Convex Optimization Based State Estimation against Sparse Integrity Attacks

Duo Han [a], Yilin Mo [a], Lihua Xie [a],

[a] *School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore.*

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 some 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. Experimental results tested on the IEEE 14-bus test system validate the theoretical analysis.

Key words: State estimation; resilient estimation; integrity attack; convex optimization

1 Introduction

Cyber-physical security has drawn increasing research attention Cárdenas et al. [2008], Amin [2012], Ozay et al. [2013], Li et al. [2015], Zhang et al. [2015] since the first Supervisory Control And Data Acquisition (SCADA) system malware (called Stuxnet) was discovered and investigated Chen [2010], Fidler [2011]. One important class of attacks is known as integrity attack on the sensory data. Due to the sparsely spatial deployment of the sensors, full protection during the collection and transmission of the sensory data cannot often be guaranteed. The attacker launches such an attack in industrial systems for various purposes, such as creating arbitrage opportunities in electricity market, stealing gas or oil without being noticed, posing potential threat to national defense, etc. Briefly speaking, the dominant feature of integrity attack is that the attacker can take full control of a subset of sensors and can arbitrarily change the measurements.

One way to deal with malicious measurements is to treat them as bad data or outliers. In the context of power systems, the problem of bad data detection has been studied over the past decades Handschin et al. [1975], Mili et al. [1985]. 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 Sandberg et al. [2010], Xie et al. [2011]. For example, Liu et al. Liu et al. [2009] successfully showed that a stealthy attack changing the state while not being detected is possible. Kim et al. Kim et al. [2014] studied a so-called framing attack. Under such an 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.

For dynamical systems, detecting malicious components via fault detection and isolation based methods has also been extensively studied Pasqualetti et al. [2010, 2011], Sundaram et al. [2010], Fawzi et al. [2014], Chong et al. [2015]. The system, however, is assumed to be noiseless in these cases, which greatly favors the failure detector. Pajic et al. Pajic et al. [2014] extended the work by considering the systems with bounded noise. On the top of

Email addresses: dhanaa@ntu.edu.sg (Duo Han), ylmo@ntu.edu.sg (Yilin Mo), elhxie@ntu.edu.sg (Lihua Xie).

sufficient conditions for exact recovery in noiseless case Fawzi et al. [2014], 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 computationally hard to solve and may not be applicable for large scale systems. In Pajic et al. [2015], the authors derived an estimator based on solving an l_1 optimization problem. However, the bounds that they derive are conservative when there are multiple sensors being attacked. In Mo et al. [2010], Mo and Sinopoli [2010], the authors also consider a noisy linear system and use reachability analysis and ellipsoid approximation to characterize all possible biases the adversary can inject to the system.

For statisticians, the concept of robust estimators has been prevailing for decades Kassam et al. [1985], Maronna et al. [2006], Huber and Ronchetti [2009]. The robustness is often measured by breakdown points Hampel [1971], Donoho and Huber [1983] or influence functions Hampel [1974]. Most literature studied one or several estimators and discussed the breakdown point properties and a unified analysis for most useful estimators is still absent. Moreover, in most of the above works, the state is usually a scalar, which may not be applicable for many control systems.

In this paper, we focus on the problem of resilient state estimation against sparse integrity attacks. To be concrete, we consider 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.

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 necessary and sufficient conditions 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 ith sensor is given by

$$z_i = H_i x + w_i, \tag{1}$$

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 ith sensor, and $w_i \in \mathbb{R}^{m_i}$ is the measurement noise for the ith sensor. The measurement matrix $H \triangleq [H_1^\top, H_2^\top, \ldots, H_i^\top]^\top \in \mathbb{R}^{(\sum_i m_i)\times n}$ is assumed to be observable, *i.e.*, H is full column rank. In the presence of attacks, the measurement equation can be written as

$$y_i = z_i + a_i = H_i x + w_i + a_i, \tag{2}$$

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 ith sensor by a_i. Denote

$$\begin{aligned} z &\triangleq [z_1^\top, z_2^\top, \dots, z_m^\top]^\top, & y &\triangleq [y_1^\top, y_2^\top, \dots, y_m^\top]^\top, \\ w &\triangleq [w_1^\top, w_2^\top, \dots, w_m^\top]^\top, & a &\triangleq [a_1^\top, a_2^\top, \dots, a_m^\top]^\top. \end{aligned} \tag{3}$$

Denote the index set of all sensors as $\mathcal{S} \triangleq \{1, 2, \dots, m\}$. For any index set $\mathcal{I} \subseteq \mathcal{S}$, define the complement set to be $\mathcal{I}^c \triangleq \mathcal{S} \backslash \mathcal{I}$. In our attack model, we assume that the attacker can only compromise at most p sensors but can arbitrarily choose a_i. Formally, a (p, m)-sparse attack can be defined as

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) $\|a_i\| = 0, \ \forall i \in \mathcal{I}^c$;
(ii) $|\mathcal{I}| \leq p$.

Define the collection of all possible index sets of malicious sensors as

$$\mathbb{C} \triangleq \{\mathcal{I} : \mathcal{I} \subset \mathcal{S}, |\mathcal{I}| = p\}.$$

The set of all possible (p, m)-sparse attacks is denoted as

$$\mathcal{A} \triangleq \bigcup_{\mathcal{I} \in \mathbb{C}} \{a : \|a_i\| = 0, i \in \mathcal{I}^c\}.$$

The main task of this work is to investigate the sufficient and necessary conditions for a generic convex optimization based 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:*

$$\|g(z) - g(z + a)\| \leq \mu(z), \ \forall a \in \mathcal{A}, \tag{4}$$

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. 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 1 *Notice that if an estimator is resilient and translation invariant, then*

$$\begin{aligned} \|g(z) - g(z + a)\| &= \|x + g(w) - x - g(w + a)\| \\ &= \|g(w) - g(w + a)\| \leq \mu(w). \end{aligned}$$

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 general convex optimization based estimator which is translation invariant.

2.2 A General 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 estimator that we study in this paper is assumed to have the following form:

$$\hat{x} = g(y) \triangleq \arg\min_{\hat{x}} \sum_{i \in \mathcal{S}} f_i(y_i - H_i \hat{x}), \tag{5}$$

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 2 *One can view $y_i - H_i\hat{x}$ as the residue for the ith 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 (5) is translation invariant. In fact, if $\hat{x}^* = g(y)$, then

$$g(y + Hu) = \arg\min_{\hat{x}} \sum_{i \in \mathcal{S}} f_i \left[y_i - H_i(\hat{x} - u) \right],$$

which implies that $g(y + Hu) - u = \hat{x}^*$.

We now investigate several commonly used estimators and show that they can be written as (5).

(a) Least Square Estimator:

$$\begin{aligned} \hat{x} &= \arg\min_{\hat{x}} \|y - H\hat{x}\|_2^2 = \arg\min_{\hat{x}} \sum_{i \in \mathcal{S}} \|y_i - H_i\hat{x}\|_2^2 \\ &= (H^\top H)^{-1} H^\top y. \end{aligned} \tag{6}$$

(b) Another example is an estimator which minimizes the sum of the l_1 norm of the residue, *i.e.*,

$$\hat{x} = \arg\min_{\hat{x}} \sum_{i \in \mathcal{S}} \|y_i - H_i\hat{x}\|_1 . \tag{7}$$

In the case where $m_i = n$ and $H_i = \mathrm{I}_n$, $\forall i$, the estimate is a vector in which the ith entry is the median over the ith entries of all measurements y_i's.

(c) The following is designed to minimize the sum of the l_2 norm of the residue:

$$\hat{x} = \arg\min_{\hat{x}} \sum_{i \in \mathcal{S}} \|y_i - H_i\hat{x}\|_2 . \tag{8}$$

The optimal estimate in the case where $m_i = n$ and $H_i = \mathrm{I}_n$, $\forall i$ is the geometric median of all y_i's, which is called an L_1 estimator in Lopuhaa and Rousseeuw [1991]. 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.

(d) Pajic et al. Pajic et al. [2014, 2015] proposed the following resilient estimator in the presence of integrity attack:

$$\begin{aligned} \underset{\hat{x},a,w}{\textit{minimize}} \quad & \left\| \begin{bmatrix} \|a_1\|_2 \\ \vdots \\ \|a_m\|_2 \end{bmatrix} \right\|_0 \\ \text{subject to} \quad & y_i = H_i\hat{x} + w_i + a_i, \\ & w = [w_1^\top, \ldots, w_m^\top]^\top \in \Omega, \end{aligned}$$

where the authors assume that the noise is bounded and lies in a convex set Ω. 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:

$$\begin{aligned} \underset{\hat{x},a,w}{\textit{minimize}} \quad & \sum_{i\in\mathcal{S}} \|a_i\|_2 \\ \text{subject to} \quad & y_i = H_i\hat{x} + w_i + a_i, \\ & w \in \Omega. \end{aligned} \tag{9}$$

Assuming that Ω can be written as a product set $\Omega = \Omega_1 \times \cdots \times \Omega_m$, then the constraint on w can be decoupled as

$$w \in \Omega \Leftrightarrow w_i \in \Omega_i, \, \forall i.$$

By the convexity of Ω, each Ω_i must also be convex. We can define the following function

$$f_i(r) \triangleq \min_{r-a_i\in\Omega_i} \|a_i\|_2. \tag{10}$$

As a result, the relaxed minimization problem can be written as

$$\hat{x} = \arg\min_{\hat{x}} \sum_{i\in\mathcal{S}} f_i(y_i - H_i\hat{x}). \tag{11}$$

(e) Similarly to the previous example, we can consider the following LASSO Tibshirani [1996] estimator:

$$\begin{aligned} \underset{\hat{x},a,w}{\textit{minimize}} \quad & \|w\|^2 + \lambda\|a\|_1 \\ \text{subject to} \quad & y = H\hat{x} + w + a. \end{aligned} \tag{12}$$

If we define the following function:

$$f(r) \triangleq \underset{a_i}{\textit{minimize}} \quad \|r - a_i\|_2^2 + \lambda \|a_i\|_1 \tag{13}$$

Then one can easily prove that the optimization problem (12) can be rewritten as

$$\hat{x} = \arg\min_{\hat{x}} \sum_{i\in\mathcal{S}} f(y_i - H_i\hat{x}). \tag{14}$$

In the next section, we shall present sufficient and necessary conditions for the resilience of the general estimator (5). Since (6), (7), (8) and (14) are all special cases of (5), we can easily analyze their individual resilience.

3 Resilience Analysis for a General 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.

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,*

$$q(t+1) - q(t) \geq q(t)/t. \tag{15}$$

Proof. For any $0 < \alpha < 1$, we have

$$q(\alpha t) \leq \alpha q(t) + q(0) = \alpha q(t).$$

Divide both side by αt, we can prove that $q(t)/t$ is monotonically non-decreasing. Therefore, $q(t+1)/(t+1) \geq q(t)/t$, which implies (15). ■

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 $u \in \mathbb{R}^n$:*

$$\lim_{t\to\infty} \frac{f_i(tH_iu)}{t} = C_i(u), \tag{16}$$

then the following statements are true:

(i) $C_i(\alpha u) = |\alpha|\, C_i(u)$ *and* $C_i(u_1 + u_2) \leq C_i(u_1) + C_i(u_2)$.
(ii) Define the function $h_i(u, v, t) : \mathbb{R}^n \times \mathbb{R}^{m_i} \times \mathbb{R} \mapsto \mathbb{R}$,

$$h_i(u, v, t) \triangleq \frac{1}{t} \left[f_i(v + tH_iu) - f_i(v) \right]. \tag{17}$$

Then the following pointwise limit holds:

$$\lim_{t\to\infty} h_i(u, v, t) = C_i(u). \tag{18}$$

Moreover, the convergence is uniform on any compact set of (u, v).
(iii) For any v and u, we have that

$$f_i(v + H_iu) - f_i(v) \leq C_i(u). \tag{19}$$

Remark 3 *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* (19)*, we know that the force from the potential function f_i along the u direction cannot exceed $C_i(u)$ (or $C_i(u)/\|u\|$ to normalize). On the other hand, Equation* (18) *implies that this bound is tight.*

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 $i \in \mathcal{S}$;

(2) the following inequality holds for all non-zero u:

$$\sum_{i\in\mathcal{I}} C_i(u) < \sum_{i\in\mathcal{I}^c} C_i(u),\ \forall \mathcal{I}\in\mathbb{C}, \tag{20}$$

then the estimator g is resilient.

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

$$\sum_{i\in\mathcal{S}} f_i(y_i - H_i \times tu) < \sum_{i\in\mathcal{S}} f_i(y_i - H_i \times (t+1)u). \tag{21}$$

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 $\mathcal{I}$, to prove (21), we will first look at benign sensors. Due to the uniform convergence of $h_i(u, v, t)$ to $C_i(u)$ on $\mathcal{U} \times \{-z_i\}$ shown in Lemma 2, given any $\delta > 0$ we can always find a finite constant $N_i(z_i, \delta)$ where $N_i : \mathbb{R}^{m_i} \times \mathbb{R} \mapsto \mathbb{R}$ such that for all $t \geq N_i(z_i, \delta)$, the following inequality holds:

$$h_i(-z_i, u, t) = \frac{1}{t}\left[f_i(tH_iu - z_i) - f_i(-z_i)\right] \geq C_i(u) - \delta, \tag{22}$$

for any $\|u\| = 1$. By (15), we can derive that

$$f_i((t+1)H_iu - z_i) - f_i(tH_iu - z_i) \geq C_i(u) - \delta. \tag{23}$$

We fix δ to be

$$\delta = \frac{1}{m} \min_{\|u\|=1} \min_{\mathcal{I}\in\mathbb{C}} \left(\sum_{i\in\mathcal{I}^c} C_i(u) - \sum_{i\in\mathcal{I}} C_i(u) \right). \tag{24}$$

and take $\beta(z)$ in the following 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

$$\begin{aligned} &f_i((t+1)H_iu - z_i) - f_i(tH_iu - z_i) \\ &\qquad\qquad \geq C_i(u) - \delta,\ \forall \|u\| = 1. \end{aligned} \tag{25}$$

Since for good sensors, $z_i = y_i$, we know that

$$\begin{aligned} &\sum_{i\in\mathcal{I}^c} \left[f_i((t+1)H_iu - z_i) - f_i(tH_iu - z_i)\right] \\ &\qquad \geq \sum_{i\in\mathcal{I}^c} C_i(u) - (m-p)\delta,\ \forall \|u\| = 1. \end{aligned} \tag{26}$$

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

$$\sum_{i\in\mathcal{I}} f_i(y_i - tH_iu) - \sum_{i\in\mathcal{I}} f_i(y_i - (t+1)H_iu) \leq \sum_{i\in\mathcal{I}} C_i(-u). \tag{27}$$

Hence from (24), (27) and (26), we know that

$$\sum_{i\in\mathcal{S}} f_i(y_i-(t+1)H_iu)-\sum_{i\in\mathcal{S}} f_i(y_i-tH_iu)$$
$$\geq \sum_{i\in\mathcal{I}^c} C_i(u)-\sum_{i\in\mathcal{I}} C_i(u)-(m-p)\delta>0,$$

which proves (21). ■

Remark 4 *A natural question after proving the resilience of an estimator is to quantify the resilience, i.e., by knowing $\mu(z)$ in (4). 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 (5).*

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

Theorem 2 (Necessary Condition I) *If $C_i(u)$ is well defined for all $u\in\mathbb{R}^n$ and all $i\in\mathcal{S}$ but there exist a unit vector u_0 and an index set $\mathcal{I}_0\in\mathbb{C}$ such that*

$$\sum_{i\in\mathcal{I}_0} C_i(u_0)>\sum_{i\in\mathcal{I}_0^c} C_i(u_0), \tag{28}$$

then the estimator is not resilient to the attack.

Proof. The resilience of the estimator is equivalent to that the optimal estimate $\hat{x}$ satisfies $\|\hat{x}\|\leq\mu(z)$ for all $a\in\mathcal{A}$, where μ is a real-valued function. To this end, we will 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 (5).

We will first look at the compromised sensors. For every $\delta>0$ we can always find a finite constant $N_i(\delta)$ such that for any $\hat{x}\in\{\hat{x}:\|\hat{x}\|\leq r\}$ and for all $t>N_i$, the following inequality holds:

$$\begin{aligned}&f_i(tH_iu_0-H_i\hat{x})-f_i(tH_iu_0-H_i(\hat{x}+u_0))\\ \geq& f_i((t+1)H_iu_0-H_i(\hat{x}+u_0))\\ &\qquad -f_i(tH_iu_0-H_i(\hat{x}+u_0))\\ \geq& h_i(u_0,-H_i(\hat{x}+u_0),t)\geq C_i(u_0)-\delta,\ \forall i\in\mathcal{I}_0.\end{aligned} \tag{29}$$

The first inequality is derived from (15). The second inequality is due to the uniform convergence of $h_i(u,v,t)$ to $C_i(u)$ on $\{u_0\}\times\{v:v=-H_ix+u_0,\ \|x\|\leq r\}$.

Let us choose

$$\delta=\frac{1}{m}\left(\sum_{i\in\mathcal{I}_0} C_i(u_0)-\sum_{i\in\mathcal{I}_0^c} C_i(u_0)\right),$$

and $t=\max_{i\in\mathcal{I}_0} N_i(\delta)$ and $y_i=tH_iu_0$ for all $i\in\mathcal{I}_0$, then we know for any $\|\hat{x}\|\leq r$,

$$\sum_{i\in\mathcal{I}_0}\left[f_i(y_i-H_i\hat{x})-f_i(y_i-H_i(\hat{x}+u_0))\right]$$
$$\geq\sum_{i\in\mathcal{I}_0} C_i(u_0)-p\delta.$$

Now let us look at the benign sensors. By Lemma 2 (iii) we have

$$f_i(z_i-H_i(\hat{x}+u_0))-f_i(z_i-H_i\hat{x})\leq C_i(u_0),\ \forall i\in\mathcal{I}_0^c. \tag{30}$$

From (29) and (30),

$$\sum_{i\in\mathcal{S}} f_i(y_i - H_i(\hat{x}+u_0)) - \sum_{i\in\mathcal{S}} f_i(y_i - H_i\hat{x}) \leq \sum_{i\in\mathcal{I}_0^c} C_i(u_0) - \sum_{i\in\mathcal{I}_0} C_i(u_0) + p\delta < 0.$$

Thus for such a y satisfying

$$y_i = \begin{cases} z_i, & \text{if } i \in \mathcal{I}_0^c \\ tH_iu_0, & \text{if } i \in \mathcal{I}_0, \end{cases}$$

$\hat{x}+u_0$ 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. ■

Theorem 3 (Necessary Condition II) *If there exist $u_0 \in \mathbb{R}^n$ and $i \in \mathcal{I}$ such that*

$$\lim_{t\to\infty} \frac{f_i(tH_iu_0)}{t} \to +\infty, \tag{31}$$

then the estimator is not resilient to the attack.

Before proving Theorem 3, we need the following lemma whose proof is reported in appendix.

Lemma 3 *If the condition* (31) *holds, for any $M > 0$ and for all v in a compact set $\mathcal{V} \subset \mathbb{R}^{m_i}$, there exists N (depending on M and the set $\mathcal{V}$) such that the following inequality holds:*

$$h_j(u_0, v, t) > M, \forall v \in \mathcal{V},\ t \geq N \tag{32}$$

Now we are ready to prove the theorem.

Proof. Similar to Theorem 2, we will prove that for any $r > 0$, there exists a y such that any $\hat{x}$ that satisfies $\|\hat{x}\| \leq r$ cannot be the optimal solution of (5).

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)

$$\sup_{\|\hat{x}\|\leq r} [f(z_i - H_i(\hat{x}+u_0)) - f(z_i - H_i\hat{x})] = M_i,$$

which implies that for all $\|\hat{x}\| \leq r$, we can find $M > 0$, such that

$$\sum_{i\neq j} f(z_i - H_i(\hat{x}+u_0)) - \sum_{i\neq j} f(z_i - H_i\hat{x}) \leq M. \tag{33}$$

Now let us consider sensor j. Due to Lemma 3, we can find a t, such that for all $\|\hat{x}\| \leq r$, the following inequality holds:

$$h_j(u_0, -H_j(\hat{x}+u_0), t) > M.$$

Using Lemma 1, we have

$$\begin{aligned} &f((t+1)H_ju_0 - H_j(\hat{x}+u_0)) - f(tH_ju_0 - H_j(\hat{x}+u_0)) \\ &= f(tH_ju_0 - H_j\hat{x}) - f(tH_ju_0 - H_j(\hat{x}+u_0)) \\ &\geq h_j(u_0, -H_j(\hat{x}+u_0), t) > M. \end{aligned} \tag{34}$$

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 (33) and (34), we know that for all $\|\hat{x}\| \leq r$, the following inequality holds

$$\sum_{i \in \mathcal{S}} f(y_i - H_i(\hat{x} + u_0)) - \sum_{i \in \mathcal{S}} f(y_i - H_i \hat{x}) < 0,$$

which implies that the optimal solution of (5) cannot be inside the ball $\{\hat{x} : \|\hat{x}\| \leq r\}$. Now since $r > 0$ is arbitrary, we know 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 3 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 3, 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.

Secondly, one can see 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 (20) 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 y_i is a scalar and provide a more 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.*, $m_i = 1$, $\forall i \in \mathcal{S}$. Throughout this section, we assume that the following limit is well-defined (otherwise by Theorem 3, the estimator cannot be resilient):

$$\alpha_i \triangleq \lim_{t \to \infty} f_i(t)/t. \tag{35}$$

It is not difficult to prove that $C_i(u) = |\alpha_i H_i u|$. With slight abuse of notation, define $C_i \triangleq \alpha_i H_i$, then $C_i(u) = |C_i u|$. For any index set $\mathcal{I} = \{i_1, \ldots, i_l\} \subset \mathcal{S}$, define

$$C_{\mathcal{I}} \triangleq \begin{bmatrix} C_{i_1}^\top & \cdots & C_{i_l}^\top \end{bmatrix}^\top. \tag{36}$$

From Theorem 1 and Theorem 2, 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:*

$$\|C_{\mathcal{I}} u\|_1 = \sum_{i \in \mathcal{I}} |C_i u| < \sum_{i \in \mathcal{I}^c} |C_i u| = \|C_{\mathcal{I}^c} u\|_1, \tag{37}$$

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:

$$\|C_{\mathcal{I}} u\|_1 > \|C_{\mathcal{I}^c} u\|_1, \tag{38}$$

then the estimator g is not resilient.

Remark 5 *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 fawzi Eldar and Kutyniok [2012]. A similar result [Fawzi et al., 2014, Proposition 6] is also given for the decoding condition without any noise. In this paper we prove a more general result, i.e., Theorem 1, 2 and 3, regarding the resiliency of a large collection of estimators in the noisy case.*

The main difficulty in Proposition 1 is to validate (37) or falsify (38) over all non-zero u's. We next show Proposition 1 in a more practically useful version when p is not large. Let $\rho \in \mathbb{R}^p$ be a vector with all entries from $\{-1, 1\}$ and $\mathcal{D}$ be the set of all possible ρ's. Note that the cardinality of $\mathcal{D}$ is 2^p.

Theorem 4 *Consider the following* $\binom{m}{p} \times 2^p$ *optimization problems for any index set* $\mathcal{I} \subset \mathcal{S}$ *with cardinality* p *and for any* $\rho \in \mathcal{D}$*:*

$$\begin{aligned} &\underset{u\in\mathbb{R}^n}{\textit{maximize}} && \rho^\top C_{\mathcal{I}} u \\ &\textit{subject to} && \|C_{\mathcal{S}} u\|_1 = 1. \end{aligned} \tag{39}$$

(a) If the optimal values of the above optimization problems are all strictly less than $1/2$*, then the estimator* g *is resilient.*
(b) If the optimal value of any one of the above optimization problems is strictly larger than $1/2$*, then the estimator* g *is not resilient.*

Proof. Since $\|C_{\mathcal{I}} u\|_1 = |C_{i_1} u| + \ldots + \left|C_{i_p} u\right|$, we know that the following two optimization problems are equivalent:

$$\begin{aligned} &\underset{u\in\mathbb{R}^n}{\textit{maximize}} && \|C_{\mathcal{I}} u\|_1 \\ &\text{subject to} && \|C_{\mathcal{S}} u\|_1 = 1, \end{aligned} \tag{40}$$

and

$$\begin{aligned} &\underset{\rho\in\mathcal{D}}{\textit{maximize}}\ \underset{u\in\mathbb{R}^n}{\textit{maximize}} && \rho^\top C_{\mathcal{I}} u \\ &\text{subject to} && \|C_{\mathcal{S}} u\|_1 = 1. \end{aligned} \tag{41}$$

Due to $\|C_{\mathcal{I}} u\|_1 + \|C_{\mathcal{I}^c} u\|_1 = \|C_{\mathcal{S}} u\|_1$, we have

$$\|C_{\mathcal{I}} u\|_1 \lesseqgtr \|C_{\mathcal{I}^c} u\|_1 \Leftrightarrow \|C_{\mathcal{I}} u\|_1 \lesseqgtr \frac{1}{2}\|C_{\mathcal{S}} u\|_1. \tag{42}$$

If for all u and $\mathcal{I}$ the optimal value of (40) is strictly less than $1/2$, from (37) and (42) we can conclude that g is resilient. In a similar way we can prove (b). ■

Theorem 4(a) requires $\binom{m}{p} \times 2^p$ enumerations of solving the optimization problem. In the next two theorems, we propose more conservative sufficient and necessary condition for resilience with computational complexity of $\binom{m}{p}$.

Theorem 5 *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*:*

$$\begin{aligned} &\underset{K\in\mathbb{R}^{n\times(m-p)}}{\textit{minimize}} && \|C_{\mathcal{I}} K\|_1 \\ &\textit{subject to} && K C_{\mathcal{I}^c} = \mathrm{I}_n, \end{aligned} \tag{43}$$

then the estimator g *is resilient.*

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

$$\|C_{\mathcal{I}}u\|_1 < \|C_{\mathcal{I}^c}u\|_1.$$

By enumerating all possible $\mathcal{I}$ we conclude the proof. ■

Notice that (43) is not necessary. Since $\xi = C_{\mathcal{I}^c}u$, ξ may not be able to take all possible value in $\mathbb{R}^{m-p}$.

Similarly, we can find a more conservative necessary condition implied by Theorem 2. By enumerating all $(C_{\mathcal{I}}, C_{\mathcal{I}^c})$ and utilizing the following result, we can identify whether g is resilient for a given H or not.

Theorem 6 *If there exists an index set $\mathcal{I}$ such that the following inequality holds:*

$$\|C_{\mathcal{I}}C_{\mathcal{I}^c}^{+}\|_1 > (\sqrt{m-p}+1)/2, \tag{44}$$

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 6:

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 following inequality holds:*

$$\|\xi_{\|}\|_1 \leq \frac{\sqrt{m}+1}{2}\|\xi\|_1. \tag{45}$$

Moreover, the above inequality is achievable when

$$\xi = \begin{bmatrix}1\\0\\\vdots\\0\end{bmatrix}, \xi_{\|} = \frac{1}{2}\begin{bmatrix}1+m^{-1/2}\\m^{-1/2}\\\vdots\\m^{-1/2}\end{bmatrix}, \xi_{\perp} = \frac{1}{2}\begin{bmatrix}1-m^{-1/2}\\-m^{-1/2}\\\vdots\\-m^{-1/2}\end{bmatrix}.$$

We are now ready to prove Theorem 6:

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 (44) holds. Since $\left\|C_{\mathcal{I}}C_{\mathcal{I}^c}^{+}\right\|_1 > (\sqrt{m-p}+1)/2$, we can find $\xi \in \mathbb{R}^{m-p}$, such that

$$\left\|C_{\mathcal{I}}C_{\mathcal{I}^c}^{+}\xi\right\|_1 > \frac{\sqrt{m-p}+1}{2}\left\|\xi\right\|_1.$$

Now we can decompose $\xi = \xi_{\|} + \xi_{\perp}$, where $\xi_{\|}$ belongs to the column space of $C_{\mathcal{I}^c}$ and $\xi_{\perp}$ is perpendicular to the column space of $C_{\mathcal{I}^c}$. By the property of Moore-Penrose inverse, $C_{\mathcal{I}^c}^{+}\xi_{\perp} = 0$. Therefore,

$$\left\|C_{\mathcal{I}}C_{\mathcal{I}^c}^{+}\xi\right\|_1 = \left\|C_{\mathcal{I}}C_{\mathcal{I}^c}^{+}\xi_{\|}\right\|_1.$$

On the other hand, since $\xi \in \mathbb{R}^{m-p}$, by Lemma 4, we have

$$\frac{\sqrt{m-p}+1}{2}\left\|\xi\right\|_1 \geq \left\|\xi_{\|}\right\|_1,$$

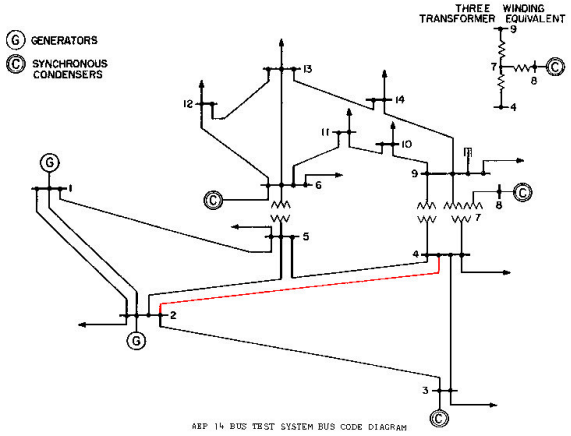

Fig. 1. Single line diagram of IEEE 14-bus test system Christie [2000].

which implies that

$$\left\|C_{\mathcal{I}}C_{\mathcal{I}^c}^{+}\xi_{\|}\right\|_1 > \left\|\xi_{\|}\right\|_1 .$$

Since $\xi_{\|}$ belongs to the column space of $C_{\mathcal{I}^c}$, there exists a u, such that $C_{\mathcal{I}^c}u = \xi_{\|}$. 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

In this section we validate our main results on the IEEE 14-bus test system Christie [2000]. 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 Zimmerman et al. [2011]. The state variables are voltage angles of all buses (excluding the slack Bus 1), and the scalar meter measurements are real power injections of all buses and real power flows of all branches. For the sake of space saving, we do not include the full H matrix here and we recommend interested readers to see Liu et al. [2011], Zimmerman et al. [2011], Christie [2000] for details.

We use the estimator g described in (12). By solving the optimization problem (13) explicitly, we know that f can be explicitly written as:

$$f(u) = \begin{cases} u^2, & \text{if } |u| \le \frac{1}{2}\lambda, \\ \lambda\,|u| - \frac{1}{4}\lambda^2, & \text{if } |u| > \frac{1}{2}\lambda. \end{cases} \tag{46}$$

One can verify that $C_i(u) = |H_i u|$. According to Theorem 4, we find that g is not resilient when $p \ge 2$. 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 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 BI_i means the sensor measuring the real power injection of i-th bus.

We can also check the tightness of Theorem 5 and Theorem 6 which are actually more suitable for a large p. Based on Theorem 5, the experimental result shows that only when $p = 1$, the estimator g is resilient. On the other hand, when $p \ge 3$, the estimator g is not resilient from Theorem 6. The only case that Theorem 5 and 6 cannot verify is when $p = 2$.

[1] The branch indices follow MATPOWER Zimmerman et al. [2011]

BP_1	BP_6	BP_7	BP_{16}	BI_1	BI_2	BI_7	BI_{12}
BI_1	BI_3	BI_5	BI_9	BI_2	BI_4	BI_9	BI_{13}

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

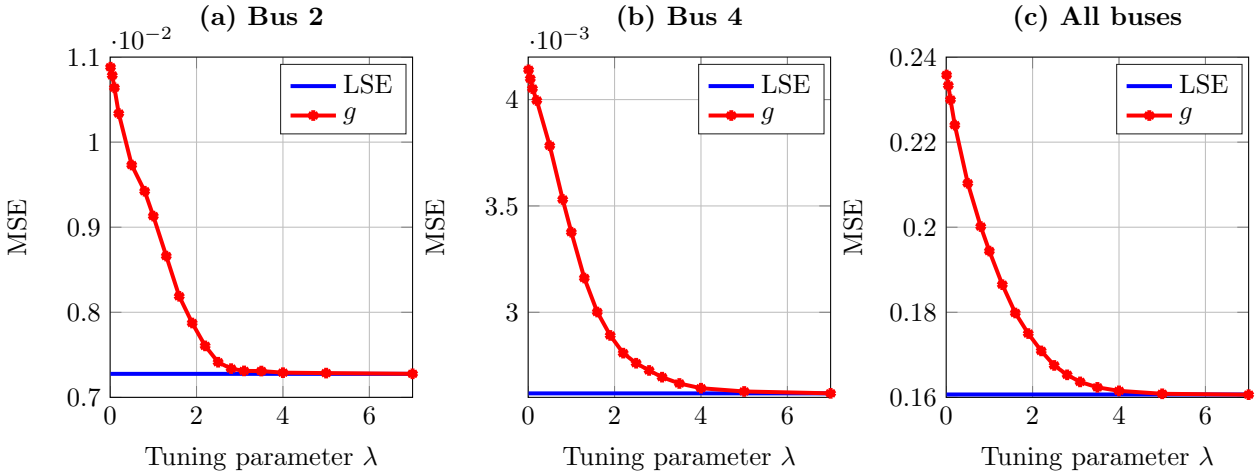

Fig. 2. Performance of the least square estimator (red dotted line) and the resilient estimator g (blue solid line) when no sensors are being attacked.

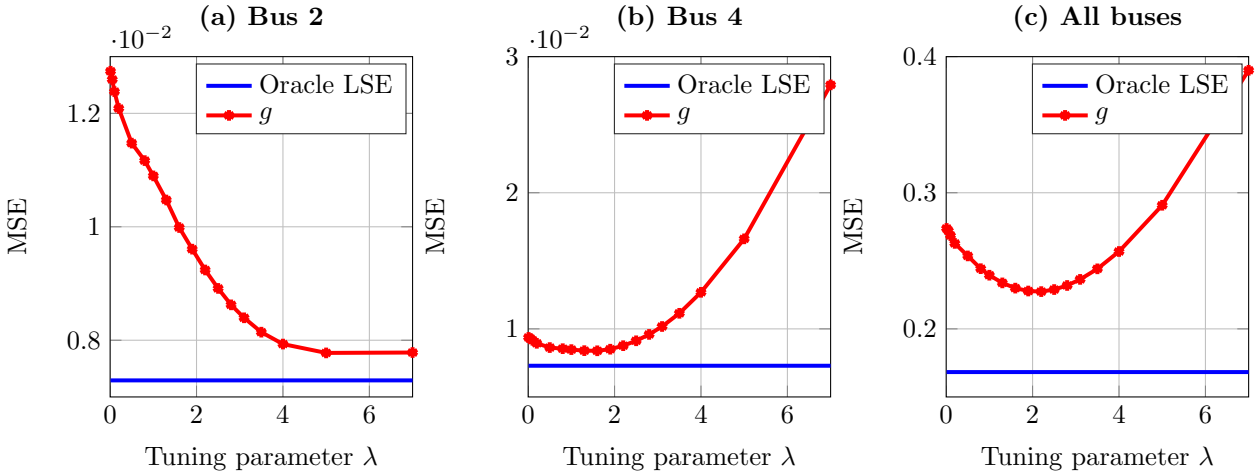

Fig. 3. Performance of the oracle least square estimator (red dotted line) and the resilient estimator g (blue solid line) when one sensor is under attacks.

5.1 Tradeoff between efficiency and resiliency

Next we conduct experiments to compare the performance of the resilient estimator g in (14) with different tuning factors λ's and the least square estimator (LSE), under either normal operation or the attack. We will see the performance of g and the important role of λ, by tuning which we can achieve a desirable tradeoff between efficiency (MSE during normal operation) and resiliency (MSE during the attack). If attacked, the sensor monitoring the power flow of the 4th branch marked in red in Fig.1 is assumed to be manipulated. Thus we focus more on the state estimation of the voltage angles of Bus 2 and 4 connected by the 4th branch. Each entry of the state vector x is assumed to be a uniform random variable in $[0, 2\pi]$. Moreover, we assume the measurement noise is Gaussian distributed with zero mean and unit variance.

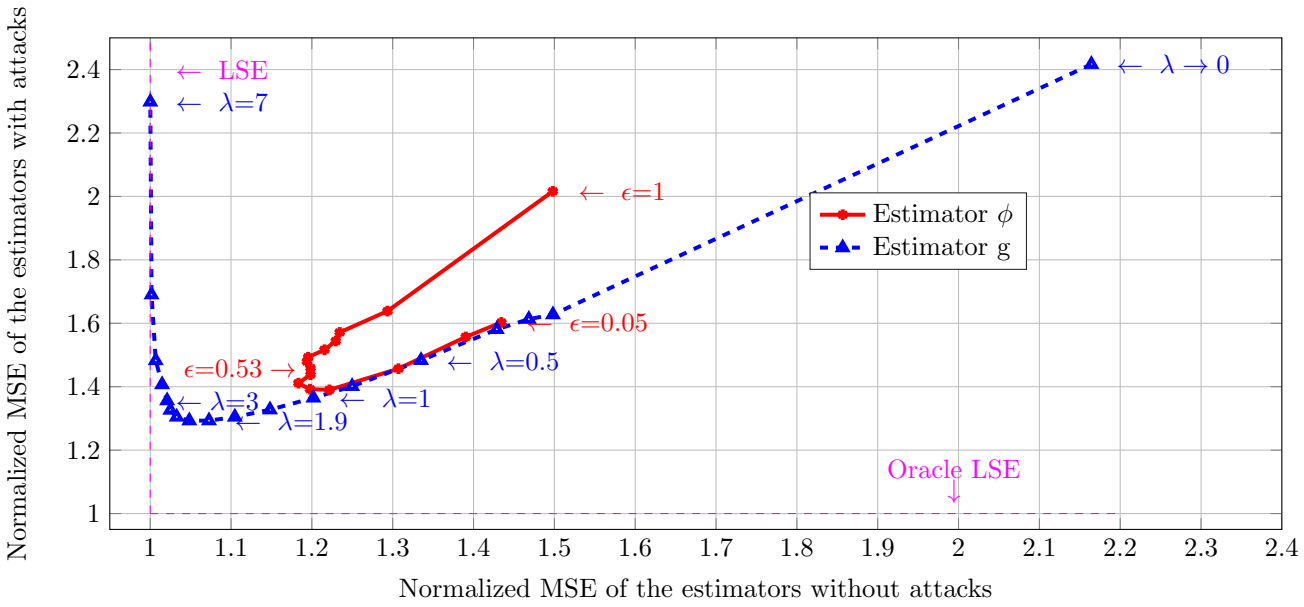

Fig. 4. Normalized MSE (all buses) of the estimators g and ϕ without any attacks versus normalized MSE (all buses) of the estimators g and ϕ under $(1, 34)$-sparse attack. The sensor monitoring the power flow of the 4th branch is assumed to be manipulated.

Normal Operation (Fig.2): Without any attacks, we plot the mean square error (MSE) of the voltage angle of Bus 2 and Bus 4, and the total MSE of all buses versus λ, respectively. The solid curve in blue represents the MSE of LSE as a benchmark. Note that by increasing λ, we can improve the estimation performance of g until it approximately reaches the optimal MSE obtained by LSE.

Under the Attack (Fig.3): The sensor monitoring the power flow of the 4th branch is assumed to be manipulated (the nominal value changed to -10^4). The solid curve in blue represents the MSE of the oracle LSE which exactly knows the id of the attacked sensor and discards the corresponding measurement. The oracle LSE is impossible to implement in practice as one in general does not know which sensors are under attack. However it provides a theoretically lower bound on the MSE for any resilient estimator.

Notice that from Fig.3, there is an optimal λ for the estimation performance under the attack. On the other hand, the estimation performance under normal operation is better with a larger λ. This requires us to design an appropriate λ to obtain a desirable tradeoff between the resiliency and efficiency of g.

5.2 Comparisons of Different Choices of Estimators

For different estimators discussed in Section 2.2, we plot their MSE under normal operation and under the attack in Fig. 4. 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. The x-axis represents the normalized MSE when there is no attack, by normalizing MSE of g over MSE of LSE.

The blue line in Fig. 4 represents the Lasso estimator (14). Notice that when $\lambda \to 0$, the Lasso estimator converges to the median estimator (7) and geometric median estimator (8). From the curve, it can be seen that a good choice of λ is around 2.

The red line in Fig. 4 represents the estimator (9). We choose the set

$$\Omega_i = \{w \in \mathbb{R} : |w| \leq \epsilon\}, \forall i.$$

Notice that Pajic et al. Pajic et al. [2014, 2015] proposed to use this estimator for the bounded noise scenario. However, in this paper, we prove that the estimator (9) is resilient to the attack even if the true w_i is outside Ω_i.

Hence, in this simulation we will use ϵ as a tuning parameter. The plot in red illustrates the efficiency and resiliency of the estimator (9) by varying ϵ. It is easy to see that for our simulation, the Lasso estimator out-performs the estimator (9). However, it is still an open question what cost function f_i should be chosen in order to achieve the optimal performance, which we would like to pursue as a future direction.

6 Concluding Remarks

We have studied the resilient estimation problem where sensor networks are exposed to (p, m)-sparse integrity attacks. The malicious measurements are assumed to be arbitrarily manipulated. No assumptions on the attack patterns and fault detection mechanism make 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 integrate 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 validate our theoretical results and illustrate how to apply the theories to real applications.

Future works include the resilience analysis for the dynamical state estimation problem. How to elegantly design the f_i's in (5) to satisfy different applications and requirements is another interesting open problem.

7 Appendix

Proof of Lemma 2:

(i) If $\alpha = 0$, then clearly $C_i(0) = 0$. On the other hand, if $\alpha \neq 0$, from the definition in (16), we have

$$\begin{aligned} C_i(\alpha u) &= \lim_{t\to\infty} \frac{1}{t} f_i(|\alpha| t H_i u) \\ &= |\alpha| \lim_{t\to\infty} \frac{1}{|\alpha|\, t} f_i(|\alpha| t H_i u) = |\alpha|\, C_i(u). \end{aligned}$$

The first inequality is due to the symmetry of f. Due to the scaling property of $C_i(u)$ and the convexity of f_i, we have

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

Therefore, we know that C_i is actually a semi-norm on $\mathbb{R}^n$.

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

$$2f_i(\frac{tH_i u}{2}) \leq f_i(v + tH_i u) + f_i(-v), \tag{47}$$

$$f_i(tH_i u) \geq 2f_i(\frac{2v + tH_i u}{2}) - f(2v). \tag{48}$$

Dividing both sides of (47) and (48) by t and taking limit over t, we have

$$C_i(u) \leq \liminf_{t\to\infty} \frac{1}{t} f_i(v + tH_i u) + \lim_{t\to\infty} \frac{1}{t} f_i(-v), \tag{49}$$

$$C_i(u) \geq \limsup_{t\to\infty} \frac{2}{t} f_i(v + \frac{t}{2} H_i u) - \lim_{t\to\infty} \frac{1}{t} f_i(2v). \tag{50}$$

Since $\lim_{t\to\infty} f_i(-v)/t = \lim_{t\to\infty} f_i(2v)/t = 0$, from (50) and (49) we have the following pointwise limit

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

Notice that for a fixed (u, v), by Lemma 1, $h(u, v, t)$ 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 Rudin [1964], $h(u, v, t)$ 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

$$f_i(v + kH_iu) - f_i(v + (k-1)H_iu) \leq f_i(v + (k+1)H_iu) - f_i(v + kH_iu).$$

Hence we can conclude that

$$\begin{aligned} & f_i(v + H_iu) - f_i(v) \\ \leq & \lim_{t\to\infty} \frac{1}{n} \sum_{i=1}^{n} (f_i(v + kH_iu) - f_i(v + (k-1)H_iu)) \\ = & \lim_{t\to\infty} \frac{1}{n} (f_i(v + kH_iu) - f_i(v)) \\ = & C_i(u). \end{aligned}$$

Thus we completes the proof. ■

Proof of Lemma 3:

From (31) and (47), it is easy to see that $h_j(u_0, v, t)$ diverges to infinity for all v, *i.e.*,

$$h_j(u_0, v, t) \to +\infty. \tag{51}$$

Next we will show this divergence is also uniform. Denote $\mathcal{W}_t \triangleq \{v : h_j(u_0, v, t) > M\}$. 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 $t \leq t'$. Since for each v there exists t such that $h_j(u_0, v, t) > M$ from (51),

$$\bigcup_{t\geq 0} \mathcal{W}_t = \mathbb{R}^{m_i}.$$

Therefore, the collection $\{\mathcal{W}_t\}$ is an open cover for the compact subset $\mathcal{V}$. Thus, we can find a finite cover $\mathcal{W}_{t_1}, \ldots, \mathcal{W}_{t_l}$ that covers $\mathcal{V}$, i.e.,

$$\mathcal{V} \subseteq \mathcal{W}_{t_1} \cup \mathcal{W}_{t_2} \cup \cdots \cup \mathcal{W}_{t_l}. \tag{52}$$

Now we can define $N = \max(t_1, \ldots, t_l)$. Since $\mathcal{W}_t$ is non-decreasing with respect to t, the RHS of (52) is $\mathcal{W}_N$. For any $t \geq N$, we have

$$\mathcal{V} \subseteq \mathcal{W}_N \subseteq \mathcal{W}_t,$$

which combined with the definition of $\mathcal{W}_t$ finishes the proof. ■

Proof of Lemma 4:

Geometrically, $\xi_{\|}$ can be written as $\xi_{\|} = \xi/2 + r$, where $r \in \{r : \|r\|_2 = \|\xi\|_2/2\}$. As a result, we have

$$\begin{aligned} \|\xi_{\|}\|_1 \leq \frac{1}{2}\|\xi\|_1 + \|r\|_1 \leq \frac{1}{2}\|\xi\|_1 + \sqrt{m}\|r\|_2 \\ = \frac{1}{2}\|\xi\|_1 + \frac{\sqrt{m}}{2}\|\xi\|_2 \leq \frac{1}{2}\|\xi\|_1 + \frac{\sqrt{m}}{2}\|\xi\|_1. \end{aligned}$$

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 ξ,

$$\|\xi\|_2 \leq \|\xi\|_1 \leq \sqrt{m}\|\xi\|_2.$$

Without loss of generality, let us assume that $\|\xi\|_1 = 1$. The achievability of (45) is easy to verify. ■

References

S Massoud Amin. Smart grid security, privacy, and resilient architectures: Opportunities and challenges. In *IEEE Power and Energy Society General Meeting*, pages 1–2, 2012.

Alvaro A Cárdenas, Saurabh Amin, and Shankar Sastry. Research challenges for the security of control systems. In *Proceedings of the 3rd Conference on Hot topics in security*, page 6, 2008.

T. M. Chen. Stuxnet, the real start of cyber warfare? [editor's note]. *IEEE Network*, 24(6):2–3, 2010. doi: 10.1109/MNET.2010.5634434.

Michelle S Chong, Masashi Wakaiki, and Joao P Hespanha. Observability of linear systems under adversarial attacks. In *Proceedings of American Control Conference*, 2015.

R Christie. Power systems test case archive, university of washington. *Electrical Engineering. Online: http://www. ee. washington. edu/research/pstca/*, 2000.

David L Donoho and Peter J Huber. The notion of breakdown point. *A Festschrift for Erich L. Lehmann*, pages 157–184, 1983.

Yonina C Eldar and Gitta Kutyniok. *Compressed sensing: theory and applications*. Cambridge University Press, 2012.

Hamza Fawzi, Paulo Tabuada, and Suhas Diggavi. Secure estimation and control for cyber-physical systems under adversarial attacks. *IEEE Transactions on Automatic Control*, 59(6):1454–1467, 2014. ISSN 00189286. doi: 10.1109/TAC.2014.2303233.

D. P. Fidler. Was stuxnet an act of war? decoding a cyberattack. *IEEE Security & Privacy*, 9(4):56–59, 2011. doi: 10.1109/MSP.2011.96.

Frank R. Hampel. A general qualitative definition of robustness. *The Annals of Mathematical Statistics*, 42(6): 1887–1896, 1971.

Frank R. Hampel. The influence curve and its role in robust estimation. *Journal of the American Statistical Association*, 69(346):383–393, 1974.

E. Handschin, F.C. Schweppe, J. Kohlas, and A. Fiechter. Bad data analysis for power system state estimation. *IEEE Transactions on Power Apparatus and Systems*, 94(2):329–337, March 1975. ISSN 0018-9510. doi: 10.1109/T-PAS.1975.31858.

Peter J. Huber and Elvezio M. Ronchetti. *Robust Statistics*. NJ: Wiely, 2009.

Saleem Kassam, H Vincent Poor, et al. Robust techniques for signal processing: A survey. *Proceedings of the IEEE*, 73(3):433–481, 1985.

Jinsub Kim, Lang Tong, and Robert J. Thomas. Data framing attack on state estimation. *IEEE Journal on Selected Areas in Communications*, 32(7):1460–1470, July 2014. ISSN 0733-8716. doi: 10.1109/JSAC.2014.2332032.

Yuzhe Li, Ling Shi, Peng Cheng, Jiming Chen, and Daniel Quevedo. Jamming attacks on remote state estimation in cyber-physical systems: A game-theoretic approach. *IEEE Transactions on Automatic Control*, 60(10):2831 – 2836, 2015.

Yao Liu, Michael Reiter, and Peng Ning. False data injection attacks against state estimation in electric power grids. In *Proceedings of ACM Conference Computer and Communnication Security*, 2009.

Yao Liu, Peng Ning, and Michael K Reiter. False data injection attacks against state estimation in electric power grids. *ACM Transactions on Information and System Security*, 14(1):13, 2011.

Hendrik P. Lopuhaa and Peter J. Rousseeuw. Breakdown points of affine equivariant estimators of multivariate location and covariance matrices. *The Annals of Statistics*, 19(1):229–248, 1991. ISSN 0090-5364. doi: 10.1214/aos/1176347978.

Ricardo A. Maronna, Douglas R. Martin, and Victor J. Yohai. *Robust Statistics: Theory and Methods*. NJ: Wiley, 2006.

L. Mili, Th. Van Cutsem, and M. Ribbens-Pavella. Bad data identification methods in power system state estimation - a comparative study. *IEEE Power Engineering Review*, PER-5(11):27–28, November 1985. ISSN 0272-1724. doi: 10.1109/MPER.1985.5528357.

Y. Mo, E. Garone, A. Casavola, and B. Sinopoli. False data injection attacks against state estimation in wireless sensor networks. In *Proceedings of IEEE Conference Decision and Control*, pages 5967–5972, 2010. doi: 10.1109/CDC.2010.5718158.

Yilin Mo and Bruno Sinopoli. False data injection attacks in cyber physical systems. In *First Workshop on Secure Control Systems*, 2010.

Mete Ozay, Inaki Esnaola, FT Vural, Sanjeev R Kulkarni, and H Vincent Poor. Sparse attack construction and state estimation in the smart grid: Centralized and distributed models. *IEEE Journal of Selected Areas in Communnication*, 31(7):1306–1318, 2013.

Miroslav Pajic, James Weimer, Nicola Bezzo, Paulo Tabuada, Oleg Sokolsky, Insup Lee, and George J. Pappas. Robustness of attack-resilient state estimators. In *Proceedings of ACM/IEEE International Conference Cyber-Physical Systems*, pages 163–174, April 2014. ISBN 978-1-4799-4930-4. doi: 10.1109/ICCPS.2014.6843720.

Miroslav Pajic, Paulo Tabuada, Insup Lee, and George J. Pappas. Attack-resilient state estimation in the presence of noise. In *Proceedings of IEEE Conference on Decision and Control*, pages 5827–5832, 2015.

F. Pasqualetti, A. Bicchi, and F. Bullo. Consensus computation in unreliable networks: a system theoretic approach. *IEEE Transactions on Automatic Control*, 57(1):90–104, Jan 2010.

Fabio Pasqualetti, Florian Dorfler, and Francesco Bullo. Cyber-physical attacks in power networks: models, fundamental limitations and monitor design. In *Proceedings of IEEE Conference Decision and Control and European Control Conference*, pages 2195–2201, 2011. doi: 10.1109/CDC.2011.6160641.

Walter Rudin. *Principles of mathematical analysis*, volume 3. McGraw-Hill New York, 1964.

Henrik Sandberg, Andre Teixeira, and Karl H. Johansson. On security indices for state estimators in power networks. In *First Workshop on Secure Control Systems*, 2010.

S. Sundaram, M. Pajic, C. Hadjicostis, R. Mangharam, and G. J. Pappas. The wireless control network: monitoring for malicious behavior. In *Proceedings of IEEE Conference Decision and Control*, 2010.

Robert Tibshirani. Regression shrinkage and selection via the lasso. *Journal of the Royal Statistical Society. Series B (Methodological)*, pages 267–288, 1996.

Le Xie, Yilin Mo, and B. Sinopoli. Integrity data attacks in power market operations. *IEEE Transactions on Smart Grid*, 2(4):659–666, 2011. doi: 10.1109/TSG.2011.2161892.

Heng Zhang, Peng Cheng, Ling Shi, and Jiming Chen. Optimal DoS attack scheduling in wireless networked control system. *IEEE Transactions on Control Systems Technology, to be published*, 2015.

Ray Daniel Zimmerman, Carlos Edmundo Murillo-Sánchez, and Robert John Thomas. MATPOWER: Steady-state operations, planning, and analysis tools for power systems research and education. *IEEE Transactions on Power Systems*, 26(1):12–19, 2011.