




Market-Level Defense Against FDIA and a New LMP-Disguising Attack Strategy in Real-Time Market Operations

Qiwei Zhang , *Student Member, IEEE*, Fangxing Li , *Fellow, IEEE*, Hantao Cui , *Member, IEEE*, Rui Bo, *Senior Member, IEEE*, and Lingyu Ren, *Member, IEEE*

Abstract—Traditional cyberattack strategies on the electricity market only consider bypassing bad data detections. However, our analysis shows that experienced market operators can detect abnormal locational marginal prices (LMPs) under the traditional attack model during real-time (RT) operations, because such attack model ignores the characteristics of the LMP itself and leads to price spikes that can be an easy-to-detect signal of abnormality. A detection approach based on the concept of critical load level (CLL) is used to help operators identify risky periods when operators would be prone to overlooking abnormal LMPs. During safe periods, the abnormal LMPs are identified according to the operator's experience, while in risky CLL intervals, a N-x cyber contingency analysis is proposed to help independent system operators (ISOs) detect abnormal LMPs. Further, this paper constructs a new type of cyberattack strategy capable of not only bypassing bad data detection in the state estimation stage but also disguising the compromised LMPs as regular LMPs to avoid market operators' alerts in a realistic scenario wherein the attacker has imperfect information on system topology. Finally, the proposed analysis method and the attack strategy are evaluated through numerical studies on the PJM 5-bus system and the IEEE 118-bus system.

Index Terms—False data injection attack (FDIA), critical load level (CLL), LMP-disguising attack, electricity market, bad data detection.

I. INTRODUCTION

DEREGULATION has led to a competitive market model based on locational marginal prices (LMPs). Market participants bid and offer energy in a competitive pool using the two-settlement mechanism, the prevailing model for electricity

Manuscript received February 28, 2020; revised June 20, 2020 and August 15, 2020; accepted August 22, 2020. Date of publication September 1, 2020; date of current version February 19, 2021. This work was supported in part by the US Department of Energy (DOE) CEDS Project "Watching Grid Infrastructure Stealthily Through Proxies (WISP)" under Award DE-OE0000899 and in part by the CURENT which is a US NSF/DOE Engineering Research Center funded under NSF Award EEC-1041877. Paper no. TPWRS-00319-2020. (*Corresponding author: Fangxing Li.*)

Qiwei Zhang, Fangxing Li, and Hantao Cui are with the Min H. Kao Department of EECS, The University of Tennessee, Knoxville, TN 37996 USA (e-mail: qzhang41@vols.utk.edu; fli6@utk.edu; hcui7@utk.edu).

Rui Bo is with the Department of ECE, Missouri University of Science and Technology, Rolla, MO 65409 USA (e-mail: rbo@mst.edu).

Lingyu Ren is with the United Technologies Research Center, East Hartford, CT 06108 USA (e-mail: renlingyu@utrc.utc.com).

Color versions of one or more of the figures in this article are available online at <https://ieeexplore.ieee.org>.

Digital Object Identifier 10.1109/TPWRS.2020.3020870

market operation in the U.S [1]. Settlements are made separately at day-ahead (DA) and real-time (RT) markets. The DA market provides base generations, and the RT market offers adjustments according to real operation conditions [2]. Both the DA market and the RT market are cleared according to LMPs. RT LMPs are calculated based on state estimation results. Remote terminal units (RTUs) at substations are responsible for transmitting measurement data to the Supervisory Control and Data Acquisition (SCADA) system. A state estimator estimates the system states that are least deviated from measured quantities. Therefore, secure and efficient market operations rely highly on the integrity of the measured data.

Various cyberattack strategies have been proposed to compromise measurement data from RTUs. Carefully synthesized false data injection attacks (FDIAs) can easily alter state estimation results [3]. In [4], an attacker armed with system topology information is able to perform an FDIA without being detected. The attacker in [5] utilizes an FDIA to change the status of breakers, and thus a topology error is introduced into state estimation.

The financial risk is of equal significance to the catastrophic physical consequences of cyberattacks [6]. In particular, a malicious attacker can compromise line flow data to ensure the profitability of their market transactions [6]. In [7], a data integrity attack strategy is developed to maximize financial incentives. Similarly, in [8], bogus trades are combined with FDIAs to guarantee a profitable transaction in power market clearing. Beyond purely compromising analog measurement data, Ref. [9] presents an attack model on digital signals, performing a topology attack to disturb market operations. In [10], three new topology attacks on line connectivity are proposed to mislead market clearings. Ref. [11] constructs an attack scenario in which the transmission line rating is compromised to manipulate RT nodal prices. In [12], a FDIA strategy for very-short-term load forecasting is proposed to benefit certain players in the market operation. In [10], instead of working on a static economic dispatch, a new type of profitable FDIA is developed to manipulate generator ramping constraints.

Several countermeasures are also designed to detect FDIAs. In [15], phasor measurement units (PMUs) are assumed to be immune to FDIAs, and thus optimal placement of PMUs effectively defends against malicious data injection. In addition, [16] and [17] develop algorithms deploying those secure measurements economically and effectively in the system. Some defense

strategies also focus on enhancing bad data detection. In [18], a data history matrix is constructed to monitor the system state, and thus the FDIAs are identified. In [19] and [23], a geometrically designed residual filter and a generalized likelihood ratio test are developed to counter FDIAs. In [20], a dynamic state estimation method is proposed to eliminate potential cyberattacks. Ref. [21] further suggests strategically hiding part of the reactance information, which improves the reliability of bad data detection. In [22], a routing strategy and a data authentication method are proposed for RTU communications, improving the security of raw measurement.

Generally, the literature on electricity market cyberattacks can be broadly divided into two types: attack strategies and defense strategies. The former usually focus on developing profitable models, while the latter focuses on state estimation level defenses, such as the optimal placement of secure measurements or enhancing bad data detection. However, ignoring the characteristics of LMPs makes it easy for experienced market operators to detect abnormal price signals during RT market operation. To the best of our knowledge, no study has developed attack detection schemes at the market-level or attack strategies without alerting both bad data detection and market operators. This paper discusses the necessity of considering market-level behavior, such as price signals, in both intrusion and detection strategy development. In particular, this paper proposes a market-level defense scheme against traditional FDIAs (essentially based on bypassing bad data detection), and then formulates a new stealthy cyberattack strategy, the LMP-disguising attack, to bypass both bad data detection and market-level detection. The main contributions of this paper are twofold:

- 1) This work illustrates how traditional attack strategies can be easily detected through market signals and proposes a market-level cyberattack defense scheme: N-x cyber contingency analysis based on the risky intervals of critical load levels (CLLs) of the market LMPs.
- 2) A new type of stealthy profitable attack strategy, the LMP-disguising attack, is formulated. It not only bypasses bad data detection but also avoids producing an abnormal price signal.

The rest of this paper is organized as follows. Section II presents an overview of state estimation and electricity market models, as well as the concept of CLLs. In Section III, an example is presented in which a market operator can detect an attack from abnormal LMP step changes, and the details of a market-level attack defense scheme are described. In Section IV, we introduce a profitable LMP-disguising attack strategy which not only bypasses bad data detection but also lowers the possibility of detection by market operators. Section V presents the simulation results on the PJM 5-bus system and the IEEE 118-bus system. Finally, a conclusion is drawn in Section VI.

II. PRELIMINARIES AND CRITICAL LOAD LEVELS

A. State Estimation and Bad Data Detection

To accurately monitor the operating status of a power grid, a state estimator efficiently identifies operational constraints such as line flows or voltage magnitudes [25], [26].

The measurements of the studied power system are nonlinearly dependent on state variables, as characterized in (1)–(3) where z and x denote an m -dimension measurement vector and an n -dimension state vector. In a system of N buses, there are $2N-1$ state variables which exclude the voltage angle of the slack bus. Normally, the generation bus with the highest capacity is selected as the slack bus.

$$\bar{z} = h(\bar{x}) + \bar{e} \quad (1)$$

$$\bar{x} = (x_1, x_2, \dots, x_n)^T \quad (2)$$

$$\bar{z} = (z_1, z_2, \dots, z_m)^T \quad (3)$$

The methodology of this paper is built on AC state estimation providing a realistic application. The weighted least square estimator aims to identify the most likely states for a given set of measurements, as in (4) where R is the variance matrix for all measurements.

$$J(\bar{x}) = \min (\bar{z} - h(\bar{x}))^T R^{-1} (\bar{z} - h(\bar{x})) \quad (4)$$

Then, the minimum is obtained under the first-order optimality condition (5), where H_{es} is an $m \times n$ full rank matrix.

$$g(\bar{x}) = \frac{\partial J(\bar{x})}{\partial \bar{x}} = H_{es}^T R^{-1} (\bar{z} - h(\bar{x})) = 0 \quad (5)$$

With line flows and bus power injections as the typical measurements considered, H_{es} can be written as follows:

$$H_{es} = \begin{bmatrix} \frac{\partial P_{inj}}{\partial \theta} & \frac{\partial P_{inj}}{\partial V} \\ \frac{\partial P_{l-1}}{\partial \theta} & \frac{\partial P_{l-1}}{\partial V} \\ \frac{\partial Q_{inj}}{\partial \theta} & \frac{\partial Q_{inj}}{\partial V} \\ \frac{\partial Q_{l-1}}{\partial \theta} & \frac{\partial Q_{l-1}}{\partial V} \end{bmatrix} \quad (6)$$

Expanding (5) with the Taylor series provides an iterative method for solving the non-linear function $g(x)$. As shown in (7), the estimated x is updated at each iteration, until the norm of Δx is smaller than a pre-specified threshold. The last iteration gives the estimation of system state \hat{x} . Thus, the estimated measurement vector is given by $h(\hat{x})$. Also, $G(x)$ is the gain matrix obtained by (8), and (7) is solved with LU decomposition [25].

$$G(\bar{x}^k) \Delta x = H_{es}(\bar{x}^k)^T R^{-1} (\bar{z} - h(\bar{x}^k)) \quad (7)$$

$$G(\bar{x}^k) = H_{es}(\bar{x}^k)^T R^{-1} H_{es}(\bar{x}^k) \quad (8)$$

After the system states are estimated, the bad data detection is an essential function to identify random errors. Raw measurements are never perfect for various reasons, such as the limited accuracy of communication mediums. The largest normalized residual test is a prevailing method to find the abnormalities in a measurement set [27]. Residuals are the difference between the estimated measurement data and the raw measurement data, as in (9). Following [27], the residual vector can be represented by a sensitivity matrix S , as shown in (10).

$$\bar{r} = \bar{z} - h(\bar{x}) \quad (9)$$

$$S = I - H_{es}(\bar{x})G(\bar{x})^{-1}H_{es}(\bar{x})^T \quad (10)$$

Then, the normalized residual is formed in (11).

$$r_i^N = \frac{r_i}{\sqrt{S_{ii}R_{ii}}} \quad (11)$$

After the normalization, a threshold is assigned to detect the presence of outliers. The bad data detector alerts the operators when r_i^N is greater than the threshold as in (12), which is normally set to 3.0 for a 99.7% confidence level.

$$\|r_i^N\|_2 > \text{threshold}, \forall i \in M \quad (12)$$

B. Electricity Market Operations

The two settlement market mechanism (i.e. DA and RT markets) is widely adopted by U.S. ISOs [23]. An RT market is complementary to a DA market for correcting the deviation in DA generation dispatch [24]. There are two main approaches employed by ISOs to settle the market: ex-ante and ex-post. In the ex-ante model, both market prices and actual dispatches are solved in the same model, 10–15 min prior to the RT operation [28]. In the ex-post model (13)–(17), generation scheduling is solved from the ex-ante model, while the LMPs calculated after the spot market cycle by an incremental model [28].

$$\min \sum_i^{N_g} c_i(\Delta P_{gi}) - \sum_j^{N_d} d_j(\Delta P_{dj}) \quad (13)$$

$$\sum_i^{N_g} \Delta P_{gi} = \sum_j^{N_d} \Delta P_{dj} \quad (14)$$

$$\sigma P_{gi}^{\min} \leq \Delta P_{gi} \leq \sigma P_{gi}^{\max} \quad (15)$$

$$\sum_{k=1}^{N_b} GSF_{l-k}(\Delta P_{gk} - \Delta P_{dk}) \leq \sigma F_l^{\max}, \forall l \in L^+ \quad (16)$$

$$\sum_{k=1}^{N_b} GSF_{l-k}(\Delta P_{gk} - \Delta P_{dk}) \geq \sigma F_l^{\min}, \forall l \in L^- \quad (17)$$

Where ΔP_{gi} is the output of the incremental generators, ΔP_{dj} is the dispatchable load, and σ is a very small positive number. P_{gi}^{\max} and P_{gi}^{\min} are the upper and lower limits for the i th generator. GSF_{l-k} is the generation shift factor for the k th bus on the l th line, F_l^{\max} and F_l^{\min} are the upper and lower limits for the l th line.

Nodal prices are the combination of Lagrangian multipliers λ , τ_1 , and τ_2 which are associated with constraints (14), (16), and (17), as shown in (18). Further, the cost of the marginal loss term is set to zero in this study.

$$\lambda_k = (1 - LF_{W,i})\lambda - \sum_{l=1}^L GSF_{k-l}(\tau_1 - \tau_2), \forall k \in N_b \quad (18)$$

C. Critical Load Level

The LMPs experience a step-change when a new constraint becomes a binding constraint [29]. In the same vein, if an existing constraint is no longer binding, the LMPs also experience a step change. Otherwise, LMPs stay the same. A CLL is defined as a loading level in which LMPs experience a step change, and a

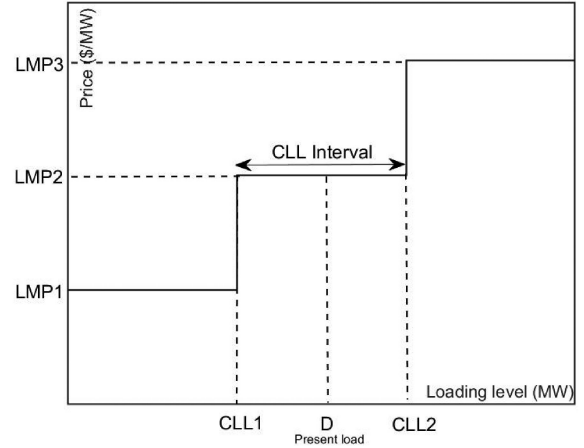


Fig. 1. Critical load level.

CLL interval is the distance between two CLLs [30], [31]. While in practice, many factors may affect the LMP curves w.r.t. to total system load, analysis of the 3-month prices obtained from published data at an ISO demonstrates the CLL or step-change pattern [29].

As shown in Fig. 1, when the load varies between $CLL1$ and $CLL2$, the LMP is equal to $LMP2$. When load D reaches $CLL2$, $LMP2$ jumps to $LMP3$ due to a new binding constraint.

The calculation of the next CLL is proposed in [30]. The load growths are fulfilled by present marginal units. Therefore, if there is a small load variation (without a change in binding constraints), the mathematical relationship between total load variation ΔD_Ω and the i th marginal unit incremental generation ΔMG_i is shown in (19)–(20), where f_i is the percentage of the i th bus incremental load compared to ΔD_Ω .

$$\sum_{i=1}^{N_{MG}} \left(\frac{\Delta MG_i}{\Delta D_\Omega} \right) = 1.0 \quad (19)$$

$$\sum_{i=1}^{N_{MG}} (GSF_{k-i} \Delta MG_i) = \sum_{i=1}^N (GSF_{k-i} f_i) \Delta D_\Omega \quad (20)$$

By solving (19)–(20), (21) is obtained. The linear equation is always solvable because the number of marginal units is equal to the number of congested lines plus one.

$$\frac{\Delta MG_i}{\Delta D_\Omega} = \pi_i \quad (21)$$

If a line limit is the next binding constraint, the distance to the next CLL is calculated by (22). It shows that the impact from the incremental load and generation is equal to the difference from the line limits and original uncongested line flow. For all uncongested lines, ∂D_Ω is calculated, and the lowest one is the allowed load growth.

$$\Delta D_\Omega = \frac{\lim it_l - \sum_{i=1}^{N_b} GSF_{k-i}(P_{gi} - P_{di})}{\sum_{i=1}^{N_{MG}} (GSF_{k-i} \pi_i) - \sum_{i=1}^N (GSF_{k-i} f_i)} \quad (22)$$

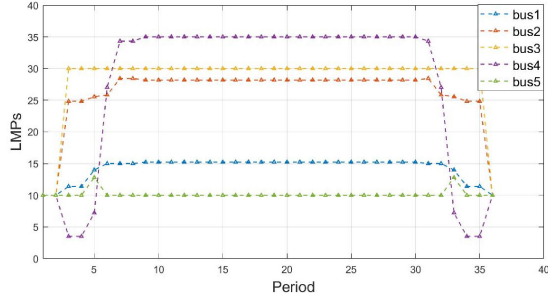


Fig. 2. LMP for the PJM 5-bus system without attack.

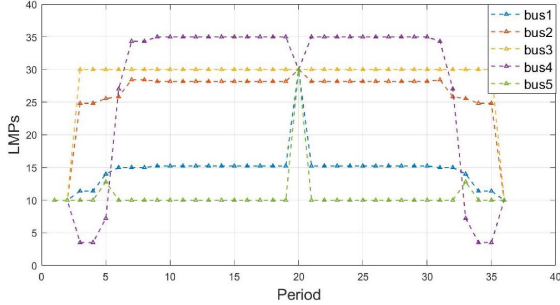


Fig. 3. LMP for the PJM 5-bus system with attack.

Similarly, if a generation limit is the next binding constraint, the distance to the next CLL is calculated by (23).

$$\Delta D_{\Omega} = \frac{\Delta MG_i}{\pi_i} = \begin{cases} \frac{\Delta MG_i^{\max} - \Delta MG_i}{\pi_i}, & \text{if } \pi_i > 0 \\ \frac{\Delta MG_i^{\min} - \Delta MG_i}{\pi_i}, & \text{if } \pi_i < 0 \end{cases} \quad (23)$$

III. ABNORMAL LMP DETECTION BASED ON RISKY CLL INTERVALS

Traditional attack strategies only consider bypassing bad data detections [6]–[14]. However, a careless attack leads LMPs to experience unusual step changes.

In this section, we first show how operators can easily detect traditional attack strategies based on their experiences when LMPs change smoothly over continuous periods. Then, an N-x cyber contingency analysis is introduced as a countermeasure to help operators identify abnormal LMP sets even when LMPs change frequently.

A. Abnormal LMP Step Changes

Fig. 2 shows a PJM 5-bus system's LMPs during a normal operating day with 40-minute clearing intervals. LMPs are the same during periods 10–30, namely the load level stays in the same CLL interval. An attacker performs an FDIA at period 20, which changes the congested line to uncongested, and the resulting LMPs are shown in Fig. 3. This attack adds two originally non-existent step changes at period 19 and period 21.

According to the operators' experience, the congestion pattern at period 20 should be consistent with previous periods because the current loading level is in the same CLL interval as previous periods. In addition, operators may compare the ex-post congestion pattern with the ex-ante congestion pattern. Although the

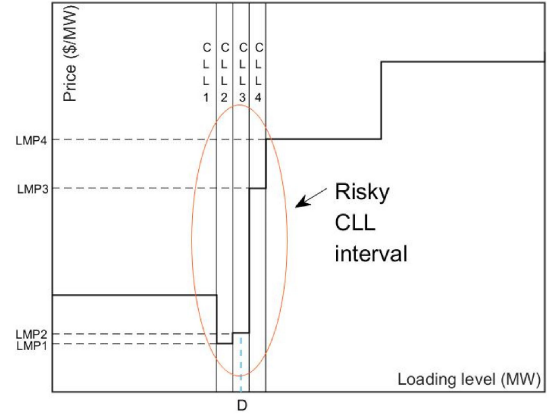


Fig. 4. Illustration of risky CLL intervals.

load varies between ex-ante and ex-post, when the current CLL interval is large, small load variation is not enough to change LMPs.

In summary, an attack vector easily induces abnormal LMP step changes without the consideration of the behavior of the resulting LMPs.

Therefore, bypassing only bad data detection is not enough to construct a stealthy attack strategy. A stealthy attack should also avoid alerting market operators.

When the LMPs change more frequently, operators may overlook abnormal LMP sets. Therefore, we introduce CLLs to identify those risky periods, and then a cyber contingency analysis is proposed to help the operator detect abnormal LMPs at each risky period.

B. Risky CLL Interval in Market Operation

When LMPs change frequently, operators are insensitive to LMP step changes. If the CLL interval is relatively narrow, a small variation leads to step changes. When the current load lies in those CLL intervals, this period is considered a risky period.

As shown in Fig. 4, when the current loading level is D , a small load variation may result in LMPs staying at $LMP2$ or changing to $LMP1$, $LMP3$, or $LMP4$.

Risky CLL intervals need to be calculated to determine the risky period. To do so, we first find a minimum possible load which is obtained by load forecasting. Then, based on this minimum possible load, repeating calculating equations (22) and (23) gives all CLLs for the system. Then the average distance between each CLL, Dis_{ave} , is calculated by (24), where N_{cll} is the number of CLLs, D_{max} is the largest CLL, and D_{min} is the smallest CLL.

$$Dis_{ave} = \frac{D_{max} - D_{min}}{N_{cll} - 1} \quad (24)$$

The distance of the i th CLL interval, Dis_i , is obtained (25).

$$Dis_i = CLL_{i+1} - CLL_i, \forall i \in N_{cll} - 1 \quad (25)$$

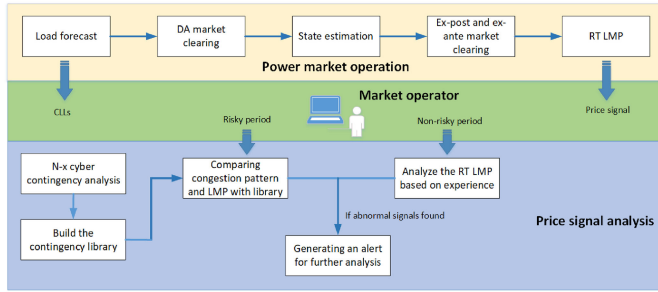


Fig. 5. Detection procedures.

A risky index r_i is proposed to represent the percentage of the i th CLL interval compared with average distance as in (26).

$$r_i = \frac{Dis_i}{Dis_{ave}}, \forall i \in N_{cll} - 1 \quad (26)$$

If the length of a CLL interval is lower than threshold α , then the CLL interval is identified as a risky CLL interval, as in (27). The corresponding risky periods are also identified as in (28). Other CLL intervals and periods are classified as safe intervals and safe periods.

$$CLL_{risky} = \{CLL_i, \forall r_i < \alpha \forall i \in N_{cll}\} \quad (27)$$

$$T_{risky} = \{t, \forall Load_t \in CLL_{risky}\} \quad (28)$$

Different operators' experiences are different. For experienced operators, a few more step changes do not affect their judgments. However, even when LMPs are smooth, novice operators may lack confidence. Using this observation, the more confident an operator is, the higher the threshold α is.

C. N-x Cyber Contingency Analysis

Intuitively, screening all load levels is preferred. However, a full set of different combinations is computationally expensive. Thus, Section III-B provides a way to differentiate safe periods from risky periods. At safe periods, operators can confidently rely on their experience to detect abnormal LMPs. At those risky periods, an N-x cyber contingency analysis is proposed to help identify abnormal LMPs. Similar to N-x contingency analysis, which takes every line out and runs a power flow simulation, the N-x cyber contingency analysis solves the market-clearing model repeatedly with each possible combination of potential cyberattack target lines, which are assumed to be uncongested at all risky CLL intervals, as shown in Algorithm BC. Throughout the paper, load distribution factors are assumed constant as conforming loads, while fixed non-conforming loads can be taken out as constant negative base generation. This is reasonable during the short term, and Algorithm BC may be re-performed in the case that load distribution factors change significantly over the long term.

In Algorithm BC, x determines how many lines can possibly be compromised depending on the vulnerability of the system. The compromise of a line means the congestion pattern of this line is altered. The total number of possible combinations N_c is

Algorithm: BC Function Build_Contingency (Risky CLLs, x).

Input All risky CLLs

Output Contingency library

```

1   For each risky CLL do
2       Solve the market-clearing model (11) -
3           (15)
4       For each possible combination do
5           Record target lines in this combination
6           For each target line  $i$  do
7               Remove  $i$ th line flow limit
8           End for
9           Solve the market-clearing model
10              (11)–(15)
11          Record CLLs, congestion patterns,
12          and LMPs
13          Add the recorded value to the library
14      End for
15  End for
16  Return the library
    
```

given by (29) where C is the combination calculator.

$$N_c = \sum_{w=1}^x C_L^w \quad (29)$$

The results of the analysis are stored in a contingency library. The library contains risky CLLs, original LMPs, the original congestion pattern, possible combinations, and the possible resulting LMP at each combination. It is worth noting that there are not many possible target lines in any given system. For a large system, such as ISO New England, the average binding transmission constraints in January 2020, their winter peak month, consisted of 142 branches [33], while the entire system has 2771 branches. Market operators can further narrow down target lines based on recent building constraint experiences.

Overall detection procedures are described in Fig. 5. Before the DA market, the load profile is estimated by load forecasting. All CLLs are calculated based on the minimum possible load. After identifying risky CLL intervals, the contingency library is built by Algorithm BC. Then, in RT market operations, operators determine if the current period is a risky period or a safe period via the obtained risky CLL intervals. If it is a safe period, then the operator checks the LMPs by experience. Otherwise, the operator compares the current congestion pattern, load level, and LMPs with their counterparts in the library to find the abnormalities. If abnormalities exist, a cyber alert is generated for further diagnosis. For example, the market operator can call the system operator to check if the suspect lines (from the library) are actually congested.

IV. LMP-DISGUIISING ATTACK

In this section, we propose an LMP-disguising attack strategy that not only bypasses bad data detection but is also able to

disguise the compromised LMPs as normal LMPs. The assumptions of the proposed attack are described in *Part A*. *Part B* and *Part C* present how the proposed attack is stealthy at the state estimation level and at the market-level, respectively. The profitability of the LMP-disguising attack is shown in *Part D*. The overall attack model is constructed in *Part E*.

A. Limited Adversary

In real market operations, system topology data is relatively secure from adversaries because the grid information is simply too extensive and volatile [14]. In this paper, a limited adversary who has imperfect information about grid topology is assumed. Therefore, the real grid admittance model is approximated by attackers as in (30). The first term is the admittance matrix estimated by attackers. The second term, Δy , is the mismatch between the actual model and the one assumed by attackers. In this model, the mismatch Δy is assumed to be independent and follows a Gaussian distribution.

$$Y^{act} = \begin{bmatrix} Y_{11} & \dots & Y_{1n} \\ Y_{n1} & \dots & Y_{nn} \end{bmatrix} + \begin{bmatrix} \Delta y_{11} & \dots & \Delta y_{1n} \\ \Delta y_{n1} & \dots & \Delta y_{nn} \end{bmatrix} \quad (30)$$

Then, the measurement Jacobian matrix H_{es} is no longer deterministic. The elements corresponding to real power injection are shown in (31)–(34) in which g^{new} and b^{new} are the real and imaginary parts of the elements in admittance matrix Y^{act} .

$$\frac{\partial P_{inj}}{\partial \theta_i} = \sum_{j=1, j \neq i}^N V_i V_j ((b_{ij}^{new} \cos \theta_{ij} - g_{ij}^{new} \sin \theta_{ij})) \quad (31)$$

$$\frac{\partial P_{inj}}{\partial \theta_j} = V_i V_j ((g_{ij}^{new} \sin \theta_{ij} - b_{ij}^{new} \cos \theta_{ij})) \quad (32)$$

$$\frac{\partial P_{inj}}{\partial V_i} = \sum_{j=1, j \neq i}^N V_j (b_{ij}^{new} \sin \theta_{ij} + g_{ij}^{new} \cos \theta_{ij}) \quad (33)$$

$$\frac{\partial P_{inj}}{\partial V_j} = V_i (b_{ij}^{new} \sin \theta_{ij} + g_{ij}^{new} \cos \theta_{ij}) \quad (34)$$

The expression for the remaining elements can be formed in a similar way. Those elements form the attackers' Jacobian matrix H_{es}^{act} which approximates the actual Jacobian matrix H_{es} . This assumption provides a more realistic application setting for the proposed attack. Without a careful selection, the attack vector stands a high possibility of failing to pass bad data detection using the imperfect topology matrix. Further, the uncertainty in the H_{es}^{act} matrix inevitably affects the effectiveness of the attack strategies.

In addition, the following assumptions are made:

- During RT operation, the adversary knows the current period's ex-ante market results and the previous period's ex-post market results, which are published by ISOs;
- The attacker has partial access to the measurement set. For example, (35) shows a compromised measurement set where z is the real measurement data, and z_a is the injected false data. However, the non-zero elements in z_a are less than the threshold.

$$\bar{z}_{com} = \bar{z} + \bar{z}_a \quad (35)$$

B. Passing Bad Data Detection

The mismatch Δy also prevents the direct modeling of bad data detection constraint (10) in the attack model. The compromised measurement vector is input for the state estimation as in (36).

$$G_{se}^{act}(\bar{x}^k) \Delta x = H_{se}^{act}(\bar{x}^k)^T R^{-1} (\bar{z}_{com} - h_{se}^{act}(\bar{x}^k)) \quad (36)$$

Then, similar to (36), a sensitivity matrix with uncertainty is formed in (37) where \hat{x} represents the estimated system states.

$$S_{es}^{act}(\bar{x}) = I - H_{es}^{act}(\bar{x}) G(\bar{x})^{-1} H_{es}^{act}(\bar{x})^T \quad (37)$$

The residual estimated by the attacker is modeled in (38) if an attack vector is applied in the raw measurement.

$$r = S_{es}^{act}(\bar{x}) \bar{z}_a \quad (38)$$

To bypass bad data detection, the attack vector must ensure that the residual is less than the threshold. With the approximated H_{se}^{act} , the attacker loses perfect control of the residual calculation. In this paper, chance constraints with an allowable confidential interval are incorporated by the proposed attack strategy providing an optimal injection vector under uncertainty. Consequently, the attacker tries to select the injected data that has the highest possibility of passing bad data detection, as in (39).

$$P(\|r_i^N\|_2 < thresh) \geq \eta \quad (39)$$

C. Disguising the Compromised LMP

The major factors contributing to the detection of traditional attack strategies through operator experience are (1) that the artificially created congestion pattern may not exist for any loading level; (2) that the compromised LMPs lead abnormal step changes which are inconsistent with previous periods.

As shown in Fig. 6, the compromised LMP from traditional attack strategies can be represented by the green or blue lines. Different traditional attack strategies' resulting LMP magnitude may vary, but the shapes are similar to these two lines. The attack is launched at period t . From period $t-1$ to period $t+1$, there was a step change of $CLLI$ at period t . However, both the green line and blue line inevitably create a new step change at period $t+1$. In addition, the resulting LMP magnitude may not exist for this system under any loading level because $LMP3$ or $LMP4$ is determined by the newly created congestion pattern.

The red line represents the resulting LMPs of the proposed attack strategy, which have the same shape as original LMPs except that the step change at period t is delayed to period $t+1$. Operators are less sensitive in this disguising attack because (1) no new congestion pattern is created; (2) the step-change magnitude is the same as before.

The same analysis can be done at any period, and the traditional cyberattack strategy always introduces a new step-change in LMPs.

To successfully launch the disguising attack, attack periods need to be carefully selected. First, target periods are restricted to those periods when system loading changes smoothly because the proposed cyber contingency analysis is not applied during

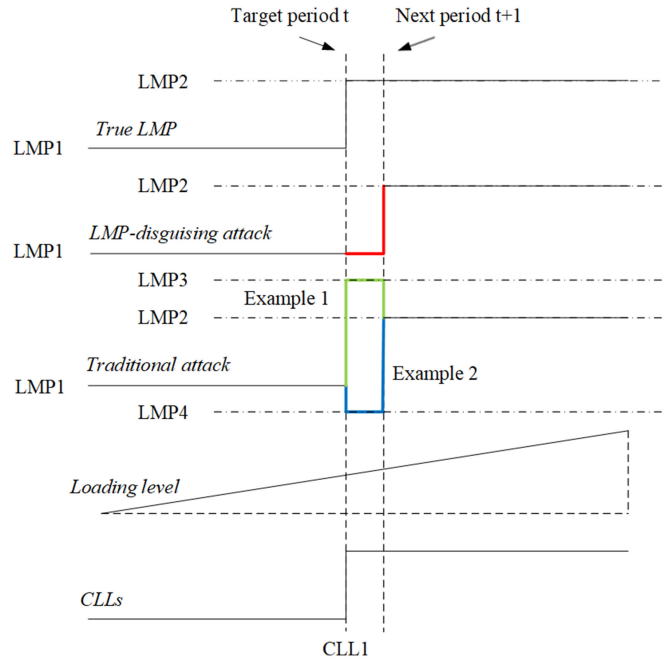


Fig. 6. LMP-disguising attack and traditional attack.

safe periods, and replicating a previous congestion pattern is hard when the pattern changes dramatically. Secondly, the step-change at the target period is induced by line congestion only since the change of congestion patterns cannot delay the step-change induced by generation constraints.

To perform such an attack, the following equations (40)–(43) suffice to ensure a delay of the step change. $f_{l,t}$ is the actual line flow, and the second term is the changed line flow due to the attack vector.

$$f_{l,t} - (I - H_{es}^{act}(\bar{x})G(\bar{x})^{-1}H_{es}^{act}(\bar{x})^T)\bar{z}_a = f_l^{\min}, \forall l \in L_{-\min} \quad (40)$$

$$f_{l,t} - (I - H_{es}^{act}(\bar{x})G(\bar{x})^{-1}H_{es}^{act}(\bar{x})^T)\bar{z}_a < f_l^{\max}, \forall l \in L_{-\max} \quad (41)$$

$$f_{l,t} + (I - H_{es}^{act}(\bar{x})G(\bar{x})^{-1}H_{es}^{act}(\bar{x})^T)\bar{z}_a > f_l^{\min}, \forall l \in L_{+\min} \quad (42)$$

$$f_{l,t} + (I - H_{es}^{act}(\bar{x})G(\bar{x})^{-1}H_{es}^{act}(\bar{x})^T)\bar{z}_a = f_l^{\max}, \forall l \in L_{+\max} \quad (43)$$

where $L_{+\max}$, $L_{+\min}$, $L_{-\max}$, and $L_{-\min}$ are defined as in (44)–(47).

$$L_{+\max} \triangleq \{l \in \{f_{l,t-1} = f_l^{\max} \text{ and } f_{l,t} < f_l^{\max}\}\} \quad (44)$$

$$L_{+\min} \triangleq \{l \in \{f_{l,t-1} > f_l^{\min} \text{ and } f_{l,t} = f_l^{\min}\}\} \quad (45)$$

$$L_{-\min} \triangleq \{l \in \{f_{l,t-1} = f_l^{\min} \text{ and } f_{l,t} > f_l^{\min}\}\} \quad (46)$$

$$L_{-\max} \triangleq \{l \in \{f_{l,t-1} < f_l^{\max} \text{ and } f_{l,t} = f_l^{\max}\}\} \quad (47)$$

It is worth noting that changing an uncongested line to a congested line requires more injected false data, which may lead

to failure to pass bad data detection. Therefore, it is preferable to attack at those periods when $L_{-\min}$ and $L_{+\max}$ are either empty or close to their limits.

D. Profit Model

Most ISOs allow virtual bidders as participants in market trading to increase competition and liquidity. Virtual bidding is purely a financial transaction which submits bids and offers to the DA market without any obligation to actually deliver or consume power in the RT market. Many ISOs have three types of virtual bidding: (1) increment offers; (2) decrement bids; and (3) up-to-congestion transactions (UTCs). UTCs best fit the needs of the proposed attacker who submits bids to purchase and sell congestions between two nodes in the DA and RT markets. The profits obtained by UTCs are expressed in (48). By substituting (18) into (48), (49) is further formulated.

$$\begin{aligned} \text{Payoff} = & ((LMP_i^{RT} - LMP_j^{RT}) \\ & - (LMP_i^{DA} - LMP_j^{DA}))P_{bid} \end{aligned} \quad (48)$$

$$\begin{aligned} \text{Payoff} = & P_{bid} \sum_{l \in L_{-\max}} (GSF_{l,i} - GSF_{l,j})\pi_l \\ & + P_{bid} \sum_{l \in L_{+\min}} (GSF_{l,i} \\ & - GSF_{l,j})\pi_l - P_{bid}(LMP_i^{DA} - LMP_j^{DA}) \end{aligned} \quad (49)$$

If the following three conditions are satisfied, then the *payoff* is always positive, as can be deduced from (49) and as is shown in [6],

$$LMP_i^{DA} - LMP_j^{DA} < 0 \quad (50)$$

$$f_{l,t} > f_l^{\min}, \forall l \in \{GSF_{l,i} - GSF_{l,j} > 0\} \quad (51)$$

$$f_{l,t} < f_l^{\max}, \forall l \in \{GSF_{l,i} - GSF_{l,j} < 0\} \quad (52)$$

Here, conditions (50)–(52) are further modified to (53)–(55) to ensure a positive profit.

$$LMP_i^{DA} - LMP_j^{DA} < 0 \quad (53)$$

$$f_{l,t}^* > f_l^{\min}, \forall l \in L_{+\min} \quad (54)$$

$$f_{l,t}^* < f_l^{\max}, \forall l \in L_{-\max} \quad (55)$$

The above conditions ensure profit regardless of target selections. Attackers with more information can select specified buses and lines to guarantee the profits. Then in this disguising attack, the same selection can also be made.

E. Overall Attack Strategy

Condition (53) is easily satisfied by carefully selecting bus i and bus j [6], [14]. However, from the attacker's perspective, $f_{l,t}$ follows Gaussian random distribution. Therefore, perfect satisfaction of (54) and (55) is not guaranteed. Hence, a confidence index ε is introduced to maximize the likelihood of satisfying

those conditions. Similar to (39), chance constraints are formulated as (56)–(57) where η_a is the confidence level.

$$P(f_{l,t}^* > f_l^{\min} + \varepsilon) \geq \eta_a \forall l \in L_{+\min} \quad (56)$$

$$P(f_{l,t}^* < f_l^{\max} - \varepsilon) \geq \eta_a \forall l \in L_{-\max} \quad (57)$$

Then, the attack optimization model can be formulated as in (58)–(65).

$$\max \varepsilon \quad (58)$$

$$P\left(\left\| \left(I - H_{es}^{act}(\bar{x})G(\bar{x})^{-1}H_{es}^{act}(\bar{x})^T \right) \bar{z}_a \right\|_2 < thresh_{\Omega} \geq \eta_a \right) \quad (59)$$

$$P(f_{l,t}^* > f_l^{\min} + \varepsilon) \geq \eta_a \forall l \in L_{+\min} \quad (60)$$

$$P(f_{l,t}^* < f_l^{\max} - \varepsilon) \geq \eta_a \forall l \in L_{-\max} \quad (61)$$

$$f_{l,t}^* = f_{l,t} + (I - H_{es}^{act}(\bar{x})G(\bar{x})^{-1}H_{es}^{act}(\bar{x})^T)\bar{z}_a \forall l \in L_{+\min} \quad (62)$$

$$f_{l,t}^* = f_{l,t} - (I - H_{es}^{act}(\bar{x})G(\bar{x})^{-1}H_{es}^{act}(\bar{x})^T)\bar{z}_a \forall l \in L_{-\max} \quad (63)$$

$$\varepsilon > 0 \quad (64)$$

$$\eta_a \eta_a \eta_a \leq \eta \quad (65)$$

To solve the chance-constrained attack model, a scenario approximation method is applied to reformulate (58)–(65) as (66)–(73) [32].

$$\max \varepsilon \quad (66)$$

$$(I - H_{es}^{act}(\bar{x})G(\bar{x})^{-1}H_{es}^{act}(\bar{x})^T)\bar{z}_a - Mz_i < thresh_{\Omega} \quad (67)$$

$$f_{l,t}^* - (f_l^{\min} + \varepsilon) + Mz_j > 0 \forall l \in L_{+\min} \quad (68)$$

$$f_{l,t}^* - (f_l^{\max} - \varepsilon) - Mz_k < 0 \forall l \in L_{-\max} \quad (69)$$

$$(51), (52)$$

$$\sum_{i=1}^N z_i \leq (1 - \eta_a)N \quad (70)$$

$$\sum_{j=1}^N z_j \leq (1 - \eta_a)N \quad (71)$$

$$\sum_{k=1}^N z_k \leq (1 - \eta_a)N \quad (72)$$

$$\eta_a \eta_a \eta_a \leq \eta \quad (73)$$

A large penalty factor and binary indicators are inserted to describe the satisfaction of the chance constraints deterministically. When the decision variable z_a falls out of the confidence level η , the binary variables z_i , z_j , and z_k activate the penalty term M to ensure the feasibility of those constraints. When the decision variable is within the confidence level, the binary indicator ensures that the penalty term is equal to 0, as shown in (74)–(76).

$$z_i = 0 \Rightarrow (I - H_{es}^{act}(\bar{x})G(\bar{x})^{-1}H_{es}^{act}(\bar{x})^T)\bar{z}_a < thresh \quad (74)$$

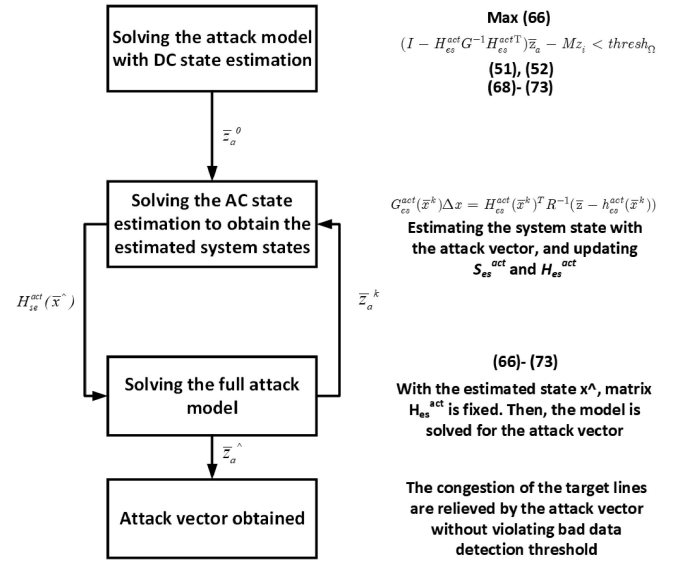


Fig. 7. Iterative optimization process.

$$z_j = 0 \Rightarrow f_{l,t}^* - (f_l^{\min} + \varepsilon) + Mz_j > 0 \forall l \in L_{+\min} \quad (75)$$

$$z_k = 0 \Rightarrow f_{l,t}^* - (f_l^{\max} - \varepsilon) - Mz_k < 0 \forall l \in L_{-\max} \quad (76)$$

Further, the residual calculations depend on the iterative solution of (36). For DC state estimation, the sensitivity matrix is fixed and independent of the system state.

$$S_{DC}(x) = I - H_{es}^{act}G^{-1}H_{es}^{actT} \quad (77)$$

Then, the attack model (66)–(73) can be directly solved.

However, when AC state estimation is considered, the sensitivity matrix S_{es}^{act} depends on the estimated system states which are related to the attack vectors. Therefore, an iterative process is proposed to obtain a valid attack vector progressively. The proposed iterative process is shown in Fig. 7. The attack model is first solved with DC state estimation providing an initial guess of the attack vector. Then, the attack vector is injected into AC state estimation. The resulting estimated states provide a new set of H_{es}^{act} and S_{es}^{act} , which are applied back to the attack model to obtain the attack vector for the next iteration. The iterative process is terminated if the attack vector changes the congestion of the target lines without violating the bad data detection threshold. Despite the implication of the phrase “iterative process,” this computation approach is efficient. The proposed attack only considers relieving the congestion of target lines. For example, assume that a line is originally congested at its upper limit 200 MW. This means that the proposed attack only needs to make a slight change to uncongest the line flow (e.g., changing it by 1 MW to 199 MW). As such, the attack vector only contains small values, but it can cause a change in the congestion pattern. Therefore, the attack vector leads to a very small change to the “largest normalized residual” and cannot be easily detected by the bad data detector. As long as the new flow is slightly lower than 200 in a numerical sense (e.g., 199, 198 or a few MWs lower than 200) regardless of the actual value, it will effectively make this line uncongested. In other words, the bad data threshold constraint is very easy to

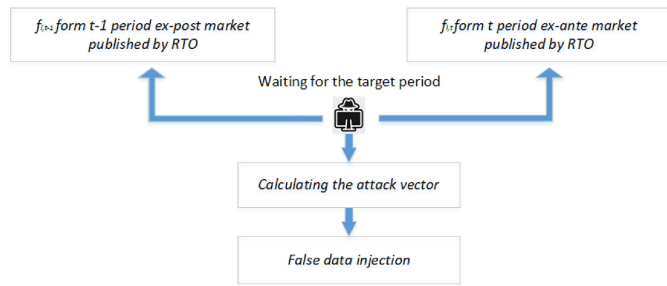


Fig. 8. Proposed attack strategy procedures.

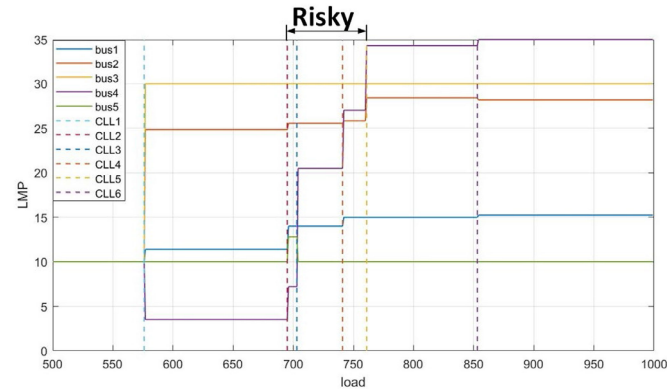


Fig. 9. PJM 5-bus system CLLs.

pass in this model, which makes it easy for the iterative process to meet the stopping criterion of success.

In the end, the overall procedures of the proposed attack strategy are shown in Fig. 8. An attacker observes the current period and last period power flow information from the last period's ex-post market results and current period's ex-ante market results, which are published by ISOs. Then, the attacker waits for the target period, as discussed in part C. Finally, the optimization model (59)–(66) is solved to determine the FDIA amount and locations.

V. CASE STUDY

In this section, we provide simulation results in both the PJM 5-bus system and the IEEE 118-bus system to illustrate how the proposed abnormal LMP analysis detects traditional attack strategies from the market-level, and demonstrate that the proposed LMP-disguising attack not only bypasses bad data detection without drawing operators' attention but also results in a monetary profit. Simulations are performed in MATLAB 2017 and Python 3.7 with software packages of MATPOWER and Gurobipy. The system parameters can be found in [34].

In this simulation study, confidence levels are all set to 0.95, and the random distribution $N(0, 0.01)$ is similar to the settings in [14].

A. Case 1: Proposed Analysis Method and Attack Strategy in a Small System: PJM 5-Bus System

First, all CLLs are calculated as in Fig. 9. The α index is defined to 1, and N-2 cyber contingency analysis is performed

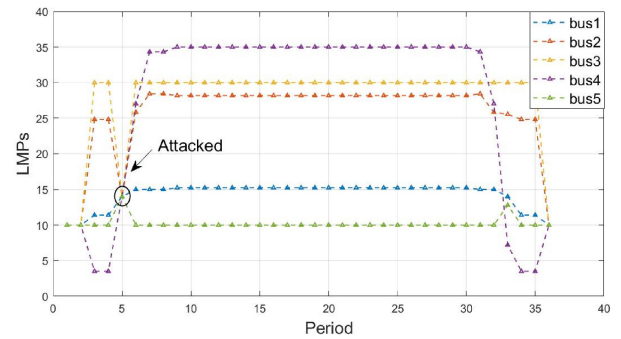


Fig. 10. LMP for PJM 5-bus system traditional attack.

since 2 is the maximum number of possibly congested lines. Then, CLL intervals in the areas with risky labels (695MW–761MW) are identified as risky.

It is worth noting that risky CLL intervals are intrinsically narrow. Therefore, risky periods normally comprise a small percentage of a normal day's operations.

- 1) *Cyber Contingency Analysis*: Using Algorithm BC, a cyber contingency library is built. In Fig. 2 and Fig. 3, we have shown when operators are confident enough to detect attacks based on experience. Therefore, in this case study, we perform a traditional attack strategy at periods $r_i < thresh$, in which operators apply the proposed analysis method to help detect abnormal LMPs. Then, period 5 is selected as an example, as shown in Fig. 10. The traditional attack strategy bypasses bad data detection by ensuring the resulting residual is smaller than the threshold.

During risky periods in RT operation, the operator compares the CLL, congestion patterns, and LMPs with counterparts in the library. It is found that congestion patterns and LMPs at period 5 match the behaviors when line 5 is compromised. Then, operators may check on whether the corresponding local RTU is compromised. Therefore, traditional attack strategies are detected by operators during safe periods or risky periods.

- 2) *LMP-Disguising Attack*: During the RT operation period, the attacker keeps observing the line flow information from the last period's ex-post market results and current period's ex-ante market results, which are published by ISOs. A step change (e.g., the line connecting buses 3 and 4 is congested) is observed at period 3. The attacker inputs this target line and desired confidence level (0.95) into the iterative process. The computation time of the attack vector is 1.24s. In this case study, the initial guess from the DC model relieves the congestion in the AC model without violating the bad data detection threshold.

The compromised LMP is shown in Fig. 11, which looks very similar to the normal operation LMP in Fig. 2. The difference is enlarged and shown in Fig. 12.

The solid line in Fig. 12 is the LMP from the disguising attack, while the dashed line is the original LMP. The step-change that previously happened at period 3 is delayed to period 4. Bad data detection is bypassed by (59) with a 95% confidence level.

As stated in Section II, the major reasons contributing to the detection of traditional attack strategies by operators' experience

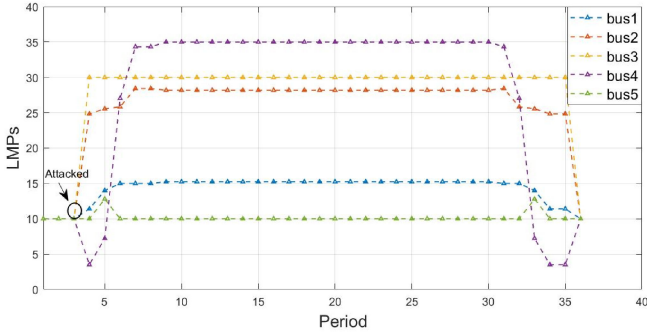


Fig. 11. PJM 5-bus system LMP by the disguising attack.

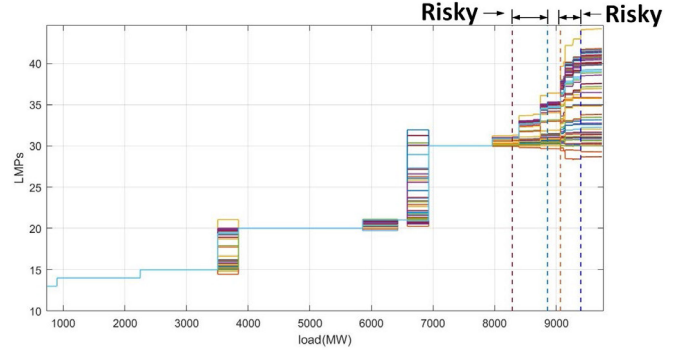


Fig. 14. IEEE 118-bus system CLLs.

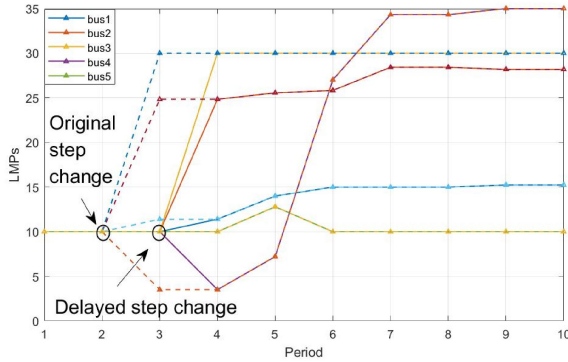


Fig. 12. Attacked LMP comparison.

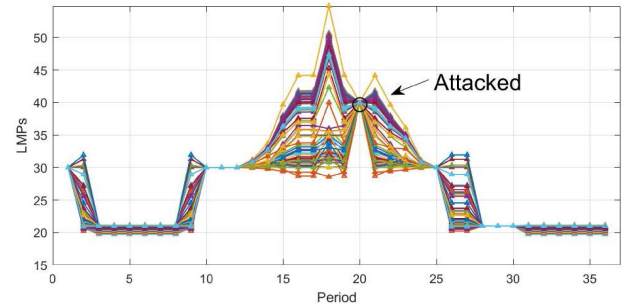


Fig. 15. IEEE 118-bus system LMP by a traditional attack.

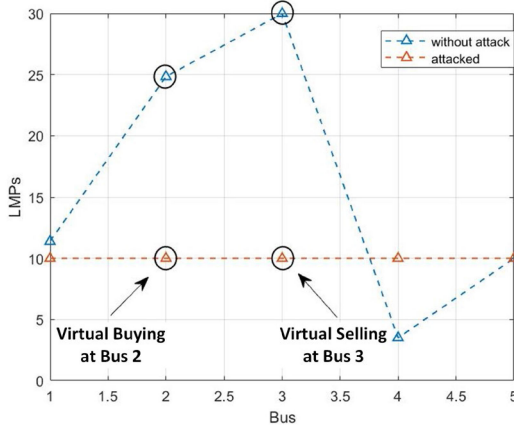


Fig. 13. LMPs at the target period.

are: (1) the resulting new congestion pattern may fall outside of the normal congestion pattern at the current loading level; (2) the compromised LMPs are not consistent with previous periods when the system loading changes smoothly. The disguising attack overcomes the above two problems, as shown in Fig. 11: (1) no new congesting pattern is created; and (2) the compromised LMP is consistent with the previous LMP because the step change at period 3 is delayed to period 4. Consequently, the disguising attack is stealthy because it is hard to identify at both the market-level and the state estimation level. Fig. 13 shows how an attacker makes profits via an FDIA at period 5.

The attacker buys a certain amount of virtual power at bus 2 and sells the same amount of virtual power at bus 3 in the DA market. During RT operation, congestion is relieved, and the price difference in the DA market is the profit. The choice of nodes is profitable as long as the attacker buys at a low-price node and sells at a high price node in the DA market, and the congestion in RT is relieved by an FDIA.

B. Case 2: Proposed Analysis Method and Attack Strategy in a Large System: IEEE 118-Bus System

In this case study, the IEEE 118-bus system is selected to further demonstrate the performance of the proposed analysis method and the attack strategy in a large system.

The CLLs are first calculated as in Fig. 14. Compared with the small system, the large system has more LMP step changes because there are more flow constraints, and generation limits are enforced. Risky CLL intervals are also identified.

1) *Cyber Contingency Analysis*: Similarly, a traditional attack is performed at period 20, as shown in Fig. 15. Since the attack happens at a risky period, the operator compares the current congestion pattern, system load, and LMPs with the counterparts in the library.

Therefore, the attack is identified since the behavior matches what occurs when lines 7, 9, 41, and 54 are compromised.

2) *LMP-Disguising Attack*: Further, in a larger system, the complicated LMP step changes result in more opportunities for attackers. An attacker sequentially finds that periods 13 and 31 qualify as target periods.

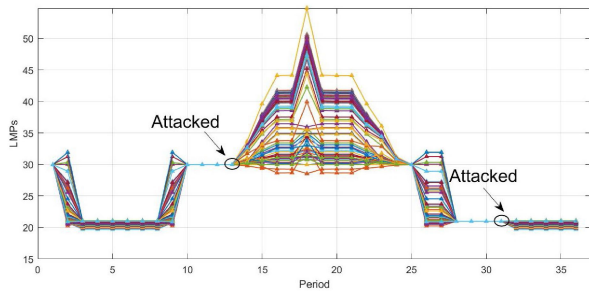


Fig. 16. IEEE 118-bus system LMP by the disguising attack.

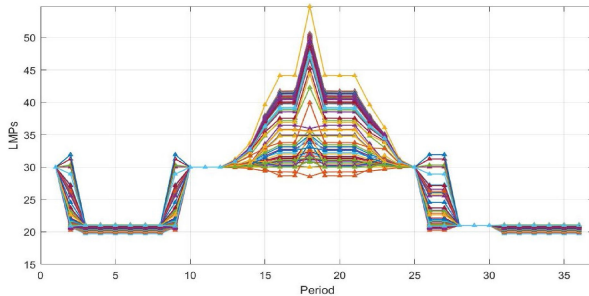


Fig. 17. IEEE 118-bus system LMP without attack.

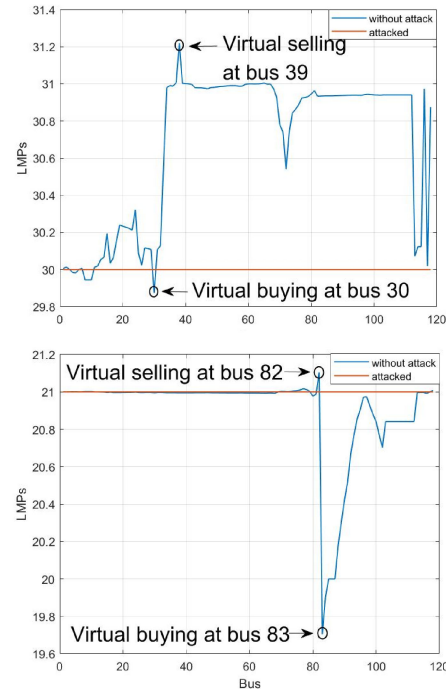


Fig. 18. LMPs at target periods.

The steps of computing attack vector are similar to the procedures in Case 1. The computation times for the attack vector at periods 13 and 31 are 39.78s and 36.55s, respectively, at the testing laptop computer. The iterative process at both periods ends within two iterations (attack model and AC state estimation in each iteration). The computation time is sufficient for real-time market operation even in a 5-minute spot market. The disguising attacks are performed, as shown in Fig. 16, and Fig. 17 shows the LMP curve under normal operations.

The LMP step changes which originally occurred at periods 13 and 31 are delayed to periods 14 and 32. Bad data detection is bypassed with a 0.95 confidence level. No noticeable abnormal LMPs are created, and step changes are reasonable. Thus, the attack is undetectable for market operators.

Fig. 18 shows how an attacker profits via the FDIA. At periods 13 and 31, the attacker buys a certain amount of electricity at bus 30 and bus 83, and sells the same amount of electricity at bus 39 and bus 82. The DA and RT market congestion difference gives the attacker monetary benefits.

VI. CONCLUSION

The key observation of this paper is that even if state estimation level detection mechanisms are bypassed, cyberattacks can easily be detected by market operators based on market-level behavior, such as abnormal price signals. Therefore, this paper investigates how abnormal price signals can be detected with the proposed algorithm using risky CLL intervals, and then disguised by a more advanced LMP-disguising attack model.

We first demonstrate that the traditional attack via bypassing only bad data detection is not enough for a successful electricity

market cyberattack. By analyzing CLLs of LMPs, we construct a market-level defense analysis method to help operators identify attacks. Then, an LMP-disguising attack strategy is developed to disguise the compromised LMPs as normal LMPs, which can bypass both bad data detection and market-level detection. The ultimate goal of proposing this attack is to facilitate future defense developments. In the case studies, the attack method is applied to both a small system and a large system to show the effectiveness and feasibility of the proposed detection method and the new LMP-disguising attack strategy. In future works, a price-aware behavior analyzer, which may be trained with loaded attack events to identify inconspicuous attack patterns, will be constructed to detect the LMP-disguising attack.

DISCLAIMER

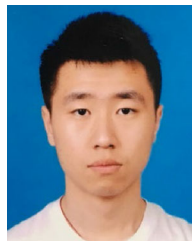
This paper was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

ACKNOWLEDGEMENT

The authors would also like to thank the useful discussions from all WISP project team members.

REFERENCES

- [1] H. Ye, Y. Ge, X. Liu, and Z. Li, "Transmission line rating attack in two-settlement electricity markets," *IEEE Trans. Smart Grid*, vol. 7, no. 3, pp. 1346–1355, May 2016.
- [2] P. R. Gribik, W. W. Hogan, and S. L. Pope, *Market-Clearing Electricity Prices and Energy Uplift*. Cambridge, MA, USA: Harvard Electricity Policy Group, 2007.
- [3] G. Liang, J. Zhao, F. Luo, S. R. Weller, and Z. Y. Dong, "A review of false data injection attacks against modern power systems," *IEEE Trans. Smart Grids*, vol. 8, no. 4, pp. 1630–1638, Jul. 2017.
- [4] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," in *Proc. 16th ACM Conf. Comput. Commun. Security*, New York, NY, USA, 2009, pp. 21–32.
- [5] A. Ashok and M. Govindarasu, "Cyber attacks on power system state estimation through topology errors," in *Proc. IEEE PES Meet.*, 2012, pp. 1–8.
- [6] L. Xie, Y. Mo, and B. Sinopoli, "Integrity data attacks in power market operations," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 659–666, Dec. 2011.
- [7] S. Tan, W.-Z. Song, M. Stewart, J. Yang, and L. Tong, "Online data integrity attacks against real-time electrical market in smart grid," *IEEE Trans. Smart Grid*, vol. 9, no. 1, pp. 313–322, Jan. 2018.
- [8] R. Moslemi, A. Mesbahi, and J. M. Velni, "Design of robust profitable false data injection attacks in multi-settlement electricity markets," *IET Gener. Transmiss. Distrib.*, vol. 12, no. 6, pp. 1263–1270, Mar. 2018.
- [9] D. Choi and L. Xie, "Economic impact assessment of topology data attacks with virtual bids," *IEEE Trans. Smart Grid*, vol. 9, no. 2, pp. 512–520, Mar. 2018.
- [10] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong, "A framework for cyber-topology attacks: Line-switching and new attack scenarios," *IEEE Trans. Smart Grid*, vol. 10, no. 2, pp. 1704–1712, Mar. 2019.
- [11] H. Ye, Y. Ge, X. Liu, and Z. Li, "Transmission line rating attack in two-settlement electricity markets," *IEEE Trans. Smart Grid*, vol. 7, no. 3, pp. 1346–1355, May 2016.
- [12] C. Liu, M. Zhou, J. Wu, C. Long, and D. Kundur, "Financially motivated FDI on SCED in real-time electricity markets: Attacks and mitigation," *IEEE Trans. Smart Grid*, vol. 10, no. 2, pp. 1949–1959, Dec. 2017.
- [13] D.-H. Choi and L. Xie, "Ramp-induced data attacks on look-ahead dispatch in real-time power markets," *IEEE Trans. Smart Grid*, vol. 4, no. 3, pp. 1235–1243, Sep. 2013.
- [14] A. Tajer, "False data injection attacks in electricity markets by limited adversaries: Stochastic robustness," *IEEE Trans. Smart Grid*, vol. 10, no. 1, pp. 128–138, Jan. 2019.
- [15] T. T. Kim and H. V. Poor, "Strategic protection against data injection attacks on power grids," *IEEE Trans. Smart Grid*, vol. 2, no. 2, pp. 326–333, Jun. 2011.
- [16] S. Bi and Y. J. Zhang, "Graphical methods for defense against false-data injection attacks on power system state estimation," *IEEE Trans. Smart Grid*, vol. 5, no. 3, pp. 1216–1227, May 2014.
- [17] R. Deng, G. Xiao, and R. Lu, "Defending against false data injection attacks on power system state estimation," *IEEE Trans. Ind. Informat.*, vol. 13, no. 1, pp. 198–207, Aug. 2015.
- [18] B. M. Sanandaji, E. Bitar, K. Poolla, and T. L. Vincent, "An abrupt change detection heuristic with applications to cyber data attacks on power systems," in *Proc. IEEE Amer. Control Conf.*, Portland, OR, USA, 2014, pp. 5056–5061.
- [19] F. Pasqualetti, F. Dorfler, and F. Bullo, "Cyber-physical attacks in power networks: Models, fundamental limitations and monitor design," in *Proc. Decision Control Eur. Control Conf.*, 2011, pp. 2195–2201.
- [20] A. F. Taha, J. Qi, J. Wang, and J. H. Panchal, "Risk mitigation for dynamic state estimation against cyber attacks and unknown inputs," *IEEE Trans. Smart Grid*, vol. 9, no. 2, pp. 886–899, Mar. 2018.
- [21] S. Bi and Y. J. Zhang, "Using covert topological information for defense against malicious attacks on DC state estimation," *IEEE J. Sel. Areas Commun.*, vol. 32, no. 7, pp. 1471–1485, Jul. 2014.
- [22] O. Vukovic, K. C. Sou, G. Dán, and H. Sandberg, "Network-aware mitigation of data integrity attacks on power system state estimation," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 6, pp. 1108–1118, Jul. 2012.
- [23] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Malicious data attacks on the smart grid," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 645–658, Dec. 2011.
- [24] F. Eldali and S. Suryanarayanan, "A data-driven justification for dedicated dynamic pricing for residences-based plug-in electric vehicles in wind energy-rich electricity grids," *IEEE Open Access J. Power Energy*, vol. 7, pp. 51–58, Jan. 2020, doi: 10.1109/OAJPE.2019.2952813.
- [25] A. Abur and A. Gomez-Exposito, *Power System State Estimation: Theory and Implementation*. New York, USA: Marcel Dekker, 2004.
- [26] J. Schoene *et al.*, "Quantifying performance of distribution system state estimators in supporting advanced applications," *IEEE Open Access J. Power Energy*, vol. 7, pp. 151–162, May 2020.
- [27] Y. Lin and A. Abur, "A highly efficient bad data identification approach for very large-scale power systems," *IEEE Trans. Power Syst.*, vol. 33, no. 6, pp. 5979–5989, Nov. 2018.
- [28] F. Li, Y. Wei, and S. Adhikari, "Improving an unjustified common practice in ex post LMP calculation," *IEEE Trans. Power Syst.*, vol. 25, no. 2, pp. 1195–1197, May 2010.
- [29] H. Yuan, F. Li, and Y. Wei, "LMP step pattern detection based on real-time data," in *Proc. IEEE PES Gen. Meet.*, Vancouver, BC, Canada, Jul. 2013, pp. 1–5.
- [30] F. Li, "Continuous locational marginal pricing (CLMP)," *IEEE Trans. Power Syst.*, vol. 22, no. 4, pp. 1638–1646, Nov. 2007.
- [31] F. Li and Rui Bo, "Congestion and price prediction under load variation," *IEEE Trans. Power Syst.*, vol. 24, no. 2, pp. 911–922, May 2009.
- [32] S. Ahmed, A. Shapiro, and E. Shapiro, "The sample average approximation method for stochastic program with integer recourse," *SIAM J. Optim.*, vol. 12, no. 2, pp. 479–502, May 2002.
- [33] ISO New England. "Final real-time five-minute binding constraints," Jan. 2020. [Online]. Available: <https://www.iso-ne.com/isoexpress/web/reports/grid/-/tree/constraint-rt-fivemin-final>
- [34] F. Li and R. Bo, "Small test systems for power system economic studies," *Power Energy Soc. Gen. Meet.*, pp. 1–4, Jul. 2010.



Qiwei Zhang (Student Member, IEEE) received the B.S.E.E. degree from North China Electrical Power University in 2016 and the M.S.E.E degree from UTK in 2018. He is currently a Ph.D. Student with the Department of Electrical Engineering and Computer Science at The University of Tennessee, Knoxville (UTK). His research interest includes cyber security in power systems, power system optimization, and market operation.



Fangxing Li (Fellow, IEEE) is also known as Fran Li. He received the B.S.E.E. and M.S.E.E. degrees from Southeast University, Nanjing, China, in 1994 and 1997, respectively, and the Ph.D. degree from Virginia Tech, Blacksburg, VA, USA, in 2001. Currently, he is the James W. McConnell Professor in electrical engineering and the Campus Director of CURENT with the University of Tennessee, Knoxville, TN, USA. His current research interests include renewable energy integration, demand response, distributed generation and microgrid, energy markets, and power system computing. Prof. Li is presently serving as the Editor-In-Chief of IEEE OPEN ACCESS JOURNAL OF POWER AND ENERGY (OAJPE) and the Chair of IEEE/PES Power System Operation, Planning and Economics (PSOPE) Committee.

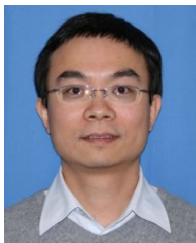


Hantao Cui (Member, IEEE) received the B.S.E.E. and M.S.E.E. degrees from Southeast University, China, in 2011 and 2013, respectively, and the Ph.D. degree from the University of Tennessee, in 2018. Currently he is a Research Assistant Professor with CURENT and the Department of Electrical Engineering and Computer Science, University of Tennessee, Knoxville. Prior to obtaining Ph.D. degree, he was appointed as a full-time Research Associate with CURENT in 2017. He serves as Associate Editor

for the *Journal of Modern Power Systems and Clean Energy*. His research interests include power system modeling and simulation, high-performance computing, and software-hardware solutions for scientific computing.



Lingyu Ren (Member, IEEE) received the Ph.D. degree from the University of Connecticut in 2017. She is presently a Senior Engineer at Raytheon Technologies Research Center, East Hartford, CT. Her current research interest is in cyber security and big data analysis in smart grids.



Rui Bo (Senior Member, IEEE) received the BSEE and MSEE degrees in electric power engineering from Southeast University (China) in 2000 and 2003, respectively, and received the Ph.D. degree from the University of Tennessee, Knoxville (UTK) in 2009. He is currently an Assistant Professor of the Electrical and Computer Engineering Department with the Missouri University of Science and Technology (formerly University of Missouri-Rolla). He worked as a Principal Engineer and Project Manager at Mid-continent Independent System Operator (MISO) from 2009 to

2017. His research interests include computation, optimization and economics in power system operation and planning, high performance computing, electricity market simulation, evaluation and design.