IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received December 18, 2017, accepted January 26, 2018, date of publication February 5, 2018, date of current version March 13, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2801861

False Data Injection Attacks on Contingency Analysis: Attack Strategies and Impact Assessment

JEONG-WON KANG, (Student Member, IEEE), IL-YOUNG JOO, (Student Member, IEEE), AND DAE-HYUN CHOI, (Member, IEEE)

School of Electrical and Electronics Engineering, Chung-Ang University, Dongjak-gu, Seoul 156-756, South Korea

Corresponding author: Dae-Hyun Choi (dhchoi@cau.ac.kr)

This work was supported in part by the Korea Electric Power Corporation under Grant R17XA05-75 and in part by the National Research Foundation of Korea Grant, Korea Government (MSIP), under Grant 2015R1C1A1A01051890.

ABSTRACT In this paper, a new class of false data injection attacks (FDIAs) on contingency analysis (CA) through state estimation (SE) is proposed, and the economic impact of the proposed attacks on real-time power market operations is quantified. Compared with the existing FDIAs, where no contingency analysis is considered for attack targets, we present a new attack strategy with which the adversary stealthily drops or adds contingency pairs of transmission line flows from or to a normal contingency list by misleading the CA process through injecting false data into SE. The manipulated contingency pairs are then embedded as security constraints into operating constraints of security-constrained economic dispatch. As a result, the proposed attacks lead to the miscalculation of locational marginal price (LMP) in real-time power markets. The capability and economic impact of the proposed attack, such as a list of manipulated contingency line pairs, attack effort, and LMP deviation from normal price, are illustrated in the IEEE 14-bus system.

INDEX TERMS False data injection attack, contingency analysis, state estimation, security constrained economic dispatch.

I. INTRODUCTION

For reliable power grid operations, system operators focus on maintaining power grid *physical security* that is the ability of power grids to withstand sudden disturbances such as natural disasters [1]. However, as emerging smart grid technologies rely more on information and communication technology (ICT), power grids are more vulnerable to cyber attacks through ICT systems. Recently, the 2015 Ukraine blackout [2] was the first cyber attack against electric power systems by compromising ICT networks and components, leading to blackouts in three Ukrainian regions. Therefore, enhancing *cybersecurity* is also increasingly critical in managing power grid operations more reliably and securely [3]. This study investigates the impact of cyber attacks on *physical security* and *cybersecurity* of smart grid.

In power system operations, on-line physical security assessment can be conducted with the following three major functions: (1) state estimation (SE); (2) contingency analysis (CA); and (3) security-constrained optimal power flow (SCOPF). The goal of SE is to process data (e.g., power injection/flow, bus voltage magnitude, and on/off status of circuit breaker) from a supervisory control and data acquisition (SCADA) system, to calculate the best estimate of the power system's state, and to construct real-time network models based on the estimate [4]. The constructed real-time network models are then used by CA module, identifying overloads due to potential contingencies such as generator or transmission line failure. In general, CA is conducted based on DC or AC power flow method and consists of static CA and dynamic CA, corresponding to: (a) line overflow and bus overvoltage; and (b) voltage stability. In this paper, static CA using DC power flow analysis is considered since static CA is more tightly coupled with SE than dynamic CA. Finally, CA calculates a list of line or generator contingencies, namely contingency list with which the SCOPF module redispatches optimal power of generators for preventing potential contingency violations [5]. Due to computation complexity in real-time power market operations, a linearized line

flow-based security-constrained economic dispatch (SCED) is conducted, which is a simplified formulation of SCOPF based on DC assumptions [6]. In this paper, we consider the proposed attack problem in the procedure of on-line power system security assessment as shown in Fig. 1. This figure illustrates the relationship among SCADA telemetry, SE, CA in cyber layer, and SCED in market layer, along with the following information flow (solid black line): normal SCADA data ⇒ SE ⇒ CA ⇒ SCED.

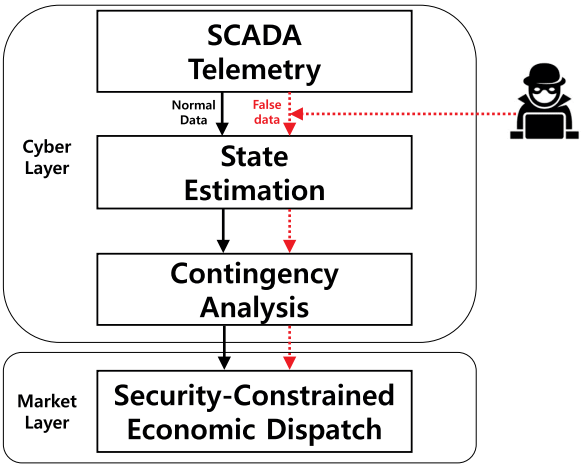


FIGURE 1. Illustration of the relationship among SCADA, SE, CA, and SCED.

It should be noted that the performance of the physical security process above highly depends on the accuracy of SE results that are calculated based on measurements from many SCADA sensors (e.g., remote terminal unit (RTU)). Therefore, compromising sensors by injecting malicious data into SE measurements could have catastrophic impact on CA and SCED solutions sequentially. This type of cyber data attack against SE is known as a false data injection attack (FDIA). This paper contributes to the following two aspects: (1) the proposal for a new class of FDIA strategies with which the adversary manipulates normal contingency list from CA through the malfunction of the SE process; and (2) economic impact analysis of SCED subject to the proposed attacks, as shown in Fig. 1 (dotted red line).

Recently, much research has focused on the development of FDIA strategies and the quantification of their impact on physical and economic grid operations. This ranges from the formulation of the attack against DC state estimator [7] (a pioneering work on FDIA problem in power grid) and AC state estimator [8]–[10] with impact analysis of attacks, network topology attack through the manipulation of circuit breaker's on/off status data [11]–[16], blind FDIA attack without the knowledge of network topology using the principal component analysis [17], imperfect false data injection based on forecasting-aided method [18], attack automatic generation control (AGC) attack [19], and economic assessment of the attack on virtual transactions [20] and real-time power market operations [21]. More recently, it has been justified that these previous studies above are theoretical examinations no longer and actual FDIA attacks would become feasible in real power grids [22].

While many studies have addressed the feasibility of FDIAs and evaluated the vulnerability of power grids to such attacks, various methods for detecting and identifying FDIA have been proposed to mitigate detrimental impact of FDIA on power grid operations. In [23], the least-budget depending method against FDI attack was presented wherein the selection of securely protected sensors was solved by a mixed integer nonlinear programming (MINLP) problem based on Bender's decomposition. Using cluster algorithm, vulnerable buses and sensitive SCADA measurements to FDIA were classified and identified, leading to effective FDIA detection [24]. A new framework to detect FDIAs against DC microgrids was proposed in [25]. In [26], short-term state forecasting-aided method was presented where the consistency between the forecasted measurements and the received measurements are checked to identify false data in critical measurements. A sequential detection problem of FDIAs was addressed and a sequential detector based on the generalized likelihood ratio was proposed to quickly detect FDIAs in [27]. More recently, machine learning technique was used to easily detect FDIA for classifying measurements into non-attack events (e.g., natural contingency and operator's control action) and attack events by using: temporal characteristics of FDIA using Conditional Deep Belief Network (CDBN) [28], semisupervised online learning method [29], and non-nested generalized exemplars (NNGE) through pre-processing of the state extraction method (STEM) [30]. A concise review of various FDIA strategies and defending methods in smart grid is summarized in [31] and [32].

Although extensive research has been conducted on the subject of FDIA problems, to the best of our knowledge, no study has proposed FDIAs on CA and quantified the economic impact of such attacks on real-time market operations. Recently, the method of FDIA on static security analysis and its impact on market operations were studied in [33]. However, no detailed algorithm of CA was considered in the attack method, and the impact analysis of real-time electricity prices subject to such attack was excluded.

In this paper, a new class of optimization-based FDIAs is presented considering *static CA*, and *the economic impact* of such attacks on real-time LMP is assessed. The main contributions of this paper are two-fold:

1) We propose two types of FDIAs on CA. The adversary stealthily drops or adds contingency pairs of transmission line flows from or to a normal contingency list by misleading the CA process through injecting false data into SE while being undetected by bad data detection (BDD) embedded in the state estimator. We model a least-effort attack as a mixed integer nonlinear programming (MINLP)-based optimization problem. The goal of the formulated optimization problem is to minimize the number of compromised analog and digital sensors to manipulate targeted contingency pairs successfully.

2) We evaluate the performance of the proposed attacks in terms of: i) the targeted dropped or added contingency pairs; ii) the manipulated analog and digital measurements; and iii) attack effort (i.e., a maximum number of compromised sensors). In addition, we investigate the impact of the manipulated contingency list due to attacks on real-time LMP that is calculated by SCED. Various case studies including the quantification of the attack performance and its economic impact on LMP are illustrated in the IEEE 14-bus system.

This paper is organized as follows. Section II provides the brief overview of SE, CA, and real-time SCED. The proposed optimization-based attack strategies are formulated in Section III. Case studies of the proposed attacks are presented in the IEEE 14-bus system in Section IV. Finally, conclusions and future studies are discussed in Section V.

II. BACKGROUND

A. STATE ESTIMATION (SE)

Assuming that N_b is the number of buses, N_l is the number of lines, and N_m is the number of measurements, we consider the linearized DC state estimation model:

$$\mathbf{z} = \mathbf{H}(\mathbf{c})\mathbf{x} + \mathbf{e}, \tag{1}$$

where $\mathbf{z}$ is the $N_m \times 1$ analog measurement vector that consists in real power injection and flow measurements, $\mathbf{x}$ is the $(N_b - 1) \times 1$ state vector that consists in the bus voltage phase angles excluding a slack bus, and $\mathbf{e}$ is the $N_m \times 1$ independent identically distributed (i.i.d.) Gaussian measurement error vector with zero mean and diagonal covariance matrix $\mathbf{R}$. $\mathbf{H}(\mathbf{c})$ is the $N_m \times (N_b - 1)$ Jacobian matrix that illustrates the relationship between $\mathbf{z}$ and $\mathbf{x}$ with the system topology. The system topology is determined by the $N_l \times 1$ binary digital measurement vector $\mathbf{c} \in \{0, 1\}^{N_l}$: 0 and 1 represent the open and closed status of the corresponding line, respectively. For a simple notation, $\mathbf{H}(\mathbf{c})$ is denoted by $\mathbf{H}$.

The SE problem is to find the optimal estimate of $\mathbf{x}$ to minimize the weighted least square of measurement error:

$$\text{minimize } J(\mathbf{x}) = \mathbf{r}^T \mathbf{R}^{-1} \mathbf{r} \tag{2}$$

$$\text{s.t. } \mathbf{r} = \mathbf{z} - \mathbf{H}\mathbf{x}, \tag{3}$$

where $\mathbf{r}$ is the estimated residual vector. If the Jacobian matrix $\mathbf{H}$ is full rank (i.e., the system is observable), the unique weighted least squares estimate of $\mathbf{x}$ is given by

$$\hat{\mathbf{x}}(\mathbf{z}) = (\mathbf{H}^T \mathbf{R}^{-1} \mathbf{H})^{-1} \mathbf{H}^T \mathbf{R}^{-1} \mathbf{z}. \tag{4}$$

During the state estimation process, the bad data detection is conducted using the Chi-squares test based on the estimated objective function $J(\hat{\mathbf{x}})$. Since $J(\hat{\mathbf{x}})$ follows a Chi-square distribution with $N_m - (N_b - 1)$ degrees of freedom, bad data will be suspected if $J(\hat{\mathbf{x}}) \geq \eta_{[(N_m-(N_b-1)),p]}$ where p is the detection confidence probability.

B. CONTINGENCY ANALYSIS (CA)

CA is an application to enable power systems to operate defensively in case of unplanned and/or unscheduled failure events such as transmission line outage and generator failure. In general, CA consists of two main components: (1) contingency selection [34]–[36]; and (2) contingency evaluation [37], [38]. The goal of contingency selection is to reduce the computation burden of subsequent contingency evaluation process by making a short list of all the contingencies, *namely mon-con pairs* (a pair of *mon*itored line/generator and their corresponding *con*tingency). Based on the short contingency list from contingency selection, contingency evaluation is to check operating violations of all lines and generating units for each contingency and to finally construct *a contingency list*, a subset of mon-con pairs [6]. In particular, the contingency list to transmission line flows can be quickly calculated using the following equation (5) based on DC power flow analysis method:

$$\widetilde{F}_{u,k} = \widehat{F}_u + \boldsymbol{\Upsilon}[u,k]\widehat{F}_k, \quad (u,k) \in \mathcal{MC} \tag{5}$$

where

$$\boldsymbol{\Upsilon}[u,k] = \boldsymbol{\Phi}_u[i,j]/(1 - \boldsymbol{\Phi}_k[i,j]), \tag{6}$$

$$\boldsymbol{\Phi}_k[i,j] = \mathbf{S}[k,i] - \mathbf{S}[k,j]. \tag{7}$$

In (5), $\mathcal{MC}$ represents the set of mon-con pairs (u,k) from contingency selection. $\widehat{F}_u$ and $\widehat{F}_k$ imply estimated power flows at lines u and k prior to line outage. We note that those power flow values are delivered from the state estimator. $\widetilde{F}_{u,k}$ is power flow at line u when line k outage occurs. $\boldsymbol{\Upsilon}[u,k]$ is the (u,k)th element of the $N_l \times N_l$ line outage distribution factor (LODF) matrix $\boldsymbol{\Upsilon}$ that illustrates the sensitivity of line u overload to line k outage. In (6), the LODF matrix $\boldsymbol{\Upsilon}$ is calculated using the $N_b \times N_b$ power transfer distribution factor (PTDF) matrix $\boldsymbol{\Phi}$ (e.g., provision of the sensitivity of line u or line k flow to real power transactions between buses i and j). The PTDF $\boldsymbol{\Phi}_k[i,j]$ for line k between a power injection at bus i and a power withdraw at bus j is computed using the generation shift factors (GSFs) ($\mathbf{S}[k,i]$, $\mathbf{S}[k,j]$) in (7). $\mathbf{S}[k,i]$ is the (k,i)th element of the $N_l \times N_b$ GSF matrix $\mathbf{S}$ that illustrate the sensitivity of line flow to injected power. Here, the GSF matrix is constructed with $\mathbf{S} = [\mathbf{0}\ \mathbf{B}\mathbf{A}\mathbf{B}_R^{-1}]$ where $\mathbf{0}$ is the $N_l \times 1$ vector with all ones, $\mathbf{B}$ is the $N_l \times N_l$ diagonal matrix with each line's susceptance, $\mathbf{A}$ is the $N_l \times (N_b - 1)$ line-to-bus incidence matrix, and $\mathbf{B}_R$ is the $(N_b - 1) \times (N_b - 1)$ reduced bus-to-bus susceptance matrix except the slack bus.

In sum, Fig. 2 illustrates the procedure of the CA. It is noted that the CA process initiates with the solution of state estimator. In this figure, (5) is used to conduct contingency evaluation where $\widetilde{F}_{u,k}$ is compared with corresponding maximum or minimum capacity limit of line flow, consequently constructing the contingency table with contingency pairs for line overloads. Those contingency pairs are then embedded as inequality constraints into the system operating constraints of SCED, which is illustrated in the next subsection.

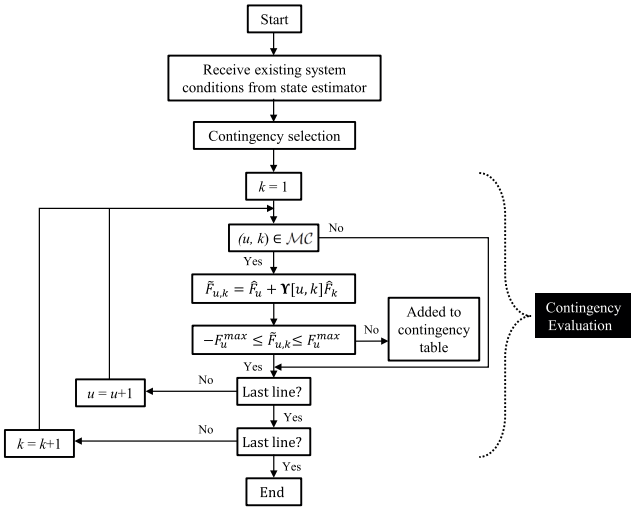


FIGURE 2. Flowchart of the procedure of contingency analysis based on DC power flow analysis method.

C. REAL-TIME SECURITY-CONSTRAINED ECONOMIC DISPATCH (SCED)

In real-time markets, SCED is formulated as follows [6]: $\forall i = 1, \ldots, N_b, \forall l = 1, \ldots, N_l$,

$$\min_{P_{g_i}} \sum_{i=1}^{N_b} C_i(P_{g_i}) \tag{8}$$

$$\text{s.t. } \lambda: \sum_{i=1}^{N_b} P_{g_i} = \sum_{i=1}^{N_b} L_{d_i} \tag{9}$$

$$\boldsymbol{\tau}: P_{g_i}^{\min} \le P_{g_i} \le P_{g_i}^{\max} \tag{10}$$

$$\boldsymbol{\mu}: F_l^{\min} \le \mathbf{S}_l(\mathbf{P}_g - \mathbf{L}_d) \le F_l^{\max} \tag{11}$$

$$\boldsymbol{\mu}_s: F_u^{s,\min} \le \boldsymbol{\Gamma}_u(\mathbf{P}_g - \mathbf{L}_d) \le F_u^{s,\max}. \tag{12}$$

In this formulation, the objective function is to minimize the total generation costs in (8). (9) is the system-wide energy balance equation. (10) is the physical capacity constraints of each generator. (11) is the network flow constraints without considering line outage where $\mathbf{S}_l$ represents the lth row of the GSF matrix $\mathbf{S}$. (12) is the security constraints that are the results of contingency evaluation as mentioned in the previous subsection. In (12), $\boldsymbol{\Gamma}_u$ is the uth row of the matrix $\boldsymbol{\Gamma}$ with $\boldsymbol{\Gamma}_u = \mathbf{S}_u + \boldsymbol{\Upsilon}[u,k]\mathbf{S}_k$. The elements in the matrix $\boldsymbol{\Gamma}$ are called as the compensated generation shift sensitivities, providing the sensitivity of line u with respect to change in net injection at any bus when line k outage occurs. It is noted that the constraints (12) are defined as *the security constraints*, which are the result of the contingency pairs from CA.

According to the definition of the nodal price, and assuming that bus 1 is the slack bus, locational marginal price (LMP) for each bus n ($i = 2, \ldots, N$) is given by

$$\mathbf{LMP} = \lambda\mathbf{1} - \begin{bmatrix} \mathbf{S} \\ \boldsymbol{\Gamma} \end{bmatrix}^T \left(\begin{bmatrix} \boldsymbol{\mu}^{\max} \\ \boldsymbol{\mu}_s^{\max} \end{bmatrix} - \begin{bmatrix} \boldsymbol{\mu}^{\min} \\ \boldsymbol{\mu}_s^{\min} \end{bmatrix} \right), \tag{13}$$

where λ, $\boldsymbol{\mu}^{\max}$, $\boldsymbol{\mu}^{\min}$, $\boldsymbol{\mu}_s^{\max}$ and $\boldsymbol{\mu}_s^{\min}$ are the Lagrangian multipliers of equality and inequality constraints in the SCED formula. λ is the LMP for the slack bus 1. $\{\boldsymbol{\mu}^{\max}, \boldsymbol{\mu}^{\min}\}$ and $\{\boldsymbol{\mu}_s^{\max}, \boldsymbol{\mu}_s^{\min}\}$ correspond to congestion prices when line flows are binding at network flow constraints and security constraints, respectively.

III. ATTACK FORMULATION

A. ATTACK MODEL AND ASSUMPTIONS

In the proposed attack, the adversary is required to have the following capabilities:

(R1) The adversary has the knowledge of system topology including the status of circuit breakers and each line's parameter/limits.

(R2) The adversary can compromise SCADA sensors by observing and manipulating measurements.

(R3) Given manipulated measurements, the adversary can conduct SE and BDD to calculate desired line flow estimate while being undetected by BDD process.

(R4) Prior to the attack, the adversary can conduct CA to obtain the contingency list. The targeted contingency pairs are dropped or added to the attack-free contingency LIST. To this end, using the manipulated line flow estimate in (R3) the adversary must be able to calculate new line flow estimates considering contingencies.

In [22], the authors have justified that the aforementioned assumptions are reasonable and FDIAs can be feasible by: (i) using off-line or on-line measurements to estimate the system topology (R1); (ii) injecting malicious data into sensors through an insecure SCADA communication protocol (R2); and (iii) understanding architecture and algorithms of power system applications such as SE, CA, and BDD from textbooks and research publications (R3), (R4).

In this study, we consider the additive attack measurement model:

$$\mathbf{z}^a = \mathbf{H}(\mathbf{c} + \boldsymbol{\beta})\mathbf{x} + \mathbf{e} + \boldsymbol{\alpha}, \tag{14}$$

where $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$ are the attack vectors for analog and digital measurements, leading to corrupted measurement vector $\mathbf{z}^a$. Using the attack measurement model (14), the proposed attack strategies are illustrated in the following two subsections.

B. ATTACK STRATEGY I

We assume that any line l can belong to one of the three types of lines $\{u, k, t\}$: line u is the monitored line, line t is the targeted line, and line k is the untargeted line. The superscript a of variable, vector, and matrix indicates that they are changed by the attack vector. $\mathcal{CP}$ and $\overline{\mathcal{CP}}$ represent the set of contingency and non-contingency pairs, respectively.

The goal of attack strategy I is to drop targeted contingency pairs $(u, t) \in \mathcal{CP}$ from an attack-free contingency table with minimum attack effort, while keeping untargeted contingency pairs (u, k) belonging to a set of non-contingency pairs $\in \overline{\mathcal{CP}}$ as well as bypassing the BDD module.

To this end, the adversary computes malicious injected analog and discrete attack measurement vectors ($\boldsymbol{\alpha}$, $\boldsymbol{\beta}$) by

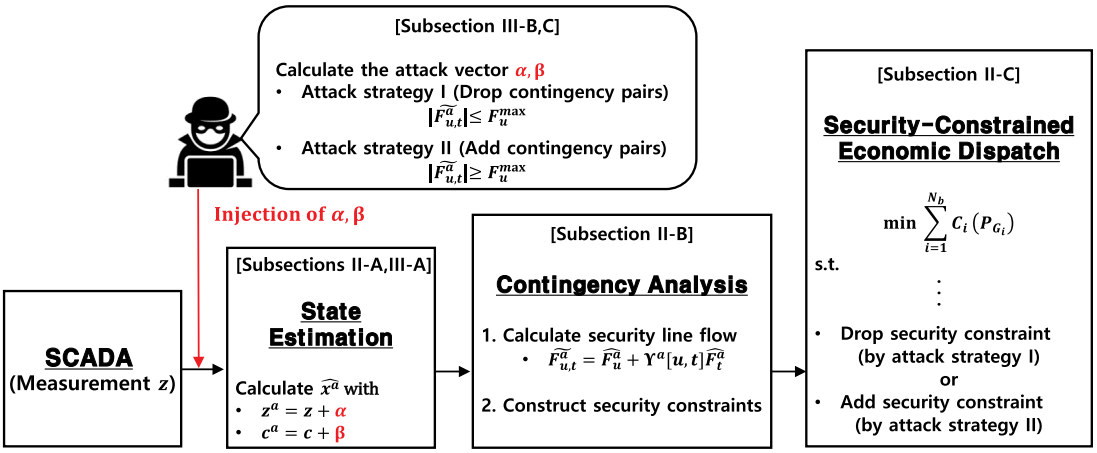


FIGURE 3. Procedure of the proposed attack among SCADA, SE, CA, and SCED.

minimizing attack effort (15) while satisfying feasible attack constraints (16)–(24) in the following optimization problem:

$$\min_{\boldsymbol{\alpha},\boldsymbol{\beta}} \ (||\boldsymbol{\alpha}||_0 + ||\boldsymbol{\beta}||_0) \tag{15}$$
$$\text{s.t. } \mathbf{z}^a = \mathbf{z} + \boldsymbol{\alpha} \tag{16}$$
$$\mathbf{c}^a = \mathbf{c} + \boldsymbol{\beta} \tag{17}$$
$$(\mathbf{A}^a)^T = \text{Diag}(\mathbf{c}^a)(\mathbf{A}^f)^T \tag{18}$$
$$J(\widehat{\boldsymbol{x}}^a) \le \eta \tag{19}$$
$$\widehat{F}^a_l = \mathbf{B}_l(\mathbf{A}^a)^T\widehat{\boldsymbol{x}}^a, \quad l \in \{u,k,t\} \tag{20}$$
$$\widetilde{F}^a_{u,k} = \widehat{F}^a_u + \boldsymbol{\Upsilon}^a[u,k]\widehat{F}^a_k, \quad (u,k) \in \overline{\mathcal{CP}} \tag{21}$$
$$\widetilde{F}^a_{u,t} = \widehat{F}^a_u + \boldsymbol{\Upsilon}^a[u,t]\widehat{F}^a_t, \quad (u,t) \in \mathcal{CP} \tag{22}$$
$$|\widetilde{F}^a_{u,k}| \le F^{\max}_u, \quad (u,k) \in \overline{\mathcal{CP}} \tag{23}$$
$$|\widetilde{F}^a_{u,t}| \le F^{\max}_u. \quad (u,t) \in \mathcal{CP} \tag{24}$$

The objective function (15) for the attack optimization problem above is defined as the attack effort that consists in the two l_0-norms of the attack vectors ($\boldsymbol{\alpha}$, $\boldsymbol{\beta}$), corresponding to a maximum number of compromised analog sensors for power injection/flow measurements and digital sensors for status of open/closed lines, respectively. Constraints (16) and (17) represent the attack measurement equations associated with analog and discrete measurement manipulation, respectively. Constraint (18) illustrates the relationship between the fully connected line-to-bus incidence matrix $(\mathbf{A}^f)^T$ and the attack matrix $(\mathbf{A}^a)^T$ due to manipulated digital measurements $\mathbf{c}^a$. Undetectability of the attack can be ensured by escaping the BDD module in constraint (19). Constraint (20) is the equation for power flow $\widehat{F}^a_l$ at line l, manipulated by the adversary through malicious change of analog and digital measurements. Using the LODF matrix $\boldsymbol{\Upsilon}^a$ modified by the adversary, flows on line u subject to line k outage $\in \overline{\mathcal{CP}}$ and line t outage $\in \mathcal{CP}$ are computed in (21) and (22), respectively. While non-contingency pairs before the attack remain secure line pairs after the attack in (23), constraint (24) guarantees the drop of targeted contingency pairs (u,t) from the contingency table, consequently misleading the CA module to select them as insecure line pairs.

C. ATTACK STRATEGY II

In attack strategy II, the adversary computes the attack measurement vectors ($\boldsymbol{\alpha}$, $\boldsymbol{\beta}$) in the following optimization problem:

$$\min_{\boldsymbol{\alpha},\boldsymbol{\beta}} \text{ Eqn. (15)} \tag{25}$$
$$\text{Eqn. (16)} - \text{(20)} \tag{26}$$
$$-\mathbf{F}^{\max} \le \widehat{\mathbf{F}}^a \le \mathbf{F}^{\max} \tag{27}$$
$$\widetilde{F}^a_{u,k} = \widehat{F}^a_u + \boldsymbol{\Upsilon}^a[u,k]\widehat{F}^a_k, \quad (u,k) \in \mathcal{CP} \tag{28}$$
$$\widetilde{F}^a_{u,t} = \widehat{F}^a_u + \boldsymbol{\Upsilon}^a[u,t]\widehat{F}^a_t, \quad (u,t) \in \overline{\mathcal{CP}} \tag{29}$$
$$|\widetilde{F}^a_{u,k}| \ge F^{\max}_u, \quad (u,k) \in \mathcal{CP} \tag{30}$$
$$|\widetilde{F}^a_{u,t}| \ge F^{\max}_u. \quad (u,t) \in \overline{\mathcal{CP}} \tag{31}$$

Compared to attack strategy I where the adversary reduces the size of contingency table, attack strategy II focuses on increasing the number of contingency pairs by adding targeted non-contingency pairs to the contingency table. The objective function (15) and constraints (16)-(20) for measurement manipulation, calculation of estimated line flows, and undetectable condition in the attack I formulation are added to the attack II formulation. When there is no contingency at all, overloading of all lines due to the attack can be escaped in (27) where $\widehat{\mathbf{F}}^a = [\widehat{F}^a_1, \widehat{F}^a_2, \ldots, \widehat{F}^a_{N_l}]^T$ and $\mathbf{F}^{\max} = [F^{\max}_1, F^{\max}_2, \ldots, F^{\max}_{N_l}]^T$. Constraints (28) and (29) represent the flow on line u when outage occurs at untargeted line k and targeted line t, belonging to sets of contingency pairs and non-contingency pairs, respectively. The list of contingency pairs including untargeted lines before the attack can remain insecure pairs after the attack in (30). Conversely, constraint (31) ensures that targeted non-contingency pairs before the attack are changed to contingency pairs with increasing size of the contingency table.

Finally, Fig. 3 illustrates the procedure of the proposed attacks I and II among SCADA, SE, CA, and SCED along with corresponding to subsections.

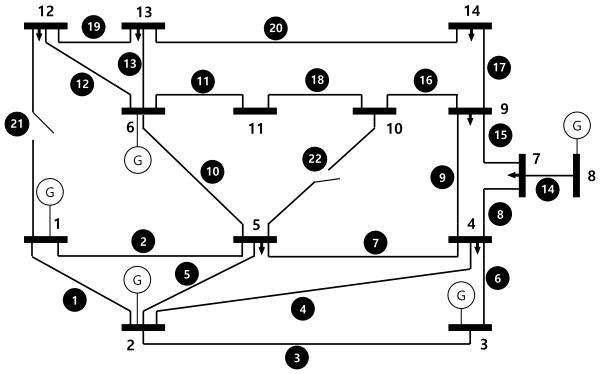


FIGURE 4. Modified IEEE 14-bus test system.

TABLE 1. Generator parameters in the IEEE 14-bus system.

Bus	$P_{g_i}^{\min}$(MW)	$P_{g_i}^{\max}$(MW)	a_i(\$/MWh)	b_i(\$/(MW)^{2}h)
1	0	180	25	0.03
2	0	300	30	0.01
3	0	210	20	0.02
6	0	250	35	0.01
8	0	160	35	0.015

IV. NUMERICAL EXAMPLE

In this section, we investigate the performance of the proposed attack and evaluate the economic impact of such attack on real-time LMP in IEEE 14-bus system, shown in Fig. 4. For the illustration of line-adding topology data attack, the IEEE 14-bus system is slightly modified with additional lines 21 and 22. System data for the modified IEEE 14-bus system are taken from MATPOWER 4.0 IEEE 14-bus test case file and provided in Appendix. For all lines, capacity limits of all power flows are set to 200 MW. We assume that all measurements have been complete; real power injection P_i^m and flow measurement F_l^m are assigned to each bus i and the one end of each line l. We assume that all the real power flow and injection measurements are corrupted by additive Gaussian noises with equal variances $\sigma^2 = 0.0001$. The measurement redundancy (i.e., the ratio of the number of measurements to the number of state variables) is 36/13. For BDD, the threshold η of the Chi-squares test with a 95% confidence level is set to 35.17. Numerical testing is performed with the optimization toolbox in MATLAB R2015b (IntelCore i5 CPU clocking at 3.50 GHz, with 4 GB of RAM). Table 1 shows the generator parameters in the IEEE 14-bus system where a_i and b_i are linear and quadratic cost coefficients for generator i.

The test scenarios for the proposed attack I and attack II are categorized into two groups, corresponding to three different cases in each group, as follows:

(G1) Cases 1, 2, and 3 (Attack I)
(G2) Cases 4, 5, and 6 (Attack II)

Case 1 and Case 4 are base cases in each group where the attack becomes more severe due to an increasing number of manipulated contingency pairs from Case 1 to Case 3 in (G1) and from Case 4 to Case 6 in (G2). Table 2 shows a list of normal contingency pairs $(u, k) \in \mathcal{CP}$, which are calculated according to the CA procedure in Fig. 2 in subsection II-B. In our simulation, those contingency pairs are fed to the SCED module of which lines 5 and 13 associated with $\mathcal{CP}_1$ and $\mathcal{CP}_4$ are binding at their flow limits. Along with the results from Table 2, the aforementioned line binding status provides a performance benchmark to compare the performance of the proposed attacks.

TABLE 2. A list of contingency pairs without attack.

Type of $\mathcal{CP}$	Overload Line (u)	Outage Line (k)
$\mathcal{CP}_1$	5	2
$\mathcal{CP}_2$	8	15
$\mathcal{CP}_3$	12	13
$\mathcal{CP}_4$	13	12
$\mathcal{CP}_5$	13	19
$\mathcal{CP}_6$	15	8
$\mathcal{CP}_7$	19	13

A. PERFORMANCE AND ECONOMIC IMPACT OF ATTACK I

In this subsection, Cases 1, 2, and 3 correspond to the attack I method with which the adversary stealthily drops targeted contingency pairs from the normal contingency list in Table 2. Table 3 summarizes the performance of attack I for the three cases. The second row of Table 3 provides targeted contingency pairs to be dropped from the contingency table. The manipulated analog and digital SCADA measurements that yield incorrect SE solution are shown in the third row of Table 3. The fourth and fifth rows reveal abnormal contingency pairs and binding condition due to malfunction of CA and SCED, respectively. The last row of Table 3 reveals the attack effort that is a maximum number of compromised sensors. We can observe from this table that as the number of compromised sensors increases for dropping more contingency pairs from Case 1 to Case 3, CA yields a decreasing number of contingency pairs, leading to a decreasing number of binding flow constraints in SCED. This observation implies that through the drop of more contingency pairs the adversary could mislead system operators into believing the current system operating conditions are more secure physically and economically even though they are actually insecure.

Fig. 5 shows the comparison of the LMPs between without attack and with attack in Cases 1, 2, and 3. In case of without attack, we observe that LMPs at buses that are connected to lines of binding contingency pairs reveal a relatively larger price gap with each other. For example, in the two binding contingency pairs, $\mathcal{CP}_1$ and $\mathcal{CP}_4$, buses 1, 2, and 5 are connected to the ends of lines 2 and 5 belonging to $\mathcal{CP}_1$, and buses 6, 12, and 13 to the ends of lines 12 and 13 belonging to $\mathcal{CP}_4$. We can observe from Fig. 5 that LMPs at buses 5, 12, and 13 (power import region) become maximum whereas LMPs at buses 1, 2, and 6 (power export region) become minimum. This observation holds true in Cases 1, 2, and 3 as well.

TABLE 3. Performance of attack I for cases 1,2, and 3.

	Case 1	Case 2	Case 3
Attack Target (Dropped Contingency Pairs)	$\mathcal{CP}_1$	$\mathcal{CP}_1, \mathcal{CP}_2$	$\mathcal{CP}_1, \mathcal{CP}_2, \mathcal{CP}_3$
Manipulated Measurements (SCADA, SE)	$P_1^m, P_{12}^m, F_{21}^m$ (Line 21 add)	Case 1+ $P_4^m, P_7^m, P_9^m, F_8^m, F_{15}^m$	Case 2+ $P_6^m, P_{13}^m, F_{13}^m$ (Line 13 remove)
Contingency Pairs (CA)	$\mathcal{CP}_2, \mathcal{CP}_3, \mathcal{CP}_5, \mathcal{CP}_6, \mathcal{CP}_7$	$\mathcal{CP}_3, \mathcal{CP}_5, \mathcal{CP}_7$	-
Binding Condition (SCED)	$\mathcal{CP}_2, \mathcal{CP}_6, F_5^{\max}$	$F_5^{\max}$	-
Attack Effort	4	9	13

TABLE 4. Performance of attack II for cases 4, 5, and 6.

	Case 4	Case 5	Case 6
Attack Target (Added Contingency Pairs)	$\mathcal{CP}_8$	$\mathcal{CP}_8, \mathcal{CP}_{11}$	$\mathcal{CP}_8, \mathcal{CP}_{11}, \mathcal{CP}_{13}$
Manipulated Measurements (SCADA, SE)	P_4^m, P_5^m, F_7^m (Line 7 remove)	Case 4+ $P_2^m, P_3^m, F_3^m, F_6^m$	Case 5+ $P_9^m, P_{13}^m, P_{14}^m, F_{17}^m, F_{20}^m$
Contingency Pairs (CA)	$\mathcal{CP}_1 \sim \mathcal{CP}_{10}$	$\mathcal{CP}_1 \sim \mathcal{CP}_{12}$	$\mathcal{CP}_1 \sim \mathcal{CP}_{15}$
Binding Condition (SCED)	$\mathcal{CP}_1, \mathcal{CP}_4$	$\mathcal{CP}_1, \mathcal{CP}_4, \mathcal{CP}_{11}, \mathcal{CP}_{12}$	$\mathcal{CP}_1, \mathcal{CP}_4, \mathcal{CP}_{11}, \mathcal{CP}_{12}, \mathcal{CP}_{13}, \mathcal{CP}_{14}$
Attack Effort	4	8	13

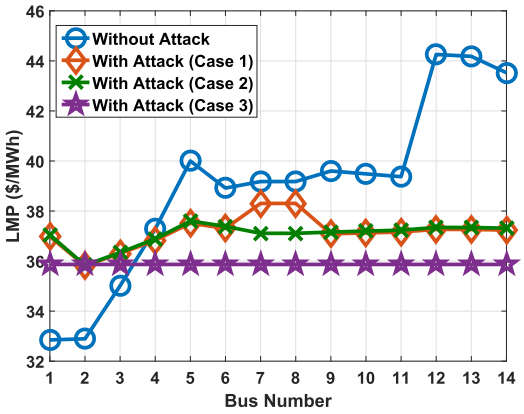


FIGURE 5. LMP of SCED without and with attack I (Cases 1, 2, and 3).

In Case 1, buses 4, 7, and 9, and buses 2, 5 are connected to the end of lines belonging to the binding $\mathcal{CP}_2$ and $\mathcal{CP}_6$, and to the end of line belonging to network flow F_5. As expected, bus 7 at power import region and bus 2 at power export region have maximum and minimum values of LMP, respectively. Another observation is that Case 1 attack results in almost uniform LMPs at buses 6, 12, and 13 compared to the LMPs without attack. This result derives from the fact that binding $\mathcal{CP}_4$ corresponding to lines 12 and 13 is dropped from normal contingency list by the adversary and hence there is no network flow congestion at lines 12 and 13. In addition, buses 1 and 12 show the largest price gap between with and without attack. It is noted that those buses are connected to the ends of line 21, which is added by the adversary while being undetected by BDD. We can conjecture from this observation that network topology change has a significantly detrimental impact on the calculation of LMP.

In Case 2, the adversary drops more contingency pairs than in Case 1, consequently leading to only a binding flow constraint at $F_5^{\max}$. As a result, LMPs at buses 7 and 8 in Case 2 become less and uniform than in Case 1. This is because those buses are connected to the ends of lines belonging to dropped $\mathcal{CP}_2$ and $\mathcal{CP}_6$. Conversely, the highest and the lowest price are obtained at buses 5 and 2, corresponding to binding flow constraint at $F_5^{\max}$.

Finally, in Case 3 the adversary drops all contingency pairs, and all security and network flow constraints become unbinding in SCED. Due to no line congestion, prices in Fig. 5 denote uniform LMPs for all buses. It should be noted that Case 3 includes line-deleting attack. Unlike expectation that line-deleting attack increases the list of contingency pairs by making system operating condition become more insecure, our simulation result shows that the coordinated topology data attack through deletion and addition of lines decreases the list of contingency pairs, subsequently leading to less binding constraints at SCED.

B. PERFORMANCE AND ECONOMIC IMPACT OF ATTACK II

In this subsection, the performance of attack II is assessed in Cases 4, 5, and 6 where the adversary stealthily adds the targeted contingency pairs to the normal contingency list in Table 2. Table 4 shows the performance of attack II for these three cases. The targeted contingency pairs ($\mathcal{CP}_8 \sim \mathcal{CP}_{15}$) that are added to the normal contingency list are shown in Table 5.

We observe from Table 4 that the number of contingency pairs (the fourth row) from CA and the number of the binding flow constraints (the fifth row) from SCED increase as long as attack effort (the sixth row) increases with an increasing number of the manipulated data (the third row) to enlarge the contingency table (the second row). Different from attack I including line-adding attack, all three cases in attack II include line-deleting attack where line 7 is removed after the attack. We can conclude from the results in Table 4 that line-deleting attack causes CA to calculate a more number of contingency pairs, consequently resulting in more

TABLE 5. Candidate contingency list for attack II.

Type of $\mathcal{CP}$	Overload Line (u)	Outage Line (k)
$\mathcal{CP}_8$	6	4
$\mathcal{CP}_9$	2	5
$\mathcal{CP}_{10}$	4	5
$\mathcal{CP}_{11}$	6	3
$\mathcal{CP}_{12}$	3	6
$\mathcal{CP}_{13}$	20	11
$\mathcal{CP}_{14}$	20	16
$\mathcal{CP}_{15}$	20	18

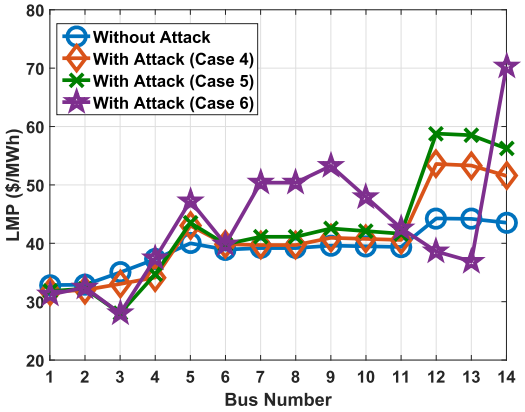


FIGURE 6. LMP of SCED without and with attack II (Cases 4, 5, and 6).

binding flow constraints in SCED. Therefore, the adversary using the attack II strategy could mislead system operators to make a wrong decision that the current system operating condition appears to becomes more insecure physically and economically.

Fig. 6 shows the comparison of the LMPs between without attack and with attack in Cases 4, 5, and 6. Compared to the results in Fig. 5 for attack I, it is observed from Fig. 6 that attack II yields more fluctuating prices at all buses. This observation results from the fact that the increase of the number of contingency pairs due to the malfunction of CA leads to the increase of the number of the binding flow constraints in SCED, consequently resulting in a larger gap between LMPs. Like the result from attack I, bus with maximum or minimum LMP due to attack II is in the ends of binding contingency pairs. For Cases 4, 5, and 6, pair of buses with the maximum and minimum LMP is summarized as follows: {bus 12 $\in \mathcal{CP}_4$, bus 1 $\in \mathcal{CP}_1$} in Case 4, {bus 12 $\in \mathcal{CP}_4$, bus 3 $\in \mathcal{CP}_{11}$} in Case 5 , and {bus 14 $\in \mathcal{CP}_{13}$, bus 3 $\in \mathcal{CP}_{11}$} in Case 6.

Fig. 7 compares the average of LMP differences at all buses between with and without attack and the attack efforts for all six cases. We first observe from this figure that attack I (Cases 1, 2, and 3) and attack II (Cases 4, 5, and 6) distort prices more significantly as the adversary compromises more sensors. Another observation is that as the attack effort in each attack strategy increases, attack I leads to negative LMP deviation from LMP without attack, whereas attack II to a positive LMP deviation. This observation is due to the

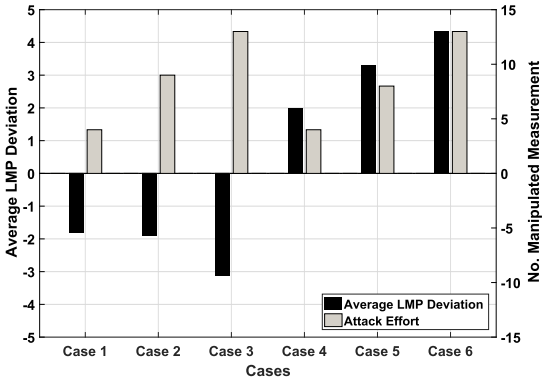


FIGURE 7. Average LMP deviation and attack effort for attack I (Cases 1, 2, and 3) and attack II (Cases 4, 5, and 6).

fact that the adversary using the attack I strategy reduces the number of contingency pairs from CA and binding flow constraints of SCED, consequently causing the network flow become less congested with lower as well as less fluctuating LMPs on average than without attack. Conversely, attack II causes network flow to become more congested and yields higher as well as more fluctuating LMPs on average than without attack.

TABLE 6. Comparison of attack performance between with and without constraints (32), (33).

Attack Target	Attack Method	Attack Effort	No. CPs After Attack	Extra Manipulated CPs
Drop of $\mathcal{CP}_3$	Attack I	4	3	$\mathcal{CP}_4, \mathcal{CP}_5, \mathcal{CP}_7$
	Attack I with (32)	5	6	-
Add of $\mathcal{CP}_{13}$	Attack II	5	10	$\mathcal{CP}_{14}, \mathcal{CP}_{15}$
	Attack II with (33)	7	8	-

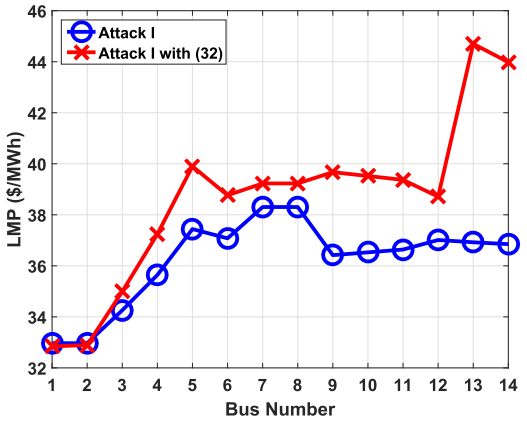
* CPs: Contingency pairs

On the other hand, the proposed attacks I and II in subsections III-B and III-C could manipulate not only targeted contingency pairs but also additional undesirable contingency pairs. For example, Case 1 and Case 4 attacks aim to drop $\mathcal{CP}_1$ and add $\mathcal{CP}_8$ from and to a contingency list, respectively. However, the results from Tables 3 and 4 show that $\mathcal{CP}_4$ in addition to $\mathcal{CP}_1$ is dropped in Case 1, and $\mathcal{CP}_9$ and $\mathcal{CP}_{10}$ in addition to $\mathcal{CP}_8$ are added. To guarantee that only targeted contingency pairs are manipulated, the following attack constraints can be added to the proposed optimization formulation for attacks I and II:

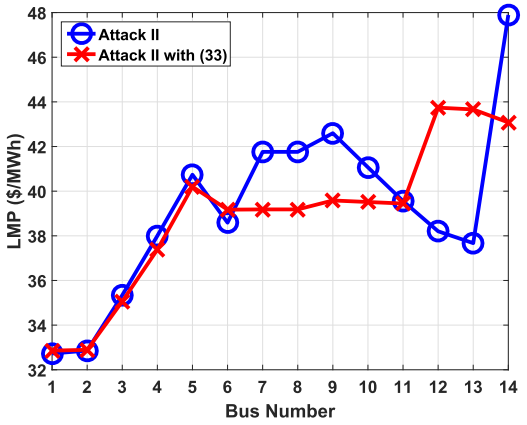
$$\text{Attack I}: \ |\widetilde{F}^a_{u,ex}| \geq F^{\max}_u, \quad (u, ex) \in \mathcal{CP}, \ ex \neq t \tag{32}$$

$$\text{Attack II}: \ |\widetilde{F}^a_{u,\overline{ex}}| \leq F^{\max}_u. \quad (u, \overline{ex}) \in \overline{\mathcal{CP}}, \ \overline{ex} \neq t \tag{33}$$

where the subscripts ex and $\overline{ex}$ represent the indices of untargeted lines in the contingency list and the non-contingency list, respectively. Table 6 shows the impact of two constraints (32) and (33) on the performance of the proposed attacks when $\mathcal{CP}_3$ and $\mathcal{CP}_{13}$ are dropped and added by the attacker, respectively. It is noted that the last column



(a)



(b)

FIGURE 8. Comparison of LMP between the proposed attack and the proposed attack with: (a) constraint (32) for $\mathcal{CP}_3$ drop and (b) constraint (33) for $\mathcal{CP}_{13}$ addition.

of Table 6 indicates contingency pairs that are untargeted, however additionally dropped or added by the attack. We can observe from this table that the attack method with (32) or (33) requires more attack effort while the attacker manipulates only targeted contingency pair successfully. Figs. 8 show the comparison of the LMPs between the proposed attack and the proposed attack with constraints (32) and (33). We can observe from these figures that an increasing number of contingency pairs due to attack leads to higher LMPs with more fluctuating prices at all buses. This observation is also verified in Fig. 5 and Fig. 6. Therefore, we conclude that more (less) contingency pairs due to the attack has more (less) detrimental impact on the prices.

Finally, the meaningful observations from simulation studies of the proposed attack I and II can be summarized as follows.

1) In attack I and II, the adversary could stealthily distort the list of normal contingency pairs more severely at the cost of more manipulated sensor measurements. In general, the adversary using the strategy of attack I (attack II) executes the line-adding (deleting) attack to drop (add) targeted contingency pairs from (to) the normal contingency list. In addition to a simple topology data attack, a coordinated attack that consists in line-adding and line-deleting attacks can be conducted to aggravate the result of CA more as shown in Case 3.
2) Given tight coupling between CA and SCED, the manipulated contingency list due to the proposed attacks leads to an incorrect calculation of LMP from SCED. A significant distortion of LMP is observed at buses that are connected to the end of changed security constraint lines due to manipulated contingency pairs and the attacked topology line. Furthermore, attack I (attack II) decreases (increases) the average of LMPs for all the buses with less (more) fluctuating LMPs. Therefore, attack I and II could provide consumers and generation companies with additional profit, respectively.

V. CONCLUSIONS

In this paper, we have proposed novel false data injection attacks on contingency analysis in real-time power system operations. We have formulated an undetectable least-effort attack as an optimization problem where the adversary could manipulate a number of contingency pairs obtained from contingency analysis by distorting the state estimation solution through injecting malicious data into SCADA measurements. Furthermore, we have assessed the economic impact of the proposed attacks on electricity prices that are calculated by security constrained economic dispatch in real-time power markets. This is the first study to characterize cyber data attacks against contingency analysis and investigate the vulnerability of real-time electricity prices to such attacks.

In future studies, a broader range of cyber data attack methods will be developed in large-scale realistic power systems considering more practical applications in energy management system, such as AC state estimation and dynamic contingency analysis. Another interesting future study is to present a profitable attack strategy with which the adversary makes a financial gain through the malfunction of contingency analysis.

APPENDIX
DATA FOR IEEE 14-BUS TEST SYSTEM

Simulation data for the test system are provided in Tables 7 and 8.

TABLE 7. Line data.

Line #	From To	X_{ij} [p.u.]	Line #	From To	X_{ij} [p.u.]
1	1-2	0.0592	12	5-12	0.2558
2	1-5	0.2230	13	6-13	0.1303
3	2-3	0.1980	14	7-8	0.1762
4	2-4	0.1763	15	7-9	0.11
5	2-5	0.1739	16	9-10	0.0845
6	3-4	0.1710	17	9-14	0.2704
7	4-5	0.0421	18	10-11	0.1921
8	4-7	0.2091	19	12-13	0.1999
9	4-9	0.5562	20	13-14	0.9480
10	5-6	0.2520	21	1-12	0.3612
11	6-11	0.1989	22	5-10	0.2985

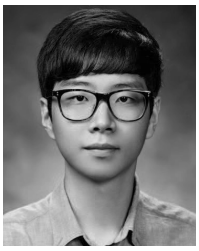
TABLE 8. Data for generator and load without attack.

Bus #	P_{g_i} [MW]	L_{d_i} [MW]	Bus #	P_{g_i} [MW]	L_{d_i} [MW]
1	189	-	8	107	-
2	104	-	9	-	131
3	201	-	10	-	-
4	-	148	11	-	-
5	-	45	12	-	44
6	226	-	13	-	57
7	-	310	14	-	130

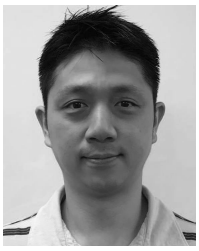
REFERENCES

[1] B. Stott, O. Alsac, and A. J. Monticelli, "Security analysis and optimization," *Proc. IEEE*, vol. 75, no. 12, pp. 1623–1644, Dec. 1987.
[2] NCCIC/ICS-CERT. *Cyber-Attack Against Ukrainian Critical Infrastructure*. Accessed: May 10, 2016. [Online]. Available: https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01
[3] A. Ashok, M. Govindarasu, and J. Wang, "Cyber-physical attack-resilient wide-area monitoring, protection, and control for the power grid," *Proc. IEEE*, vol. 105, no. 7, pp. 1389–1407, Jul. 2017.
[4] F. C. Schweppe and J. Wildes, "Power system static-state estimation—Part I: Exact model," *IEEE Trans. Power App. Syst.*, vol. PAS-89, no. 1, pp. 120–135, Jan. 1970.
[5] A. J. Wood, B. F. Wollenberg, and G. B. Sheblé, *Power Generation, Operation, and Control*. New York, NY, USA: Wiley, 2014.
[6] K. E. Van Horn, A. D. Domínguez-García, and P. W. Sauer, "Measurement-based real-time security-constrained economic dispatch," *IEEE Trans. Power Syst.*, vol. 31, no. 5, pp. 3548–3560, Sep. 2016.
[7] 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. Secur.*, Nov. 2009, pp. 21–32.
[8] 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.
[9] X. Liu and Z. Li, "False data attacks against AC state estimation with incomplete network information," *IEEE Trans. Smart Grid.*, vol. 8, no. 5, pp. 2239–2248, Sep. 2017.
[10] J. Liang, L. Sankar, and O. Kosut, "Vulnerability analysis and consequences of false data injection attack on power system state estimation," *IEEE Trans. Power Syst.*, vol. 31, no. 5, pp. 3864–3872, Sep. 2016.
[11] 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.
[12] X. Liu, Z. Li, X. Liu, and Z. Li, "Masking transmission line outages via false data injection attacks," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 7, pp. 1592–1602, Jul. 2016.
[13] X. Liu and Z. Li, "Local topology attacks in smart grids," *IEEE Trans. Smart Grid.*, vol. 8, no. 6, pp. 2617–2626, Nov. 2017.
[14] 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.*, to be published.
[15] J. Zhang and L. Sankar, "Physical system consequences of unobservable state-and-topology cyber-physical attacks," *IEEE Trans. Smart Grid.*, vol. 7, no. 4, pp. 2016–2025, Jul. 2016.
[16] S. Wang, W. Ren, and U. M. Al-Saggafi, "Effects of switching network topologies on stealthy false data injection attacks against state estimation in power networks," *IEEE Syst. J.*, vol. 11, no. 4, pp. 2640–2651, Dec. 2017.
[17] Z. H. Yu and W. L. Chin, "Blind false data injection attack using PCA approximation method in smart grid," *IEEE Trans. Smart Grid*, vol. 6, no. 3, pp. 1219–1226, May 2015.
[18] J. Zhao, G. Zhang, J. Y. Dong, and K. P. W. Davoudi, "Forecasting-aided imperfect false data injection attacks against power system nonlinear state estimation," *IEEE Trans. Smart Grid.*, vol. 7, no. 1, pp. 6–8, Jan. 2016.
[19] R. Tan *et al.*, "Modeling and mitigating impact of false data injection attacks on automatic generation control," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 7, pp. 1609–1624, Jul. 2017.
[20] 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.
[21] 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.
[22] 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.
[23] 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, Feb. 2017.
[24] R. Xu, Z. Guan, L. Wu, J. Wu, and X. Du, "Achieving efficient detection against false data injection attacks in smart grid," *IEEE Access.*, vol. 5, pp. 13787–13798, 2017.
[25] O. A. Beg, T. T. Johnson, and A. Davoudi, "Detection of false-data injection attacks in cyber-physical dc microgrids," *IEEE Trans. Ind Informat.*, vol. 13, no. 5, pp. 2693–2703, Oct. 2017.
[26] J. Zhao, G. Zhang, M. La Scala, Z. Y. Dong, C. Chen, and J. Wang, "Short-term state forecasting-aided method for detection of smart grid general false data injection attacks," *IEEE Trans. Smart Grid*, vol. 8, no. 4, pp. 1580–1590, Jul. 2017.
[27] S. Li, Y. Yilmaz, and X. Wang, "Quickest detection of false data injection attack in wide-area smart grids," *IEEE Trans. Smart Grid*, vol. 6, no. 6, pp. 2725–2735, Nov. 2015.
[28] Y. He, G. J. Mendis, and J. Wei, "Real-time detection of false data injection attacks in smart grid: A deep learning-based intelligent mechanism," *IEEE Trans. Smart Grid.*, vol. 8, no. 5, pp. 2505–2516, Sep. 2017.
[29] M. Ozay, I. Esnaola, F. T. Y. Vural, S. R. Kulkarni, and H. V. Poor, "Machine learning methods for attack detection in the smart grid," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 27, no. 8, pp. 1773–1786, Aug. 2016.
[30] U. Adhikari, T. H. Morris, and S. Pan, "Applying non-nested generalized exemplars classification for cyber-power event and intrusion detection," *IEEE Trans. Smart Grid*, to be published.
[31] 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.
[32] R. Deng, G. Xiao, R. Lu, H. Liang, and A. V. Vasilakos, "False data injection on state estimation in power systems—Attacks, impacts, and defense: A survey," *IEEE Trans. Ind. Informat.*, vol. 13, no. 2, pp. 411–423, Apr. 2017.
[33] J. Chen *et al.*, "Impact analysis of false data injection attacks on power system static security assessment," *J. Mod. Power Syst. Clean Energy*, vol. 4, no. 3, pp. 496–505, Jun. 2016.
[34] S. Vemuri and R. E. Usher, "On-line automatic contingency selection algorithms," *IEEE Trans. Power App. Syst.*, vol. PAS-102, no. 2, pp. 346–3543, Feb. 1983.
[35] G. C. Ejebe and B. F. Wollenberg, "Automatic contingency selection," *IEEE Trans. Power App. Syst.*, vol. PAS-98, no. 1, pp. 97–109, Jan. 1979.
[36] G. Irisarri, A. M. Sasson, and D. Levner, "Automatic contingency selection for on-line security analysis—Real-time tests," *IEEE Trans. Power App. Syst.*, vol. PAS-98, no. 5, pp. 1552–1559, Oct. 1979.
[37] N. Balu *et al.*, "On-line power system security analysis," *Proc. IEEE*, vol. 80, no. 2, pp. 262–280, Feb. 1992.
[38] Y. Yang, X. Guan, and Q. Zhai, "Fast grid security assessment with $N-k$ contingencies," *IEEE Trans. Power Syst.*, vol. 32, no. 3, pp. 2193–2203, May 2017.

JEONG-WON KANG (S'17) received the B.S. degree in electrical and electronics engineering from Chung-Ang University, Seoul, South Korea, in 2015, where he is currently pursuing the M.S. degree. His current research interest includes power system state estimation and cybersecurity of smart grid.



IL-YOUNG JOO (S'17) received the B.S. degree in electrical and electronics engineering from Chung-Ang University, Seoul, South Korea, in 2015, where he is currently pursuing the M.S. degree. His current research interests include home energy management systems.



Dae-Hyun Choi (S'10–M'17) 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. From 2002 to 2006, he was a researcher with Korea Telecom, Seoul, where he was involved in designing and implementing home network systems. From 2014 to 2015, he was a Senior Researcher with LG Electronics, Seoul, where he developed home energy management systems. He is currently an Assistant Professor with the School of Electrical and Electronics Engineering, Chung-Ang University, Seoul, South Korea. 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. He received the Best Paper Award from the 2012 IEEE Third International Conference on Smart Grid Communications, Tainan City, Taiwan.