Secure Market Operation in Presence of Critical Model Parameters in State Estimation

Yuzhang Lin, *Member*, *IEEE*, Ali Abur, *Fellow*, *IEEE*, and Hanchen Xu

***Abstract*—This paper is concerned about the impact of network parameter errors on the reliable operation and management of electricity markets. Specifically, the paper investigates the so-called critical parameters in a network model whose errors cannot be detected or estimated due to the lack of local measurement redundancy. Due to this property of critical parameters, it will be impossible to detect, identify and correct errors in these parameters. Given the fact that electricity market applications are heavily model-dependent, the locational marginal prices (LMPs) can be shown to be seriously distorted in the presence of critical parameter errors. Furthermore, if such errors are maliciously injected by adversaries, they will go undetected. Meanwhile, prices and revenues associated with power transactions may be strategically manipulated. An approach for quantifying the impact of critical parameters on the management of electricity markets is proposed. Conditions related to network topology and measurement configuration leading to the appearance of critical parameters are classified, and meter placement strategies for avoiding critical parameters are presented as well. Simulation results obtained by using IEEE test systems are given to verify the proposed analysis and design methods.**

***Index Terms*—Anomaly detection, cyber security, electricity market, parameter estimation, power system modeling, state estimation.**

I. Introduction

MAINTAINING an accurate database of model parameters is crucial for the reliable execution of a number of power network applications such as state estimation (SE), optimal power flow, contingency analysis, protective relaying, and control. In deregulated electricity markets, the market settlement is carried out by solving an economic dispatch (ED) problem. The solution yields the optimal output for each generator, as well as the energy price at each node in the network, known as the locational marginal price (LMP) [1], [2]. In the ED problem formulation, branch power flows are expressed in terms of the injection shift factors (ISFs), which are calculated using the network topology and parameters. If the parameters of a network model contain substantial errors, the ISFs can be significantly affected, which will in turn bias the congestion patterns and the calculation of the LMPs. Therefore, ensuring the accuracy of model parameters is a pre-requisite for establishing an unbiased and fair electricity market.

With heavier reliance on communication and information systems, the cyber security of power system operation draws increasing attention in recent years. Intrusion events into various parts of the system with various objectives have been reported in different countries [3]. In view of this trend, a large volume of work has been dedicated to studying the potential attack paths and strategies, and possible defense measures to enhance the security of power systems as cyber-physical systems. Among them, a number of publications have focused on the so-called false data injection (FDI) attacks [4] - [9]. There have also been studies on how FDI attacks can be utilized to manipulate the outcomes of real-time electricity markets [10] - [12]. It is still an open question whether this type of attack is actually implementable, since it is generally necessary to manipulate and coordinate a large number of measurements in real time so that the injected false data is undetectable by the state estimator.

Even through establishing high security for a strategic subset of power system measurements has been extensively discussed, there has not been much work reported on the security of the power system model database or its impact on system operation. This database resides and is managed at the energy management systems (EMSs) of control centers, which are generally better protected and thus more difficult to access compared with the networks at the substation level. However, such possibilities cannot be discounted or completely ignored. In fact, the cyber attack against Ukraine power grid in December 2015 [13] has revealed that knowledgeable cyber adversaries are capable to intrude into the computer networks in control centers. Specifically, for the vulnerability of model database under cyber attacks, the following points require special attention:

1) While the access to model databases in control centers is more difficult than that to substation measurements, it is much easier to introduce a one-time change to a certain set of model parameters than to continuously generate plausible real-time false data in a large measurement set.

2) The model database can be accessed and modified by

Manuscript received: January 4, 2020; accepted: May 28, 2020. Date of CrossCheck: May 28, 2020. Date of online publication: July 9, 2020.

This work was supported in part by the National Science Foundation (No. 1947617).

Y. Lin (corresponding author) is with University of Massachusetts, Lowell, MA 01854, USA (e-mail: yuzhang_lin@uml.edu).

A. Abur is with Northeastern University, Boston, MA 02115, USA (e-mail: abur@ece.neu.edu).

H. Xu is with the University of Illinois at Urbana-Champaign, Urbana, IL 61801, USA (e-mail: hxu45@illinois.edu).

DOI: 10.35833/MPCE.2020.000007

using the credentials of internal personnel, while there is no legitimate means to modify the measurement dataset even for internal personnel.

3) While false data in real-time measurements can only affect online applications, parameter errors can affect both online and offline applications, thus will have a wider impact on power system operation.

In this paper, a new security vulnerability of the model database is identified, and its impact on electricity markets is demonstrated. It involves the so-called "critical parameters" in power network models, which have been formally defined and studied in a recent publication [14]. In general, parameter errors can be detected when measurements do not fit the model parameters [14] - [20]. Based on SE, statistical tests can be developed to detect and identify the errors. However, due to the lack of local measurement redundancy, errors associated with certain parameters can neither be detected, nor estimated, irrespective of the magnitude of the errors. In other words, any errors in these parameters will remain "invisible" and permanent. Such errors, whether due to unintentional reasons or deliberate manipulation by adversaries, are likely to exert a long-lasting impact on the model-based applications. In this paper, it is shown that undetectable errors in critical parameters may have significant impact on the ISFs and congestion patterns, thus can significantly bias the LMPs of certain nodes. It should be noted that, unlike the well-discussed FDI attacks which generally require coordinated manipulation of a large number of measurements in order to keep the stealthy property, the manipulation of critical model parameters is, by nature, undetectable. Therefore, cyber adversaries may choose to manipulate any single critical parameter without any coordination, which increases its chance to be implemented.

In view of the vulnerabilities associated with critical parameters, an effective method for ranking the significance of impacts from different critical parameters on the market outcomes in a given system is subsequently presented in this paper. In order to eliminate critical parameters, they are further classified into two distinct groups: those associated with critical measurements (or critical *k*-tuples), and those associated with irrelevant branches. The approaches to meter placement are then discussed and shown to be effective for converting critical parameters into non-critical ones. Simulation results on the IEEE 57-bus system are given to illustrate the analyses and methods proposed in this paper.

The contributions of this paper are summarized below:

1) The conceptual linkage between the critical parameter issues in model error identification and the security of electricity market operation is explicitly established, which has been overlooked in the existing body of literature.

2) An effective approach to evaluating the impacts of critical model parameters on the operation of electricity markets is developed.

3) The conditions for existence of critical parameters are classified into two categories, and the guidelines of meter placement for eliminating the criticality of these parameters are proposed and discussed.

The motivations of cyber attacks can be broadly classified into two categories: inflicting heavy damages to power systems, and gaining economic benefits without being detected. The analysis presented in this paper focuses on the security threats based on the second type of motivations.

Compared with the related work [14] where the concept of critical parameters is formally defined and validated based on the theory of SE, the unique contributions of this paper are the development of the conceptual linkage between critical parameters and secure operation of electricity markets, and the development of a systematic assessment and mitigation framework for secure market operation.

It should also be noted that it is possible to have simultaneous measurement and model parameter errors, but measurement errors are not explicitly discussed in this paper, partly because they are irrelevant to the analysis of critical parameters, and partly because this problem has been well addressed in the previous work such as [14].

The rest of this paper is organized as follows. In Section II, the formulation and solution of the parameter error detection and identification problem are reviewed. In Section III, the ED problem and LMPs are briefly described. Section IV introduces the concept of critical parameters, shows its impact on the electricity markets, and proposes an approach to quantifying the impact of critical parameters. Section V further studies various circumstances of critical parameters, and proposes a simple meter placement approach to handle them. Simulation results in the IEEE 57-bus system are given in Section VI. Finally, Section VII concludes the paper.

II. SE and Parameter Error Detection

In general, the principle of detecting model parameter errors is based on checking the network model against the measurements. Based on the understanding of measurement error distribution, statistical tests can be designed to detect the inconsistency between the measurements and the model parameters. The chi-square test [19] and the largest normalized Lagrange multiplier (LNLM) test [14], [16] - [18] are two approaches developed based on this general principle. In order to introduce these tests, the weighted least square (WLS) SE problem needs to be reviewed first.

Suppose there are n state variables and m measurements in a power system. Consider the set of measurement equations:

$$\boldsymbol{z}=\boldsymbol{h}(\boldsymbol{x},\boldsymbol{p})+\boldsymbol{e} \tag{1}$$

where $\boldsymbol{z}$ is the measurement vector; $\boldsymbol{x}$ is the state vector; $\boldsymbol{e}$ is the measurement error vector; $\boldsymbol{p}$ is the parameter vector; and $\boldsymbol{h}$ is the nonlinear function linking the state variables to the measurements. Assuming Gaussian distribution for the measurements, the maximum likelihood estimator of the state variables can be obtained by solving the WLS SE problem given below [14]:

$$\begin{cases}\min\limits_{x,p} J=\dfrac{1}{2}\left(\boldsymbol{z}-\boldsymbol{h}(\boldsymbol{x},\boldsymbol{p})\right)^{\mathrm{T}}\boldsymbol{R}^{-1}\left(\boldsymbol{z}-\boldsymbol{h}(\boldsymbol{x},\boldsymbol{p})\right)\\ \text{s.t. } \boldsymbol{p}=\boldsymbol{p}_0\end{cases} \tag{2}$$

where $\boldsymbol{R}$ is the covariance matrix associated with the measurement errors; and $\boldsymbol{p}_0$ is the vector containing the original

values of the parameters. The equality constraints are equivalent to assuming that all parameter values are error-free. At the solution point $\boldsymbol{x}^*$, dropping the coefficient 1/2, the objective function J^* can be expressed as:

$$J^* = \left(\boldsymbol{z} - \boldsymbol{h}\left(\boldsymbol{x}^*, \boldsymbol{p}_0\right)\right)^{\mathrm{T}} \boldsymbol{R}^{-1} \left(\boldsymbol{z} - \boldsymbol{h}\left(\boldsymbol{x}^*, \boldsymbol{p}_0\right)\right) \tag{3}$$

For the i^{th} measurement, we define

$$e_i = \frac{z_i - h_i\left(\boldsymbol{x}, \boldsymbol{p}_0\right)}{\sigma_i} \tag{4}$$

where σ_i is the standard deviation of error of the i^{th} measurement. Then, (3) can be rewritten as:

$$J^* = \sum_{i=1}^{m} e_i^2 \tag{5}$$

If the parameters are actually error-free and the measurement errors obey normal distributions, J^* will approximately have a chi-square distribution with $m-n$ degrees of freedom:

$$J^* \sim \chi^2_{m-n} \tag{6}$$

With a specified confidence level $1-\alpha$, a threshold t can be set up such that

$$CHI2CDF\left(t, m-n\right) = 1-\alpha \tag{7}$$

where $CHI2CDF\left(\cdot\right)$ is the chi-square cumulative distribution function.

If $J^* > t$, it can be inferred with the false alarm probability α that either the model parameters are erroneous or the measurements contain gross errors. Hence, it can be used as an approach to the detection of model parameter errors.

For more accurate detection and identification of model parameter errors, the LNLM test has later been developed [14], [16]-[18].

The Lagrangian formulation of (2) can be written as:

$$L\left(\boldsymbol{x}, \boldsymbol{p}, \boldsymbol{\lambda}\right) = \frac{1}{2}\left(\boldsymbol{z} - \boldsymbol{h}\left(\boldsymbol{x}, \boldsymbol{p}\right)\right)^{\mathrm{T}} \boldsymbol{R}^{-1} \left(\boldsymbol{z} - \boldsymbol{h}\left(\boldsymbol{x}, \boldsymbol{p}\right)\right) - \boldsymbol{\lambda}^{\mathrm{T}} \boldsymbol{p} \tag{8}$$

where $\boldsymbol{\lambda}$ is the Lagrange multiplier vector associated with the equality constraints $\boldsymbol{p} = \boldsymbol{p}_0$. At the point of solution, the first-order necessary condition must be met:

$$\frac{\partial L\left(\boldsymbol{x}^*, \boldsymbol{p}, \boldsymbol{\lambda}\right)}{\partial \boldsymbol{p}} = \boldsymbol{H}_p^{\mathrm{T}} \boldsymbol{R}^{-1} \left(\boldsymbol{z} - \boldsymbol{h}\left(\boldsymbol{x}^*, \boldsymbol{p}\right)\right) + \boldsymbol{\lambda} = \boldsymbol{0} \tag{9}$$

where $\boldsymbol{H}_p^{\mathrm{T}}$ is the Jacobian matrix of the measurement vector with respect to the parameter vector $\boldsymbol{p}$.

The measurement residual vector is defined as:

$$\boldsymbol{r} = \boldsymbol{z} - \boldsymbol{h}\left(\boldsymbol{x}^*, \boldsymbol{p}_0\right) \tag{10}$$

Then, the Lagrange multiplier vector can be recovered by:

$$\boldsymbol{\lambda} = -\boldsymbol{H}_p^{\mathrm{T}} \boldsymbol{R}^{-1} \boldsymbol{r} \tag{11}$$

In the absence of parameter errors, the measurement residuals can be linked to the measurement errors as [19]:

$$\boldsymbol{r} = \boldsymbol{S}\boldsymbol{e} \tag{12}$$

$$\boldsymbol{S} = \boldsymbol{I} - \boldsymbol{H}\left(\boldsymbol{H}^{\mathrm{T}} \boldsymbol{R}^{-1} \boldsymbol{H}\right)^{-1} \boldsymbol{H}^{\mathrm{T}} \boldsymbol{R}^{-1} \tag{13}$$

where $\boldsymbol{S}$ is the sensitivity matrix; $\boldsymbol{I}$ is an identity matrix; and $\boldsymbol{H}$ is the Jacobian matrix of $\boldsymbol{h}$ with respect to the state vector. Hence, the Lagrange multipliers will have a zero mean:

$$E\left(\boldsymbol{\lambda}^{\mathrm{T}}\right) = E\left(-\boldsymbol{H}_p^{\mathrm{T}} \boldsymbol{R}^{-1} \boldsymbol{r}\right) = -\boldsymbol{H}_p^{\mathrm{T}} \boldsymbol{R}^{-1} E\left(\boldsymbol{r}\right) = -\boldsymbol{H}_p^{\mathrm{T}} \boldsymbol{R}^{-1} E\left(\boldsymbol{S}\boldsymbol{e}\right) = -\boldsymbol{H}_p^{\mathrm{T}} \boldsymbol{R}^{-1} \boldsymbol{S} E\left(\boldsymbol{e}\right) = \boldsymbol{0} \tag{14}$$

where $E\left(\cdot\right)$ is the expectation function.

The covariance matrix of the Lagrange multipliers can be expressed as:

$$\operatorname{cov}\left(\boldsymbol{\lambda}\right) = E\left(\boldsymbol{\lambda}\boldsymbol{\lambda}^{\mathrm{T}}\right) = E\left(\boldsymbol{H}_p^{\mathrm{T}} \boldsymbol{R}^{-1} \boldsymbol{r}\boldsymbol{r}^{\mathrm{T}} \left(\boldsymbol{R}^{-1}\right)^{\mathrm{T}} \boldsymbol{H}_p\right) = \boldsymbol{H}_p^{\mathrm{T}} \boldsymbol{R}^{-1} \operatorname{cov}\left(\boldsymbol{r}\right) \left(\boldsymbol{R}^{-1}\right)^{\mathrm{T}} \boldsymbol{H}_p \tag{15}$$

It is known that the covariance matrix of the residuals can be expressed as:

$$\operatorname{cov}\left(\boldsymbol{r}\right) = \boldsymbol{S}\boldsymbol{R} \tag{16}$$

Combining (15) and (16) will yield

$$\operatorname{cov}\left(\boldsymbol{\lambda}\right) = \boldsymbol{H}_p^{\mathrm{T}} \boldsymbol{R}^{-1} \operatorname{cov}\left(\boldsymbol{r}\right) \left(\boldsymbol{R}^{-1}\right)^{\mathrm{T}} \boldsymbol{H}_p = \boldsymbol{H}_p^{\mathrm{T}} \boldsymbol{R}^{-1} \boldsymbol{S}\boldsymbol{R} \left(\boldsymbol{R}^{-1}\right)^{\mathrm{T}} \boldsymbol{H}_p = \boldsymbol{H}_p^{\mathrm{T}} \boldsymbol{R}^{-1} \boldsymbol{S}\boldsymbol{H}_p \tag{17}$$

Denoting $\operatorname{cov}(\boldsymbol{\lambda})$ as $\boldsymbol{\Lambda}$, the normalized Lagrange multiplier (NLM) associated with the i^{th} parameter can be obtained by:

$$\lambda_i^{\mathrm{N}} = \frac{\lambda_i}{\sqrt{\Lambda_{ii}}} \tag{18}$$

where λ_i and Λ_{ii} are the elements of $\boldsymbol{\lambda}$ and $\boldsymbol{\Lambda}$, respectively.

In the absence of parameter errors, it should follow a standard normal distribution. Hence, for a specified confidence level $1-\alpha$, a threshold t can be set up such that

$$\Phi\left(t\right) = 1 - \frac{\alpha}{2} \tag{19}$$

where $\Phi\left(\cdot\right)$ is the standard normal distribution function.

If for any i, $\left|\lambda_i^{\mathrm{N}}\right| > t$, an error is detected, and the parameter associated with the LNLM will be identified as the erroneous parameter.

III. Economic Dispatch and Locational Marginal Price

In current industrial practice, the electricity market is settled by solving an ED problem, where a DC power flow model is used. For simplicity, consider the lossless ED problem:

$$\begin{cases} \min\limits_{s_j} \sum\limits_{j=1}^{N} c_j s_j \\ \text{s.t.} \sum\limits_{j=1}^{N} s_j = \sum\limits_{j=1}^{N} d_j \leftrightarrow \xi \\ \quad s_j^{\min} \le s_j \le s_j^{\max} \leftrightarrow v_j^{\min}, v_j^{\max} \quad j = 1, 2, ..., N \\ \quad f_l^{\min} \le \sum\limits_{j=1}^{N} \Psi_{lj}\left(s_j - d_j\right) \le f_l^{\max} \leftrightarrow \mu_l^{\min}, \mu_l^{\max} \quad l = 1, 2, ..., L \end{cases} \tag{20}$$

where L is the number of branches; N is the number of buses; c_j is the marginal generation cost at bus j; s_j is the power generation at bus j; d_j is the load at bus j; $f_l^{\min}$ and $f_l^{\max}$ are the lower and upper limits of the power flow along branch l determined by security constraints, respectively; $s_j^{\min}$ and $s_j^{\max}$ are the lower and upper limits for the power generation at bus j, respectively; Ψ_{lj} is an entry in the ISF matrix representing the incremental power flow along branch l induced

by per-unit increment of power injection at bus j; ξ is the Lagrange multiplier associated with the power balance constraint; $v_j^{\min}$ and $v_j^{\max}$ are Lagrange multipliers associated with the generation capacity constraints; and $\mu_l^{\min}$ and $\mu_l^{\max}$ are the Lagrange multipliers associated with the branch capacity constraints. The determination of the ISF matrix $\boldsymbol{\Psi}$ is solely dependent on the network model:

$$\boldsymbol{\Psi} = \boldsymbol{B}_f \boldsymbol{A} \boldsymbol{B}^{-1} \tag{21}$$

where $\boldsymbol{B}_f = \mathrm{diag}(b_1, b_2, \ldots, b_L)$ is the primitive susceptance matrix; $\boldsymbol{A}$ is the branch-bus incidence matrix; and $\boldsymbol{B}$ is the nodal susceptance matrix. Since the DC power flow model is adopted, only branch reactance is involved in the computation of $\boldsymbol{\Psi}$.

The solution of (20) will not only provide the generation dispatch that yields the lowest total cost for the entire system, but also yield the LMPs as by-products. The LMP at a given bus j can be recovered by [1], [2]:

$$LMP_j = \xi^* + \sum_{l=1}^{L} \mu_l^{\min *} \Psi_{lj} - \sum_{l=1}^{L} \mu_l^{\max *} \Psi_{lj} \tag{22}$$

where ξ^*, $\mu_l^{\min *}$, and $\mu_l^{\max *}$ are the values of ξ, $\mu_l^{\min}$, and $\mu_l^{\max}$ at the solution point of (20), respectively. $\mu_l^{\min *}$ and $\mu_l^{\max *}$ are also known as the shadow prices associated with the congestion along the corresponding branch. They represent the increment of the total cost with per-unit incremental change of the power flow limit of the l^{th} branch. When the power flow along a branch reaches its limit, i.e., the corresponding inequality constraint is binding, the shadow price $\mu_l^{\min *}$ or $\mu_l^{\max *}$ will be nonzero. When there is no congestion across the system, all the terms associated with the congestion shadow prices will be zero, and ξ^* will be the LMP for all nodes. Obviously, the branch congestion pattern has a significant impact on the LMPs.

IV. Critical Parameter and Its Impact on Security of Electricity Markets

Although various types of methods for detection and estimation of parameter errors have been proposed, their capabilities are always limited by the redundancy of measurements. The concept of critical parameters is used to describe one type of such situations [14]. The Lagrange multiplier vector $\boldsymbol{\lambda}$ can be expressed as a linear combination of parameter errors and measurement errors [14]:

$$\boldsymbol{\lambda} = \boldsymbol{\Lambda} \boldsymbol{p}_e - \boldsymbol{H}_p^{\mathrm{T}} \boldsymbol{R}^{-1} \boldsymbol{S} \boldsymbol{e} \tag{23}$$

where $\boldsymbol{p}_e$ is the parameter error vector.

Critical parameters can be identified by checking the rows or columns of the matrix $\boldsymbol{\Lambda}$. For the i^{th} parameter, if the corresponding column (or equivalently, the corresponding row since $\boldsymbol{\Lambda}$ is symmetrical) $\boldsymbol{\Lambda}_i$ is a null vector, this parameter is a critical parameter, and any error in this parameter cannot be detected. The rationale is that if there is an error $p_{e,i} \neq 0$, the component that is induced into $\boldsymbol{\lambda}$ will be

$$\boldsymbol{\lambda}^{(i)} = p_{e,i} \boldsymbol{\Lambda}_i = \boldsymbol{0} \tag{24}$$

Hence, it will not be reflected in $\boldsymbol{\lambda}$. Furthermore, since $\Lambda_{ii} = 0$, it is also impossible to evaluate the NLM associated with this parameter.

Note that the incapability of detecting an error in a critical parameter is not a limitation of the LNLM approach, but rather a limitation of the measurement configuration of the system. This issue cannot be resolved by developing an alternative method, if the measurement configuration has already been specified. For example, if the augmented SE approach [19]-[21] is used to estimate a critical parameter, the system will become unobservable.

Apparently, if errors are present in critical parameters, they are likely to remain in the database permanently without being detected. If it occurs, the LMPs in the electricity market can be biased. From (22), it can be observed that the impact of undetectable parameter errors on LMPs are threefold:

1) Congestion patterns. In the ED solution, the Lagrange multipliers (shadow prices) $\mu_l^{\min *}$ or $\mu_l^{\max *}$ will be zero if the corresponding branches are not congested, i.e., the corresponding flow constraints in (20) are not binding. On the other hand, $\mu_l^{\min *}$ or $\mu_l^{\max *}$ will be nonzero if the corresponding branches become congested, i.e., the corresponding flow constraints in (20) become binding. In the presence of critical parameter errors, those flow constraints which are not actually binding can appear to be binding, and vice versa. In other words, with parameter errors, branches that are not actually congested can appear congested, and vice versa. This bias will abruptly change Lagrange multipliers $\mu_l^{\min *}$ or $\mu_l^{\max *}$, from zero to nonzero, or the other way around, creating a jump in the second or third term of (22), thus creating a jump in the LMPs.

2) Congestion shadow prices. For those branches that are congested, the Lagrange multipliers $\mu_l^{\min *}$ or $\mu_l^{\max *}$ indicate the sensitivity of the objective function to the binding constraints in the ED problem (20). In other words, they show how sensitive the total generation cost is, if the flow limit of the congested branch changes. When parameter errors are present, the shape of the flow constraints will change, since their expressions contain the ISFs which are determined by the model parameters. As the flow constraints are reshaped, the sensitivity of the objective function to the constraints will also change, which is then reflected in the changes of the Lagrange multipliers (shadow prices) $\mu_l^{\min *}$ or $\mu_l^{\max *}$. This will result in continuous (instead of abrupt) changes of the second or third term of (22), thus affecting the LMPs.

3) ISFs on their own. Besides exerting indirect influences on LMPs through the Lagrange multipliers $\mu_l^{\min *}$ or $\mu_l^{\max *}$, the ISFs also appear in (22) by themselves. This implies that even with specified shadow prices of congested branches (fixed $\mu_l^{\min *}$ or $\mu_l^{\max *}$), the change of ISFs will still influence the second and third terms of (22), thus contributing to the distortion of LMPs. The interpretation for such influences is that ISFs represent the contributions of incremental bus injections to incremental branch flows, thereby representing the effect of selling or purchasing electricity at a specific bus on the degree of congestion in a specific branch.

Therefore, there may be two types of situations jeopardizing electricity market operation:

1) Random errors in critical parameters due to natural or unintentional reasons such as device aging, variation of am-

bient conditions, unreported device status changes, or human entry errors. An unfair trading environment will be formed for different market participants.

2) False values in critical parameters injected by cyber adversaries. This can occur when credentials of internal personnel are leaked to cyber adversaries, and the model parameter database is hacked. In this case, electricity market operation can be manipulated to create unlawful economic benefits for cyber adversaries.

In order to evaluate the impacts of critical parameter errors on market operation, the relationships between critical parameters and market LMPs should be obtained. Such relationships are very complicated: they are discontinuous at points where the congestion pattern is changed. Therefore, it is very difficult, if not impossible, to derive this relationship in a closed-form. In order to find this relationship, numerical analysis is developed and exploited in this paper. This analysis is important, since not all critical parameters may significantly impact market operation, and only those with high impact need to be treated by additional measures. In this case, the worse-case analysis is applied: for a given system with its typical power flow profile, the greatest deviations of LMPs resulting from possibly undetectable errors are found for each critical parameter.

The steps for obtaining the relation between LMPs and errors in critical parameters, as well as identifying the critical parameters with high impacts on market operations, are summarized as below.

Step 1: for a given system, denote the set of bus numbers as N. The LMPs in the original case can be obtained by doing the following.

1) Set all the parameters at their original values, and form ISF matrix $\boldsymbol{\Psi}$ using (21).

2) Solve the ED problem (20).

3) Compute the LMPs for each node of the system using (22). Denote the LMP of bus j as LMP_j.

Step 2: form matrix $\boldsymbol{\Lambda}$ using (17).

Step 3: identify all the critical parameters by identifying the null columns of $\boldsymbol{\Lambda}$. Since the DC power flow model is applied in the market analysis, only reactance-type parameters need to be considered. Denote the critical parameter set as Υ.

Step 4: for each critical parameter, determine its plausible interval using the rules of thumb. A simple example is that line reactance cannot be negative. In addition, typical ranges of reactance per length for overhead transmission lines of a given voltage level are readily known, and based on the estimated lengths of the lines, the plausible interval for the reactance of each line can be determined. Denote the plausible interval of parameter p_i as $p_i=[p_i^{\min},p_i^{\max}]$.

Step 5: for each critical parameter p_i, do the following.

1) Select an increment Δp_i, such that $p_i^{\max}-p_i^{\min}=c\Delta p_i$ ($c\in\mathbb{N}$). Set parameter error step index $k=0$.

2) Set $p_i=p_i^{\min}+k\Delta p_i$, and form ISF matrix $\boldsymbol{\Psi}$ using (21).

3) Solve the ED problem (20).

4) Compute the LMPs for each bus of the system using (22). Denote the LMP of bus j as $LMP_j^{(i,k)}$.

5) Compute the deviation of the LMPs due to the parameter error: $\Delta LMP_j^{(i,k)}=LMP_j^{(i,k)}-LMP_j$.

6) Find the largest differences of LMP deviations between different nodes when $p_i=p_i^{\min}+k\Delta p_i$:

$$\Delta LMP^{(i,k)}=\max_{j\in\{1,2,\ldots,N\}}\left\{\Delta LMP_j^{(i,k)}\right\}-\min_{j\in\{1,2,\ldots,N\}}\left\{\Delta LMP_j^{(i,k)}\right\} \quad (25)$$

7) If $k<c$, set $k=k+1$, and go to 2); otherwise, find the largest difference of LMP deviations between different nodes induced by possible errors in critical parameter p_i:

$$\Delta LMP_{\max}^{(i)}=\max_{k\in[0,c]}\left\{\Delta LMP^{(i,k)}\right\} \quad (26)$$

8) Proceed to the next critical parameter in Υ.

Step 6: rank all the critical parameters in Υ according to $\Delta LMP_{\max}^{(i)}$, and the parameters corresponding to greater values are those with higher impact on the security of electricity market operation.

The whole procedure is illustrated in Fig. 1. In the above procedure, $\Delta LMP_{\max}^{(i)}$ is developed as an indicator of the impact of a critical parameter on electricity market, in that it represents the worst case which may be taken advantage of by adversaries. For example, if the false parameter value that corresponds to $\Delta LMP_{\max}^{(i)}$ is adopted in the model database, the maximum illegal revenue can be made by conducting a bilateral transaction or purchasing the financial transmission rights between the bus that has the most positive LMP deviation, which corresponds to the first term of the right-hand side of (25), and the bus that has the most negative LMP deviation, which corresponds to the second term of the right-hand side of (25).

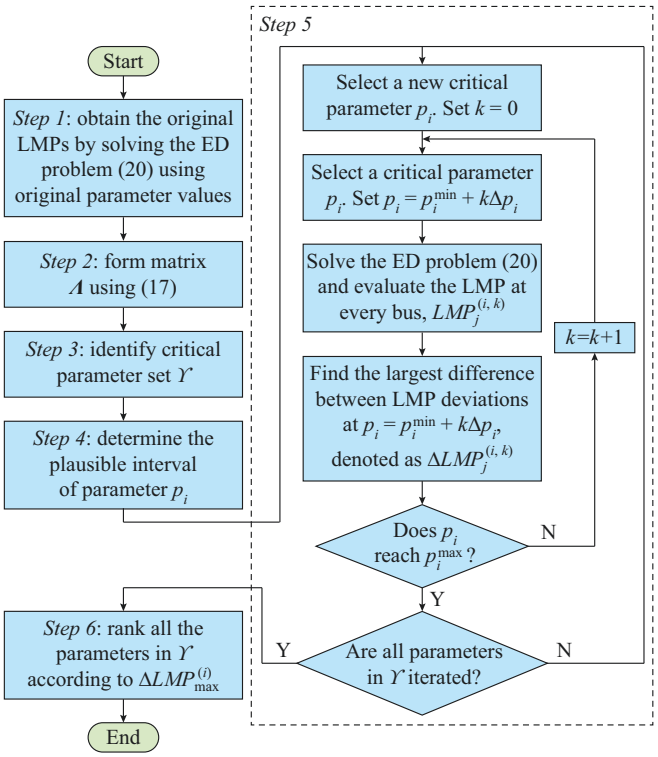

Fig. 1. Flow chart for identifying high-impact critical parameters.

It should be mentioned that the computational efficiency of the above procedure is not considered as a major factor limiting its implementation. The reasons are two-fold.

1) Searching for the high-impact critical parameters is not

a time-sensitive task. It is performed in the time scale of system planning (months), not in the time scale of system operation.

2) The determination of the impact of each individual parameter is completely independent, thus fully parallel or distributed computing architecture can be used if necessary. Specifically, *Step 5* of the procedure, which carries a vast majority of computational burden, can be performed fully in parallel for each critical parameter p_i.

Another concept related to critical parameters is the "critical *k*-tuples" of parameters. The definitions and properties of "critical *k*-tuples" are also given in [14]. They are a group of parameters whose errors can be detected, but cannot be effectively identified. In other words, their errors can be easily detected, but cannot be easily distinguished from one another. In the cyber security of system operation, critical *k*-tuples are less important than critical parameters, because once the errors are detected in a critical *k*-tuple, it is always possible to physically inspect each of the parameters in this tuple, and find out the true error source. For critical parameters, however, even the detection is impossible, which leads to the possibility of errors staying unnoticed permanently. Therefore, critical parameters are the focus of study in this paper.

Finally, it should be mentioned that the LMP deviations resulting from parameter errors will change with respect to load scenarios. However, as the principle of analysis remain unchanged, the security assessment framework presented above can be immediately extended to incorporate multiple load scenarios. For example, the system operator may pick the load curve of a typical day, and the index defined in (26) can be evaluated for each time interval of the day: $\Delta \boldsymbol{LMP}^{(i)}_{\max} = [\Delta LMP^{(i)}_{\max,1}, \Delta LMP^{(i)}_{\max,2}, \ldots, \Delta LMP^{(i)}_{\max,D}]^{\mathrm{T}}$, where D is the number of intervals. Finally, the comprehensive security risk index can be obtained by summing up all the entries of $\Delta \boldsymbol{LMP}^{(i)}_{\max}$, because when a permanent parameter error is introduced, the total distortion of market revenue of a day will be the sum of the distortion of the market revenues during each interval. If needed, the proposed security assessment procedure for critical parameters can also be extended to AC/DC power systems. The SE problem (2) and the ED problem (20) have to be replaced by their respective formulations incorporating DC components, which have been studied in detail in [22], [23] and [24], [25], respectively. Other than that, the proposed security assessment procedure remains effective.

Based on the above analysis, meter placement can be developed for converting the critical parameters which have potential great effects on the market to non-critical parameters, as will be discussed in the next section.

V. Types of Critical Parameters and Meter Placement Strategies

In order to develop methods for addressing the critical parameter issue, it is important to understand how they may occur in a network. Insights can be gained by looking at the expression of the Lagrange multipliers associated with parameter errors (11). For the i^{th} entry of $\boldsymbol{\lambda}$,

$$\lambda_i = -\sum_{j=1}^{m} \frac{1}{\sigma_j^2} H_{p,ji} r_j \tag{27}$$

where r_j and $H_{p,ji}$ are the elements of $\boldsymbol{r}$ and $\boldsymbol{H}_p$, respectively.

Actually, the Jacobian matrix $\boldsymbol{H}_p$ is a sparse matrix, and in its i^{th} column, only those entries corresponding to the measurements associated with the i^{th} parameter (i.e., the measurements which are functions of the i^{th} parameter) will be non-zero. Define this set of measurements as Γ_i, then (27) can be rewritten as:

$$\lambda_i = -\sum_{j \in \Gamma_i} \frac{1}{\sigma_j^2} H_{p,ji} r_j \tag{28}$$

Based on (28), it can be observed that two major categories of critical parameters exist. They will be referred to as "SE-relevant critical parameters" and "SE-irrelevant critical parameters".

A. SE-relevant Critical Parameters

In [14], the concept of critical parameters was first developed in analogy to the well-known concept of critical measurements in SE. A measurement is referred to as a critical measurement if its error is always undetectable. Due to the lack of redundancy, the residual of a critical measurement is identically zero. It has exclusive influence on the state estimate, since the state estimate always satisfies the equation of a critical measurement. Therefore, critical measurements are of great concerns in SE, in that their errors cannot be detected and will impact the SE solution.

Similar situations can be found for model parameters. Based on (28), the simplest and most common situation is when $\Gamma_i \neq \varnothing$, but all the measurements in Γ_i are critical measurements, as shown in (29), since the residuals of critical measurements are identically zero.

$$\lambda_i = -\sum_{j \in \Gamma_i} \frac{1}{\sigma_j^2} H_{p,ji} r_j \equiv -\sum_{j \in \Gamma_i} \frac{1}{\sigma_j^2} H_{p,ji} \cdot 0 = 0 \tag{29}$$

In this case, although this parameter is associated with some measurements, its Lagrange multiplier will be identically zero, hence its error cannot be detected. Meanwhile, since it still appears in measurement functions, the state estimate can be significantly biased by its error. Therefore, its properties are exactly analogous to the properties of a critical measurement. More complicated situations of this type appear when a parameter is associated with a critical pair (or more generally, a *k*-tuple) of measurements (the definitions can be found in [15]), whose residuals are not identically zero, but always satisfy the following condition:

$$\lambda_i = -\sum_{j \in \Gamma_i} \frac{1}{\sigma_j^2} H_{p,ji} r_j \equiv 0 \tag{30}$$

In this paper, the critical parameters which may affect the SE solution are defined as SE-relevant critical parameters.

Definition 1: for a critical parameter p_i, if $\Gamma_i \neq \varnothing$, this parameter is referred to as a SE-relevant critical parameter.

Remark 1: a SE-relevant critical parameter can be eliminated by turning at least one of the associated critical measurements into non-critical, or breaking at least one of the associated critical pair/*k*-tuple of measurements.

The rationale for Remark 1 is straightforward. If $z_j \in \Gamma_i$,

and it is converted into a non-critical measurement, $r_j \equiv 0$ doesn't hold; and since $H_{p,ji} \neq 0$, $\lambda_i \equiv 0$ doesn't hold any more, thus p_i becomes non-critical. A similar conclusion can be drawn for more complicated situations when a critical pair/*k*-tuple of measurements is broken and (30) no longer holds.

Obviously, based on the above analysis, the problem of removing SE-relevant critical parameters is converted into the problem of removing the criticality of the associated measurements. For the latter, meter placement approaches have been developed in literature. For example, the method described in [26] can be used which can provide the optimal meter placement strategy for this matter.

B. SE-irrelevant Critical Parameters

Based on (28), it can be observed that the other type of situations that can lead to critical parameters is the absence of associated measurements. Specifically, if $\Gamma_i = \varnothing$, then there will be no term on the right-hand side, thus (30) can be rewritten as:

$$\lambda_i = -\sum_{j \in \varnothing} \frac{1}{\sigma_j^2} H_{p,ji} r_j \equiv 0 \tag{31}$$

Consequently, any error in this parameter will be undetectable. When a model parameter does not appear in any of the measurement functions, it means that it is associated with an "irrelevant branch" [15] (except the parameters of a shunt device). A branch is called an irrelevant branch if its model does not appear in any measurement equations. The placement or removal of an irrelevant branch will not change the observability and SE formulation/solution of a network. An example of an irrelevant branch is given in Fig. 2. In this example, the system is observable with the measurements of real and reactive power injections at bus 1, real and reactive power flows along branch 1-2 and branch 1-3, and voltage magnitude at bus 1. Branch 2-3 is an irrelevant branch since it is not incident to any measurements. The removal of branch 2-3 does not change the observability of the system. Moreover, with a given set of values of the measurements, the removal of branch 2-3 does not change the state estimate as well.

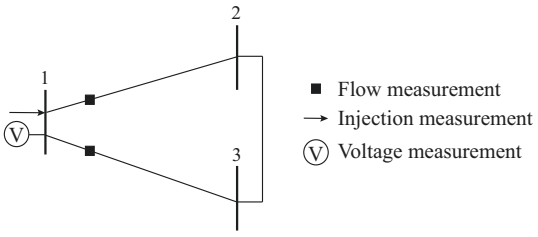

Fig. 2. An example of irrelevant branch (branch 2-3).

If a parameter is associated with an irrelevant branch, it is not of concern from the perspective of SE, since it does not have any impact on SE. However, it is still of concern in this paper, because other applications in power system operation may be impacted by this type of parameters. The electricity market is certainly one of them, since the ED solution is determined by the parameters of all branches, and parameters of irrelevant branches are apparently part of the vulnerability of the model database due to the fact that there is no capability of detecting and estimating their errors. In view of this, they are still broadly considered as one category of critical parameters in this paper, despite the fact that they are not exactly analogous to the concept of critical measurement.

Definition 2: for a critical parameter p_i, if $\Gamma_i = \varnothing$, this parameter is referred to as a SE-irrelevant critical parameter.

Remark 2: SE-irrelevant critical parameters can be eliminated by turning the corresponding irrelevant branch into a relevant one. If the system is observable, it can be done by placing a pair of real and reactive injection measurements at one of the terminal buses, or placing a pair of real and reactive flow measurements along this branch.

Clearly, either injection measurements at terminal buses or flow measurements along the branch contain the parameters of this branch in their measurement equations, so the set of associated measurements will no longer be empty for these parameters. Furthermore, given that the system is originally observable, the added measurements will not be critical, i.e., their removal will not lead to loss of observability of the system. Therefore, after they are added, the parameters of concern will not become SE-relevant critical parameters (see Definition 1). Consequently, they will become non-critical.

The analysis in Section IV and this section can be readily combined to form a systematic meter placement strategy for removing the security risks in electricity market operation imposed by critical model parameters. First, the critical parameters are identified, and their impacts on the LMPs can be obtained and ranked as described in Section IV. Then, if the budget is limited, meter placement is considered to remove critical parameters with impacts from high to low. They are classified as either SE-relevant or irrelevant, then additional meters can be placed as described in this section.

VI. Simulation Results

In this section, simulation cases on the IEEE 57-bus system will be presented. The objectives of this section are three-fold:

1) Verifying the concept that critical parameter errors may have a significant impact on the energy prices in electricity markets, thus becoming a potential security vulnerability for system operation.

2) Illustrating how the proposed security assessment can be implemented to evaluate the security risks imposed by each critical parameter, and prioritizing them for the investment of countermeasures.

3) Verifying that the proposed meter placement strategy is effective for transforming a critical parameter into a non-critical one, thus eliminating the security risk identified in this paper.

It should be noted that numerical results may vary with respect to the chosen test system or network topology, but it does not affect the verification and illustration of the proposed concept and method, or the general conclusions reached from the demonstrated results.

All simulations for SE and ED are performed in MATLAB 2018b. Dispatchable generators are assumed at buses 1, 2, 3, 6, 8, 9, 12, 23, and 37. In order to consider the ef-

fect of congestion patterns, branch flow limits are set such that the following 6 branches are congested in the correct network model: 4-3, 2-1, 3-15, 45-44, 15-1, and 38-37. There exist 41 pairs of power injection measurements, 61 pairs of power flow measurements, and 9 voltage measurements, yielding a measurement redundancy of 1.88. Applying the analysis of Sections IV and V, the critical parameters (reactance only) and their types are identified as shown in Table I. There are 13 critical parameters in the system, among which 9 are SE-relevant and 4 are SE-irrelevant.

TABLE I
CRITICAL PARAMETERS, THEIR TYPES AND IMPACTS ON LMPS

Critical parameter	Type	Largest difference between LMP deviations ($)	Ranking
$x_{34\text{-}32}$	SE-relevant	91.07	1
$x_{48\text{-}49}$	SE-irrelevant	85.12	2
$x_{45\text{-}44}$	SE-relevant	78.25	3
$x_{15\text{-}45}$	SE-irrelevant	71.57	4
$x_{31\text{-}32}$	SE-relevant	69.75	5
$x_{49\text{-}50}$	SE-irrelevant	30.86	6
$x_{48\text{-}38}$	SE-relevant	30.36	7
$x_{44\text{-}38}$	SE-relevant	19.53	8
$x_{13\text{-}9}$	SE-irrelevant	6.84	9
$x_{47\text{-}48}$	SE-relevant	0.81	10
$x_{30\text{-}31}$	SE-relevant	0.32	11
$x_{25\text{-}30}$	SE-relevant	0.13	12
$x_{33\text{-}32}$	SE-relevant	0.00	13

The impact of their errors on the LMPs can be found by following the steps given in Section IV. As an illustrative example, the results associated with the critical parameter (reactance) of branch 45-44, are shown in Figs. 3 and 4. It is assumed that errors of −80% through 100% of the original values cannot be detected using the rule of thumb, and in this interval, the LMP deviations from their original values with respect to the parameter error are plotted in Fig. 3. The thin solid curves in different colors show the LMP deviations of different buses, and the dashed curves in red show their envelopes.

Obviously, the LMPs at different buses have different responses to the parameter error. When the error is zero, the deviations of LMPs are all zero; as the error grows in the positive direction, deviations of LMPs first keep close to zero, then have a jump at 17% of the error. This is due to the change of the congestion pattern: the parameter error removes congestion on originally congested branch 45-44. In response to the change of the congestion pattern, some buses experience positive or negative LMP changes, and others stay almost unchanged. Beyond this point, LMPs change slightly as the error grows, but the changes are quite modest. No further jumps are observed which implies that the congestion pattern stays unchanged. LMP deviations are more complicated in the negative direction, but can be explained in a similar way. It is found that LMPs deviate most severely in the range of −30% to −37% parameter error. When the magnitude of the parameter error gets larger, another congestion pattern change occurs, which interestingly reduces the deviations of LMPs. It is evident from this example that the deviations of LMPs do not always grow proportional to the magnitude of the parameter error.

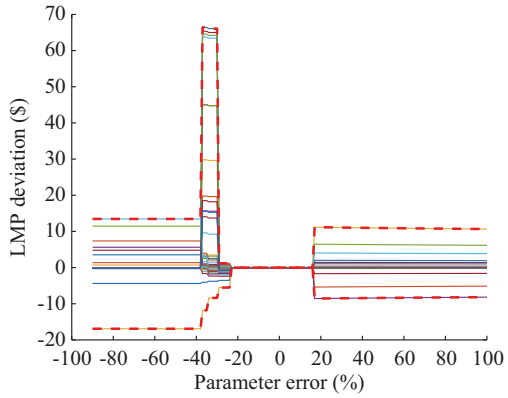

Fig. 3. LMP deviations of buses with respect to parameter error in $x_{45\text{-}44}$.

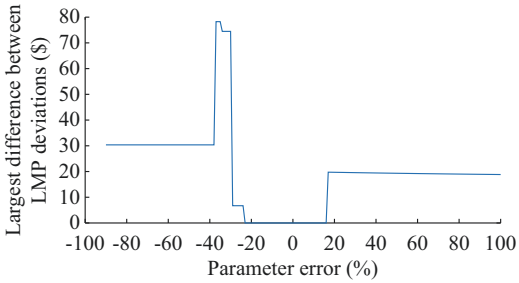

Fig. 4. Largest difference between LMP deviations of buses with respect to parameter error is $x_{45\text{-}44}$.

The largest difference between the deviations of LMPs of different buses is plotted against the magnitude of the parameter error in Fig. 4. It is the difference between the upper envelope and lower envelope of all the curves in Fig. 3. It implies the worst case: the largest bias of the revenue of conducting a bilateral transaction, or holding a point-to-point financial transmission right. This curve peaks at (−37%, $78.25). If the parameter error is injected by a cyber adversary, this point will actually correspond to the optimal strategy that the adversary may take: by injecting an error of −37% to this model parameter, and conducting a bilateral transaction from bus 36 (corresponding to the upper envelope in Fig. 3) to bus 45 (corresponding to the lower envelope in Fig. 3), or holding a financial transmission right from bus 45 to bus 36, the adversary will earn the largest illegal revenue per unit power, which is $78.25 per unit power.

A similar study can be repeated for each critical parameter, and their impacts on the electricity market can be ranked accordingly, as shown in Table I. It is seen that some critical parameters can lead to drastic distortion of LMPs, such as the reactance of branch 34-32, 48-49, 45-44, and so forth. It is also observed that some critical parameters have insignificant impact on the market. For example, the largest difference of the deviations of LMPs that can be incurred from an error of the reactance of branch 25-30 is $0.13, a negligible amount. This analysis provides useful information for prioritization of critical parameters for mitigation measures such

as meter placement.

Again, the reactance of branch 45-44 is used as an example to show the removal of criticality by placing additional measurements. Note that the real and reactive power flow measurements on branch 45-44 are the only measurements that are functions of this parameter and that are critical measurements. Therefore, this parameter is a SE-relevant critical parameter. By adding a pair of real and reactive power injection measurements at bus 45, the criticality of the power flow measurements on branch 45-44 is eliminated, i.e., they become redundant measurements. In this case, the reactance of branch 45-44 will become non-critical as well.

Monte Carlo simulations are conducted to demonstrate the detectability of errors in the reactance of branch 45-44 before and after power injection measurements are added at bus 45. The measurements are synthesized from power flow solution, and random Gaussian noise is intentionally added across the entire measurement set. The chi-square test and the LNLM test are carried out 100 times, and the frequency of successful error detection is evaluated for each test. The results before and after meter placement are shown in Fig. 5.

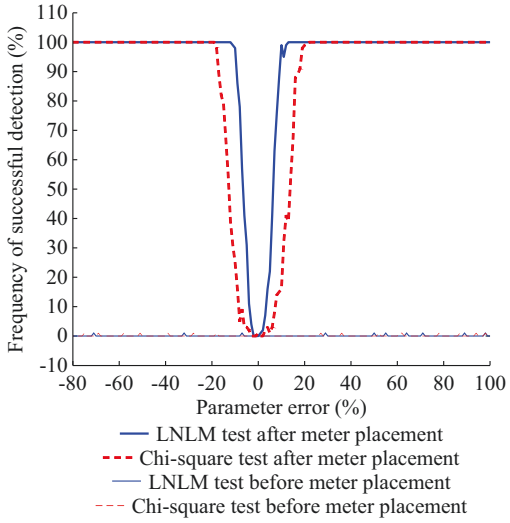

Fig. 5. Frequency of successful error detection before and after meter placement.

It is clear from Fig. 5 that before the injection measurements at bus 45 are placed, both the chi-square test and the LNLM test are unable to detect any error in the reactance of branch 45-44 when the error ranges from −80% to 100%. The frequency of successful error detection almost always stays at zero, with the occasional nonzero values resulting from false alarms created by measurement noise, not actual detection of the parameter error. This result verifies again that no matter how substantial the error of a critical parameter is, it is impossible to detect it. In contrast, it can be found that, after the placement of the injection measurements at bus 45, the error in this parameter becomes detectable, namely, it is no longer a critical parameter. In both the positive and negative directions, the frequency of successful detection for both tests grows with respect to the magnitude of the error, and reaches 100% (i.e., guaranteed detection) after a certain point. It is also seen that the LNLM test has a higher sensitivity than the chi-square test: when the magnitude of the error goes beyond −12% or 13% of the true value, the frequency of detection is 100%, while for the chi-square test, the detection cannot be guaranteed until the magnitude of the error goes beyond −20% or 22%.

In order to study the sensitivity of the LMP deviations to the loading condition, more simulations are conducted for the example of the reactance of branch 45-44. The load at one of the terminal buses of this branch, i. e., bus 44, is scaled to 80%, 100%, 120%, and 140% of the base-case load, and the procedure for evaluating the largest difference between LMP deviations with respect to the error in the reactance of branch 45-44 is repeated. The results under different loading conditions are comparatively shown in Fig. 6. The curves of 80%, 100%, and 120% loading conditions are quite similar. As the load increases, the peak of the curve moves to the right (from negative towards zero), indicating that the LMP deviations become more sensitive to the parameter error. At the same time, the peak of the curve also gets thinner, indicating that the large deviations occur within a narrower range. When the load increases to 140% of the base-case load, the shape of the curve significantly changes compared to the lighter loading condition, indicating that the congestion patterns experienced within the whole range of parameter error have changed. This study shows that in order to perform a comprehensive assessment on the impact of a critical parameter on electricity market operation, loading conditions for all intervals during the day should be considered. The procedure for incorporating multiple loading scenarios in the security assessment of critical parameters has been described in Section V.

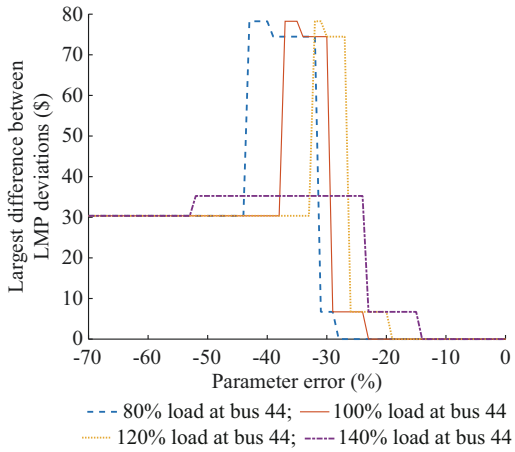

Fig. 6. Impact of loading condition on the largest difference between LMP deviations.

Finally, it should be emphasized again that both critical and non-critical parameters may have significant impacts on the evaluation of LMPs, and the discussion of this paper is focused on the critical parameters only because the errors cannot be effectively detected without implementing additional measures, thus imposing a security threat to system operation. The example discussed above can be used again to help clarify this point. In the original measurement configuration, due to the lack of local measurement redundancy,

the reactance of branch 45-44 is a critical measurement. It has a significant impact on the energy prices (as shown in Fig. 3), and its error cannot be detected (as shown by thin solid curves in Fig. 5). After the placement of power injection measurements at bus 45, this parameter becomes non-critical. Its error becomes detectable (as shown by thick dashed curves in Fig. 5), nevertheless, its presence has the same impact on the energy prices (as shown in Fig. 3). It is not considered as a security vulnerability only because the error can now be easily detected and corrected.

VII. Conclusion

This paper presents the formal linkage between the critical model parameter issue and the security of electricity market operation. It is shown that undetectable errors in critical parameters can significantly bias LMPs, regardless of whether they come from inadvertent mistakes or malicious attacks. A numerical method is developed to obtain the complicated and discontinuous relation between them, and identify the critical parameters which may severely influence electricity market operation. Subsequently, the properties of critical parameters are further studied, and meter placement strategies are discussed for different types of situations. Finally, case studies are performed in the IEEE 57-bus test system, verifying and illustrating the proposed analysis and design methods.

References

[1] A. L. Ott, "Experience with PJM market operation, system design, and implementation," *IEEE Transactions on Power Systems*, vol. 18, no. 2, pp. 528-534, May 2003.
[2] T. Zheng and E. Litvinov, "Ex post pricing in the co-optimized energy and reserve market," *IEEE Transactions on Power Systems*, vol. 21, no. 4, pp. 1528-1538, Nov. 2006.
[3] I. Feranadez. (2013, Apr.). Cybersecurity for industrial automation & control environments. [Online]. Available: http://www2.schneider electric. com/documents/support/white-papers/white-paper-cybersecurity-for-industrial-automation-control.pdf
[4] R. Deng, G. Xiao, R. Lu *et al*., "False data injection on state estimation in power systems – attacks, impacts, and defense: a survey," *IEEE Transactions on Industrial Informatics*, vol. 13, no. 2, pp. 411-423, Apr. 2017.
[5] Y. Song, X. Liu, Z. Li *et al*., "Intelligent data attacks against power systems using incomplete network information: a review," *Journal of Modern Power Systems and Clean Energy*, vol. 6, no. 4, pp. 630-641, Jul. 2018.
[6] G. Hug and J. A. Giampapa, "Vulnerability assessment of AC state estimation with respect to false data injection cyber-attacks," *IEEE Transactions on Smart Grid*, vol. 3, no. 3, pp. 1362-1370, Sept. 2012.
[7] M. Göl and A. Abur, "Identifying vulnerabilities of state estimators against cyber-attacks," in *Proceedings of 2013 IEEE Grenoble Conference*, Grenoble, France, Jun. 2013, pp. 1-4.
[8] M. Göl and A. Abur, "Effective measurement design for cyber security," in *Proceedings of 2014 Power Systems Computation Conference*, Wroclaw, Poland, Feb. 2014, pp. 1-8.
[9] N. Zivkovic and A. T. Saric, "Detection of false data injection attacks using unscented Kalman filter," *Journal of Modern Power Systems and Clean Energy*, vol. 6, no. 5, pp. 847-859, Sept. 2018.
[10] L. Xie, Y. Mo, and B. Sinopoli, "Integrity data attacks in power market operations," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 659-666, Dec. 2011.
[11] O. Kosut, L. Jia, R. J. Thomas *et al*., "Malicious data attacks on the smart grid," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 645-658, Dec. 2011.
[12] L. Jia, J. Kim, R. J. Thomas *et al*., "Impact of data quality on real-time locational marginal price," *IEEE Transactions on Power Systems*, vol. 29, no. 2, pp. 627-636, Mar. 2014.
[13] R. M. Lee, M. J. Assante, and T. Conway. (2016, Mar.). Analysis of the cyber attack on the Ukrainian power grid. [Online]. Available: https://www. nerc. com/pa/CI/ESISAC/Documents/EISAC_SANS_Ukraine_DUC_18Mar2016.pdf/
[14] Y. Lin and A. Abur, "A new framework for detection and identification of network parameter errors," *IEEE Transactions on Smart Grid*, vol. 9, no. 3, pp. 1698-1706, May 2018.
[15] A. Abur and A. Gómez-Expósito, *Power System State Estimation: Theory and Implementation*, New York: Marcel Dekker, 2004.
[16] J. Zhu and A. Abur, "Identification of network parameter errors," *IEEE Transactions on Power Systems*, vol. 21, no. 2, pp. 586-592, May 2006.
[17] Y. Lin and A. Abur, "Highly efficient implementation for parameter error identification method exploiting sparsity," *IEEE Transactions on Power Systems*, vol. 32, no.1, pp. 734-742, Jan. 2017.
[18] Y. Lin and A. Abur, "Enhancing network parameter error detection and correction via multiple measurement scans," *IEEE Transactions on Power Systems*, vol. 32, no. 3, pp. 2417-2425, May 2017.
[19] O. Alsac, N. Vempati, B. Stott *et al*., "Generalized state estimation," *IEEE Transactions on Power Systems*, vol. 13, no. 3, pp. 1069-1075. Aug. 1998.
[20] X. Bian, X. R. Li, H. Chen *et al*., "Joint estimation of state and parameter with synchrophasors – Part I: state tracking," *IEEE Transactions on Power Systems*, vol. 26, no. 3, pp. 1196-1208, Jul. 2011.
[21] X. Bian, X. R. Li, H. Chen *et al*., "Joint estimation of state and parameter with synchrophasors – Part II: parameter tracking," *IEEE Transactions on Power Systems*, vol. 26, no. 3, pp. 1209-1219, Jul. 2011.
[22] A. de la Villa-Jaen, E. Acha, and A. Gómez-Exposito, "Voltage source converter modeling for power system state estimation: STATCOM and VSC-HVDC," *IEEE Transactions on Power Systems*, vol. 23, no. 4, pp. 1552-1559, Nov. 2008.
[23] V. Donde, X. Feng, I. Segerqvist *et al*., "Distributed state estimation of hybrid AC/HVDC grids by network decomposition," *IEEE Transactions on Smart Grid*, vol. 7, no. 2, pp. 974-981, Mar. 2016.
[24] V. Sarkar and S. A. Khaparde, "Implementation of LMP-FTR mechanism in an AC-DC system," *IEEE Transactions on Power Systems*, vol. 23, no. 2, pp. 737-746, Apr. 2008.
[25] S. Chondrogiannis and M. P. Blanco, "Market integration scheme of a multi-terminal HVDC grid in the North Seas," *IEEE Transactions on Power Systems*, vol. 31, no. 3, pp. 2415-2422, Sept. 2016.
[26] F. H. Magnago and A. Abur, "A unified approach to robust meter placement against loss of measurements and branch outages," *IEEE Transactions on Power Systems*, vol. 15, no. 3, pp. 945-949, Aug. 2000.

Yuzhang Lin received the B.S. and M.S. degrees from Tsinghua University, Beijing, China, and the Ph.D. degree from Northeastern University, Boston, USA. He is currently an assistant professor in the Department of Electrical and Computer Engineering, University of Massachusetts, Lowell, USA. His research interests include modeling, monitoring, security, and data analysis of smart grids.

Ali Abur received the B.S. degree in electrical engineering from Orta Doğu Teknik Üniversitesi, Ankara, Turkey, and the M.S. and Ph.D. degrees from The Ohio State University, Columbus, USA. He is currently a professor at the Electrical and Computer Engineering Department, Northeastern University, Boston, USA. His current research interests include power system modeling and estimation, detection and location of faults in power grids with distributed energy sources.

Hanchen Xu received the B.Eng. and M.S. degrees in electrical engineering from Tsinghua University, Beijing, China, in 2012 and 2014, respectively. He obtained the M.S. degree in applied mathematics and the Ph.D. degree in electrical engineering from the University of Illinois at Urbana-Champaign, Urbana, USA, in 2017 and 2019, respectively. His current research interests include optimization, reinforcement learning, with applications to power systems and electricity market.