, and L. Xie, “Robust state estimation against sparse integrity attacks,” 2016. [Online]. Available: https://arxiv.org/abs/1601.04180

[23] M. Pajic, P. Tabuada, I. Lee, and G. J. Pappas, “Attack-resilient state estimation in the presence of noise,” in Proc. IEEE Conf. Decision and Control, 2015, pp. 5827–5832.

[24] R. Tibshirani, “Regression shrinkage and selection via the lasso,” J. Royal Statistical Society. Series B (Methodological), pp. 267–288, 1996.

[25] Y. C. Eldar and G. Kutyniok, Compressed sensing: theory and applications. Cambridge University Press, 2012.

[26] The UW Power Systems Test Case Archive. [Online]. Available: https://www.ee.washington.edu/research/pscta/

[27] R. D. Zimmerman, C. E. Murillo-Sánchez, and R. J. Thomas, “MATPOWER: Steady-state operations, planning, and analysis tools for power systems research and education,” IEEE Trans. Power Systems, vol. 26, no. 1, pp. 12–19, 2011.

[28] W. Rudin, Principles of mathematical analysis. McGraw-Hill New York, 1964, vol. 3.