# Power Market Cybersecurity and Profit-targeting Cyberattacks

A Dissertation Presented for the

Doctor of Philosophy

Degree

The University of Tennessee, Knoxville

Qiwei Zhang

August 2022

# Acknowledgments

First and foremost, I would like to express my deepest gratitude to my advisor, Dr. Fangxing (Fran) Li, for his continuous support of this dissertation and all other research works during my Ph.D. study at the University of Tennessee.

I am grateful to Dr. Kevin Tomsovic, Dr. Hector Pulgar, and Dr. Mingzhou Jin for devoting time and efforts to serve as the dissertation committee members.

I would like to thank all the group members in the Electric Network Laboratory for Intelligent Transactive ENergy (Enliten Lab) for the discussions on research works.

Special thanks to Watching Grid Infrastructure Stealthily through Proxies (WISP) research team for invaluable discussions and guidance. Without them, it would be impossible to finish this dissertation.

Finally, I would like to thank my parents, Hongyan Li and Sunping Zhang, and all of my family members, whose love and encouragement are always with me throughout my life.

# Abstract

The COVID-19 pandemic has forced many companies and business to operate through remote platforms, which has made everyday life and everyone more digitally connected than ever before. The cybersecurity has become a bigger priority in all aspects of life. A few real-world cases have demonstrated the current capability of cyberattacks as in [1], [2], and [3]. These cases invalidate the traditional belief that cyberattacks are unable to penetrate real-world industrial systems. Beyond the physical damage, some attackers target financial arbitrage advantages brought by false data injection attacks (FDIAs) [4]. Malicious breaches into power market operations could induce catastrophic consequences on fair financial settlements and reliable transmission services. In this dissertation, an in-depth study is conducted to investigate power market cybersecurity and profit-targeting cyberattacks.

In the first work, we demonstrate the importance of market-level behavior in defending cyberattacks and designing cyberattacks. A market-level defense analysis is developed to help operators identify cyberattacks, and an LMP-disguising attack strategy is developed to disguise the abnormal LMPs, which can bypass both the bad data detection and market-level detection.

In the second work, we propose a comprehensive CVA model for delivering a detailed analysis of four aspects of vulnerability: highly probable cyberattack targets, devastating attack targets, risky load levels, and mitigation ability under different degrees of defense.

In the third work, we identify that revenue adequacy, a fundamental power market operation criterion, has not been analyzed under the context of cybersecurity, and we explore

the impact of FDIAs targeting real-time (RT) market operations on ISO revenue adequacy analytically and numerically.

In the last work, we extend the power system cybersecurity analysis to multi-energy system (MES) framework. An optimally coordinated (OC-FDIA) targeting MES is proposed. Then, we show that the OC-FDIA cause much more severe damages than single-system FDIA and uncoordinated FDIAs. Further, an effective countermeasure is developed against the proposed OCFDIA based on deep learning technique (DL).

**Keywords**: False data injection attack, power market operations, locational marginal price, multi-energy system.

# Table of Contents

# List of Tables

# List of Figures

# List of Abbreviations

| | |
|---|---|
| ED | Economic dispatch |
| DA | Day-ahead |
| RT | Real-time |
| LMP | Locational marginal price |
| ISO | Independent system operator |
| SE | State estimation |
| RTU | Remote terminal unit |
| FDIA | False data injection attack |
| GSF | Generation shift factors |
| ISO | Independent system operator |
| CVA | Cyber-vulnerability analysis |
| FTR | Financial transmission right |
| BDI | Bad data identification |
| MES | Multienergy system |

# Chapter 1 Introduction

This chapter first briefly discusses the two-settlement power market from the cybersecurity perspective. Then, state-of-the-art works on electricity market cyberattacks are categorized and summarized. The background of this dissertation is presented along with a comprehensive review where relevant research works are divided by their research directions. More details of this chapter can be found in [5]

## 1.1 Electricity market and cyberattacks

Wholesale electricity markets in the U.S. are organized by independent system operators (ISOs) and usually consist of day-ahead (DA) and real-time (RT) markets. The offers and bids from generator companies and load aggregators are collected by ISOs. Unit commitment and DA economic dispatch (ED) are solved to determine DA unit dispatches and LMPs. DA LMPs are calculated based on 24-hour advance load forecasting. The purpose of the RT market is to offer adjustments for load forecasting differences between RT and DA. The RT market is cleared based on RT operation conditions obtained from state estimation. Therefore, attacking the DA market is generally less feasible because ISOs have plenty of time to detect and analyze. A significant number of profit-targeting cyberattacks in the literature perform FDIA on state estimation to affect RT LMP calculations. The prevailing market operation models can be found in [5]. Different from a traditional malicious data intrusion, attack strategies on the electricity market require: (1) the attackers' participation in market-clearing; (2) the profitability of the attack strategies; and (3) bypassing control center detection, such as bad data identification.

### *1.1.1 Where to Attack*

Main attack paths for power market cyberattacks are the coupling between state estimation and RT LMPs. The state estimation decides the constraint of the RT market-clearing model, and thus, the RT market model depends on state estimation results. The majority of the market attacks in the literature are performed on state estimation [5].

As shown in Figure 1.1, attackers perform a MITM attack to compromise data streaming between the control center and local RTUs. In this way, the raw measurement from RTU is modified by the attacker, which change the estimated grid states. For example, by manipulating the estimated line flow, the congestion pattern is compromised. The Lagrangian multiplier associated with the compromised line is changed to 0 or from 0 to a positive number, and thus LMPs are compromised. There are also other attack paths in the literature: the market participant interfaces where generators and loads submit bids and offers [6], communication at the demand side [7] and line limit information manipulation [8]. In general, most of the market-clearing parameters has the possibility of being attacked based on previous literature.

### *1.1.2 How to Gain Profit*

To gain profit from the electricity market, the attackers have to participate in market operation. However, owning a generation resource or cooperating with the generator company may increase the possibility of revealing attackers' identity. Therefore, a virtual bidding transaction best fits the attackers’ needs. Virtual bidding is an arbitrage from the DA market to the RT market to increase liquidity in market operations.

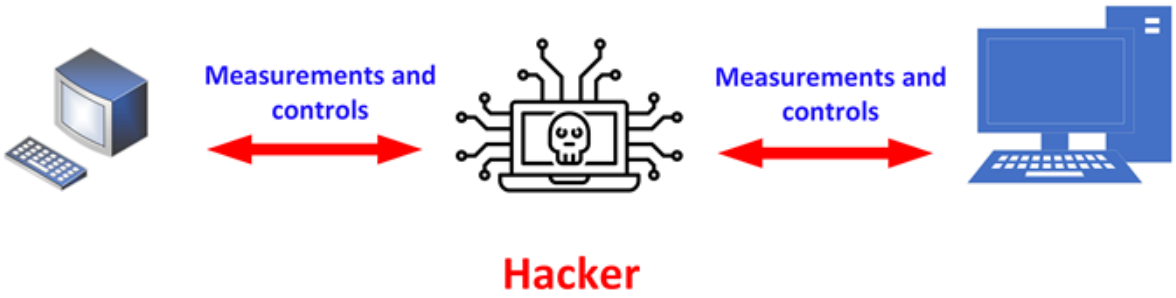


Figure 1.1: MITM attack between RTU and control center.

Normally, three types of virtual bidding are offered in the U.S.: increment offers (INCs), decrement bids (DECs), and UTCs [4]. In an INC, the bidder sells a certain amount of power at a node in the DA market and buys it back at the RT market. This trade is profitable when the DA LMP exceeds the RT LMP. Virtual bidding is a purely financial transaction that requires no physical power delivery or consumption. Thus, virtual bidding is the preferred way for an attacker to gain profit. LMPs are in general not fully manipulatable by attacks [5], but the created price difference can guarantee attackers' profit if the following conditions are satisfied [4].

1): Careful selection of bus A and B in the DA market (1.1). $LMP^{A}_{DA}$ and $LMP^{B}_{DA}$ represent the value of LMP at bus A and bus B in DA market.

$$(LMP^{A}_{DA} - LMP^{B}_{DA}) \geq 0 \tag{1.1}$$

2): For lines whose generation shift factors satisfy that $GSF_{l-A} > GSF_{l-B}$, those lines are modified to non-negative congested lines (1.2). $\kappa^{+}_{l}$ and $\kappa^{+}_{l}$ represent the Lagrangian multiplier of the transmission limit constraint.

$$\sum_{l=1}^{N_L} (k^{+}_{l} - k^{-}_{l}) \geq 0 \tag{1.2}$$

3): For lines whose generation shift factors satisfy that $GSF_{l-A} < GSF_{l-B}$, those lines are modified to non-positive congested lines (1.3).

$$\sum_{l=1}^{N_L} (k^{+}_{l} - k^{-}_{l}) \leq 0 \tag{1.3}$$

### *1.1.3 How to avoid detections*

Measurements transmitted from RTUs are imperfect due to the finite accuracy of meters or telemetric systems. With sufficient redundancy of measurements, a typical module of bad data detection is expected to filter out the errors. Therefore, the injected attack vector could be identified by the bad data detection module. Avoiding bad data detection is commonly considered in electricity market attack strategies [5]. The largest normalized residual test is a prevailing model for bad data detection to find the anomalies in a measurement set. The difference $r$ between estimated measurement data $z$ and raw measurement data $\tilde{z}$ is calculated in (1.4). Then, (1.5) describes the relation between residuals and errors, where $H$ is the system topology matrix and $R$ is the weighting matrix. The obtained residuals are normalized by (1.6) and (1.7). If the calculated $r_i^N$ exceeds a certain threshold (1.8), the measurement $i$ is identified as bad data.

$$r = z - \tilde{z} \tag{1.4}$$

$$r = (I - H(H^T R^{-1} H)^{-1} H^T R^{-1})(h(x) + e) \tag{1.5}$$

$$S = I - H(H^T R^{-1} H)^{-1} H^T R^{-1} \tag{1.6}$$

$$r_i^N = \frac{r_i}{\sqrt{S_{ii} R_{ui}}} \tag{1.7}$$

$$\left\| r_i^N \right\|_2 > threshold \text{"} i \hat{I} M \tag{1.8}$$

To avoid detection, the additional residual *res* induced by FDIAs, as in (1.9), needs to be controlled. Thus, if the resulting $r^N$ is less than a threshold, the attack is assumed to be undetectable.

$$res = (I - H_{act}(H'_{act} R^{-1} H_{act})^{-1} H'_{act} R^{-1}) z_a \tag{1.9}$$

### *1.1.4 Impact of power market cyberattacks*

The profit-targeting FDIAs on the energy market bring financial arbitrages to some market participants. However, such FDIAs are detrimental to the overall market operation, regardless of the profit-targeting objective for some participants. For example, in [4], the congestion price is controlled by manipulating the congestion patterns. Thus, the compromised congestion price between certain nodes creates profits for targeted market players. However, the change of congestion prices inevitably changes the LMPs at other nodes. Some normal market players may suffer from a significant loss, and some normal market players may receive a "free-ride" profit due to the FDIA. However, social-welfare suffers from an inevitable loss because the FDIA deviates the financial settlement from the original equilibrium. Further, in [9] and [10], the topological information is manipulated by the attacker which causes price deviations. Although the physical topology is unchanged, the compromised topology information induces erroneous generation dispatches, which may cause transmission line physical overload and outage. In [11], the load side management is compromised to manipulate LMPs. An erroneous load forecast or demand response induces excessive ancillary services, which not only diminishes social-welfare but also delivers incorrect signals for contingency analysis.

Market operation is a crucial part of supporting an economical and reliable grid operation. Although the intended impact of profit-targeting FDIAs is only to create profits for the targeted market players, the influence on market settlements leads to a chain reaction in the system. Therefore, the impact of such FDIAs is not limited to the profitability of certain market players. Profit-targeting FDIAs could induce catastrophic consequences in grid operations both financially and physically.

## 1.2 State-of-the-art

Many works have investigated the impact of cyberattacks on the electricity market. We briefly summarize and analyze the state-of-the-art works according to their research directions in this section. Major research directions are identified, and are shown in Figure 1.2.

### *1.2.1 Attacker and defender interaction*

The attacker's goal is to compromise market prices while the control center tries to identify and mitigate the attacks. Thus, the interaction between an attacker and a control center (defender) is intrinsically a zero-sum game. Reference [12] models the Nash equilibrium of the attacker and defender where the attacker and defender compete to increase/decrease the power flow from state estimation. Attackers and defenders are assumed to have a mixed strategy where the players randomly select moves. Further, instead of assuming that the attacker and defender act simultaneously, in [13], the dynamic interaction is further modeled through multiact dynamic game theory. The zero-sum game models the interaction of a single attacker and a single control center well. A more realistic setting can be provided by further modeling multiple attacker players and a defender player.

### *1.2.2 Imperfect topology information*

If the system topology is known, the extra residual induced by FDIAs can be reduced to zero by modifying the attack vector. However, the system topology is extensive and volatile, and the attacker is unable to have the full topology information.

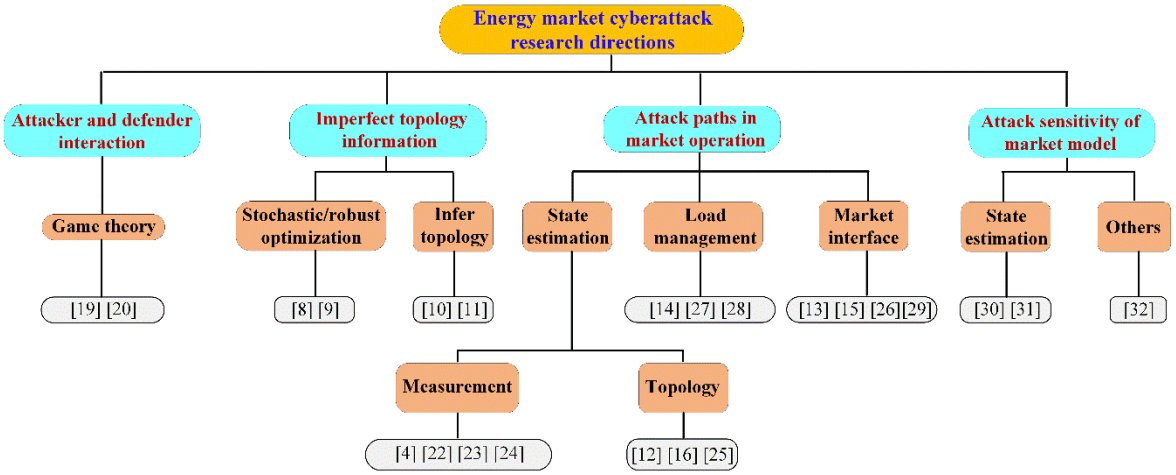


Figure 1.2 A schematic picture of cyberattack research directions in electricity markets

Under this scenario, attacks are more likely to be detected by bad data detection. Some works launch profitable attacks without full grid information. In [14], an independent component analysis (ICA) is applied to infer the topology matrix. With enough observation of measurement vector, each element in topology matrix is estimated. In [15] and [16], the attacker is assumed to have partial access to topology information. To ensure profitability under the topology information uncertainty, [15] proposes a robust FDIA to guarantee worst-case profits. [16] further models FDIAs through stochastic programming, where the bad data detection criterion is modified to a chance constraint, which means the possibility of passing bad data detection is larger than confidence level. The overall attack procedure is similar to attack strategies that have full information, but solving the chance constraint requires model reformulation and more computations. In [17], the attack vector is constructed without inferring topology matrix. The subspace of topology matrix is tracked by measurement data, and thus as long as the attack vector lies in the subspace of topology matrix, the residual is controlled within the threshold. The above works focus on utilizing mathematic techniques to infer grid information or construct the attack vector by analyzing the relation between the state estimation and attack vectors. Reference [18] provides a new path in which the topology matrix is inferred by observing successive RT LMPs.

### *1.2.3 Congestion pattern attack*

Congestion pattern modification is the most commonly referred attack strategy in market cyberattacks. Reliving congested line is generally more practical than congesting a uncongested line. 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. Such modification of the congestion pattern changes RT LMPs. In [19], both the financial gains and the possible blackout caused by modifying congestion patterns are discussed. In [20], an attacker adds or removes a transmission line from a contingency list to affect SCED. In [22], bogus trading in the DA market is combined with congestion pattern modifications to generate profit. [23] presents an attack strategy which not only avoids bad data detection but also maximizes profits.

### *1.2.4 Topology attack*

Similar to congestion pattern attacks, the topology attack modifies the digital information of break or switch status sent to topology processors. Thus, the optimal power flow (OPF) calculation is significantly altered. Different from congestion pattern attacks which normally relieve line congestions, topology attacks can add or switch off lines. From a market-clearing perspective, congestion pattern attacks take away particular line limits, but topology attacks change the generation shift factors. Therefore, the topology error can cause more damage than the congestion pattern attack. Current topology attack strategies focus on damaging market operations and social welfare. Profitable topology attack strategies considering the altered dispatch are an area for future research. The topology attack literature is reviewed as

follows to provide insights for further developments. The economic impact of adding, removing and switching a line in a topology processor is provided in [10]. [24] combines the virtual bidding and topology attack to quantify economic impact. In [25], topology attacks and general FDIAs are combined to disturb the Australian electricity market LMP calculation, and the huge financial loss caused by such an attack is demonstrated.

### *1.2.5 New attack paths*

Other than traditional attack strategies like modifying the breaker status or congestion pattern, market attackers have shown other attack paths to gain illegal profit. In [12], a MITM attack is performed to modify the bid information of load aggregators and generator companies. A load redispatch (LR) attack compromises only load measurement and line flow measurement to affect power generation, as proposed in [11]. [26] further applies the LR attack to produce desired congestion patterns, and thus the RT LMPs are controlled. Most existing RT market attack-related works perform an attack on the ex-post market while [27] innovatively formulates a FDIA applied at the very-short-term load forecasting. Thus, the ex-ante unit dispatch schedule is misguided, and the actual power generation is significantly affected which gives the corrupt generator owner benefits. Instead of focusing on compromising data streaming between a control center and RTUs, research work [7] investigates the possibility of attacking communication between responsive demand and aggregators to disturb RT LMPs. In [28], the inter-temporal generator ramping constraint is compromised to withhold generator capacity. In this scenario, look-ahead dispatch is applied instead of static SCED. The extra dual variables associated with the ramping constraint inevitably influence the LMPs, and thus modifying the ramping limit achieves a similar

effect when modifying the congestion pattern. In [10], the transmission line ratings, namely the lower/upper bounder of line flow constraints, are compromised to manipulate the profit of market players.

### *1.2.6 Sensitivity analysis*

Performing cyberattacks or defending cyberattacks on the electricity market is a complicated task. An attacker prefers to inject as small of an amount of bad data as possible or compromise as few sensors as possible, but generate a monetary gain as large as possible. Similarly, a defender wishes to protect sensors and mitigate attacks with the least amount of effort. To balance this trade-off, sensitive analysis is paramount to potential attackers and defenders. Research work [29] derives the mathematical representation between the congestion cost and topology errors, and thus the topology errors' impact on LMPs is formulated. In [30], both the error in system state and topology impact on LMPs are analyzed. It is shown that LMPs experience more variation if a topology error is combined with bad meter data. Research [31] quantifies LMP sensitivity over bad meter data and shows that the buses with the highest sensitivity are most likely to be of interest to a potential attacker.

## 1.3 Dissertation Outline

Chapter 2 shows the market-level signal can be an easy-to-detect signal of abnormality due to cyberattacks. We build a detection strategy based on the concept of critical load level (CLL) to help operators identify risky periods when operators would be prone to overlooking abnormal LMPs. Further, we construct a new type of cyberattack strategy capable of 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. The goal of this chapter is to demonstrate the necessity of considering market-level behavior in both intrusion and detection strategy development.

Chapter 3 identifies that there is a lack of cyber-vulnerability analysis (CVA) for power market, which hinders operators from systematically identifying potential threats from a cybersecurity perspective. Therefore, we propose a comprehensive CVA model for delivering a detailed analysis of four aspects of vulnerability: highly probable cyberattack targets, devastating attack targets, risky load levels, and mitigation ability under different degrees of defense. Users can simulate interactions between attackers and defending operators under different attack events.

Chapter 4 identifies that ISO revenue adequacy has not been analyzed under the context of cyberattacks. The lack of such analysis prevents ISOs from comprehensively assessing the financial consequences of market cyberattacks. Therefore, we explore the impact of FDIAs on real-time (RT) market operations on ISO revenue adequacy analytically and numerically. Four remarks are made on revenue adequacy under cyberattacks, and impact analysis model is developed correspondingly.

Chapter 5 extends the cybersecurity discussion in Chapter 1~4 to MES context. An optimal coordinated FDIA targeting MES is proposed. Then, a countermeasure to the proposed coordinated FDIA is developed to mitigate the damage based on DNNs. Operators are provided with a list of mitigation actions, which compromises between mitigation effectiveness and no-attack loss.

Chapter 6 concludes the work and provides directions for potential future work on power market cybersecurity and profit-targeting cyberattacks.

## 1.4 Contributions

The contributions of this work are listed as follow:

- This work proposes a market-level cyber defense strategy to discuss the necessity of considering market-level behavior in both intrusion and detection strategy development.
- This work presents a comprehensive cyber-vulnerability model for delivering a detailed analysis of four aspects of vulnerability: highly probable cyberattack targets, devastating attack targets, risky load levels, and mitigation ability under different degrees of defense.
- This work concludes four remarks on revenue adequacy issue under cyberattacks, and develops an impact analysis model to numerically analyze the revenue adequacy issue under cyberattacks.

# Chapter 2 Market-Level Defense Against FDIA and a New LMP-Disguising Attack Strategy in Real-Time Market Operations

Traditional cyberattack strategies on the electricity market only consider bypassing bad data detections during the state estimation stage. This chapter shows that abnormal locational marginal prices (LMPs) caused by cyberattack can be detected by experienced operators, because current cyberattack model ignores the characteristics of the LMP 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 operators detect abnormal LMPs. Further, this chapter constructs a new type of cyberattack strategy capable of not only bypassing bad data detection but also disguising the compromised LMPs as regular LMPs in a realistic scenario wherein the attacker has imperfect information on system topology. The proposed defense and attack strategy demonstrate the necessity of considering market-level behavior in both intrusion and detection strategy development. Finally, the developed works are evaluated through numerical studies on the PJM 5-bus system and the IEEE 118-bus system. More details of this chapter can be found in [87].

## 2.1 Introduction

As introduced in Chapter 1, 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 chapter discusses the necessity of considering market-level behavior, such as price signals, in both intrusion and detection strategy development. In particular, this chapter 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 chapter 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 chapter is organized as follows. Section 2.2 presents an overview of state estimation and electricity market models, as well as the concept of CLLs. In Section 2.3, 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 2.4, 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 2.5 presents the simulation results on the PJM 5-bus system and the IEEE 118-bus system. Finally, a conclusion is drawn in Section 2.6.

## 2.2 Preliminaries and Critical Load Levels

### *2.2.1 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.

The measurements of the studied power system are non-linearly dependent on state variables, as characterized in (2.1)-(2.3) where *z* and *x* denote an *m*-dimension measurement vector and an *n*-dimension state vector. In a system of *N* busses, 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.

$$\bar{z} = h(\bar{x}) + \bar{e} \tag{2.1}$$

$$\bar{x} = (x_1, x_2, \ldots, x_n)^T \tag{2.2}$$

$$\bar{z} = (z_1, z_2, \ldots, z_m)^T \tag{2.3}$$

The methodology of this model 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 (2.4) where $R$ is the variance matrix for all measurements.

$$J(\bar{x}) = \min \ (\bar{z} - h(\bar{x}))^T R^{-1} (\bar{z} - h(\bar{x})) \tag{2.4}$$

Then, the minimum is obtained under the first-order optimality condition (2.5), where $H_{es}$ is an m×n full rank matrix.

$$g(\bar{x}) = \frac{\partial J(\bar{x})}{\partial \bar{x}} = H_{es}^T R^{-1} (\bar{z} - h(\bar{x})) = 0 \tag{2.5}$$

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

$$H_{es} = \begin{vmatrix} \frac{\partial P_{inj}}{\partial q} & \frac{\partial P_{inj}}{\partial V} \\ \frac{\partial P_{l-l}}{\partial q} & \frac{\partial P_{l-l}}{\partial V} \\ \frac{\partial Q_{inj}}{\partial q} & \frac{\partial Q_{inj}}{\partial V} \\ \frac{\partial Q_{l-l}}{\partial q} & \frac{\partial Q_{l-l}}{\partial V} \end{vmatrix} \tag{2.6}$$

Expanding (2.5) with the Taylor series provides an iterative method for solving the non-linear function $g(x)$. As shown in (2.7), the estimated $x$ is updated at each iteration, until the norm of $\Delta x$ is smaller than a pre-specified threshold. The last iteration gives the estimation of system state $x^{\wedge}$. Thus, the estimated measurement vector is given by $h(x^{\wedge})$. Also, $G(x)$ is the gain matrix obtained by (2.8), and (2.7) is solved with LU decomposition.

$$G(\bar{x}^k)\Delta x = H_{es}(\bar{x}^k)^T R^{-1} (\bar{z} - h(\bar{x}^k)) \tag{2.7}$$

$$G(\bar{x}^k) = H_{es}(\bar{x}^k)^T R^{-1} H_{es}(\bar{x}^k) \tag{2.8}$$

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. Residuals are the difference between the estimated measurement data and the raw measurement data, as in (2.9). Following [32], the residual vector can be represented by a sensitivity matrix *S*, as shown in (2.10).

$$\bar{r} = \bar{z} - h(\bar{x}^{\wedge}) \tag{2.9}$$

$$S = I - H_{es}(\bar{x}^{\wedge})G(\bar{x}^{\wedge})^{-1}H_{es}(\bar{x}^{\wedge})^{T} \tag{2.10}$$

Then, the normalized residual is formed in (2.11).

$$r_i^N = \frac{r_i}{\sqrt{S_{ii}R_{ii}}} \tag{2.11}$$

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 (2.12), which is normally set to 3.0 for a 99.7% confidence level.

$$\left\| r_i^N \right\|_2 > threshold, \forall i \in M \tag{2.12}$$

### *2.2.2 Electricity Market Operations*

The two-settlement market mechanism (i.e. DA and RT markets) is widely adopted by U.S. ISOs [33]. An RT market is complementary to a DA market for correcting the deviation in DA generation dispatch. 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. In the ex-post model (2.13)-(2.17), generation scheduling is solved from the ex-ante model, while the LMPs calculated after the spot market cycle by an incremental model.

$$\min \sum_{i}^{N_g} c_i(\Delta P_{gi}) - \sum_{j}^{N_d} d_j(\Delta P_{dj}) \tag{2.13}$$

$$\sum_{i}^{N_g} \Delta P_{gi} = \sum_{j}^{N_d} \Delta P_{dj} \tag{2.14}$$

$$sP_{gi}^{\min} \le \Delta P_{gi} \le sP_{gi}^{\max} \tag{2.15}$$

$$\sum_{k=1}^{N_b} GSF_{l-k}(\Delta P_{gk} - \Delta P_{dk}) \le sF_l^{\max}, \forall l \in L^{+} \tag{2.16}$$

$$\sum_{k=1}^{N_b} GSF_{l-k}(\Delta P_{gk} - \Delta P_{dk}) \ge sF_l^{\min}, \forall l \in L^{-} \tag{2.17}$$

Where $\Delta P_{gi}$ is the output of the incremental generators, $\Delta P_{dj}$ 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, $\tau_1$, and $\tau_2$ which are associated with constraints (2.14), (2.16), and (2.17), as shown in (2.18). Further, the cost of the marginal loss term is set to zero in this study.

$$l_k = (1 - LF_{W,i})l - \sum_{l=1}^{L} GSF_{k-l}(t_1 - t_2), \forall k \in N_b \tag{2.18}$$

### *2.2.3 Critical Load Level*

The LMPs experience a step-change when a new constraint becomes a binding constraint [30]. 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 CLL interval is the distance between two CLLs. 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 [30]. As shown in Figure 2.1, 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 [35]. 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 $\Delta D_{\Omega}$ and the $i^{th}$ marginal unit incremental generation $\Delta MG_i$ is shown in (2.19)-( 2.20), where $f_i$ is the percentage of the $i^{th}$ bus incremental load compared to $\Delta D_{\Omega}$.

$$\sum_{i=1}^{N_{MG}} \left(\frac{\Delta MG_i}{\Delta D_W}\right) = 1.0 \tag{2.19}$$

$$\sum_{i=1}^{N_{MG}} (GSF_{k-i} \Delta MG_i) = \sum_{i=1}^{N} (GSF_{k-i} f_i) \Delta D_W \tag{2.20}$$

By solving (2.19)-(2.20), (2.21) is obtained. The linear equation is always solvable because the number of marginal units is equal to the number of congested lines plus one.

$$\frac{\Delta MG_i}{\Delta D_W} = p_i \tag{2.21}$$

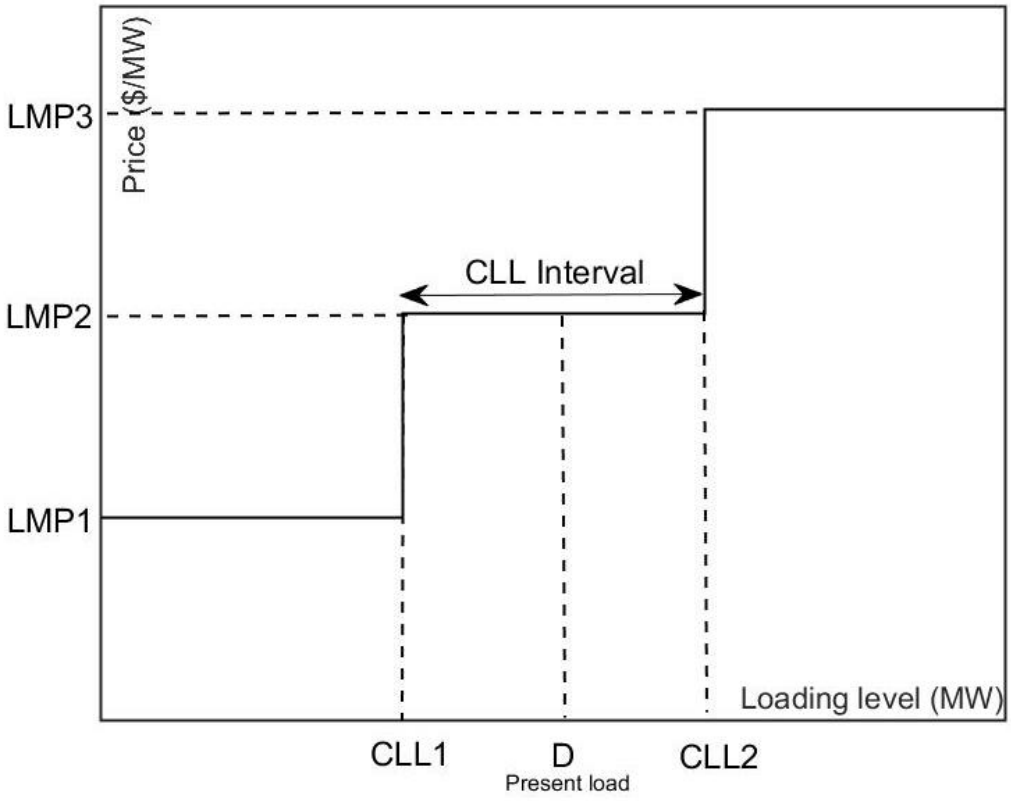


Figure 2.1 Critical load level.

If a line limit is the next binding constraint, the distance to the next CLL is calculated by (2.22). 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, $\partial D_{\Omega}$ is calculated, and the lowest one is the allowed load growth.

$$\Delta D_{W} = \frac{\lim it_l - \sum_{i=1}^{N_b} GSF_{k-i}(P_{gi} - P_{di})}{\sum_{i=1}^{N_{MG}} (GSF_{k-i}\, p_i) - \sum_{i=1}^{N} (GSF_{k-i}\, f_i)} \tag{2.22}$$

Similarly, if a generation limit is the next binding constraint, the distance to the next CLL is calculated by (2.23).

$$\Delta D_{W} = \frac{\Delta MG_i}{p_i} = \begin{cases} \dfrac{\Delta MG^{\max}_i - \Delta MG_i}{p_i}, if\, p_i > 0 \\ \dfrac{\Delta MG^{\min}_i - \Delta MG_i}{p_i}, if\, p_i < 0 \end{cases} \tag{2.23}$$

## 2.3 Abnormal LMP Detection Based on Risky CLL Intervals

Traditional attack strategies only consider bypassing bad data detections. 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.

### *2.3.1 Abnormal LMP Step Changes*

Figure 2.2 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 Figure 2.3. 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 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.

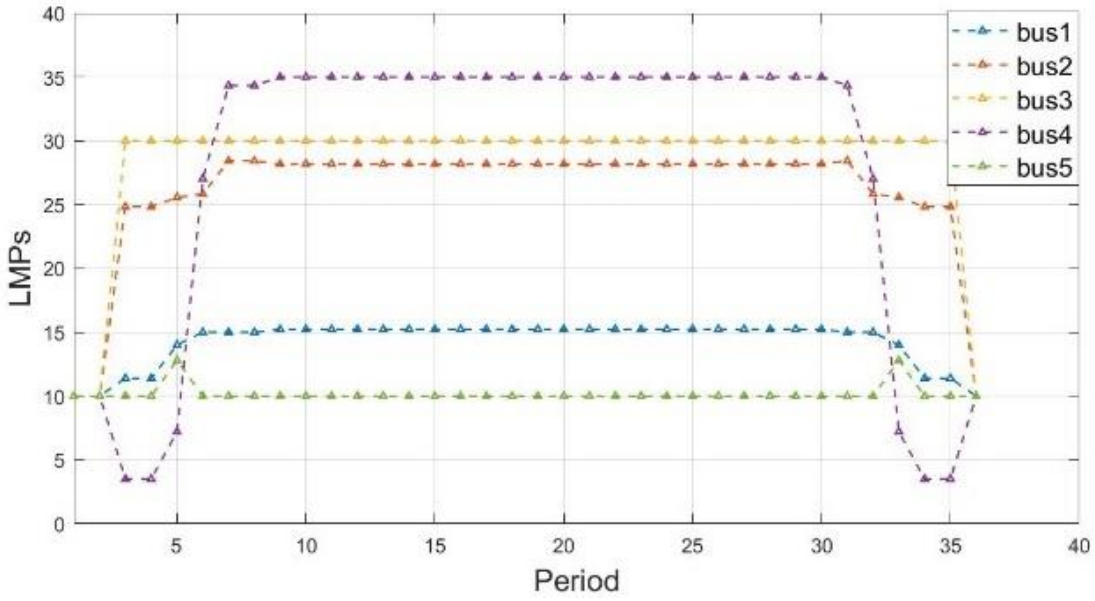


Figure 2.2 LMP for PJM 5-bus system without attack.

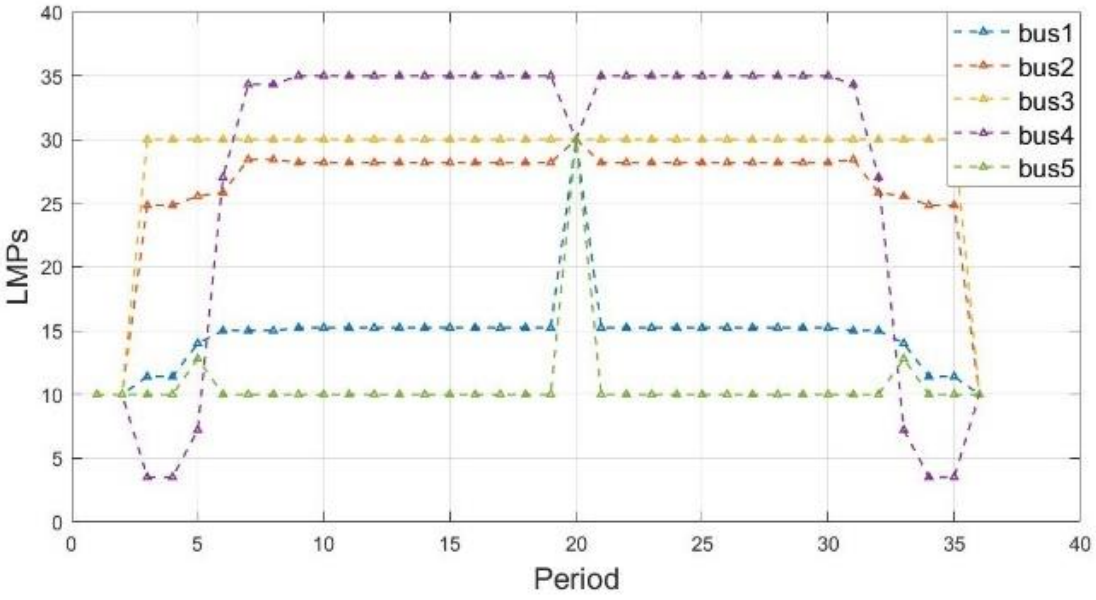


Figure 2.3 LMP for PJM 5-bus system with attack.

### *2.3.2 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 Figure 2.4, 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 (2.22) and (2.23) gives all CLLs for the system. Then the average distance between each CLL, $Dis_{ave}$, is calculated by (2.24), where $N_{dl}$ is the number of CLLs, $D_{max}$ is the largest CLL, and $D_{min}$ is the smallest CLL.

$$Dis_{ave} = \frac{D_{\max} - D_{\min}}{N_{cll} - 1} \tag{2.24}$$

The distance of the $i^{th}$ CLL interval, $Dis_i$, is obtained (2.25).

$$Dis_i = CLL_{i+1} - CLL_i, \forall i \in N_{cll} - 1 \tag{2.25}$$

A risky index $r_i$ is proposed to represent the percentage of the $i^{th}$ CLL interval compared with average distance as in (2.26).

$$r_i = \frac{Dis_i}{Dis_{ave}}, \forall i \in N_{cll} - 1 \tag{2.26}$$

If the length of a CLL interval is lower than threshold $\alpha$, then the CLL interval is identified as a risky CLL interval, as in (2.27). The corresponding risky periods are also identified as in (28). Other CLL intervals and periods are classified as safe intervals and safe periods.

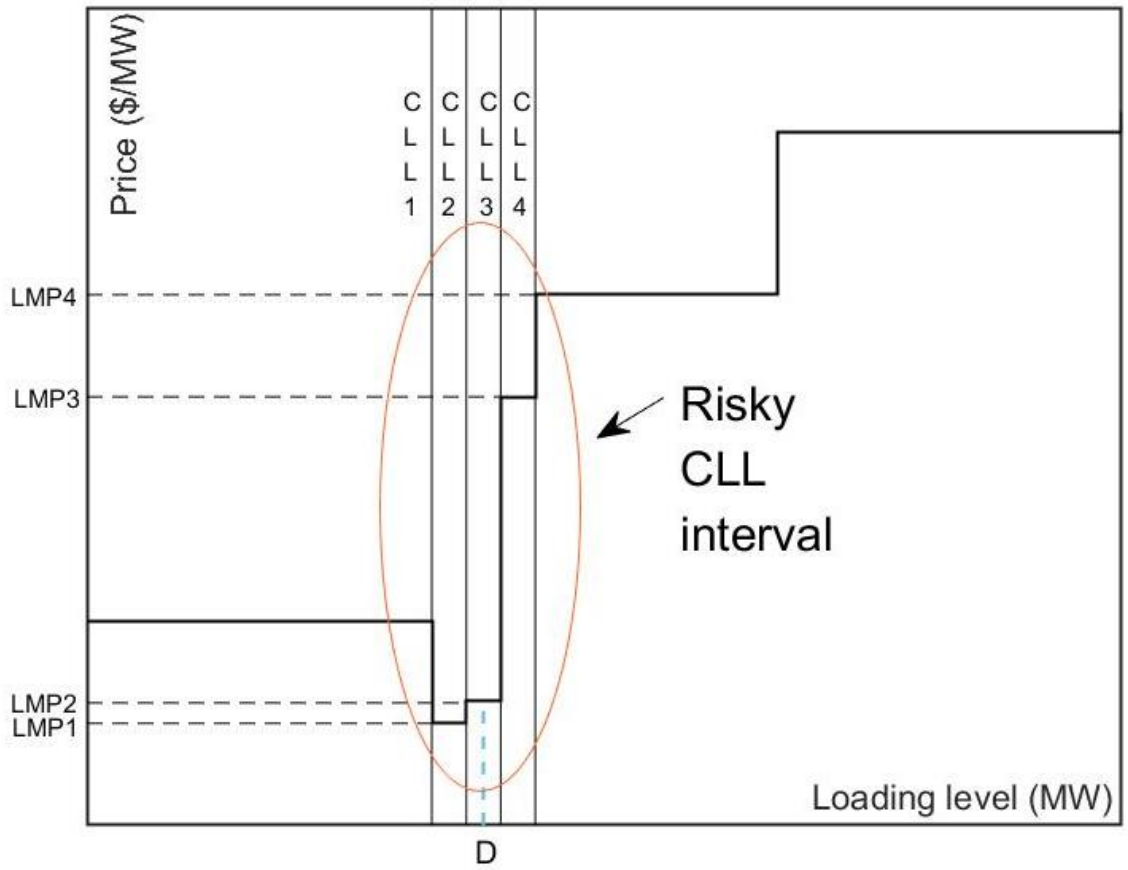


Figure 2.4. Illustration of risky CLL intervals.

$$CLL_{risky} = \{\text{CLL}_i, \text{"} r_i < a \text{"i Î } N_{cll}\} \quad (2.27)$$

$$T_{risky} = \{t, \text{ " Load}_t \text{ Î } CLL_{risky}\} \quad (2.28)$$

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 $\alpha$ is.

### *2.3.3 N-x cyber contingency analysis*

Intuitively, screening all load levels is preferred. However, a full set of different combinations is computationally expensive. Thus, *Subsection 2.3.2* 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 Table 2.1.

Throughout the Chapter, 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 Table 2.1 may be re-performed in the case that load distribution factors change significantly over the long term.

Table 2.1 Algorithm building contingency library

| | |
|---|---|
| **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) - (15) |
| 3 | **For** each possible combination **do** |
| 4 | Record target lines in this combination |
| 5 | **For** each target line *i* **do** |
| 6 | Remove $i^{th}$ line flow limit |
| 7 | **End for** |
| 8 | Solve the market-clearing model (11)-(15) |
| 9 | Record CLLs, congestion patterns, and LMPs |
| 10 | Add the recorded value to the library |
| 11 | **End for** |
| 12 | **End for** |
| 13 | **Return** the library |

In Table 2.1, $x$ 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 given by (2.29) where $C$ is the combination calculator.

$$N_c = \sum_{w=1}^{x} C_L^w \tag{2.29}$$

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 [36], 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 Figure 2.5. 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.

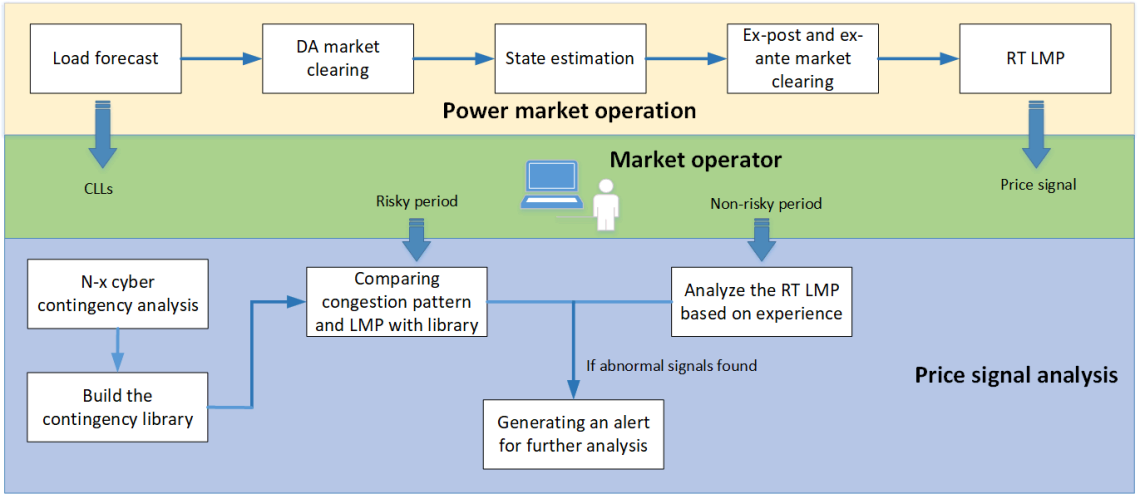


Figure 2.5 Detection procedures.

## 2.4 LMP-Disguising 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 subsection 2.4.1. subsection 2.4.2 and subsection 2.4.3 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 section 2.4.4. The overall attack model is constructed in subsection 2.4.5.

### *2.4.1 Limited Adversary*

In real market operations, system topology data is relatively secure from adversaries because the grid information is simply too extensive and volatile. In this Chapter, a limited adversary who has imperfect information about grid topology is assumed. Therefore, the real grid admittance model is approximated by attackers as in (2.30). The first term is the admittance matrix estimated by attackers. The second term, $\Delta y$, is the mismatch between the actual model and the one assumed by attackers. In this model, the mismatch $\Delta y$ is assumed to be independent and follows a Gaussian distribution.

$$Y^{act} = \begin{vmatrix} Y_{11} & \dots & Y_{1n} \\ Y_{n1} & \dots & Y_{nn} \end{vmatrix} + \begin{vmatrix} \mathrm{D}y_{11} & \dots & \mathrm{D}y_{1n} \\ \mathrm{D}y_{n1} & \dots & \mathrm{D}y_{nn} \end{vmatrix} \tag{2.30}$$

Then, the measurement Jacobian matrix $H_{es}$ is no longer deterministic. The elements corresponding to real power injection are shown in (2.31)-( 2.34) in which $g^{new}$ and $b^{new}$ are the real and imaginary parts of the elements in admittance matrix $Y^{act}$.

$$\frac{\P P_{inj}}{\P q_i} = \sum_{j=1, j \neq i}^{N} V_i V_j ((b_{ij}^{new} \cos q_{ij} - g_{ij}^{new} \sin q_{ij}) \tag{2.31}$$

$$\frac{\P P_{inj}}{\P q_j} = V_i V_j ((g_{ij}^{new} \sin q_{ij} - b_{ij}^{new} \cos q_{ij}) \quad (2.32)$$

$$\frac{\P P_{inj}}{\P V_i} = \sum_{j=1, j \neq i}^{N} V_j (b_{ij}^{new} \sin q_{ij} + g_{ij}^{new} \cos q_{ij}) \quad (2.33)$$

$$\frac{\P P_{inj}}{\P V_j} = V_i (b_{ij}^{new} \sin q_{ij} + g_{ij}^{new} \cos q_{ij}) \quad (2.34)$$

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:

a) 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;

b) The attacker has partial access to the measurement set. For example, (2.35) 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.

$$\bar{z}_{com} = \bar{z} + \bar{z}_a \quad (2.35)$$

### *2.4.2 Passing Bad Data Detection*

The mismatch $\Delta y$ also prevents the direct modeling of bad data detection constraint (2.10) in the attack model. The compromised measurement vector is input for the state estimation as in (2.36).

$$G_{se}^{act}(\bar{x}^{k})\Delta x = H_{se}^{act}(\bar{x}^{k})^{T} R^{-1}(\bar{z}_{com} - h_{se}^{act}(\bar{x}^{k})) \quad (2.36)$$

Then, similar to (2.36), a sensitivity matrix with uncertainty is formed in (2.37) where $x^{\wedge}$ represents the estimated system states.

$$S_{es}^{act}(\bar{x}^{\wedge}) = I - H_{es}^{act}(\bar{x}^{\wedge})G(\bar{x}^{\wedge})^{-1}H_{es}^{act}(\bar{x}^{\wedge})^{T} \quad (2.37)$$

The residual estimated by the attacker is modeled in (2.38) if an attack vector is applied in the raw measurement.

$$r = S_{es}^{act}(\bar{x}^{\wedge})\bar{z}_{a} \quad (2.38)$$

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 model, 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 (2.39).

$$P(\left\| r_{i}^{N} \right\|_{2} < thresh) \geq h \quad (2.39)$$

### *2.4.3 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 Figure 2.6, the compromised LMP from traditional attack strategies can be represented by the green or blue lines.

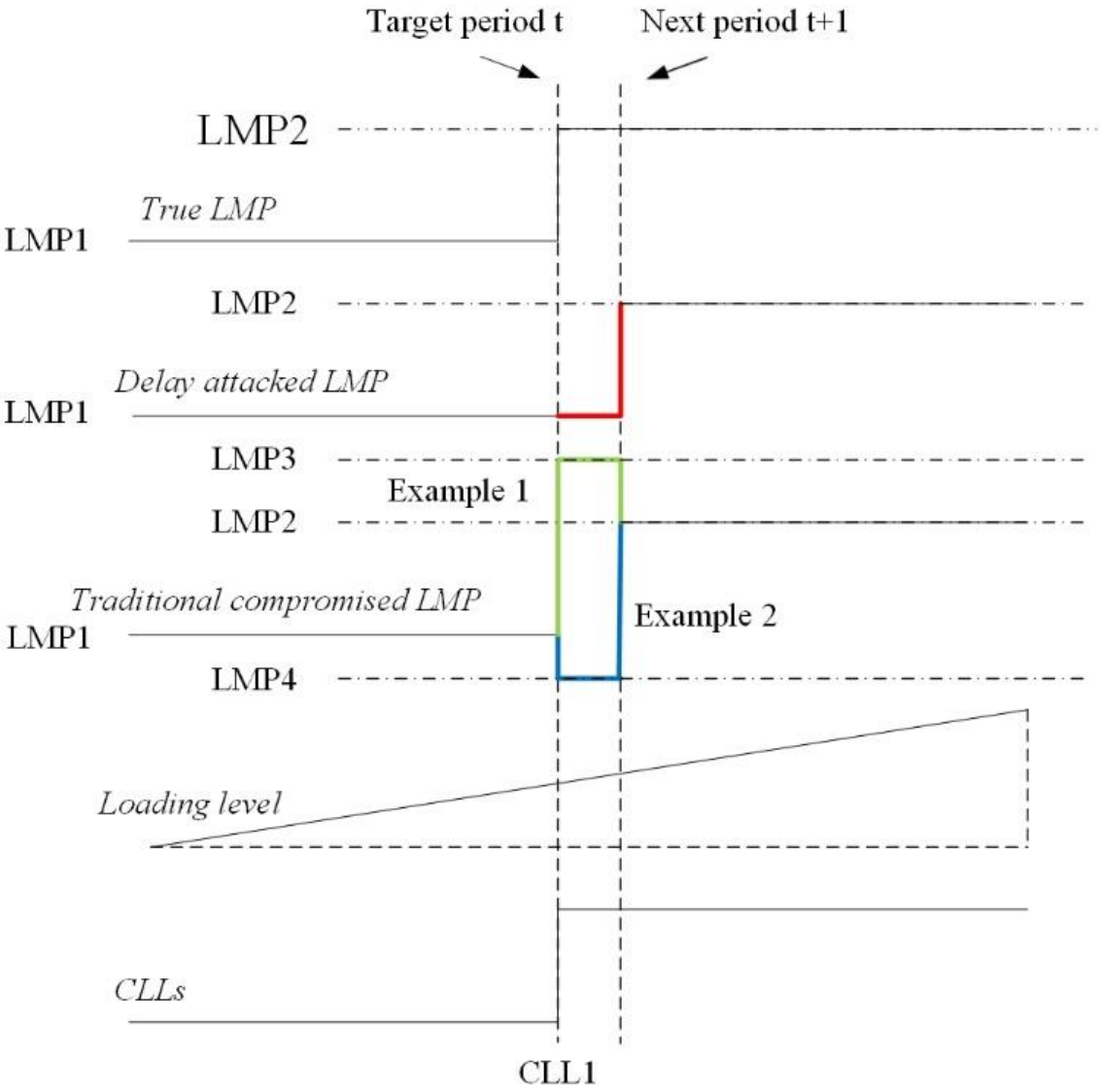


Figure 2.6 LMP-disguising attack and traditional attack.

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 *CLL1* 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 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 (2.40)-( 2.43) 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.

$$f_{l,t} - (I - H_{es}^{act}(\bar{x}^{\wedge})G(\bar{x}^{\wedge})^{-1}H_{es}^{act}(\bar{x}^{\wedge})^{\mathrm{T}})\bar{z}_a = f_l^{\min}, "l \hat{I} L_{- \min} \quad (2.40)$$

$$f_{l,t} - (I - H_{es}^{act}(\bar{x}^{\wedge})G(\bar{x}^{\wedge})^{-1}H_{es}^{act}(\bar{x}^{\wedge})^{T})\bar{z}_a < f_l^{max} \forall l \in L_{-max} \quad (2.41)$$

$$f_{l,t} + (I - H_{es}^{act}(\bar{x}^{\wedge})G(\bar{x}^{\wedge})^{-1}H_{es}^{act}(\bar{x}^{\wedge})^{T})\bar{z}_a = f_l^{max} \forall l \in L_{+max} \quad (2.42)$$

$$f_{l,t} + (I - H_{es}^{act}(\bar{x}^{\wedge})G(\bar{x}^{\wedge})^{-1}H_{es}^{act}(\bar{x}^{\wedge})^{T})\bar{z}_a > f_l^{min} \forall l \in L_{+min} \quad (2.43)$$

where $L_{+max}$, $L_{+min}$, $L_{-max,}$ and $L_{-min}$ are defined as in (2.44)-(2.47).

$$L_{+max} \leftarrow \{l \in \{f_{l,t-1} = f_l^{max} \text{ and } f_{l,t} < f_l^{max}\}\} \quad (2.44)$$

$$L_{+min} \leftarrow \{l \in \{f_{l,t-1} > f_l^{min} \text{ and } f_{l,t} = f_l^{min}\}\} \quad (2.45)$$

$$L_{-min} \leftarrow \{l \in \{f_{l,t-1} = f_l^{min} \text{ and } f_{l,t} > f_l^{min}\}\} \quad (2.46)$$

$$L_{-max} \leftarrow \{l \in \{f_{l,t-1} < f_l^{max} \text{ and } f_{l,t} = f_l^{max}\}\} \quad (2.47)$$

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.

### *2.4.4 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 (2.48). By substituting (2.18) into (2.48), (2.49) is further formulated.

$$Payoff = ((\mathrm{LMP}_i^{RT} - \mathrm{LMP}_j^{RT}) - (\mathrm{LMP}_i^{DA} - \mathrm{LMP}_j^{DA}))\,\mathrm{P}_{bid} \tag{2.48}$$

$$\begin{aligned} Payoff = {} & P_{bid} \sum_{l \in L_{-\max}} (\mathrm{GSF}_{l,i} - \mathrm{GSF}_{l,j}) p_l + \\ & P_{bid} \sum_{l \in L_{+\min}} (\mathrm{GSF}_{l,i} - \mathrm{GSF}_{l,j}) p_l - P_{bid} (\mathrm{LMP}_i^{DA} - \mathrm{LMP}_j^{DA}) \end{aligned} \tag{2.49}$$

If the following three conditions are satisfied, then the *payoff* is always positive, as can be deduced from (2.49). Here, conditions (2.50)-(2.52) are further modified to (2.53)-(2.55) to ensure a positive profit.

$$\mathrm{LMP}_i^{DA} - \mathrm{LMP}_j^{DA} < 0 \tag{2.50}$$

$$f_{l,t} > f_l^{\min} \forall l \in \{GSF_{l,i} - GSF_{l,j} > 0\} \tag{2.51}$$

$$f_{l,t} < f_l^{\max} \forall l \in \{GSF_{l,i} - GSF_{l,j} < 0\} \tag{2.52}$$

$$\mathrm{LMP}_i^{DA} - \mathrm{LMP}_j^{DA} < 0 \tag{2.53}$$

$$f^*_{l,t} > f_l^{\min} \forall l \in L_{+\min} \tag{2.54}$$

$$f^*_{l,t} < f_l^{\max} \forall l \in L_{-\max} \tag{2.55}$$

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.

### *2.4.5 Overall Attack Strategy*

Condition (2.53) is easily satisfied by carefully selecting bus *i* and bus *j*. However, from the attacker's perspective, $f_{l,t}$ follows Gaussian random distribution. Therefore, perfect satisfaction of (2.54) and (2.55) is not guaranteed. Hence, a confidence index $\varepsilon$ is introduced to maximize the likelihood of satisfying those conditions. Similar to (2.39), chance constraints are formulated as (2.56)- (2.57) where $\eta_a$ is the confidence level.

$$P(f^{*}_{l,t} > f_l^{\min} + e) \geq h_a \quad \forall l \in L_{+\min} \tag{2.56}$$

$$P(f^{*}_{l,t} < f_l^{\max} - e) \geq h_a \quad \forall l \in L_{-\max} \tag{2.57}$$

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

$$\max \ e \tag{2.58}$$

$$P(\left\|(I - H_{es}^{act}(\hat{\bar{x}})G(\hat{\bar{x}})^{-1}H_{es}^{act}(\hat{\bar{x}})^{\mathrm{T}})\bar{z}_a\right\|_2 < thresh_{\mathrm{W}}) \geq h_a \tag{2.59}$$

$$P(f^{*}_{l,t} > f_l^{\min} + e) \geq h_a \quad \forall l \in L_{+\min} \tag{2.60}$$

$$P(f^{*}_{l,t} < f_l^{\max} - e) \geq h_a \quad \forall l \in L_{-\max} \tag{2.61}$$

$$f^{*}_{l,t} = f_{l,t} + (I - H_{es}^{act}(\hat{\bar{x}})G(\hat{\bar{x}})^{-1}H_{es}^{act}(\hat{\bar{x}})^{\mathrm{T}})\bar{z}_a \quad \forall l \in L_{+\min} \tag{2.62}$$

$$f^{*}_{l,t} = f_{l,t} - (I - H_{es}^{act}(\hat{\bar{x}})G(\hat{\bar{x}})^{-1}H_{es}^{act}(\hat{\bar{x}})^{\mathrm{T}})\bar{z}_a \quad \forall l \in L_{-\max} \tag{2.63}$$

$$e > 0 \tag{2.64}$$

$$h_a h_a h_a \leq h \tag{2.65}$$

To solve the chance-constrained attack model, a scenario approximation method is applied to reformulate (2.58)-(2.65) as (2.66)-(2.73).

$$\max \ e \tag{2.66}$$

$$(I - H_{es}^{act}(\hat{\bar{x}})G(\hat{\bar{x}})^{-1}H_{es}^{act}(\hat{\bar{x}})^{\mathrm{T}})\bar{z}_a - Mz_i < thresh_{\mathrm{W}} \tag{2.67}$$

$$f^{*}_{l,t} - (f_l^{\min} + e) + \mathrm{M}z_j > 0 \quad \forall l \in L_{+\min} \tag{2.68}$$

$$f^{*}_{l,t} - (f_l^{\max} - e) - \mathrm{M}z_k < 0 \quad \forall l \in L_{-\max} \tag{2.69}$$

(2.51), (2.52)

$$\sum_{i=1}^{N} z_i \leq (1 - h_a)N \tag{2.70}$$

$$\sum_{j=1}^{N} z_j \leq (1 - h_a)N \tag{2.71}$$

$$\sum_{j=1}^{N} z_k \leq (1 - h_a)N \tag{2.72}$$

$$h_a h_a h_a \leq h \tag{2.73}$$

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 $\eta$, 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 (2.74)- (2.76).

$$z_i = 0 \Rightarrow (I - H_{es}^{act}(\hat{\bar{x}})G(\hat{\bar{x}})^{-1}H_{es}^{act}(\hat{\bar{x}})^{T})\bar{z}_a < thresh \tag{2.74}$$

$$z_j = 0 \Rightarrow f_{l,t}^{*} - (f_l^{\min} + e) + Mz_j > 0 \quad \forall l \in L_{+\min} \tag{2.75}$$

$$z_k = 0 \Rightarrow f_{l,t}^{*} - (f_l^{\max} - e) < 0 \quad \forall l \in L_{-\max} \tag{2.76}$$

Further, the residual calculations depend on the iterative solution of (2.36). For DC state estimation, the sensitivity matrix is fixed and independent of the system state.

$$S_{DC}(\hat{x}) = I - H_{es}^{act}G^{-1}H_{es}^{act} \tag{2.77}$$

Then, the attack model (2.66)- (2.73) 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 Figure 2.7.

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 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 Figure 2.8. 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.

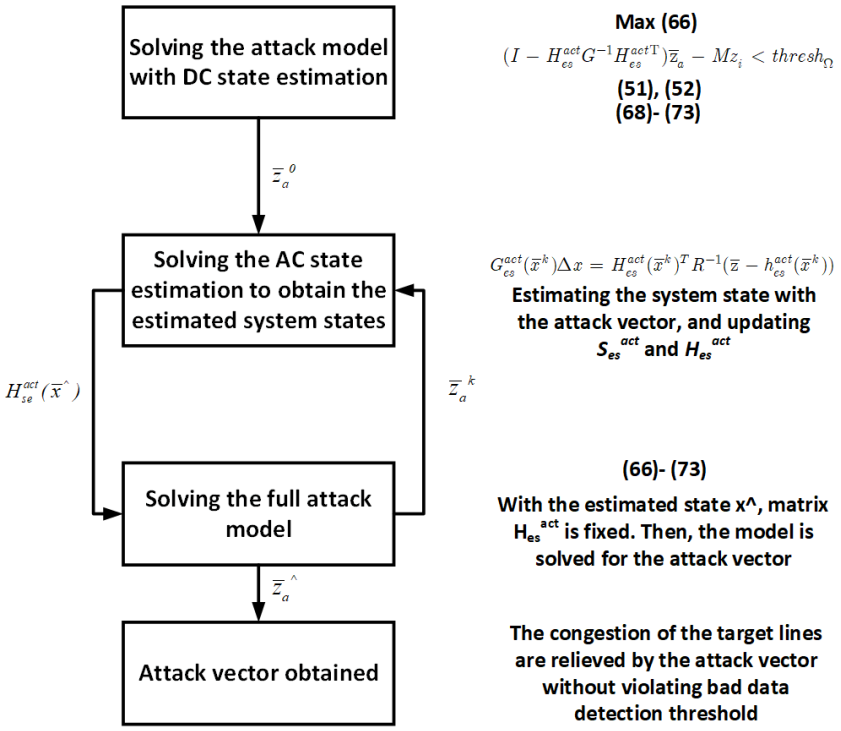


Figure 2.7 Iterative optimization process.

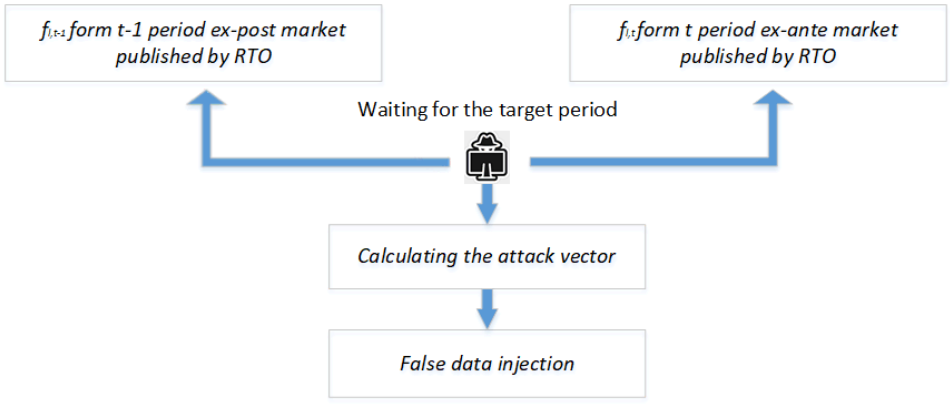


Figure 2.8 Proposed attack strategy procedures.

Then, the attacker waits for the target period, as discussed in subsection 2.4.3. Finally, the optimization model (2.59)-( 2.66) is solved to determine the FDIA amount and locations.

## 2.5 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 [37]. 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 [16].

### *2.5.1 Case 1: Proposed Analysis Method and Attack Strategy in a Small System: PJM 5-Bus System*

First, all CLLs are calculated as in Figure 2.9. The $\alpha$ index is defined to 1, and N-2 cyber contingency analysis is performed 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 Figure 2.2 and Figure 2.3, we have shown when operators are confident enough to detect attacks based on experience.

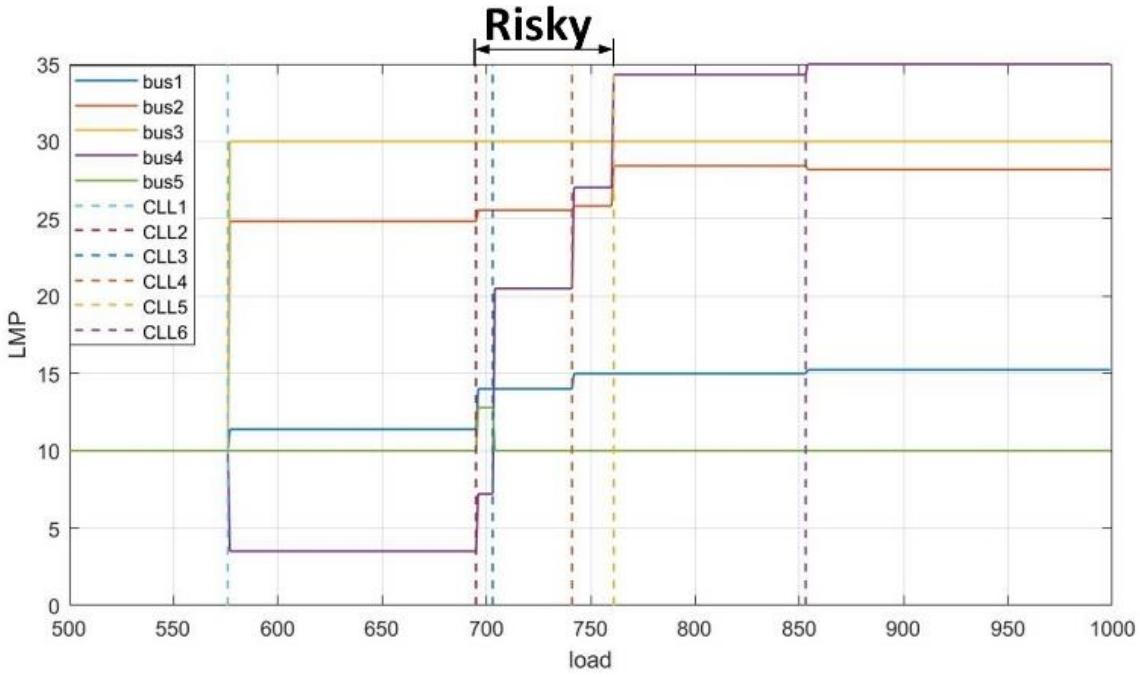


Figure 2.9 PJM 5-bus system CLLs.

Then, 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 Figure 2.10. 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.

**(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. A step change is observed at period 3. The attacker inputs this target line and desired confidence level (0.95) into the iterative process. 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 Figure 2.11, which looks very similar to the normal operation LMP in Figure 2.12. The difference is enlarged and shown in Figure 2.12. The solid line in Figure 2.12 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 2.2, the major reasons contributing to the detection of traditional attack strategies by operators' experience 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.

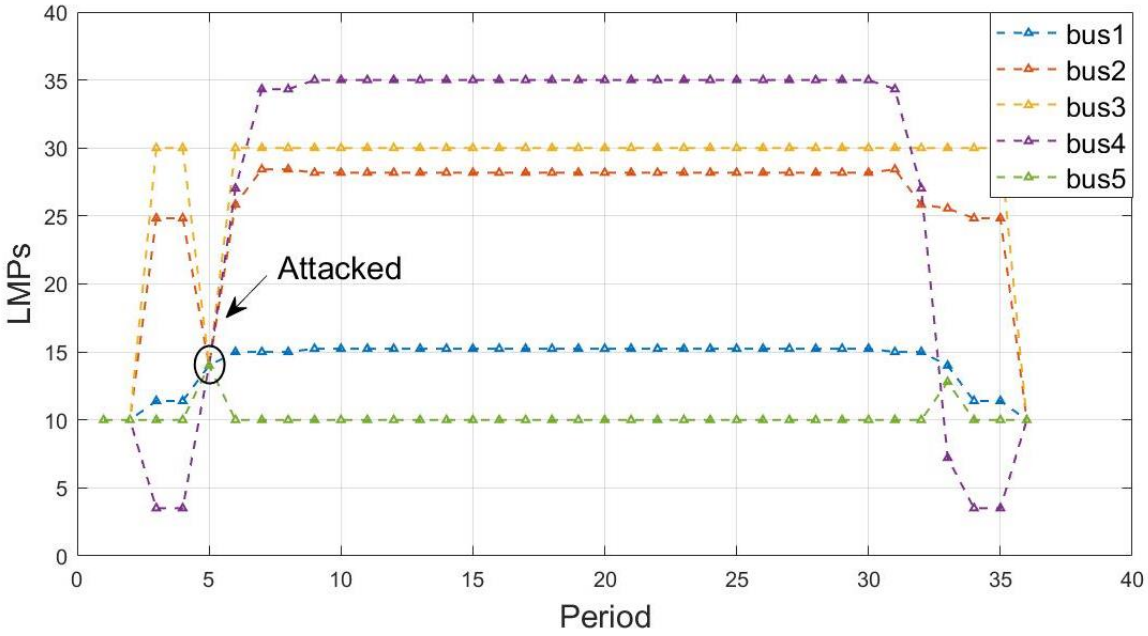


Figure 2.10 LMP for PJM 5-bus system traditional attack.

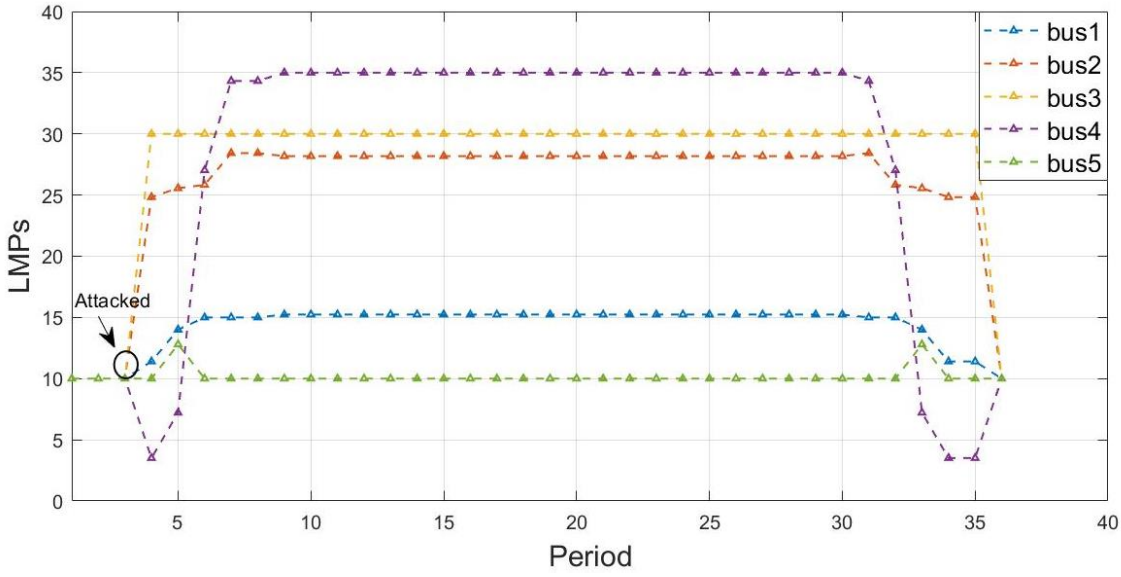


Figure 2.11 PJM 5-bus system LMP by the disguising attack.

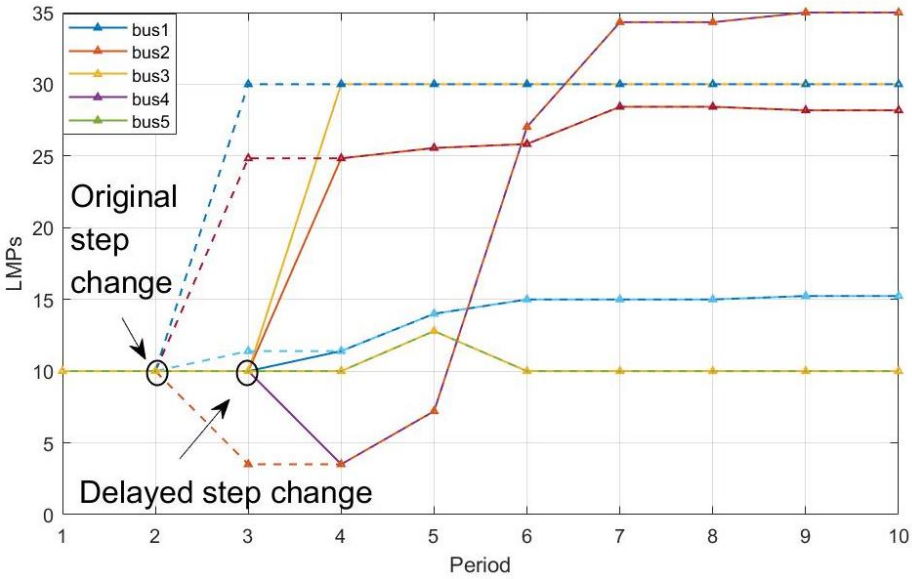


Figure 2.12. Attacked LMP comparison.

The disguising attack overcomes the above two problems, as shown in Figure 2.11: (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. Figure 2.13 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.

### *2.5.2 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 Figure 2.14. 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 Figure 2.15. 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.

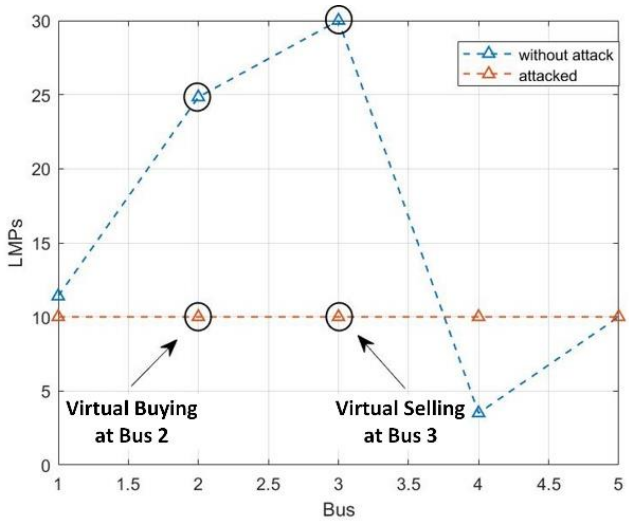


Figure 2.13 LMPs at target period.

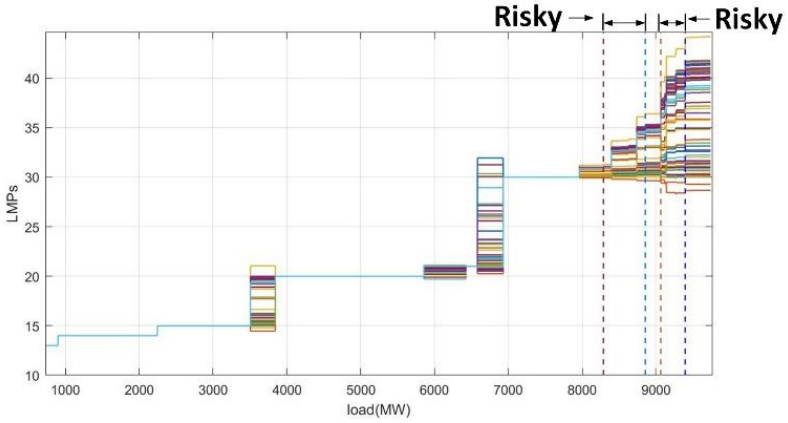


Figure 2.14 IEEE 118-bus system CLLs.

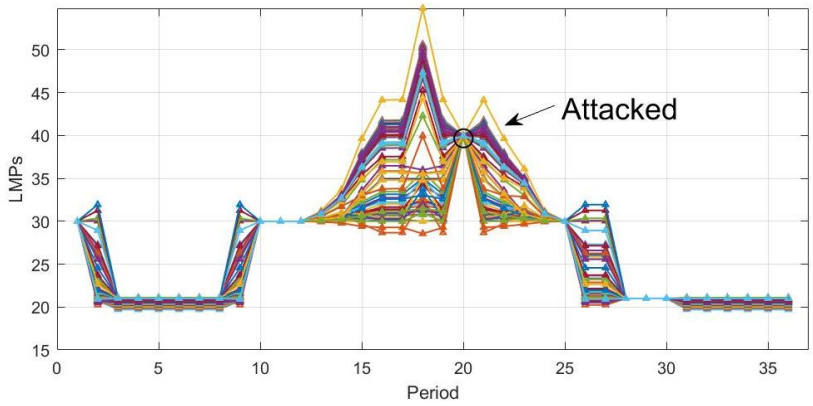


Figure 2.15 IEEE 118-bus system LMP by a traditional attack.

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.

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 Figure 2.16, and Figure 2.17 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.

Figure 2.18a and Figure 2.18b show 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.

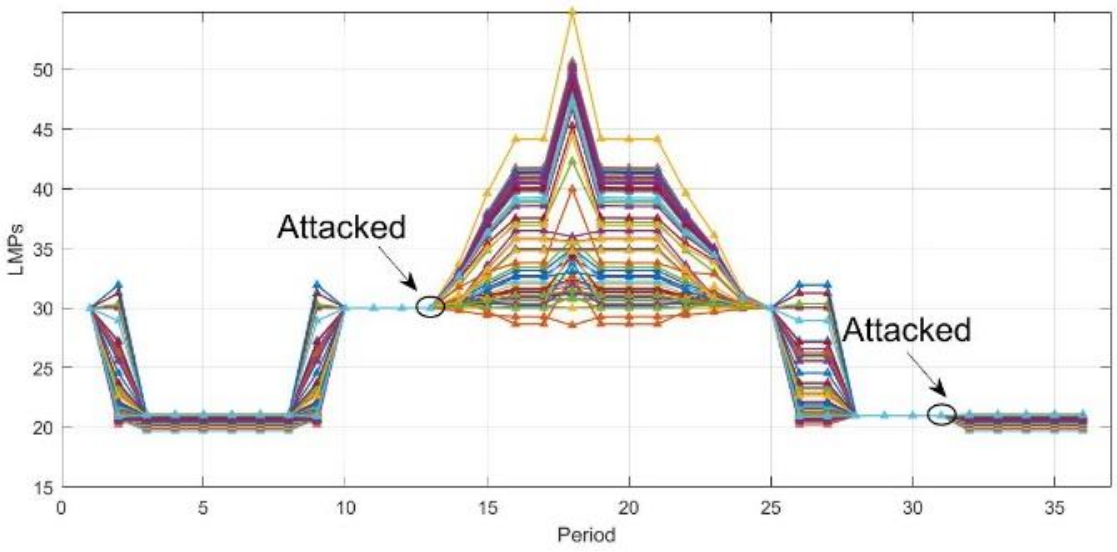


Figure 2.16 IEEE 118-bus system LMP without attack.

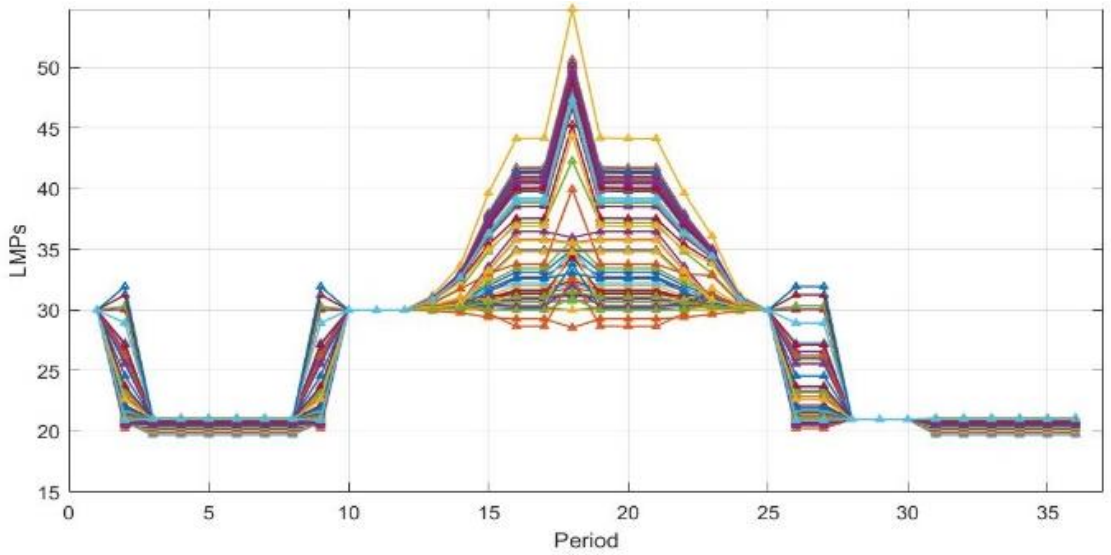


Figure 2.17 IEEE 118-bus system LMP by the disguising attack.

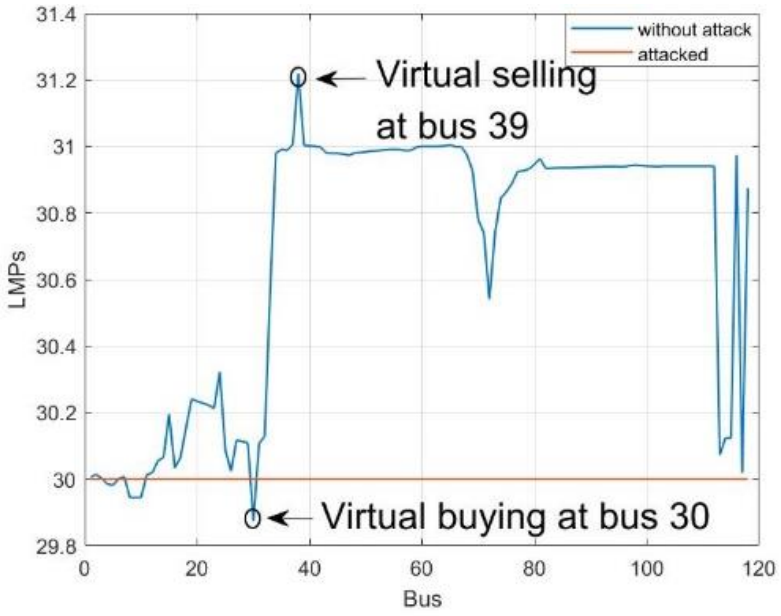


Figure 2.18a LMPs at target periods part a.

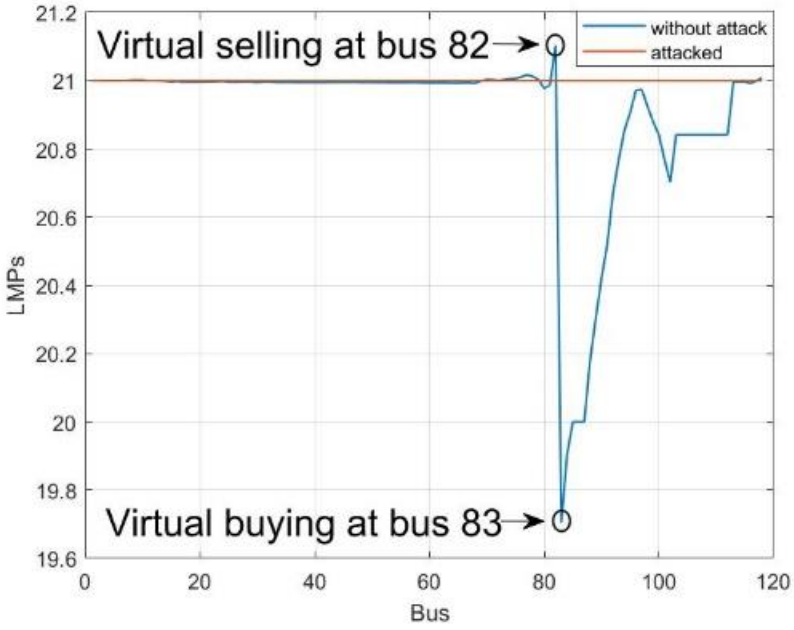


Figure 2.18b LMPs at target periods part b.

## 2.6 Summary

The key observation of this chapter 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 chapter 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.

# Chapter 3 Cyber-Vulnerability Analysis for Real-Time Power Market Operation

Existing market-targeting cybersecurity research has focused on developing attack strategies or detection schemes. However, the lack of cyber-vulnerability analysis (CVA) hinders operators from systematically evaluating the real-time (RT) market-clearing model and identifying potential threats from a cybersecurity perspective. This Chapter proposes a comprehensive CVA model for delivering a detailed analysis of four aspects of vulnerability: highly probable cyberattack targets, devastating attack targets, risky load levels, and mitigation ability under different degrees of defense. Users can simulate interactions between attackers and defending operators under different attack events, and the corresponding market settlements are also obtained. The proposed bi-level model is recast into mixed-integer linear programming through Karush–Kuhn–Tucker (KKT) conditions. A simulation study on an IEEE-30 bus system demonstrates the accuracy and effectiveness of the proposed CVA model. More details of this chaper can be found in [21].

## Nomenclature

*Lower level variables and parameters:*

*Parameters:*

| | |
|---|---|
| $C_i$ | Bidding prices of $i^{th}$ unit |
| $d_i$ | Load at bus $i$ |
| $P_i^{max}$, $P_i^{min}$ | Up and down generation limits for unit $i$ |

| | |
|---|---|
| $GSF_{l\text{-}i}$ | Generation shift factor which gives the fraction of a change in the injection at bus $i$ that appears on a branch $l$ |
| $L_i^{max}$, $L_i^{min}$ | Up and down transmission capacity for branch $i$ |
| $A_{df}$ | Defense degrees |

*Variables:*

| | |
|---|---|
| $P_i$ | Scheduled generation for unit $i$ |
| $V_l^+$, $V_l^-$ | Defense decision for congestion status of $l^{th}$ up/down line flow constraints |
| $V_i^b$, $V_i^d$, $V_i^p$ $V_l^{L+}$, $V_l^{L-}$ | Defense decision for bid of $i^{th}$ unit, load at $i^{th}$ bus, capacity of $i^{th}$ unit, up flow limit of $l^{th}$ branch, and down flow limit of $l^{th}$ branch |
| $N_i^b$, $N_i^d$, $N_i^p$ $N_l^{L+}$, $N_l^L$ | Defense value for bid of $i^{th}$ unit, load at $i^{th}$ bus, capacity of $i^{th}$ unit, up flow limit of $l^{th}$ branch, and down flow limit of $l^{th}$ branch |

*Upper level variables and parameters:*

*Parameters:*

| | |
|---|---|
| $A_{ak}$ | Attack degrees |
| $q_i^b$, $q_i^d$, $q_i^p$ $q_l^{L+}$, $q_l^{L-}$ | Penetration level of data manipulation in bid of $i^{th}$ unit, load at $i^{th}$ bus, capacity of $i^{th}$ unit, up flow limit of $l^{th}$ branch, and down flow limit of $l^{th}$ branch |

*Variables:*

| | |
|---|---|
| $M_i^b$, $M_i^d$, $M_i^p$ $M_l^{L+}$, $M_l^{L-}$ | Attack value for bid of $i^{th}$ unit, load at $i^{th}$ bus, capacity of $i^{th}$ unit, up flow limit of $l^{th}$ branch, and down flow limit of $l^{th}$ branch. |
| $\delta_l^+$, $\delta_l^-$ | Attack decision for congestion status of $l^{th}$ up/down line flow constraints |
| $B_i^b$, $B_i^d$, $B_i^p$ $B_l^{L+}$, $B_l^{L-}$ | Attack decision for bid of $i^{th}$ unit, load at $i^{th}$ bus, capacity of $i^{th}$ unit, up flow limit of $l^{th}$ branch, and down flow limit of $l^{th}$ branch |

*Lagrange multipliers:*

| | |
|---|---|
| $\lambda$ | Lagrange multiplier for power balance constraint |
| $\gamma_l^+$, $\gamma_l^-$ | Lagrange multipliers for up and down flow limits of $l^{th}$ branch |
| $\mu_i^+$, $\mu_i^-$ | Lagrange multipliers for upper and lower generation limits of $i^{th}$ unit |
| $\alpha_{l,j}^+$, $\alpha_{l,j}^-$, $\alpha_{i,j}^+$, $\alpha_{i,j}^-$ | Lagrange multipliers for the 1st reformed defense mitigation limits constraints |
| $\kappa_{l,j}^+$, $\kappa_{l,j}^-$, $\kappa_{i,j}^+$, $\kappa_{i,j}^-$ | Lagrange multipliers for the 2nd reformed defense mitigation limits constraints |
| $\beta$ | Lagrange multipliers for defense ability constraint |

*Parameters and variables for reformulations:*

*Parameters*

| | |
|---|---|
| $Q_m$, $Q_s$, $Q_g$ | *Big numbers with* $Q_g >> Q_m$ |
| *Variables* | |
| $\delta_l^+\_V_l^+$, $\delta_l^-\_V_l^-$ | Binary variables represent $\delta_l^+ + V_l^+$, $\delta_l^- + V_l^-$ |
| $\delta_l^+\_V_l^+\_P_i$, $\delta_l^-\_V_l^-\_P_i$ | Continuous variables represent $(\delta_l^+ + V_l^+)\cdot P_i$, $(\delta_l^- + V_l^-)\cdot P_i$, |
| $\delta_l^+\_V_l^+\_M_i^j$, $\delta_l^-\_V_l^-\_M_i^j$ | Continuous variables represent $(\delta_l^+ + V_l^+)\cdot M_i^j$, $(\delta_l^- + V_l^-)\cdot M_i^j$, and $j \in \{p^+, p^-, d^+, d^-, b^+, b^-, L^+, L^-\}$ |
| $u_i^{p+}$, $u_i^{p-}$ | Binary variables for the reformed complementary slackness of generation capacity constraint of unit $i$ |
| $u_l^{L+}$, $u_l^{L-}$ | Binary variables for the reformed complementary slackness of $l^{th}$ flow limits |

## 3.1 Introduction

As discussed in Chapter 1, malicious communication breaches into power market operations could induce catastrophic consequences on fair financial settlements and reliable transmission services. Followed by the initial discussion of market-targeted cyberattacks presented in [4], the literature discussing various cyberattacks on power market operations is abundant. The three main directions of market-targeted cyberattack research can be summarized as: (1) developing new attack strategies, (2) developing new detection schemes, and (3) investigating the sensitivity of cyberattacks. In the first category, state estimation (SE) is the most popular intrusion path. In [22], a robust false-data injection attack (FDIA) on SE is designed to create a financial bias on market settlements along with bogus bids. In

[38], an undetectable parameter attack on the system model is designed for financial profit in market operations. In [25], a topology attack is combined with an FDIA to lead customers to pay a higher bill through undetectable price deviations. In [10], three new topology attacks on SE are developed to mislead both economic dispatch and reliable operation. Next, ref. [14] determines that the grid topology is too extensive to be known by attackers, and a new profitable attack method without prior information on grid topology is proposed. Similarly, imperfect topology information is dealt with via robust optimization and stochastic programming in [15] and [16]. Various new attack paths and scenarios on market operation have been identified: a transmission line rating attack [8], a ramping constraints attack [28], and very short-term load forecasting [27]. For the second category of market-targeting cyberattack research, developing new detection schemes, detecting cyberattacks on market operations mainly focuses on SE level protections. In [39], a least-budget defense algorithm is proposed to secure pre-selected sensors, leading to the failure of bad data detection attacks. Refs. [40] and [41] have focused on enhancing the bad data detection algorithm itself by investigating the statistical difference between the random noise and the FDIA. In the last category of market-targeted cyberattack research, the sensitivity of cyberattacks, sensitivities of SE manipulation on market-clearing results have been fully investigated. In [30] and [31], the sensitivity of locational marginal prices (LMPs) to bad meter data has been formulated, and buses with higher sensitivity are found prone to being attack targets. In [24], the mathematic representation for the sensitivity of profitability to topology data is investigated.

Various market cyberattacks and their corresponding defense strategies have been identified and demonstrated in existing research works. They generally focus on elaborating

the attack paths or specific strategies, for example, the attacker's injection of false data to SE which changes the congestion pattern to modify LMPs. However, from the market operators' viewpoint, no matter where the attack path lays, whether in SE or the market gateway, the potential targets in a market operation are as follows: unit bids, demand management, generation capacities, line ratings, and congestion patterns. Therefore, it is important for the market operator to identify the vulnerability among all those attack paths. To the best of our knowledge, no previous research has developed a comprehensive analysis model regarding the vulnerability of the electricity market model involving all potential attack objectives and targets. Therefore, this Chapter first provides an impact analysis model that emulates market-clearing under various cyberattacks, and then proposes a set of algorithms to identify the vulnerability from different aspects.

The detailed contributions of this Chapter are as follows:

- A comprehensive cyber-vulnerability analysis (CVA) model is proposed in which market data from all sources is assumed to be susceptible to attacks, including line ratings, congestion patterns, generation capacity withholds, market-interface, etc. Namely, all parameters in the ISO's market model are assumed to be attackable. Next, various attack objectives are categorized and considered. The market operator can apply the proposed model to perform impact analysis on market cyberattacks.
- Four specific impact analysis algorithms are proposed to identify the vulnerability of power market parameters comprehensively. The four proposed algorithms target four vital aspects of the vulnerability of power market parameters: (1) Vulnerability in terms of possibility: which attack paths are most likely to be attacked? (2) Vulnerability in terms of severity: which attack paths have the most impact on market operation? (3) Vulnerability

in terms of load level: at which load level are attacks more likely to occur? (4) Vulnerability in terms of defense strategies: how defense degrees impact the effectiveness of market cyberattacks?

The rest of this Chapter is organized as follows. Section 3.2 first presents the formulation of the proposed CVA model. Section 3.3 describes the proposed algorithms based on the CVA model in detail. In Section 3.4, the reformulation and linearization steps for solving the proposed model are presented. Section 3.5 conducts a detailed simulation study on an IEEE 30-bus system to demonstrate the effectiveness of the proposed vulnerability analysis. Finally, conclusions and future studies are discussed in Section 3.6.

## 3.2 Proposed Analysis Model on Market FDIAs

### *3.2.1 Preliminary on real-time (RT) market model*

Ex-ante and ex-post are two primary models for RT market-clearing. In the ex-ante model, generation dispatches and LMPs are calculated based on the forecasted conditions for the next trading period. Optimal generation dispatches are determined given the expected load and physical security constraints. The ex-post model is purely a price-setting model in which generation dispatches are determined via the ex-ante model, while the LMPs are calculated by the ex-post model. The proposed analytical model can be applied to both the ex-ante and ex-post models. The ex-ante model is applied here as an illustration, shown in (3.1)-( 3.5).

$$\min \sum_i C_i(p_i) \tag{3.1}$$

$$\sum_i P_i - \sum_i d_i = 0 \tag{3.2}$$

$$P^{\min}_i \le P_i \le P^{\max}_i, \forall i \in NG \tag{3.3}$$

$$\sum_{i=1}^{N_b} GSF_{l-i}(P_i - d_i) \leq L_l^{\max} \quad \forall l \in L \tag{3.4}$$

$$\sum_{i=1}^{N_b} GSF_{l-i}(P_i - d_i) \geq L_l^{\min} \quad \forall l \in L \tag{3.5}$$

The market-clearing price is composed of the Lagrange multipliers associated with (3.2)-( 3.5), as shown in (3.6).

$$LMP = l + \sum_{L} GSF_{l-i}(g_l^{+} - g_l^{-}) \tag{3.6}$$

### *3.2.2 Proposed CVA model*

The proposed analytic model provides a flexible platform to emulate different attack strategies and defense degrees under various assumptions. This section presents the construction of the CVA model. The CVA model contains an attacker and a defending market operator. The attacker wants to optimize its objective (e.g., LMP manipulations), then it anticipates the optimal response from the market operator. In this setting, the attack's optimization problem contains a nested optimization task that corresponds to the market operator's optimization problem. The defending ability is modeled for the impact analysis of defense degrees, which is clarified in detail in *Section 3.3.4*. Therefore, the proposed model is constructed as a bilevel optimization problem. The attacker modifies the parameters that impact the market-clearing result, and the market operator clears the market with defending variables, which in turn affects the attacker's objective. The overall structure of the proposed model for CVA is shown in Figure 3.1.

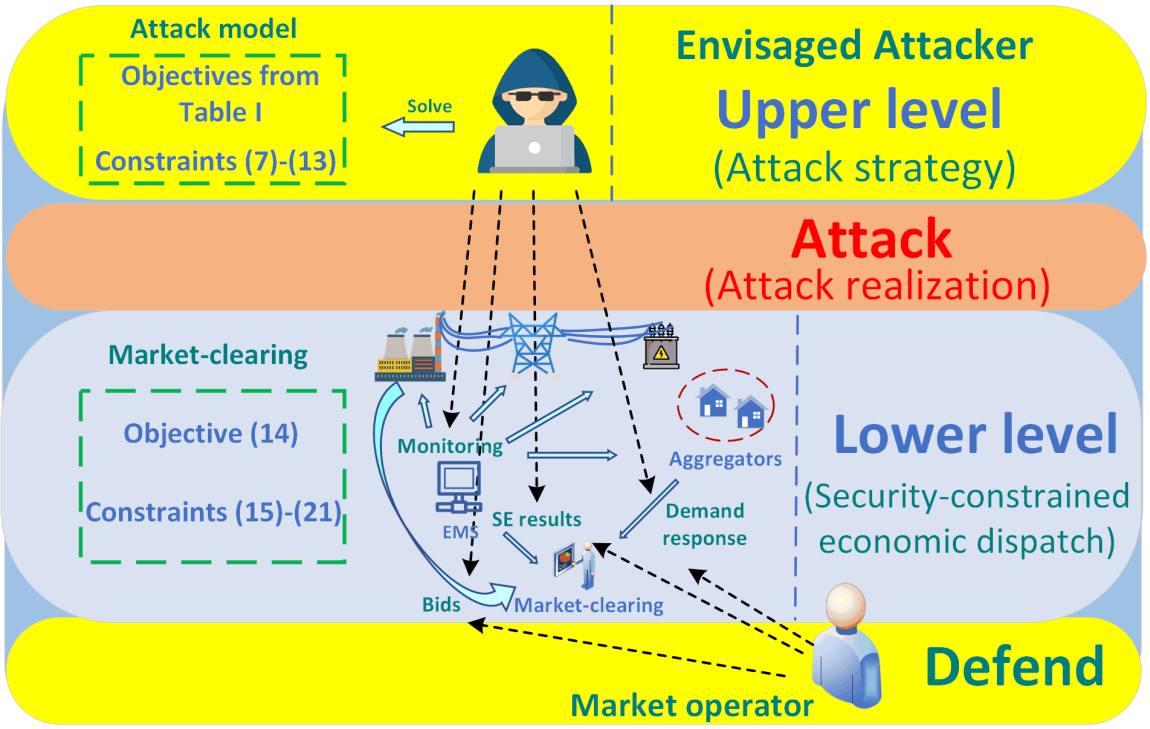


Figure 3.1 Proposed CVA model structure

**Upper level (attacker):**

Although most of the existing research assumes that attacks on the market are profit-driven, the purpose of cyberattacks on market operation varies from one attacker to another. Generally, potential objectives for power market cyberattacks can be categorized into three types: (1) financial settlements, (2) generation dispatches, and (3) transmission congestions. Therefore, the proposed model considers different attack objectives from each of the above categories, as shown in Table 3.1 to provide a general attack evaluation. The objective of the upper level model can be selected from Table 3.1 based on different analysis purposes, which are discussed in *Section 3.3*.

The upper level of the analysis model incorporates all potential attack targets in market operation. When the market operator solves a RT economic dispatch problem, data from multiple sources are used, including: (1) short term load forecasts and demand management from energy management systems (EMSs); (2) bidding prices and generator capacities from market gateway; and (3) congestion patterns and line ratings from EMSs. Therefore, to conduct a comprehensive analysis, all of the above data sources are assumed to be susceptible to attacks, as shown in (3.7)- (3.11). Although some parameters may not be easily compromised unless the cyber threats are from insiders, the proposed CVA model in this Chapter considers comprehensive scenarios to provide a general analytic framework for market operators to identify possible cyber vulnerabilities. Specific constraints and variables can be simplified or removed if decision makers consider these parameters to be perfectly secure. The maximum amount of those attacks is constrained by the penetration level value $q$ and the targets' original value.

Table 3.1 Potential attack objectives

| *Type* | *Objective* | *Model* |
|---|---|---|
| Financial settlements | LMP | $LMP_i$ |
| | Social-welfare | $\sum C_i(P_i)$ |
| Generation | Generation dispatch | $P_i$ |
| Transmission | Congestion price | $LMP_i - LMP_j$ |
| | Congestion pattern | $L$ |

$$- q_i^b c_i B_i^b \leq M_i^b \leq q_i^b c_i B_i^b, \ \forall i \in NG \tag{3.7}$$

$$- q_i^d d_i B_i^d \leq M_i^d \leq q_i^d d_i B_i^d, \ \forall i \in L \tag{3.8}$$

$$- q_i^p P_i^{\max} B_i^p \leq M_i^p \leq q_i^p P_i^{\max} B_i^p, \ \forall i \in NG \tag{3.9}$$

$$- q_l^{L+} L_l^{\max} B_l^{L+} \leq M_l^{L+} \leq q_l^{L+} L_l^{\max} B_l^{L+}, \ \forall i \in L_{d_l^+} \tag{3.10}$$

$$q_l^{L-} L_l^{\min} B_l^{L-} \leq M_l^{L-} \leq - q_l^{L+} L_l^{\min} B_l^{L-}, \ \forall i \in L_{d_l^-} \tag{3.11}$$

$$d_l^- + d_l^+ \leq 1, \ \forall l \in L \tag{3.12}$$

$$\sum_l d_l^- + d_l^+ + B^{L+}{}_l + B^{L-}{}_l + \sum_i B^b{}_i + B^p{}_i + B^d{}_i \leq A_{ak} \tag{3.13}$$

Constraint (3.12) means that congestion pattern attacks happen either at upper or lower limits because a line flow can either be on the upper or lower limit. The attacker degree is constrained in (3.13), which represents how many targets the attacker can compromise.

**Lower level (market operator):**

The market operator is placed at a lower level equipped with the capability to defend against attacks. The original economic dispatch model (3.1)-(3.5) becomes (3.14)-(3.18) with the considered attacks and corresponding defenses. To identify the critical attack path and defense efficiency, the defense degree is constrained in (3.19), which represents the number of attacks that can be defended against. Although operators want to defend against all possible attacks, there is always a recourse limit such that they have to defend against the attacks that they identify as most threatening. It worth noting that the defender knows where the attacker attacked in this bilevel formulation. However, the defender proposed analysis presented in this work is aimed at analyzing the effectiveness of the defense degree, which is explained in detail in *Section 3.3.4*. Equations (3.20) and (3.21) indicate that if an attack

is identified, then it is totally countered, and equation (3.22) shows the defense is only placed where the attack happens.

$$\min \sum_i (C_i + M_i^b - N_i^b)P_i \tag{3.14}$$

$$\sum_i P_i - \sum_i (d_i + M_i^d - N_i^d) = 0 \tag{3.15}$$

$$0 \le P_i \le P^{\max}_i + M_i^p - N_i^p, \ \forall i \in NG \tag{3.16}$$

$$(d_l^+ \mid V_l^{d+}) \sum_{i=1}^{N_b} GSF_{l-i}(P_i - (d_i - M_i^d + N_i^d)) \le L_l^{\max} + M_l^{L+} - N_l^{L+}, \ \forall l \in L \tag{3.17}$$

$$(d_l^- \mid V_l^{d-}) \sum_{i}^{N_b} GSF_{l-i}(P_i - (d_i - M_i^d + N_i^d)) \ge L_l^{\min} + M_l^{L-} - N_l^{L-}, \ \forall l \in L \tag{3.18}$$

$$\sum_i \sum_j V^j{}_i + \sum_l \sum_j V^j{}_l + \sum_l V^{d^+}{}_l + \sum_l V^{d^-}{}_l - A_{df} \le 0 \tag{3.19}$$

$$N_i^j = V_i^j M_i^j, \ \forall i \in N^b, \ \forall j \in \{d, p, b\} \tag{3.20}$$

$$N_l^j = V_l^j M_l^j, \ \forall l \in L, \ \forall j \in \{L^+, L^-\} \tag{3.21}$$

$$V_i \le B_i, \ \forall i \in \{d, p, b, L^+, L^-\} \tag{3.22}$$

The proposed CVA model is used to perform a vulnerability analysis from four different aspects, which will be elaborated in the next section.

## 3.3 The Capability of The Proposed Analysis Model

As discussed in the introduction, potential attack targets, risky operating conditions, and defense effectiveness are the most vital elements in developing a defense strategy. Therefore, the following four aspects are selected to construct the CVA model.

### *3.3.1 Identifying highly probable attack targets (Algorithm 1):*

Some parameters are compromised more frequently than others. For example, congestion patterns can be a vital attack route for both LMP manipulation and diminishing social-welfare. As shown in Figure 3.2, protection of the congestion pattern makes it hard for those two types of market attackers to achieve their desired goals. Therefore, in Algorithm 1, the CVA model is solved iteratively for all interested attack objectives, and the attack route for each attack objective is recorded. The frequently attacked parameters (routes) are identified as vulnerable parameters in terms of the probability of being attacked. Providing protection to the identified parameters diminishes overall attack interest in the market operation. Further, the attacker has different optimal attack routes when they have different attack degrees. Therefore, market operators can also identify vital attack routes under different attack degrees through Table 3.2 (*Algorithm 1*). The detailed procedure of this identification is shown in *Algorithm 1 HPA,* where HPA stands for "highly probable attack" analysis.

### *3.3.2 Identifying devasting attack targets (Algorithm 2):*

Different from highly probable attack targets (Algorithm 1), devasting attack targets vary from one attack objective to another. The attacks on one parameter could be more effective than the attacks on other parameters for a particular attack objective. As shown in Figure 3.3, modifying load information could be more effective than modifying line rating. Thus, protection of these attack targets largely diminishes the attackers' interest in a specific attack objective.

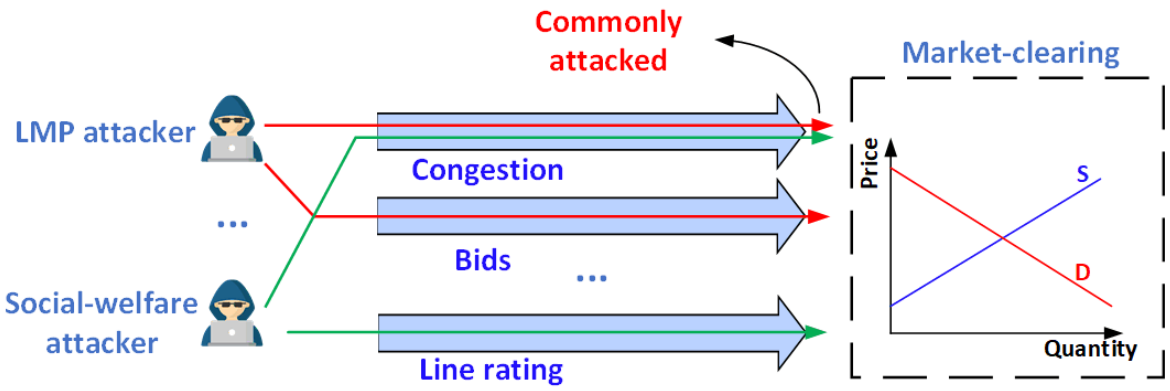


Figure 3.2 Identifying highly probable attack targets

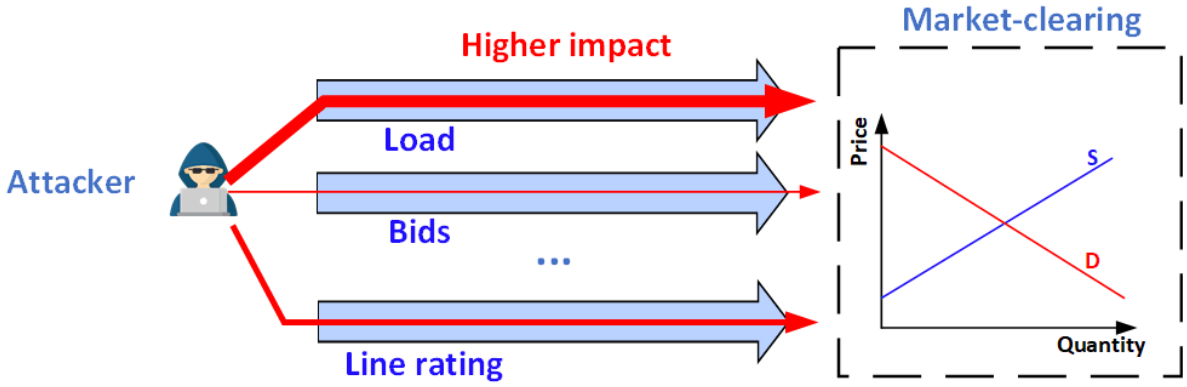


Figure 3.3 Identifying devasting attack targets

Table 3.2 Algorithm for highly probable attack targets identifications

| | |
|---|---|
| **Algorithm 1** | Function HPA (market parameters, attack objectives) |
| **Input** | Real-time market parameters and interested attack objectives |
| **Output** | Highly probable attack targets |
| 1 | **For** each possible attack degree **do** |
| 2 | **For** each attack objective in Table 3.1 **do** |
| 3 | Solving the CVA model (7) - (22) |
| 4 | Record the attack binary variable *B* for each target |
| 5 | **End for** |
| 6 | Sum variable *B* in all attack objectives for each target |
| 7 | **End for** |
| 8 | Identify targets that have high values of sum (*B*) |
| 9 | **Return** the Identified Targets |

It should be noted that an attack on the congestion pattern is not applicable to this algorithm because the congestion status is a binary variable that does not have a penetration level. Further, LMPs experience step changes regarding some attack routes, such as attacks in load levels, which means the LMP does not change until the modified parameter is large enough. For these attack scenarios, Table 3.3 (Algorithm 2) can identify the critical attack penetration level that leads to the step change. In Algorithm 2, the CVA model is solved iteratively with a gradual increase of the penetration level $\Delta q$ under an interested attack objective. The selection of $\Delta q$ is based on the market operator's need, and the smaller the $\Delta q$, the higher the level of accuracy that can be obtained. The detailed procedure of this identification is shown in *Algorithm 2 DAT*, where DAT stands for "devasting attack targets" analysis.

### *3.3.3 Formulating risky load levels (Algorithm 3):*

Different load levels result in different market settlements and dispatches. Therefore, the load level is a critical element of a successful cyberattack. As shown in Figure 3.4, an attacker with the same ability could obtain different profits from market-clearing under different load levels. Therefore, the higher the profitability is, the riskier the load level is. In Table 3.4 (Algorithm 3), the CVA model is solved iteratively with all interested attack objectives at different load levels. The obtained attack objective values are scaled and summed for each load level. If the value is higher than a certain threshold, then the load level can be identified as risky. In this study, the same load participation factors are assumed. If the market operator interests in different load participation factors, the load level and the participation factors are both recorded when solving the CVA model, and the risky load level becomes a risky set containing a load level and load participation factors.

Table 3.3 Algorithm for devasting attack targets identifications

| | |
|---|---|
| **Algorithm 2** | Function DAT (market parameters, attack objectives) |
| **Input** | Real-time market parameters and interested attack objectives |
| **Output** | Devasting attack targets |
| 1 | Select interested attack objective from Table 3.1 |
| 2 | **For** each attack target **do** |
| 3 | Set attack variables $B$ associated with other attack targets equal to 0 |
| 4 | **While** penetration level $q$ is less than a threshold |
| 5 | Solving the CVA model (7) - (22) |
| 6 | $q = q + \Delta q$ |
| 7 | Record the value of attack objective |
| 8 | **End while** |
| 9 | **End for** |
| 10 | Compare the slope of different attack targets |
| 11 | Identify targets that have steep slopes |
| 12 | **Return** the Identified Targets |

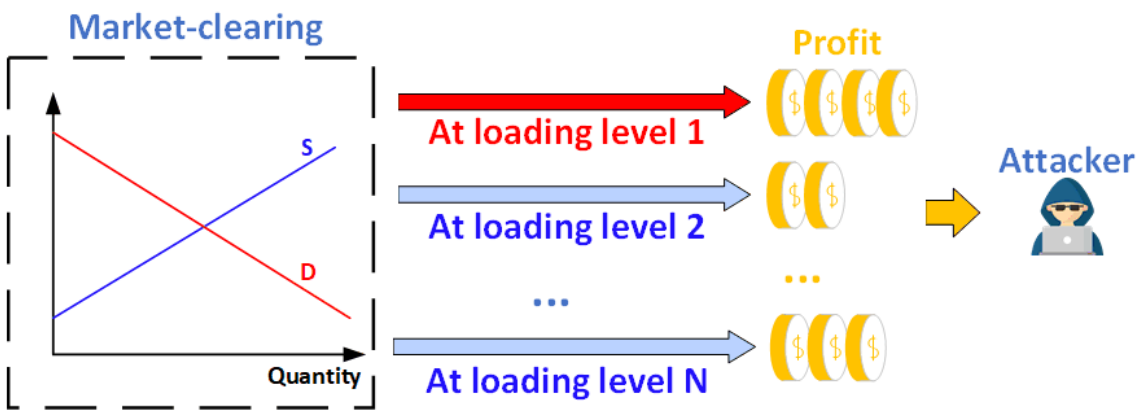


Figure 3.4 Formulating risky load levels

Table 3.4 Algorithm for risky load level identifications

| | |
|---|---|
| **Algorithm 3** | Function RLL (market parameters, attack objectives) |
| **Input** | Real-time market parameters and interested attack objectives |
| **Output** | Risky load levels |
| 1 | **For** each load level **do** |
| 2 | Obtain market-clearing result without attacks |
| 3 | **For** each interested attack objective **do** |
| 4 | Solving the CVA model (7) - (22) |
| 5 | Record the difference between the attacked value and the normal value |
| 6 | **End for** |
| 7 | Sum attack objectives with specified weights $\sum W_i \cdot obj_i$ |
| 8 | **End for** |
| 9 | Identify load levels that have high weighted values |
| 10 | **Return** the Identified Load Levels |

The market operator should take extra caution when the current load level is identified as risky. The detailed procedure of this identification is shown in *Algorithm 3 RLL*, where RLL stands for "risky load level" analysis.

### *3.3.4 Investigating the mitigation ability of different defense degrees (Algorithm 4):*

The goal of this subsection is to investigate the impact of defense degrees on the effectiveness of the attack. As shown in Figure 3.5, if some of the most effective attack routes are defended by the operator, the attacker might switch to other attack routes. However, those backup attack routes are not as effective. Therefore, investigation of the defense degree to which the attacker may lose the attack interests is an important aspect of the development of defense strategies. The proposed Algorithm 4 in Table 3.5 solves the CVA model iteratively with a gradual increase of defense degrees, and the corresponding value of the attack objective is recorded. When the value of the attack objective discourages the attack, the defense degree is identified as the critical defense degree.

The detailed procedure of this identification is shown in *Algorithm 4 DDD*, where DDD stands for "different defense degrees" analysis. The above four proposed analysis algorithms are demonstrated with examples in *Section 3.5*. Analysis in this Chapter is performed using the attack objectives in Table 3.1, but future users can integrate any additional attack objectives in a similar way. The proposed analysis algorithms aim to solve the CVA model iteratively, which could raise a concern about scalability. Indeed, the number of combinations of attack objectives and attack targets can be astronomical for a real system.

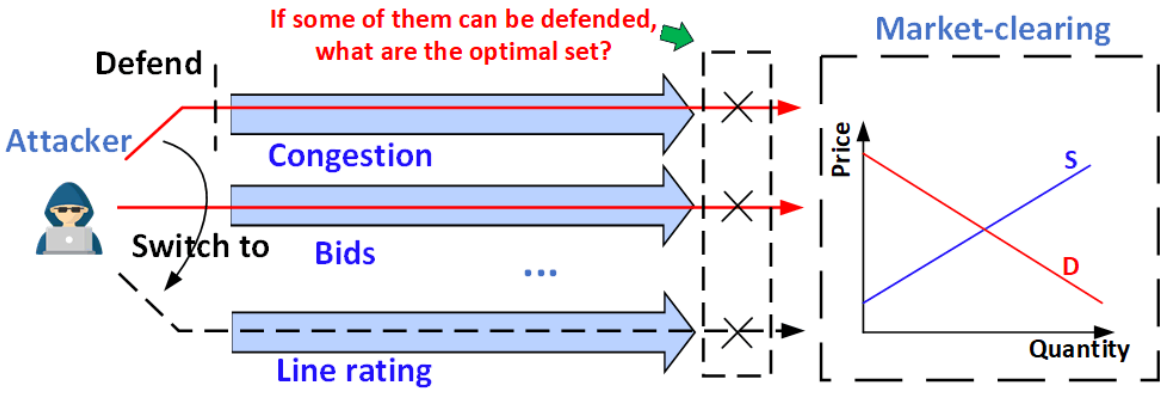


Figure 3.5 The mitigation ability of different degrees

Table 3.5 Algorithm for defense degree impact identifications

| | |
|---|---|
| **Algorithm 4** | Function DDD (market parameters, attack objectives) |
| **Input** | Real-time market parameters and interested attack objectives |
| **Output** | Defense mitigation ability plot/list |
| 1 | **For** each attack objective **do** |
| 2 | Set an interested attack degree $A_{ak}$ and set the defense degree $A_{df} = A_{ak}$ |
| 3 | **while** defense degree $A_{df}$ is larger than 0 **do** |
| 4 | Solving the CVA model (7) - (22) |
| 5 | Record the objective value |
| 6 | $A_{df} = A_{df} - 1$ |
| 7 | **End while** |
| 8 | Plot/list the objective value versus defense degree |
| 9 | **End for** |
| 10 | **Return** the plot/list |

However, the potential attack objectives and attack targets can be filtered to a much smaller portion depending on ISOs or the decision maker's preference. For example, the ISO New England system has 2771 branches, but the average active transmission constraint in January 2020, their winter peak month, is just 142 branches [45].

The attacker's ability is also limited because the attacker may not have access to all parameters. Therefore, the number of combinations can be reduced. Further, the proposed algorithms are for the purpose of analyzing vulnerability, not for protecting market operation in RT. Thus, the proposed analysis could be performed offline and in the cycle of a few weeks (or even months) depending on the market operator's preference. Therefore, the computation is a minor concern for the proposed vulnerability analysis algorithms.

## 3.4 Reformulation of The Proposed CVA Model

Section 3.2 describes the mathematical model for CVA, and Section 3.3 discusses how to apply the CVA model to identify cyber vulnerability for an RT market model. This section presents the steps to solve the CVA model. Normally, the lower-level problem can be converted to constraints through Karush-Kuhn-Tucker (KKT) conditions. Then, the bi-level problem becomes a single-level problem. However, the lower-level problem of the CVA model contains binary variables, which violate the optimality condition of the KKT conditions. Here, we apply the following reformulations to convert the lower-level problem with binary variables through KKT conditions.

*Step 1) Constraints (*3*.20) and (*3*.21) linearization*

Constraints (3.20) and (3.21) contain the multiplication of binary variables and continuous variables. The detailed equations for linearizing (3.20) and (3.21) can be found in *Appendix A.1*.

*Step 2) Lower-level problem convexification*

The binary variables in the lower-level problem are convexified through a penalty function before the KKT conversion. The binary defense decision variable $V$ is reformed with continuous representation. Equation (3.23) redefines $V$ as a finite continuous value with an upper limit $W$. Then, equation (3.24) restricts the feasible value for the continuous variable $V$ to be either 1 or 0. It is worth noting that although now the binary variable $V$ is remodeled through continuous representation, the feasibility region is still non-convex.

$$W \geq V \geq 0 \tag{3.23}$$

$$V(V - 1) = 0 \tag{24}$$

$$\min \quad cost + Q(V(V - 1))^2 \tag{25}$$

Then, constraint (3.24) is removed by adding a penalty term in the objective function, as shown in (3.25). The large number $Q$ will penalize the objective function unless $V$ is either 1 or 0. The square of $V(V-1)$ has the same feasible region as $V(V-1)$, but the square is a convex representation. In this formulation, the lower-level problem is convexified. The selection of the large number $Q$ is a challenge for optimization problems involving penalties because a penalty term may not be exactly zero at the obtained optimal solution. In this study, a large value is assigned to $Q$ initially, and then it is gradually increased until an optimal solution is obtained (i.e., the solution does not change and the value of $V$ is close to binary). When the penalized variables are close but not exactly binary (e.g., 0.99 or 0.01), they are rounded to 0 or 1.

*Step 3) Formulating KKT conditions*

The optimality conditions of the lower-level problem in a bi-level formulation are well-established, such as in [42]. Therefore, the complete KKT constraint set is not elaborated here.

*Step 4) Linearizing nonlinear terms*

The CVA model contains nonlinear elements that render the implementation of the optimizations. In particular, the multiplication of the status of congestion attacks and other variables leads to various nonlinear elements. The constraints that contain nonlinear terms are listed in *Appendix A.2*. The detailed steps for linearizing all the nonlinear elements in those constraints are attached in *Appendix A.3, Appendix A.4,* and *Appendix A.5*.

## 3.5 Case study

A thorough simulation study of an IEEE 30-bus system is given in this section to demonstrate the effectiveness of the proposed vulnerability analysis algorithms. The system topology is shown in Figure 3.6. The detailed system parameters can be found in [38].

### *3.5.1 Identifying highly probable attack targets*

This study aims to demonstrate *Algorithm 1* in *Section 3.3.1*. The CVA model is solved iteratively for various attack objectives from Table 5.1. The computational time of Algorithm 1 in this study is 70.32 s.

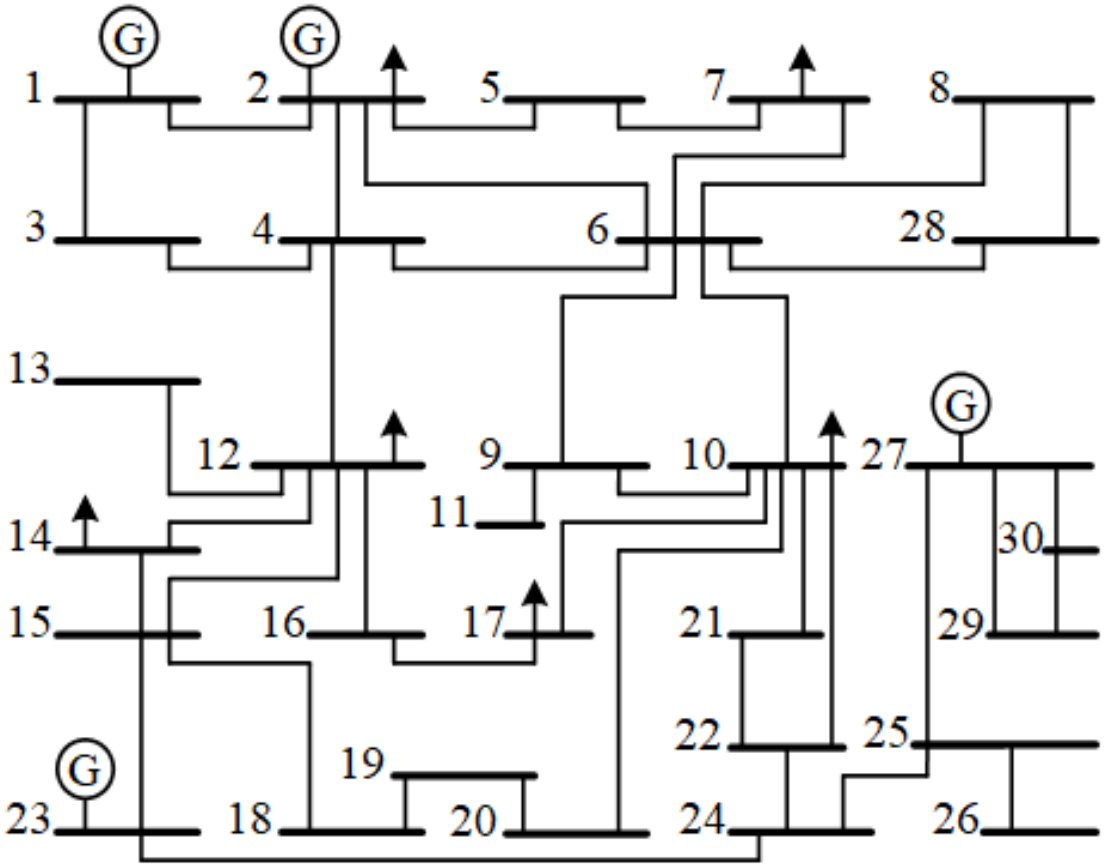


Figure 3.6 One-line diagram of IEEE-30 bus system

Figure 3.7 shows various attacked parameters for each attack objective. The Y-axis shows different objectives of the attacks, and the X-axis shows different attack targets in market operation. Triangles on a specific row represent optimal attack targets for a specific attack objective. For example, for the attack that is to maximize the LMP at bus 1, the optimal attack targets are the load at bus 12 and the line rating at line 15. In other words, an attack on these two parameters will more effectively alter the LMP at bus 1 than the attacks on any other different combination of two parameters. Therefore, by enumerating the number of triangles on each column, the probability of being attacked can be estimated for each parameter from the perspective of being a highly probably attack target. In other words, the column that has the most triangles indicates the parameter that has the highest probability of being attacked. In this study, the line rating of line 15 is the most vulnerable parameter, which will be the most frequent attack target. Therefore, when this target is protected, most attacks become less effective. Although the attackers' objective is usually unknown in reality, protection of highly probable targets reduces overall attack interest in the market operation. The upper subplot and lower subplot in Figure 3.7 represent different attack degrees (2 and 3), namely, how many parameters the attacker is able to modify. When the attack degree increases from 2 to 3, the possibility of attacking the line rating of line 15 increases from 48.6% to 71.6%. Therefore, if the line rating of line 15 is immune from attacks, interests in most attacks on this market are greatly reduced.

### *3.5.2 Identifying devasting attack targets*

This study aims to demonstrate *Algorithm 2* in *Section 3.3.2*. The CVA model for interested attack objectives is solved iteratively for a gradual increase of the penetration levels of different attack targets.

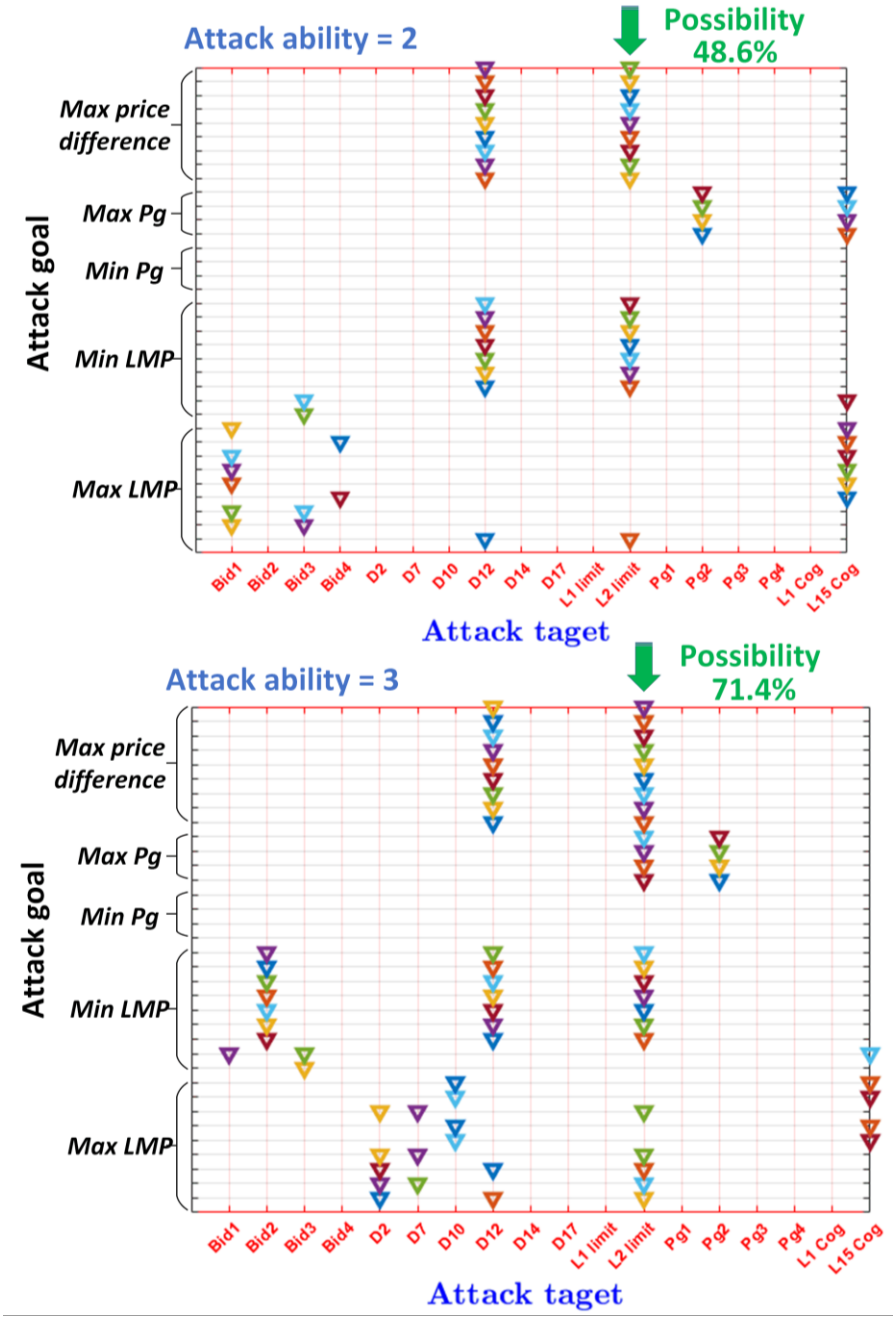


Figure 3.7 Identifying the most likely attack target

The deviations between the objective value under normal operation and under attack are recorded. The computational time of Algorithm 2 in this study is 135.25 s. We select the most popular two attack objectives in the literature as examples: (1) diminishing the social welfare and (2) manipulating LMPs (bus 10). The impact analyses of 4 different attack targets on those two objectives are shown in Table 3.6 and Table 3.7. Simulations on other attack objectives and targets can be performed similarly.

For LMP manipulation, an attack on unit 4's bid is more effective when the penetration level is low, and an attack on unit 3's capacity becomes more effective when the penetration level is higher than 40%. For diminishing social-welfare, attacking the load at bus 2 is more effective when the penetration level is lower than 30% or higher than 90%, and attacking unit 3's bid is more effective for other penetration levels. Further, a step-change phenomenon is observed for both attack objectives. The social welfare loss exhibits a step-change pattern with the bid modification attack and continuously changes with the remaining attacks. By comparison, the LMP continuously changes with the bid modification attack and exhibits a step-change pattern with the remaining attacks. This indicates that the bid modification attack does not impact social welfare unless it changes the dispatch results since it does not change the generation cost in practice, but the bids of marginal units directly impact the LMP. If the most sensitive attack target is identified and protected, the attack interests for a specific attack are significantly reduced.

### *3.5.3 Evaluating risk load levels*

This study aims to demonstrate *Algorithm 3* in *Section 3.3.3*. The CVA model for all attack objectives is solved iteratively under different load levels. The deviations between the objective value under normal operation and under attack are recorded.

Table 3.6 Impact analysis on LMP manipulations

| P. Levels / Deviation ($) / Targets | 10% | 20% | 30% | 40% | 50% | 60% | 70% | 80% | 90% | 100% |
|---|---|---|---|---|---|---|---|---|---|---|
| **Bids of G3** | 0 | 0 | 3.0 | 5.4 | 7.7 | 10.2 | 12.6 | 14.9 | 17.3 | 19.7 |
| **Bids of G4** | 2.6 | 5.1 | 7.7 | 10.3 | 12.8 | 15.4 | 18.0 | 20.6 | 23.1 | 25.7 |
| **Capacity of G3** | 0 | 0 | 0 | 0 | 51.9 | 51.9 | 51.9 | 51.9 | 51.9 | 51.9 |
| **Load at bus 2** | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

Table 3.7 Impact analysis on diminishing social-welfare

| P. Levels / Deviation ($) / Targets | 10% | 20% | 30% | 40% | 50% | 60% | 70% | 80% | 90% | 100% |
|---|---|---|---|---|---|---|---|---|---|---|
| **Bids of G3** | 0 | 0 | 207.1 | 207.1 | 207.1 | 207.1 | 207.1 | 207.1 | 207.1 | 207.1 |
| **Bids of G4** | 0 | 0 | 0 | 0 | 0 | 22.0 | 22.0 | 22.0 | 22.0 | 22.0 |
| **Capacity of G3** | 1.2 | 3.6 | 5.5 | 7.3 | 9.1 | 10.9 | 12.7 | 14.5 | 16.4 | 18.1 |
| **Load at bus 2** | 30.0 | 60.0 | 90.0 | 120.0 | 150.0 | 180.0 | 210.0 | 240.0 | 270.0 | 300.0 |

The computational time of Algorithm 3 in this study is 965.36 s. Figure 3.8 shows the risk evaluation of different load levels by a heat map. Different attack objectives have their own heat map (i.e., risk zone).

Here, all risk zones are summed and scaled to be between 0 and 1, where 0 means not risky, and 1 means the riskiest. Thus, the greater the overlap of the risk zones, the brighter the square is. That is, a brighter area means more impact on the market operation.

As shown in Figure 3.8, at first, the heavier the load is, the more an attacker can do. However, when the load becomes higher, the impact decreases because the margin for manipulation by the attacker is decreased. In other words, when more generations are at maximum, there is less room for an attacker to manipulate the parameters without being detected.

*1) Investigating the mitigation ability of different degrees of defense*

This study aims to demonstrate *Algorithm 4* in *Section 3.3.4*. The understanding of how defenses improve the deviation from the optimal dispatch provides a guideline for a market operator to develop defense strategies. The CVA model is solved iteratively with a gradual increase of the defense degree. The computation time of Algorithm 4 in this study is 65.39 s. As shown in Table 3.8, the value of deviation from a normal value gradually decreases to zero with the increasing defense degree.

When more highly effective attack routes are blocked (i.e., at higher defense degrees), the attacker has to switch to less effective attack routes, and thus, the impact of cyberattacks is alleviated. Although the attack still impacts market operations unless all of the compromised parameters are corrected, the attacker could lose interest when the degree of defense is higher than a certain threshold such that the attacker's gain from a cyberattack is very low.

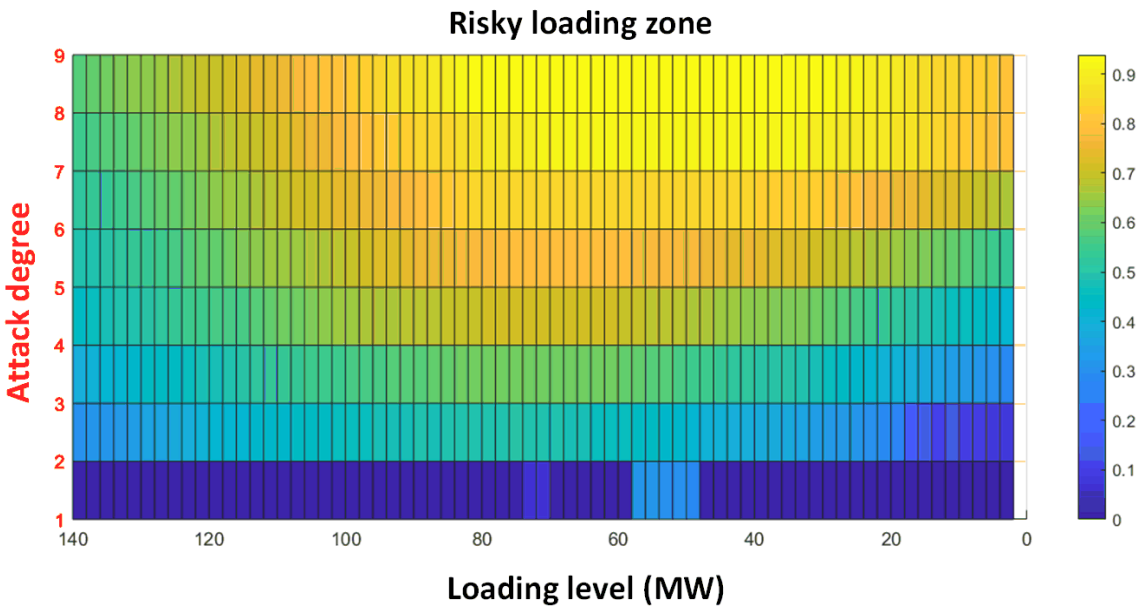


Figure 3.8 Vulnerable market operating zone

Table 3.8 Impact analysis on defense degree

| Degree / Deviation (%) / Objective | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|---|
| **Social-welfare loss** | 109.2 | 105.1 | 101.0 | 86.2 | 72.1 | 55.3 | 35.7 | 24.6 | 0 |
| **LMP (bus 10)** | 215.9 | 215.9 | 215.9 | 215.9 | 215.9 | 215.9 | 132.0 | 30.3 | 0 |

The proposed analysis provides the market operator with information on critical defense degrees. As shown in the first row of Table 3.8, when 3 of the most effective attack routes can be protected, the maximum social welfare deviation dropped from 109.2% to 86.2%, which may discourage the attacks. Further, the social welfare loss due to cyberattacks decreases almost linearly with the increasing defense level. For an LMP manipulation attack, as in the second row of Table 3.8, the defense is not effective (i.e., the deviation created by the attack is 215.9%) until 5 parameters can be defended, which means the attackers can still achieve the desired outcome via the undefended measures. When the defense degree is larger than 5, the optimal value of the attack objective starts to decrease. It should be pointed out that the proposed algorithm provides useful information for a decision maker while the actual threshold to determine the number of defense degrees is a choice of the decision maker.

## 3.6 Conclusions

In this Chapter, the missing components in the current research on power market cybersecurity are discussed. Next, a CVA model is proposed for market operators to perform impact analysis on market cyberattacks. Then, four vital components related to cyber vulnerability in the system are discussed, and four vulnerability analysis algorithms are proposed. The proposed algorithms can help the market operator identify highly probable attack targets, devastating attack targets, risky load levels, and the mitigation ability of different defense degrees. In summary, the proposed CVA model provides a new method to identify various aspects that are vulnerable to cyberattacks in market operation, which provides valuable references for further development of cyber defense strategy.

# Chapter 4 Cyber-Impact Analysis for ISO Revenue Adequacy Considering FDIA in Real-time Market Operations

The consensus on the potential of market-targeting cyberattacks to cause catastrophic damage has driven recent research on power market cybersecurity analysis. This Chapter identifies two missing components in the current literature. First, ISO revenue adequacy has not been analyzed under the context of cyberattacks. Under the impact of false data injection attacks (FDIAs), the market settlement is disturbed, which impacts revenue adequacy for ISOs. The lack of such analysis prevents market operators from comprehensively assessing the financial consequences of market cyberattacks. Second, market attackers need to anticipate the market-clearing results to maximize their attack objectives. Thus, current literature focuses on formulating the attacker model and the market-clearing model as a bilevel problem. However, the coupling between the attack decision, the dispatch at ex-ante, and the price calculation at ex-post has not been explored. To fill those two research gaps, this Chapter first analytically explores the impact of FDIAs on real-time (RT) market operations on ISO revenue adequacy. Then, a cyber-impact analysis platform is proposed to numerically analyze the revenue adequacy. The attacker model, ex-ante dispatch model, and the ex-post incremental model are formulated as a trilevel problem to provide a more reliable cyber-impact analysis on revenue adequacy. The proposed analysis and platform are demonstrated with the New England 39-bus system. More details of this chapter can be found in [J8].

## Nomenclature

*Superscript:*

| | |
|---|---|
| *DA, RT* | Indicating the variable/parameter in the real-time (RT) and day-ahead (DA) models. |
| *expost, exante* | Indicating the variable/parameter in ex-ante and ex-post models. |
| *att* | Indicating the variable/parameter is compromised by attacks. |

*Sets*

| | |
|---|---|
| $N_g$, $N_d$, $N_b$, $N_l$, | Set of generators, loads, buses, and lines in the system. |
| $N_l^{+cog}$, $N_l^{-cog}$ | Set of positive and negative congested lines. |

*Parameters:*

| | |
|---|---|
| $P_i^{min}$, $P_i^{max}$ | The lower and upper generation capacity for the $i^{th}$ unit. |
| $\Delta P^{min}$, $\Delta P^{max}$ | The lower and upper generation capacity for the hypothetical incremental unit. |
| $F_l^{min}$, $F_l^{max}$ | The lower and upper transmission line rating for the $l^{th}$ line. |
| $c_i$ | Generation bidding price of the $i^{th}$ unit. |
| $D_i$ | Load at the $i^{th}$ bus. |
| $\Delta D_i$ | Real-time deviation for load at the $i^{th}$ bus. |
| $\Delta P_{di}$ | Dispatchable loads. |
| $d_i$ | Bidding price of dispatchable loads |
| $f_{i,j}$ | Bidding price for FTR from bus $i$ to bus $j$. |
| $q_{i,j}^{max}$, $q_{i,j}^{min}$ | Upper and lower bound of FTR transactions. |

| | |
|---|---|
| $O_{l,i}^{gsf}$, $O_l^r$, $O_l^d$, $O_l^c$ | Penetration level for attacks on shift factors, line ratings, loads, and bidding prices |

*Variables:*

| | |
|---|---|
| $P_i$ | Generation dispatch for the $i^{th}$ unit. |
| $q_{i,j}$ | FTR transaction from bus $i$ to bus $j$. |
| $q_i$ | Net FTR injection at bus $i$. |
| $\lambda$ | Lagrangian multiplier for power balance constraint. |
| $\gamma_i^+$, $\gamma_i^-$ | Lagrangian multipliers for $i^{th}$ upper and lower generation limits. |
| $\mu_l^+$, $\mu_l^-$ | Lagrangian multipliers for $l^{th}$ upper and lower transmission limits. |
| $\Delta\mu_l^{+att}$, $\Delta\mu_l^{-att}$ | The impact of attacks on $\mu_l^+$ and $\mu_l^-$. |
| $\Delta P_i^{att}$ | The impact of attacks on the $i^{th}$ dispatch. |
| $\delta_{l,i}^{gsf}$, $\delta_l^r$, $\delta_l^d$, $\delta_l^c$ | Attack decisions on shift factors, line ratings, loads, and bidding prices. |
| $\delta_l^+$, $\delta_l^-$ | Attack decisions for the $l^{th}$ congestion pattern. |
| $\Delta GSF_{l-i}$ | Attack value for shift factors. |
| $p_i$ | Attack value for $i^{th}$ generation capacity |
| $r_l$ | Attack value for $l^{th}$ line ratings. |
| $\Delta c_i$ | Attack value for $i^{th}$ unit's bidding. |
| $\Delta D_i^{att}$ | Attack value for loads at bus $i$. |
| $\Delta P_i$ | The impact of RT load deviation on the $i^{th}$ dispatch. |
| $\Delta D_i$ | Load deviations in real-time at bus $i$ |
| $GSF_{l-i}^m$ | The value of the shift factor after attack ($GSF_{l-i}^m = GSF_{l-i} + \Delta GSF_{l-i}$). |

| | |
|---|---|
| $LMP_i$ | Locational marginal price at bus *i*. |
| $Pay^{FTR}$ | Payments to FTR holders. |
| $R^{DA}$, $R^{RT}$ | Revenue surplus from DA and RT markets. |
| $\Delta LF_l$ | RT line flow deviation from DA line flow at the $l^{th}$ line. |
| $\Delta LF_l^{att}$ | The impact of attacks on $\Delta LF_l$. |
| $LF_l^{FTR}$ | Hypothetical FTR flow at $l^{th}$ line. |
| $\varphi_l^-$, $\varphi_l^+$ | Slack variables for negative/positive transmission constraint limits. |

## 4.1 Introduction

Following the existing research works as shown in Chapter 1, this Chapter identifies two unexplored topics. Although research works has started to investigate power market cyberattacks, as presented in the above subsection, this Chapter identifies two missing components.

Firstly, revenue adequacy, a vital financial consideration for ISOs, has not been investigated under the context of cyber intrusions. Specifically, a false data injection attack (FDIA) may disturb the market settlement and impact the revenue adequacy for the ISO under attack. The lack of such analysis prevents ISOs from comprehensively assessing the financial consequences of market cyberattacks.

Secondly, the prevailing attack model commonly contains a nested real-time (RT) market-clearing model to formulate a bilevel optimization problem because the attacker needs to anticipate RT market-clearing results to maximize the attack objective. However, the prevailing ex-post RT market model contains an ex-ante dispatch model and an ex-post pricing model. Some attacks impact both the ex-ante and ex-post while some attacks only

impact one of them. For example, the transmission line rating attack only impacts ex-ante dispatch, while the congestion pattern attack mainly targets ex-post pricing. The trilevel coupling between attack decisions, the ex-ante dispatch, and the price calculation at ex-post has not been explored in the literature.

Therefore, this Chapter aims to address these two missing components. The detailed contributions are as follows:

- This Chapter is the first attempt to investigate ISO revenue adequacy under the context of cyber intrusions. The revenue adequacy problem is formulated under the existence of cyberattacks. Sufficient conditions for cyberattacks causing revenue shortfalls are developed and analyzed. Four remarks on the impact of cyberattacks on revenue adequacy are presented in detail. The formulated conditions and remarks provide ISOs with a theoretical analysis foundation on the impact of cyberattacks on revenue adequacy.
- The proposed cyber-impact analysis is the first attempt to model the coupling between attack decisions, ex-ante dispatches, and ex-post pricing, which provides a more reliable analysis platform and helps ISOs comprehensively evaluate the potential financial consequences of cyberattacks. The proposed platform is applied to the New England 39-bus system to demonstrate the severity of the potential revenue shortfall.

The rest of this Chapter is organized as follows. Section 4.2 analyzes the impact of cyber intrusions on ISO revenue adequacy, and four remarks on the revenue adequacy are discussed in detail. In Section 4.3, the cyber-impact analysis model is proposed and formulated. Each level is described in detail. Section 4.4 presents reformulations and algorithms to solve the proposed model. Section 4.5 demonstrates the proposed platform on

the New England 39-bus system. Finally, Section 4.6 summarizes this Chapter and draws conclusions.

## 4.2 Impact of Cyber-intrusion on Revenue Adequacy

The prevailing two-settlement market-clearing process uses LMPs to settle electricity purchases and sales, which reflects the price of electricity generation, thermal loss, and cost of transmission congestions [88]. As the name suggests, the LMP is calculated by the location where power is received or delivered. The generation bus and load bus are usually settled by different prices, which leaves a revenue surplus due to congestions [43]. Thus, FTR is proposed to entitle transmission holders to receive revenue surplus. Although the following section briefly discuss the FTR scheme, more details on FTR can be found in [44]-[47].

In general, a system is revenue adequate if the revenues collected from the two-settlement market-clearing process in the form of congestion payments are sufficient to fully fund payments for the FTRs. In this section, we first briefly discuss the two-settlement market-clearing scheme and FTR auction model. Then, revenue adequacy is analyzed under the context of cyber intrusions. Sufficient conditions for cyberattacks causing revenue shortfalls are developed, and four remarks are discussed in detail on the impact of cyberattacks on ISO revenue adequacy.

### *4.2.1 Market-clearing Scheme and FTR Auction Model*

Two-settlement market-clearing contains a day-ahead (DA) market and an RT market [50]. The DA market is cleared a day ahead, and the RT market offers adjustment for real

time deviations [48]. The ex-post pricing scheme has been widely applied in ISOs, such as ISO-NE, PJM, and MISO, for RT market-clearing, where the dispatch is determined by the ex-ante model, while the LMP is calculated after the cycle of spot market by an ex-post incremental model.

The DA and ex-ante dispatch models have the same formulation as shown in (4.1)-( 4.4), and the difference lies in the forecast intervals.

$$\min \sum_{i}^{N_g} c_i \cdot P_i \tag{4.1}$$

$$\sum_{i}^{N_g} P_i = \sum_{i}^{N_d} D_i \tag{4.2}$$

$$P_i^{\min} \le P_i \le P_i^{\max} \tag{4.3}$$

$$F_l^{\min} \le \sum_{i=1}^{N_b} GSF_{l-i}(P_i - D_i) \le F_l^{\max}, \ \forall l \in N_l \tag{4.4}$$

The formulation of LMP is shown in (4.5).

$$LMP_i = l + \sum_{l}^{N_l} GSF_{l-i}(m_l^- - m_l^+) \tag{4.5}$$

The ex-post incremental model is shown in (4.6)-( 4.10).

$$\min \sum_{i}^{N_g} c_i \cdot P_i^{expost} - \sum_{j}^{N_d} d_j \cdot \Delta P_{dj} \tag{4.6}$$

$$\sum_{i}^{N_g} P_i^{expost} = \sum_{j}^{N_d} \Delta P_{dj} \tag{4.7}$$

$$\Delta P_i^{\min} \le P_i^{expost} \le \Delta P_i^{\max} \tag{4.8}$$

$$\sum_{i=1}^{N_b} GSF_{l-i}(P_i^{expost} - \Delta P_{di}) \le 0, \ \forall l \in N_l^{+cog} \tag{4.9}$$

$$\sum_{i=1}^{N_b} GSF_{l-i}(P_i^{expost} - DP_{di}) \geq 0, \ \forall l \in N_l^{cog} \tag{4.10}$$

The portion of FTR that can be awarded is required to be within limits when all FTRs exist simultaneously in the system. The FTR auction model is shown in (4.10)-(4.13).

$$\max \sum_{i}^{N_b} \sum_{j \neq i}^{N_b} f_{i,j} \cdot q_{i,j} \tag{4.10}$$

$$q_i = \sum_{j \neq i}^{N_b} q_{i,j} - \sum_{k \neq i}^{N_b} q_{k,j}, \ \forall i \in N_b \tag{4.11}$$

$$F_l^{\min} \leq \sum_{i=1}^{N_b} GSF_{l-i} q_i \leq F_l^{\max}, \ \forall l \in N_l \tag{4.12}$$

$$q_{i,j}^{\min} \leq q_{i,j} \leq q_{i,j}^{\max}, \ \forall \{i,j\} \in N_b, \ i \neq j \tag{4.13}$$

The above models are presented briefly as background, and the model details can be found in [49], [51], and [44].

### *4.2.2 Impact of Cyber-Intrusions on Revenue Adequacy*

Periodical FTR auctions are held monthly and yearly, and it decides the financial right allocation of transmission capacities. FTR auctions entitle the holder to receive a stream of revenues based on the hourly congestion price in the DA market. This Chapter considers the point-to-point type of transmission right. The FTR holder receives payments, which are equal to the FTR quantity multiplied by the price difference between the injection bus and withdrawn bus. The total payment to FTR holders under a DA market-clearing result is shown in (4.14).

$$Pay^{FTR} = \sum_{i}^{N_b} \sum_{j \neq i}^{N_b} q_{i,j} \cdot (LMP_j^{DA} - LMP_i^{DA}) \tag{4.14}$$

By replacing the LMP with equation (4.5), the equation (4.14) can be reformulated as (4.15). The payment to FTR holders is equal to the congestion price multiplied by the FTR quantity at all lines.

$$Pay^{FTR} = \sum_{i}^{N_b} \sum_{j \neq i}^{N_b} q_{i,j} \times \left(\sum_{l} GSF_{l-i} - GSF_{l-j}\right) \times \left(\mu_l^{+DA} - \mu_l^{-DA}\right) = \sum_{l}^{N_l} LF_l^{FTR} \times \left(\mu_l^{+DA} - \mu_l^{-DA}\right) \quad (4.15)$$

The ISO collects payments from load aggregators and pays generation companies. The net revenue in the DA market is formulated in (4.16). Equation (4.16) can be reformulated as (4.17) by (4.5), which means the net revenue is also equal to the congestion price multiplied by the transmission capacity at all lines.

$$R^{DA} = \sum_{i}^{N_b} (D_i - P_{gi}) \times LMP_i^{DA} \quad (4.16)$$

$$R^{DA} = \sum_{l}^{N_l} F_l^{\max} \times \mu_l^{+DA} - F_l^{\min} \times \mu_l^{-DA} \quad (4.17)$$

Based on equations (4.15) and (4.17), constraint (4.12) in the FTR auction model ensures revenue adequacy at the DA market ($R^{DA} > Pay^{FTR}$) under normal operations, which is also referred to as a simultaneous feasibility test [45]. In the same vein, the net revenue for RT operation is shown in (4.18), which means the net revenue is equal to the deviation of RT line flow from the DA line flow multiplied by the RT congestion price. Under normal operations, $R^{RT}$ is non-negative because $\Delta LF$ is positive for nonzero $\mu^+$ and negative for nonzero $\mu^-$. Thus, revenue adequacy is always ensured, and it is independent of the dispatch results. The net revenue of ISOs is shown in (4.19).

$$R^{RT} = \sum_{l} \Delta LF_l \times \left(\mu_l^{+RT} - \mu_l^{-RT}\right) \quad (4.18)$$

$$N = R^{DA} + R^{RT} - Pay^{FTR} \quad (4.19)$$

As presented in the literature review, cyberattacks can alter RT market-clearing results through various attack paths. DA cyberattacks have not been fully explored and justified in the literature, and thus, they are not discussed in this Chapter. However, the discussion of DA market cyberattacks will be similar to RT market cyberattacks. RT cyberattacks can inject false data on bids, line rating, demand response, etc., which impacts both the $\Delta LF$ and the congestion price $\mu$ for RT operations. Then, (4.18) can be reformulated as in (4.20), which represents RT revenue under cyberattacks.

$$R^{RT,att} = \sum_{l} \Delta LF_l^{att} \cdot \left[ \left( m_l^{+RT} + \Delta m_l^{+att} \right) - \left( m_l^{-RT} + \Delta m_l^{-att} \right) \right] \tag{4.20}$$

Assuming the cyberattack is the only unexpected event when $\mu^{DA}$ and $\mu^{RT}$ are the same, the revenue adequacy (4.19) can be reformulated as in (4.21).

$$N = \sum_{l} \left( F_l^{\max} - LF_l^{FTR} + \Delta LF_l^{att} \right) \cdot m_l^{+DA} - \left( F_l^{\min} - LF_l^{FTR} + \Delta LF_l^{att} \right) \cdot m_l^{-DA} + \Delta LF_l^{att} \cdot \left( \Delta m_l^{+att} - \Delta m_l^{-att} \right)$$

(4.21)

Therefore, if the value of $N$ is negative, the cyberattack leads to revenue shortfalls. The sufficient conditions (but not necessary) can be developed as the following conditions (A1) and (A2) to make the value of $N$ negative.

**(A1)** **For a positively congested line:**

$$\Delta LF_l^{att} \le LF_l^{FTR} - F_l^{\max}, \quad l \in N_l^{+cog} \tag{4.22}$$

$$\Delta m_l^{+att} \ge 0, \quad l \in N_l^{+cog} \tag{4.23}$$

**(A2)** **For a negatively congested line:**

$$\Delta LF_l^{att} \ge LF_l^{FTR} - F_l^{\min}, \quad l \in N_l^{-cog} \tag{4.24}$$

$$\Delta m_l^{-att} \le 0, \quad l \in N_l^{-cog} \tag{4.25}$$

If the attacker can inject false data making $\Delta LF$ and $\mu$ satisfy (A1)-(A2), it is sufficient for the attack, causing an ISO revenue shortfall.

Four remarks are discussed in detail on the impact of a cyberattack on revenue adequacy by the proposed sufficient conditions. The four remarks are also demonstrated in Section 3.5 on the New England 39-bus system by the proposed model in Section 3.4.

***Remark 1***. Considering an important scenario when all transmission rights have been auctioned as shown in (4.26), the total payment to FTR holders $Pay^{FTR}$ is equal to the revenue from DA operation $R^{DA}$. Then, revenue adequacy purely depends on RT operations, which is an easier goal for attacks to achieve.

$$LF_l^{FTR} = F_l^{\max} \text{ or } F_l^{\min}, \quad \forall l \in N_l \tag{4.26}$$

With (4.26), the sufficient conditions (A1)-(A2) can be relaxed as (4.27)-( 4.30), which ensure the negative revenue from RT operations. Equations (4.27) and (4.29) ensure $\Delta LF_l$ at a positive congestion line is negative and $\Delta LF_l$ at a negative congestion line is positive. Equations (4.28) and (4.30) satisfy (4.23) and (4.25) with the help of line rating attack $r_l$. Equations (4.27)-(4.30) are sufficient conditions for cyberattacks causing negative RT revenue, and they are sufficient conditions for cyberattacks causing revenue shortfall when all of the transmission rights have been auctioned.

$$\Delta LF_l^{att} \leq 0, \quad \forall l \in N_l^{+cog} \tag{4.27}$$

$$F_l^{\max} - r_l = \Delta LF_l^{att}, \quad \forall l \in N_l^{+cog} \tag{4.28}$$

$$\Delta LF_l^{att} \geq 0, \quad \forall l \in N_l^{-cog} \tag{4.29}$$

$$F_l^{\min} + r_l = \Delta LF_l^{att}, \quad \forall l \in N_l^{-cog} \tag{4.30}$$

***Remark 2***. Generally, RT demands slightly deviate from the DA forecast. When load forecast error is considered, (4.27)-(4.30) can be reformulated as (4.31)-( 4.34). It is worth noting that when load forecast errors contribute to relieving congestion (negative or positive), it helps the cyberattack cause revenue shortfalls because (4.31) and (4.33) can be satisfied by particular load forecast errors, instead of cyberattacks. It is also worth mentioning that load deviations do not necessarily worsen/relieve the shortfall created by an attack but that deviations do increase/decrease the value of necessary false data being injected.

$$\Delta LF_l^{att} + \Delta LF \le 0, \quad \forall l \in N_l^{+cog} \tag{4.31}$$

$$F_l^{\max} - r_l = \Delta LF_l^{att} + \Delta LF, \ \forall l \in N_l^{+cog} \tag{4.32}$$

$$\Delta LF_l^{att} + \Delta LF \ge 0, \ \forall l \in N_l^{-cog} \tag{4.33}$$

$$F_l^{\min} + r_l = \Delta LF_l^{att} + \Delta LF, \ \forall l \in N_l^{-cog} \tag{4.34}$$

The incremental change in the line flow caused by load forecast error is shown in (4.35). The impact of an attack on the value of line flow is shown as in (4.36). Therefore, the sufficient conditions (4.31)-(4.34) can be reformulated as (4.37)-( 4.40), which relates the sufficient conditions with market parameters (attack paths).

$$\Delta LF_l = \sum_i (\Delta D_i - \Delta P_i) \cdot GSF_{l-i} \tag{4.35}$$

$$\Delta LF_l^{att} = \sum_i (\Delta D_i^{att} - \Delta P_i^{att}) \cdot GSF_{l-i} \tag{4.36}$$

$$\sum_i (\Delta D_i^{att} + \Delta D_i - \Delta P_i^{att}) \cdot GSF_{l-i} \le 0, \ \forall l \in N_l^{+cog} \tag{4.37}$$

$$F^{\max} - r_l = \sum_i (\Delta D_i^{att} + \Delta D_i - \Delta P_i^{att}) \cdot GSF_{l-i}, \ \forall l \in N_l^{+cog} \tag{4.38}$$

$$\sum_i (\Delta D_i^{att} + \Delta D_i - \Delta P_i^{att}) \cdot GSF_{l-i} \ge 0, \ \forall l \in N_l^{-cog} \tag{4.39}$$

$$F^{\min} + r_l = \sum_i (\Delta D_i^{att} + \Delta D_i - \Delta P_i^{att}) \times GSF_{l-i}, \forall l \in N_l^{cog} \quad (4.40)$$

***Remark 3***. Injecting false data on demand, bidding, and unit capacity does not affect revenue adequacy if not combined with transmission line rating attacks. From the necessary conditions, although the above three types of attack can manipulate the value of congestion price, meaning that (4.23) and (4.25) can be ensured, conditions (4.22) and (4.24) cannot be satisfied unless combined with the transmission line rating attack. However, the transmission line rating attack alone can theoretically satisfy the sufficient conditions (A1)-(A2). From this observation, the transmission line rating attack ensures the feasibility of causing a shortfall and the other types of attacks enhance the severity of the resulting shortfall.

***Remark 4.*** Unexpected line derating and outage may also lead to a revenue shortfall [46]. As shown in (4.31)-(4.34), when unexpected line derating happens with particular load forecast error, high revenue shortfalls could happen without a cyberattack. However, compared with unexpected contingency events, the threat from cyberattacks is much more severe because it not only strategically selects the most effective lines to de-rate, but also able to inject false data at other parameters to enhance the revenue shortfall. Furthermore, a conventional procedure for allocating revenue shortfall is that an ISO prorates the shortfall to all FTR settlements. However, allocating the shortfall caused by attacks could make some FTRs lose the ability to hedge against congestion rents for bilateral transactions due to the significant number of shortfalls.

In summary, this section analytically discusses the impact of cyberattacks on revenue adequacy and sufficient conditions for revenue shortfalls. The next section will formulate a

impact analysis platform to numerically investigate revenue adequacy under the context of a cyberattack.

## 4.3 Cyber-impact Analysis Platform for Revenue Adequacy

In Section 4.2, the impacts of cyberattacks on revenue adequacy has been analytically investigated. This section presents a cyber-impact analysis platform to numerically evaluate the impact of cyberattacks on revenue adequacy.

The proposed cyber-impact platform places an attacker model at the upper-level, an ex-ante model at the middle-level, and an ex-post model at the lower-level. The detailed mathematical model and descriptions are provided in following subsections.

### *4.3.1 Upper-level (Attacker model):*

To investigate the impact of a cyberattack on revenue adequacy, the objective of the attacker model is set to maximize the revenue shortfall (4.21), as shown in (4.40).

$$\max \; - N \tag{4.40}$$

**Assumption of the attack model:**

**The proposed model is a cyber-impact analysis model for ISOs. Therefore, the upper-level model considers as many attack paths as possible.** Some parameters may not be easily compromised unless the cyber threats are from insiders, the proposed model considers comprehensive scenarios for market operators to analyze revenue adequacy. Specific attack paths can be removed if decision makers consider these parameters to be perfectly secure or unpractical.

The potential attack targets are generally the market-clearing parameters. As discussed in the literature review, most if not all parameters of the RT market-clearing model have been justified as attackable and profitable. **This model considers the following false data injection based on previous literature: (1) demand; (2) line rating; (3) congestion pattern; (4) unit capacity; (5) bidding.**

The above data sources are assumed to be susceptible to attacks in the proposed platform, as shown in (4.41)-(4.44). The attack values on the parameters are constrained by the penetration level $o$, the attack decision $\delta$, and their original value. The details of congestion pattern attacks are discussed in the lower-level model.

$$- d_i^p \cdot P_i^{\max} \cdot o_i^p \le p_i \le d_i^p \cdot P_i^{\max} \cdot o_i^p \tag{4.41}$$

$$d_l^r \cdot F_l^{\min} \cdot o_l^r \le r_l \le d_l^r \cdot F_l^{\max} \cdot o_l^r \tag{4.42}$$

$$- d_i^d \cdot D_i \cdot o_i^d \le \Delta D_i^{att} \le d_i^d \cdot D_i \cdot o_i^d \tag{4.43}$$

$$d_i^c \cdot c_i \cdot o_i^c \le \Delta c_i \le d_i^c \cdot c_i \cdot o_i^c \tag{4.44}$$

The attacker is assumed to have limited attack abilities. The value of $S$ restricts the number of parameters that the attacker can perturb, as in (4.45). Equation (4.46) shows that the congestion pattern attack for a line is either for positive congestion or for negative congestion.

$$\sum_i \sum_l d_l^r + d_i^p + (1 - d_l^+) + (1 - d_l^-) + d_i^c + d_i^d \le S \tag{4.45}$$

$$d_l^+ + d_l^- \le 1 \tag{4.46}$$

In summary, the upper level models an envisaged attacker who aims to create a revenue shortfall with limited abilities.

### *4.3.2 Middle-level (Ex-ante dispatch model):*

The injected false data impacts the RT economic dispatch obtained by the ex-ante model (4.1)-(4.5) because some parameters are compromised. The upper-level decision variables impact the bid at the objective (4.1), unit capacity at (4.3), line rating at (4.4), and load in (4.2) and (4.4). Therefore, the ex-ante model (4.1)-(4.5) can be reformulated as in (4.47)-(4.52) considering cyberattacks. The false data injected by attackers deviate dispatch decisions, which are sent to generators. The compromised dispatch, in turn, impacts the goal of the attacker.

$$\min \sum_{i}^{N_g} (c_i + \Delta c_i) \cdot P_i^{exante} \tag{4.47}$$

$$\sum_{i}^{N_g} P_i^{exante} = \sum_{i}^{N_d} D_i^{exante} \tag{4.48}$$

$$D_i^{exante} = D_i + \Delta D_i + \Delta D_i^{att}, \forall i \in N_b \tag{4.49}$$

$$P_i^{\min} \le P_i^{exante} \le P_i^{\max} + p_i \tag{4.50}$$

$$\sum_{i=1}^{N_b} GSF_{l-i} \cdot (P_i^{exante} - D_i^{exante}) \le F_l^{\max} + r_l, \forall l \in N_l \tag{4.51}$$

$$\sum_{i=1}^{N_b} GSF_{l-i} \cdot (P_i^{exante} - D_i^{exante}) \ge F_l^{\min} + r_l, \forall l \in N_l \tag{4.52}$$

### *4.3.3 Lower-level (Ex-post pricing model):*

The ex-post pricing model is an incremental model based on the results of state estimations. A remote transmission unit collects various measurements, such as generation and line flow, and sends them to the state estimator. The resulting data, such as generations and congestion patterns, are used for calculating market settlements. The random errors are filtered by bad data detection, and thus, the injected false data is assumed to be the only source of bad data. Similar to (4.47)-(4.52), considering the compromised parameters, the original ex-post model (4.6)-(4.10) can be reformulated as (4.53)-(4.57). The ex-ante model determines the dispatch, and state estimation outputs the congestion pattern, which provides the transmission binding constraints in the ex-post model as in (4.56) and (4.57). The congestion pattern attack can compromise state estimation results to manipulate transmission binding constraint sets $N_l^{+cog}$ and $N_l^{-cog}$ in (4.57) and (4.58).

$$\min \sum_{i}^{N_g} (c_i + \Delta c_i) \cdot P_i^{expost} \tag{4.53}$$

$$\sum_{i}^{N_g} P_i^{expost} = 0 \tag{4.54}$$

$$\Delta P_i^{\min} \le P_i^{expost} \le \Delta P_i^{\max} \tag{4.55}$$

$$\sum_{i=1}^{N_b} GSF_{l-i} \cdot P_i^{expost} \le 0, \forall l \in N_l^{+cog} \tag{4.56}$$

$$\sum_{k=1}^{N_b} GSF_{l-i} \cdot P_i^{expost} \ge 0, \forall l \in N_l^{-cog} \tag{4.57}$$

The ex-post model determines the LMP at each bus to clear the market, which impacts the value of the attack objective. The reformulations and solution algorithms for the proposed model are presented in the next section.

## 4.4 Solution methodology

The structure of the proposed trilevel problem is different from conventional trilevel models where each level interacts with each other. The middle-level ex-ante model only passes the congestion status to the lower-level ex-post model, and the lower-level ex-post model does not impact the solution of middle-level problem. This characteristic will be exploited in the proposed solution algorithm to make it efficient, which is specifically discussed in subsection 4.3.3. The detailed solution of the proposed trilevel problem is presented in the following subsections.

### *4.4.1 Modeling the Transmission Binding Constraint Set*

The first step of solving the trilevel problem is to connect the middle-level ex-ante problem with the lower-level ex-post problem because the set of transmission binding constraints ($N_l^{+cog}$, $N_l^{-cog}$) is not explicitly modeled in (4.56) and (4.57). The line flow constraints in (4.51) and (4.52) can be reformulated to (4.58) and (4.59) with slack variable $\varphi$. When $\varphi^+$ or $\varphi^-$ for the $l^{\text{th}}$ line is 0, the $l^{\text{th}}$ line is positively or negatively congested. Otherwise, the $l^{\text{th}}$ line flow constraint is not binding. Then, the increment line flow constraints (4.56) and (4.57) in the ex-post model can be reformulated as in (4.60) and (4.61). When $\varphi_l^+$ or $\varphi_l^-$ for the $l^{\text{th}}$ line is 0 in the ex-ante model, the $l^{th}$ line constraint is binding in the ex-post model. When $\varphi_l^+$ or $\varphi_l^-$ for the $l^{\text{th}}$ line is not 0 in the ex-ante model, the $l^{th}$ line constraint is not binding in the ex-post model. Thus, equations (4.60) and (4.61) are equivalent to (4.56) and (4.57).

Further, the binary variable for a congestion pattern attack from the upper-level problem also decides the number of transmission binding constraints at the ex-post pricing model. When $\delta_l^+$ or $\delta_l^-$ is 0 (i.e., congestion pattern attack happens at $l^{\text{th}}$ line), constraint (4.60) or (4.61) is removed. When $\delta_l^+$ or $\delta_l^-$ is 1 (i.e., no attack), constraint (4.60) or (4.61) stays. The congestion pattern attack in this model only considers relieving a congested line because relieving a congested line is generally more feasible than congesting a line. For example, if a line is originally congested at its upper limit 200 MW, then the 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 in order to remain undetectable.

$$\sum_{i=1}^{N_b} GSF_{l-i} \times (P_{gi}^{exante} - D_i^{exante}) + y_l^+ = F_l^{\max} + r_l, l \in N_l \tag{4.58}$$

$$\sum_{i=1}^{N_b} GSF_{l-i} \times (P_i^{exante} - D_i^{exante}) - y_l^- = F_l^{\min} + r_l, l \in N_l \tag{4.59}$$

$$d_l^+ \times \sum_{i=1}^{N_b} GSF_{l-i} \times P_i^{expost} \le y_l^+, l \in N_l \tag{4.60}$$

$$d_l^- \times \sum_{k=1}^{N_b} GSF_{l-i} \times P_i^{expost} \ge -y_l^-, l \in N_l \tag{4.61}$$

### *4.4.2 Converting the Lower-level Problem*

Next, the lower-level problem is converted with Karush-Kuhn-Tucker (KKT) conditions. The lower-level problem (4.53)-(4.57) is equivalent to (4.54), (4.55), (4.60), (4.61), and (4.62)-(4.68) because the lower-level problem is a convex model. Thus, with the value of $\varphi_l$ from the ex-ante model and the attack decision from the attacker model, solving the KKT equations gives the LMP at each bus, which is the same as solving (4.54)-( 4.58).

(4.54), (4.55), (4.60), (4.61)

$$(c_i + \Delta c_i) - l^{expost} + g_i^{+expost} - g_i^{-expost} + w^{expost} = 0 \tag{4.62}$$

$$w = \sum_{l=1}^{N_L} GSF_{l-i} \times (d_l^{+} \times m_l^{+expost} - d_l^{-} \times m_l^{-expost}) \tag{4.63}$$

$$d_l^{+} \times m_l^{+expost} \times (\sum_{i=1}^{N_b} (GSF_{l-i} \times P_i^{expost}) - y_l^{+}) = 0 \tag{4.64}$$

$$d_l^{-} \times m_l^{-expost} \times (-\sum_{i=1}^{N_b} (GSF_{l-i} \times P_i^{expost}) - y_l^{-}) = 0 \tag{4.65}$$

$$g_i^{-expost} \times (\Delta P_i^{\min} - P_i^{expost}) = 0 \tag{4.66}$$

$$g_i^{+expost} \times (P_i^{expost} - \Delta P_i^{\max}) = 0 \tag{4.67}$$

It is worth noting that although the variables representing a congestion pattern attack are binary variables in the lower-level model, the upper-level variables are treated as parameters in the lower-level problem. When the value of $\delta_l$ is 0, all the KKT conditions related to the $l^{th}$ transmission constraint are removed. When the value of $\delta_l$ is 1, the KKT conditions related to the $l^{th}$ transmission constraint are included.

### *4.4.3 Converting the Middle-level Problem*

The structure of the proposed model is shown in Figure 4.1. The trilevel coupling is explained as follows. The upper-level decision variable impacts the optimal solution of the middle-level and lower-level problems. The optimal solution of the middle-level and lower-level problems also impact the optimality of the upper-level problem. Thus, the upper-level problem interacts with both the middle-level and lower-level problems.

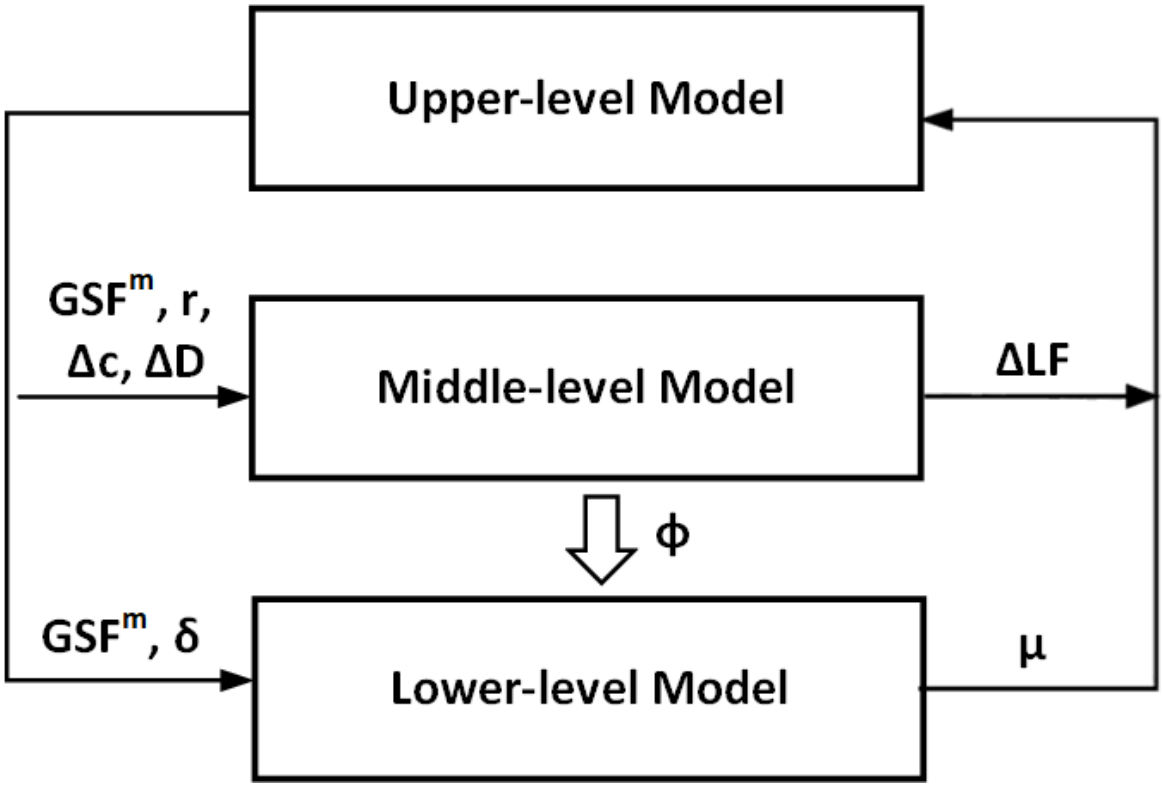


Figure 4.1 Structure of the proposed model

However, different from conventional trilevel problems, the middle-level and lower-level problems in the proposed model exhibit a one-way relationship. The middle-level problem only needs to pass the value of $\varphi_l$ to the lower-level and does not need to anticipate the solution of the lower-level problem for its own optimization. Thus, the middle-level problem can also be converted by KKT conditions based on this unique one-way relationship. Eventually, the model is converted into the upper-level problem with two sets of KKT conditions. The middle-level problem (4.47)-( 4.52) can be converted to KKT conditions as in (4.48)-( 4.50), (4.58), (4.59), and (4.68)-( 4.73).

Then, the optimization problem (4.40)-( 4.57) is equivalent to solving (4.40)-(4.46), (4.47)-(4.52), (4.54), (4.55), (4.58)-(4.61), and (4.62)-(4.73).

$$(4.47) - (4.52),\ (4.58),\ (4.59)$$

$$c_i + \mathrm{D}c_i - l^{exante} + g_i^{+exante} - g_i^{-exante} + w^{exante} = 0 \tag{4.68}$$

$$w^{exante} = \sum_{l=1}^{N_L} GSF_{l-i} \cdot (m_l^{+exante} - m_l^{-exante}) \tag{4.69}$$

$$m_l^{+exante}\left(\sum_{i=1}^{N_b} GSF_{l-i} \cdot (P_i^{exante} - D_i^{exante}) - y_l^{+}\right) = 0 \tag{4.70}$$

$$m_l^{-exante} \cdot \sum_{i=1}^{N_b} (-GSF_{l-i} \cdot (P_i^{exante} - D_i^{exante}) + y_l^{-}) = 0 \tag{4.71}$$

$$g_i^{-exante} \cdot (P_{gi}^{\min} - P_{gi}^{exante}) = 0 \tag{4.72}$$

$$g_i^{+exante} \cdot (P_i^{exante} - P_i^{\max} - p_i) = 0 \tag{4.73}$$

In summary, Sections 4.3 presents the trilevel cyber-impact analysis model formulation, and Section 4.4 develops the solution techniques of the trilevel model based on the model characteristics. The unique interaction between the lower-level model and the middle-level

model, as discussed in the opening paragraph and subsection 4.4.3, is utilized to make the solution algorithm efficient.

## 4.5 Case study

In this section, the impact of cyberattacks on ISO revenue adequacy is analyzed on the New England 39-bus system using the proposed platform. The detailed system parameters can be found in [52]. The system topology is sketched in Figure 4.2. The simulation studies were performed with MATLAB 2018 on a PC with Intel i7-8650U processor and 8GB RAM. Four case studies are conducted to show the impact of cyberattacks on revenue shortfall in detail. The four case studies discuss and analyze the four remarks in *Section 4.3.2* accordingly.

### *4.5.1 Case Study 1: Margin of the Revenue Shortfall*

As shown in Remark 1, cyberattacks can more easily cause revenue shortfall when all transmission rights are auctioned. If only a part of the transmission capacity is auctioned, the unauctioned capacity leaves ISOs revenue surplus (margin), which can be used to recover shortfalls.

As shown in Table 4.1, the revenue margin decreases proportionally with the transmission capacities margin. When all of the capacities are auctioned, the revenue margin goes to 0. An attack scenario is performed on the proposed analysis platform to analyze the revenue shortfall. The attack is assumed to have three attack degrees and a 20% penetration level. The resulting shortfall by the attack is shown in the third column of Table 4.1.

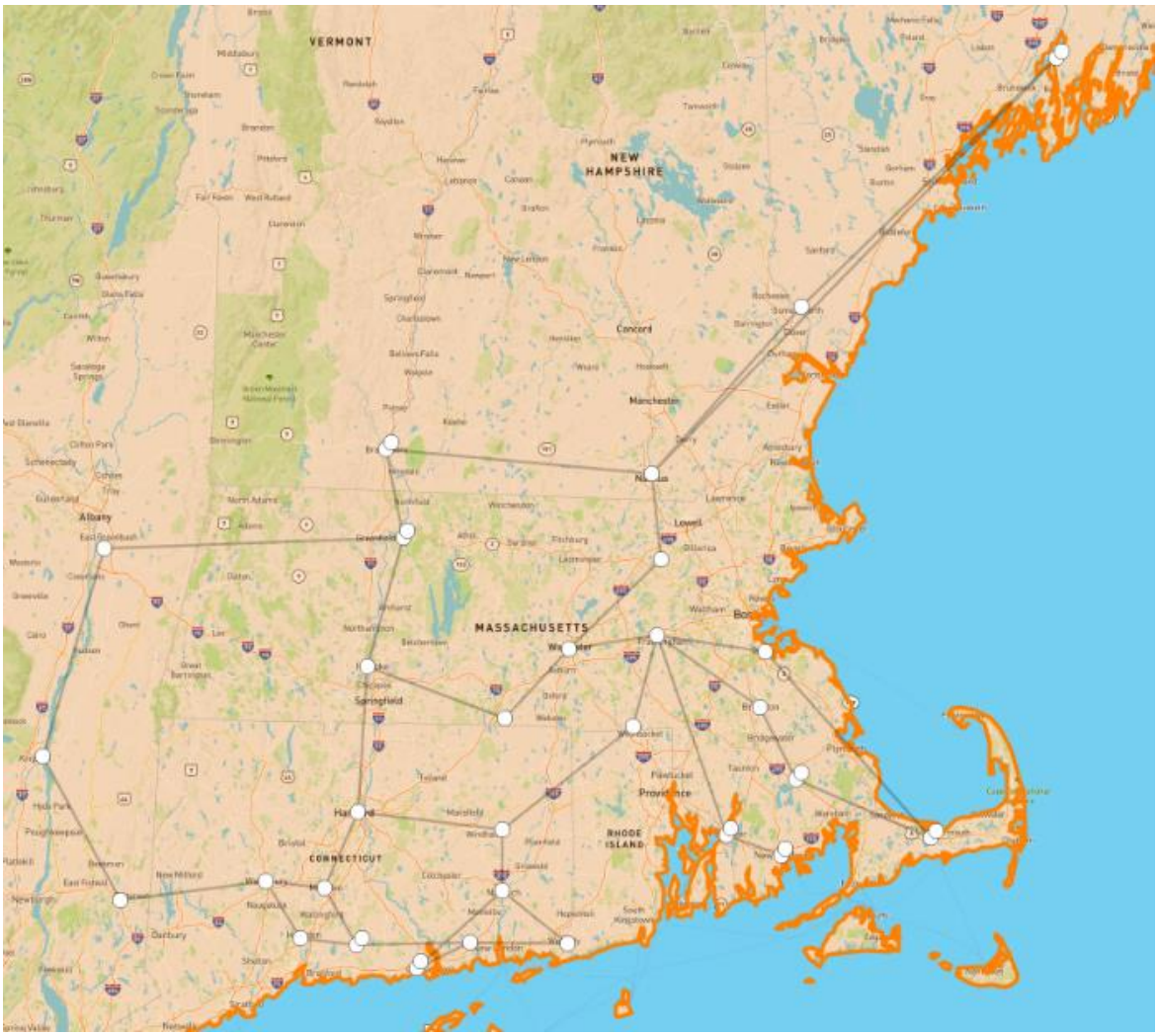


Figure 4.2 One-line diagram of the New England 39-bus system (for illustration only)

Table 4.1 Margin of The Revenue Shortfall

| Capacity Margin | Revenue Margin | Shortfall by attack |
|---|---|---|
| 0% | 0$ | 145026.2$ |
| 25% | 76801.1$ | 68225.1$ |
| 50% | 153602.3$ | N/A (-8577.1$<0) |
| 75% | 230403.4$ | N/A (-185378.2$<0) |

When all of the transmission capacities are auctioned (i.e., the margin is 0), the attack can cause a shortfall of $145,025.20. However, the attack cannot cause shortfalls when the capacity margin is high. For example, when the margin is 75%, a shortfall is not achievable. Furthermore, 47.2% is the critical point for the capacity margin, below which the cyberattack can cause a revenue shortfall.

It is worth mentioning that a conservative revenue margin may lead to inefficient FTR auctions and market operations, although the revenue margin can recover part of the revenue shortfall led by the attacks. Furthermore, the capacity margin does not impact the selection of attack decisions although it diminishes the effectiveness of cyberattacks.

### *4.5.2 Case Study 2: Importance of Real-time Load Deviations*

As shown in Remark 2, RT load deviations can increase/decrease the amount of false data needed to be injected. The following example is considered in order to demonstrate this phenomenon. If the attacker wants to induce a short fall greater than $20,000 shortfall, a negative 90MW line rating attack at line 2-30 can be combined with an attack at bus 25 that increase the demand by 150MW. Similarly, if the RT deviation at bus 25 is more than 150MW, the same shortfall can be achieved without applying the demand attack.

Furthermore, based on the proposed cyber-impact analysis model, the RT load deviation also impacts the effectiveness of cyberattacks on revenue shortfall. Some load deviations may reduce the shortfall caused by attacks, and some load deviations may increase the shortfall caused by attacks. The cyber-impact analysis platform is performed iteratively considering load deviation at each bus from negative 60% to positive 60%. Figure 4.3 shows a heat map describing the impact of load deviation at each bus on revenue shortfall.

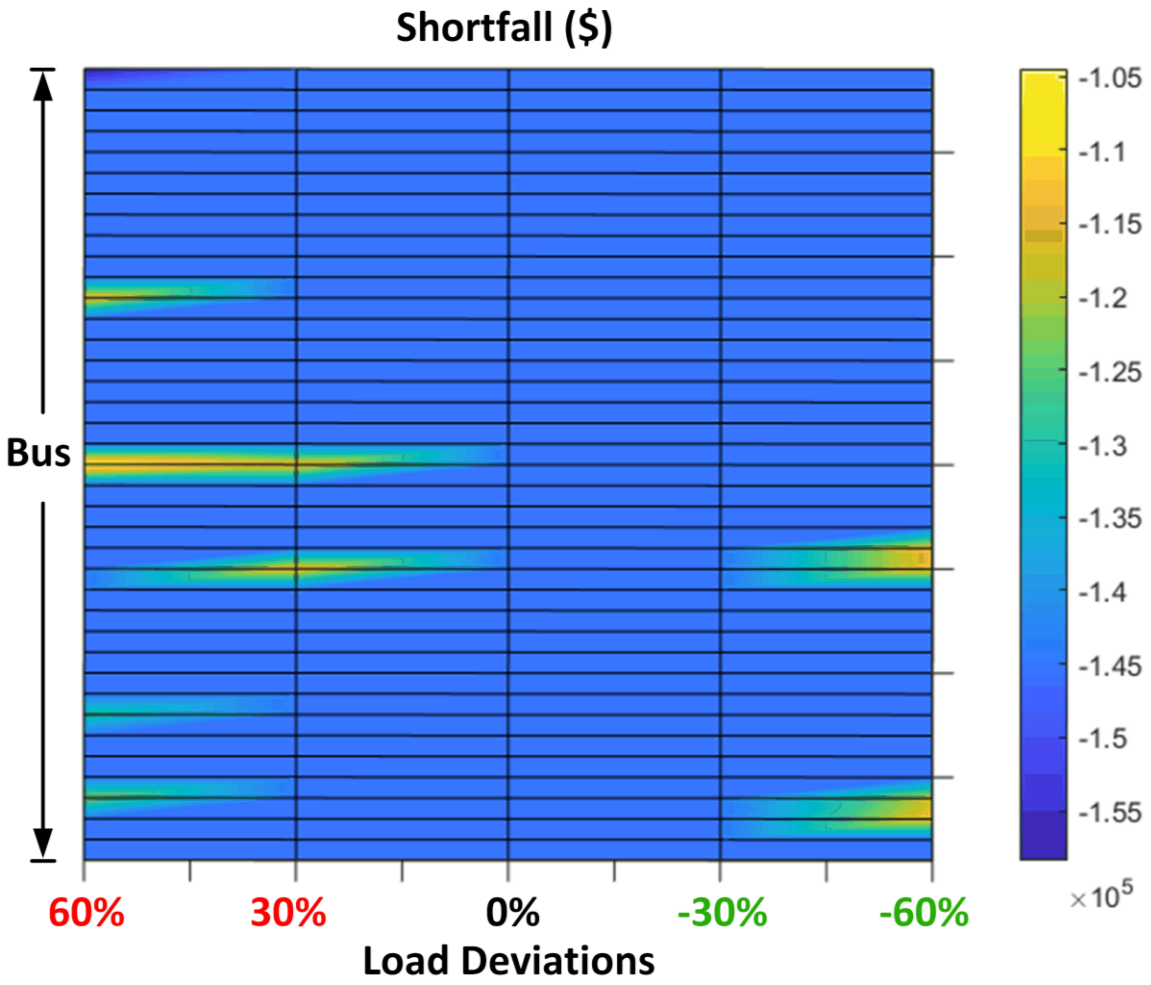


Figure 4.3 Impact of load deviation at each bus on revenue shortfall

The brighter/darker color means that the load deviation decreases/increases the effectiveness of cyberattacks. From the heat map, the load deviations at bus 4, bus 9, bus 16, bus 21, and bus 29 decrease the shortfall. The load deviation at bus 39 can increase the shortfall. Load deviations at other busses have no impact. This phenomenon aligns with Remark 2 that load deviations can help the false data injection but do not necessarily impact the value of shortfalls. The reason is that some load deviations cause a step change at shadow prices, while other deviations do not cause step changes. Thus, load deviation is a vital consideration for designing cyberattacks causing shortfalls. It is worth mentioning that the heat map only shows single bus load deviations for illustrative purposes, and that load deviation may have more impact if combined at different buses.

### *4.5.3 Case Study 3: Importance of Different Types of Attacks.*

As shown in Remark 3, cyberattacks on demands, bids, and unit capacities do not affect revenue adequacy if the attack is not combined with transmission line rating attacks. Thus, the cyber-impact analysis platform is first performed on the three types of attack individually, and the three attacks cannot cause shortfalls, as shown in the first row of Table 4.2. Any penetration level (i.e., the amount of injected false data) cannot induce shortfalls when $r_l$ is 0. The rest of Table 4.2 shows the effectiveness of load attack, bid attack, and unit capacity attack with respect to penetration levels when a line rating attack is fixed to a 20% penetration level ($r_l$ is not 0). The shortfall experiences step changes with demand attack and unit capacity attack because, between the penetration levels of 10% and 15%, both of the attacks induce a step change for shadow prices. The shortfall changes linearly with the penetration level of the bid attack because the value of the bid attack at the marginal unit directly impacts the value of the shadow prices.

Table 4.2 Effectiveness of different types of attacks

| Penetration level | Shortfall by load attack ($ $\times 10^4$) | Shortfall by bid attack ($ $\times 10^4$) | Shortfall by unit attack ($ $\times 10^4$) |
|---|---|---|---|
| $r_l = 0$ | 0 | 0 | 0 |
| 0% | 6.96 | 6.96 | 6.96 |
| 5% | 6.96 | 7.52 | 6.96 |
| 10% | 6.96 | 8.07 | 6.96 |
| 15% | 7.86 | 8.62 | 7.86 |
| 20% | 7.86 | 9.18 | 7.86 |

Table 4.3 shows the shortfall induced by the line rating attack only, and the higher the penetration level, the larger the shortfall will be. The 0% penetration level of the three attacks in Table 4.2 is when the line rating attack happens alone with the 20% penetration level as in table 4.3.

Comparing Table 4.2 and Table 4.3, the line rating attack provides a base value for the shortfall, and the other attacks further increase the shortfalls. This phenomenon aligns with Remark 3 that line rating attacks serve as the base for attacks causing a shortfall, and the other attacks further enhance the severity of the shortfall.

### *4.5.4 Case Study 4: Severity of Revenue Shortfall Caused by Cyberattacks*

As indicated in Remark 4, cyberattacks are able to cause a much more significant impact on revenue shortfall than other unexpected contingency events. This case study compares unexpected contingency events and cyberattacks using the proposed cyber-impact analysis model.

In a DA market-clearing scenario, three lines are congested: line 2-3, line 2-30, and line 6-11. Thus, to induce a revenue shortfall, three unexpected contingency events are considered to be 10% line-derating at each of the lines.

To show the severity of the revenue shortfall caused by a cyberattack fairly, the penetration level of the line rating attack is also considered to be 10%, and the line rating attack can only perform at one line. As show in Figure 4.4, the attack can lead up to 141%, 903%, and 180% shortfall than event 1 to event 3.

Table 4.3 Effectiveness of line rating attack

| Penetration level | 5% | 10% | 15% | 20% |
|---|---|---|---|---|
| Shortfall by line rating attack ($\$ \times 10^4$) | 1.08 | 2.74 | 4.11 | 6.96 |

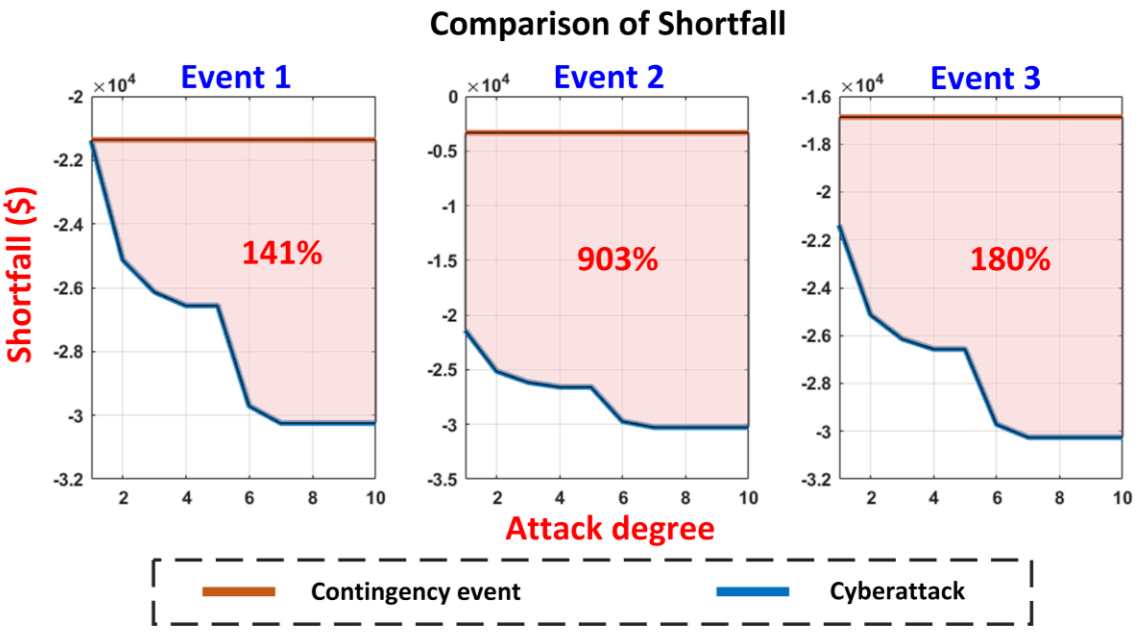


Figure 4.4. Comparison of shortfall between contingency events and cyberattacks

Further, the significant amount of shortfall impacts bilateral transactions. Conventional solutions to cover the revenue shortfall are prorating the settlements to all FTRs, which makes the FTR lose the ability to create a perfect hedge for bilateral contracts when the shortfall is high. The allocation procedure in [47] is considered to be an example. Considering a FTR transaction between node 3 and node 2, the revenue loss due to the shortfall allocation under contingency events and cyberattacks is shown in Table 4.4. The attack can induce up to an 89.4% revenue loss for this FTR, which basically makes the FTR lose its ability to hedge the congestion charge for bilateral transactions.

## 4.6 Conclusions

In conclusion, this Chapter identifies two missing components in current electricity market cybersecurity research: (1) the lack of impact analysis of cyberattacks on ISO revenue adequacy, which prevents ISOs from comprehensively understanding the financial consequences of cyberattacks; and (2) the lack of investigations into the trilevel coupling between attack decisions, ex-ante dispatches, and ex-post pricing because previous research focuses only on the bilevel modeling of the attack and RT market-clearing. Therefore, we first provide a theoretical analysis of the impact of cyberattacks on revenue adequacy by formulating sufficient conditions and summarizing four remarks. Next, a cyber-impact analysis platform for revenue adequacy analysis with an attacker model on the upper-level, an ex-ante model at the middle-level, and an ex-post model at the lower-level is proposed to numerically investigate the impact of cyberattacks on revenue adequacy. In the end, the New England 39-bus system is applied to discuss the theoretical analysis remarks on impact of cyberattacks on revenue adequacy with the proposed numerical analysis platform.

Table 4.4 Revenue loss for FTR 3-2 due to allocation

| | Event 1 | Event 2 | Event 3 | Attack |
|---|---|---|---|---|
| Revenue lost (%) | 48.4 | 32.3 | 36.8 | Up to 89.4 |

# Chapter 5 Optimally Coordinated False Data Injection Attack against Multienergy System and Corresponding Countermeasure

The worldwidely ambition in combating climate change has expediated the renewables penetrations and decarbonizations. Multienergy system (MES) operations, where different energy systems are optimally coordinated, have been recognized as a key element in future low-carbon energy operations. Flexible transitions across different energy vectors will remarkedly facilitate the accommodation of intermittent generation resources. However, optimal energy transitions require intense exchanges of information and control signals, which inevitably intensify the risk of cyberattacks. Existing cybersecurity research works mainly targets single energy system, and there are only a few pioneer cybersecurity analyses for MES, which mainly focus on uncoordinated cyberattacks. A lack of detailed discussion and analysis on the optimally coordinated cyberattack targeting MES prevents operators from accurately evaluating the potential damages of cyberattack in MES operations. Therefore, this paper firstly proposes an optimally coordinated false data injection attack (OC-FDIA) against MES. Then, we show that the OC-FDIA cause much more severe damages than single-system FDIA and uncoordinated FDIAs. Further, an effective countermeasure is developed against the proposed OCFDIA based on deep learning technique (DL). Eventually, the proposed OC-FDIA and its countermeasure are demonstrated through a MES test case integrated with IEEE 39-bus system and 14-bus gas system. More details of this chapter can be found in [J10].

## Nomenclature

*Sets*

| | |
|---|---|
| $node^{gas}$, $node^{e}$ | Set of gas and electric network nodes |
| $line^{gas}$, $line^{e}$ | Set of gas pipelines and electric transmission lines |
| $node^{GW}$, $node^{EG}$ | Set of gas well and electric unit nodes |
| $node^{ptg}$, $node^{gfg}$ | Set of power-to-gas nodes and gas-fired-unit nodes |
| $node^{c}$ | Set of gas compressor node |
| $T$ | Set of time intervals |

*Electric network:*

| | |
|---|---|
| $P_i^{max}$, $P_i^{min}$ | Upper and lower limits for electric units |
| $L_l^{max}$, $L_l^{min}$ | Upper and lower limits for electricity line flow |
| $GSF$ | Generation shift factors |
| $ramp_i^{min}$, $ramp_i^{max}$ | Ramping limits for electric units |
| $D_{i,t}^{E}$ | Electric load |
| $P_{i,t}$ | Generation for electric units |

*Gas network:*

| | |
|---|---|
| $f$, $c$, $D$, $A$, $u_0$ | Friction factor, sound speed in gas pipeline, pipeline diameter, pipeline cross-section area, gas flow velocity |
| $dx$, $dt$ | Pipeline segment length and time interval segment |
| $I_{i,t}^{GW,min}$, $I_{i,t}^{GW,max}$ | Gas well injection boundary |
| $pr_{i,}^{min}$, $pr_i^{max}$ | Gas nodal pressure boundary |
| $D_{i,t}^{G}$ | Gas load |

| | |
|---|---|
| $m_{l,to,t}$, $m_{l,from,t}$ | Gas mass flow at the sending node and receiving node |
| $pr_{i,t}$ | Gas nodal pressure |
| $I_{i,t}^{GW}$ | Gas well injection |

*Energy Conversion Devices:*

| | |
|---|---|
| $\alpha_i$, $\beta_i$ | Gas-fired unit and power-to-gas generation conversion rate |
| $P_i^{gfg,max}$, $P_i^{gfg,min}$, $P_i^{ptg,max}$, $P_i^{ptg,min}$ | Upper and lower limits for gas-fired units and power-to-gas units |
| $P_{i,t}^{ptg,\,e}$, $P_{i,t}^{ptg,\,g}$ | Power-to-gas units power generation for electricity and gas |
| $I_{i,t}^{ptg}$ | Power-to-gas units gas production |
| $P_i^{gfg,\,e}$, $D_i^{gfg}$ | Gas-fired unit generation and gas consumption |

*Attack and countermeasure:*

| | |
|---|---|
| $M_{i,t}^{e,d}$, $M_{i,t}^{g,d}$, $M_{i,t}^{g,\rho}$ | Value of LR-FDIA, GD-FDIA, and GL-FDIA |
| $q_{i,t}^{e,d}$, $q_{i,t}^{g,d}$, $q_{i,t}^{g,\rho}$ | Attack percentage of LR-FDIA, GD-FDIA, and GL-FDIA |
| $\Delta P_{i,t}^{def}$, $\Delta Pro_{i,t}^{def}$ | mitigation value at defending electric unit and gas well |
| $\Delta P_{i,t}^{def,\,max}$, $\Delta Pro_{i,t}^{def,\,max}$ | Boundary of mitigation value |

## 5.1 Introduction

Driven by the Paris Agreement in 2015, worldwide efforts have been put to limit greenhouse gas emissions mitigating climate change. The U.S. has assembled task forces to reach 100% carbon pollution-free electricity by 2035 and achieve net-zero emission by 2050 [53]. The E.U. has published a Climate Change Law making the 55% emission reduction goal legally binding [54].

Among various decarbonization technologies, multienergy system (MES) is becoming one of the most promising solutions for decarbonization [55]. MES supports stable energy transition among different energy vectors shaping the future energy system from fossil-dependence toward renewable-basis. Further, the high-penetration of gas-fired generations (GTG), and deployment of power-to-gas technology have already imposed strong interdependency between power and gas system in operation, planning, and control. Under MES coordination, different energy networks, such as power and gas, can fully utilize energy conversion devices to improve energy efficiency.

The MES operation breaks down the barrier in energy operations and information flow among different energy systems, but it also intensifies the risk of cyberattacks. The notorious cyberattacks on the Ukraine power system in 2015 [56] and the colonial pipeline cyberattack on the U.S. gas sector in 2021 [57] have caused a significant economic loss in power and gas system, respectively. The MES deployment would potentially escalate the impact of such cyberattacks since the coupling between different energy systems is much stronger. For example, the cyberattacks on Ukraine's power system would endanger the natural gas system operations. Previous single system cybersecurity analysis is no longer adequate for MES, and cybersecurity analysis on MES is still under-investigated. A brief literature review is provided as follows.

The concept of MES is defined in [58] as that multiple energy systems optimally interact with each other at various levels, such as a city or a country level. Research work [59] and [60] have provided comprehensive reviews on MES operations and demonstrated the impressive potential of MES in achieving decarbonizations. The existing MES research can be broadly divided into three categories that are advanced modeling, efficient optimization,

and coherent market structures. In the first category, various MES operation models have been proposed. Research work [61] illustrates the limitation of the steady-state gas flow model and provides a convex relaxation scheme for MES operation model considering gas flow dynamics. Research work [62] and [63] propose two new linearized MES operation models reflecting gas dynamics. Research work [64] and [65] focus on integrated heat and electricity operations considering heat dynamics and system planning, respectively. In the second category, efficient optimization techniques are applied to solve MES operation model. In [66] and [67], the MES operation model is optimized by heuristic algorithms and distributed algorithms, respectively. The last category aims to analyze the market settlement and scheme for MES. Research works [68] and [69] capture the market equilibrium in integrated electricity-heat and electricity-gas systems. Research work [70] proposes a locational marginal price formulation to settle the transaction in integrated electricity-heat operations. The above literature is selected as representatives for each of the MES research categories.

Despite the large body of MES research works, the cybersecurity for MES is under-investigated. Existing cybersecurity researches mainly focus on a single energy system, particularly on power systems, as shown in the previous Chapters. Similarly, natural gas system relies on the SCADA system introducing vulnerability from cyberattacks. Research work [71] proposes an undetectable FDIA on gas system measurement data. Research work [72] provides an online-learning detection against FDIA in natural gas power systems.

However, the above single-energy system cybersecurity research is inadequate under MES operation frameworks due to the strong coupling among different energy systems. A few pioneer cybersecurity research works have shifted the focus to MES. Research work [73]

proposes the first FDIA on gas systems targeting gas load and gas density in MES operations. Research work [74] proposes a robust MES dispatch model to ensure a stable integrated operation of the power and heat system under cyberattacks. Research work [75] analyzes the propagation/ripple effect of cyberattack under the MES framework considering power and heat systems. Research work [76] proposes a class of FDI attacks targeting natural gas demand and analyzes their impact on power systems under MES operations. Research work [77] proposes a learning-based detection against cyberattacks targeting energy conversion devices in integrated power and gas system operations. Research work [78] proposes a trilevel defense strategy against transmission line and gas pipeline attacks in integrated power and gas system operations.

The above technical chapters 2, 3, and 4 only concern power system cybersecurity. This chapter extends the scope of this dissertation to multienergy systems. The motivation and contributions are presented as follows. Following the existing MES cybersecurity research works, this paper proposes a new coordinated FDIA (OC-FDIA) strategy and its countermeasure, where FDIAs on different energy systems are coordinated to maximize the damage. The detailed contributions are presented as follows:

- Existing MES cybersecurity research works model natural gas systems without considering gas flow dynamics. However, different from instantaneous power deliveries, gas dynamics are much slower. Steady-state models may fail to represent short-term gas flow changes induced by cyberattacks. This paper proposes and analyzes the OC-FDIA and its countermeasure in MES, considering the characteristics of gas flow dynamics.

- To the best of our knowledge, this paper is the first attempt to propose and analyze the FDIA coordination among different energy systems. Previous works mainly focus on analyzing the propagation effect of cyberattacks in MES, such as how attacks on one energy system impact another system, but the proposed OC-FDIA aims to utilize the propagation effects causing more severe damages. Further, a countermeasure is provided to mitigate the proposed OC-FDIA based on deep learning (DL).

## 5.2 MES Operation Model Considering Gas Dynamics

The large share of gas-fired generations (GfG) and increasing deployment of power-to-gas (PtG) technology has made the coordination between power systems and gas systems one of the most promising ways to improve energy efficiency.

Therefore, the MES in this paper consists of a power system and a natural gas system with flexible energy transition units (i.e., GfG and PtG). The detailed MES operation models are described in the following subsections.

### *5.2.1 Gas network model considering gas flow dynamics*

The electricity is delivered instantaneously, but gas flow could take hours to travel from source to demand, which requires spatio-temporal representations [61]. Under the isothermal condition, equation (1) and (2) describes the gas flow dynamics through a set of partial differential equations.

$$\frac{\P}{\P t} p(x,t) + \frac{4c^2}{pD^2} \frac{\P}{\P x} m(x,t) = 0, \text{"} i \hat{I} node^{gas} \quad (1)$$

$$\frac{\partial}{\partial x}p(x,t) + \frac{4}{pD^2}\frac{\partial}{\partial t}m(x,t) + \frac{\partial}{\partial x}p(x,t)u^2(x,t) = -\frac{8fc^2}{p^2D^5}\frac{m^2(x,t)}{p(x,t)}, \forall i \in node^{gas} \quad (2)$$

Then, a finite difference method is applied to approximate the solution to (1) and (2) as in (3) and (4) based on [62] and [79], which has demonstrated a good balance between model complexity and solution efficiency. Every pipeline in the gas system is segmented by $\Delta x$, and each time interval is segmented by $\Delta t$ based on pipeline physical characteristics. The criteria of $\Delta x$ and $\Delta t$ selection can be found in [61].

$$pr_{i+1,t+1} + pr_{i,t+1} - pr_{i+1,t} - pr_{i,t} + \frac{c^2dt}{dxA}(m_{l,to,t+1} - m_{l,from,t+1} + m_{l,to,t+1} - m_{l,from,t}) = 0 \quad (3)$$
$$, \forall i \in node^{gas}, \forall t \in T$$

$$\frac{1}{A}(m_{l,to,t+1} + m_{l,from,t+1} + m_{l,to,t+1} + m_{l,from,t}) + \frac{dt}{dx}(pr_{i+1,t+1} - pr_{i,t+1} + pr_{i+1,t} - pr_{i,t}) +$$
$$\frac{fu_0dt}{4DA}(m_{l,from,t+1} + m_{l,to,t+1} + m_{l,from,t} + m_{l,to,t}) = 0_i, \quad (4)$$
$$\forall i \in node^{gas}, \forall l \in line^{gas}, \forall t \in T$$

$$m_{i,from,t}, m_{i,to,t} \geq 0_i, \forall i \in Line^{gas}, \forall t \in T \quad (5)$$

For each pipeline segment, (3)-(5) are modeled to represent the gas flow dynamics.

In addition to gas flow equations, gas system state variables are restricted within a certain range due to physical characteristics and security considerations. The upper and lower limits for the gas well supply and gas node pressure are shown in (6) and (7). The gas compressor is modeled in (8) [62], where the nodal pressure can be increased up to $\Gamma$ times at the compressor node.

$$I_{i,t}^{GW,Min} \leq I_{i,t}^{GW} \leq I_{i,t}^{GW,Max}, \forall i \in node^{GW}, \forall t \in T \quad (6)$$

$$pr_i^{\min} \leq pr_{i,t} \leq pr_i^{\max}, \forall i \in node^{gas}, \forall t \in T \quad (7)$$

$$pr_i^{\min} \leq pr_{i,t} \leq \Gamma pr_i^{\max}, \forall i \in node^{c}, \forall t \in T \quad (8)$$

The gas system nodal mass flow balance is formulated in (9).

$$I_{i,t}^{GW} + I_{i,t}^{p2g} - D_{i,t}^{gas} - D_{i,t}^{g2g} + \sum_{L} m_{l,to,t} - \sum_{L} m_{l,from,t} = 0, \forall i \in node^{gas}, \forall t \in T \quad (9)$$

### *5.2.2 Power network model*

A common power system economic dispatch model is shown in (10)-(14). The DC power flow is considered to formulate the power system network constraints. Constraint (10) ensure the overall power balance. Constraints (11)-(14) set the boundary for generator outputs, power flow, and generator ramping, respectively. The presented power system model is common in MES studies, and detailed descriptions can be found in [80] and [81].

$$\sum_{i} P_{i,t} - \sum_{i} D_{i,t}^{E} = 0, \forall i \in node^{e}, \forall t \in T \quad (10)$$

$$P^{\min}{}_{i} \le P_{i,t} \le P^{\max}{}_{i}, \forall i \in node^{EG}, \forall t \in T \quad (11)$$

$$\sum_{i=1}^{N_b} GSF_{l-i}(P_{i,t} - D_{i,t}^{E}) \le L_{l}^{\max} \forall l \in line^{e}, \forall t \in T \quad (12)$$

$$\sum_{i=1}^{N_b} GSF_{l-i}(P_{i,t} - D_{i,t}^{E}) \ge L_{l}^{\min} \forall l \in line^{e}, \forall t \in T \quad (13)$$

$$ramp^{\min}{}_{i} \le P_{i,t} - P_{i,t-1} \le ramp^{\max}{}_{i}, \forall i \in node^{EG}, \forall t \in T \quad (14)$$

### *5.2.3 Energy conversion devices*

Bi-directional energy conversion devices couple the power system and gas system to enhance energy efficiency. The GfG unit consumes gas to generate electricity, which is described by (15). The conversion coefficient $\alpha_i$ represents the energy conversion

relationship and device efficiency. The generation limits of GfG units are restricted by (16) [62].

$$D_{i,t}^{gfg} = a_i P_{i,t}^{gfg}, "i \hat{I} node^{gfg}, "t \hat{I} T \quad (15)$$

$$P_i^{gfg,\min} \pounds P_{i,t}^{gfg} \pounds P_i^{gfg,\max}, "i \hat{I} node^{gfg}, "t \hat{I} T \quad (16)$$

The PtG unit consumes electricity to produce natural gas. For example, surplus renewable energy could be converted to hydrogen gas through PEM-electrolysis technology. The relationship between the produced gas and consumed power can be represented by (17). The subscription *k* and *i* indicate that the PtG is converting energy from bus *i* in the power system to node *k* in the natural gas system. The generation limits of PtG units are restricted by (18) [62].

$$I_{k,t}^{ptg} = b_i P_{i,t}^{ptg,g}, "i \hat{I} p2g \quad (17)$$

$$P_i^{ptg,\min} \pounds \frac{1}{b_i} I_{i,t}^{ptg} + P_{i,t}^{ptg,e} \pounds P_i^{ptg,\max}, "i \hat{I} node^{ptg} \quad (18)$$

### *5.2.4 Overall MES operation model*

The overall objective of the MES operation is to minimize the supply cost, as shown in (19). The power system operation cost consists of conventional unit costs, and PtG unit costs for electricity generation. The gas system operation cost consists of gas well cots and PtG unit costs for gas generations.

$$\min \sum_{t} \left\{ \underbrace{\sum C_{i,t}(P_{i,t}^{TU}) + \sum C_{i,t}(P_{i,t}^{ptg})}_{Power\ System} + \underbrace{\sum C_i(I_{i,t}^{ptg}) + \sum C_i(I_{i,t}^{GW})}_{Gas\ System} \right\}$$

**Subject to**

$$\begin{aligned} &\text{Gas system constraint } (3)\text{-}(9) \\ &\text{Power system constraint } (10)\text{-}(14) \\ &\text{Conversion devices constraint } (15)\text{-}(18) \end{aligned} \tag{19}$$

The operation constraint in power systems, gas systems, and conversion devices are described above. MES operators solve the above optimal dispatch model to determine the power system and gas system dispatches.

In summary, this section describes the operation model of a MES consisting of a power system and a natural gas system. The proposed attack strategy against the MES operation is presented and analyzed in the next section.

## 5.3 Optimally Coordinated FDIA against MES Operations

The proposed Optimally Coordinated FDIA (OC-FDIA) is a bilevel optimization model, where the attacker is modeled at the upper-level, and the overall MES operation model is placed at lower-level. The attacker selects the most effective attack paths in MES operations targeting different energy systems.

**Upper-level attacker model**

Various cyberattack paths in power systems have been proposed and demonstrated in previous literature, such as line rating attacks in [8] and load redistribution (LR) attacks in [11]. A few cyberattack paths in gas systems have also been investigated, such as gas load

attack (GL-FDIA) and gas density attack (GD-FDIA) [73]. The proposed OC-FDIA model considers the most common type of FDIAs in power and gas systems: LR attack, GL-FDIA, and GD-FDIA. Other types of attacks can be easily added similarly based on the interest of future researchers.

The LR attack is modeled through (20)-(21) based on [11]. Constraint (20) is to limit the attack magnitude ensuring the stealthy. Constraint (21) ensure the total load is unchanged.

$$- q_{i,t}^{e,d} D_i^E \le M_{i,t}^{e,d} \le q_{i,t}^{e,d} D_{i,t}^E, \ \forall i \in node^e, \forall t \in T \tag{20}$$

$$\sum_i M_i^{e,d} = 0, \ \forall i \in node^e, \forall t \in T \tag{21}$$

Similar to the LR attack, the GL-FDIA and GD-FDIA are modeled in (22)-(24) based on [73]. Different from the [73], which considers a steady-state gas flow model, this paper includes gas flow dynamics. Therefore, the gas density impacts the value of gas pressure as in (24) instead of the Weymouth coefficient. The attacker's objective considered in this paper is to damage the operation cost (19), but any other objectives can be integrated similarly.

$$- q_{i,t}^{g,d} D_{i,t}^G \le M_{i,t}^{g,d} \le q_{i,t}^{g,d} D_{i,t}^G, \ \forall i \in node^{gas}, \forall t \in T \tag{22}$$

$$0 \le M_{i,t}^{g,r} \le s_{i,t}^{g,r} r_{i,t}^{g,r}, \ \forall i \in node^{gas}, \forall t \in T \tag{23}$$

$$pr_{i,t} = pr_{i,t} + c^2 M_{i,t}^{g,r}, \forall i \in node^{gas}, \forall t \in T \tag{24}$$

**Lower-level MES operation**

Considering the LR attack, GL-FDIA, and GD-FDIA, the normal MES operation model is disturbed. Power balance constraint remains the same because attack constraint (21)

restricts the sum of LR equal to 0. The power flow constraints (12)-(13) become (25)-(26). Although the total generation remains the same, an effective LR attack changes the marginal pattern of economic dispatches.

$$\sum_{i=1}^{N_b} GSF_{l-i}(P_{i,t} - D_{i,t}^{E} + M_{i,t}^{e,d}) \le L_l^{\max}, \forall l \in L, \forall t \in T \tag{25}$$

$$\sum_{i=1}^{N_b} GSF_{l-i}(P_{i,t} - D_{i,t}^{E} + M_{i,t}^{e,d}) \ge L_l^{\min}, \forall l \in L, \forall t \in T \tag{26}$$

The gas flow equation (3) and (4) is reformulated to (27) and (28) under the GD-FDIA.

$$\begin{aligned} &pr_{i+1,t+1} + pr_{i,t+1} - pr_{i+1,t} - pr_{i,t} + c^2(M_{i+1,t+1}^{g,r} + M_{i,t+1}^{g,r} - M_{i+1,t}^{g,r} - M_{i,t}^{g,r}) \\ &+ \frac{c^2 dt}{dxA}(m_{l,to,t+1} - m_{l,from,t+1} + m_{l,to,t+1} - m_{l,from,t}) = 0 \\ &, \forall i \in node^{gas}, \forall t \in T \end{aligned} \tag{27}$$

$$\begin{aligned} &\frac{1}{A}(m_{l,to,t+1} + m_{l,from,t+1} + m_{l,to,t+1} + m_{l,from,t}) + \frac{dt}{dx}\left\{pr_{i+1,t+1} - pr_{i,t+1} + pr_{i+1,t} - pr_{i,t} \right. \\ &\left. + c^2(M_{i+1,t+1}^{g,r} - M_{i,t+1}^{g,r} + M_{i+1,t}^{g,r} - M_{i,t}^{g,r})\right\} \\ &\frac{fu_0 dt}{4DA}(m_{l,from,t+1} + m_{l,to,t+1} + m_{l,from,t} + m_{l,to,t}) = 0, \forall i \in node^{gas}, \forall l \in line^{gas}, \forall t \in T \end{aligned} \tag{28}$$

The gas nodal pressure boundary is reformulated to (29).

$$pr_i^{\min}{}_i \le pr_i + c^2 M_{i,t}^{g,r} \le pr_i^{\max}{}_i, \forall i \in node^{gas} \tag{29}$$

The gas nodal balance equation (9) is reformulated to (30) under the GL-FDIA.

$$I_{i,t}^{GW} + I_{i,t}^{ptg} - D_{i,t}^{gas} - D_{i,t}^{g2g} - M_{i,t}^{g,d} + \sum_{L} m_{l,to,t} - \sum_{L} m_{l,from,t} = 0_i, \forall i \in node^{gas}, \forall t \in T \tag{30}$$

The overall OC-FDIA model is shown in (31). By considering multiple types of FDIAs in different energy systems, the optimization model provides an optimal FDIA combination.

$$\max \quad (19)$$

**Subject to**

$$\text{Attack constraint } (20)\text{-}(24) \tag{31}$$

$$M^{E,d}_{i,t}, M^{G,d}_{i,t}, M^{G,r}_{i,t} \in \underbrace{\arg}_{\text{Attack decision}} \left\{ \text{Lower-level problem: } (5),(6),(10),(11),(14),(25)\text{-}(30) \right\}$$

**Why the OC-FDIA cause more server damages**

The above subsection proposes a new type of cyberattack named OC-FDIA coordinate FDIA targeting different energy systems to cause more damage to MES operations. This subsection will analytically illustrate the severity of the proposed OC-FDIA by comparing it with single-system and uncoordinated FDIAs, and the case study in Section V will numerically demonstrate the severity of the proposed OC-FDIA.

**Traditional single-system FDIA**

This type of FDIA has a minimal impact on other energy systems in general. For example, if a LR attack happens at power systems, the disturbance could be entirely covered by conventional units, and the gas system operation is not impacted. Even if the attack disturbs the GfG unit generations, causing a change $\Delta d^{G}_{i,t}$ in the gas consumptions, the MES operation model tries to cover the $\Delta d^{G}_{i,t}$ at minimal cost, decreasing the impact, as shown in Figure 5.1.

**Uncoordinated FDIA in MES operations**

This type of FDIA disturbs multiple energy systems, but the impact may not be significant. For example, if a LR attack $\Delta d^{E}$ increases the generations and gas consumption of a GfG unit, a FDIA $\Delta d^{G}$ at gas systems may lower the gas supply price for the GfG unit (e.g., switch from PtG to gas well).

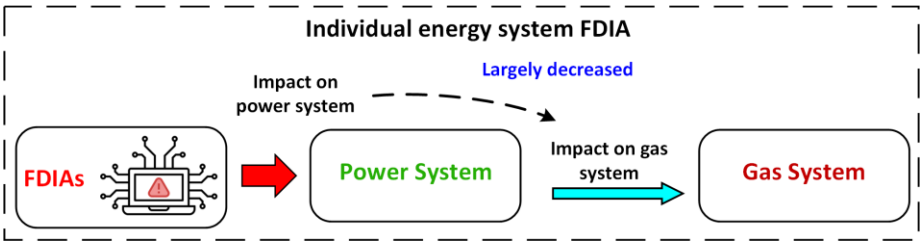


Figure 5.1. Individual energy system FDIA

Then, the effectiveness of $\Delta d^E$ is decreased, although the $\Delta d^G$ also damages the operation. Without coordination, FDIA at different systems may decrease each other's impact, as shown in Figure 5.2

(3) The proposed OC-FDIA

Figure 5.3 illustrates the structure of the OC-FDIA, where the FDIA at power systems is strategically coordinated with FDIA at gas systems to cause more damage. Considering the same scenario when a $\Delta d^E$ increase the generations and gas consumption of a GfG unit, the FDIA $\Delta d^G$ may try to switch the gas supply at GfG unit from the gas well to PtG, increasing the operation cost.

In summary, the conventional single-system FDIA has limited impact on other systems, and FDIA at different energy systems may cancel the impact with each other without coordination. However, the proposed OC-FDIA will coordinate the FDIA at different energy systems to amplify the damage to the MES operations.

## 5.4 Countermeasure to The Proposed OC-FDIA

This section develops a countermeasure to mitigate the proposed OC-FDIA.

### *5.4.1 Countermeasure model formulation*

The countermeasure adjusts the dispatch to mitigate the OC-FDIA by perturbing the boundary of the operation model. Without the mitigation action, the attacker freely applies the OC-FDIA model to achieve maximum damage to the system. With the mitigation action, the OC-FDIA deviates from the optimal solution, which decreases the damage.

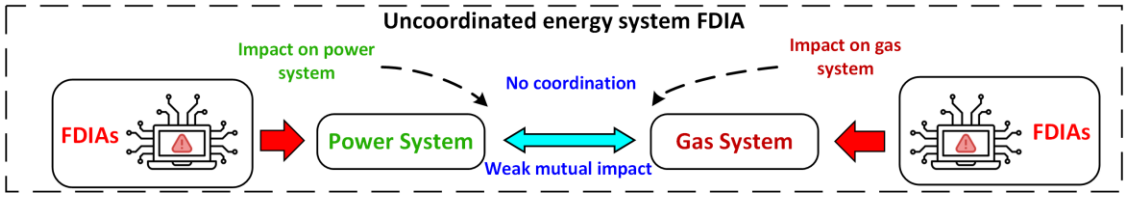


Figure 5.2. Uncoordinated FDIA

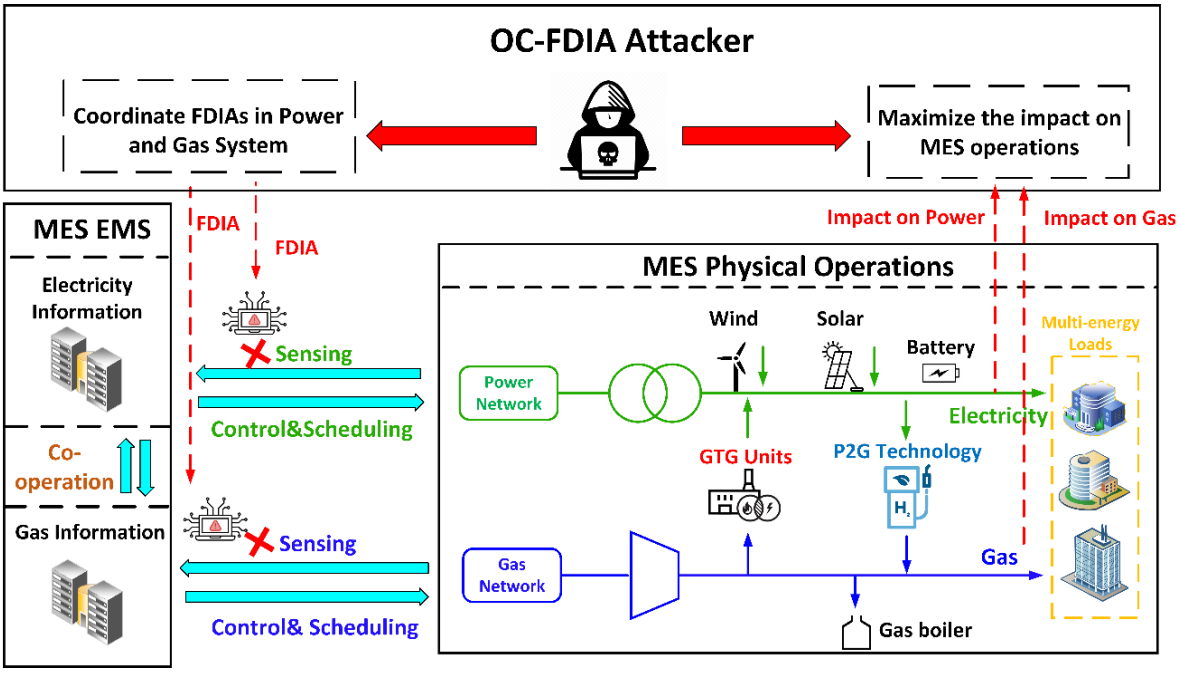


Figure 5.3. OC-FDIA

The mitigation strategy represents a robust MES dispatch result, where the OC-FDIAs are not able to cause expected damage.

Defending units are selected to perform the mitigation actions, and perturbation variables are restricted, as shown in (32)-(33). The $\Delta P_i^{def}$ and $\Delta P_i^{def}$ are the boundaries of perturbations on defending units. The MES dispatch is also perturbed by the mitigation actions, as shown in (34) and (35).

$$\Delta P_i^{def,\max} \le \Delta P_i^{def} \le 0, \forall i \in node^{E,def} \tag{32}$$

$$\Delta Pro_i^{def,\max} \le \Delta Pro_i^{def} \le 0, \forall i \in node^{G,def} \tag{33}$$

$$P^{\min}_i \le P_{i,t} \le P^{\max}_i - \Delta P_i^{def}, \forall i \in node^{e,def}, \forall t \in T \tag{34}$$

$$I_{i,t}^{GW,Min} \le I_{i,t}^{GW} \le I_{i,t}^{GW,Max} - \Delta Pro_i^{def}, \forall i \in node^{g,def}, \forall t \in T \tag{35}$$

The overall mitigation model is a two-stage optimization model, as shown in (36)-(38). The mitigation action is determined at the first stage and aims to maximize the mitigation effectiveness (29) and minimize the no-attack loss (38), which are realized in the second stage. The following three factors are considered in the model to ensure practical implementation of the proposed countermeasure.

- Firstly, mitigations result in robust operations decreasing the impact of cyberattacks, but they inevitably deviate normal MES operations from the optimal dispatch. This means that when there is no attack, mitigations induce loss to normal MES operations. In an ideal situation, mitigation strategies are only applied when the attack happens, which means the “no-attack loss” is 0. However, defenders/operators generally cannot accurately foresee when the attack will happen. Experienced operators are more likely to estimate the possibility of being attacked instead of sensing the exact attack directly.

Therefore, the proposed countermeasure is modeled to maximize the mitigation ability (37) and minimize the no-attack loss (38). A list of mitigation actions is provided to operators to choose based on their preference.

- Secondly, the defender hardly knows the capability of attackers until the operation has been damaged, and attackers hardly know mitigation actions before they launch the attacks. Defenders anticipate potential OC-FDIAs under different attack abilities (e.g., variable $q$), without knowing the exact value. Attackers anticipate the MES operation without knowing the mitigation action. Therefore, the mitigation strategy is a two-stage model instead of Stackelberg model. The first stage determines the mitigation action (36). The second stage (37)-(38) realizes the effectiveness of the no-attack loss and mitigation action against OC-FDIA.
- Thirdly, mitigation is achieved by perturbing the boundary of defending units to disturb the solution of OC-FDIA. The perturbation of defending units is always negative to ensure the feasibility, and defending units are selected from base units, which are generally dispatched at maximum. Operators are suggested to select defending units as less as possible to decrease the no-attack loss.

***First stage:*** *determine mitigations*

$$\begin{aligned} &\text{Determine } \mathrm{D}P_i^{def}, \mathrm{D}Pro_i^{def} \\ &\textit{Subject to} \\ &\text{Perturbation constraint } (32),(33) \end{aligned} \tag{36}$$

***Second stage:*** *realization of mitigation abilities and no-attack loss*

$$\min_{\text{Mitigate}} \{\text{OC- FDIA model (31)}, (34), (35) \text{ replace } (6), (11)\} \quad (37)$$

**Mitigation Effectiveness**

$$\min_{\text{Decrease}} \{\text{MES operation model (19)}, (3)\text{-}(5), (7)\text{-}(10), (12)\text{-}(18), (34), (35)\} \quad (38)$$

**No-attack Loss**

### *5.4.2 Solution methodology*

The proposed countermeasure (36)-(38) is a two-stage model with a bilevel optimization integrated at the second stage, which requires expensive computations. The objective of the first stage variables is to minimize the expectation over a series of bilevel models, which impedes model-based algorithms from returning a valid solution timely. Therefore, deep learning is applied to facilitate the optimization process. General descriptions of the applied deep neural network (DNN) model, including the active function and affine transformation function can be found in [82] and [83]. Two DNNs are trained and applied to quickly approximate the optimal solution of (36)-(38). The overall process is shown in Figure 5.4. Firstly, a DNN, named comprehensive search DNN (CS-DNN), is trained to replace the mapping from first-stage mitigation action to the second-stage mitigation effectiveness and no-attack loss. The training data consists of a group of mitigation samples generated uniformly according to constraints (36) and (37), a group of mitigation effectiveness under different attackers by solving (37), and a group of no-attack loss by solving (38) based on generated mitigation samples. The DNN mapping is almost instantaneous. Therefore, the well-trained CS-DNN is used to give a comprehensive search over a large number of randomly generated mitigation samples. Among a large amount of output, a list of optimal solutions can be identified as the minimal no-attack loss (37) and maximum mitigation effectiveness (38).

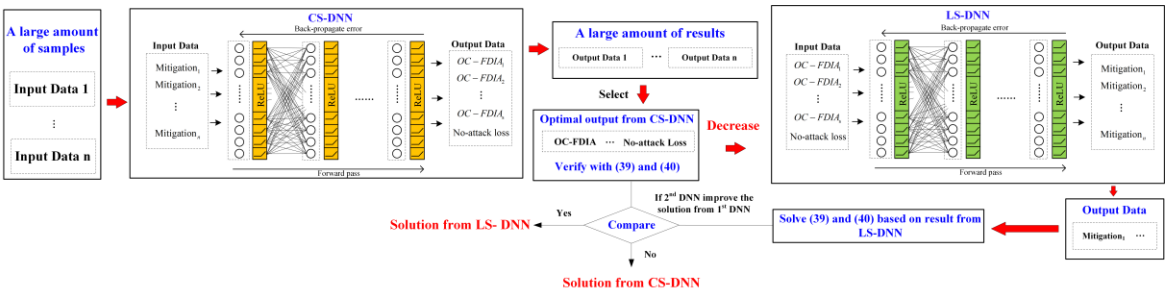


Figure 5.4. Overall process of the applied

Secondly, a DNN, named local search DNN (LS-DNN), reverses the input-output relationship of the CS-DNN, which means that the LS-DNN is trained with the value of mitigation effectiveness and no-attack loss as input and with mitigation actions as output. In this way, the well-trained LS-DNN will output mitigation actions that correspond to the given mitigation effectiveness and no-attack loss. It is worth noting that the input data for the well-trained LS-DNN needs to be close to the training set to ensure the mapping accuracy. Therefore, for each optimal solution from the CS-DNN, a small perturbation is applied to increase the value of mitigation effectiveness and decrease no-attack loss value. The increased mitigation effectiveness and decreased no-attack loss are applied as input to the LS-DNN, which returns a corresponding new mitigation action. If the mitigation action returned from the LS-DNN provides a better no-attack loss and mitigation, then the solution from the LS-DNN is used. Otherwise, the solution from the CS-DNN is used.

In one word, the CS-DNN provides a comprehensive random search over the solution space since the DNN mapping is extremely fast and the number of defending units is small. The LS-DNN aims to progress around the solution returned from the CS-DNN. Through the two DNN approximations, operators are provided with a speedy tool to determine mitigation actions. The mitigation effectiveness is shown in section V.B, and the training of the DNNs are described in the Appendix.

## 5.5 Case Study

In this section, numerical studies are performed to demonstrate the proposed OC-FDIA and its countermeasure. The simulation is performed on a widely used MES case consisting of an IEEE 39-bus NEW England test system [52] and a 14-bus gas system [84]. Detailed

parameters can be found in [52] and [84]. Simulation runs were performed in MATLAB 2017 on a laptop with an Intel i7-8650U processor and 16 GB RAM.

### *5.5.1 Analyses of OC-FDIA in MES operations*

**Significant loss caused by the proposed OC-FDIA**

In this study, the damage caused by OC-FDIA is compared with conventional single system FDIA and uncoordinated FDIA strategies. The attacker is assumed to be able to launch attacks on all of the electricity and gas buses under the attack budget constraint. The single system FDIA is considered optimal FDIA in the power system alone and optimal FDIA in the gas system alone with the same attack penetration level as OC-FDIA. Although single system FDIAs inject false data in one energy system, they generally cause propagation/ripple effects, meaning that the other system is impacted through energy coupling in MES. The uncoordinated FDIA strategies are considered the combination of the single system FDIAs. The LR attack penetration ability, GL-FDIA penetration ability, and GD-FDIA penetration ability gradually increase with a maximum value of 26%. The operation cost loss caused by OC-FDIA, single system FDIA, and uncoordinated FDIA are compared in Table 5.1.

Overall, the OC-FDIA is expected to cause 83.1%, 374.7%, and 33.1% more loss than the two single-system FDIAs and uncoordinated FDIA. The OC-FDIA leads to more server damage than other FDIAs in Table 5.1. It is worth noting the difference between the loss caused by OC-FDIA and others sharply increases with the attack ability. When the attack ability is low, the difference between the loss caused by OC-FDIA and others is less

significant. For example, when the attack ability is 5%, the loss caused by OC-FDIA is only 2.7% more than the loss caused by the uncoordinated FDIA, but the loss difference increases to 43.5% when the attack ability is increased to 25%. In one word, the OC-FDIA can cause much more severe damages than conventional FDIAs, and the impact of the OC-FDIA sharply increases when the attacker is more competent because higher attack abilities offer more room for FDIA in different energy systems to coordinate.

Further, loss caused by uncoordinated FDIA is generally not equal to the sum of loss caused by two single-system FDIAs, although the considered uncoordinated FDIA is a combination of the two single-system FDIAs. When the attack ability is as low as 5%, loss caused by uncoordinated FDIA equals to the sum of loss caused by two single-system FDIAs (i.e., the value of column 5 equals to the sum of the value of column 3 and column 4). The reason is that the FDIAs do not lead to propagation/ripple effects when attack ability is low, which means that the FDIA on one system does not impact the operation of another system.

When the attack ability is higher, the propagation/ripple effects emerge. It is worth noting that the loss caused by uncoordinated FDIA could be less than the sum of loss caused by two single-system FDIAs (i.e., the value of column 5 less than the sum of the value of column 3 and column 4), such as the third row in Table 5.1. The reason is that the propagation/ripple effects could cancel the impact of each other without coordination between FDIAs. However, the OC-FDIA coordinates FDIAs by utilizing the propagation/ripple effects to maximize the damage to MES operations. The above observations show that the propagation/ripple effects are vital for the proposed OC-FDIA to cause more damage than other FDIAs.

Table 5.1. Loss caused by OC-FDIA, single system FDIA, and uncoordinated FDIA

| | **OC-FDIA** | **FDIA on Power** | **FDIA on Gas** | **Uncoordinated FDIA** |
|---|---|---|---|---|
| **5%** | 3911.2$ | 2700.0$ | 1106.6$ | 3806.6$ |
| **10%** | 9615.9$ | 7331.2$ | 2208.4$ | 8323.0$ |
| **15%** | 14199.9$ | 10040.5$ | 2532.5$ | 12839.4$ |
| **20%** | 22054.2$ | 12394.0$ | 4848.9$ | 17356.8$ |
| **25%** | 37200.4$ | 17793.9$ | 7539.8$ | 25921.0$ |

**Propagation effect of the proposed OC-FDIA**

Therefore, the propagation/ripple effects from the OC-FDIA are analyzed next. The OC-FDIA consists of two FDIAs targeting power and gas networks, denoted as IN-FDIA. The two IN-FDIAs are different from previous single-system FDIAs, and they are the FDIA that CO-FDIA injects into different energy systems. Figure 5.5 compares the propagation/ripple effects of the proposed OC-FDIA, where the two IN-FDIAs are injected together, with the propagation/ripple effects when the two IN-FDIAs are injected separately. Although the false data value of OC-FDIA is the same as the two IN-FDIAs, the coordination by OC-FDIA causes more damage. The green area in the upper subplot of Figure 5.6 represents the extra loss caused by the OC-FDIA than the loss sum of two IN-FDIAs. The extra loss increases with the increasing attack ability percentage. The green area represents the extra 40.3% loss by the OC-FDIA. Then, the propagation effect from power system to gas system and from gas system to power system are examined individually.

### *5.5.2 Countermeasure to the proposed OC-FDIA*

**Effectiveness of the Mitigation Against OC-FDIA**

Two units are determined as defending units for perturbations: a power unit at electricity node 31 and a gas well at gas node 4. Based on operators' experience, the attacker with penetration ability from 2% to 26% happens with the same possibility, and they can launch attacks at electricity node 7, 23, and 29 and gas node 11 and 14. The applied DNNs find the optimal mitigation to perturb the boundary of the two defending units by 7.6% and 5.5%, respectively.

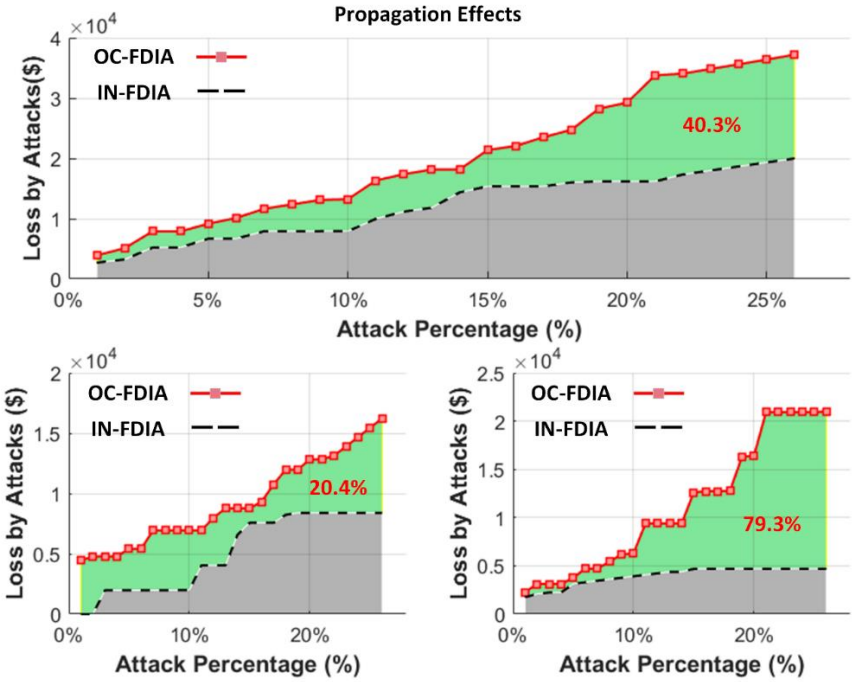


Figure 5.5. Propagation effect of the proposed OC-FDIA

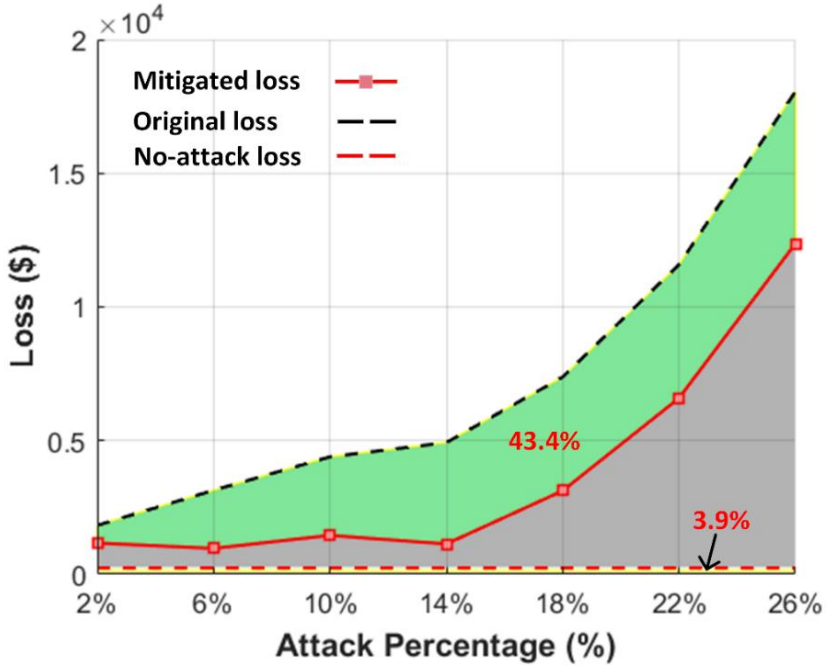


Figure 5.6. Mitigation effectiveness and no-attack loss

The training and accuracy for the applied DNNs can be found in the Appendix section. The result of mitigation effectiveness and no-attack loss are shown in Figure 5.6.

Under the mitigation action, the effectiveness of OC-FDIA is decreased by 43.4%, as shown in the green area, which largely discourages attackers from launching such attacks. It is worth noting that the loss under mitigation is similar when penetration is less than 14%, which means the mitigation can always achieve a desirable value, but when penetration is higher than 14%, the mitigated loss increases with the loss by OC-FDIA. It is worth noting that mitigation actions induce loss to normal operations when there is no attack, as shown in the yellow area of Figure 5.6, but the no-attack loss is considerably small, which is only 3.9% of the normal operations. Therefore, the mitigation provides operation a solution to largely mitigate the OC-FDIA attack without sacrificing large losses on normal operations.

Further, operators may have different preferences on the bearable no-attack loss and the desired mitigation. A list of mitigation actions can be generated by applying the DNNs rapidly. Four different mitigations are provided in Table 5.2.

If the operator can bear a higher no-attack loss, the mitigation effectiveness can be increased. However, it should be noted that mitigation effectiveness increases much slower. For example, when the no-attack loss increases almost ten times (i.e., from 1.3% to 12.3%), the mitigation effectiveness only increases 30% (i.e., from 37.1% to 48.6%). Operators can apply different mitigation actions from the list based on their preferences.

Table 5.2. Mitigation action list

| | **1** | **2** | **3** | **4** |
|---|---|---|---|---|
| **No-attack Loss (Yellow Area in Fig. 6)** | 1.3% | 3.9% | 8.6% | 12.3% |
| **Mitigation Effectiveness (Green Area in Fig. 6)** | 37.1% | 43.4% | 46.8% | 48.6% |
| **Defensing unit 1** | 1.2% | 7.6% | 9.3% | 13.3% |
| **Defensing unit 2** | 3.4% | 5.6% | 6.7% | 8.9% |

# Chapter 6 Conclusions and Future Works

## 6.1 Conclusions and Contributions

With the rapidly increasing financial-motivated cyberattack, such as ransomwares, the financial risk is of equal significance to the catastrophic physical consequences of power system cyberattacks.

Chapter 2 demonstrates 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 goal of this chapter is to demonstrate the necessity of considering market-level signals in developed cyberattack defense strategies.

Chapter 3 proposes a CVA model for operators to perform impact analysis on market cyberattacks. Then, four vital components related to power market cyber vulnerability are discussed, and four vulnerability analysis algorithms are proposed. The proposed algorithms can help the market operator identify highly probable attack targets, devastating attack targets, risky load levels, and the mitigation ability of different defense degrees. In summary, the proposed CVA model provides a new method to identify various aspects that are vulnerable to cyberattacks in market operation, which provides valuable references for further development of cyber defense strategy.

Chapter 4 first identifies two missing components in current electricity market cybersecurity research: (1) the lack of impact analysis of cyberattacks on ISO revenue

adequacy, which prevents ISOs from comprehensively understanding the financial consequences of cyberattacks; and (2) the lack of investigations into the trilevel coupling between attack decisions, ex-ante dispatches, and ex-post pricing because previous research focuses only on the bilevel modeling of the attack and RT market-clearing. Then, we provide a theoretical analysis of the impact of cyberattacks on revenue adequacy by formulating sufficient conditions and summarizing four remarks. Next, a cyber-impact analysis platform for revenue adequacy analysis with an attacker model on the upper-level, an ex-ante model at the middle-level, and an ex-post model at the lower-level is proposed to numerically investigate the impact of cyberattacks on revenue adequacy.

Chapter 5 extend the cybersecurity investigation in this dissertation to multienergy system. An optimal coordinated FDIA model, named OC-FDIA, is proposed, where FDIAs at different energy systems are coordinated to caused more damages. Then, a countermeasure to the proposed OC-FDIA is developed to mitigate the damage based on DNNs. Operators are provided with a list of mitigation actions, which compromises between mitigation effectiveness and no-attack loss. Eventually, the severity of the proposed OC-FDIA and the effectiveness of the developed countermeasure are demonstrated and discussed analytically and numerically.

## 6.2 Suggestion for Future Works

This dissertation can be improved and extended in the following aspects:

- This work mainly focusses on analyzing the impact of cyberattack on electricity operations, although the chapter 5 extends the scope to multienergy system. With the promotion of decarbonization and clean energy generation, the development of

multienergy system has becoming increasingly important. We will perform more comprehensive cybersecurity analysis over multienergy system operations.

- The growth of distributed energy resources, the integration of renewable generations, the deployment of smart meters, etc., are burdening conventional cybersecurity analysis. The complex, versatile, and large amount of data gathering and handling will overload the traditional model-based approach and necessitate an AI-based cybersecurity analysis and defense. We will apply cutting-edge AI techniques for efficient power market cybersecurity analysis under the context of clean generations.

# References


[1] 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 Grid*, vol. 8, no. 4, pp. 1630–1638, Jul. 2017.

[2] G. Liang, S. Weller, J. Zhao, F. Luo, and Z. Dong, ‘‘The 2015 Ukraine blackout: Implications for false data injection attacks,’’ *IEEE Trans. Power Syst.*, vol. 32, no. 4, pp. 3317–3318, 2017.

[3] T. Tsvetanov, and S. Slaria. "The effect of the Colonial Pipeline shutdown on gasoline prices." *Economics Letters*, vol. 209, 2021.

[4] 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.

[5] Q. Zhang, F. Li, Q. Shi, K. Tomsovic, J. Sun and L. Ren, "Profit-Oriented False Data Injection on Electricity Market: Reviews, Analyses, and Insights," in IEEE Transactions on Industrial Informatics, vol. 17, no. 9, pp. 5876-5886, Sept. 2021.

[6] Khanna, K., Panigrahi, B.K., Joshi, A.: “Bid modification attack in smart grid for monetary benefits,” *IEEE Int. Symp. on Nanoelectronic and Information Systems (iNIS)*, 2016, pp. 224–229.

[7] H. S. Karimi, K. Jhala, B. Natarajan, “Impact of Real-Time Pricing Attack on Demand Dynamics in Smart Distribution Systems,” *North American Power Symposium (NAPS)*, 2018, pp. 1-6.

[8] 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.

[9] J. Kim and L. Tong, "On topology attack of a smart grid: Undetectable attacks and countermeasures," *IEEE J. Sel. Areas Commun.,* vol. 31, no. 7, pp. 1294–1305, Jul. 2013.

[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. 9, no. 4, pp. 3820-3829, Mar. 2017.

[11] Y. Yuan, Z. Li, and K. Ren, "Modeling load redistribution attacks in power systems," *IEEE Trans. Smart Grid,* vol. 2, no. 2, pp. 382–390, Jun. 2011.

[12] M. Esmalifalak, G. Shi, Z. Han, and L. Song, "Bad data injection attack and defense in electricity market using game theory study," *IEEE Trans. Smart Grid,* vol. 4, no. 1, pp. 160–169, Mar. 2013.

[13] J. Ma, Y. Liu, L. Song, and Z. Han, "Multiact dynamic game strategy for jamming attack in electricity market," *IEEE Trans. Smart Grid,* vol. 6, no. 5, pp. 2273–2282, Sep. 2015.

[14] M. Esmalifalak, H. Nguyen, R. Zheng, L. Xie, L. Song, and Z. Han, "A stealthy attack against electricity market using independent component analysis," *IEEE Syst. J.,* vol. 12, no. 1, pp. 297–307, Mar. 2018.

[15] M. R. Mengis and A. Tajer, "Data injection attacks on electricity markets by limited adversaries: Worst-case robustness," *IEEE Trans. Smart Grid,* vol. 9, no. 6, pp. 5710–5720, Nov. 2020.

[16] 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.

[17] 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.

[18] V. Kekatos, G. B. Giannakis, and R. Baldick, “Online energy price matrix factorization for power grid topology tracking,” *IEEE Trans. Smart Grid*, vol. 7, no. 3, pp. 1239–1248, May 2016.

[19] M. Esmalifalak, Z. Han, and L. Song, “Effect of stealthy bad data injection on network congestion in market-based power system,” in *Proc. IEEE Wireless Commun. Netw. Conf.*, Apr. 2010, pp. 2468–2472.

[20] J.-W. Kang, I.-Y. Joo, and D.-H. Choi, “False data injection attacks on contingency analysis: Attack strategies and impact assessment,” *IEEE Access*, vol. 6, pp. 8841–8851, 2018.

[21] Q. Zhang and F. Li, "Cyber-Vulnerability Analysis for Real-Time Power Market Operation," in *IEEE Transactions on Smart Grid*, vol. 12, no. 4, pp. 3527-3537, July 2021.

[22] 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.

[23] L. Jia, R. Thomas, and L. Tong, “Malicious data attack on real-time electricity market,” in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process.*, May 2011, pp. 5952–5955.

[24] D.-H. 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.

[25] G. Liang, S. R. Weller, F. Luo, J. Zhao, and Z. Y. Dong, "Generalized FDIA-based cyber topology attack with application to the australian electricity market trading mechanism," *IEEE Trans. Smart Grid*, vol. 9, no. 4, pp. 3820–3829, Jul. 2017.

[26] S. Bi, Y. J. Zhang, "False-data injection attack to control real-time price in electricity market", *IEEE Global Communications Conference (GLOBECOM)*, 2013, pp. 772-777.

[27] 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 Transactions on Smart Grid*, vol. 10, no. 2, pp. 1949–1959, Dec. 2017.

[28] 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.

[29] Dae-Hyun Choi and Le Xie, "Impact of power system network topology errors on real-time locational marginal price", *Journal of Modern Power Systems and Clean Energy*, vol. 5, no. 5, pp. 797-809, Sep. 2017.

[30] L. Jia, J. Kim, R. J. Thomas, and L. Tong, "Impact of data quality on real-time locational marginal price," *IEEE Trans. Power Syst*., vol. 29, no. 2, pp. 627–636, Mar. 2014.

[31] D.-H. Choi and L. Xie, "Sensitivity analysis of real-time locational marginal price to SCADA sensor data corruption," *IEEE Trans. Power Syst.*, vol. 29, no. 3, pp. 1110–1120, May 2014.

[32] 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.

[33] 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.

[34] 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.

[35] F. Li, “Continuous locational marginal pricing (CLMP),” IEEE Trans. Power Syst., vol. 22, no. 4, pp. 1638–1646, Nov. 2007.

[36] 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

[37] F. Li and R. Bo, “Small test systems for power system economic studies,” *Power Energy Soc. Gen. Meet.*, pp. 1–4, Jul. 2010.

[38] H. Xu, Y. Lin, X. Zhang and F. Wang, "Power System Parameter Attack for Financial Profits in Electricity Markets," *IEEE Transactions on Smart Grid*, vol. 11, no. 4, pp. 3438-3446, July 2020.

[39] 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.

[40] Y. Huang, J. Tang, Y. Cheng, H. Li, K. Campbell and Z. Han, “Real-time detection of false data injection in smart grid networks: An adaptive CUSUM method and analysis,” *IEEE Syst. J.*, vol. 10, no. 2, pp. 532–543, Jun. 2016.

[41] G. Chaojun, P. Jirutitijaroen, and M. Motani, “Detecting false data injection attacks in AC state estimation,” *IEEE Trans. Smart Grid*, vol. 6, no. 5, pp. 2476–2483, Sep. 2015.

[42] X. Wang, F. Li, J. Dong, M. Olama, Q. Zhang, Q. Shi, B. Park, T. Kuruganti, "Tri-Level Scheduling Model Considering Residential Demand Flexibility of Aggregated HVACs

and EVs Under Distribution LMP," in *IEEE Transactions on Smart Grid*, vol. 12, no. 5, pp. 3990-4002, Sept. 2021.

[43] X. Wang, F. Li, Q. Zhang, Q. Shi and J. Wang, "Profit-Oriented BESS Siting and Sizing in Deregulated Distribution Systems," in *IEEE Transactions on Smart Grid*, doi: 10.1109/TSG.2022.3150768.

[44] S. Deng, S. Oren, and A.P. Meliopoulos, "The inherent inefficiency of simultaneously feasible financial transmission rights auctions," *Energy Economics*, vol. 32, no. 4, pp. 779-785, July, 2010.

[45] W. W. Hogan, "Financial transmission rights, revenue adequacy and multi-settlement electricity markets," vol. 31813, 2013. [Online]. Available: https://sites.hks.harvard.edu/fs/whogan/Hogan_FTR_Rev_Adequacy_031813.pdf.

[46] V. Sarkar and S. A. Khaparde, "A Comprehensive Assessment of the Evolution of Financial Transmission Rights," IEEE Transactions on Power Systems, vol. 23, no. 4, pp. 1783-1795, Nov. 2008.

[47] S. S. Oren and K. W. Hedman, "Revenue adequacy, shortfall allocation and transmission performance incentives in FTR/FGR markets," 2010 IREP Symposium Bulk Power System Dynamics and Control - VIII (IREP), Rio de Janeiro, Brazil, 2010, pp. 1-6.

[48] Q. Zhang and F. Li, "Financial Resilience and Financial Reliability for Systemic Risk Assessment of Electricity Markets With High-Penetration Renewables," in *IEEE Transactions on Power Systems*, vol. 37, no. 3, pp. 2312-2321, May 2022.

[49] Q. Zhang, F. Li, W. Feng, X. Wang, L. Bai and R. Bo, "Building Marginal Pattern Library With Unbiased Training Dataset for Enhancing Model-Free Load-ED Mapping," in *IEEE Open Access Journal of Power and Energy*, vol. 9, pp. 88-98, 2022.

[50] Q. Zhang, F. Li, H. Wang, Y. Xue, “Zigzag search for multi-objective optimization considering generation cost and emission, *Applied Energy*, vol. 255, 2019.

[51] F. Li, Y. Wei and S. Adhikari, "Improving an Unjustified Common Practice in Ex Post LMP Calculation," *IEEE Transactions on Power Systems*, vol. 25, no. 2, pp. 1195-1197, May 2010.

[52] R. D. Zimmerman, C. E. Murillo-Sanchez, and R. J. Thomas, “MATPOWER: Steady-State Operations, Planning and Analysis Tools for Power Systems Research and Education,” *IEEE Transactions on Power Systems*, vol. 26, no. 1, pp. 12–19, Feb. 2011.

[53] U.S. White House National Climate Task Force, Jan. 2021. [Online]. Available: https://www.whitehouse.gov/climate/

[54] E.U. European Climate Law, July, 2021. [Online]. Available: https://ec.europa.eu/clima/eu-action/european-green-deal/european-climate-law_en

[55] W. Huang, N. Zhang, Y. Cheng, J. Yang, Y. Wang and C. Kang, "Multienergy Networks Analytics: Standardized Modeling, Optimization, and Low Carbon Analysis," in *Proceedings of the IEEE*, vol. 108, no. 9, pp. 1411-1436, Sept. 2020.

[56] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong, “The 2015 Ukraine blackout: Implications for false data injection attacks,” *IEEE Trans. Power Syst.*, vol. 32, no. 4, pp. 3317–3318, Jul. 2017.

[57] J. Voas, N. Kshetri and J. F. DeFranco, "Scarcity and Global Insecurity: The Semiconductor Shortage," in *IT Professional*, vol. 23, no. 5, pp. 78-82, 1 Sept.-Oct. 2021.

[58] P. Mancarella, “MES (multi-energy systems): An overview of concepts and evaluation models,” Energy, vol. 65, pp. 1–17, 2014.

[59] M. J. O'Malley *et al*., "Multicarrier Energy Systems: Shaping Our Energy Future," in *Proceedings of the IEEE*, vol. 108, no. 9, pp. 1437-1456, Sept. 2020.

[60] E. A. Martínez Ceseña, E. Loukarakis, N. Good and P. Mancarella, "Integrated Electricity– Heat–Gas Systems: Techno–Economic Modeling, Optimization, and Application to Multienergy Districts," in *Proceedings of the IEEE*, vol. 108, no. 9, pp. 1392-1410, Sept. 2020.

[61] R. Bayani and S. D. Manshadi, "Natural Gas Short-Term Operation Problem with Dynamics: A Rank Minimization Approach," in *IEEE Transactions on Smart Grid*, Early Access, 2022.

[62] J. Fang, Q. Zeng, X. Ai, Z. Chen and J. Wen, "Dynamic Optimal Energy Flow in the Integrated Natural Gas and Electrical Power Systems," in *IEEE Transactions on Sustainable Energy*, vol. 9, no. 1, pp. 188-198, Jan. 2018.

[63] W. Liu, P. Li, W. Yang and C. Y. Chung, "Optimal Energy Flow for Integrated Energy Systems Considering Gas Transients," in *IEEE Transactions on Power Systems*, vol. 34, no. 6, pp. 5076-5079, Nov. 2019.

[64] S. Yao *et al*., "Dynamic Optimal Energy Flow in the Heat and Electricity Integrated Energy System," in *IEEE Transactions on Sustainable Energy*, vol. 12, no. 1, pp. 179-190, Jan. 2021.

[65] X. Zhang, G. Strbac, N. Shah, F. Teng and D. Pudjianto, "Whole-System Assessment of the Benefits of Integrated Electricity and Heat System," in *IEEE Transactions on Smart Grid*, vol. 10, no. 1, pp. 1132-1145, Jan. 2019.

[66] A. Shabanpour-Haghighi and A. R. Seifi, "Energy Flow Optimization in Multicarrier Systems," in *IEEE Transactions on Industrial Informatics*, vol. 11, no. 5, pp. 1067-1077, Oct. 2015.

[67] D. Xu, Q. Wu, B. Zhou, C. Li, L. Bai and S. Huang, "Distributed Multi-Energy Operation of Coupled Electricity, Heating, and Natural Gas Networks," in *IEEE Transactions on Sustainable Energy*, vol. 11, no. 4, pp. 2457-2469, Oct. 2020.

[68] S. Chen, A. J. Conejo, R. Sioshansi and Z. Wei, "Equilibria in Electricity and Natural Gas Markets With Strategic Offers and Bids," in *IEEE Transactions on Power Systems*, vol. 35, no. 3, pp. 1956-1966, May 2020.

[69] C. Wang, W. Wei, J. Wang, F. Liu and S. Mei, "Strategic Offering and Equilibrium in Coupled Gas and Electricity Markets," in *IEEE Transactions on Power Systems*, vol. 33, no. 1, pp. 290-306, Jan. 2018.

[70] Y. Cao, W. Wei, L. Wu, S. Mei, M. Shahidehpour and Z. Li, "Decentralized Operation of Interdependent Power Distribution Network and District Heating Network: A Market-Driven Approach," in *IEEE Transactions on Smart Grid*, vol. 10, no. 5, pp. 5374-5385, Sept. 2019.

[71] Z. Wang and R. S. Blum, "Elimination of Undetectable Attacks on Natural Gas Networks," in *IEEE Signal Processing Letters*, vol. 28, pp. 1002-1005, 2021.

[72] G. Li, Y. Shen, P. Zhao, X. Lu, J. Liu, Y. Liu, et al., "Detecting cyberattacks in industrial control systems using online learning algorithms", *Neurocomputing*, vol. 364, pp. 338-348, 2019.

[73] P. Zhao, C. Gu and D. Huo, "Coordinated Risk Mitigation Strategy For Integrated Energy Systems Under Cyber-Attacks," in *IEEE Transactions on Power Systems*, vol. 35, no. 5, pp. 4014-4025, Sept. 2020.

[74] B. Huang, Y. Li, F. Zhan, Q. Sun and H. Zhang, "A Distributed Robust Economic Dispatch Strategy for Integrated Energy System Considering Cyber-Attacks," in *IEEE Transactions on Industrial Informatics*, vol. 18, no. 2, pp. 880-890, Feb. 2022.

[75] S. Ding, W. Gu, S. Lu, R. Yu, L. Sheng, "Cyber-attack against heating system in integrated energy systems: Model and propagation mechanism," in *Applied Energy*, vol. 311, April, 2022.

[76] B. Zhao, *et al*., "A coordinated scheme of electricity-gas systems and impacts of a gas system FDI attacks on electricity system," in *Int. J. Electr. Power Energy Syst.*, vol. 131, Oct. 2021.

[77] A. M. Sawas, H. Khani and H. E. Z. Farag, "On the Resiliency of Power and Gas Integration Resources Against Cyber Attacks," in *IEEE Transactions on Industrial Informatics*, vol. 17, no. 5, pp. 3099-3110, May 2021.

[78] C. Wang *et al*., "Robust Defense Strategy for Gas–Electric Systems Against Malicious Attacks," in *IEEE Transactions on Power Systems*, vol. 32, no. 4, pp. 2953-2965, July 2017.

[79] H. Shuai, X. M. Ai, J. K. Fang, T. Ding, Z. Chen, and J. Y.Wen, “Real-Time Optimization of the Integrated Gas and Power Systems Using Hybrid Approximate Dynamic Programming," *International Journal of Electrical Power & Energy Systems*, vol. 118, pp. 105776, 2020.

[80] Q. Zhang and F. Li, "Financial Resilience and Financial Reliability for Systemic Risk Assessment of Electricity Markets With High-Penetration Renewables," in *IEEE Transactions on Power Systems*, vol. 37, no. 3, pp. 2312-2321, May 2022.

[81] Q. Zhang, W. Feng, M. M. M. Kamel, B. Wang and F. Li, "Extended LMP under High-Penetration Wind Power," *2018 IEEE PES Transmission & Distribution Conference and Exhibition - Latin America (T&D-LA)*, 2018.

[82] J. Zhao, F. Li, X. Chen, and Q. Wu, "Deep Learning based Model-free Robust Load Restoration to Enhance Bulk System Resilience with Wind Power Penetration" *IEEE Transactions on Power Systems*, vol. 37, no. 3, pp. 1969-1978, May 2022.

[83] J. Zhao, F. Li, S. Mukherjee and C. Sticht, "Deep Reinforcement Learning-Based Model-Free On-Line Dynamic Multi-Microgrid Formation to Enhance Resilience," in *IEEE Trans. on Smart Grid*, vol. 13, no. 4, pp. 2557-2567, July 2022.

[84] L. Bai et al., "Interval optimization based operating strategy for gas-electricity integrated energy systems considering demand response and wind uncertainty," *Appl. Energy*, vol. 167, pp. 270–279, Apr. 2016.

[85] S. Pineda and J. M. Morales, "Solving Linear Bilevel Problems Using Big-Ms: Not All That Glitters Is Gold," *IEEE Transactions on Power Systems*, vol. 34, no. 3, pp. 2469-2471, May 2019.

[86] A. J. Conejo and C. Ruiz, "Complementarity, Not Optimization, is the Language of Markets," in *IEEE Open Access Journal of Power and Energy*, vol. 7, pp. 344-353, Oct. 2020.

[87] Q. Zhang, F. Li, H. Cui, R. Bo and L. Ren, "Market-Level Defense Against FDIA and a New LMP-Disguising Attack Strategy in Real-Time Market Operations," in *IEEE Transactions on Power Systems*, vol. 36, no. 2, pp. 1419-1431, March 2021.

[88] X. Kou *et al*., "Model-Based and Data-Driven HVAC Control Strategies for Residential Demand Response," in *IEEE Open Access Journal of Power and Energy*, vol. 8, pp. 186-197, 2021.

[89] Q Shi, W Liu, B Zeng, H Hui, F Li. Enhancing distribution system resilience against extreme weather events: concept review, algorithm summary, and future vision. *Int J Electr Power Energy Syst Jun*. 2022;138:1–13.

# Full Publications List

## Journal papers

[J1] **Qiwei Zhang**, Fangxing Li, Wei Feng, Xiaofei Wang, Linquan Bai, Rui Bo, "Building Marginal Pattern Library with Unbiased Training Dataset for Enhancing Model-Free Load-ED Mapping," ***IEEE Open Access Journal of Power and Energy***, vol. 9, pp. 88-98, Feb 2022.

[J2] **Qiwei Zhang** and Fangxing Li, "Financial Resilience and Financial Reliability for Systemic Risk Assessment of Electricity Markets with High-Penetration Renewables," ***IEEE Transactions on Power Systems***, vol. 37, no. 3, pp. 2312-2321, May 2022.

[J3] **Qiwei Zhang**, Fangxing Li, "Cyber-Vulnerability Analysis for Real-time Market Operations", Journal: ***IEEE Transactions on Smart Grid***, vol. 12, no. 4, pp. 3527-3537, July 2021.

[J4] **Qiwei Zhang**, Fangxing Li, Qingxin Shi, Kevin Tomsovic, Jinyuan Sun, Lingyu Ren, "Profit-Oriented False Data Injection on Energy Market: Reviews, Analysis and Insights", Journal: ***IEEE Transactions on Industrial Informatics***, vol. 17, no. 9, pp. 5876-5886, Sept. 2021.

[J5] **Qiwei Zhang**, Fangxing Li, Hantao Cui, Rui Bo, Lingyu Ren, "Market-Level Defense against FDIA and a New LMP-Disguising Attack Strategy in Real-Time Market Operations," Journal: ***IEEE Transactions on Power Systems***, vol. 36, no. 2, pp. 1419-1431, Mar. 2021.

[J6] **Qiwei Zhang** and Fangxing Li, “From Systematic Risk to Systemic Risk: Analysis over Day-Ahead Market Operation under High Renewable Penetration by CoVaR and ΔCoVaR,” ***IEEE Transactions on Sustainable Energy***, vol. 12, no. 2, pp. 761-771, Apr. 2021.

[J7] **Qiwei Zhang**, Fangxing Li, Honggang Wang, Yaosuo Xue, "Zigzag Search for Multi-objective Optimization Considering Generation Cost and Emission," ***Applied Energy (Elsevier)***, vol. 255, article 113814, Dec. 2019.

[J8] **Qiwei Zhang**, Fangxing Li, Xiaofei Wang, “A Trilevel Cyber-Impact Analysis for ISO Revenue Adequacy Considering FDIA in Real-time Market Operations,” (*Under Second Round Revision*, Submitted to ***IEEE Transactions on Power Systems***)

[J9] **Qiwei Zhang**, Fangxing Li, Linquan Bai, Jin Zhao, Hang Shuai, “Coupling Analysis for Multienergy System by Cross-CLL and Ref-CLL” (*Under First Round Review*, Submitted to ***International Journal of Electrical Power & Energy Systems***)

[J10] **Qiwei Zhang**, Fangxing Li, Jin Zhao, Buxin She, “Optimally Coordinated False Data Injection Attack against Multienergy System and Countermeasure” (***To be submitted***)

[J11] Xiaofei Wang, Fangxing Li, Jin Dong, Mohammed Olama, **Qiwei Zhang**, Qingxin Shi, Byungkwon Park, and Teja Kuruganti, "Tri-level Scheduling Model Considering Residential Demand Flexibility of Aggregated HVACs and EVs under Distribution LMP," *IEEE Transactions on Smart Grid,* vol. 12, no. 5, pp. 3990-4002, Sept. 2021.

[J12] Yunwei Shen, Yang Li, **Qiwei Zhang**, Qingxin Shi, Fangxing Li, "State-shift priority based progressive load control of residential HVAC units for frequency regulation," ***Electric Power Systems Research (Elsevier)***, vol. 182, article 106194, May 2020.

[J13] Yunwei Shen, Yang Li, **Qiwei Zhang**, Fangxing Li, and Zhe Wang, "Consumer Psychology Based Optimal Portfolio Design for Demand Response Aggregators," ***Journal of Modern Power Systems and Clean Energy***, vol. 9, no. 2, pp. 431-439, Mar. 2021.

**Conference papers**

[C1] **Qiwei Zhang**, Yunwei Shen, Fangxing Li, "Shadow Price Formulation and Decomposition for Economic Emission Dispatch," 16th European Energy Market Conference (EEM 2019), 6 pages, Ljubljana, Slovenia, Sept. 18-20, 2019.

[C2] **Qiwei Zhang**, Wei Feng, Mariana Kamel, Beibei Wang, Fangxing Li, "Extended LMP under High-Penetration Wind Power," IEEE PES T&D Conference and Exposition - Latin America, 5 pages, Lima,Peru, Sept. 18-21, 2018.

[C3] Qingxin Shi, Wei Feng, **Qiwei Zhang**, Xiaofei Wang, and Fangxing Li, "Overvoltage Mitigation through Volt-VAR Control of Distributed PV Systems," IEEE PES T&D Conf. and Expo, 5 pages, Chicago, IL, Oct. 12-15, 2020.

[C4] Yunwei Shen, **Qiwei Zhang**, Qingxin Shi, Fangxing Li, Yang Li, Yajun Wang, Siqi Wang, "Progressive Demand Control of Thermostatically Controlled Appliances for Power System Frequency Regulation," IEEE PES General Meeting 2019, 5 pages, Atlantat, GA, Aug. 4-8, 2019.

[C5] Wei Feng, Xiao Kou, **Qiwei Zhang**, F. Li, "Impact of Neutral Current on Concentric Cable Overloading," 2018 IEEE/PES Transmission and Distribution Conference and Exposition (T&D), Denver, CO, USA, 2018, pp. 1-9.

# Appendices

# Appendix A.Reformulation for CVA Model

The reformulations and linearization of the CVA model are included in this *Appendix*.

## *A.1 Constraint (3.20) and (3.21) linearization*

The first constraint (3.20) is linearized and replaced by (A1.1) and (A1.2). Similarly, (3.21) is replaced by (A1.3) and (A1.4).

$$-V_i^j M_{i,j}^{\min} \le N_i^j \le V_i^j M_{i,j}^{\max}, \ \forall i \in NG, \ \forall j \in \{d,p,b\} \tag{A1.1}$$

$$M_i^j - (1 - V_i^j)Q_s \le N_i^j \le M_i^j + (1 - V_i^j)Q_s, \quad \forall i \in NG, \ \forall j \in \{d,p,b\} \tag{A1.2}$$

$$-V_l^j M_{l,j}^{\min} \le N_l^j \le V_l^j M_{l,j}^{\max}, \ \forall l \in L, \ \forall j \in \{L^+,L^-\} \tag{A1.3}$$

$$M_i^j - (1 - V_l^j)Q_s \le N_l^j \le M_i^j + (1 - V_l^j)Q_s, \quad \forall l \in L, \ \forall j \in \{L^+,L^-\} \tag{A1.4}$$

## *A.2 Constraints that contain nonlinear elements*

(3.17) and (3.18)

$$g_l^+(d_l^+ \mid V_l^{d+})\left(\sum_i GSF_{l-i}(P_i - (d_i - M_i^d + N_i^d)) - L_l^{\max} - M_l^{L+} + N_l^{L+}\right) = 0, \ \forall l \in L \tag{A2.1}$$

$$g_l^-(d_l^- \mid V_l^{d-})\left(\sum_i L_l^{\min} + M_l^{L-} - N_l^{L+} - GSF_{l-i}(P_i - (d_i - M_i^d + N_i^d))\right) = 0, \ \forall l \in L \tag{A2.2}$$

$$(C_i + M_i^b - N_i^b) + l + m_l^+ - m_l^- + \sum_L GSF_{l-i}((d_l^+ + V_l^{d+})g_l^+ - (d_l^- + V_l^{d-})g_l^-) = 0, \ \forall i \in NG \tag{A2.3}$$

$$-l + \sum_l GSF_{l-i}(g_l^-(d_l^- \mid V_l^{d-}) - g_l^+(d_l^+ \mid V_l^{d+})) + a^+_{i,j} - a^-_{i,j} + k^+_{i,j} - k^-_{i,j} = 0, \ \forall i \in NG \tag{A2.4}$$

$$g_l^+(d_l^+ \mid V_l^{d+}) + a^+_{i,j} - a^-_{i,j} + k^+_{i,j} - k^-_{i,j} = 0, \ \forall i \in NG \tag{A2.5}$$

$$-g_l^-(d_l^- \mid V_l^{d-}) + a^+_{i,j} - a^-_{i,j} + k^+_{i,j} - k^-_{i,j} = 0, \ \forall i \in NG \tag{A2.6}$$

### *A.3 Linearizing δ_V·M and δ_V·N*

The variable $\delta\_V$ represents the OR gate operation of the variable $\delta$ and $V$. Therefore, the relationship between $\delta\_V$, $\delta$, and $V$ is shown in (A3.1)-(A3.3).

$$d_l^j \_ V_l^{dj} \geq V_l^{dj}, \quad \forall l \in L \ \forall j \in \{+,-\} \tag{A3.1}$$

$$d_l^j \_ V_l^{dj} \geq d_l^j, \quad \forall l \in L \ \forall j \in \{+,-\} \tag{A3.2}$$

$$d_l^j \_ V_l^{dj} \leq V_l^{dj} + d_l^j, \quad \forall l \in L \ \forall j \in \{+,-\} \tag{A3.3}$$

Similar to (A1.1)-(A1.4), $\delta\_V \cdot M$ is replaced by a new continuous variable $\delta\_V\_M$, with constraints (A3.4) and (A3.4).

$$-q_i^d \times d_i \times \left(d_l^j \_ V_l^{dj}\right) \leq d_l^j \_ V_l^{dj} \_ M_i^d \leq q_i^d \times d_i \times \left(d_l^j \_ V_l^{dj}\right), \quad \forall j \in \{+,-\} \tag{A3.4}$$

$$M_i^d - (1 - d_l^j \_ V_l^{dj}) Q_s \leq d_l^j \_ V_l^{dj} \_ M_i^d \leq M_i^d + (1 - d_l^j \_ V_l^{dj}) Q_s, \quad \forall j \in \{+,-\} \tag{A3.5}$$

In element $\delta\_V \cdot N$, variable $N$ is constrained by (A1.1)-(A1.4). A new continuous variable $\delta\_V\_N$ is introduced to replace $\delta\_V \cdot N$ with (A3.6)-(A3.10).

$$d_l^j \_ V_l^{dj} \_ V_i^d \leq V_i^d, \ \forall l \in L \ \forall j \in \{+,-\} \ \forall d \in D \tag{A3.6}$$

$$d_l^j \_ V_l^{dj} \_ V_i^d \leq d_l^j \_ V_l^{dj}, \ \forall l \in L \ \forall j \in \{+,-\} \ \forall d \in D \tag{A3.7}$$

$$d_l^j \_ V_l^{dj} \_ V_i^d \geq d_l^j \_ V_l^{dj} + V_i^d - 1, \quad \forall l \in L \ \forall j \in \{+,-\} \ \forall d \in D \tag{A3.8}$$

$$-q_i^d \times d_i \times d_l^j \_ V_l^{dj} \_ V_i^d \leq d_l^j \_ V_l^{dj} \_ N_i^d \leq q_i^d \times d_i \times d_l^j \_ V_l^{dj} \_ V_i^d, \quad \forall l \in L \ \forall j \in \{+,-\} \ \forall d \in D \tag{A3.9}$$

$$M_i^d - (1 - d_l^j \_ V_l^{dj} \_ V_i^d) Q_s \leq d_l^j \_ V_l^{dj} \_ N_i^d \leq M_i^d + (1 - d_l^j \_ V_l^{dj} \_ V_i^d) Q_s, \quad \forall l \in L \ \forall j \in \{+,-\} \ \forall d \in D \tag{A3.10}$$

### *A.4 Linearizing δ_V·P*

The upper limits of $P$ contain variables and parameters. Thus, the reformulation is applied recursively. Then, the $\delta\_V \cdot P$ is represented by a new continuous variable $\delta\_V\_P$ with constraints (A4.1)- (A4.10).

$$d_l^j \_ V_l^{dj} \_ P_i \le P_i^{\max} d_l^j \_ V_l^{dj} + d_l^j \_ V_l^{dj} \_ M_i^P - d_l^j \_ V_l^{dj} \_ N_i^P, \quad \forall j \in \{+,-\} \forall i \in NG \tag{A4.1}$$

$$P_i - (1 - d_l^j \_ V_l^{dj}) Q_s \le d_l^j \_ V_l^{dj} \_ P_i \le P_i + (1 - d_l^j \_ V_l^{dj}) Q_s, \quad \forall j \in \{+,-\} \forall i \in NG \tag{A4.2}$$

$$-q_i^P P_i^{\max} d_l^j \_ V_l^{dj} \le d_l^j \_ V_l^{dj} \_ M_i^P \le q_i^P P_i^{\max} d_l^j \_ V_l^{dj}, \quad \forall j \in \{+,-\} \forall i \in NG \tag{A4.3}$$

$$M_i^P - (1 - d_l^j \_ V_l^{dj}) Q_s \le d_l^j \_ V_l^{dj} \_ M_i^P \le M_i^P + (1 - d_l^j \_ V_l^{dj}) Q_s, \quad \forall j \in \{+,-\} \forall i \in NG \tag{A4.4}$$

$$d_l^j \_ V_l^{dj} \_ V_i^P \le V_i^P, \quad \forall j \in \{+,-\} \forall i \in NG \tag{A4.5}$$

$$d_l^j \_ V_l^{dj} \_ V_i^P \le d_l^j \_ V_l^{dj}, \quad \forall j \in \{+,-\} \forall i \in NG \tag{A4.6}$$

$$d_l^j \_ V_l^{dj} \_ V_i^P \ge d_l^j \_ V_l^{dj} + V_i^P - 1, \quad \forall j \in \{+,-\} \forall i \in NG \tag{A4.7}$$

$$-q_i^P P_i^{\max} d_l^j \_ V_l^{dj} \_ V_i^P \le d_l^j \_ V_l^{dj} \_ N_i^P \le q_i^P P_i^{\max} d_l^j \_ V_l^{dj} \_ V_i^P, \quad \forall j \in \{+,-\} \forall i \in NG \tag{A4.8}$$

$$M_i^d - (1 - d_l^j \_ V_l^{dj} \_ V_i^d) Q_s \le d_l^j \_ V_l^{dj} \_ N_i^d \le M_i^d + (1 - d_l^j \_ V_l^{dj} \_ V_i^d) Q_s, \quad \forall j \in \{+,-\} \forall i \in NG \tag{A4.9}$$

$$\sum_{i=1}^{N_b} GSF_{l-i} (d_l^+ \_ V_l^{d+} \_ P_i - d_l^+ \_ V_l^{d+} d_i + d_l^+ \_ V_l^{d+} \_ M_i^d - d_l^+ \_ V_l^{d+} \_ N_i^d)) \le L_l^{\max} + M_l^{L+} - N_l^{L+}, \quad \forall j \in \{+,-\} \forall i \in NG \tag{A4.10}$$

### *A.5 Linearizing complementary slackness constraints*

The technique (Fortuny-Amat reformulation) of linearizing complementary slackness has been well established in [85] and [86]. All complementary slackness constraints in this model are dealt with via this technique. For example, (A2.5) is equivalent to (A5.1)-(A5.2). Similarly, other complementary slackness constraints can be reformed. However, after this reformulation, they are still not linear due to variable $\delta \_ V$.

$$d_l^+ \_ V_l^{d+} \times g_l^+ \le u_l^{L+} \times Q_g, \quad \forall l \in L \tag{A5.1}$$

$$d_l^+ \_ V_l^{d+} \times (L_l^{\max} + M_l^{L+} - \sum_i GSF_{l-i} (P_i - (d_i - M_i^d))) \le (1 - u_i^{L+}) \times Q_g, \quad \forall l \in L \tag{A5.2}$$

Therefore, we add a new constraint (A5.3) to remove $\delta\_V$ from (A5.1) and (A5.2). Similarly, $\delta\_V$ in other constraints can be removed.

$$d_l^+ \_ V_l^{d+} \text{ ³ } u_l^{L+}, \text{ "l Î L} \qquad \text{(A5.3)}$$

# Appendix B. DNN Accuracy

The training and accuracy of applied DNNs are shown in this Appendix. Two thousand mitigation samples are generated uniformly between zero and the upper limit in (32) and (33). The feasibility region for both defensing units is sliced into 10 pieces, which gives 100 combinations. For each combination, 20 samples are generated, which results in 2000 mitigation samples. Models (37) and (38) are solved for each mitigation sample to obtain the corresponding value of mitigation effectiveness and no-attack loss, which forms the training dataset. The training accuracy and MES loss of the two DNNs are shown in Figure B1. The accuracy rates of CS-DNN and LS-DNN in the test dataset (i.e., 500 test samples) are 99.4% and 98.6%, respectively.

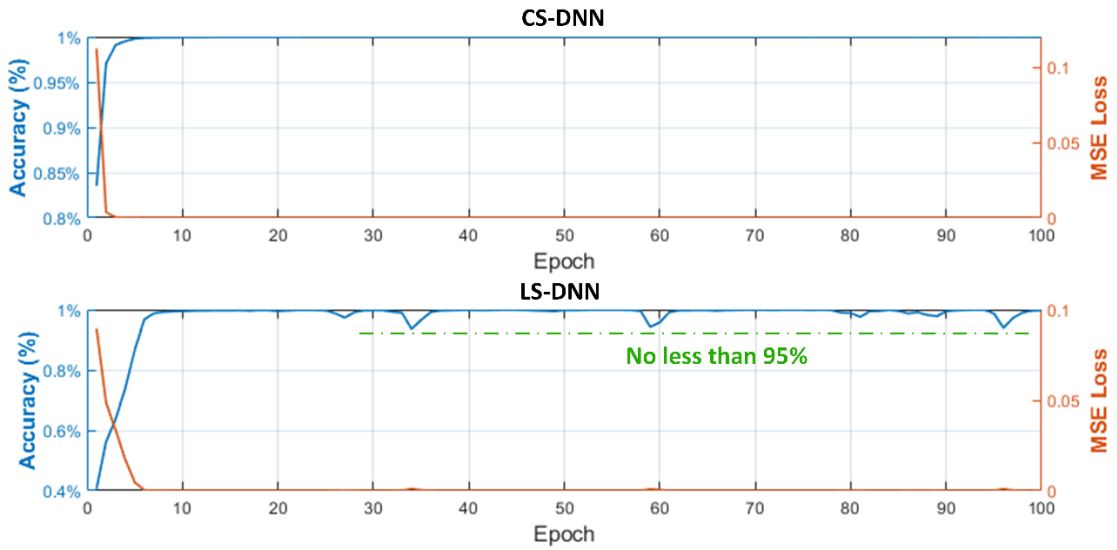


Figure B1. Accuracies of the CS-DNN and LS-DNN

# Vita

Qiwei Zhang joined Professor Fangxing Li's group at the University of Tennessee, Knoxville in August 2016 for Master degree, and he continues to pursue a Ph. D. degree at the same research group starting at August 2018. He received B.S degree in Automation from North China Electric Power University at August 2016. His research interests include electricity market operation and cybersecurity.