Topology Perturbation for Detecting Malicious Data Injection

Kate L. Morrow, Erich Heine, Katherine M. Rogers, Rakesh B. Bobba, Thomas J. Overbye

University of Illinois at Urbana-Champaign
Urbana, IL, USA
Email:{morrow4, eheine, krogers6, rbobba, overbye}@illinois.edu

Abstract

Bad measurement data exists in power systems for a number of reasons. Malicious data injection attacks, which alter the values of measurements without being detected, are one potential cause of bad data and may have serious consequences. A solution for bad data detection in power systems is proposed in this work, particularly designed to detect malicious data attacks. By applying known perturbations to the system and measuring the changes elsewhere, the approach 'probes' the system for unexpected responses in terms of measurement values. Using a developed 'keyspace' approach, the perturbation used is rendered unpredictable to the attacker, making it difficult for the attacker to adapt his attacks. Thus, unexpected measurement values after a probe provide an indication of both bad and malicious data. The proposed approach is analyzed for sample systems using MATLAB.

I. Introduction

Operators of distributed critical infrastructures such as the power grid rely on measurements from remote sensors in the field to monitor and control their systems. Typically, an industrial control system known as a Supervisory Control and Data Acquisition (SCADA) system is used to collect measurements from sensors in the network. The measurements, often taken every 2 to 4 seconds, are then used to estimate the state of the system and to guide the control operations.

Given the criticality of the power grid, it is an attractive attack target. Adversaries may attempt to manipulate sensor measurements, insert fake control commands, delay measurements and/or control commands, and resort to other malicious actions. It is crucial to protect these systems against such malicious activity to ensure safe and reliable operation of the power grid. Applications like state estimation in the power grid are accompanied by bad data detection systems that can detect, identify, and correct measurement data that is inconsistent with the rest of the data given by the current system topology [19], [10], [9], [15], [24], [22], [36], [8], [25], [39], [32], [2], [40], [3], [5]. However, none of the traditional bad data detection schemes are designed with maliciously injected bad data in mind, but rather are meant to detect bad data due to faulty sensors, communication errors, and other failures.

In this work, we propose a 'probing' approach for detecting false data injection attacks. Specifically, our approach relies on perturbing the power system by changing the impedance on a set of chosen lines. We acheive this by leveraging D-FACTS devices in order to create observable changes in the system, which an adversary is unable to anticipate. We investigate the level of perturbation needed to thwart attacks and study the deviation from optimal caused by perturbation.

It is important to highlight that there is nothing which limits our approach to D-FACTS devices in particular. The proposed approach may be analogously examined and developed for reactive power injection or other input perturbation schemes. In fact, it may be the case that other means of perturbation are simpler or less costly to implement. However, such a comparison is beyond the scope of the current paper.

The rest of this paper is organized as follows. In Section II, we provide a brief background on D-FACTS devices and perturbation. We motivate and present our general approach in Section III, then discuss practical considerations and challenges in Section IV. We present our tools and experimental setup in Section V and analysis of our results in Section VI. Finally, we conclude and present future work in Sections VII and VIII.

II. Background

The motivation for this work comes from a need to design a bad data detector that is application-independent and robust against attacks. Bad data detection solutions in the literature are often overly specific to a particular application. Power system state estimation in particular falls into this category. Background on power system state estimation and bad data detection is found in the power systems literature, including [31], [21], and [37]. Topology error detection for state estimation is considered in [38], [1], [18]. The value of measurement placement for bad data detection is recognized in [6].

A. Bad Data Detection - Related Work

Until recently, it was generally assumed the bad data detection systems accompanying state estimators are sufficient to detect and recover from deliberate sensor measurement manipulation. The failure of typical bad data detection methods for malicious attacks can be suspected from the analysis in [23], but the issue has been largely brought to the attention of the power system cyber security community more recently by [17].

The work by Liu *et al.* [17], [16] demonstrated that an adversary, armed with the knowledge of system topology, can inject false data into state estimators that use linearized power flow models (also known as DC state estimation) without being detected. The work by Teixeira *et al.* [33] shows that it is possible to launch false data injection attacks with partial knowledge of the system topology, on both linear and non-linear state estimation. Such undetected false data injection was possible because the current bad data detection techniques were designed to deal with faults and errors, including correlated ones, but not with coordinated malicious changes. These works highlight the need to develop defense strategies to protect power system applications from manipulated data.

Recent work has proposed solutions to address the problem of false data injection [4], [7], [13], [14]. Generally speaking, the approaches can be classified into two categories: cyber-based or physical system property-based approaches. Approaches in the first category typically involve deploying cryptographic mechanisms on the communications between the sensors in the field and the control center, or deploying tamper-resistant or tamper-evident sensor hardware. Approaches in the second category involve revisiting bad data detection schemes with adversary-induced bad data in mind, rather than generic errors and faults. However, not all approaches fall squarely into just one category; approaches need not be mutually exclusive but can complement each other.

An approach to detecting bad data injection attacks is proposed in [4], [7], which leverages the underlying physical system properties to decide which sensor measurements to protect against manipulation in order to detect false data injection attacks on DC state estimation using traditional bad data detection. This work is agnostic about the protection mechanism itself. In [13], the approach proposes leveraging historical knowledge about the measurements along with physical system properties to detect false data injection attacks.

B. Perturbation - 'kicking the system'

The proposed approach takes advantage of power system interconnectedness. That is, when a power system is perturbed in certain ways, the effect of that perturbation on measurable quantities elsewhere in the system can be readily calculated. Hence, by injecting known perturbations into the system, we can effectively 'probe' the system. Since we (or generically, the defenders of the power grid) perform the probing, we know the injected probing signal. Then, based on knowledge of the power system model, we know the changes we expect to see as a result. Thus, we develop a probing technique for power systems to identify data which does not respond as expected.

The manner in which the system is probed is unknown to everyone except us, so it is secret, like a private key. From the perspective of providing system defense, even if an attacker is highly knowledgeable about the system, he or she does not know the 'probing sequence' that will be injected. Thus, the premise is that a malicious intruder cannot calculate and produce the correct response for the measurements or meters under his or her control. If the attacker knows the underlying power system model, he or she could hypothetically change the injected data according to the model. However, even when the attacker has such a high level of knowledge about the system, the attack will be detected with this probing technique since the probing signal is unknown to the attacker.

Using probing for the purposes of cyber security for control systems is investigated by [20]. This work perturbs the system to detect replay attacks on a simulated chemical plant control system. It focused on a discrete time, linear time-invariant control system with Linear Quadratic Gaussian (LQG) controller, perturbed by adding an i.i.d. Guassian distributed control signal with zero mean and a specific co-variance.

Probing is also useful for peforming system diagnos-

tics in power systems. In fact, power system probing is not a new concept and is often used in the western interconnect of the US (WECC) [12], [41]. The probing tests used in WECC and their results are reported in several NASPI documents [34], [35]. A study of probing signal designs used in the WECC tests is found in [26]. The most common probing signals for power systems, from [11], are a rectangular pulse or square wave, brief periodic waveforms, sustained sinusoid signals, and sustained noise signals. For example, in [11], square waves are used to probe specific oscillatory modes.

C. Perturbations with D-FACTS Devices

Sensitivities are commonly used in power systems to examine the linearized effect a change in one variable causes on a value elsewhere in the system. Sensitivities in power systems can be considered in matrix form, where the dimensions are determined by the number of independently changed variables and the number of dependent values. In this work the independent control variable is line impedance, so we need to study sensitivities such as real power line flows (or other types of measurements) to line impedance. A potential alternative approach could utilize sensitivity of voltages to reactive power output, or any other pair of variables where we can perturb the control value and observe the changes in measurements. In this work, the perturbations we examine are from Distributed Flexible AC Transmission System (D-FACTS) devices. These are devices which hang on transmission lines and are capable of performing active impedance injection.

Our determination of D-FACTS settings and placement is primarily based on sensitivity analysis. The relevant sensitivities are calculated by taking the derivative of measurement equations with respect to line impedance. Hence, the work in this paper builds upon the sensitivity analysis of D-FACTS devices, but for a different purpose. Changing a D-FACTS setting effectively changes the reactive impedance of a line, within some range. Assume that the desired output measurement variables are the real power flows. The equation for real power flow on a line is:

$$\mathbf{P}_{ij} = \mathbf{V}_i^2[\mathbf{G}_{ii}] + \mathbf{V}_i\mathbf{V}_j[\mathbf{G}_{ij}cos(\theta_{ij}) + \mathbf{B}_{ij}sin(\theta_{ij})], \tag{1}$$

where $\mathbf{G}_{ij}$ and $\mathbf{B}_{ij}$ denote the elements in position i,j of the real and imaginary components of the system admittance matrix, respectively:

$$\mathbf{Y_{bus}} = \mathbf{G} + j\mathbf{B}. \tag{2}$$

Matrix $\mathbf{Y_{bus}}$ therefore contains the network line parameters due to:

$$\mathbf{I} = \mathbf{Y_{bus}}\mathbf{V}. \tag{3}$$

The shunt elements at bus i for line i,j comprise $\mathbf{G}_{ii}$. The state variables are voltage magnitude $\mathbf{V}$ and θ, where θ_{ij} is the angle difference between buses i and j.

In order to be able to effect deliberate perturbations of measured power flows with D-FACTS, analysis is needed of the impact on line flows that will result following a change in D-FACTS setting. These and other sensitivities related to D-FACTS devices are thoroughly explained in [28]. When evaluating the effect of changing line impedance on line flows, the partial derivative of (1) must be taken with respect to two sets of variables, line impedance $\mathbf{x}$ and the state variables $\mathbf{s}_{\theta,\mathbf{V}}$. These are the direct and the indirect sensitivities, respectively. A chain rule of calculated matrices represents the full relationship between line flows and line impedances. Details of calculation for these matrices, as well as a general strategy for using D-FACTS devices to provide control in power systems, is found in [28]. Results for power systems applications of real power loss minimization, voltage control, and real power flow control are also reported in [29] and [30].

III. Approach

Our approach assumes initial D-FACTS settings that are optimal with respect to minimizing power losses. It may be possible to extend our approach to initial settings such that some other desirable objective function is met, however such a study is outside the scope of the present work. We then perturb the system slightly from this optimal state and observe the effect of the perturbation through its impact on measurements. The injected perturbation has some predicable impact on all of the measurements, and as long as we know what the perturbation is, we know what observed measurement changes to expect. Therefore, if the measurements do not change in the way we expect, there may be cause for alarm and further investigation.

In this model, we assume that the adversary is modifying measurement values from the devices in the field. This may be via data channel compromise, device compromise, or some limited compromise of the control center itself—the control channel (up-to and including the D-FACTS devices themselves) must remain safe for this scheme to work. Furthermore, the adversary is assumed to have limited resources and

computational capabilities, and is therefore incapable of calculating the effects of an observed probe and updating the compromised measurement data stream in real-time.

Specifically, we perturb the system by changing the D-FACTS settings to a pre-determined value. A requirement of this value is to minimally affect the power flow and stability of the overall system, while still producing measurement changes that are observable and distinguishable from system noise. The vector of new settings for each D-FACTS device is termed a 'key'. This key is chosen randomly from a set of acceptable keys. Random selection of the key prevents the adversary from simply matching his data injection to the next state in a sequence, and provides security. Keys, keyspaces, and key choice are explored further in Section IV.

The sensitivity matrix $\mathbf{A}$ describes how measurement variables such as line flows (or other chosen measurements) are expected to change in response to a change in impedance. Each key, $\mathbf{k}_i$, is a vector of impedance settings for D-FACTS-equipped lines, where $\mathbf{k}_0$ denotes the optimal operating point. These along with the current set of D-FACTS settings, $\mathbf{x}$, provide the predicted set of measured values. The perturbation applied to the system, $\Delta\mathbf{x}$, is given by:

$$\Delta\mathbf{x} = \mathbf{k}_i - \mathbf{x}. \tag{4}$$

For a chosen set of measurements, the predicted perturbed measurements $\mathbf{m}_{pred}$ are then:

$$\mathbf{m}_{pred} = \mathbf{A}\Delta\mathbf{x} + \mathbf{m}_0 \tag{5}$$

where $\mathbf{m}_0$ are the measured line flows prior to the perturbation. Let the measurements observed during the perturbation be $\mathbf{m}_{obs}$. Bad data can be detected by examining $\mathbf{m}_{obs} - \mathbf{m}_{pred}$, noting any values outside an acceptable error range. These flagged values provide a starting point for further investigation of compromise. Additional validation of the measurements can be provided by examining the inverse calculation (assuming $\mathbf{A}$ is invertible):

$$\mathbf{A^{-1}}(\mathbf{m}_{obs} - \mathbf{m}_0) = \Delta\mathbf{x}_{inv} \tag{6}$$

and comparing $\Delta\mathbf{x}_{inv}$ to $\Delta\mathbf{x}$. An important attribute of our approach is that $\mathbf{m}_0$ need not be a trustworthy set of observations. Detection is done through the comparison of expected changes to actual changes and the concealed nature of the perturbation, not from the inherent trustworthiness of any given observation. Effectively, the approach separates detection from trust determination, which can begin after an observation has been deemed suspect.

IV. Keys, Keyspaces, and other Challenges

The effectiveness of the usage of a perturbation sequence depends primarily on the inability of an adversary to correctly guess the perturbation in effect and to accordingly manipulate the effect of the probe on the measurements. To quantize this inability to guess the perturbation, and to ensure it is within acceptable bounds, we define a "keyspace" to be a bubble of acceptable operating points around the optimum (as achieved by the use of D-FACTS devices). A "key" is one such operating point: a vector of the impedance values on the lines with D-FACTS devices. This keyspace must then be populous enough to meet the desired level of protection against accurate guessing.

The "size" (number of keys in the set) of a keyspace depends on two categories of factors. Firstly, the 'resolution' of the space is constrained by the physical restrictions of the system, such as the control precision of D-FACTS devices or the measurement precision of the sensors used as observation points. Secondly, the bounds of the keyspace are determined by chosen parameters, such as the limits on the percentage of line impedance the D-FACTS devices can change, and the acceptable level of power loss. The volume of this space must be at least large enough to prevent the adversary from having a reasonable chance of accurately guessing the key in use. There may also be additional requirements on the size of the keyspace, as we later discuss in Section VI-A.

In addition to pre-defining the set of keys in the keyspace, there is the consideration of how to use the keys. One option is "continuous polling" by using a key at a regular time interval. Alternatively the use of this tool could be reserved for certain times when there is suspicion of bad data coming from somewhere in the system. In either case, it is necessary to maintain operation under one key long enough to reach a quasi-steady state and then observe all desired system measurements. One important point to note, in the case of using multiple keys in sequence when bad data is suspected, is that we propose moving back to the optimal key $\mathbf{k}_0$ between successive pairs of keys, instead of moving directly from $\mathbf{k}_a$ to $\mathbf{k}_b$. This is for purposes of mitigating instability risks—an important consideration which places further requirements on the size of the available keyspace.

Given the current state of the system (as well as potentially the history of keys used so far in the current probe), there will be a dynamic subset of the predetermined keyspace that is feasible for use. Possible constraints include the need to avoid creating undesirable resonance or transients, and generally to keep the

power system in a reliable operating condition. The volume of currently usable keys must still be large enough to avoid accurate guessing by an adversary. There is also work to be done on considering what key (or subset of keys) will best "target" a certain node for investigation. Such calculations will result in subspaces of the pre-determined keyspace, which must in turn each be of sufficient volume as well.

One important point about terminology: in this section, where we have said "current state," it is understood that this is merely the "currently measured state." By the very nature of the problem our work is trying to address, it is highly likely that the measured current state is not equal to the actual physical state. This complicates the decision of which key to use at a given time. If we cannot trust our data, then cannot know if a key vetted to be "safe" for the current measured state is safe for the underlying, actual physical state. One approach is to pick an initial probe which is inherently "safe" for a wide variety of operating conditions. The idea is to facilitate a "failsafe" initial probe of the system such that, at worst, its use results only in a minimal violation of desirable power system operation constraints. Other specific solutions for this conflict are to be investigated.

V. Implementation and Experiments

In order to analyze the validity of the method proposed in Section III, we implemented a set of tools in MATLAB leveraging those used by Rogers in [28]. Specifically, we wanted to: 1) analyze the size of available keyspaces for sample test systems under various constraints, and 2) examine the properties of the keys within those keyspaces.

Below is a brief discussion of the tools developed and the methodology used to analyze our proposed approach.

A. Existing tools

We have access to two tools which are leveraged heavily in analysis of the perturbation method. These tools find optimal D-FACTS placement and solve the power flow equations for analysis.

- *Power flow solver:* This is an implementation of a standard AC power flow solver which takes parameters representing the system under study as input. It is custom-designed to allow for re-numbering of lines and matrix indices for ease of use with the D-FACTS placement code. Its results have been verified for accuracy against other power flow solvers to ensure correctness.
- *D-FACTS placement:* This Matlab code uses a simple steepest-descent optimization algorithm to determine the most effective D-FACTS placements and the optimal (minimal power loss) settings. [28]

B. New Tools

We also implement new tools to do further analysis of perturbation. These tools have the broad purpose of finding and analyzing keyspaces.

- *Keyspace analysis:* To find the raw set of acceptable keys, this tool tests all the available keys in a given system against certain bounds. This tool has several parameters for a given system: a vector detailing the D-FACTS settings for minimum power loss, a maximum distance from the unaltered line impedance to which a D-FACTS can be set, a "step size" denoting incremental values available to the D-FACTS within that distance, and a maximum distance from minimum power loss that is deemed acceptable. Using these parameters, the Keyspace Analysis tool iterates over each possible D-FACTS setting, solves for the power flow with those settings, and finally determines if the new power loss is within the allowed distance from the minimum loss point. If this additional loss is in the allowed range, the key is considered valid.
- *Linear solution analyzer:* This tool analyzes keyspaces to determine if a sensitivity matrix produces a sufficiently accurate model for each key. The sensitivity matrix allows for fast linear analysis of the changes caused by a key to derive the expected values. The linear solution analyzer compares the linear solution and the full AC power solution, and if the difference between solutions is within an acceptable error range, it declares the key as valid.

C. Experiments

Using the tools described above, we analyze 6 different bus systems: a 7-bus test case, a 38-bus utility system, a 37-bus test case, the IEEE 14-bus test case, the IEEE 24-bus Reliability Test System, and the WSCC 9-bus case. For each of these, we calculate the raw keyspaces using a 20% maximum change of line impedance, in discrete steps of 5%, and an acceptance threshold of 1% additional loss from the power loss minimum. We then analyze the actual changes (as given by the AC power flow solution) effected by keys to determine how many are within 1% and 0.5% of

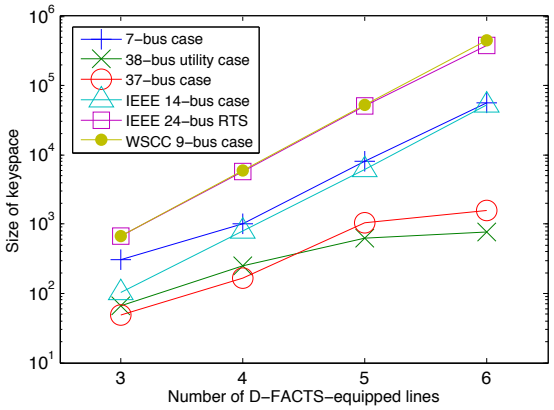

Figure 1. Size of keyspace within 1% of minimum power loss for various systems

the linear solution. We also examine the size of these measurement changes relative to their unperturbed values. These experiments provide the basis data for the following analysis in Section VI.

VI. Results and Analysis

In this section we analyze the results of experiments on the 6 bus systems described above in Section V. First we discuss the general results in Section VI-A, and then describe an in-depth case study of the IEEE 24-Bus Reliability Test System in Section VI-B. We have also made more case studies available on our website [1]. Finally in Section VI-C we present a scenario highlighting the utility of this work.

A. General analysis

As shown in Figure 1, sufficiently large keyspaces are attained for most of our test systems even when restricting the possible operating points to a small neighborhood around the optimum operating point (with respect to power loss), while placing D-FACTS on only a few lines. Specifically, with 3 D-FACTS-enabled lines the keyspace size ranged between 48 and 678 across the six systems. When D-FACTS-enabled lines were increased to 6 the keyspace size ranged between 762 and 454263. One feature of the graph worth noting is that in our set of six systems, there are three pairs whose keyspace sizes trend similarly to each other. It will be worth investigating a larger set of systems, in an attempt to discern any underlying system characteristics which affect the size of keyspaces. It may be that larger systems need a higher number of D-FACTS-equipped lines (resulting in a percentage of lines covered that is closer to that of 3-6 covered lines in the smaller systems) in order to obtain keyspaces of size similar to that of the smaller systems. Perhaps the size of keyspaces also depends on features of the physical system, such as graph connectivity.

There are various factors that may constrain the size of a given keyspace, some of which we have investigated in the present work. Even with these constraints, however, it is still evident that a sufficient subset of keys can be available for use. One such constraint is that the changes effected by a chosen key must actually be observable at the designated measurements points. We call this the "observability constraint". Another potential constraint is to require that the actual changes effected by a key remain within a certain percentage of the values expected through linear analysis. We call this the "linearity constraint". We have examined all of our experimental keyspaces for keys lying within or outside the bounds defined by the two constraints. The results of these tests (using power flows as the measured values) are summarized in Table I. For the systems under consideration the keyspace size did not decrease much even with a stringent linearity constraint ($\leq 0.5\%$) but saw a significant reduction when the observability constraint is increased to 5% or above.

The choice to only use keys satisfying the observability constraint or the linearity constraint is one that will need to be made on a case-by-case basis. An operator may have very precise measurement units, but not enough computing power to solve for measurement changes outside of reasonable linear bounds. This operator would therefore likely need to restrict the keyspace to keys that satisfy the linearity constraint to a specified percentage. Alternatively, an operator may have great computing power but imprecise measurement units. In this case, the operator would likely chose to only use keys who effect sufficiently large changes in measurements. This inherent freedom of picking customized keyspaces makes our perturbation tool widely extensible.

Another important factor which will determine the size of the keyspace is the distance needed between keys (the keyspace "resolution"), in order for the changes each key induces in measurements to be distinguishable from one another. Again, what determines "distinguishable" will vary based on the quality of the observable measurement data. Finally, and perhaps most importantly, there may be constraints on the keyspace due to grid stability requirements. This, too, will be a concern that must be determined on a case-by-case basis. However, we have made some initial

[1] http://go.illinois.edu/KERK

Table I. Size of keyspaces with constraints on power flow measurements. The values used in calculating percentages are all vector norms.

# of DFACTS-equipped lines	3	4	5	6
7-bus case				
No constraints:	306	1005	7944	56712
If actual changes are:				
$\leq$ 1% of linear model	292	1005	7944	56712
$\leq$ 0.5% of linear model	218	866	7252	50946
$\geq$ 1% of optimum values	300	1000	7902	56342
$\geq$ 5% of optimum values	94	201	1373	9000
38-bus utility case				
No constraints:	67	252	622	762
If actual changes are:				
$\leq$ 1% of linear model	66	251	621	761
$\leq$ 0.5% of linear model	59	232	590	733
$\geq$ 1% of optimum values	62	239	603	744
$\geq$ 5% of optimum values	4	17	25	22
37-bus case				
No constraints:	48	168	1060	1552
If actual changes are:				
$\leq$ 1% of linear model	39	168	1047	1538
$\leq$ 0.5% of linear model	39	161	919	1394
$\geq$ 1% of optimum values	31	157	1041	1529
$\geq$ 5% of optimum values	0	10	184	180
IEEE 14-bus case				
No constraints:	102	796	6150	52616
If actual changes are:				
$\leq$ 1% of linear model	102	793	5969	52121
$\leq$ 0.5% of linear model	96	708	4313	38788
$\geq$ 1% of optimum values	98	788	6123	52410
$\geq$ 5% of optimum values	27	264	3133	27589
IEEE 24-bus Reliability Test System				
No constraints:	677	5803	50507	381536
If actual changes are:				
$\leq$ 1% of linear model	643	5525	47271	356425
$\leq$ 0.5% of linear model	435	3691	29416	228071
$\geq$ 1% of optimum values	614	5723	49745	378443
$\geq$ 5% of optimum values	0	583	8015	63968
WSCC 9-bus case				
No constraints:	678	5980	51990	454263
If actual changes are:				
$\leq$ 1% of linear model	678	5980	51990	454263
$\leq$ 0.5% of linear model	659	5892	51705	453247
$\geq$ 1% of optimum values	523	4564	39624	338991
$\geq$ 5% of optimum values	40	246	1429	5494

attempts at mitigating potentially destabilizing effects by restricting ourselves to a small area of operation around an optimal operating point, in this case the minimum power loss point.

B. In depth case study: IEEE 24-Bus Reliability Test System

To provide an example of how a viable keyspace might be obtained on an actual system, we present

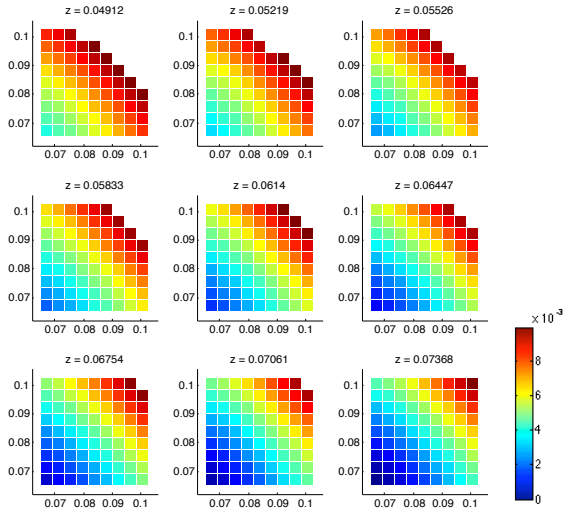

Figure 2. Power loss heat map for RTS system with 3 D-FACTS-equipped lines. Color represents the ratio of additional loss to minimum loss.

an implementation for the IEEE 24-bus Reliability Test System (RTS) [27]. This system provides a large keyspace with only a small number of D-FACTS-equipped lines. As shown in Figure 2, only 3 lines with D-FACTS-equipped lines is enough to obtain a keyspace of 677 points within 1% of the minimum power loss.

Suppose we need to impose further constraints on the keyspace, such as the previously-mentioned linearity or observability concerns. The size of keyspaces on this system due to such constraints is detailed in Figure 3. The figure only details restrictions on the keyspace using power flows as the chosen measurement. This is because for this example case, when choosing voltage as the measurement to be observed, there are no keys (for any of 3 through 6 D-FACTS-equipped lines) effecting a norm change of at least 1%. We suspect that the discrepancy between changes in power flow versus those seen in voltage may be due in part to the fact that the D-FACTS devices in our experimental setup are placed on lines which will have the greatest impact on power flow. It may be worth investigating if a different strategic placement of D-FACTS devices would provide keys effecting greater changes in voltages.

C. Alice and Bob kick the system

Below we present a scenario in which a utility operator Alice must make a decision regarding the

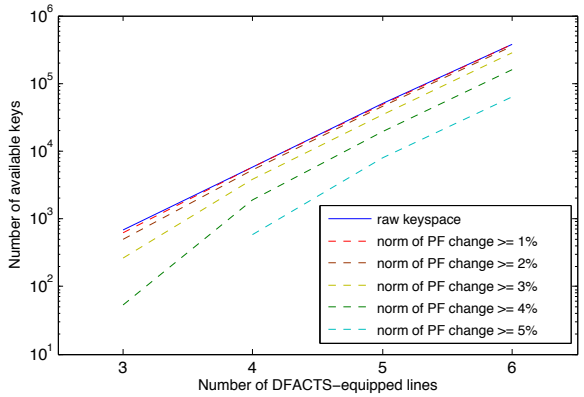

Figure 3. Size of keyspace in IEEE 24-bus RTS system, under observability constraints

operation of the power system, based on information to her in the control room. An adversary, Bob, has hi-jacked a communications channel, allowing him to report incorrect results for some sensors in the system operated by the utility. For simplicity let us assume that there is no noise in the measurements. This scenario uses the system analyzed in-depth previously in Section VI-B.

Bob's compromise of the communications channel allows him to perform what is known as a replay attack; he will inject false values into the messages from sensors containing measurement values. For this scenario, the messages replayed are those from a similar day in the past on which an event occurred that resulted in an outage.

Alice is well-trained and experienced, and thus sees this situation as a potential problem. She now has a decision to make: take remedial action, potentially affecting customers; or do nothing, potentially resulting in a larger outage.

Without perturbation analysis: Alice has only her experience and best judgement to go by. While in reality there is no actual risk of outage, Alice has no way of knowing that. She decides to take remedial action, resulting in some customer outages.

With perturbation analysis: Alice knows that she has some time to make the load-shed decision. The utility has a policy to validate any incoming measurements which would result in drastic action. Following policy, Alice initiates the Perturbation Analysis System (PAS). Prior to running PAS, the D-FACTS devices are set to $\mathbf{x}_0$ and the sensors report that the measurements used to observe perturbations is $\mathbf{m}_0$.

The analysis tool randomly selects a perturbation key $\mathbf{k}$ from its precomputed list of available keys. These available keys have been precomputed to include only those that allow for accurate and fast linear prediction of expected measurement values. Specifically, in this case keys are included only if the "real" values (as determined from solving the nonlinear power flow equations) should fall within 0.5% of the linearly expected values. That is to say, for linearly expected values of $\mathbf{m}_{pred}$, and values from the power flow solution $\mathbf{m}_{obs}$:

$$\frac{||\mathbf{m}_{obs} - \mathbf{m}_{pred}||}{||\mathbf{m}_{pred}||} \leq .005 \tag{7}$$

where:

$$\mathbf{m}_{pred} = \mathbf{A}(\mathbf{k} - \mathbf{x}_0) + \mathbf{m}_0 \tag{8}$$

and $\mathbf{A}$ is the sensitivity matrix relating changes in impedance to changes in measured values.

This randomly-selected key then is used to send commands to the D-FACTS devices on the utility's lines. The system is left in its new state for a short while, to allow for stabilization. Then a new set of measurements is gathered. At this point the measurements coming in, $\mathbf{m}_{obs}$, are values which are appropriate for the new state of the system, with the exception of those in Bob's replay attack. His spoofed measurements will not have altered to reflect the system change [2] as they are being replayed from a past event.

Finally, the solver compares the expected and observed measurement values using Eq. (7). The resulting value is $>.005$. This indicates there is a problem with the measurements. Alice then begins a more thorough investigation of the situation, delaying her decision to take remedial actions until there is a confirmation of the problem. Bob's attack is thwarted because he could not account for the unexpected changes in the power system.

With regular perturbation analysis: The PAS system regularly perturbs the system (perhaps every n minutes, where n is a random number with a Gaussian distribution around a reasonable interval). When this is happening, Bob's replay attack is caught during the first automatic perturbation, allowing early detection of the attack. This allows Alice to begin an investigation without requiring a decision about potentially costly remedial actions.

VII. Conclusions

In this work we have proposed and analyzed a perturbation-based approach for detecting both fault-induced and maliciously-injected bad data in the power

[2]Or they will have altered to a different key as was used during the previous event.

grid. Our analysis shows that the approach is valid and promising. Specifically, we have showed that it is possible to find a sufficiently large set of perturbation keys that keep the system close to an optimal operating point—in this case within 1% of minimal power loss—with only a few D-FACTS-equipped lines. Furthermore, large subsets of keys in the identified keyspaces allow for a fast linear analysis. However, more work needs to be done to understand the viability of the approach in real systems, where there will be measurement noise and changes in power flow due to load dynamics.

VIII. Future Work

There are several issues that in need of further investigation before the perturbation-based technique proposed here could become useful and viable. Specifically, our present analysis is limited to the case where the D-FACTS were already placed in the system for minimizing power loss. Analyzing the approach without any constraints on D-FACTS device placement might yield more favorable results in terms of keyspaces and their properties. Understanding the relationship between keyspace size and the number of lines, connectivity, or topology of a system is another open direction; this might provide better insight into where to place D-FACTS devices from a security perspective. Apart from just detecting the presence of bad data, we believe that this approach could also be extended to identify the bad data by applying a sequence of perturbations. Bad data identification algorithms that leverage a sequence of perturbations is another exciting future direction. Lastly, the potential introduction of transient effects or stability issues by this approach is an important concern that needs to be addressed before this approach can become viable.

Acknowledgment

This material is based upon work supported in part by the Department of Energy under Award Number DE-OE0000097 and by the U.S. Department of Energy Consortium for Electric Reliability Technology Solutions (CERTS).

References

[1] Bad data detection and identification. *International Journal of Electrical Power and Energy Systems*, 12:94–103, April 1990.

[2] A. Abur. A bad data identification method for linear programming state estimation. *Power Systems, IEEE Trans. on*, 5(3):894–901, Aug 1990.

[3] E. Asada, A. Garcia, and R. Romero. Identifying multiple interacting bad data in power system state estimation. In *Power Engineering Society General Meeting, 2005. IEEE*, pages 571–577 Vol. 1, June 2005.

[4] R. B. Bobba, K. M. Rogers, Q. Wang, H. Khurana, K. Nahrstedt, and T. J. Overbye. Detecting false data injection attacks on dc state estimation. 2010.

[5] J. Chen and A. Abur. Placement of pmus to enable bad data detection in state estimation. *Power Systems, IEEE Trans. on*, 21(4):1608–1615, Nov. 2006.

[6] J. Chen and A. Abur. Placement of pmus to enable bad data detection in state estimation. *IEEE Trans. on Power Systems*, 21:1608–1615, 2006.

[7] G. Dán and H. Sandberg. Stealth attacks and protection schemes for state estimators in power systems. In *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conf. on*, pages 214 –219, oct. 2010.

[8] X. N. de, W. Shi-ying, and Y. Ers-keng. An application of estimation-identification approach of multiple bad data in power system state estimation. *Power Apparatus and Systems, IEEE Trans. on*, PAS-103(2):225–233, Feb. 1984.

[9] D. Falcao, P. Cooke, and A. Brameller. Power system tracking state estimation and bad data processing. *Power Apparatus and Systems, IEEE Trans. on*, PAS-101(2):325–333, Feb. 1982.

[10] E. Handschin, F. Schweppe, J. Kohlas, and A. Fiechter. Bad data analysis for power system state estimation. *Power Apparatus and Systems, IEEE Trans. on*, 94(2):329–337, Mar 1975.

[11] J. Hauer and J. DeSteese. A tutorial on detection and characterization of special behavior in large electric power systems. Technical report, Pacific Northwest National Laboratory, Cambridge, MA Rep. PNL-14655, July 2004.

[12] J. Hauer, W. Mittelstadt, K. Martin, J. Burns, H. Lee, J. Pierre, and D. Trudnowski. Use of the wecc wams in wide-area probing tests for validation of system performance and modeling. *IEEE Trans. on Power Systems*, 24(1):250–257, Feb 2009.

[13] O. Kosut, L. Jia, R. J. Thomas, and L. Tong. Limiting false data attacks on power system state estimation. In *CISS*, pages 1–6, 2010.

[14] O. Kosut, L. Jia, R. J. Thomas, and L. Tong. Malicious data attacks on smart grid state estimation: Attack strategies and countermeasures. In *Smart Grid Communications SmartGridComm 2010 First IEEE International Conf. on*. IEEE, 2010.

[15] W. Kotiuga and M. Vidyasagar. Bad data rejection properties of weughted least absolute value techniques applied to static state estimation. *Power Apparatus and Systems, IEEE Trans. on*, PAS-101(4):844–853, April 1982.

[16] Y. Liu, P. Ning, and M. Reiter. False data injection attacks against state estimation in electric power grids. *To appear in ACM Trans. in Information and Systems Security (TISSEC), 2011.*

[17] Y. Liu, M. K. Reiter, and P. Ning. False data injection attacks against state estimation in electric power grids. In *CCS '09: Proceedings of the 16th ACM Conf. on Computer and communications security*, pages 21–32, New York, NY, USA, 2009. ACM.

[18] R. L. Lugtu, D. F. Hackett, K. C. Liu, and D. D. Might. Power system state estimation: Detection of topological errors. *IEEE Trans. on Power Apparatus and Systems*, PAS-99:2406–2412, 1980.

[19] H. Merrill and F. Schweppe. Bad data suppression in power system static state estimation. *Power Apparatus and Systems, IEEE Trans. on*, PAS-90(6):2718–2725, Nov. 1971.

[20] Y. Mo and B. Sinopoli. Secure control against replay attacks. *Proceedings of the 47th Annual Allerton Conf. on Communication Control and Computing*, pages 911–918, 2009.

[21] A. Monticelli. *State estimation in electric power systems: a generalized approach*. Kluwer Academic Publishers, 1999.

[22] A. Monticelli and A. Garcia. Reliable bad data processing for real-time state estimation. *Power Apparatus and Systems, IEEE Trans. on*, PAS-102(5):1126–1139, May 1983.

[23] A. Monticelli, F. F. Wu, and M. Yen. Multiple bad data identification for state estimation by combinatorial optimization. *Power Engineering Review, IEEE*, PER-6(7):73 –74, july 1986.

[24] X. Nian-de, W. Shi-ying, and Y. Er-keng. A new approach for detection and identification of multiple bad data in power system state estimation. *Power Apparatus and Systems, IEEE Trans. on*, PAS-101(2):454–462, Feb. 1982.

[25] W. Peterson and A. Girgis. Multiple bad data detection in power system state estimation using linear programming. In *System Theory, 1988., Proceedings of the Twentieth Southeastern Symp. on*, pages 405–409, Mar 1988.

[26] J. Pierre, N. Zhou, F. Tuffner, J. Hauer, D. Trudnowski, and W. Mittelstadt. Probing signal design for power system identification. *Power Systems, IEEE Trans. on*, 25(2):835 –843, may 2010.

[27] I. C. Report. Ieee reliability test system. *IEEE Trans. on Power Apparatus and Systems*, PAS-98:2047–2054, 1979.

[28] K. M. Rogers. Power system control with distributed flexible ac transmission system devices. Master's thesis, UIUC, 2009.

[29] K. M. Rogers and T. J. Overbye. Some applications of distributed flexible ac transmission system (d-facts) devices in power systems. In *Power Symp., 2008. NAPS '08. 40th North American*, pages 1 –8, sept. 2008.

[30] K. M. Rogers and T. J. Overbye. Power flow control with distributed flexible ac transmission system (d-facts) devices. In *North American Power Symp. (NAPS), 2009*, pages 1–6, oct. 2009.

[31] F. C. Schweppe and J. Wildes. Power System Static-State Estimation, Part I: Exact Model. *IEEE Trans. on Power Apparatus and Systems*, PAS-89(1):120–125, 1970.

[32] I. Slutsker. Bad data identification in power system state estimation based on measurement compensation and linear residual calculation. *Power Systems, IEEE Trans. on*, 4(1):53–60, Feb 1989.

[33] A. Teixeira, S. Amin, H. Sandberg, K. Johansson, and S. Sastry. Cyber security analysis of state estimators in electric power systems. In *Decision and Control (CDC), 2010 49th IEEE Conf. on*, pages 5991 –5998, dec. 2010.

[34] D. Trudnowski and T. Ferryman. Wecc modal baseline analysis results as of june 2010. Technical report, NASPI, June 2010.

[35] D. Trudnowski, J. Pierre, N. Zhou, F. Tuffner, J. Hauer, and B. Mittelstadt. Wecc dynamic probing tests: Purpose and results. Technical report, NASPI, October 2008.

[36] T. Van Cutsem, M. Ribbens-Pavella, and L. Mili. Hypothesis testing identification: A new method for bad data analysis in power system state estimation. *Power Apparatus and Systems, IEEE Trans. on*, PAS-103(11):3239–3252, Nov. 1984.

[37] A. Wood and B. Wollenberg. *Power Generation, Operation, and Control*. John Wiley and Sons, 2nd edistion edition, 1996.

[38] F. Wu and W. Liu. Detection of topology errors by state estimations. *IEEE Trans. on Power Systems*, 4:176–183, Jan 1989.

[39] F. Wu, W.-H. Liu, and S.-M. Lun. Observability analysis and bad data processing for state estimation with equality constraints. *Power Systems, IEEE Trans. on*, 3(2):541–548, May 1988.

[40] B. Zhang, S. Wang, and N. Xiang. A linear recursive bad data identification method with real-time application to power system state estimation. *Power Systems, IEEE Trans. on*, 7(3):1378–1385, Aug 1992.

[41] N. Zhou, J. Pierre, and J. Hauer. Initial results in power system identification from injected probing signals using a subspace method. *IEEE Trans. on Power Systems*, 21(3):1296–1302, Aug 2006.