J. Mod. Power Syst. Clean Energy (2019) 7(5):1071–1080
https://doi.org/10.1007/s40565-019-0561-2

Non-linear state recovery in power system under bad data and cyber attacks

Ali TAJER[1], Saurabh SIHAG[1], Khawla ALNAJJAR[2]

Abstract The problems of recovering the state of power systems and detecting the instances of bad data have been widely studied in literature. Nevertheless, these two operations have been designed and optimized for the most part in isolation. Specifically, state estimators are optimized based on the minimum mean-square error criteria, which is only optimal when the source of distortions in the data is Gaussian random noise. Hence, the state estimators fail to perform optimality when the data is further contaminated by bad data, which cannot necessarily be modeled by additive Gaussian terms. The problem of power state estimation has been studied extensively. But the fundamental performance limits and the attendant decision rules are unknown when the data is potentially compromised by random bad data (due to sensor failures) or structured bad data (due to cyber attacks, which are also referred to false data injection attacks). This paper provides a general framework that formalizes the underlying connection between state estimation and bad data detection routines. We aim to carry out the combined tasks of detecting the presence of random and structured bad data, and form accurate estimations for the state of power grid. This paper characterizes the optimal detectors and estimators. Furthermore, the gains with respect to the existing state estimators and bad data detectors are established through numerical evaluations.

Keywords State estimation, Power system security, Bad data detection, Data injection attack

CrossCheck date: 28 April 2019

Received: 16 November 2018 / Accepted: 28 April 2019 / Published online: 30 July 2019

✉ Ali TAJER
tajer@ecse.rpi.edu

Saurabh SIHAG
sihas@rpi.edu

Khawla ALNAJJAR
kalnajjar@sharjah.ac.ae

[1] Rensselaer Polytechnic Institute, 110 8th Street, Troy, NY 12180, USA

[2] University of Sharjah, United Arab Emirates, P. O. Box 27272, Sharjah, UAE

1 Introduction

1.1 Motivation

Estimating the state of power grid, i.e., recovering bus voltages and phase angles, was initially formalized in the 1970s. State estimation involves designing algorithms that leverage the data collected by various measurement units across the grid as well as other information about power grid (e.g., topology and dynamics) in order to form an estimation for the state of power grid [1]. These state estimations serve multiple purposes including informing control actions, predicting loads, updating pricing policies and identifying abnormalities in power grid. In support of these tasks, various types of measurements are collected and transmitted to a control center via remote terminal units. Therefore, intelligent electronic devices and state estimation algorithms are key to build a real-time network model within the energy management system (EMS) [2, 3]. Traditional state estimation approaches, which are conducted centrally in power grid control center, perform three main routines [4].

1) Observability analysis: its role is to determine whether a unique state estimation can be characterized for the state of the system. Observability analysis is generally performed prior to state estimation.
2) State estimation: it is responsible for characterizing an optimal estimation for the complex voltages at different buses by leveraging the real-time measurements.
3) Bad data detection: the estimations formed are used in order to determine whether the measurements bear any errors, identify them when they are deemed to exist, and eliminate them in order to enhance state estimation fidelity.

There exists a rich literature of various approaches to bad data detection under different assumptions on the data model or network topology. The existing design principles for bad data detection often use gross measurement errors, that is the difference between the measurements and the estimations of measurements, which is found by using the state estimation. When such gross measurement errors are small enough, the estimation is deemed reliable, and when the errors are large enough, the measurements are considered to contain bad data [4]. Such bad detector approaches are effective against the bad data that has a random cause (e.g., failure in power grid). Nevertheless, when the disruptions are structured (not random), there exists a high likelihood that the bad data can bypass the bad data detectors. For instance, when the disruptions affect the measurements in a way that they conform to the physical laws and the topology of power grid, they can appear as legitimate measurements [5]. Such a possibility raises concerns about security vulnerabilities that state estimation faces, which can be capitalized by the adversaries to launch attacks. Such attack, for instance, can contaminate the measurements without being detected, while misleading the state estimators, rendering wrong estimations for the system. The possibility of such attacks is especially strenuous as more advanced measurement units are incorporated into EMS.

The effectiveness of cyber attacks for contaminating the measurements and misleading the state estimators, while remaining hidden from bad data detector strongly hinges on the extent of information that the attackers possess on power grid. The two extreme cases in which the attackers either have full and perfect information about power grid, or have no information extensively studied in the literature. When the attacker has no information, all it can do is to produce random bad data. Such bad data can be efficiently detected by using the traditional bad data detectors [4], even though the existing approaches, as we will discuss later are not optimal. On the other hand, in which the attackers have full and perfect information about all the dynamics of power grid, the attacks can be designed intelligently so that they appear as legitimate data and can bypass the traditional bad data detection algorithms [5]. While such attacks can cause severe damages, assuming that they are not realistic. Specifically, the strong assumption that all the instantaneous dynamics of power grid fully known to the attackers is hard to meet in practice.

In this paper, we propose a framework for recovering the state of the system while facing the potential risk that the measurements are contaminated by random bad data or structured bad data. Furthermore, we assume that when the data is contaminated by structured bad data (i.e., attacks), the attackers are assumed to have only partial information about power grid topology and its time-varying dynamics. The objective of this framework is two-fold. The primary objective is forming a reliable estimation for the state. The second objective of forming reliable state estimation pertains to detect whether there exists any source of random or structured bad data in the measurements.

1.2 Existing studies

The focus of this paper is on false data injection attacks (FDIAs). The main objective of the FDIAs is to disrupt power grid functions while avoiding the possibility of being detected by bad data detectors [6]. Even though the FDIAs mainly aim to distort state estimation, their disruptions exceed and can affect a wide range of control and dispatch decisions. More specifically, a compromised estimation of the system state can lead to non-optimal dispatch. There exist studies that investigate the minimum number of measurements that should be tampered with to make an effective attack. The dynamics between the number of measurement units protected (or compromised) and the effectiveness of the attacks are studied in [7].

An analytical approach to evaluate the impact of FDIAs that can evade bad data detectors and affect electricity market is formalized in [8]. The study in [9] presents another FDIA design strategy, which maximizes the generated market revenue with a single measurement attack. Based on the multi-step electricity price (MEP) model introduced in [10], the impact of FDIAs in the real-time market against MEP is investigated in [11]. In order to incorporate the inter-temporal constraints, [12] proposes an attack strategy to withhold generation capacity for profit by manipulating the ramp constraints of the generators during look-ahead dispatch. In [13], an FDIA strategy based on the geometric characterization of the real-time marginal prices on the state space of power grid is proposed.

Game-theoretic approaches to model the interactions between the attack and defense strategies are investigated in [14, 15]. Specifically, the study in [14] focuses on mechanisms based on attacks that disrupt state estimation,

and consequently, manipulate the ensuing decisions that rely on the state estimation. The study in [15] examines the compromising of the communication channels that carry the measurement information to manipulate market decisions. The idea of directly jamming the pricing signals is studied in [16], where the attackers can make a profit without intruding the power system and changing the reported data. The study in [17] analyzes attack strategies by using a nonlinear model for power systems and state estimators. The impacts of adversaries with limited information about the network on the market operations are studied in [18–20].

2 Preliminaries

2.1 Bad data and attack models

Consider a general non-linear system model, the measurement vector $\boldsymbol{y} \in \mathbb{R}^n$ is related to the state of the system $\boldsymbol{x} \in \mathbb{R}^m$ according to:

$$\boldsymbol{y} = \boldsymbol{h}(\boldsymbol{x}) + \boldsymbol{z} \tag{1}$$

where $\boldsymbol{h}$ captures the dynamics and topology of power grid, and $\boldsymbol{z}$ accounts for the measurement noise. This model represents the instances at which the only source of the contamination in the measurements is noise. Furthermore, when there exists random failure in the network (e.g., malfunctioning measurement units) or an attacker or a group of attackers compromising the measurements, the non-linear system model changes according to:

$$\boldsymbol{y} = \boldsymbol{h}(\boldsymbol{x}) + \boldsymbol{z} + \boldsymbol{b} \tag{2}$$

where $\boldsymbol{b}$ accounts for the effects of injected random or structured bad data. Based on the currently widely-used approaches, for a given state estimation, denoted by $\hat{\boldsymbol{x}}$, the set of measurement is considered to contain bad data based on a gross measurement test. Specifically, it is decided that the bad data exists if the gross measurement error exceeds a pre-specified threshold τ, i.e.:

$$\text{declare bad data if} \quad \|\boldsymbol{y} - \boldsymbol{h}(\hat{\boldsymbol{x}})\|_2 \geq \tau \tag{3}$$

The key weakness of such a bad data detector is that it does not detect bad data vectors $\boldsymbol{b}$ that are designed properly so that the distorted measurement $\boldsymbol{h}(\boldsymbol{x}) + \boldsymbol{z} + \boldsymbol{b}$ appears as a legitimate measurement vector. For instance, in a linearized system model, when $\boldsymbol{b}$ is aligned in the range space of the Jacobian matrix $\boldsymbol{H}$ (found by linearizing $\boldsymbol{h}$). It can bypass the residue-based detectors, as discussed in [5]. Furthermore, even when bad data is detected, the only existing remedy is to collect fresh measurements in the hope of having better data, and subsequently, producing a reliable estimation.

The primary cause of such weaknesses for the bad data detector in (3) is that: ① the state estimation and the bad data detection decisions are treated as independent routines as it ignores the inherent coupling between the two decisions; and ② it tends not to fully capitalize on the rich redundancy in the measurements because the dimension of the observation space n is significantly larger than that of the state space m. When these two routines (e.g., state estimator and bad data detector) are designed by properly leveraging the fundamental underlying connection, and the redundancy in measurements is capitalized effectively, it is possible to mitigate the effects of bad data to a large extent. Specifically, while the objective is estimating the state, a decision should also be made, in parallel, about the underlying observation model. These combined decisions can be cast as a composite hypothesis test problem, in which hypothesis H_0 represents the model in which the only data contamination is noise, and hypotheses H_1 and H_2 represent the cases in which the data is contaminated by structured and random bad data, respectively:

$$\begin{cases} H_0: & \boldsymbol{y} = \boldsymbol{h}(\boldsymbol{x}) + \boldsymbol{z} \\ H_1: & \boldsymbol{y} = \boldsymbol{h}(\boldsymbol{x}) + \boldsymbol{z} + \boldsymbol{b} \quad \text{structured bad data} \\ H_2: & \boldsymbol{y} = \boldsymbol{h}(\boldsymbol{x}) + \boldsymbol{z} + \boldsymbol{b} \quad \text{random bad data} \end{cases} \tag{4}$$

We remark that cases of random and structured bad data are treated under different models to emphasize that the nature and models of the data under these two scenarios are distinct. Specifically, random bad data accounts for the naturally-occurring failures in power grid such as line outages when power grid is stressed. The disruptions in the measurements when such failures occur often follow a random behavior. In contrast, under cyber attacks, the disruptions are designed carefully in order to impose a certain interruption on the functions in power grid. For instance, an attacker exploits some information about the network in order to launch an attack that effectively distorts the state estimation $\hat{\boldsymbol{x}}$, while not being detected by the bad data detector.

2.2 Information model of attacker

In this paper, the focus is on the data injection attack model presented in (2). In such models, the attacker tampers with the measurement units (e.g., phasor measurement units) such that they report false data to the network operator. Such attacks can lead to a series of disruptions in the monitoring (e.g., state estimation) and the ensuing actions (e.g., generation and dispatching).

As commented earlier, the effectiveness and the design of the effective cyber attacks strongly hinge on the amount of information that the attacker has about the network topology and dynamics. All such information is embedded in $\boldsymbol{h}$. For instance, in a linearized system with $\boldsymbol{H}$, this information is embedded in the entries of $\boldsymbol{H}$. In order to distinguish the full information about the network and what is known to the attacker, we define $\bar{\boldsymbol{h}}$ as the partial information about $\boldsymbol{h}$ known to the attacker. For instance, in a linearized setting, instead of the full information about $\boldsymbol{H}$, the attacker knows only a noisy version of this matrix, which we denote by $\bar{\boldsymbol{H}}$. Clearly, the case of $\bar{\boldsymbol{h}} = \boldsymbol{h}$ represents the scenario in which the attacker has full information about the network. In this paper, we consider a general setting and do not impose any constraint on the relevance of $\bar{\boldsymbol{h}}$ and $\boldsymbol{h}$. Such an assumption facilitates a wide range of attack information models. All the analyses provided are general and can be applied to all choices of $\bar{\boldsymbol{h}}$. Such choices span the scenario of fully informed attackers ($\bar{\boldsymbol{h}} = \boldsymbol{h}$) to the more practical assumption. And it has only partial information about $\boldsymbol{h}$ available to the attacker.

For a given $\bar{\boldsymbol{h}}$, the attack strategy can be modeled as a function that maps $\bar{\boldsymbol{h}}$ to $\boldsymbol{b}$, i.e.,

$$\phi : \mathbb{R}^{n\times m} \rightarrow \mathbb{R}^{n\times 1} \tag{5}$$

We remark the optimal design of $\boldsymbol{b}$ in a linearized system when the information about the Jacobian matrix associated with $\boldsymbol{h}$ is fully known to the attackers [21].

3 State recovery under bad data

3.1 Data models

We define the sets $\Omega_{\boldsymbol{x}} \subseteq \mathbb{R}^m$ and $\Omega_{\boldsymbol{b}} \subseteq \mathbb{R}^m$ as the spaces of valid values for $\boldsymbol{x}$ and $\boldsymbol{b}$, respectively. Furthermore, we assume that $\boldsymbol{x}$ and $\boldsymbol{b}$ are distributed in their designated spaces $\Omega_{\boldsymbol{x}}$ and $\Omega_{\boldsymbol{b}}$ according to known statistical models. It is noteworthy that the distribution of $\boldsymbol{x}$ in space $\Omega_{\boldsymbol{x}}$ can be found by leveraging the historical data about the state parameters. When such patterns are not available or they are not reliable enough for forming a statistical model, we assume that $\boldsymbol{x}$ is distributed in $\Omega_{\boldsymbol{x}}$ according to a uniformed distribution. Similarly, by leveraging the information and the historical data on the failure patterns of the measurement units, the distribution of $\boldsymbol{b}$ in space $\Omega_{\boldsymbol{b}}$ can be characterized. Finally, in case of structured bad data (attacks), due to the unknown nature of the attacks or attack strategies, we assume that $\boldsymbol{b}$ takes values in its designated space $\Omega_{\boldsymbol{b}}$ according to a uniformed distribution.

We denote the the probability density function (PDF) of $\boldsymbol{x}$ under hypothesis H_i by $\pi_i(\boldsymbol{x})$, for $i \in \{0, 1, 2\}$. Finally, by accounting for the randomness of the noise measurements $\boldsymbol{z}$, the measurements under hypothesis H_i are distributed according to:

$$H_i : \quad \boldsymbol{y} \sim f_i(\boldsymbol{y} \mid \boldsymbol{x}) \quad \text{and} \quad \boldsymbol{x} \sim \pi_i(\boldsymbol{x}) \tag{6}$$

where f_i is the PDF of $\boldsymbol{y}$, which is governed by the distribution of noise. Based on this formulation, the state estimation problem reduces to concurrently detect the true hypothesis and estimate the unknown vector $\boldsymbol{x}$.

There exists a few sub-optimal approaches in solving such combined problems. All these approaches decouple the joint problem into two disjoint estimation and detection routine. One major class is that the problem is reduced to an estimation-driven detection. An estimation is formed under each hypothesis, reducing it into a pure detection problem, and then an optimal detection routine is carried out. The most prevalent approach in this direction is the generalized likelihood ratio test (GLRT). The second major class involves parallel detection and estimation, in which multiple estimations are formed under various hypotheses. Also, a detection decision is formed in parallel. If the detection rules are in favor of hypothesis H_i, then the estimation formed under hypothesis H_i will be admitted as the estimation of interest. Despite their popularity, all such approaches are sub-optimal.

In this paper, we take a radically different approach to treat the combined problem. Aiming to form reliable estimations, we provide a natural formulation in which the objective is optimizing a relevant cost function, while in parallel, controlling the detection power. This approach results in novel optimal designs for estimators that are designed based on a decoupling approach.

3.2 Bad data detection

To formalize the detection routine and characterize optimal detection rules, we start by defining a randomized test with decision rules denoted by $\{\delta_0(\boldsymbol{y}), \delta_1(\boldsymbol{y}), \delta_2(\boldsymbol{y})\}$. In this test, given data $\boldsymbol{y}$, the rule $\delta_i(\boldsymbol{y})$ denotes the likelihood of deciding H_i for $i \in \{0, 1, 2\}$. These probability terms satisfy:

$$\begin{cases} \delta_i(\boldsymbol{y}) \geq 0 \\ \sum_{i=0}^{2} \delta_i(\boldsymbol{y}) = 1 \end{cases} \tag{7}$$

Accordingly, we define the decision vector as $\boldsymbol{\delta}(\boldsymbol{y}) = [\delta_0(\boldsymbol{y}), \delta_1(\boldsymbol{y}), \delta_2(\boldsymbol{y})]$. Furthermore, we denote the true hypothesis and the decision of the detector by $T \in \{H_0, H_1, H_2\}$ and $D \in \{H_0, H_1.H_2\}$, respectively.

Based on these definitions, the probability of deciding in favor of hypothesis H_i while the true hypothesis is H_j, for $i \neq j$ is given by:

$$\begin{aligned} P_{ij}(\boldsymbol{\delta}(\boldsymbol{y})) =& \mathbb{P}(D = H_i \mid T = H_j) \\ =& \int_{\boldsymbol{y}} \int_{\boldsymbol{x}} \delta_i(\boldsymbol{y})\, f_j(\boldsymbol{y} \mid \boldsymbol{x})\, \pi_j(\boldsymbol{x})\, \mathrm{d}\boldsymbol{x}\, \mathrm{d}\boldsymbol{y} \\ =& \int_{\boldsymbol{y}} \delta_i(\boldsymbol{y})\, f_j(\boldsymbol{y})\, \mathrm{d}\boldsymbol{y} \end{aligned} \tag{8}$$

We have six such error probability terms. Next, by defining the estimation costs, we show how these detection error terms can be integrated with the estimation cost to form a combined approach for designing the estimators and detectors.

3.3 State estimation

Based on the observed data $\boldsymbol{y}$, besides discerning the underlying true model H_i, we also form an estimation for $\boldsymbol{x}$. We denote the estimation of $\boldsymbol{x}$ based on the collected data $\boldsymbol{y}$ by $\hat{\boldsymbol{x}_i}(\boldsymbol{y})$. To quantify the fidelity of the estimation under hypothesis H_i, we define the cost function $C_i(\boldsymbol{x}, \hat{\boldsymbol{x}_i}(\boldsymbol{y}))$, which captures the difference between the estimation and the ground truth. A popular cost function pertains to the minimum mean-square error (MMSE) criterion, which is given by:

$$C_i(\boldsymbol{x}, \boldsymbol{u}) = \|\boldsymbol{x} - \boldsymbol{u}\|^2 \tag{9}$$

For a given generic cost function $C_i(\boldsymbol{x}, \boldsymbol{u})$, we will also evaluate the average posterior cost function. Such an average cost function quantifies the estimation error cost after observing $\boldsymbol{y}$, and it is given by:

$$C_{i,p}(\boldsymbol{u} \mid \boldsymbol{y}) \triangleq \mathbb{E}_{i,\boldsymbol{x}}[C_i(\boldsymbol{x}, \boldsymbol{u}) \mid \boldsymbol{y}] \tag{10}$$

where the expectation is computed with respect to $\boldsymbol{x}_i$ under hypothesis $\boldsymbol{H}_i$. Therefore, the minimum average posterior cost function is given by:

$$C^*_{i,p}(\boldsymbol{y}) \triangleq \inf_{\boldsymbol{u}} C_{i,p}(\boldsymbol{u} \mid \boldsymbol{y}) \tag{11}$$

These cost functions have pivotal roles in designing the estimator and detector as they capture the quality of estimation. Finally, the optimizer of the average posterior cost is [22] denoted by:

$$\hat{\boldsymbol{x}}^*_i(\boldsymbol{y}) \triangleq \arg\inf_{\boldsymbol{u}} C_{i,p}(\boldsymbol{u} \mid \boldsymbol{y}) \tag{12}$$

3.4 Combined state recovery and bad data detection

In this subsection, we propose an approach that incorporates both estimation and detection decision rules in a unified framework. Given randomized detection rules $\boldsymbol{\delta}(\boldsymbol{y})$ and state estimators $\boldsymbol{u}_i(\boldsymbol{y})$, under hypothesis H_i, we define the conditional average estimation costs as:

$$J_i(\delta_i(\boldsymbol{y}), \boldsymbol{u}_i(\boldsymbol{y})) \triangleq \mathbb{E}_{i,\boldsymbol{x}}[C(\boldsymbol{x}, \boldsymbol{u}_i(\boldsymbol{y})) \mid D = H_i] \tag{13}$$

The expectation is taken with respect to $\boldsymbol{x}$ and $\boldsymbol{y}$ under H_i. Given the individual cost functions under different hypotheses, we aggregate the three cost functions into a unified one. Specifically, for a given measurement vector $\boldsymbol{y}$, randomized detection rules $\boldsymbol{\delta}(\boldsymbol{y})$, and estimators $\boldsymbol{u}(\boldsymbol{y}) = [U_0(\boldsymbol{y}), U_1(\boldsymbol{y}), U_2(\boldsymbol{y})]$, we define:

$$J(\boldsymbol{\delta}(\boldsymbol{y}), \boldsymbol{u}(\boldsymbol{y})) = \max_{i \in \{0,1,2\}} J_i(\delta_i(\boldsymbol{y}), \boldsymbol{u}_i(\boldsymbol{y})) \tag{14}$$

This aggregate cost function captures only the performance of the estimators. To integrate the quality of the detectors, which are captured by the probability terms $P_{ij}(\boldsymbol{\delta}(\boldsymbol{y}))$ defined in (8), we formulate the combined problem as the one that minimizes the estimation performance subject to controlled quality for the error probability terms $P_{ij}(\boldsymbol{\delta}(\boldsymbol{y}))$ according to:

$$\begin{cases} \mathcal{P}(\boldsymbol{\alpha}) \triangleq \inf\limits_{\boldsymbol{\delta}(\boldsymbol{y}), \boldsymbol{u}(\boldsymbol{y})} J(\boldsymbol{\delta}(\boldsymbol{y}), \boldsymbol{u}(\boldsymbol{y})) \\ \text{s.t.} \quad P_{ij}(\boldsymbol{\delta}(\boldsymbol{y})) \le \alpha_{ij} \quad i \neq j \end{cases} \tag{15}$$

Parameters $\boldsymbol{\alpha} = [\alpha_{ij}]$, where $\alpha_{ij} \in (0, 1)$ ensure that the probability of declaring H_i while the underlying true hypothesis is H_j are controlled in a desired level. In the next section, we discuss how the problem $\mathcal{P}(\boldsymbol{\alpha})$ can be solved in a closed form.

4 Optimal state estimator and decision rule

4.1 Feasibility of $\mathcal{P}(\boldsymbol{\alpha})$

Note that solving (15) does not always have a feasible solution for any arbitrary choice of $\{\alpha_{ij}\}$. Specifically, from the Neyman-Pearson (NP) theory, we know that when facing a multi-hypothesis testing problems, the probability of decision errors cannot be made arbitrarily small at the same time. The set of simultaneously feasible choices of $\{\alpha_{ij}\}$ can be found by solving the following problems, in which five of the error probabilities are controlled to remain below a specified threshold, and the sixth term is minimized. Without the loss of generality, we aim to minimize $P_{01}(\boldsymbol{\delta}(\boldsymbol{y}))$, while controlling the rest of error terms, i.e.:

$$\begin{cases} \beta \triangleq \min\limits_{\boldsymbol{\delta}(\boldsymbol{y})} P_{01}(\boldsymbol{\delta}(\boldsymbol{y})) \\ \text{s.t.} \quad P_{ij}(\boldsymbol{\delta}(\boldsymbol{y})) \le \alpha_{ij} \quad (i,j) \neq (0,1) \end{cases} \tag{16}$$

This problem can be solved readily by leveraging the same line of argument as in NP test [22]. Note that solving (16) is merely for the purpose of characterizing the

solution β and not the decision rule. Once this problem is solved, if β satisfies $\beta \leq \alpha_{01}$, then the combined estimation and detection problem in (15) is feasible, and vice versa.

4.2 Optimal state estimator

Close scrutiny of (15) indicates that the estimators appear only in the objective function of the optimization problems and the constraints depend only on the detectors. This observation suggests that the problem in (15) can be decomposed into two problems. Firstly, the estimators are characterized for any given set of detectors. Specifically, for any given choices of the detectors $\boldsymbol{\delta}(\boldsymbol{y})$, the optimal estimators can be found as the solution to:

$$\inf_{\boldsymbol{u}(\boldsymbol{y})} J(\boldsymbol{u}(\boldsymbol{y})) \tag{17}$$

This observation is summarized in the following theorem.

Theorem 1 (state estimator) The solution to the optimization problem

$$\bar{\boldsymbol{x}}^*(\boldsymbol{y}) \;=\; \arg \inf_{\boldsymbol{u}\boldsymbol{x}(\boldsymbol{y})} J(\boldsymbol{\delta}(\boldsymbol{y}), \boldsymbol{u}(\boldsymbol{y})) \tag{18}$$

is

$$\bar{\boldsymbol{x}}^*(\boldsymbol{y}) = [\hat{\boldsymbol{x}}_0^*(\boldsymbol{y}) \;,\; \hat{\boldsymbol{x}}_1^*(\boldsymbol{y}) \;,\; \hat{\boldsymbol{x}}_2^*(\boldsymbol{y})] \tag{19}$$

The proof can be found in Appendix A.

Irrespectively of the structure of the detection rules, the result of Theorem 1 is that the Bayesian estimators are optimal. This implies that the combined estimation and detection problems can be reduced to a bad data detection problem, which we will investigate in Subsection 4.3, followed by state estimators with the structures in (12).

4.3 Optimal bad data detectors

With the estimators designed in the previous subsection, these estimators can be substituted into the problem (15), rendering a purely detection problem. This detection problem can be found as the solution to:

$$\begin{cases} \mathcal{P}(\boldsymbol{\alpha}) = \inf\limits_{\boldsymbol{\delta}(\boldsymbol{y})} J(\boldsymbol{\delta}(\boldsymbol{y}), \bar{\boldsymbol{x}}^*(\boldsymbol{y})) \\ \text{s.t.} \quad P_{ij}(\boldsymbol{\delta}(\boldsymbol{y})) \leq \alpha_{ij} \quad i \neq j \end{cases} \tag{20}$$

For this purpose, we define:

$$\tilde{J}(\boldsymbol{\delta}(\boldsymbol{y})) = \inf_{\bar{\boldsymbol{x}}(\boldsymbol{y})} J(\boldsymbol{\delta}(\boldsymbol{y}), \bar{\boldsymbol{x}}(\boldsymbol{y})) = J(\boldsymbol{\delta}(\boldsymbol{y}), \bar{\boldsymbol{x}}^*(\boldsymbol{y})) \tag{21}$$

which transforms (20) as:

$$\begin{cases} \mathcal{P}(\boldsymbol{\alpha}) = \inf\limits_{\boldsymbol{\delta}(\boldsymbol{y})} \tilde{J}(\boldsymbol{\delta}(\boldsymbol{y})) \\ \text{s.t.} \quad P_{ij}(\boldsymbol{\delta}(\boldsymbol{y})) \leq \alpha_{ij} \quad i \neq j \end{cases} \tag{22}$$

By solving $\mathcal{P}(\boldsymbol{\alpha})$ in (22), we find the closed-form characterization for the detection rules, which essentially determine whether the system is suffering from bad data, and if so, whether it is structured bad data (attack) or random bad data. For this purpose, by recalling the definitions of J_i, J, and $\tilde{J}$ in (13), (14), and (21), respectively, we obtain:

$$\begin{aligned} \tilde{J}(\boldsymbol{\delta}(\boldsymbol{y})) &= J(\boldsymbol{\delta}(\boldsymbol{y}), \bar{\boldsymbol{x}}^*(\boldsymbol{y})) \\ &= \max_{i\in\{0,1,2\}} J_i(\boldsymbol{\delta}(\boldsymbol{y}), \hat{\boldsymbol{x}}_i^*(\boldsymbol{y})) \\ &= \max_{i\in\{0,1,2\}} \mathbb{E}_{i,\boldsymbol{x}}[C(\boldsymbol{x}, \hat{\boldsymbol{x}}_i^*(\boldsymbol{y})) \mid D = H_i] \\ &= \max_{i\in\{0,1,2\}} \mathbb{E}_{i,\boldsymbol{x}}[C_{i,\mathrm{p}}^*(\boldsymbol{y}) \mid D = \mathsf{H}_i] \\ &= \max_{i\in\{0,1,2\}} \frac{\int_{\boldsymbol{y}} \delta_i(\boldsymbol{y})\, f_i(\boldsymbol{y})\; C_{i,p}^*(\boldsymbol{y})\; \mathrm{d}\boldsymbol{y}}{\int_{\boldsymbol{y}} \delta_i(\boldsymbol{y})\, f_i(\boldsymbol{y})\; \mathrm{d}\boldsymbol{y}} \end{aligned} \tag{23}$$

We remark that each of the three terms involved in (23) is quasi-linear in $\delta_i(\boldsymbol{y})$, which are quasi-convex [23]. Furthermore, weighted maximum preserves quasi-convexity. Hence, the term $J(\boldsymbol{\delta}(\boldsymbol{y}))$ is quasi-convex and can be solved by finding the solutions to an equivalent family of feasibility problems [23–25]. More specifically, for solving $\mathcal{P}(\boldsymbol{\alpha})$, we first characterize a relevant feasibility problem. For characterizing and solving such a feasibility problem, based on (23), for any given $t \in \mathbb{R}_+$ that satisfies $\tilde{J}(\boldsymbol{\delta}(\boldsymbol{y})) \leq t$ for $i \in \{0, 1, 2\}$, we have:

$$\int_{\boldsymbol{y}} \delta_i(\boldsymbol{y})\, f_i(\boldsymbol{y})\; \left[C_{i,p}^*(\boldsymbol{y}) - t\right]\; \mathrm{d}\boldsymbol{y} \;\leq\; 0 \tag{24}$$

As a result, for any given set of values $\boldsymbol{\alpha}$, which controls bad data detection power and the real number t, we generate the following feasibility problem:

$$\begin{cases} \text{set all} \quad \boldsymbol{\delta}(\boldsymbol{y}) \quad \text{that satisfy} \\ \mathcal{Q}(\boldsymbol{\alpha}, t) \triangleq \int_{\boldsymbol{y}} \delta_i(\boldsymbol{y})\, f_i(\boldsymbol{y})\; \left[C_{i,p}^*(\boldsymbol{y}) - t\right]\; \mathrm{d}\boldsymbol{y} \leq 0 \\ P_{ij}(\boldsymbol{\delta}(\boldsymbol{y})) \leq \alpha_{ij} \quad i \neq j \end{cases} \tag{25}$$

The relationship specified in (24) indicates that the two problems $\mathcal{Q}(\boldsymbol{\alpha}, t)$ and $\mathcal{P}(\boldsymbol{\alpha})$ are related according to:

$$\begin{cases} \text{if} \quad \mathcal{Q}(\boldsymbol{\alpha}, t) \neq \phi \quad \text{then} \;\; \mathcal{P}(\boldsymbol{\alpha}) \leq t \\ \text{if} \quad \mathcal{Q}(\boldsymbol{\alpha}, t) = \phi \quad \text{then} \;\; \mathcal{P}(\boldsymbol{\alpha}) > t \end{cases} \tag{26}$$

Based on this property, it can be readily verified that the optimal value of $\mathcal{P}(\boldsymbol{\alpha})$ can be found through a bi-section search with the steps detailed in Algorithm 1.

Algorithm 1: Detection algorithm

Initialize $t_{\min} = 0$ and $t_{\max} = \mathbb{E}[C_i(\boldsymbol{x}, \boldsymbol{0}) \mid \boldsymbol{y}]$
Evaluate the average posterior costs in (10)
repeat
  $t_0 \leftarrow (t_{\min} + t_{\max})/2$
    Solve $\tilde{\mathcal{Q}}(\boldsymbol{\alpha}, t_0)$
 if $\tilde{\mathcal{Q}}(\boldsymbol{\alpha}, t_0) > 0$
    $t_{\min} \leftarrow t_0$
  else
    $t_{\max} \leftarrow t_0$
  end if
  until $t_{\max} - t_{\min} \leq \epsilon$ for ϵ sufficiently small
  $\mathcal{P}(\boldsymbol{\alpha}) \leftarrow t_{\max}$
  Output $\boldsymbol{a}$ and $\boldsymbol{c}$ to characterize the rules in (36)

Based on the connections between the two problems $\mathcal{Q}(\boldsymbol{\alpha}, t)$ and $\mathcal{P}(\boldsymbol{\alpha})$, we have observed that for solving $\mathcal{P}(\boldsymbol{\alpha})$, we can instead solve $\mathcal{Q}(\boldsymbol{\alpha}, t)$ combined with a bi-section search. In the next step, we specify how to optimally solve $\mathcal{Q}(\boldsymbol{\alpha}, t)$. In order to proceed, we introduce the slack variable γ and define the following auxiliary problem, which can be readily verified to be convex.

$$\begin{cases} \inf\limits_{\boldsymbol{\delta}(\boldsymbol{y})} \gamma \\ \text{s.t. } \tilde{\mathcal{Q}}(\boldsymbol{\alpha}, t) = \int_{\boldsymbol{y}} \delta_i(\boldsymbol{y}) f_i(\boldsymbol{y}) \left[C^*_{i,p}(\boldsymbol{y}) - t\right] \mathrm{d}\boldsymbol{y} \leq \gamma \\ P_{ij}(\boldsymbol{\delta}(\boldsymbol{y})) \leq \alpha_{ij} + \gamma \quad i \neq j \end{cases} \tag{27}$$

Based on the definitions of the problems $\mathcal{Q}(\boldsymbol{\alpha}, t)$ and $\tilde{\mathcal{Q}}(\boldsymbol{\alpha}, t)$, we have the following two statements, which are equivalent:

$$\mathcal{Q}(\boldsymbol{\delta}, t) = \emptyset \iff \tilde{\mathcal{Q}}(\boldsymbol{\delta}, t) > \boldsymbol{0} \tag{28}$$

This equivalent implies that for establishing the feasibility of $\mathcal{Q}(\boldsymbol{\delta}, t)$, we need to equivalently compare the value of $\tilde{\mathcal{Q}}(\boldsymbol{\delta}, t)$ with a fixed threshold. As the final step, we characterize the solution of $\tilde{\mathcal{Q}}(\boldsymbol{\delta}, t)$, which in turn provides a closed-form characterization of the decision rules $\boldsymbol{\delta}(\boldsymbol{y})$.

For solving $\tilde{\mathcal{Q}}(\boldsymbol{\delta}, t)$, which is a convex problem, we firstly form the Lagrangian by assigning the non-negative Lagrange multipliers a_i, $i \in \{0, 1, 2\}$ to the constraints:

$$\int_{\boldsymbol{y}} \delta_i(\boldsymbol{y}) f_i(\boldsymbol{y}) \left[C^*_{i,p}(\boldsymbol{y}) - t\right] \mathrm{d}\boldsymbol{y} \leq \gamma \tag{29}$$

and assigning the non-negative Lagrangian multipliers c_{ij}, for $i \neq j$ and $i, j \in \{0, 1, 2\}$, to constraints

$$P_{ij}(\boldsymbol{\delta}(\boldsymbol{y})) \leq \alpha_{ij} + \gamma \tag{30}$$

By defining $\boldsymbol{a} = [a_i]$ and $\boldsymbol{c} = [b_{ij}]$, which satisfy:

$$\sum_i a_i + \sum_{ij} b_{ij} = 1 \tag{31}$$

the Lagrangian is given by:

$$\begin{aligned} \boldsymbol{\mathcal{L}}(\boldsymbol{\delta}, \gamma, \boldsymbol{a}, \boldsymbol{c}) \triangleq & \left(1 - \sum_i a_i - \sum_{ij} b_{ij}\right)\gamma \\ & + \sum_i a_i \int_{\boldsymbol{y}} \delta_i f_i(\boldsymbol{y}) \left[C^*_{i,p}(\boldsymbol{y}) - t\right] \mathrm{d}\boldsymbol{y} \\ & + \sum_{ij} c_{ij}\Big(P_{ij}(\boldsymbol{\delta}(\boldsymbol{y})) - \alpha_{ij}\Big) \end{aligned} \tag{32}$$

As a result, the dual of the Lagrangian function is given by:

$$\begin{aligned} g(\boldsymbol{a}, \boldsymbol{c}) \triangleq & \min_{\boldsymbol{\delta}, \gamma} \mathcal{L}(\boldsymbol{\delta}, \gamma, \boldsymbol{a}, \boldsymbol{c}) \\ = & \min_{\boldsymbol{\delta}, \gamma} \Big\{ \sum_i a_i \int_{\boldsymbol{y}} \delta_i(\boldsymbol{y}) f_i(\boldsymbol{y}) \left[C^*_{i,p}(\boldsymbol{y}) - t\right] \mathrm{d}\boldsymbol{y} \\ & + \sum_{ij} c_{ij}\Big(P_{ij}(\boldsymbol{\delta}(\boldsymbol{y}))\Big)\Big\} \\ & - \sum_{ij} c_{ij}\alpha_{ij} \end{aligned} \tag{33}$$

By leveraging the expression of $P_{ij}(\boldsymbol{\delta})$ in (8), the Lagrangian dual can be equivalently state as:

$$g(\boldsymbol{a}, \boldsymbol{c}) = \min_{\boldsymbol{\delta}, \gamma} \sum_i \int \delta_i(\boldsymbol{y}) A_i(\boldsymbol{y}) \mathrm{d}\boldsymbol{y} - \sum_{ij} c_{ij}\alpha_{ij} \tag{34}$$

in which we have defined:

$$A_i(\boldsymbol{y}) \triangleq a_i f_i(\boldsymbol{y}) \left[C^*_{i,p}(\boldsymbol{y}) - t\right] + \sum_{j \neq i} c_{ij} f_j(\boldsymbol{y}) \tag{35}$$

Based on these observations and properties, the optimal detection rules are formalized in the next theorem.

Theorem 2 The problem $\mathcal{P}(\boldsymbol{\alpha})$ has a globally optimal solution and the decision rule $\boldsymbol{\delta}(\boldsymbol{y})$ that optimizes $\mathcal{P}(\boldsymbol{\alpha})$ (and $g(\boldsymbol{a}, \boldsymbol{c})$) is given by:

$$\begin{cases} \delta_0(\boldsymbol{y}) = 1 & \text{if } A_0(\boldsymbol{y}) \geq \max\{A_1(\boldsymbol{y}), A_2(\boldsymbol{y})\} \\ \delta_1(\boldsymbol{y}) = 1 & \text{if } A_1(\boldsymbol{y}) \geq \max\{A_0(\boldsymbol{y}), A_2(\boldsymbol{y})\} \\ \delta_2(\boldsymbol{y}) = 1 & \text{if } A_2(\boldsymbol{y}) \geq \max\{A_0(\boldsymbol{y}), A_1(\boldsymbol{y})\} \end{cases} \tag{36}$$

As a result, based on Theorem 2, we start by computing the Lagrange multipliers $\boldsymbol{a}$ and $\boldsymbol{c}$, in order to compute the constants $A_i(\boldsymbol{y})$. These constants determine the system operates under which model.

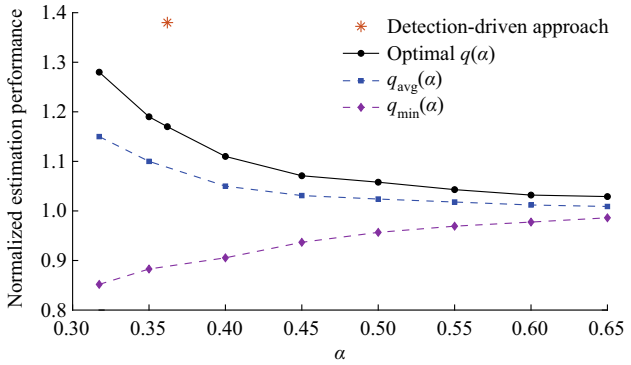

Fig. 1 Normalized estimation performance versus α

5 Case study

In this section, we evaluate the performance of the optimal framework on the IEEE 14-bus system, in which the measurement units undergo potential false data injection attacks. We evaluate both a DC linearized system and the AC non-linear system models. In this model, any combination of the 14 measurement units on the buses can be compromised.

The benchmark method to compare against the approach developed in this paper is the detection-driven approach. In this approach, the effect of the state parameters are ignored, and a purely detection problem is considered to determine whether the measurements are entirely legitimate, or they bear random or structured bad data. This is carried out by performing a simple hypothesis testing over the three possible hypotheses $\{H_0, H_1, H_2\}$ defined in (6). Once a decision is formed, based on that an estimator is designed to form reliable state estimations.

We compare the average estimation cost for a detection-driven approach, where the correct decision about $\{H_0, H_1, H_2\}$ is followed by Bayesian estimation. The degradation in the estimation cost normalized by the estimation cost under an attack-free setting is depicted in Fig. 1, which shows how the estimation quality suffers from the existence of the random and structured bad data. The plots in this figure illustrate the variations of this estimation quality versus $\alpha \triangleq \alpha_{ij}$, which control the detection error rates, as specified in (15).

Figure 1 consists of three curves, one representing the estimation cost averaged over all the costs under different hypothesis q, the best estimate among different estimations under different models $q_{\max}$, and the worst estimate among different estimations under different models $q_{\min}$. Besides, we also depict the performance of the detection-driven approach, which appears as one isolated point. The detection-driven approach is forced to take a specific detection quality. It does not enjoy the flexibility of the optimal approach that can place any desired emphasis on the estimation detection and bad data/attack detection problems. Furthermore, the detection-driven approach produces considerable weaker estimations.

6 Conclusion

In this paper, we have investigated the non-linear state estimation in power system when the system is vulnerable to structured or random bad data. Forming estimations in such scenarios is inherently coupled with detecting the true model of the system. We have shown that all the existing approaches are sub-optimal, which essentially decouple the involved estimation and detection routines. Based on that premise, we have provided a general framework that treats the state estimation and bad data detection problem in a unified way. We have characterized the optimal state estimators and bad data detectors in closed forms.

Acknowledgements This work was provided by the US national Science Foundation (No. ECCS-1554482).

Appendix A

From(13), we have:

$$J_i(\delta_i(\boldsymbol{y}), \boldsymbol{u}_i(\boldsymbol{y})) = \mathbb{E}[C(\boldsymbol{x}, \boldsymbol{u}_i(\boldsymbol{y}))\,|\,D=H_i] = \frac{\int_{\boldsymbol{y}} \int_{\boldsymbol{x}} \delta_i(\boldsymbol{y}) C(\boldsymbol{x}, \boldsymbol{u}_i(\boldsymbol{y})) f_i(\boldsymbol{y} \mid \boldsymbol{x}) \pi(\boldsymbol{x}) \mathrm{d}\boldsymbol{x}\mathrm{d}\boldsymbol{y}}{\int_{\boldsymbol{y}} \delta_i(\boldsymbol{y}) f_i(\boldsymbol{y}) \mathrm{d}\boldsymbol{y}} \tag{A1}$$

Using the definition of $C_{i,p}(\boldsymbol{u}_i(\boldsymbol{y}) \mid \boldsymbol{y})$ from (11), a lower bound on $J_i(\delta_i, \boldsymbol{u}_i(\boldsymbol{y}))$ is given by:

$$J_i(\delta_i(\boldsymbol{y}), \boldsymbol{u}_i(\boldsymbol{y})) = \frac{\int_{\boldsymbol{y}} \delta_i(\boldsymbol{y}) C_{i,p}(\boldsymbol{u}_i(\boldsymbol{y}) \mid \boldsymbol{y}) f_i(\boldsymbol{y}) \mathrm{d}\boldsymbol{y}}{\int_{\boldsymbol{y}} \delta_i(\boldsymbol{y}) f_i(\boldsymbol{y}) \mathrm{d}\boldsymbol{y}} \geq \frac{\int_{\boldsymbol{y}} \delta_i(\boldsymbol{y}) \inf_{\boldsymbol{u}_i(\boldsymbol{y})} C_{i,p}(\boldsymbol{u}_i(\boldsymbol{y}) \mid \boldsymbol{y}) f_i(\boldsymbol{y}) \mathrm{d}\boldsymbol{y}}{\int_{\boldsymbol{y}} \delta_i(\boldsymbol{y}) f_i(\boldsymbol{y}) \mathrm{d}\boldsymbol{y}} \tag{A2}$$

which implies that:

$$J_i(\delta_i(\boldsymbol{y}),\boldsymbol{u}_i(\boldsymbol{y})) \geq \frac{\int_{\boldsymbol{y}} \delta_i(\boldsymbol{y}) C^*_{i,p}(\boldsymbol{y}) f_i(\boldsymbol{y}) \mathrm{d}\boldsymbol{y}}{\int_{\boldsymbol{y}} \delta_i(\boldsymbol{y}) f_i(\boldsymbol{y}) \mathrm{d}\boldsymbol{y}} \tag{A3}$$

Based on the definition of $\hat{\boldsymbol{x}}^*_i(\boldsymbol{y})$ provided in (12), this lower bound is clearly achieved when the estimator $\boldsymbol{u}_i(\boldsymbol{y})$ is chosen to be:

$$\hat{\boldsymbol{x}}^*_i(\boldsymbol{y}) = \arg \inf_{\boldsymbol{u}_i(\boldsymbol{y})} C_{i,p}(\boldsymbol{u}_i(\boldsymbol{y}) \mid \boldsymbol{y}) \tag{A4}$$

which proves that the estimator characterized in (12) is an optimal estimator that minimizes the cost $J_i(\delta_i, \boldsymbol{u}_i)$. The corresponding minimum average estimation cost is:

$$J_i(\delta_i(\boldsymbol{y}),\hat{\boldsymbol{x}}^*_i(\boldsymbol{y})) = \frac{\int_{\boldsymbol{y}} \delta_i(\boldsymbol{y}) C^*_{i,p}(\boldsymbol{y}) f_i(\boldsymbol{y}) \mathrm{d}\boldsymbol{y}}{\int_{\boldsymbol{y}} \delta_i(\boldsymbol{y}) f_i(\boldsymbol{y}) \mathrm{d}\boldsymbol{y}} \tag{A5}$$

Next, we prove that:

$$\begin{aligned} &\max_i \min_{\boldsymbol{u}} \{J_i(\delta_i(\boldsymbol{y}),\boldsymbol{u}_i(\boldsymbol{y}))\} \\ &\quad \equiv \min_{\boldsymbol{u}} \max_i \{J_i(\delta_i(\boldsymbol{y}),\boldsymbol{u}_i(\boldsymbol{y}))\} \end{aligned} \tag{A6}$$

Recall from (14), the overall estimation cost $J(\boldsymbol{\delta},\boldsymbol{u})$ is defined as:

$$J(\boldsymbol{\delta}(\boldsymbol{y}),\boldsymbol{u}(\boldsymbol{y})) = \max_i \{J_i(\delta_i(\boldsymbol{y}),\boldsymbol{u}_i(\boldsymbol{y}))\} \tag{A7}$$

Define $S(\boldsymbol{s},\boldsymbol{\delta},\boldsymbol{u})$ as a convex function of $J_i(\delta_i(\boldsymbol{y}),\boldsymbol{u}_i(\boldsymbol{y}))$, $i \in \{0,1,\ldots,T\}$, and it is given by:

$$S(\boldsymbol{x},\boldsymbol{\delta},\boldsymbol{u}) \triangleq \sum_{i=0}^{T} s_i J_i(\delta_i,\boldsymbol{u}_i) \tag{A8}$$

where $\boldsymbol{s} = [s_0, s_1, \ldots, s_T]$, and they satisfy:

$$\begin{cases} \sum_{i=0}^{T} s_i = 1 \\ s_i \in [0,1] \end{cases} \tag{A9}$$

We can represent $J(\boldsymbol{\delta},\boldsymbol{u})$ as a function of $S(\boldsymbol{x},\boldsymbol{\delta},\boldsymbol{u})$ in the following form:

$$J(\boldsymbol{\delta},\boldsymbol{u}) = \max_{\boldsymbol{x}} S(\boldsymbol{x},\boldsymbol{\delta},\boldsymbol{u}) \tag{A10}$$

Let $s^* = \{\Omega^*_j : j = 0,1,\ldots,T\}$ be defined as:

$$s^* \triangleq \arg\max_{\boldsymbol{x}} S(\boldsymbol{x},\boldsymbol{\delta},\boldsymbol{u}) \tag{A11}$$

where $s^* = 1$ if:

$$j = \arg\max_i \{J_i(\delta_i,\boldsymbol{u}_i)\} \tag{A12}$$

From (A4) and (A5), we observe that:

$$\begin{aligned} \max_{\boldsymbol{x}} \min_{\boldsymbol{u}} S(\boldsymbol{x},\boldsymbol{\delta},\boldsymbol{u}) &= \max_{\boldsymbol{x}} S(\boldsymbol{x},\boldsymbol{\delta},\hat{\boldsymbol{x}}) \\ &\geq \min_{\boldsymbol{u}} \max_{\boldsymbol{x}} S(\boldsymbol{x},\boldsymbol{\delta},\boldsymbol{u}) \end{aligned} \tag{A13}$$

At the same time, we have:

$$\max_{\boldsymbol{x}} S(\boldsymbol{x},\boldsymbol{\delta},\boldsymbol{u}) \geq \max_{\boldsymbol{x}} \min_{\boldsymbol{u}} S(\boldsymbol{x},\boldsymbol{\delta},\boldsymbol{u}) \tag{A14}$$

which implies that:

$$\min_{\boldsymbol{u}} \max_{\boldsymbol{x}} S(\boldsymbol{x},\boldsymbol{\delta},\boldsymbol{u}) \geq \max_{\boldsymbol{x}} \min_{\boldsymbol{u}} S(\boldsymbol{x},\boldsymbol{\delta},\boldsymbol{u}) \tag{A15}$$

From (A13) and (A15), it is easily concluded that:

$$\max_{\boldsymbol{x}} \min_{\boldsymbol{u}} S(\boldsymbol{x},\boldsymbol{\delta},\boldsymbol{u}) = \min_{\boldsymbol{u}} \max_{\boldsymbol{x}} S(\boldsymbol{x},\boldsymbol{\delta},\boldsymbol{u}) \tag{A16}$$

which completes the proof for (A6).

References

[1] Scheweppe FC, Wildes J, Bose A (1970) Power system static state estimation, parts I, II and III. IEEE Trans Power Appar Syst 89(1):120–135

[2] Wu FF, Moslehi K, Bose A (2005) Power system control centers: past, present, and future. Proc IEEE 93(11):1890–1908

[3] Monticelli F (2000) Electric power system state estimation. Proc IEEE 88(2):262–282

[4] Abur A, Gómez-Expósito A (2004) Power system state estimation: theory and implementation. Marcel Dekker, New York

[5] Liu Y, Ning P, Reiter MK (2009) False data injection attacks against state estimation in electric power grids. In: Proceedings of the 16th ACM conference on computer and communications security, Chicago, USA, 9–13 November 2009, 12 pp

[6] Cui S, Han Z, Kar S et al (2012) Coordinated data-injection attack and detection in the smart grid: a detailed look at enriching detection solutions. IEEE Sig Proc Mag 29(5):106–115

[7] Kim TT, Poor HV (2011) Strategic protection against data injection attacks on power grids. IEEE Trans Smart Grid 2(2):326–333

[8] Negrete-Pincetic M, Yoshida F, Gross G (2009) Towards quantifying the impacts of cyber attacks in the competitive electricity market environment. In: Proceedings of IEEE PowerTech conference, Bucharest, Romania, 28 June–2 July 2009, 8 pp

[9] Jia L, Thomas R, Tong L (2011) Malicious data attack on real-time electricity market. In: Proceedings of IEEE international conference on acoustics, speech and signal processing, Prague, Czech Republic, 22–27 May 2011, pp 5952–5955

[10] Lei X, Yu D, Bai X (2010) Research on multistep electricity price model with bidirectional regulation for large consumers. In: Proceedings of international conference on electrical and control engineering, Wuhan, China, 25–27 June 2010, pp 4114–4117

[11] Lin J, Yu W, Yang X (2013) On false data injection attack against multistep electricity price in electricity market in smart grid. In: Proceedings of IEEE global communications conference, Atlanta, USA, 9–13 December 2013, pp 760–765

[12] Choi DH, Xie L (2013) Ramp-induced data attacks on look-ahead dispatch in real-time power markets. IEEE Trans Smart Grid 4(3):1235–1243

[13] Jia L, Thomas R, Tong L (2012) Impacts of malicious data on real-time price of electricity market operations. In: Proceedings of Hawaii international conference on system science, Maui, USA, 4–7 January 2012, pp 1907–1914
[14] Esmalifalak M, Shi G, Han Z et al (2013) Bad data injection attack and defense in electricity market using game theory study. IEEE Trans Smart Grid 4(1):160–169
[15] Ma J, Liu Y, Song L et al (2015) Multiact dynamic game strategy for jamming attack in electricity market. IEEE Trans Smart Grid 6(5):2273–2282
[16] Li H, Han Z (2011) Manipulating the electricity power market via jamming the price signaling in smart grid. In: Proceedings of IEEE global communications conference, Houston, USA, 5–9 December 2011, pp 1168–1172
[17] Jia L, Thomas R, Tong L (2012) On the nonlinearity effects on malicious data attack on power system. In: Proceedings of IEEE PES general meeting, San Diego, USA, 22–26 July 2012, pp 1–8
[18] Mengis MR, Tajer A (2018) Data injection attacks on electricity markets by limited adversaries: worst-case robustness. IEEE Trans Smart Grid 9(6):5710–5720
[19] Tajer A (2019) False data injection attacks on electricity markets by limited adversaries: stochastic robustness. IEEE Trans Smart Grid 10(1):128–138
[20] Xue M, Tajer A (2016) Worst-case robust attacks by limited adversaries against electricity markets. In: Proceedings of annual asilomar conference on signals, systems, and computers, Pacific Grove, USA
[21] Tajer A, Kar S, Poor HV et al (2011) Distributed joint cyber attack detection and state recovery in smart grids. In: Proceedings of IEEE smart grid communications, Brussels, Belgium, 17–20 October 2011, pp 202–207
[22] Poor HV (1998) An introduction to signal detection and estimation, 2nd edn. Springer, Berlin
[23] Boyd S, Vandenberghe L (2004) Convex optimization. Cambridge University Press, Cambridge
[24] Dinkelabach W (1967) On nonlinear fractional programming. Manag Sci 13(7):492–498
[25] Schaible S (1976) Fractional programming. II, on Dinkelbach's algorithm. Manage 22(8):868–873

Ali TAJER is an Associate Professor of Electrical, Computer, and Systems Engineering at Rensselaer Polytechnic Institute, USA. During 2007-2010 he was with Columbia University where he received the M.A degree in Statistics and Ph.D. degree in Electrical Engineering, and during 2010-2012 he was with Princeton University as a Postdoctoral Research Associate. His research interests include mathematical statistics and network information theory, with applications in data analytics and power grids. Dr. Tajer Serves as an Editor for the IEEE Transactions on Communications, an Editor for the IEEE Transactions on Smart Grid. In the past he has also served as the Guest Editor-in-Chief for the IEEE Transactions on Smart Grid, as a Guest Editor for the IEEE Signal Processing Magazine, and as an Associate Editor for the IEE Transactions on Smart Grid. He is a senior member of the IEEE and received a United States NSF CAREER award in 2016.

Saurabh SIHAG received the B.Tech and M.Tech degrees in electrical engineering from the Indian Institute of Technology Kharagpur, India, in 2016. Since Fall 2016, he has been working towards the Ph.D. degree at the Department of Electrical, Computers, and Systems Engineering, Rensselaer Polytechnic Institute, Troy, USA. His research interests include statistical signal processing, information theory, and high-dimensional statistics.

Khawla ALNAJJAR received the Ph.D. degree in electrical and electronics engineering from the University of Canterbury, New Zealand, in 2015. She is currently an Assistant Professor with the Department of Electrical and Computer Engineering, University of Sharjah, United Arab Emirates. Her research interests include wireless communication systems, mathematical statistics and network information theory and power grids.