This article has been accepted for inclusion in a future issue of this journal. Content is final as presented, with the exception of pagination.

Economic Impact Assessment of Topology Data Attacks With Virtual Bids

Dae-Hyun Choi, *Member, IEEE*, and Le Xie, *Member, IEEE*

***Abstract*—This paper presents a new mathematical framework for the economic impact analysis of topology data attacks in electricity markets with virtual bidding activities. The network topology information is very important for system operators to manage the grid in a secure manner. However, this network topology can be manipulated by an adversary through the change of the circuit breaker's on/off status. This, combined with virtual bids submitted by the attackers, could lead to financial misconduct and potential profit for the attacker in the power market. This paper aims at developing an analytical framework to evaluate the economic profit of an attacker who conducts topology data attack and submits virtual bids accordingly. This framework can be used for system operators as a cybersecurity tool to quickly find the most profitable pair of virtual bidding buses and the most influential transmission line on the change in profit once topology data attack is initiated. Furthermore, the sensitivity of the adversary's profit with respect to the change in generator's marginal cost and susceptance for any targeted line is assessed in the proposed framework. IEEE 14-bus system is used to validate and test the proposed framework in various system operation conditions and attack scenarios.**

***Index Terms*—Power market, economic dispatch, virtual bidding, power system network topology, topology data attack.**

I. Introduction

CYBER data attacks on power grids are becoming more feasible as smart grid operations highly rely on large volumes of heterogeneous sensor data collected by substation intelligent electronic device (IED), phasor measurement unit (PMU) and smart meter. While a variety of cyber data attack methods have been proposed and tested in a real environment, it is desirable for system operators to analyze the impact of such attacks on the economical operations of smart grid. This paper aims to develop a novel mathematical framework to investigate how much an adversary profits from data attacks through the manipulation of power system network topology on real-time power market operations.

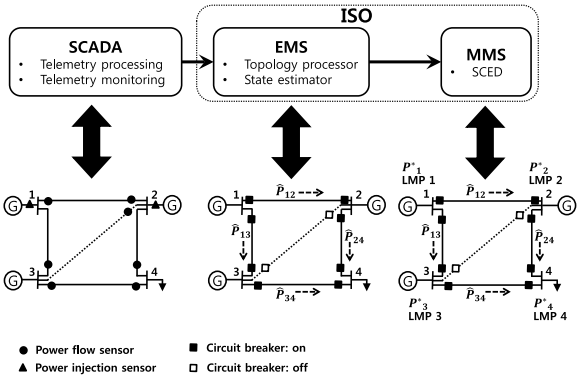


Fig. 1. Illustration of the relationship among SCADA, EMS and MMS.

For real-time grid operations, energy management system (EMS) is a key component in the control center of Independent System Operators (ISOs). EMS is typically integrated with a supervisory control and data acquisition (SCADA) system that conducts data collection and control at the supervisory level. SCADA system monitors real-time grid conditions using two types of sensors: (1) analog sensor for measuring voltage, power flow; and (2) discrete sensor for identifying circuit breaker's on/off status. Therefore, the accuracy of these sensor data is of vital importance for the well functioning of real-time operation.

EMS assists market management system (MMS) to perform reliable economic grid operations [1]. As shown in Fig. 1, SCADA telemetry data is fed into state estimator (SE) in EMS, which subsequently provides a base power flow and network topology estimate to a subsystem of MMS, security constrained economic dispatch (SCED). Finally, SCED calculates a real-time economic dispatch (i.e., an optimal generation output P^* and locational marginal price (LMP) at bus) while considering all system operation constraints updated by SE regularly.

Given the tight coupling between SE and SCED, malicious discrete data change could lead to the malfunction of topology processor and SE, thus generating a wrong network topology. As a result, this results in the miscalculation of real-time LMP. In this paper, the main concern is on the comprehensive assessment of the financial risk caused by cyber threats through covert topology change.

Manuscript received July 13, 2015; revised November 16, 2015; accepted February 15, 2016. This work was supported in part by the Chung-Ang University Research Grants in 2015, and in part by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIP) under Grant 2015R1C1A1A01051890. Paper no. TSG-00812-2015.

D.-H. Choi is with the School of Electrical and Electronics Engineering, Chung-Ang University, Seoul 156-756, South Korea (e-mail: dhchoi@cau.ac.kr).

L. Xie is with the Department of Electrical and Computer Engineering, Texas A&M University, College Station, TX 77845 USA (e-mail: le.xie@tamu.edu).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TSG.2016.2535246

1949-3053 © 2016 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission.
See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

This article has been accepted for inclusion in a future issue of this journal. Content is final as presented, with the exception of pagination.

TABLE I
CYBER DATA ATTACKS ON MARKET OPERATIONS

Type	Attack Target	ED/OPF	Market	Congestion	Bidding Method	Undetectable/Profitable Attack Strategy
(A1)	Power flow estimate	ST ED	DA/RT	DA/RT	VB	Yes/Yes [6]
(A2)	Power flow estimate	ST ED	RT	RT	GB	Yes/Yes [7]
(A3)	Power injection estimate	LA ED	RT	No	GB	Yes/Yes [8]
(A4)	Network topology estimate	ST ED	RT	RT	GB	Yes/No [9]
(A5)	Network topology estimate	OPF	RT	RT	GB	Yes/No [10]

* DA: Day-ahead, RT: Real-time, VB: Virtual bidding, GB: Generation bidding, ED: Economic dispatch, ST: Static, LA: Look-ahead, OPF: Optimal power flow

Recently, considerable efforts have been focused on the analysis of the impact of cyber data attacks on power grid operations. In particular, most of the work on the subject of cyber data attack is related to false data injection (FDI) attack problem. In this problem, an adversary manipulates the solution of power system state estimator through the injection of false data into sensors while escaping bad data processing algorithm, consequently resulting in an abnormal physical and economical grid operations. A FDI attack problem in a linearized DC state estimation has been first addressed in [2]. The vulnerability of DC state estimator to FDI attacks has been investigated more rigorously, and the countermeasures to defend such attacks based on the placement of phasor measurement units (PMUs) has been proposed [3]–[5]. Novel defending mechanisms using graphical methods against FDI attacks have been developed. The attack problems have been formulated in a variant Steiner tree problem in a graph [11] and using covert topological information in a mixed integer linear programming (MILP) framework in the same problem [12]. In [13] and [14], the impact of FDI attacks on a nonlinear AC state estimation has been investigated, addressing much more difficulty of AC state estimation-based attack than the attacks against DC state estimation.

On the other hand, the strong coupling between SE and SCED opens new vulnerable points for the FDI attacker to manipulate the wholesale LMP for making a profit. Table I summarizes representative literature for five types of FDI attacks (A1)∼(A5) that lead to the misconduct of real-time market operations. According to the type of the targeted estimate, the above attacks are classified into two groups manipulating: (i) power flow and/or injection estimate for (A1)∼(A3); and (ii) topology estimate for (A4)∼(A5). In the first group, (A1) attack makes a profit in virtual bidding market whereas (A2) and (A3) attacks in real-time market. In addition, (A3) attack is different from (A1) and (A2) attacks in that the former attacks on look-ahead dispatch by manipulating the ramping constraint of the generator embedded in look-ahead dispatch, whereas the latter on static dispatch without the generator's ramping constraint. In the second group, (A4) and (A5) attacks manipulate network topology estimate and distort the results for real-time LMP and optimal generation cost in SCED and optimal power flow (OPF), respectively. More recently, a profitable virtual bidding-based attack through the manipulation of transmission line rating data has been proposed [15].

While much work, from an attacker's perspective, has been focused on the development of covert attack methods, a framework for the study of the impact of such attacks on market operations, *from a system operator's perspective*, has not been developed yet. Our recent work started to investigate the impact of power flow/injection estimate perturbation on LMP sensitivity [16]. The change of network topology estimate may result in much more severe impact on real-time LMP result than that of power flow/injection estimate. The adversary could then leverage financial instruments such as virtual bidding to take advantage of such topology attack in electricity market transactions.

Virtual bidding is a financial instrument with which market participants buy or sell virtual energy in day-ahead market, and then sell or buy the same amount of virtual energy in real-time market. No physical energy is delivered or consumed with virtual bids. Virtual bidding is beneficial in that it provides price convergence between day-ahead and real-time markets, mitigate market power, and hedge physical positions in day-ahead market to manage exposure to real-time prices [17], [18].

Recently, through the statistical analysis of generator/transmission outages and weather patterns, some traders with virtual bids have created artificial congestion in day-ahead market to increase the value of Financial Transmission Right (FTR) positions. The Federal Energy Regulatory Commission (FERC) has treated this trade activity as the violation of the Commission's Anti-Manipulation Rule and has imposed heavy penalties on them [19]. This type of market manipulation through virtual bidding would be even more aggravated if a topology attack is conducted.

The main contributions of this paper are suggested as follows:

- Given the situation where the adversary with virtual bids makes a profit by manipulating network topology, we formulate a mathematical framework to quantify the adversary's profit from topology data attack. The expression for the attack profit is a closed-form solution with attack-free and attack-confined congestion costs. Each congestion cost is written as a function of marginal costs (i.e., energy costs of part-loaded marginal unit) and distribution factors. This framework enables system operators to quickly assess the profit of the proposed attack without exhaustively running economic dispatch.
- We present numerical results to demonstrate the performance of our developed framework in four different cases with varying marginal units and congestion pattern. With the proposed attack performance metric, we find the transmission line that maximizes the profit once it is

This article has been accepted for inclusion in a future issue of this journal. Content is final as presented, with the exception of pagination.

deleted from the network and identify the most profitable pair of virtual buses for any line exclusion.
- We investigate the impact of varying susceptance for the targeted line and marginal cost on the attack profit. The results from numerical examples may provide guidelines to maintain robust grid conditions against cyber data attacks in light of a secure market operation.

The rest of the paper is organized as follows. Section II reviews real-time power market pricing models along with the introduction of LMP formulation. Section III provides a problem statement. The proposed framework to quantify the financial performance of virtual bidding-based topology data attack is developed in Section IV. Section V presents the simulation results for the proposed framework in various system operation conditions and attack scenarios. Finally, concluding remarks are made in Section VI.

II. Preliminaries

The main notations used throughout this paper are summarized in Table II.

TABLE II
NOMENCLATURE

i	Index for buses i
l	Index for transmission line l
C_i	Energy cost for generator i
P_{g_i}	Scheduled power output for generator i
L_{d_i}	Fixed demand at bus i
$P_{g_i}^{\min}$, $P_{g_i}^{\max}$	Min/max generation limits for generator i
$F_l^{\min}$, $F_l^{\max}$	Min/max flow limits at line l
$S_{l,i}$	Distribution factor of transmission line l to bus i
λ_i	Locational marginal price at bus i
λ_s	Shadow price of the system energy balance equation
τ_i	Shadow price of the capacity constraint for generator i for generators
μ_l	Shadow price of the transmission line constraint for transmission line l
N_b	Total number of buses
N_l	Total number of transmission lines
$\mathcal{CL}_+, \mathcal{CL}_-$	Sets of positively and negatively congested lines
$\widetilde{\mathcal{CL}}_+^k, \widetilde{\mathcal{CL}}_-^k$	Sets of positively and negatively congested lines when the line k is excluded
$\mathcal{G}_{\text{MU}}$	Set of marginal units
$\widetilde{\mathcal{G}}_{\text{MU}}^k$	Set of marginal units when the line k is excluded
$\mathbf{1}_k$	$k \times 1$ column vectors with all ones

A. Real-Time Pricing Model

For real-time power market operations, there are two types of real-time pricing models: (1) ex-ante model where LMPs are computed before the actual deployment of dispatch orders; and (2) ex-post model where LMPs are computed after the fact using real-time estimates for settlement purposes.

1) The Ex-Ante Model [20]:

$$\min_{P_{g_i}} \quad \sum_{i=1}^{N_b} C_i P_{g_i} \tag{1}$$

$$\text{s.t.} \quad \lambda_s : \sum_{i=1}^{N_b} P_{g_i} = \sum_{i=1}^{N_b} L_{d_i} \tag{2}$$

$$\boldsymbol{\tau} : \widehat{P}_{g_i}^{\min} \le P_{g_i} \le \widehat{P}_{g_i}^{\max} \quad \forall i = 1, \ldots, N_b \tag{3}$$

$$\boldsymbol{\mu} : F_l^{\min} \le \sum_{i=1}^{N_b} \widehat{S}_{li}(\mathbf{z})(P_{g_i} - L_{d_i}) \le F_l^{\max} \quad \forall l = 1, \ldots, N_l \tag{4}$$

where

$$\widehat{P}_{g_i}^{\max} = \min\Big\{P_{g_i}^{\max}, \widehat{P}_{g_i}(\mathbf{z}) + R_i \Delta T\Big\}$$
$$\widehat{P}_{g_i}^{\min} = \max\Big\{P_{g_i}^{\min}, \widehat{P}_{g_i}(\mathbf{z}) - R_i \Delta T\Big\}.$$

2) The Ex-Post Model [21]:

$$\min_{P_{g_i}} \quad \sum_{i=1}^{N_b} C_i P_{g_i} \tag{5}$$

$$\text{s.t.} \quad \lambda_s : \sum_{i=1}^{N_b} P_{g_i} = \sum_{i=1}^{N_b} \widehat{P}_{g_i}(\mathbf{z}) \tag{6}$$

$$\boldsymbol{\tau} : \widehat{P}_{g_i}^{\min} \le P_{g_i} \le \widehat{P}_{g_i}^{\max} \quad \forall i = 1, \ldots, N_b \tag{7}$$

$$\boldsymbol{\mu}_{\max} : \sum_{i=1}^{N_b} \widehat{S}_{li}(\mathbf{z})(P_{g_i} - L_{d_i}) \le \widehat{F}_l(\mathbf{z}) \quad \forall l \in \mathcal{CL}_+ \tag{8}$$

$$\boldsymbol{\mu}_{\min} : \sum_{i=1}^{N_b} \widehat{S}_{li}(\mathbf{z})(P_{g_i} - L_{d_i}) \ge \widehat{F}_l(\mathbf{z}) \quad \forall l \in \mathcal{CL}_- \tag{9}$$

where

$$\hat{P}_{g_i}^{\max} = \widehat{P}_{g_i}(\mathbf{z}) + \Delta P_{g_i}^{\max}, \ \widehat{P}_{g_i}^{\min} = \widehat{P}_{g_i}(\mathbf{z}) + \Delta P_{g_i}^{\min}.$$

In the above ex-ante and ex-post models, a hat symbol represents estimate of a true parameter value as a function of sensor data $\mathbf{z}$. The objective functions are to minimize the total generation costs in (1) and (5). (2) and (6) are the system-wide energy balance equations. (3) and (7) are the physical capacity constraints of each generator embedded with its ramping limits ($R_i \Delta T$) and incremental generation limits ($\Delta P_{g_i}^{\max}$, $\Delta P_{g_i}^{\min}$), respectively. (4), (8) and (9) are the transmission line constraints. The lagrangian multipliers associated with the operation constraints are used to compute LMP at any bus in the entire power system.

B. Distribution Factor Matrix and LMP Formulation

Let us define the matrix $\mathbf{M}_r = \mathbf{A}_r \mathbf{B} \mathbf{A}_r^T$ as the $(N_b - 1) \times (N_b - 1)$ reduced node-to-node susceptance matrix that explains the relationship between real power injections at any bus except the slack bus and the phase angles. Here $\mathbf{B} = diag(s_1, s_2, \ldots, s_{N_l})$ is the $N_l \times N_l$ diagonal branch susceptance matrix and $\mathbf{A}_r$ is the $(N_b - 1) \times N_l$ reduced node-to-branch incidence matrix without a slack bus. Then, the $N_l \times (N_b - 1)$ distribution factor matrix can be defined as

$$\mathbf{S}_d = \mathbf{B} \mathbf{A}_r^T \mathbf{M}_r^{-1}. \tag{10}$$

In this paper, we use the $N_l \times N_b$ extended distribution factor matrix $\mathbf{S} = [\mathbf{0}_{N_l} \ \mathbf{S}_d]$ with zero column vector corresponding to the location of a slack bus 1.

Using the extended distribution factor matrix, the $N_b \times 1$ real-time LMP vector $\boldsymbol{\lambda}$ is calculated as follows [22]:

$$\boldsymbol{\lambda}(\mathbf{z}) = \lambda_s(\mathbf{z}) \mathbf{1}_{N_b} - \widehat{\mathbf{S}}^T(\mathbf{z}) \big[\boldsymbol{\mu}_{\max}(\mathbf{z}) - \boldsymbol{\mu}_{\min}(\mathbf{z})\big]. \tag{11}$$

This article has been accepted for inclusion in a future issue of this journal. Content is final as presented, with the exception of pagination.

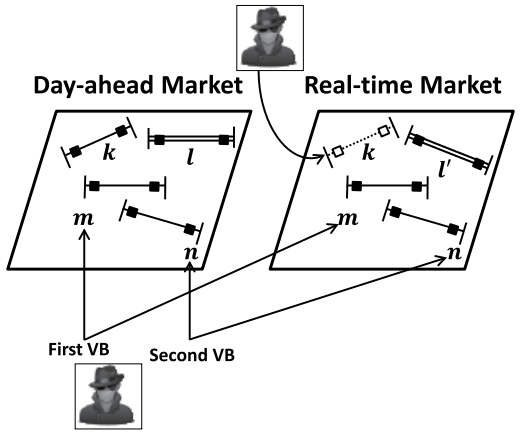


Fig. 2. Illustration of topology data attack exploiting virtual bidding transactions.

In equation (11), the first term and the second term imply the energy component (i.e., LMP at slack bus) and the congestion component (i.e., the congestion cost), respectively. It should be noted that the corrupted $\mathbf{z}$ affects congestion component for the distribution factor matrix with topology estimate $\widehat{\mathbf{S}}$ and the shadow price vector, $\boldsymbol{\mu}_{\max}$ and $\boldsymbol{\mu}_{\min}$, which in turn yields the miscalculated LMP.

III. Problem Statement

We consider the situation where an adversary with virtual bidding can exclude the transmission line without being detected by system operators. This adversary could be a generation company, a load serving entity or a third party because the bidders in virtual bidding (VB) market do not necessarily own generator or serve load.

In Fig. 2, we suppose that the line l is congested in day-ahead (DA) market. The adversary is assumed to successfully manipulates network topology in real-time (RT) market, consequently leading to the undetectable line k exclusion along with the varying congested line l'. Let us denote two pairs of LMPs at virtual buses m and n: the attack-free day-ahead LMPs $(\lambda^{\mathrm{DA}}_{l,m}, \lambda^{\mathrm{DA}}_{l,n})$ and attack-confined real-time LMPs $(\widetilde{\lambda}^{k}_{l',m}, \widetilde{\lambda}^{k}_{l',n})$. To make a profit, the adversary conducts the following two pairs of virtual bidding transactions with the virtual power P_v at two arbitrarily chosen buses:

- First virtual bidding (INC):
  1) Sell P_v at bus m with $\lambda^{\mathrm{DA}}_{l,m}$ in DA market
  2) Buy P_v at bus m with $\widetilde{\lambda}^{k}_{l',m}$ in RT market
- Second virtual bidding (DEC):
  1) Buy P_v at bus n with $\lambda^{\mathrm{DA}}_{l,n}$ in DA market
  2) Sell P_v at bus n with $\widetilde{\lambda}^{k}_{l',n}$ in RT market

First virtual bidding and second virtual bidding correspond to a virtual supply offer and a virtual demand bid, known as an increment offer (INC) and a decrement bid (DEC), respectively. In short, the virtual bidding transaction is summarized in Table III.

Then, the attack profit $\mathcal{PF}$ is written as the sum of two pairs of virtual bidding transactions and finally regrouped with LMP terms associated with each market:

TABLE III
A Paired Virtual Bidding Transactions

	Day-ahead Market		Real-time Market	
Virtual Bidding Bus	Bus m	Bus n	Bus m	Bus n
Sell (P_v MW)	$\lambda^{\mathrm{DA}}_{l,m}$	$\times$	$\times$	$\widetilde{\lambda}^{k}_{l',n}$
Buy (P_v MW)	$\times$	$\lambda^{\mathrm{DA}}_{l,n}$	$\widetilde{\lambda}^{k}_{l',m}$	$\times$

$$\begin{aligned}\mathcal{PF} &= \underbrace{P_v\left(\lambda^{\mathrm{DA}}_{l,m} - \widetilde{\lambda}^{k}_{l',m}\right)}_{\text{First VB}} + \underbrace{P_v\left(\widetilde{\lambda}^{k}_{l',n} - \lambda^{\mathrm{DA}}_{l,n}\right)}_{\text{Second VB}} \\ &= P_v\left[\underbrace{\left(\lambda^{\mathrm{DA}}_{l,m} - \lambda^{\mathrm{DA}}_{l,n}\right)}_{\text{DA Market}} - \underbrace{\left(\widetilde{\lambda}^{k}_{l',m} - \widetilde{\lambda}^{k}_{l',n}\right)}_{\text{RT Market}}\right]. \end{aligned} \tag{12}$$

It should be noted that the bracket expression in equation (12) is defined and rewritten using equation (11) as

$$\begin{aligned}\Delta\Lambda^{k}_{l}(m,n) &= \left(\lambda^{\mathrm{DA}}_{l,m} - \lambda^{\mathrm{DA}}_{l,n}\right) - \left(\widetilde{\lambda}^{k}_{l',m} - \widetilde{\lambda}^{k}_{l',n}\right) \\ &= \mu_l\left(S^{\mathrm{DA}}_{l,n} - S^{\mathrm{DA}}_{l,m}\right) - \mu_{l'}\left(\widetilde{S}^{k}_{l',n} - \widetilde{S}^{k}_{l',m}\right). \end{aligned} \tag{13}$$

Obviously, a positive $\Delta\Lambda^{k}_{l}(m,n)$ assures the profitability for the adversary ($\mathcal{PF} > 0$) since the virtual power P_v is always positive. As such, $\Delta\Lambda^{k}_{l}(m,n)$ is chosen as a metric to quantify an increasing/decreasing amount of the profit as well as check the profitability with its sign through the manipulation of network topology in virtual bidding market. In this paper, this metric is defined as a virtual bidding profit signal (VBPS), and our primary goal is to develop mathematical expressions for VBPS that evaluate the profit obtained from virtual bidding based-topology data attack.

Remark 1: Equation (13) includes no energy price λ_s (i.e., energy neutral) because energy prices at a pair of virtual bidding buses in each power market are cancelled out with each other. Due to this fact, closed-form VBPS expressions are derived easily. These expressions with the closed-form shadow price formula [23] are provided in the following section.

IV. The Proposed Framework for the Evaluation of Virtual Bidding Profit Signal (VBPS)

This section presents an analytical framework to test and evaluate the adversary's VBPS introduced in Section III. The main task for the development of the proposed framework is to derive a closed-form equation for VBPS based on congestion costs between virtual bidding buses m and n.

To this end, we first introduce our previous result (see, e.g., Proposition 1 in [23]), a closed-form formula of shadow price μ_l for a single congested transmission line l:

$$\mu_l = \frac{\Delta C(j,i)}{\Delta S_l(i,j)} \tag{14}$$

where $\Delta C(j,i) = C_j - C_i$ and $\Delta S_l(i,j) = S_{l,i} - S_{l,j}$ for $i,j \in \mathcal{G}_{\mathrm{MU}}$ and $l \in \mathcal{CL}$ ($\mathcal{CL} = \mathcal{CL}_+ \cup \mathcal{CL}_-$). Equation (14) illustrates the impact of marginal costs and distribution factors on the calculation of the shadow price without running economic dispatch.

This article has been accepted for inclusion in a future issue of this journal. Content is final as presented, with the exception of pagination.

$$\text{(C1) } \mathcal{G}_{\text{MU}} = \widetilde{\mathcal{G}}^k_{\text{MU}},\ \mathcal{CL}_+ = \widetilde{\mathcal{CL}}^k_+ : \Delta\Lambda^k_l(m,n) = \mathbf{\Phi}^{(\text{C1})}_{l,l}\begin{bmatrix}\Delta C^{\text{DA}}(j,i)\\ -\Delta C(j,i)\end{bmatrix}, \mathbf{\Phi}^{(\text{C1})}_{l,l} = \begin{bmatrix}\frac{\Delta S^{\text{DA}}_l(n,m)}{\Delta S^{\text{DA}}_l(i,j)} & \frac{\Delta \widetilde{S}^k_l(n,m)}{\Delta \widetilde{S}^k_l(i,j)}\end{bmatrix} \tag{15}$$

$$\text{(C2) } \mathcal{G}_{\text{MU}} \neq \widetilde{\mathcal{G}}^k_{\text{MU}},\ \mathcal{CL}_+ = \widetilde{\mathcal{CL}}^k_+ : \Delta\Lambda^k_l(m,n) = \mathbf{\Phi}^{(\text{C2})}_{l,l}\begin{bmatrix}\Delta C^{\text{DA}}(j,i)\\ -\Delta C(q,p)\end{bmatrix}, \mathbf{\Phi}^{(\text{C2})}_{l,l} = \begin{bmatrix}\frac{\Delta S^{\text{DA}}_l(n,m)}{\Delta S^{\text{DA}}_l(i,j)} & \frac{\Delta \widetilde{S}^k_l(n,m)}{\Delta \widetilde{S}^k_l(p,q)}\end{bmatrix} \tag{16}$$

$$\text{(C3) } \mathcal{G}_{\text{MU}} = \widetilde{\mathcal{G}}^k_{\text{MU}},\ \mathcal{CL}_+ \neq \widetilde{\mathcal{CL}}^k_+ : \Delta\Lambda^k_l(m,n) = \mathbf{\Phi}^{(\text{C3})}_{l,l'}\begin{bmatrix}\Delta C^{\text{DA}}(j,i)\boldsymbol{\chi}_{\mathcal{CL}_+}(l)\\ -\Delta C(j,i)\boldsymbol{\chi}_{\widetilde{\mathcal{CL}}^k_+}(l')\end{bmatrix}, \mathbf{\Phi}^{(\text{C3})}_{l,l'} = \begin{bmatrix}\frac{\Delta S^{\text{DA}}_l(n,m)}{\Delta S^{\text{DA}}_l(i,j)} & \frac{\Delta \widetilde{S}^k_{l'}(n,m)}{\Delta \widetilde{S}^k_{l'}(i,j)}\end{bmatrix} \tag{17}$$

$$\text{(C4) } \mathcal{G}_{\text{MU}} \neq \widetilde{\mathcal{G}}^k_{\text{MU}},\ \mathcal{CL}_+ \neq \widetilde{\mathcal{CL}}^k_+ : \Delta\Lambda^k_l(m,n) = \mathbf{\Phi}^{(\text{C4})}_{l,l'}\begin{bmatrix}\Delta C^{\text{DA}}(j,i)\boldsymbol{\chi}_{\mathcal{CL}_+}(l)\\ -\Delta C(q,p)\boldsymbol{\chi}_{\widetilde{\mathcal{CL}}^k_+}(l')\end{bmatrix}, \mathbf{\Phi}^{(\text{C4})}_{l,l'} = \begin{bmatrix}\frac{\Delta S^{\text{DA}}_l(n,m)}{\Delta S^{\text{DA}}_l(i,j)} & \frac{\Delta \widetilde{S}^k_{l'}(n,m)}{\Delta \widetilde{S}^k_{l'}(p,q)}\end{bmatrix} \tag{18}$$

Using equations (11) (with the shadow price related to only a positive line congestion) and (14), equation (13) for VBPS is rewritten as

$$\Delta\Lambda^k_l(m,n) = \left\{\Delta C^{\text{DA}}(j,i)\left[\frac{\Delta S^{\text{DA}}_l(n,m)}{\Delta S^{\text{DA}}_l(i,j)}\right]\right\}\boldsymbol{\chi}_{\mathcal{CL}}(l) - \left\{\Delta C(q,p)\left[\frac{\Delta \widetilde{S}^k_{l'}(n,m)}{\Delta \widetilde{S}^k_{l'}(p,q)}\right]\right\}\boldsymbol{\chi}_{\widetilde{\mathcal{CL}}^k}(l') \tag{19}$$

where, for $i,j \in \mathcal{G}_{\text{MU}}$, $p,q \in \widetilde{\mathcal{G}}^k_{\text{MU}}$, $l \in \mathcal{CL}_+$, and $l' \in \widetilde{\mathcal{CL}}^k_+$,

$$\Delta C^{\text{DA}}(j,i) = C^{\text{DA}}_j - C^{\text{DA}}_i, \quad \Delta C(q,p) = C_q - C_p$$
$$\Delta S^{\text{DA}}_l(n,m) = S^{\text{DA}}_{l,n} - S^{\text{DA}}_{l,m}, \quad \Delta S^{\text{DA}}_l(i,j) = S^{\text{DA}}_{l,i} - S^{\text{DA}}_{l,j}$$
$$\Delta \widetilde{S}^k_{l'}(n,m) = \widetilde{S}^k_{l',n} - \widetilde{S}^k_{l',m}, \quad \Delta \widetilde{S}^k_{l'}(p,q) = \widetilde{S}^k_{l',p} - \widetilde{S}^k_{l',q}.$$

Here, $\boldsymbol{\chi}_{\mathcal{CL}_+}(l)$ and $\boldsymbol{\chi}_{\widetilde{\mathcal{CL}}^k_+}(l')$ represent the characteristic functions based on the sets $\mathcal{CL}_+$ and $\widetilde{\mathcal{CL}}^k_+$ for congested lines l and l', corresponding to DA and RT markets, respectively. For example, if the line l is an element in the set $\mathcal{CL}_+$ in DA market, $\boldsymbol{\chi}_{\mathcal{CL}_+}(l) = 1$, otherwise $\boldsymbol{\chi}_{\mathcal{CL}_+}(l) = 0$.

According to the varying locations of marginal unit (MU) (i.e., a part-loaded generator) and congested line due to the line k error, equation (19) is finally categorized into the four different cases ((C1)∼(C4)) in matrix form (15)∼ (18), shown at the top of this page. In (C1) and (C4), both marginal unit and congested line are unchanged and changed with the line exclusion, respectively, whereas either of marginal unit and congested line is changed in (C2) and (C3). These matrix equations consist in two submatrices with different roles. The first $N_b(N_b-1)/2 \times 2$ submatrix $\mathbf{\Phi}_{l,l}$ provides information about the impact of topology change on VBPS for $m = 1,\ldots,N_b-1$ and $n = m+1,\ldots,N_b$. The second 2×1 submatrix associated with marginal costs measures the impact of different marginal costs on VBPS during topology change.

These formulated VBPS equations are the main results in this paper. They can be used by system operators in the following beneficial ways. The attacker's financial performance can be quickly quantified in an online manner for each case and compared with each other among different cases. In an offline way, the results based on historical data provide some guideline to maintain secure grid operations against a profitable topology data attack in virtual power market, and help to develop robust state estimation and economic dispatch algorithms to potential cyber data attacks.

Remark 2: Network decongestion in both DA and RT markets is excluded in the attack scenario because the adversary has no profit in such situation. Thus, for (C1) and (C2) the network in DA market must be congested for the adversary to make a profit. This implies that both $\boldsymbol{\chi}_{\mathcal{CL}_+}(l)$ and $\boldsymbol{\chi}_{\widetilde{\mathcal{CL}}^k_+}(l')$ equal to one. On the other hand, for (C3) and (C4) the network in at least either of two markets must be congested. Therefore, the corresponding characteristic functions are incorporated into equations (17) and (18), having the relationship with $\boldsymbol{\chi}_{\mathcal{CL}_+}(l) \vee \boldsymbol{\chi}_{\widetilde{\mathcal{CL}}^k_+}(l') = 1$.

Remark 3: The developed VBPS formulation can be used to examine the impact of not only the line exclusion but also the line susceptance change on the profit. This is readily carried out by modifying the element in the branch susceptance matrix $\widetilde{\mathbf{B}}$ subject to the attack:

$$\widetilde{\mathbf{B}} = diag(s_1, s_2, \ldots, s_{k-1}, s_k + ds_k, s_{k+1}, \ldots, s_{N_l}), \tag{20}$$

which corresponds to the kth line susceptance perturbatoin with $\widetilde{s}_k = s_k + ds_k$. Note that $\widetilde{s}_k = 0$ represents the kth line exclusion.

V. Simulation Results

In this section, a numerical study on IEEE 14-bus system in Fig. 3 is presented to illustrate the proposed framework. The simulation setup and scenario for the analysis of the proposed approach along with performance metrics are also explained in detail.

A. Simulation Setup and Performance Metric

IEEE 14-bus system is chosen as a test system to assess the attacker's performance:

- The attack-free IEEE 14-bus system consists in the five generators (Table IV) and a total of twenty transmission lines with their corresponding closed breakers as shown in Fig. 3. The line index number k is specified near each line.
- The networks in the day-ahead and real-time markets are assumed to have at most a single transmission line congestion.

Under this circumstance, the attack scenarios are tested with the following assumptions:

- An adversary participates in the day-ahead and real-time markets to conduct virtual bidding transactions.

This article has been accepted for inclusion in a future issue of this journal. Content is final as presented, with the exception of pagination.

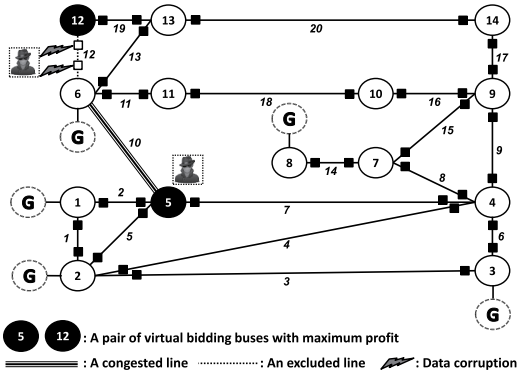


Fig. 3. Topology data attack with virtual bids in IEEE 14-bus system.

TABLE IV
GENERATOR PARAMETERS OF THE IEEE 14-BUS TEST SYSTEM

Bus	$P_{\min}$	$P_{\max}$	Ramp Rate	Marginal Cost
1	0MW	330MW	15MW/5min	40$/MWh
2	0MW	140MW	70MW/5min	15$/MWh
3	0MW	100MW	5MW/5min	55$/MWh
6	0MW	100MW	10MW/5min	70$/MWh
8	0MW	100MW	30MW/5min	90$/MWh

- With the knowledge of network topology, the adversary changes the condition of network topology in real-time market (i.e., the exclusion of a transmission line) to obtain a larger VBPS. This topology data attack can be feasible by manipulating the status of circuit breaker associated with the targeted line from on to off [9].
- The aforementioned topology data attack is limited to only a single line exclusion at a time in this paper.
- After attack, the network in real-time market has at most a single line congestion.
- Fig. 3 illustrates the situation where the adversary excludes the line 6-12 when the line 5-6 is congested, consequently making a maximum VBPS at a pair of virtual buses (5,12).

To evaluate the economic performance of topology data attack in terms of VBPS, the following performance metrics are used and calculated as:

$$k_{\max} = \arg\max_{k} \Delta\Lambda_l^k(m,n) \tag{21}$$

$$(m_{\max}, n_{\max}) = \arg\max_{(m,n)} \Delta\Lambda_l^k(m,n) \tag{22}$$

where $k_{\max}$ and $(m_{\max}, n_{\max})$ represent the index of the most influential transmission line on VBPS and the most profitable pair of virtual bidding buses with respect to VBPS.

B. Effect of Different Attack Lines on VBPS

We consider the situation where the line 5-6 is congested in both power markets. In this environment, it is assumed that the adversary as a virtual bidder wishes to make a profit at arbitrarily chosen virtual bidding buses by deleting some target line. Six different lines are selected to investigate their exclusion impact on VBPS. Among the selected six lines, two lines (the lines 12-13 and 1-5) are the most and least influential

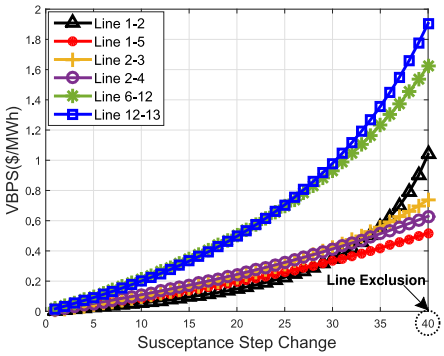


Fig. 4. Impact of the varying line susceptance for different lines on VBPS when the line 5-6 is congested.

ones on VBPS when they are excluded individually. In the simulation study, it is verified that the selection of different line sets do not violate our conclusion. To quantify and compare the sensitivity of VBPS with respect to the change in the susceptance for the selected attack line, the susceptance vector is used with increasing elements with a step size of number that is uniformly divided by forty from the true susceptance value to zero.

Fig. 4 shows the impact of the varying susceptance for six different lines on VBPS. The results in this figure are associated with (C1). In the x-axis, the fortieth step represents the line exclusion, corresponding to that line with zero susceptance. In this figure, we can verify $k_{\max} = 19$ among these six lines. In addition, the sensitivity of VBPS to the change in each line susceptance is compared with each other. For example, we observe that compared to the other lines' sensitivities the sensitivity for the line 1-2 increases slowly from 1 to 30 and fast from 31 to 40 in the x-axis.

Fig. 5 shows pairs of virtual bidding buses with a maximum profit, $(m_{\max}, n_{\max})$, for each line attack illustrated in Fig. 4. A total of 91 pairs of virtual bidding buses ($m = 1, \ldots, 14$, $n = m + 1$) are tested for six different line exclusions in the simulation. For each line exclusion, all profits for 91 pairs of buses are calculated, compared with each other and then a pair of buses with a maximum profit are selected using equation (22). For the line 1-2, 1-5, 2-3, 2-4, 6-12 and 12-13 exclusions, the corresponding $(m_{\max}, n_{\max})$ are $(2, 6)$, $(5, 6)$, $(2, 3)$, $(2, 4)$, $(5, 12)$, $(12, 13)$, respectively. We observe from these results that the adversary could make a maximum profit when he conducts virtual bidding at buses connected to the ends of the congested line or the excluded line. Another observation is that $(m_{\max}, n_{\max})$ can change according to different susceptance in the same attack line. For example, for the lines 1-2 and 1-5, $(m_{\max}, n_{\max}) = (1, 2)$ and $(m_{\max}, n_{\max}) = (1, 5)$ are obtained at the susceptance steps in Fig. 4, [15, 29] and [1, 2, 3, 5, 6, 9, 15, 16, 18, 21, 25, 27, 31, 34], respectively. Obviously, these pairs of virtual bidding buses are different from $(m_{\max}, n_{\max}) = (2, 6)$ and $(m_{\max}, n_{\max}) = (5, 6)$ associated with the lines 1-2 and 1-5 exclusions.

C. Effect of Different Marginal Costs on VBPS

In this subsection, we examine the impact of varying marginal costs on VBPS given a fixed attack line exclusion.

This article has been accepted for inclusion in a future issue of this journal. Content is final as presented, with the exception of pagination.

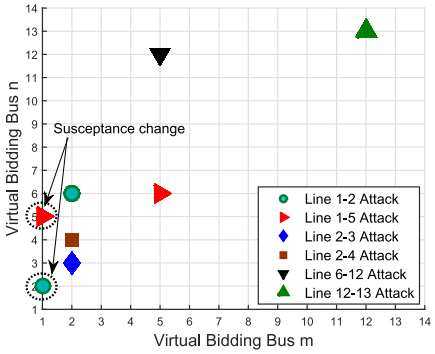


Fig. 5. Pairs of virtual bidding buses with a maximum profit from topology data attack illustrated in Fig. 4.

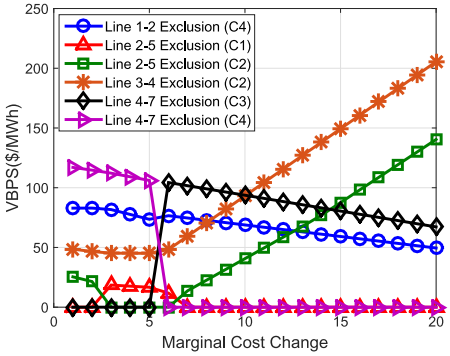


Fig. 6. Impact of the varying marginal cost of generator at bus 1 on VBPS when the line 2-4 is congested.

Let us assume the line 2-4 is congested. Four randomly chosen lines (1-2, 2-5, 3-4, 4-7) are considered to evaluate the change of VBPS with increasing marginal cost. Marginal cost of generator at bus 1 is set to increase with a step size of 1.5$/MWh from 20$/MWh to 50$/MWh. Fig. 6 shows two line exclusion groups, {(2-5), (3-4)} and {(1-2), (4-7)}, which generally lead to the increase and decrease of VBPS with increasing marginal cost, respectively. This positive or negative direction of VBPS due to varying marginal cost can be readily verified by checking the elements in the matrix $\mathbf{\Phi}_{l,l}$, which are computed by distribution factors related to $(m_{\max}, n_{\max})$ and the locations of marginal units (i, j) and (p, q).

Finally, the phenomena for the impact of the changing line susceptance (Fig. 4) and marginal cost (Fig. 6) on VBPS are normally unexpected by system operators without running economic dispatch. It is therefore important for them to adopt analytical framework such as shown in this paper to conduct analysis of such impacts from cyber attacks on the prices.

D. Comparison of the Performance of Continuous and Topology Data Attacks in Virtual Power Market

Fig. 7 shows LMP results for normal condition, continuous data attack [6] and topology data attack in the ex-post real-time market. A key observation from this figure is that topology data attack obtains a greater maximum VBPS than continuous data attack at buses 2 and 4. Indeed, continuous data attack makes a positive VBPS by only changing real-time network from congestion to decongestion. Therefore, VBPS is at most

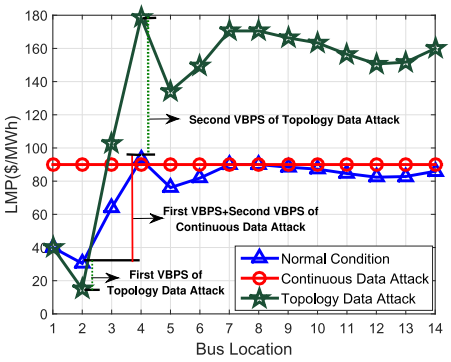


Fig. 7. Ex-post LMP results when the line 2-4 is congested under normal condition, continuous data attack and topology data attack.

the difference between the highest and lowest LMPs in day-ahead market. Furthermore, the profit for this attack is obtained only when the network is congested in day-ahead market. On the other hand, topology data attack is not restricted to network congestion condition for generating a positive VBPS.

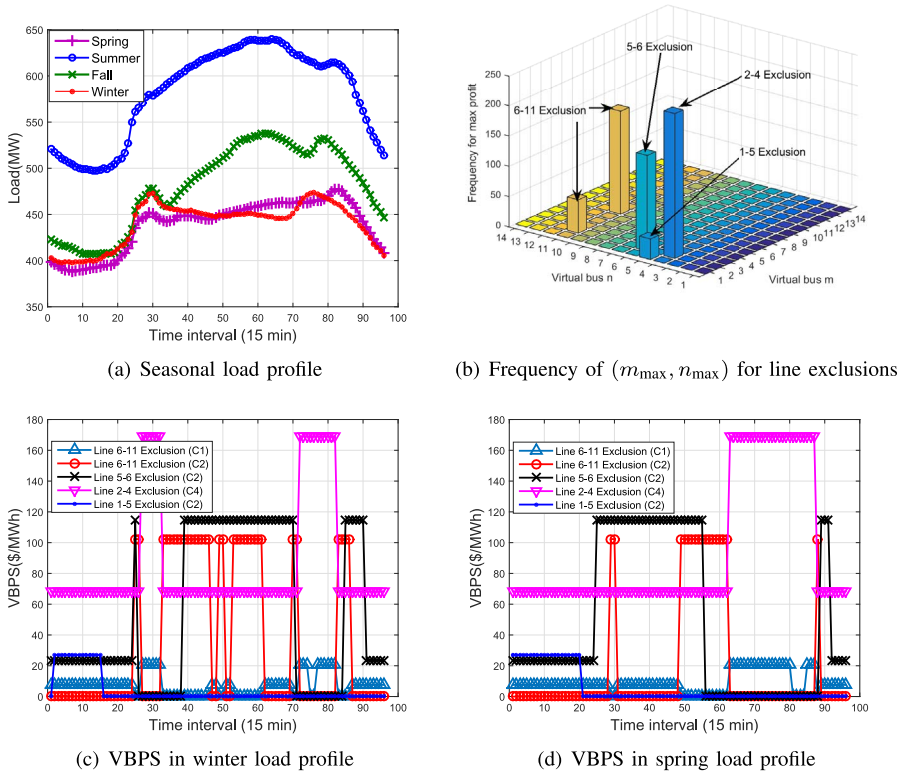
E. Analysis of VBPS in Multiple Interval Dispatch

In this subsection, the proposed framework is tested and analyzed under different loading conditions while the line 2-4 is congested. Fig. 8(a) provides 15-minute four load patterns in different seasons from ERCOT. Based on this load data, the frequency of $(m_{\max}, n_{\max})$ is computed for randomly chosen four line exclusions (1-5, 2-4, 5-6, 6-11), which is shown in Fig. 8(b). From this figure, we verify $k_{\max} = 4$ in terms of frequency for a maximum VBPS, leading to $(m_{\max}, n_{\max}) = (2, 4)$ in (C4). We also observe that $(m_{\max}, n_{\max})$ for each line exclusion are buses at the ends of the excluded line or the congested line. Figs. 8(c), (d) show VBPS at every dispatch interval in winter and spring load profiles. In these figures, the maximum VBPS for the line 2-4 exclusion is larger than the other line exclusions. Therefore, it is concluded that the line 2-4 is the most influential line on VBPS in terms of frequency and an amount of VBPS. On the other hand, the line 1-5 exclusion results in the least number of frequencies and amount of VBPS.

Lastly, the applications of the proposed VBPS equations can be summarized as follows.

1) *Secure Virtual Power Market Operation Tool:* the proposed VBPS equations offer system operators with an analysis tool to rapidly find the most (or least) influential transmission line on VBPS and the most (or least) profitable pair of virtual bidding buses in response to topology data attacks. The analysis results could be used to make a resilient operating procedure against such attacks in the light of secure virtual power market operations. In addition, the results for the effect of marginal costs on VBPS may provide generation companies as virtual bidders with some guideline to make their own bidding strategies.
2) *Sensor Upgrade and Protection:* the simulation results in the proposed framework show that the attacker could

This article has been accepted for inclusion in a future issue of this journal. Content is final as presented, with the exception of pagination.



(a) Seasonal load profile

(b) Frequency of $(m_{\max}, n_{\max})$ for line exclusions

(c) VBPS in winter load profile

(d) VBPS in spring load profile

Fig. 8. Simulation results for $(m_{\max}, n_{\max})$, $k_{\max}$ and VBPS at multiple dispatch intervals with varying seasonal load.

make a maximum profit when he conducts virtual bidding at buses connected to the ends of the congested line and/or the excluded line. Based on these results, analog and discrete sensors monitoring these lines should be upgraded and protected with high priority to mitigate the impact of the attacker's data manipulation from a cybersecurity perspective.

3) *Enhancement of the Robustness of EMS/MMS Applications:* the proposed VBPS equations and analysis results could be potentially integrated in the applications for EMS/MMS (e.g., power system state estimation, topology error processing and contingency analysis) in order to support robust virtual bidding market operations against topology data attacks.

VI. Conclusion

This paper presents a new approach to quantifying the economic impact of topology data attack while virtual bidding mechanism is conducted by the attacker. A closed-form framework has been developed to quickly calculate the adversary's profit at any pair of virtual bidding buses obtained through any transmission line exclusion in real time market. This framework has been validated and tested in the IEEE 14-bus system under various system operation conditions and attack scenarios (e.g., the locations of marginal unit, congested line and attack line) and different loading conditions. From a cybersecurity perspective in smart grid, this work is a first step toward providing system operators with an analysis tool and countermeasures to examine and mitigate financial risks of cyber threats in real-time power market.

In the future, we plan to propose other type of topology data attack (e.g., line parameter data attack) and test the feasibility of this attack. The financial risk analysis of the proposed attacks would also be carried out in our developed framework under realistic grid conditions and various attack scenarios.

References

[1] X. Luo, D. Obadina, and M. Boddeti, "The roles of energy management system in Texas nodal power market," in *Proc. IEEE Power Eng. Soc. Gen. Meeting*, Calgary, AB, Canada, Jul. 2009, pp. 1–7.

[2] Y. Liu, M. K. Reiter, and P. Ning, "False data injection attacks against state estimation in electric power grids," in *Proc. 16th ACM Conf. Comput. Commun. Sec.*, Chicago, IL, USA, Nov. 2009, pp. 21–32.

[3] 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.

[4] T. T. Kim and H. V. Poor, "Strategic protection against data injection attacks on power grids," *IEEE Trans. Smart Grid*, vol. 2, no. 2, pp. 326–333, Jun. 2011.

[5] A. Giani *et al.*, "Smart grid data integrity attacks," *IEEE Trans. Smart Grid*, vol. 4, no. 3, pp. 1244–1253, Sep. 2013.

[6] L. Xie, Y. Mo, and B. Sinopoli, "Integrity data attacks in power market operations," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 659–666, Dec. 2011.

[7] 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.

[8] 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.

[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] M. A. Rahman, E. Al-Shaer, and R. Kavasseri, "Impact analysis of topology poisoning attacks on economic operation of the smart power grid," in *Proc. IEEE 34th Int. Conf. Distrib. Comput. Syst.*, Madrid, Spain, Jun. 2014, pp. 649–659.

This article has been accepted for inclusion in a future issue of this journal. Content is final as presented, with the exception of pagination.

[11] S. Bi and Y. J. Zhang, "Graphical methods for defense against false-data injection attacks on power system state estimation," *IEEE Trans. Smart Grid*, vol. 5, no. 3, pp. 1216–1227, May 2014.
[12] S. Bi and Y. J. Zhang, "Using covert topological information for defense against malicious attacks on DC state estimation," *IEEE J. Sel. Areas Commun.*, vol. 32, no. 7, pp. 1471–1485, Jul. 2014.
[13] G. Hug and J. A. Giampapa, "Vulnerability assessment of AC state estimation with respect to false data injection cyber-attacks," *IEEE Trans. Smart Grid*, vol. 3, no. 3, pp. 1362–1370, Sep. 2012.
[14] L. Jia, R. J. Thomas, and L. Tong, "On the nonlinearity effects on malicious data attack on power system," in *Proc. IEEE Power Eng. Soc. Gen. Meeting*, San Diego, CA, USA, Jul. 2012, pp. 1–8.
[15] H. Ye, Y. Ge, X. Liu, and Z. Li, "Transmission line rating attack in two-settlement electricity markets," *IEEE Trans. Smart Grid*, to be published, doi: 10.1109/TSG.2015.2426418.
[16] 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.
[17] (Feb. 2014). *Report on the Impact of Virtual Transactions*. [Online]. Available: https://www.pjm.com/~/media/documents/ferc/2014-filings/20140207-er13-1654-000.ashx.
[18] A. Jha and F. A. Wolak, "Testing for market efficiency with transactions costs: An application to convergence bidding in wholesale electricity markets," Dept. Econ., Stanford Univ., Stanford, CA, USA, Tech. Rep., Apr. 2015. [Online]. Available: http://web.stanford.edu/group/fwolak/cgi-bin/sites/default/files/CAISO_VB_draft_VNBER_final.pdf.
[19] "MISO virtual and FTR trading," 146 FERC 61,072, Order Approving Stipulation and Consent Agreement, Docket no. IN12-6-000.
[20] F. Li and R. Bo, "DCOPF-based LMP simulation: Algorithm, comparison with ACOPF, and sensitivity," *IEEE Trans. Power Syst.*, vol. 22, no. 4, pp. 1475–1485, Nov. 2007.
[21] F. Li, Y. Wei, and S. Adhikari, "Improving an unjustified common practice in ex post LMP calculation," *IEEE Trans. Power Syst.*, vol. 25, no. 2, pp. 1195–1197, May 2010.
[22] F. F. Wu, P. Varaiya, P. Spiller, and S. Oren, "Folk theorems on transmission access: Proofs and counterexamples," *J. Regul. Econ.*, vol. 10, no. 1, pp. 5–23, Jul. 1996.
[23] D.-H. Choi and L. Xie, "Impact analysis of locational marginal price subject to power system topology errors," in *Proc. 4th IEEE Smart Grid Commun. Conf.*, Vancouver, BC, Canada, Oct. 2013, pp. 55–60.

Dae-Hyun Choi (S'10–M'06) received the B.S. degree in electrical engineering from Korea University, Seoul, South Korea, in 2002, and the M.Sc. and Ph.D. degrees in electrical and computer engineering from Texas A&M University, College Station, TX, USA, in 2008 and 2014, respectively. He is currently an Assistant Professor with the School of Electrical and Electronics Engineering, Chung-Ang University, Seoul. From 2002 to 2006, he was a Researcher with Korea Telecom, Seoul, where he researched designing and implementing home network systems. His research interests include power system state estimation, electricity markets, the cyber-physical security of smart grids, and the theory and application of cyber-physical energy systems.

Le Xie (S'05–M'10) received the B.E. degree in electrical engineering from Tsinghua University, Beijing, China, in 2004; the M.Sc. degree in engineering sciences from Harvard University, Cambridge, MA, USA, in 2005; and the Ph.D. degree in electrical and computer engineering from Carnegie Mellon University, Pittsburgh, PA, USA, in 2009. He is currently an Associate Professor with the Department of Electrical and Computer Engineering, Texas A&M University, College Station. His industry experience includes an internship (2006) at ISO-New England, and Edison Mission Energy Marketing and Trading (2007). His research interest includes modeling and control of large-scale complex systems, smart grid application with renewable energy resources, and electricity markets.