Identifying Security Vulnerabilities in Electricity Market Operations Induced by Weakly Detectable Network Parameter Errors

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

***Abstract*—In this work, a new security vulnerability in electricity market operations is identified. It involves certain parameters in the network model database whose errors, by nature, are difficult to detect and identify. These errors can either occur due to unintentional reasons or be maliciously introduced by cyber adversaries. It is shown that by impacting the injection shift factors (ISFs) and transmission line congestion patterns, these errors may exert biases on locational marginal prices (LMPs), and thus impact the revenues received by the holders of financial transmission rights (FTRs). A method is then developed for identifying the network parameters whose errors are difficult to detect and may have severe impacts on the LMPs and FTR revenues. Simulation results in the IEEE 57-bus system are presented to illustrate and verify the analysis and the proposed method. The proposed framework can be used to conduct cyber vulnerability assessment for power system model databases.**

***Index Terms*—cyber security, electricity market, financial transmission right, locational marginal price, parameter estimation, state estimation, anomaly detection**

I. Introduction

CONGESTION management is one of the most important objectives in the electricity market design and operation. A transmission line or a transformer is said to be congested if it operates at the limits imposed by security requirements. In the case of congestions, generators have to be re-dispatched in order to alleviate congestion at higher generation costs. In deregulated electricity markets, price signals are used to reflect the economic costs induced by congestions, and drive the operating point away from congested situations. In the U.S., the Federal Energy Regulatory Commission (FERC) has put forth standard market design (SMD) based on the concept of locational marginal price (LMP) [1]. In a bilateral transaction, for instance, if the transaction is contributing to the existing congestion, the portion of additional cost induced by this transaction will be reflected by the difference between the LMP at the point of delivery and the one at the point of receipt. This difference is usually referred to as the congestion charge associated with this transaction.

In day-ahead or real-time markets, the LMP at each node is computed by solving the economic dispatch (ED) problem. Before the market is cleared, the LMPs cannot be accurately projected by individual market participants, since they depend on global information of the network and bidding strategies of all parties. Therefore, market participants are always subject to the risk of high congestion charges raised by occurrence of unpredictable and severe congestions in the power grid. In order to hedge this risk, the independent system operator (ISO) or regional transmission organization (RTO) offers financial tools referred to as financial transmission rights (FTRs) [2] – [5]. They can be purchased in long-term, annual, or monthly auctions, with a specified amount of power and its path of transfer. At actual market clearing, the holders of FTRs will receive revenues if there is a difference of LMPs along the predetermined transfer path. Supposedly, they can be used to offer reimbursements for congestion charges that may occur.

In recent years, there is an increasing concern about cyber security issues in power system operations, and a growing trend of studying power systems as cyber-physical systems [6]. Along this line, a large volume of research has been dedicated to the so-called false data injection (FDI) attacks. The basic idea of FDI attacks is that if measurement data are accessed by cyber adversaries, and manipulated in such a way that the falsified values are conforming, the bad data detection function associated with state estimation (SE) may not be able to detect them. Typical methods for FDI attacks include the sparse attack model aiming to identify the minimum number of measurements to modify [7], the critical measurement attack model targeting the measurements whose errors are inherently undetectable [8], and the local attack model where the network information is only partially available [9]. In addition, a number of studies have been presented on analyzing the impacts of FDI attacks on the operation of electricity markets. Ref. [10] initiates the investigation along this line, while a countermeasure is proposed in [11], and the behaviors of cyber adversaries with partial information are studied in [12]. In general, successful FDI attacks require real-time and coordinated manipulation of a large number of measurements, thus its practicality in the real world is still an open question that requires further justification.

In this work, a new security vulnerability which may impact the operation of electricity markets is identified and investigated. It involves parameter errors in the network model

This work was supported in part by the ERC Program of the National Science Foundation under NSF Award EEC-1041877, and in part by the NSF Award No. 1947617.

database. It is known that the operation of electricity markets is heavily dependent on models. Errors in network model parameters can bias the congestion pattern and the relationship between the congestion and power injections, thus can significantly affect the evaluation of LMPs. Generally, parameter errors can be detected, identified, and corrected with methods developed based on SE. Classical methods for parameter error detection include residual-sensitivity-based methods [13] and augmented-state-estimation methods [14]. Recently developed Lagrange-multiplier-based methods significantly enhance the detection capability compared to the classical methods [15] – [16]. However, it has been shown more recently that even for the Lagrange-multiplier-based methods, there are vulnerable parameters in power network models whose errors are difficult to detect in a reliable manner [17] – [18]. The reasons leading to these weakly detectable errors may include weak network topology and measurement configuration, etc. If weakly detectable errors occur, they are likely to stay undetected and remain in the model database permanently, and will yield long-lasting negative impacts on the electricity markets as well as other applications. Compared to the extensively discussed FDI attacks which target measurement data, it may be more difficult to access model parameter dataset since it is stored at control centers. However, the following features regarding the cyber threat to model dataset make it worth special attention.

1. It does not require *coordinated* manipulation of a *large volume* of data. Weakly detectable errors are, by nature, difficult to detect, and thus do not have to be coordinated. The adversaries need to falsify only one or a small subset of parameters, which makes the attacks easier to implement.

2. It does not require intrusion and manipulation of data in *real time*. The change of a parameter can be done at any time, in an offline manner, and needs to be done only once. That makes it more practical and implementable compared to manipulating measurement data continuously in real time.

3. It can be implemented when cyber adversaries acquire database access privileges from internal personnel. Note that model parameters can be legitimately modified when logging into the database as internal personnel, while there is no normal means to modify measurement data. Therefore, for model parameters, it is very difficult to differentiate a malicious manipulation from a normal modification.

4. It exerts wider impacts on power system operations, including electricity markets. While typical FDI attacks can only affect *online* applications, network parameter errors can affect both *online and offline* applications. In terms of electricity markets, it can affect both the day-ahead market and the real-time market. Note that the vast majority of energy are traded in the day-ahead market.

Considering the factors mentioned above, the security vulnerabilities posed by weakly detectable model parameter errors cannot be neglected. However, existing work addressing the information security problem associated with power system model database is rather rare, presenting a significant research gap to fill. In this paper, the linkage between weakly detectable parameter errors and the operation of electricity markets will be explicitly studied. It follows our previous publication [19], where this topic was discussed for the first time in literature. While Ref. [19] only illustrates the concept that weakly detectable parameter errors can distort LMPs by simulating an error on a single transmission line, no systematic approach was developed for system-wide analysis. This paper, in contrast, provides a systematic approach for comprehensive vulnerability assessment of market operations in a large-scale system. The contributions of this paper are summarized as follows.

1. It draws attention to the information security problem associated with weakly detectable model parameter errors, and clarifies the linkage between weakly detectable parameter errors and secure operation of electricity markets.

2. It develops a framework for identifying the vulnerabilities of model database in electricity market operation. Specifically, the network parameters which may have weakly detectable errors that yield drastic biases of LMPs are identified, which paves the way for the development of effective defense measures.

3. Case study results explicitly demonstrate, for the first time, that maliciously injected model parameter errors can severely bias congestion patterns, LMPs, and FTR revenues in electricity markets.

II. Economic Dispatch, Locational Marginal Price, and Financial Transmission Rights

It is known that the electricity market is cleared by solving the ED problem. In studying the impacts of network parameter errors on the congestion patterns and FTR revenues, and power losses in the transmission network do not play an important role. Therefore, without significantly affecting the analysis in this paper, one can consider a simplified lossless ED model:

$$\begin{aligned} \min_{s} \quad & \sum_{j=1}^{N} c_j s_j \\ & \sum_{j=1}^{N} s_j = \sum_{j=1}^{N} d_j \\ \text{s.t.} \quad & f_l^{\min} \le \sum_{j=1}^{N} \Psi_{lj} \left(s_j - d_j \right) \le f_l^{\max} \quad l = 1,2,...,L \\ & s_j^{\min} \le s_j \le s_j^{\max} \quad j = 1,2,...,N \end{aligned} \tag{1}$$

where L is the number of branches, N is the number of buses, s_j is the power generation at bus j, d_j is the power consumption at bus j, c_j is the marginal generation cost at bus j, s_j^{min} is the lower limit of power generation at bus j, s_j^{max} is the upper limit of power generation at bus j, fl^{min} is the lower limit of power flow along branch l, fl^{max} is the upper limit of power flow along branch l, and Ψ_{lj} is the injection shift factor (ISF) from bus j to branch l. It represents the incremental change of the power flow along branch l induced by per unit change of the power injection at bus j. With the DC power flow model, which is consistent with the ED problem, the ISF matrix can be evaluated as:

$$\mathbf{\Psi} = \mathbf{B_f A B}^{-1} \tag{2}$$

where $\mathbf{B_f}$ is the imaginary part of the primitive admittance

matrix, **A** is the branch-bus incidence matrix, and **B** is the imaginary part of the admittance matrix. Ψ_{lj} is the entry at the *l*th row and *j*th column of **Ψ**.

At the solution point of (1), if a branch is found to be operating at its power limit, then this branch is defined as a congested branch.

The Lagrange multipliers associated with each inequality constraint can be obtained from the solution to (1), and the LMPs can be computed as follows [20] – [21]:

$$LMP_j = \xi^* + \sum_{l=1}^{L} \mu_l^{\min *} \Psi_{lj} - \sum_{l=1}^{L} \mu_l^{\max *} \Psi_{lj} \tag{3}$$

where LMP_j is the LMP at the *j*th node, ξ^* is the Lagrange multiplier associated with the power balance equation, $\mu_l^{\min *}$ and $\mu_l^{\max *}$ are the Lagrange multipliers associated with the inequality constraints regarding the lower and upper power flow limits of branch *l*, respectively. They are commonly known as the shadow prices associated with the congestion of branch *l*, which represent the incremental changes of generation costs with the change of the power flow limits f_l^{min} and f_l^{max}, respectively. Apparently, $\mu_l^{\min *}$ and $\mu_l^{\max *}$ are nonzero only when the corresponding inequality constraints are binding, i.e., the branch is congested at f_l^{min} or f_l^{max}. Therefore, if there is no congestion in the system and the power losses are ignored, every node in the system will have the same LMP as ξ^*. In the presence of congestions, the corresponding $\mu_l^{\min *}$ and $\mu_l^{\max *}$ will be nonzero, which leads to different LMPs at different nodes.

Congestions can sometimes make LMPs at certain nodes unexpectedly high, which can result in undesirable congestion charges for market participants. The FTRs are financial tools designed to hedge this risk. Consider a bilateral transaction defined as below:

$$\omega = \{i, j, q\} \tag{4}$$

where *i* and *j* are the bus indices of the point of receipt (where the power is injected) and the point of delivery (where the power is withdrawn), respectively, and *q* is the amount of power to be transferred. Apparently, the congestion charge associated with transaction ω is given by

$$\tau^{\omega} = \left(LMP_j - LMP_i\right) q \tag{5}$$

If the difference of LMPs between the point of delivery and the point of receipt is a large positive value, then the congestion charge is high. To avoid this risk, the FTR defined as below can be introduced:

$$\varphi = \{i, j, \gamma, \rho\} \tag{6}$$

where *i* and *j* are the bus indices of the point of receipt and point of delivery, respectively, γ is amount of power, and ρ is the per unit premium that the market participant pays for purchasing the FTR. When the market is actually cleared, if congestions actually occur, the holder of FTR φ will receive the revenue:

$$\upsilon^{\varphi} = \left(LMP_j - LMP_i\right) \gamma \tag{7}$$

and the profit of holding FTR φ will be the difference between revenue and the premium:

$$\delta^{\varphi} = \left(LMP_j - LMP_i - \rho\right) \gamma \tag{8}$$

It should be noted that although FTRs are designed such that their revenues can offset congestion charges, the holders will receive the revenues irrespective of whether they actually conduct any power transactions or not. The revenues of FTRs are exclusively determined by the difference between the clearing LMPs of the two nodes which are pre-decided as the "point of delivery" and "point of receipt" when the FTR is purchased.

Clearly, the network model plays a vital role in the aforementioned market applications. If the parameters of the network model contain errors, they will impact the ISFs which appear in (1) and (3), and hence the evaluation of LMPs and FTR revenues. Needless to say, it is important to keep an error free model parameter database. Yet, this is not trivial in practice. In the next section, methods developed for the detection and identification of network parameter errors will be reviewed.

III. State Estimation and Parameter Error Detection

State estimation is a powerful tool, which can not only provide reliable estimate of the operating state of power systems, but can also be used to calibrate meters and network models. The most straightforward idea is to augment the state vector and estimate the parameter of concern simultaneously with the state variables [14]. However, a major practical issue is the selection of parameters to be estimated. In a large-scale real-world system whose model contains thousands or even more parameters, it is generally difficult to obtain the set of suspect parameters to be estimated without loss of network observability. Therefore, methods are developed to first detect and identify erroneous parameters, and then include the identified ones in the augmented state vector for estimation. For the detection and identification of erroneous parameters, the largest normalized Lagrange multiplier (LNLM) test can be used [15] – [18]. For deriving this test, the WLS SE problem can be written as

$$\begin{aligned} \min_{\mathbf{x},\mathbf{p}} \quad & J = \frac{1}{2}\left(\mathbf{z} - \mathbf{h}\left(\mathbf{x},\mathbf{p}\right)\right)^T \mathbf{R}^{-1} \left(\mathbf{z} - \mathbf{h}\left(\mathbf{x},\mathbf{p}\right)\right) \\ \text{s.t.} \quad & \mathbf{p} = \mathbf{p_0} \end{aligned} \tag{9}$$

where **z** is the measurement vector that has *m* variables, **x** is the state vector that has *n* variables, **h** is the nonlinear function linking the state vector to the measurement vector, **R** is the covariance matrix of measurement errors, **p** is the network parameter vector, $\mathbf{p_0}$ is the stored parameter vector in the model database, and *J* is the objective function. After problem (9) is solved, the Lagrange multiplier vector associated with the equality constraints can be recovered by [18]:

$$\boldsymbol{\lambda} = -\mathbf{H}_{\mathbf{p}}^T \mathbf{R}^{-1} \mathbf{r} \tag{10}$$

where $\mathbf{H_p}$ is the Jacobian matrix $\partial\mathbf{h}/\partial\mathbf{p}$, and **r** is the residual vector defined by

$$\mathbf{r} = \mathbf{z} - \mathbf{h}\left(\mathbf{x}^*, \mathbf{p_0}\right) \tag{11}$$

It is well-known that in the absence of parameter errors, the residual vector is linked to the measurement error vector by [22]:

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

where the sensitivity matrix

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

where **H** is the Jacobian matrix $\partial\mathbf{h}/\partial\mathbf{x}$. With (10) and (12), it can be shown that if measurement errors follow Gaussian distributions with zero means and covariance matrix **R**, then the Lagrange multipliers will have Gaussian distributions with zero means and the following covariance matrix:

$$\mathbf{\Lambda}=\mathrm{cov}\left(\boldsymbol{\lambda}\right)=\mathbf{H}_\mathbf{p}^T\mathbf{R}^{-1}\mathbf{S}\mathbf{H}_\mathbf{p} \tag{14}$$

Thereby, the normalized Lagrange multiplier (NLM) for the *k*th parameter can be defined as [15], [18]:

$$\lambda_k^N=\frac{\lambda_k}{\sqrt{\Lambda_{kk}}} \tag{15}$$

In the absence of parameter errors, the NLM will have a standard normal distribution. With a specified probability of false alarm, the absolute value of the NLM can be checked against a threshold *t*, which satisfies

$$\Phi\left(t\right)=1-\alpha/2 \tag{16}$$

For any *k*, if one has $|\lambda_k^N| > t$, a parameter error can be inferred. In this case, the parameter which corresponds to the largest NLM will be identified as an erroneous parameter. The detailed proof of this identification criterion can be found in [18].

Subsequently, augmented state estimation approaches can be used to effectively estimate the identified erroneous parameter. After its value is corrected, the SE and LNLM test can be performed again to identify the next erroneous parameter.

IV. Weakly Detectable Errors and Their Impact on FTR Revenues

Despite the general effectiveness of the parameter error detection and identification methods, their capabilities are limited by many factors regarding the local characteristics of the system. It is recently shown in [18] that errors in certain parameters are inherently difficult to detect, even if their magnitudes are substantial. A brief quantitative analysis of this phenomenon is given below.

The relationship between the Lagrange multipliers and parameter errors are given as below [18]:

$$\boldsymbol{\lambda}=\mathbf{\Lambda}\mathbf{p}_\mathbf{e}-\mathbf{H}_\mathbf{p}^T\mathbf{R}^{-1}\mathbf{S}\mathbf{e} \tag{17}$$

where $\mathbf{p}_\mathbf{e}$ is the parameter error vector. Based on (17), it can be derived that in the absence and presence of a parameter error, the probability distribution of the NLM corresponding to the *k*th parameter in the network model will be given by

$$H_0:\quad \lambda_k^N\sim N\left(0,1\right) \tag{18}$$

$$H_1:\quad \lambda_k^N\sim N\left(\sqrt{\Lambda_{kk}}p_{e,k},1\right) \tag{19}$$

They are the null and alternative hypotheses of the LNLM test, respectively. Hence, in the presence of a parameter error $p_{e,k}$, the probability of missing this error can be evaluated by

$$\beta\left(p_{e,k}\right)=\Pr\left(\left|\lambda_k^N\right|\le t\right)\approx\Phi\left(t-\sqrt{\Lambda_{kk}}\left|p_{e,k}\right|\right) \tag{20}$$

With a given probability $0<\beta\ll 1$, a model parameter error $p_{e,k}$ is refer to as *β weakly detectable* the probability of detecting this error is less than *β*. The condition for a model parameter error $p_{e,k}$ to be *β weakly detectable* is given as follows:

$$\Lambda_{kk}\le\frac{t-\Phi^{-1}\left(\beta\right)}{p_{e,k}^2} \tag{21}$$

Obviously, Λ_{kk} has a small value, an error in the *k*th parameter of the network model is likely to be weakly detectable. Typical reasons for a small value of Λ_{kk} include weak network topology, sparse measurement configuration, low measurement accuracy class, and small value of the parameter [17] – [18].

If the error is introduced into the model database without being detected, electricity market operations can be affected. The errors of parameters will propagate into the ISFs as per (2), and impact the LMPs in the following three ways.

1. Congestion pattern. It can be observed from the inequality constraints associated with branch flow limits in (1) that when ISFs are changed, phantom congestions can be created on branches that are actually not congested, and vice versa. congestion pattern changes may cause abrupt changes of the dual variables $\mu_l^{\min*}$ or $\mu_l^{\max*}$ between zeros and finite numbers. As per (3), discontinuous changes of LMPs can be observed when parameter errors cause congestion pattern changes.

2. Congestion shadow price. Besides changes in the congestion patterns (i.e. the set of binding inequality constraints), the change of ISFs will also lead to continuous changes in the shape of the binding constraints, which will lead to continuous changes of the dual variables (shadow prices) $\mu_l^{\min*}$ or $\mu_l^{\max*}$ that are associated with the congested branches, thus leading to continuous changes of the LMPs.

3. Relationship between a branch congestion and a power injection. It can be noted from (3) that the additional terms induced by congestions are the products of the shadow prices ($\mu_l^{\min*}$ or $\mu_l^{\max*}$) and the ISFs. It implies that the LMP of a node is determined partly by the sensitivity of the power injection at this node to the power flows along the congested branches. Clearly, if the ISFs are biased, the contributions of the power injection at a node to the existing congestions will be distorted, which will affect the LMPs.

From the above analysis, it can be shown that the LMPs are nonlinear, discontinuous, and non-convex functions of network parameter errors. For a given weakly detectable parameter error $p_{e,k}$, the profit of FTR φ can be written as

$$\delta^\varphi\left(p_{e,k}\right)=\left(LMP_j\left(p_{e,k}\right)-LMP_i\left(p_{e,k}\right)-\rho\right)\gamma \tag{22}$$

Therefore, the illegal profit made by the FTR holder will be given by

$$\begin{aligned}\Delta\delta^\varphi\left(p_{e,k}\right)&=\delta^\varphi\left(p_{e,k}\right)-\delta^\varphi\left(0\right)\\&=\left(LMP_j\left(p_{e,k}\right)-LMP_j\left(0\right)\right)\gamma-\left(LMP_i\left(p_{e,k}\right)-LMP_i\left(0\right)\right)\gamma\end{aligned} \tag{23}$$

The greatest impact of errors in a given parameter can be evaluated by maximizing the product of the illegal profit and the probability of detection failure, which can also be referred to as the security risk imposed by this vulnerable parameter:

$$\max_{p_{e,k}}\quad\Delta\delta^\varphi\left(p_{e,k}\right)\cdot\beta\left(p_{e,k}\right) \tag{24}$$

The solution to problem (24) corresponds to the worst case faced by the system operators or defenders, or the optimal attack strategy of the cyber adversaries. This case may not be

actually encountered by the defenders or achieved by the attackers (since the attackers may not have complete information for the entire system), but it can be used to quantify the impacts an erroneous parameter can have on market operations.

Next, a systematic for identifying the security vulnerabilities studied above will be presented. The assumption is that cyber adversaries may seek to maximize their economic benefits by injecting weakly detectable parameter errors. From the system operators' point of view, as the impact of parameters on LMPs vary widely, only those which may have significant impact will be of concern. Since a closed form relationship between LMPs and network parameters isdifficult to derive, it is obtained by a numerical method instead. The procedure for vulnerability assessment is summarized below.

1) For a given system, denote the set of bus numbers as N. Obtain the LMPs in the error-free case by doing the following.

1.1) Set all the parameters at the original values stored in the model database, $\mathbf{p_0}$, and form ISF matrix $\mathbf{\Psi}$ using (2).

1.2) Solve the ED problem (1).

1.3) Compute the LMPs for each node of the system using (3). Denote the LMP of bus j as $\underline{LMP_j}$.

2) Form matrix $\mathbf{\Lambda}$ (i.e. the covariance matrix of Lagrange multipliers associated with parameter errors) using (14).

3) With specified tolerance of error $p_{e,crt} > 0$, and probability of missing errors, β_{crt}, identify all the vulnerable parameters by substituting $p_{e,k} = p_{e,crt}$ into (20), and search for parameters with $\beta > \beta_{crt}$. Denote the vulnerable parameter set as Υ:

$$\Upsilon = \left\{ p_k \middle| \Phi\left(t - \sqrt{\Lambda_{kk}}\, p_{crt}\right) > \beta_{crt} \right\} \tag{25}$$

4) For each vulnerable parameter, determine its plausible interval using a priori knowledge (a simple example being, line reactance cannot be negative). Denote the plausible interval of parameter p_k as $P_k = [p_k^{\min}, p_k^{\max}]$.

5) For each vulnerable parameter p_k, do the following:

5.1) Select an increment Δp_k, such that $p_k^{\max} - p_k^{\min} = c\Delta p_k$ ($c \in \mathbb{N}$). Set $d = 0$.

5.1) Set $p_k = p_k^{\min} + d\Delta p_k$, and form ISF matrix $\mathbf{\Psi}$ using (2).

5.2) Solve the ED problem (1).

5.3) Compute the LMPs for each bus of the system using (3). Denote the LMP of bus j as $\underline{LMP_j^{(k,d)}}$.

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

5.5) Find the largest difference of LMP deviations between different nodes when $p_k = p_k^{\min} + d\Delta p_i$:

$$\Delta\delta^{(k,d)} = \max_{j\in N}\left\{\Delta LMP_j^{(k,d)}\right\} - \min_{j\in N}\left\{\Delta LMP_j^{(k,d)}\right\} \tag{26}$$

and the transfer path (i.e. point of receipt and point of delivery) that yields the largest difference of LMP deviations:

$$\begin{aligned}\varsigma^{(k,d)} &= \left(a^{(k,d)}, b^{(k,d)}\right) \\ &= \left(\arg\min_{j\in N}\left\{\Delta LMP_j^{(k,d)}\right\}, \arg\max_{j\in N}\left\{\Delta LMP_j^{(k,d)}\right\}\right)\end{aligned} \tag{27}$$

5.6) Compute the probability of failure of parameter error detection, $\beta^{(k,d)}$, using (20).

5.7) Compute the expected value of the illegal profit that can be made by purchasing FTR along the transfer path $\varsigma^{(k,d)}$ at p_k:

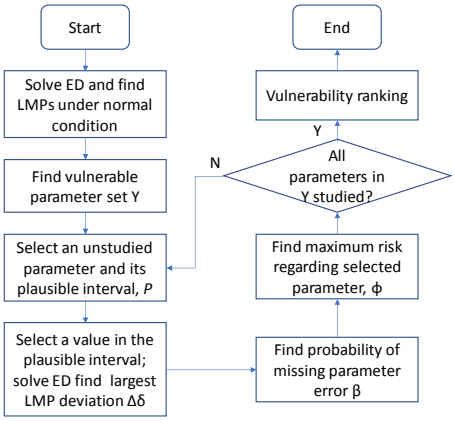

Figure 1. Flow Chart of the Proposed Algorithm for Searching Power System Model Database Vulnerabilities

$$\phi^{(k,d)} = \varsigma^{(k,d)} \cdot \beta^{(k,d)} \tag{28}$$

5.6) If $d < c$, set $d \leftarrow d+1$, and go to Step 5.2; otherwise, find the largest possible illegal profit that can be made by injecting errors into vulnerable parameter p_k:

$$\phi_{\max}^{(k)} = \max_{d\in[0,c]}\left\{\phi^{(k,d)}\right\} \tag{29}$$

Find the magnitude of parameter error that yields the largest possible illegal profit as follows:

$$d_k^{opt} = \arg\max_{d\in[0,c]}\left\{\phi^{(k,d)}\right\} \tag{30}$$

$$p_{e,k}^{opt} = p_k^{\min} + d_k^{opt}\Delta p_k - p_{0,k} \tag{31}$$

5.7) Proceed to the next vulnerable parameter in Υ.

6) Rank the all the vulnerable parameters in Υ according to $\phi_{\max}^{(k)}$, and the parameters corresponding to greater values are those with higher impacts on the security of electricity market operation.

The flow chart of the proposed algorithm is shown in Figure 1. The whole procedure can be automated to search for the vulnerabilities of any given power system model database.

Finally, several remarks will be made for the above analysis.

1. Although the computational burden of the above procedure can be substantial for large-scale systems, it is not considered as a major limiting factor for its implementation. The reasons are two folds. (1) The search of high-impact critical parameters is not a time-sensitive task. The proposed approach is not performed to detect cyber attacks in real time. Instead, it is performed in the planning stage, aiming to identify those model parameters which, once modified, are difficult to detect and bias LMPs seriously. These parameters will form a list of vulnerabilities for market operation, and ranked according to their impacts. This information will hopefully guide system operators to efficiently allocate their resources to develop protection measures for these parameters against potential cyber attacks. (2) The evaluations of the impacts of each individual parameters are completely independent from each other, thus fully parallel or distributed computing architecture can be used if needed. In practice, the identification algorithm can be conveniently performed every few weeks or months using the parallel or distributed computing resources in control centers.

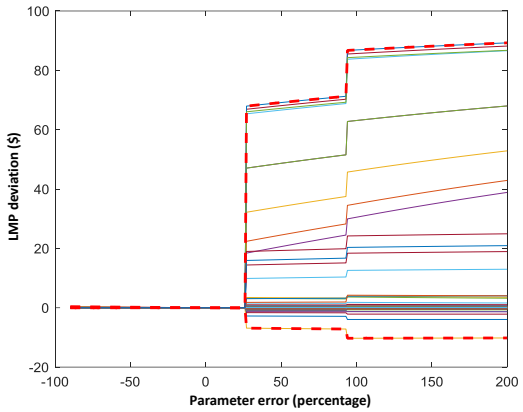

Figure 2. LMP deviations of buses with respect to error in $x_{24\text{-}25}$ (colored solid lines indicating different buses, and red dashed lines indicating the envelops)

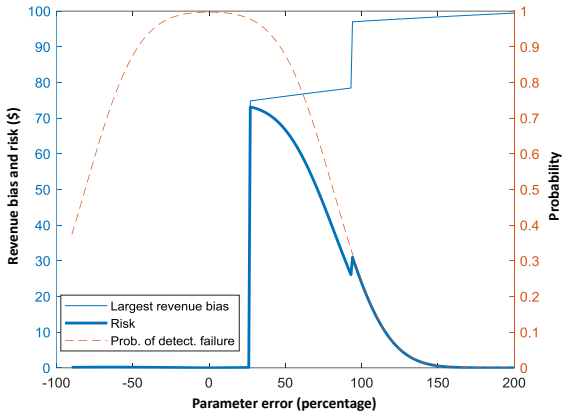

Figure 3. Largest difference between LMP deviations, probability of detection failure, and the security risk induced by error in $x_{24\text{-}25}$

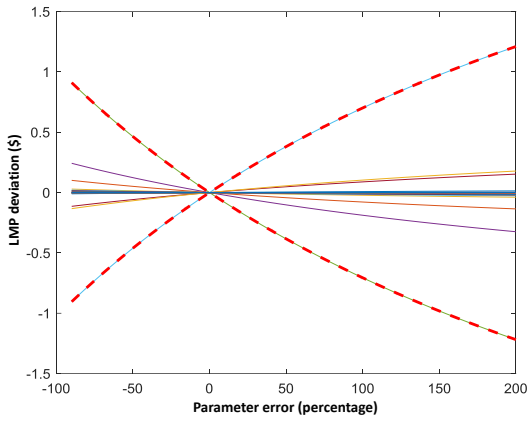

Figure 4. LMP deviations of buses with respect to error in $x_{19\text{-}20}$ (colored solid lines indicating different buses, and red dashed lines indicating the envelops)

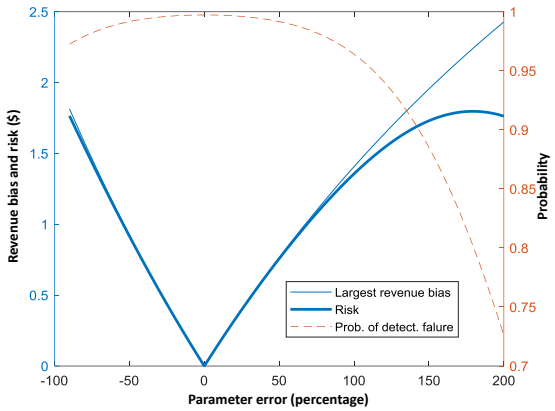

Figure 5. Largest difference between LMP deviations, probability of detection failure, and the security risk induced by error in $x_{19\text{-}20}$

2. Although the presented vulnerability assessment framework only handles one loading and topology scenario, it is readily extendable to incorporate multiple loading and topology scenarios. Since the total profit gained by the cyber adversaries is the sum of profits gained in each intervals, step 1 – 5 can be run for the typical loading and topology scenarios in each intervals of a day, then step 6 is carried out based on the sum of the maximum profits for all the intervals.

3. In the existing studies, the motivations of cyber attacks can be broadly classified into two categories: inflicting heavy damages to power systems [23] – [24], and gaining economic benefits without being detected [10] – [12]. The analysis presented in this paper focuses on the security threats with the second type of motivations. Discussions on security threats with the first type of motivations are out of the scope of this work.

4. While this paper focuses on the weakly detectable parameter errors, it is not the only information security vulnerability associated with power system model parameter databases. In a recent work [25], information security issues regarding another type of parameter errors, namely critical parameter errors, are revealed. A critical parameter error is an error that always remains undetectable irrespective of the magnitude of the error, i.e. the probability of error detection is identically zero; whereas a weakly detectable parameter error is an error that can be detected with a low but nonzero probability, and such probability is a function of the magnitude of the error. Obviously, the former is a more extreme case compared to the latter. In power system models, these two types of errors pertain to two different sets of parameters. In other words, the errors in some parameters are critical, and the errors in some parameters are weakly detectable. The vulnerability assessments for these two types of errors follow different paths, in that for critical parameter errors, the profit for cyber adversaries is deterministic (the probability of not being detected being 100%).

5. While the simplified lossless ED model (1) is presented in this paper, more realistic analysis can be readily conducted by replacing (1) with a more detailed market model with various economic and operational constraints incorporated. This does not affect the procedure and effectiveness of the proposed vulnerability analysis discussed in this section.

V. Case Studies

In this section, simulation results in the IEEE 57-bus test system will be presented to verify the proposed analysis and method. Dispatchable generators are assumed at buses 1, 2, 3, 6, 8, 9, 12, 23, and 37, and 6 branches set to be congested under the correct network model: branches 4-3, 2-1, 3-15, 45-44, 15-

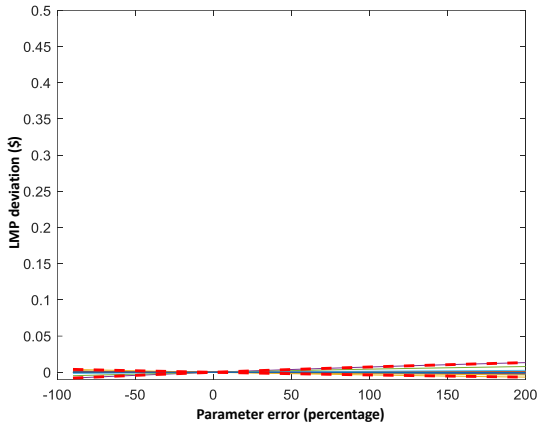

Figure 6. LMP deviations of buses with respect to error in $x_{52\text{-}53}$ (colored solid lines indicating different buses, and red dashed lines indicating the envelops)

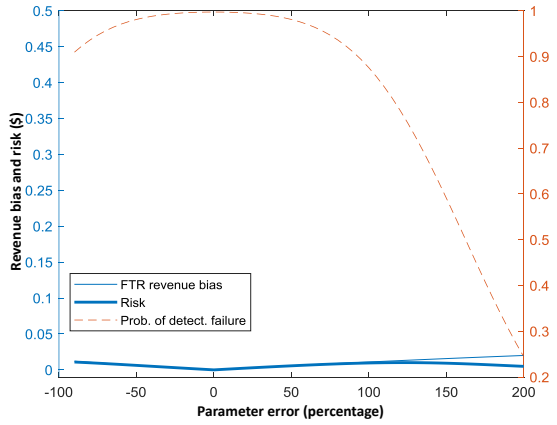

Figure 7. Largest difference between LMP deviations, probability of detection failure, and the security risk induced by error in $x_{52\text{-}53}$

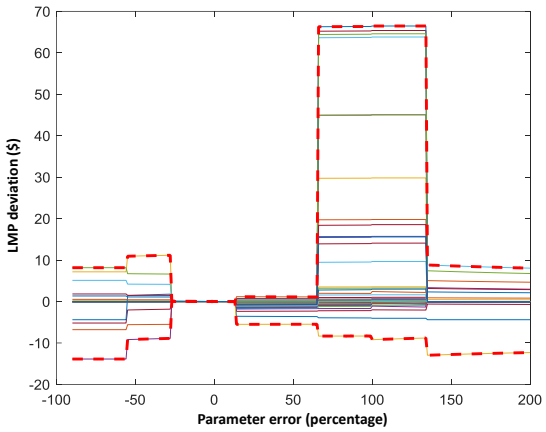

Figure 8. LMP deviations of buses with respect to error in $x_{15\text{-}13}$ (colored solid lines indicating different buses, and red dashed lines indicating the envelops)

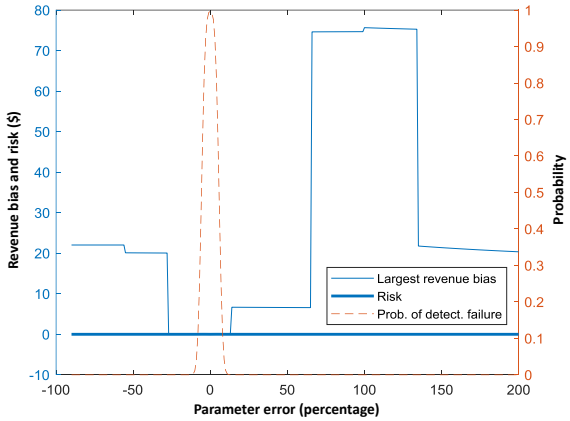

Figure 9. Largest difference between LMP deviations, probability of detection failure, and the security risk induced by error in $x_{15\text{-}13}$

1, and 38-37. There are 46 pairs of power injection measurements, 66 pairs of power flow measurements, and 21 voltage measurements, resulting in a measurement redundancy rate of 2.15. The standard deviations of measurement noise are uniformly set at 0.01 p.u. Using the method presented in section IV, the vulnerable parameters whose errors may not be reliably detected are identified, and their impacts on the LMPs and FTR revenues are investigated. Four types of scenarios will be presented and studied, followed by the presentation of results of the whole system. It should be noted that since there is no rival approach in the literature which is capable of addressing the issue discussed in this paper, no "baseline" approach can be provided for a comparative study.

A. Presence of Security Vulnerability: Weakly Detectable Errors and Biased Congestion Patterns

In the IEEE 57-bus system simulation case, the deviations of LMPs of all the buses from their true values with respect to the error in the reactance of branch 24-25 is plotted in Figure 2. Different thin colored lines represent the deviations of LMPs at different buses from their true values, and the thick red dashed lines show their envelopes. Obviously, when the parameter error is zero, the LMPs are identical to the true values, i.e. the deviations are zero. When the parameter error grows in the negative direction, the deviations remain almost zero. However, when it grows in the positive direction, two major jumps can be observed for the LMPs of many buses. They occur due to the fact that the parameter error changes the congestion pattern of the system. As has been discussed in section IV, parameter errors, when growing to a certain extent, can lead to phantom congestions for actually non-congested branches, and vice versa, and they will lead to discontinuous changes of LMPs. From Figure 2, it can be observed that for the same congestion pattern change, some LMPs change positively, and others change negatively. With a given magnitude of parameter error, if the buses corresponding to upper and lower envelops are defined as the point of delivery and point of receipt, respectively, then the FTR will make the greatest biased/illegal revenue. Therefore, the difference between the value of the upper envelop and that of the lower envelop (i.e. the largest difference between LMP deviations) can be used as an indicator for vulnerability assessment, as is exactly done in (26).

In order to effectively assess the risk induced by a parameter error, the probability that the error remains undetected also needs to be accounted for. In Figure 3, the largest difference between LMPs and the probability of detection failure are both

plotted. It can be found that when the magnitude of the error increases, the illegal revenue will increase, but the probability that the error is not detected will decrease. The product of these two variables will indicate the security risk, as is computed by (28), and shown by the thick blue line in Figure 3. The greatest risk is created at the first jump of the LMPs, which corresponds to a 27% error with respect to its true value. If the error is introduced by a malicious attack, this magnitude of error will correspond to the optimal strategy which yields the maximum expected value of illegal profit.

B. Presence of Security Vulnerability: Weakly Detectable Errors and Biased Shadow Prices and ISFs

The deviations of LMPs caused by the error in the reactance of branch 19-20 are plotted in Figure 4. Different from the first scenario, the changes of LMPs are continuous with respect to the parameter error. Clearly, the congestion pattern remains unchanged in the entire range of error plotted in Figure 4. Otherwise, jumping of LMPs would have been observed. The continuous changes of LMPs result from the impact of the parameter error on the Lagrange multipliers (shadow prices) associated with the actually congested branches, and the ISFs that they are multiplied by. In Figure 5, it can be found that when the error is 180% of the true value, the risk is maximized. It can be concluded from this example that even if parameter errors do not change the congestion pattern, they may still induce substantial biases in LMPs and FTR revenues by impacting the shadow prices and ISFs associated with congested branches.

C. Absence of Security Vulnerabilities: Weakly Detectable Errors with Negligible Impact on LMPs

Weakly detectable errors do not present security vulnerabilities for electricity markets, unless they have significant impacts on the LMPs. Figure 6 and 7 illustrate a scenario where the parameter error has a negligible impact on the LMPs. It involves the reactance of branch 52-53, whose variations neither changes the congestion pattern, nor affects the shadow prices or ISFs associated with the congested branches. It can be seen from Figure 7 that although within a wide range of magnitude there exists a substantial probability of detection failure, the risk it imposed on the market is rather small since the LMP deviations that the error induces are modest. This example verifies the argument that the errors which may significantly bias the LMPs need to be selectively identified and addressed.

D. Absence of Security Vulnerability: Reliably Detectable Errors

As a reference, the case of the reactance of branch 15-13 whose errors can be reliably detected, is presented. In Figure 8 and 9, it can be seen that erroneous values of this parameter can also lead to substantial biases of LMPs. However, from Figure 9, it can be found that the probability of detection failure drops drastically to almost zero as the magnitude of the error increases. The red dashed line in Figure 9 has a much thinner shape than those of Figure 3, 5, and 7. As a matter of fact, there is no overlapping area between the red dashed line (probability of detection failure) and the thin blue line (FTR revenue bias). Noting that the risk is the product of these two, it remains almost zero across the entire range of error magnitude.

E. Vulnerability Assessment Results for the System

Finally, the 15 parameters which present the greatest security vulnerabilities are listed in Table I. They are ranked according to the maximized risks, which are listed in column 2. Column 3 lists the magnitudes of errors that lead to the maximum risks, column 4 lists the corresponding FTR revenue biases, and column 5 lists the probabilities of detection failure. To mention once again, column 2 is evaluated as the product of column 4 and 5. The most remarkable fact observed in Table 1 is that the risks that errors in different parameters impose on the market vary widely. The risk presented by the first parameter, $x_{24\text{-}25}$, is 40 times greater than that presented by the last parameter, $x_{19\text{-}20}$. Again, this shows the significance of conducting a systematic vulnerability assessment. Although both $x_{24\text{-}25}$ and $x_{19\text{-}20}$ may contain errors that are weakly detectable, the possible consequences for electricity market operations are completely different. For per MWh of energy, error in $x_{24\text{-}25}$ can lead to the risk of \$73.13 revenue bias, which can completely overwhelm normal revenues under the error-free condition; whereas error in $x_{19\text{-}20}$ can lead to the risk of \$1.797 revenue bias only, which does not significantly disrupt normal market operations. With the information provided in TABLE I, it becomes obvious that more resources should be allocated to address the vulnerability associated with $x_{24\text{-}25}$. It provides useful guidance on systematic management of information security of power system model database.

VI. Conclusion

In this paper, security vulnerabilities of electricity markets created by weakly detectable errors of network model parameters are identified and investigated. Three paths along which weakly detectable parameter errors may bias LMPs and FTR revenues are explicitly discussed, and a numerical approach for quantitatively assessing the security risks imposed by weakly detectable parameter errors is developed. In the

TABLE I
Security Vulnerability Identification Results

Param.	Maximized Risk (\$)	Param. Relative Error	FTR Revenue Bias (\$)	Prob. of Detection Failure
$x_{24\text{-}25}$	73.13	27%	74.82	0.9774
$x_{36\text{-}37}$	72.4	-62%	73.22	0.9889
$x_{40\text{-}56}$	69.93	-9%	71.14	0.9830
$x_{34\text{-}32}$	69.82	-18%	71.48	0.9768
$x_{31\text{-}32}$	68.7	-43%	69.75	0.9848
$x_{38\text{-}37}$	50.42	28%	58.07	0.8621
$x_{45\text{-}44}$	36.31	-30%	74.47	0.4875
$x_{15\text{-}45}$	31.66	-37%	70.03	0.4521
$x_{39\text{-}57}$	24.67	37%	71.74	0.3439
$x_{44\text{-}38}$	18.09	69%	19.53	0.9262
$x_{41\text{-}43}$	12.07	124%	75.97	0.1588
$x_{49\text{-}50}$	5.667	-54%	30.86	0.1836
$x_{21\text{-}20}$	3.003	-90%	3.331	0.9015
$x_{22\text{-}38}$	2.339	200%	2.501	0.9350
$x_{19\text{-}20}$	1.797	180%	2.247	0.7998

simulation section, it is verified in the IEEE 57-bus test system that certain weakly detectable errors can induce drastic changes of LMPs, leading to potential benefits for cyber adversaries. Furthermore, four scenarios demonstrating various conditions which result in the presence or absence of security vulnerabilities are presented. It is observed that the errors which are difficult to detect may not necessarily induce significant biases of LMPs, and the errors which induce significant biases of LMPs may not necessarily be difficult to detect. Such observations demonstrate the need for developing a systematic approach for vulnerability assessment which quantitatively takes both factors into account, which is exactly the main goal and achievement of this paper. As the mechanisms of parameter errors inducing biases in congestion patterns, shadow prices, and ISFs are general, the phenomena observed in the IEEE 57-bus test system are representative for what may occur in other test systems and real-world utility systems, and the proposed vulnerability identification method will remain effective. The development of protection measures is being worked on and will be reported in a future publication.

REFERENCES

[1] Remedying Undue Discrimination through Open Access Transmission Service and Standard Electricity Market Design. Federal Energy Regulatory Commission. [Online]. Available: http://www.ferc.gov/

[2] PJM Manual 06: Financial Transmission Rights. PJM Interconnection. [Online]. http://www.pjm.com/-/media/documents/manuals/m06.ashx

[3] V. Sarkar and S. A. Khaparde, "A comprehensive assessment of the evolution of financial transmission rights", *IEEE Transaction on Power Systems*, vol. 23, no. 4, pp. 1783-1795, Nov 2008.

[4] Tao Li, M. Shahidehpour, "Risk-constrained FTR bidding strategy in transmission markets", *IEEE Transaction on Power Systems*, vol. 20, no. 2, pp. 1014-1021, May 2005.

[5] H. Ye, Y. Ge, M. Shahidehpour, and Z. Li, "Uncertainty marginal price, transmission reserve, and day-ahead market clearing with robust unit commitment", *IEEE Transaction on Power Systems*, vol 32, no. 3, 1782-1795, May 2017.

[6] S. Sridhar, A. Hahn and M. Govindarasu, "Cyber–physical system security for the electric power grid", *Proceedings of the IEEE*, vol. 100, no. 1, pp. 210-224, Jan 2012.

[7] M. Ozay, I. Esnaola, F. T. Yarman Vural, S. R. Kulkarni, and H. V. Poor, "Sparse attack construction and state estimation in the smart grid: Centralized and distributed models," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 7, pp. 1306–1318, 2013.

[8] M. Göl and A. Abur, "Identifying vulnerabilities of state estimators against cyber-attacks," 2013 IEEE Grenoble Conference, Grenoble, 2013, pp. 1-4.

[9] X. Liu, Z. Bao, D. Lu, and Z. Li, "Modeling of local false data injection attacks with reduced network information," *IEEE Transactions on Smart Grid*, vol. 6, no.4, pp. 1686-1696, Jul. 2015.

[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] J. Giraldo, A. Crdenas, N. Quijano, "Integrity attacks on real-time pricing in smart grids: impact and countermeasures," *IEEE Transactions on Smart Grid*, vol. 8, no. 5, pp. 2249-2257, Sep. 2017.

[12] M. R. Mengis and A. Tajer, "Data injection attacks on electricity markets by limited adversaries: worst-case robustness," *IEEE Transactions on Smart Grid*, vol. 9, no. 9, pp. 5710-5720, Nov. 2018.

[13] W. Liu and S. Lim, "Parameter error identification and estimation in power system state estimation," *IEEE Trans. Power Systems*, vol. 10, no. 1, pp. 200-209, Feb. 1995.

[14] O. Alsac, N. Vempati, B. Stott, and A. Monticelli, "Generalized state estimation," *IEEE Trans. Power Systems*, vol. 13, no. 3, pp. 1069-1075. Aug. 1998.

[15] J. Zhu and A. Abur, "Identification of network parameter errors", *IEEE Transactions on Power Systems*, vol. 21, no. 2, pp. 586-592, May 2006.

[16] 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.

[17] 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.

[18] 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.

[19] Y. Lin and A. Abur, "Identifying security vulnerabilities of weakly detectable network parameter errors in congestion revenue right markets", Allerton Conference on Communication, Control and Computing, University of Illinois at Urbana-Champaign, IL, USA, 2017.

[20] 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.

[21] F. Li, "Continuous locational marginal pricing (CLMP)," *IEEE Transactions on Power Systems*, vol. 22, no. 4, pp. 1638–1646, Nov. 2007.

[22] A. Abur and A. Gómez-Expósito, *Power System State Estimation: Theory and Implementation*, New York, NY: Marcel Dekker, 2004.

[23] S. Sridhar and M. Govindarasu, "Model-based attack detection and mitigation for automatic generation control," *IEEE Transactions on Smart Grid*, vol. 5, no. 2, pp. 580–591, Mar. 2014.

[24] A. Farraj, E. Hammad, A. A. Daoud, and D. Kundur, "Game-theoretic analysis of cyber switching attacks and mitigation in smart grid systems," *IEEE Transactions on Smart Grid*, vol. 7, no. 4, pp. 1846-1855, Jul. 2016.

[25] H. Xu, Y. Lin, X. Zhang and F. Wang, "Power System Parameter Attack for Financial Profits in Electricity Markets," *IEEE Transactions on Smart Grid*, DOI: 10.1109/TSG.2020.2977088. (early access)

Yuzhang Lin (Member, IEEE) received the B.S. and M.S. degrees from Tsinghua University, Beijing, China, respectively, and the Ph.D. degree from Northeastern University, Boston, MA, USA. He is currently an Assistant Professor with the Department of Electrical Computer Engineering, University of Massachusetts, Lowell, MA, USA. His research interests include modeling, monitoring, cyber-physical security, and data analysis of smart grids.

Ali Abur (F'03) received his B.S. in EE from Orta Dogu Teknik Universitesi, Turkey and his M.S. and Ph.D. from The Ohio State University. He is currently a Professor at the Electrical and Computer Engineering Department at Northeastern University, Boston, MA, USA.

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