Local Cyber-Physical Attack for Masking Line Outage and Topology Attack in Smart Grid

Hwei-Ming Chung, *Student Member, IEEE*, Wen-Tai Li, *Member, IEEE*, Chau Yuen, *Senior Member, IEEE*, Wei-Ho Chung, *Member, IEEE*, Yan Zhang, *Senior Member, IEEE*, and Chao-Kai Wen, *Member, IEEE*

***Abstract*—Malicious attacks in the power system can eventually result in a large-scale cascade failure if not attended on time. These attacks, which are traditionally classified into *physical* and *cyber attacks*, can be avoided by using the latest and advanced detection mechanisms. However, a new threat called *cyber-physical attacks* which jointly target both the physical and cyber layers of the system to interfere the operations of the power grid is more malicious as compared with the traditional attacks. In this paper, we propose a new cyber-physical attack strategy where the transmission line is first physically disconnected, and then the line-outage event is masked, such that the control center is misled into detecting as an obvious line outage at a different position in the local area of the power system. Therefore, the topology information in the control center is interfered by our attack. We also propose a novel procedure for selecting vulnerable lines, and analyze the observability of our proposed framework. Our proposed method can effectively and continuously deceive the control center into detecting fake line-outage positions, and thereby increase the chance of cascade failure because the attention is given to the fake outage. The simulation results validate the efficiency of our proposed attack strategy.**

***Index terms*– Cyber-physical system, joint attacks, smart grid, power line outages, power flow.**

NOMENCLATURE

A. Sets and Indices

j, k	Bus index.
l	Line index.
n_b	Total bus number in the system.
n_{br}	Total line number in the system.
i	Represent $\sqrt{-1}$.
$\mathcal{G}$	Graph representing the topology of the system.
$\mathcal{N}$	Sets of the buses in the system.
$\mathcal{E}$	Sets of the lines in the system.
$\mathcal{L}$	Sets of the buses connected to real line outage position.
$\mathcal{M}$	Sets of the buses connected to fake line outage position.
$\mathcal{B}$	Set of boundary buses in the attack region.
$\mathcal{A}$	Set of buses except boundary buses in the attack region.
ϕ	Empty set.

B. Variables

$\mathbf{z}(\bar{\mathbf{z}})$	Measurement vector before (after) attack.
S_l	Complex power flow on line l. Equal to $P_l + iQ_l$.
$\overline{S}_l$	Modified complex power flow on line l. Equal to $\overline{P}_l + i\overline{Q}_l$.
l_o	Real outage line.
l_m	Fake outage line.
v_j	Complex voltage of bus j.
V_j	Voltage magnitude of bus j.
W_j	Squared voltage magnitude of bus j.
C_l	Squared current magnitude of line l.
θ_j	Voltage phase of bus j.
$P_j^D(\overline{P}_j^D)$	Real load of bus j before (after) attack.
$\overline{Q}_j^D$	Reactive load of bus j after attack.

C. Parameters

P_e	Parameter error vector of the system.
$\mathbf{R}$	Measurement error covariance matrix.
Y_l	Admittance of line l. Equal to $G_l + iB_l$.
Z_l	Impedance of line l.
$\mathbf{L}$	Line outage distribution factors matrix.
f_l	Influence factor of line l.
P_l^{max}	The thermal limit of line l.
V_{max}	Maximum voltage magnitude.
V_{min}	Minimum voltage magnitude.

D. Operators

$\lvert A \rvert$	Cardinality of set A.
$\mathbf{a} \cdot \mathbf{b}$	Element-wise multiplication of vector a and b.
$\Re(a)$	Real part of complex value a.

Other notations are defined in the text.

I. INTRODUCTION

A Power system plays an important role in supporting modern lives and economy. Upon a late detection, the initial

This work was partially supported by the "Center for mmWave Smart Radar Systems and Technologies under the Featured Areas Research Center Program within the framework of the Higher Education Sprout Project by the Ministry of Education, and partially supported under Ministry of Science and Technology 107-3017-F-009-001, 104-2221-E-007-147-MY3, 105-2221-E-007-144-MY3, and Digital Economy Advancement Project 106-2218-E-002-014-MY4, in Taiwan. Also, the work of W.-T. Li and C. Yuen was supported by the project under Grant NSFC 61750110529.

H.-M. Chung was with Singapore University of Technology and Design, Singapore. He and Y. Zhang are with Department of Informatics, University of Oslo, Oslo 0373, Norway, (e-mail: hweiminc@ifi.uio.no, yanzhang@ieee.org).

W.-T. Li and C. Yuen are with the Singapore University of Technology and Design, Singapore 487372 (e-mail: {wentai_li, yuenchau}@sutd.edu.sg).

W.-H. Chung (corresponding author) is with the Department of Electrical Engineering, National Tsing Hua University, and Center for mmWave Smart Radar Systems and Technologies, National Chiao Tung University, HsinChu City 300, Taiwan (e-mail: whchung@ee.nthu.edu.tw).

C.-K. Wen is with the Institute of Communications Engineering, National Sun Yat-sen University, Kaohsiung 804, Taiwan (e-mail: chaokai.wen@mail.nsysu.edu.tw).

failures in a power system, may lead to a large-scale cascade failure, and adversely affect the economy and security of a nation [1]. Malicious attacks on a power system can lead to an initially undetectable failure and eventually result in failure if not attended in time. These attacks can be classified into *cyber* and *physical attacks*. For *physical attacks*, [2], [3] proposed a target selection methods that allow the terrorists to physically attack the power system components (e.g., transmission lines, generators, and transformers), cause a direct power system outage, and triggers cascading failures, e.g. [4] explored the attacks on the transmission substations in California in 2014. However, with the aid of recent technological advancements, power system operators are able to detect these attacks easily and prevent a system failure.

Given that *physical attacks* are easily observable, attackers have resorted to *cyber attacks* where they inject carefully predesigned data to the measurements sent by Supervisory Control and Data Acquisition (SCADA), thereby forcing power system operators into making wrong dispatches. Although various data processing modules, such as state estimation (SE) and bad data detection, have been built to prevent system operation failures and malicious attacks, these mechanisms can be corrupted by carefully designed cyber attacks. Accordingly, this topic has attracted much research attention over the past few years [5]–[21].

The authors in [5] proposed classic false data injection (FDI) attacks that cannot be detected by bad data detection techniques and where the attacker can change the measurements of sensors and capture sufficient information about the power system. These designed attacks must obey the physical laws, such as Kirchhoff's Current Law, and Kirchhoff's Voltage Law. The authors in [6] and [7] studied classic FDI attacks with incomplete information about the system, and [6], [7] revealed that cyber attacks can bypass SE and bad data detection techniques even if limited network information is available. Furthermore, the authors attempted to construct the cyber attack by using principal component analysis without prior information as those in [8]. Then, recent development of FDI attacks was summarized in [9].

By targeting both the cyber and physical levels of a power system, the recently emerged *cyber-physical attacks* can interfere with the operations of the system more efficiently than the classic FDI attacks with only pure *cyber attacks*. *Cyber-physical attacks* can still be classified into line-removing and line-maintaining attacks as described in [10].

In a line-maintaining attack, the attacker physically disconnects the transmission line and simultaneously masks this outage event with altered sensor measurements. Other forms of advanced line-maintaining attacks have been studied in [11]–[18]. Specifically, the authors in [11], [12] masked the outage event with a local redistribution attack that was extended to a local attack with incomplete topology information. A line-maintaining attack was recently launched at the Ukrainian electrical grid in 2015 [13], where the physical components of the system were disconnected and the SCADA system was illegally attacked by a third party. Such attack left $225,000$ customers without power. The attack was designed based on finding out the line that can cause the most damaging to the system in [14]. Then, the authors in [15], [16] attempted to modify the PMU data to mask the outage event. The attack model was further derived using the power flow method [17] and SE [18].

Meanwhile in a line-removing attack, also called topology attacks, the attacker generates a fake outage event to disturb the regular system operation. This attack must avoid the trivial solution in order not to be detected by the control center. Using this approach, the attacker can efficiently mislead the control center with an incorrect network topology and then lead the system to an unstable situation by sending the wrong dispatches. Line-removing attacks have been studied with both partial and whole information of the system and have been mitigated using countermeasure [19], [20]. The authors in [21] focused on a line-removing attack in a local area and proposed a method for locating the attack region.

Based on the discussions above, the previous approaches have obtained the promising results and demonstrated the potential of the *cyber-physical attacks*. However, most of these approaches were based on DC model, which is different from the real-world system; also, false data constructed by DC model may cause large residual in AC state estimation [22]. Only few studies, such as [17], [18], [23], proposed the construction of the attack in AC system. However, in [17], [18], they still constructed the attack with DC model first and then transformed to AC system. Then, in [23], it focused more on vulnerability assessment of AC state estimation under cyber-attack. Moreover, there existed no study that combined line-maintaining and line-removing attacks to create more malicious attack to the power system. Also, when implementing the *cyber-physical attacks*, one must notice that not all transmission lines in the power system can be selected as attack targets because some lines are strictly protected by the control center. Only few studies, such as [10], considered the rules of selection.

Motivated by the above observations, we develop a novel attack strategy that combines the line-removing and line-maintaining attack strategies in the AC system. The attack is implemented in the local area and cannot be easily detected because our design ensures that the physical laws of the power system are satisfied. Unlike previous studies, we propose a rule for selecting target lines instead of randomly selecting such lines. We also use the traditional SE method that combines normalized Lagrange multipliers and measurement residuals [24]–[26] to test the effectiveness of our proposed attack strategy. The contributions of this study are summarized as follows:

- We propose a novel attack strategy with AC model, which aims to physically attack the transmission line and simultaneously mask the real outage event with the cyber attack by misleading the control center into checking another fake outage line. With this approach, the control center cannot obtain the accurate information about the topology. Therefore, the control center needs to develop another method of detecting the system topology.
- Instead of randomly selecting target lines, we design a target line selection rule based on line outage distribution factor (LODF). According to the simulation, the proposed

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2018.2865316, IEEE Transactions on Smart Grid

target line selection results in higher success rate and no false alarm, which is better than random target line selection. This method can also help control center to identify the locations vulnerable to attacks as in [27], [28].

- We apply the conventional SE and bad data detection techniques to test the effectiveness of the proposed attack. The simulation results reveal that the control center detects the fake outage position and that the real outage event is successfully hidden. This highlights the need of developing another effective detection mechanism.

II. System Model

As shown in Fig. 1, the system considered in this study is divided into two parts, namely the SE and the cyber-physical attack model. We briefly illustrate the SE based on the AC power flow model and the basic calculation of the power system in this section. Then, our proposed attack strategy is introduced in the next section. The attack strategy must follow the physical laws introduced in this section.

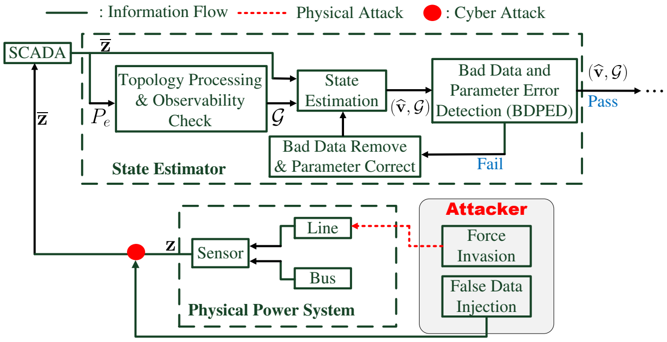

Fig. 1. The system block diagram.

A. Power Flow Model

We consider a power transmission network with n_b buses and n_{br} lines, and let $\mathcal{N}$ and $\mathcal{E}$ denote the sets of buses and lines, respectively. The power network can then be represented as a graph denoted as $\mathcal{G} = \{\mathcal{N}, \mathcal{E}\}$. Assuming a line $l \in \mathcal{E}$ that connects buses j and k, the apparent power of the line flowing from buses j to k denoted as S_l can be represented as follows:

$$S_l = Y_l^* |v_j|^2 - Y_l^* v_j v_k^*, \tag{1}$$

where Y_l is the admittance of line l, and v_j and v_k are the voltages of buses j and k respectively. The voltage of bus j can be represented in polar form as follows:

$$v_j = V_j e^{i\theta_j}, \tag{2}$$

where V_j is the voltage magnitude, θ_j is the corresponding phase, and i represents $\sqrt{-1}$. The vector of all power flows is $\mathbf{s} = [S_1 \cdots S_{n_{br}}] \in \mathbb{C}^{n_{br}\times 1}$, and the voltage of the buses is denoted as $\mathbf{v} = [v_1 \cdots v_{n_b}] \in \mathbb{C}^{n_b \times 1}$. The apparent power of line l, can be divided into real and reactive power, P_l and Q_l, which are

$$P_l = |V_j|^2 G_l - V_j V_k \left(G_l \cos(\theta_j - \theta_k) + B_l \sin(\theta_j - \theta_k)\right), \tag{3}$$

$$Q_l = -|V_j|^2 B_l - V_j V_k \left(G_l \sin(\theta_j - \theta_k) - B_l \cos(\theta_j - \theta_k)\right), \tag{4}$$

where $G_l + iB_l = Y_l$, and $S_l = P_l + iQ_l$.

B. State Estimation

Based on the power flow model, we then introduce the state estimator as shown in Fig. 1. The system states are represented by the voltage of the bus, $\mathbf{v}$. Therefore, the measurements received by the SCADA system without attacks can be expressed as follows:

$$\mathbf{z} = h(P_e, \mathcal{G}, \mathbf{v}) + \mathbf{n}, \tag{5}$$

where $\mathbf{z}$ usually comprises the measurements of bus injection power and line power flow, and $h(\cdot)$ is the nonlinear function relating to the measurements that depend on the network topology $\mathcal{G}$, network parameter error vector $P_e \in \mathbb{C}^{n_{br}\times 1}$ representing the parameter errors, and system state vector $\mathbf{v}$. The measurement errors are denoted as $\mathbf{n}$. We further denote the measurements modified by the attacker as $\overline{\mathbf{z}}$.

After obtaining the measurement expression, we adopt the weighted least-squares SE to estimate the system state $\mathbf{v}$. The SE problem aims to minimize the sum of squares of the weighted deviations of the measurements estimated from $\overline{\mathbf{z}}$. The SE problem is then solved by the following optimization problem where zero parameter errors are assumed:

$$\mathcal{F}1: \quad \min_{\widehat{\mathbf{v}}, P_e} \left(\overline{\mathbf{z}} - h\left(P_e, \mathcal{G}, \widehat{\mathbf{v}}\right)\right)^T \mathbf{R}^{-1} \left(\overline{\mathbf{z}} - h\left(P_e, \mathcal{G}, \widehat{\mathbf{v}}\right)\right) \tag{6a}$$

$$\text{s.t.} \quad P_e = 0, \tag{6b}$$

where $\widehat{\mathbf{v}}$ is the estimated system state vector, P_e is the parameter error vector, and $\mathbf{R}$ is the measurement error covariance matrix.

C. Bad Data and Parameter Error Detection

After applying SE, we must bypass bad data and parameter error detection to ensure that the measurements are free from bad data or parameter errors. Accordingly, we apply the normalized residual and Lagrange multiplier method for the detection.

The measurement residual vector can be expressed as:

$$\mathbf{r} = \overline{\mathbf{z}} - h(P_e, \mathcal{G}, \mathbf{v}). \tag{7}$$

If the Lagrange multiplier method is applied in (6), then $\boldsymbol{\lambda}$ denotes the Lagrange multiplier related to the parameter error. Given $\mathbf{r}$ and $\boldsymbol{\lambda}$, the normalized residual, $\mathbf{r}^N$, and normalized Lagrange multipliers, $\boldsymbol{\lambda}^N$, can be calculated. The normalized residuals are linked to the corresponding measurements, and the normalized Lagrange multipliers are related to the parameter. Further details about this procedure can be found in [24]–[26]. With $\mathbf{r}^N$ and $\boldsymbol{\lambda}^N$, the errors follow the Gaussian distributions, and we choose the largest value between these two parameters of the corresponding line. If the chosen value is below the identification threshold, then the measurements

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2018.2865316, IEEE Transactions on Smart Grid

are free from bad data or parameter errors. By contrast, the measurement or parameter corresponding to the chosen largest value will be identified as the error. The part corresponding to this error will be eliminated, and the detection mechanism is reapplied. Such procedure is performed recursively until no errors are detected.

III. Proposed Cyber Physical Attack Model

In this section, the attacker block in Fig. 1 is illustrated. We first explain the capabilities of the attackers and the limitations of selecting the target lines, and then introduce the components for launching the attacks separately, namely, selection of target lines, identification of the cyber attack region, and alteration of measurements. Here, the target lines include the real and the fake outage lines.

A. Introduction of the Attack

We assume that the attackers have the following capabilities:

1) the attacker has knowledge about the topology $\mathcal{G}$ of the entire system;
2) the attacker has the capability to observe the sub-network of $\mathcal{G}$ and perform the power flow calculation for the sub-network; and
3) the attacker only has the capability to change the states of the measurements in the sub-network rather than whole network.

To launch an attack, the attackers are limited to finite sets of target lines because of the following reasons:

1) the line that connects to a "three-winding transformer", or in between two generators cannot be physically attacked;
2) the real and fake outage events cannot take place next to each other; otherwise, the real outage position can be easily observed if the operator goes to repair the line at fake outage position. Here, the term "next to" means that real and fake outage lines have the same end bus. The mathematical expression can be expressed as
$$\mathcal{L} \cap \mathcal{M} \neq \phi; \tag{8}$$
3) the generator output cannot be modified;
4) the line injecting power to no-load bus cannot be selected because the load occurring in no load buses can be immediately detected by control center;
5) the load of the buses in the attack region cannot be modified to be negative. Moreover, the difference of the states and measurements before and after the attack must be controlled within a specified range; and
6) if the system is separated into two parts when a line is being attacked, then this line cannot be selected.

B. Real Outage Position Selection for the Physical Attack

When choosing the real outage line, we intend to know the system operation after the outage of a specific line; however, the attacker cannot run the power flow for the whole system. Therefore, instead of running optimal power flow problem, we employ the LODFs matrix, $\mathbf{L} \in \mathbb{R}^{n_{br} \times n_{br}}$, whose definition and calculation can be found in [29]. Specifically, we use the LODF matrix from the DC model to obtain approximate information of a target line if it has been disconnected, because the characteristic of the transmission system is sometimes close to the assumptions of the DC model. The entry in the m-th row and n-th column of $\mathbf{L}$, $l_{m,n}$, represents the fraction of the power flow of the n-th line that will be shifted to the m-th line when the n-th line faces an outage. By using the LODF matrix, we can define an influence factor, $\mathbf{f}$, whose l-th element can be represented as follows:

$$f_l = \Big(\big(L_{\{:,l\}}\big)^T \operatorname{sign}\left(\Re(\mathbf{s})\right) \Big) P_l, \tag{9}$$

where $L_{\{:,l\}}$ denotes the l-th column taken from $\mathbf{L}$, and $\operatorname{sign}\left(\Re(\mathbf{s})\right)$ denotes the sign of real power. The parameter f_l represents that the amount of the power flow increment for the whole system if the l-th line is disconnected. In this case, we can determine the real outage line as follows:

$$l_o = \underset{l}{\operatorname{argmax}} \left\{ f_l |\ l = 1, \ldots, n_{br} \right\}. \tag{10}$$

The l_o is the selected real outage position. Then, the buses connected by l_o are assigned to set $\mathcal{L}$.

C. Fake Outage Position Selection and Cyber Attack Region

After presenting the selection of the real outage position, we then illustrate the method of choosing the fake outage position without considering the selection of real outage position. More clearly, in the part, we assume all the lines remain closed in the system, such that we can ignore the influence from the real outage event. The idea behind misleading the control center is to let the control center find a fake outage event in the system instead of a real one, thereby hindering the control center from detecting the real outage event and even prompting it to make a wrong operation or decision. The system faces more risk as the control center spends more time in locating the real outage line. Moreover, when dispatching the power flows, the control center will avoid assigning the flow to the fake-outage position. Then, based on this response, the attacker can attempt to create an initial failure. In the power system, if the power flows are over the thermal limit, meaning the lines are overloaded, this can cause a failure in the power system. To this end, after the fake outage position is selected, the control center can be misled, and redispatched flow over the residual lines, where the residual lines may end up reaching their thermal limit, and leading to more outage event. In this context, the optimization problem of selecting the fake outage line is expressed as follows:

$$\mathcal{F}2 : \max_{w_l, \forall l = 1, \cdots, n_{br}} \quad \sum_{l \in \mathcal{E}} \frac{\overline{P}_l}{P_l^{\max}} \tag{11a}$$

$$\text{s.t.} \quad w_l \in \{0, 1\}, \tag{11b}$$

$$\sum_{l=1}^{n_{br}} w_l = 1, \tag{11c}$$

$$\overline{\mathbf{p}} = \mathbf{p} + \left(\mathbf{w}^T \mathbf{p}\right) \cdot (\mathbf{L}\mathbf{w}). \tag{11d}$$

Eq. (11a) is the objective function that adds the fraction of the real power after certain line has no flow, $\overline{P}_l$, to its thermal

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2018.2865316, IEEE Transactions on Smart Grid

limit, $P_l^{\max}$, for all lines. Constraints (11b) and (11c) are the equations related to the selection vector, $\mathbf{w} = [w_1 \cdots w_{n_{br}}] \in \mathbb{R}^{n_{br} \times 1}$. Eq. (11d) calculates the real power after certain line has no flow, $\overline{\mathbf{p}}$, based on the LODF matrix. Therefore, the fake outage position is determined as $l_m = \{\ l \mid w_l \neq 0,\ \forall l = 1, \ldots, n_{br}\}$. The buses linked by the fake outage line, l_m, are assigned to set $\mathcal{M}$. Appendix A shows the proof of the selecting criteria.

After the method of selecting the target line is presented, we discuss the method to determine the cyber attack region, based on the limitation that the attackers can only alter the measurement of some selected sensors but not all sensors in the system. Therefore, we assume that the attacks only have a limited capability to observe and alter a sub-network of $\mathcal{G}$. To launch an attack, the attacker maliciously changes the measurements in a sub-network of $\mathcal{G}$ denoted as $\overline{\mathcal{G}} = \{\overline{\mathcal{N}}, \overline{\mathcal{E}}\}$. The buses and lines in the attack region are assigned to set $\overline{\mathcal{N}}$ and $\overline{\mathcal{E}}$, respectively. We further separate set $\overline{\mathcal{N}}$ into sets $\mathcal{A}$ and $\mathcal{B}$. The boundary buses in $\overline{\mathcal{G}}$ are assigned to set $\mathcal{B}$, when the others are assigned to set $\mathcal{A}$.

The key idea of finding the attack region is that we have to find a new path to re-dispatch the flow, to supply the load of the buses in $\mathcal{M}$, and to obtain a favorable estimate for the power flow of l_o and the states of the buses in $\mathcal{L}$. The sub-network can be obtained using the breadth-first search (BFS) algorithm, which will be discussed later in this paper.

D. Measurements Modification

For the measurement modification, we formulate an optimization problem and meanwhile the physical laws have to be considered as mentioned in the Section II-A. To follow these rules, we add the power flow calculation to the constraints. However, the voltage square in (1) makes the equation become difficult to solve. The voltage magnitude constraints from the original power flow model also faces the same issue. To overcome these issues, we use the *DistFlow* model [30], [31], a convex relaxation technique from the original power flow, to reformulate the AC power flow equations. In this model, we include two auxiliary variables, namely $\mathbf{W} = [W_1 \cdots W_{n_b}] \in \mathbb{R}^{n_b \times 1}$ and $\mathbf{C} = [C_1 \cdots C_{n_{br}}] \in \mathbb{R}^{n_{br} \times 1}$, which denote the squared magnitude of bus voltages and line currents, respectively. The equation in (1) can then be rewritten as follows:

$$|S_l|^2 = W_j C_l. \tag{12}$$

Given that the formulation in (12) is still not convex, we apply the following convex relaxation:

$$|S_l|^2 \leq W_j C_l, \tag{13}$$

where (13) is a widely supported second-order cone constraint. The relation of $\mathbf{W}$, $\mathbf{C}$, and $\mathbf{s}$ can be denoted as

$$W_j - W_k = (Z_l^* S_l + Z_l S_l^*) - |Z_l|^2 C_l, \tag{14}$$

where Z_l is the impedance of line l that connects buses j and k. The transmission loss of line l can then be calculated as $Z_l C_l$.

With the power flow model, we then formulate the objective function as minimizing the required attacker ability, that is, we minimize the difference in the measurement before and after the attack. These measurements may include the voltage magnitudes, voltage phases, loads of buses, and power flows of the lines. However, the power flows of the lines are closely related to the voltage magnitudes, voltage phases, and loads of buses. Therefore, the objective function can be defined as follows:

$$J = \|\overline{\mathbf{s}} - \mathbf{s}\|_2, \tag{15}$$

where $\overline{\mathbf{s}}$ is the modified power flow in the attack region.

According to the discussions above, the optimization can be formulated with J as the objective function. Then, power flow equations and altered range of the measurements are regarded as the constraints. The optimization formulation is then formulated as

$$
\begin{aligned}
\mathcal{F}3: \quad & \min_{\mathbf{W}, \overline{\mathbf{P}}^D, \overline{\mathbf{Q}}^D, \overline{\mathbf{s}}} \quad J && && \text{(16a)}\\
& \text{s.t.} && && \\
& W_j = |v_j|^2, && \forall j \in \mathcal{B}, && \text{(16b)}\\
& V_{\min}^2 \leq W_j \leq V_{\max}^2, && \forall j \in \mathcal{A}, && \text{(16c)}\\
& W_j - W_k = (Z_l^* \overline{S}_l + Z_l \overline{S}_l^*) - |Z_l|^2 C_l, && \forall j, k \in \overline{\mathcal{N}}, l \in \overline{\mathcal{E}}, && \text{(16d)}\\
& (1-\tau) P_j^D < \overline{P}_j^D < (1+\tau) P_j^D, && \forall j \in \overline{\mathcal{N}}, && \text{(16e)}\\
& \overline{P}_j^D + i \overline{Q}_j^D = \sum_l \left(\overline{S}_l + Z_l C_l \right), && \forall j \in A, l \in \mathcal{E}, && \text{(16f)}\\
& -P_l^{\max} < \overline{P}_l < P_l^{\max}, && \forall l \in \overline{\mathcal{E}}, && \text{(16g)}\\
& \left| \overline{S}_l \right|^2 \leq W_j C_l, && \forall j \in \overline{\mathcal{N}}, l \in \overline{\mathcal{E}}. && \text{(16h)}
\end{aligned}
$$

Eq. (16b) shows that the voltage magnitude of the boundary buses must remain the same, and Eq. (16c) shows that the voltage magnitudes in $\mathcal{A}$ must be controlled within a specified range. $V_{\max}$ and $V_{\min}$ represent the upper and lower bound of the voltage magnitude, respectively. Eq. (16d) shows relation of $\mathbf{W}$, $\mathbf{C}$, and the modified apparent power at the "from" end of line l, $\overline{S}_l$, that connects buses j and k. Eq. (16e) shows that the real load of bus j inside the region before, P_j^D, and after modification, $\overline{P}_j^D$, must be maintained within a specified range. Moreover, τ indicates the modification range. The power injected into the bus must meet the load listed in Eq. (16f) and $\overline{Q}_j^D$ is the reactive load of bus j. Eq. (16g) shows that the modified flows of the l-th line, $\overline{P}_l$, must be managed under the thermal limits. Eq. (16h) calculates the apparent power flow in the attack region.

If the attacker wishes to implement the attack using DC model, then the optimization problem can be easily formulated. The DC model assumes that if all voltage magnitudes are set to 1, then no transmission loss takes place, and the phase difference can be neglected. Based on this assumption, the formulation is explained in detail in [32].

IV. Implementation Strategy

In this section, we explain the implementation strategy of the proposed attack scheme by gathering the attack components presented in Section III. This strategy is divided into three phases including total 8 steps as shown in Fig. 2. Step 1 is the first phase which is used to find the real outage position.

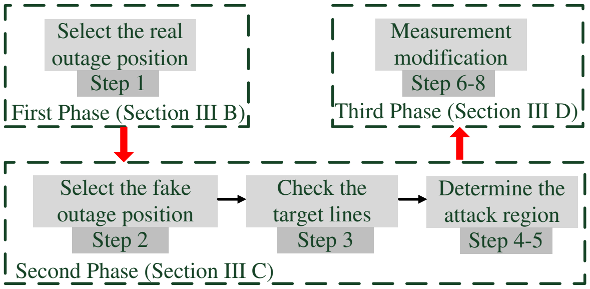
Select the real outage position
Step 1
First Phase (Section III B)
Measurement modification
Step 6-8
Third Phase (Section III D)
Select the fake outage position
Step 2
Check the target lines
Step 3
Determine the attack region
Step 4-5
Second Phase (Section III C)

Fig. 2. The implementation strategy of the proposed attack.

Then, the second phase is from Step 2 to 5 containing the fake outage position selection and attack region determination. In the final, the third phase focuses on the measurement modification listed in Step 6 to 8.

In the first phase, we use Eq. (10) to determine the real outage position. The procedure is outlined as follows:

Step 1: We select the line whose disconnection generates the greatest influence on the system. Therefore, l_o is selected as the description in (10), and the buses linked by l_o are assigned to $\mathcal{L}$. We then use LODF to calculate the power flow after l_0 faces an outage.

With the real outage position obtained in Step 1, we then use Problem $\mathcal{F}2$ to select the corresponding fake outage position. After determining the target lines, we must check if the selection fulfills the rules described in Section III-A. We then detailly describe the steps of deciding the attack region. The region of sub-network $\overline{\mathcal{G}}$ is obtained by using the BFS algorithm to find the shortest path for redispatching the power flow. The procedure is outlined as follows:

Step 2: We apply the fake outage position selection algorithm listed in Algorithm 1 to select the fake outage position. We construct vector $\mathbf{u}$ at the beginning of the algorithm, and then assign each element of $\mathbf{u}$ with the objective function of Problem $\mathcal{F}2$ on the basis of the results of the exhaustive search. Line l_0 must avoid being selected, when line l_m obtains the largest value of the objective function.

Step 3: After selecting the target lines, we must check if these lines are reasonable or follow the rules described in Section III-A. If these lines are not reasonable or do not follow such rules, we then eliminate the unreasonable line l_o from $\mathbf{f}$ or l_m from $\mathbf{u}$, and then start again from Step 1. Otherwise, we proceed to the Step 4.

Step 4: Assume that l_m flows from buses j to k. The trivial solution is that we only add and subtract the flow amount to and from buses j and k, respectively. However, this trivial solution can be easily recognized by the control center. In this case, we only add the flow amount to the load of bus j and try to find another path to supply the load at bus k to prevent the application of a trivial solution.

Step 5: To find a path for supplying bus k, we initially consider $\overline{\mathcal{N}}$ and $\overline{\mathcal{E}}$ in $\overline{\mathcal{G}}$ as empty sets. Afterward, we use BFS algorithm described in Algorithm 2 to find the shortest path for redispatching the flow. The path obtained from Algorithm 2 is regarded as the sub-network $\overline{\mathcal{G}}$. We add l_o to $\overline{\mathcal{E}}$ and the buses in $\mathcal{L}$ to $\overline{\mathcal{N}}$ as the attack region. The sub-network $\overline{\mathcal{G}}$ is therefore determined.

Algorithm 1: Fake outage position selection algorithm

```
Input: Power flow $\mathbf{p}$, LODF matrix $\mathbf{L}$
Output: fake outage position $l_m$
$\mathbf{u} = [u_1 \cdots u_{n_{br}}] \in \mathbb{R}^{n_{br} \times 1}$
for $l$ = 1 to $n_{br}$ do
    if $l = l_o$ then
        $u_l = 0$
    else
        $\overline{\mathbf{p}} = \mathbf{p} + P_l \cdot \mathbf{L}_{\{1:n_{br},l\}}$
        $u_l = \sum_{l \in \mathcal{E} \setminus l_o} \frac{P_l}{P_l^{\max}}$
    $l_m = \underset{l}{\operatorname{argmax}} \{u_l | l = 1, \ldots, n_{br}\}$
```

From step 1 to step 3, the attack strategy involves many condition checks, and therefore the attackers may spend most of time on searching the target lines. However, if the attackers can analyze the power system and find out the lines, which do not follow the limitation in Section III-A, before launching the attacks, the target lines selection can converge more quickly. Then, with the target lines and the attack region, the modification is then based on the solution to Problem $\mathcal{F}3$. The procedure is outlined as follows:

Step 6: After selecting the attack region, we first set the power flow of the fake outage position to 0. Then, solve the optimization Problem $\mathcal{F}3$ based on the AC model listed in (16). However, if the attacker wishes to employ the DC model, then the formulation in [32] must be solved. This formulation is a convex optimization problem that can be dealt with using many existing algorithms and toolboxes.

Step 7: If the problem has no solution, then the current attack region cannot satisfy the constraints. We then reapply Algorithm 2, and go back to Step 6. Otherwise, we proceed to Step 8.

Step 8: We set $\overline{\mathbf{z}} = \mathbf{z}$ and replace the power flow measurements of $\overline{\mathbf{z}}$ in $\overline{\mathcal{G}}$ with the $\overline{\mathbf{s}}$ from the solution to Problem $\mathcal{F}3$.

With the proposed mechanism, the normalized Lagrange multiplier of fake outage position will have the largest value compared to others. In this case, the operator can easily detect an outage event happening at the fake position. Appendix B presents the proof of this statement.

V. Case Study

In this section, we adopt the IEEE 14-bus [33], 24-bus [34], and 118-bus systems [35] to validate our proposed attacking mechanism. Specifically, we employ the 14-bus test system to illustrate the proposed method in detail. Fig. 3 shows the topology of the 14-bus system, when Table I lists the thermal flow limit of each line. Table I lists the thermal flow limit of each line in 14-bus system. We then use 118-bus test system to demonstrate the efficiency of the proposed attack mechanism in a large system, and the corresponding thermal limits can be found in [35]. Without any specification, the modification rage,

Algorithm 2: BFS algorithm for finding fake outage position

```
Input: System topology $\mathcal{G}$, bus $k$, sub-network $\overline{\mathcal{G}}$, line $l_o$
Output: Sub-network $\overline{\mathcal{G}}$
1  Find a bus $g$ having a generator and is the nearest to bus $k$
2  Current system configuration is $\mathcal{W} = \{\mathcal{N}, \mathcal{E} \setminus \{\overline{\mathcal{E}}, l_o\}\}$.
3  $g$ : starting bus. $k$ : destination bus.
4  let the bus $g$ be the progress bus and the level $t = 0$. Rest buses are set as unvisited buses.
5  Search all of the unvisited buses connected to the buses in progress buses. Put such unvisited buses to progress buses and previous progress buses are assigned as visited buses.
6  if $j \in$ progress bus then
7      go to step 11 of Algorithm 2.
8  else
9      repeat step 5 of Algorithm 2 again.
10     $t = t + 1$.
11 Backtrack from the destination bus to the starting bus level-by-level, and identify the shortest path. The buses and lines in the path are given to $\overline{\mathcal{N}}$ and $\overline{\mathcal{E}}$ respectively.
```

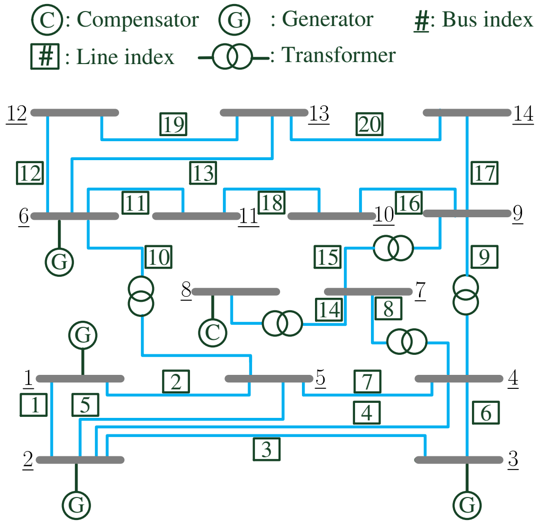

Fig. 3. IEEE 14-bus test system [33].

TABLE I
THE THERMAL FLOW LIMIT AND INFLUENCE FACTOR OF IEEE 14-BUS SYSTEM

Line number	1	2	3	4	5
Limit (MW)	200	100	100	100	100
f_l	-28.37	14.60	53.23	4.81	-32.18
Line number	6	7	8	9	10
Limit (MW)	50	100	50	100	100
f_l	-10.71	-30.43	-4.75	6.86	10.65
Line number	11	12	13	14	15
Limit (MW)	50	20	50	50	50
f_l	2.16	-7.33	12.45	NaN	-33.05
Line number	16	17	18	19	20
Limit (MW)	20	20	20	20	20
f_l	-2.62	-0.22	-1.36	-1.36	1.10

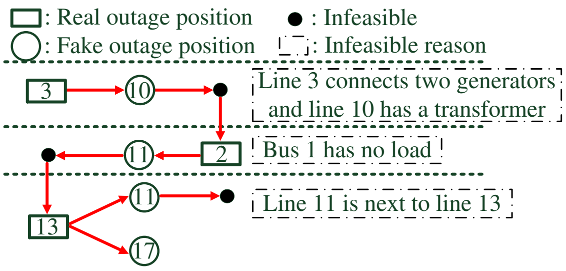

Fig. 4. Target lines selection procedure of 14-bus system.

τ, for all measurements and loads is set to 25%. The voltage magnitude must be controlled between 1.05 p.u. and 0.95 p.u.. The measurements used for the bad data and parameter error detection include the real power of all lines at the "from" end, the voltage magnitude of all buses, and the voltage phase of the reference bus. The errors for all measurements are assumed to be $n_i \sim N(0, 0.001)$. The identification threshold of bad data and parameter error detection is set to 3 which is outside the 99.80% confidence interval. The blue and red colors in the simulation results denotes the real and fake outage positions, respectively. We use the software toolbox MATPOWER [36] to run the power flow and provide the initial information of the system. To solve the optimization problem in (16), we use CVX [37], a package for solving convex programs. The SE results are obtained through Gauss-Newton method [26]. Also, all the simulations for computation were conducted with an Intel i7-6700 computer with 3.4 GHz CPU and 8GB RAM. The increment ratio of the j-th measurement, Δ_j, which denotes the incremental amount compared to the original measurement, can be expressed as follows:

$$\Delta_j = \frac{|\bar{z}_j| - |z_j|}{|z_j|} \times 100\%. \tag{17}$$

A. Implementing the Attack in the 14 Bus System

We select the target lines following Steps 1 to 3 outlined in Section IV. The influence factors of all the lines are listed in Table I. Line 3 has the largest value in the influence factor and the corresponding fake outage position is line 10 based on the solution of Problem $\mathcal{F}2$. However, line 3 is connected to two generators and a transformer is located at line 10. Therefore, these target lines are not feasible, and we have to find another sets of real and fake outage positions. The second largest value in Table I is line 2. Line 2 is selected as real outage position, and line 11 is the corresponding fake outage position. However, line 2 connects bus 1 and bus 5, and bus 1 has no load; line 2 cannot be the real outage line. We then selected the third largest value in Table I. Line 13 is

TABLE II
THE SETS USED IN THE MODIFICATION FOR 14-BUS SYSTEM

Set	Bus number	Description
$\mathcal{A}$	$12, 13, 14$	The buses in the attack region
$\mathcal{B}$	6	The boundary bus of the attack region
$\mathcal{L}$	$6, 13$	The buses connecting the real outage line
$\mathcal{M}$	$9, 14$	The buses connecting the fake outage line

Set	Line number	Description
$\bar{\mathcal{E}}$	$12, 13, 19, 20$	The lines in the attack region

selected as the real outage position here, and line 11 is still the corresponding fake outage position. However, line 11 is next to line 13. We then eliminate line 11 from the possible solutions, and resolve the Problem $\mathcal{F}2$ again. Following the proposed recursive way, we eventually select lines 13 and 17 as the real and fake outage lines, respectively. Fig. 4 illustrates the target line selection process in detail.

Given that the flowing path of the fake outage position is from buses 9 to 14, we must find a path for supplying the load of bus 14. The nearest generator is located at bus 6. Therefore, we use Algorithm 2 to find the shortest path from the starting bus, bus 6, to the destination bus, bus 14. Table II summarizes the attack region based on the results of Algorithm 2. Table III and IV present the measurements before and after modification based on the solutions of Problem $\mathcal{F}3$. The computation time for solving Problem $\mathcal{F}3$ is 0.40 second.

We then perform SE as well as bad data detection by using these modified measurements. We perform the detection by calculating the normalized residual and Lagrange multipliers, and then sort the results shown in Table V(a) in a descending order. Table V(a) shows two large Lagrange multipliers that are related to x_{17} and x_{20} and are larger than the identification threshold. We then eliminate those measurements that are related to x_{17} and x_{20} before reapplying bad data detection. Table V(b) shows the results of the second round of detection. The largest value in Table V(b) is much lower than the threshold. Therefore, we successfully mislead the control center into detecting an error on the fake outage position.

B. Consequences of the Attack in the 118 Bus System

Following the same procedure, we apply the proposed attack mechanism to the 118-bus test system. We then select lines 4 and 21 as the positions of the real and fake outage events, respectively. The attack region contains 16 buses and 19 lines. We also employ the modified measurements for the bad data and parameter error detection, which results are summarized in Table VI. In the simulation, the computation time for solving Problem $\mathcal{F}3$ is 0.80 second. For the first round detection presented in Table VI(a), the operator easily observes that line 21 has an obvious error. After eliminating the measurements related to line 21, Table VI(b) shows no error in the measurements. Therefore, in the large system, the operator can also be misled into detecting a fake outage event.

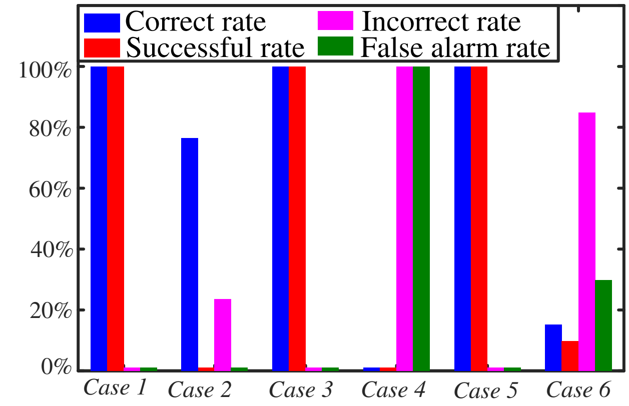

Fig. 5. Correct and successful rate for different cases.

C. Observability and Effect of Target Lines Selection

The bad data and parameter error detection can be influenced by noise. We collect the results of $1,000$ Monte Carlo simulations and study the influence of target line selection. Specifically, we examine the following cases:

- *Cases* 1*,* 3*, and* 5 : Select target lines based on the proposed method in the 14-bus, 24-bus, and 118-bus systems, respectively; and
- *Cases* 2*,* 4*, and* 6 : Randomly select target lines in the 14-bus, 24-bus, and 118-bus systems, respectively.

For the 24-bus system, τ is set to 60% because each line has a very huge power flow. Therefore, the measurements in a local area with a small τ cannot be easily modified. If the loads vary over a certain range, it cannot pass the sanity check from the control center even the results cannot be detected by the bad data detection. This setting just helps us demonstrate the proposed attack strategy in 24-bus system.

If the Lagrange multiplier of the fake outage position has the largest value among others, then this parameter is regarded as a correct attack. Meanwhile, if the corresponding Lagrange multiplier is larger than the threshold, then the attack is regarded as a successful attack. By contrast, an incorrect attack is defined as the other Lagrange multiplier or measurement residual of the line, which is not fake outage position, obtains the largest value. A false alarm is defined when the largest Lagrange multiplier or measurement residual of the line, which is not the fake outage position, is larger than the threshold. Table VII shows the selected target lines for the six cases. Fig. 5 and Table VII present the results.

Based on the simulation results presented in Fig. 5, our proposed selection framework allows a fake outage event to occur every time for the 14-bus, 24-bus, and 118-bus systems. However, we cannot guarantee the performance of our framework if the target lines are randomly selected. The random selection method also leads to a high false alarm rate for the system. For *Case* 2, the fake outage position can be captured by the operator. However, the corresponding normalized Lagrange multipliers are all lower than the threshold as shown in Table VII, thereby leading to a 0% success rate. In the 24-bus system, an unexpected fake outage event is revealed

TABLE III
THE VOLTAGE AND LOAD BEFORE AND AFTER ATTACK WITH 14-BUS TEST SYSTEM

Bus number	Voltage Magnitude (p.u.)			Voltage Phase (Angle)			Load (MVA)		
	Before	After	Increment	Before	After	Increment	Before	After	Increment
6	1.0500	1.0500	0.00%	-0.1499	-0.1499	0.00%	$11.20 + 7.50i$	$8.96 + 7.65i$	-12.60%
12	1.0350	1.0363	0.13%	-0.1648	-0.1656	0.48%	$6.10 + 1.60i$	$4.58 + 0.95i$	-25.83%
13	1.0304	1.0290	-0.14%	-0.1658	-0.1682	1.48%	$13.50 + 5.80i$	$10.13 + 5.66i$	-21.02%
14	1.0161	1.0042	-1.17%	-0.1778	-0.2033	13.78%	$14.90 + 5.00i$	$11.18 + 1.49i$	-28.24%

TABLE IV
THE POWER FLOW BEFORE AND AFTER ATTACK FOR 14-BUS SYSTEM

Line number	Power flow (MVA)		
	Before	After	Increment
12	$7.58 + 2.58i$	$7.79 + 2.32i$	1.51%
13	$16.90 + 7.36i$	$18.93 + 7.47i$	10.40%
17	$10.49 + 3.41i$	0	-100.00%
19	$1.41 + 0.83i$	$2.85 + 0.62i$	78.26%
20	$4.60 + 1.98i$	$11.39 + 1.92i$	130.64%

TABLE V
THE DETECTION RESULTS FOR 14-BUS SYSTEM

(a) First Round

Parameter Measurement	λ_j^N, r_j^N
x_{17}, x_{20}	3.4160
x_{13}	3.1934
x_{11}, x_{16}, x_{18}	2.6841
x_{12}, x_{19}	0.4600

(b) Second Round

Parameter Measurement	λ_j^N, r_j^N
x_{12}, x_{13}, x_{19}	0.8050
x_7	0.0430
x_5	0.0340
$r_{12}, r_{13}, r_{19}, r_{33}$	0.0255

TABLE VI
THE DETECTION RESULTS FOR 118-BUS SYSTEM

(a) First Round

Parameter Measurement	λ_j^N, r_j^N
x_{21}	10.9228
x_{23}, x_{24}	7.4409
x_{26}	7.0079
x_{36}	6.0390

(b) Second Round

Parameter Measurement	λ_j^N, r_j^N
x_8, x_{37}	2.2111
x_{20}, x_{22}	2.2018
x_{96}	1.9532
x_{30}	1.8193

TABLE VII
THE PARAMETER SETTING AND THE AVERAGE NORMALIZED LAGRANGE MULTIPLIER OF CORRECT ATTACK FOR SIX CASES

	l_o	l_m	$\lvert\mathcal{N}\rvert$	$\lvert\mathcal{E}\rvert$	Average $\lambda_{l_m}^N$
Case 1	13	17	4	4	3.4159
Case 2	13	19	3	2	0.1412
Case 3	21	23	10	14	24.9058
Case 4	21	20	9	11	0
Case 5	4	21	16	19	10.8885
Case 6	4	2	5	4	3.2296

TABLE VIII
THE POWER FLOW MODIFICATION FOR 14-BUS SYSTEM

Line number	Transmission loss (MVA)	
	Calculated	Real
12	$0.3584 + 0.7460i$	$0.0736 + 0.1531i$
13	$0.2484 + 0.4892i$	$0.2484 + 0.4892i$
19	$0.0175 + 0.0159i$	$0.0118 + 0.0107i$
20	$0.2154 + 0.4386i$	$0.2154 + 0.4386i$

to the operator for *Case* 4. Therefore, if the target lines are randomly selected, then the unpredictable events are revealed to the operator. In this case, the results cannot be controlled. For *Case* 6, if the estimation results are not influenced by noise, then line 1 shows the largest normalized parameter error. However, this error is below the detection threshold. Given that this normalized Lagrange multiplier can only exceed the threshold under the influence of noise, and then the noise may also make the errors of other positions exceed the threshold, thereby hiding the expected fake outage information from the operator. Moreover, given that the observed outage position is not fixed, the operator can easily notice that the system has been injected with false data by the attacker.

D. Comparison of the AC and DC models

In Seciton V-C, the attacks designed by AC model can cause very high impact on the system operation. By contrast, according to [22], the attacks constructed by DC model can cause high residual in AC state estimation, such that the attacks can be easily observed. This is because only voltage phases, real powers, and loads are modifiable in the DC model; however, AC state estimation further needs voltage magnitudes and reactive powers. Also, the transmission loss has to be considered in the AC state estimation, such that the power flows at the "from" and "to" ends are different. This approach cannot be obtained with DC model.

Given that transmission loss is considered in the formulation, we then use 14-bus system as an example to explain the rationale behind our use of the AC model. Table VIII summarizes the transmission losses in the attack region. The calculated losses are based on $Z_l C_l$ as shown in (16f), and the real losses are taken from MATPOWER according to the modified voltage and current system topology. Based on the results, the real and calculated transmission losses of lines 13 and 20 are the same, while those of lines 12 and 19 are slightly different. These results can be attributed to (13) where the second-order cone programming relaxation is applied, and to the fact that the conditions of the boundary buses are bounded in (16b). Therefore, the $\left|\overline{S}_l\right|^2$ of some lines are not equal to W_jC_l, and hence making the calculated losses larger than the real losses. However, these differences are smaller than the power flow. To measure the influence of miscalculated loss on the dispatch in the attack region, we utilize the following parameter:

$$O_{\text{inf}} = \frac{1}{\left|\overline{\mathcal{E}}\right|} \sum_{l \in \left|\overline{\mathcal{E}}\right|} \frac{\Re(Loss_l^{\text{cal}} - Loss_l^{\text{real}})}{\Re(\overline{\mathbf{s}})} \tag{18}$$

where O_{inf} is the influence factor, $Loss_l^{\text{cal}}$ is the calculated loss, and $Loss_l^{\text{real}}$ is the real loss of line l. Then, the influence factors for the 14-bus, 24-bus, and 118-bus systems are 0.95%, 2.32%, and 1.71%, respectively. The comparison results show that the error of the calculation is very small compared to the line flow. Therefore, the influence is limited, and the calculated error can be regarded as noise when the measurements are entered into the detection mechanism.

In this work, we aim to create an initial failure through the proposed method, and then induce the cascade failure to the power system. From Section V-A to V-C, we have already demonstrated that the fake outage line can be continuously appeared as an outage event, and then mislead the control center. With this approach, an initial failure can be created. Then, the cascade failure can be propagated from the initial failure as described in [38]. One more thing that we can discuss is the impact after the attack such as economic impact. Although the impacts due to cascading failure or blackout are the main purpose of the proposed attack strategy, these impacts are hard to be quantized and evaluated. Therefore, we just discuss the economic impact in terms of the operation cost in Appendix C.

VI. Conclusion

In this paper, we propose a joint line-removing and line-maintaining attack strategy based on the AC model in which the attacker maliciously injects false data in the cyber layer to cover a physical event in the power system. The target of the attack strategy is to create an initial failure and then induce the cascade failure in the system. When launching the attack, the target lines are identified based on the LODF matrix. The attack region is obtained through the method developed by the BFS algorithm, and then we modify the measurements from the power flow equations. The simulation results reveal that our proposed scheme successfully misleads the control center and masks the line-outage event.

The potential countermeasures can be separated into two parts. One possible method is to use historical data to predict the future income. Then, if the future states have huge difference compared to predicted states, it can be assumed that there is an attack event in the system. Another method is to study the statistical characteristic of the states in the system. More specifically, the statistical characteristic of data generated by the attack is different from previous time slots; therefore, the method such as change point detection can be applied.

References

[1] V. Rampurkar, P. Pentayya, H. A. Mangalvedekar, and F. Kazi, “Cascading Failure Analysis for Indian Power Grid,” *IEEE Trans. Smart Grid*, vol. 7, no. 4, pp. 1951–1960, Jul. 2016.

[2] J. Salmeron, K. Wood, and R. Baldick, “Analysis of Electric Grid Security Under Terrorist Threat,” *IEEE Trans. Power Syst.*, vol. 19, no. 2, pp. 905–912, May 2004.

[3] Å. J. Holmgren, E. Jenelius, and J. Westin, “Evaluating Strategies for Defending Electric Power Networks Against Antagonistic Attacks,” *IEEE Trans. Power Syst.*, vol. 22, no. 1, pp. 76–84, Feb. 2007.

[4] R. Smith, “Assault on California Power Station Raises Alarm on Potential for Terrorism,” *The Wall Street Journal*, May 2014.

[5] Y. Liu, P. Ning, and M. K. Reiter, “False Data Injection Attacks Against State Estimation in Electric Power Grids,” in *Proc. ACM 16th conf. Comp. & Comm. Security (CCS)*, Chicago, Illinois, USA, Nov. 2009, pp. 21–32.

[6] Md. A. Rahman and H. M. Rad, “False Data Injection Attacks with Incomplete Information Against Smart Power Grids,” in *Proc. IEEE Global Comm. Conf. (GLOBECOM)*, California, USA, Dec. 2012, pp. 3153–3158.

[7] X. Liu, Z. Bao, D. Lu, and Z. Li, “Modeling of Local False Data Injection Attacks With Reduced Network Information,” *IEEE Trans. Smart Grid*, vol. 6, no. 4, pp. 1686–1696, Jul. 2015.

[8] 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.

[9] 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.

[10] J. Zhang and L. Sankar, “Implementation of Unobservable State-preserving Topology Attacks,” in *Proc. North American Power Sym. (NAPS)*, North Carolina, USA, Oct. 2015.

[11] X. Liu and Z. Li, “Local Load Redistribution Attacks in Power Systems With Incomplete Network Information,” *IEEE Trans. Smart Grid*, vol. 5, no. 4, pp. 1665–1676, Jul. 2014.

[12] Z. Li, M. Shahidehpour, A. Alabdulwahab, and A. Abusorrah, “Analyzing Locally Coordinated Cyber-Physical Attacks for Undetectable Line Outages,” *IEEE Trans. Smart Grid*, vol. 9, no. 1, pp. 35–47, Jan. 2018.

[13] R. M. Lee, M. J. Assante, and T. Conway, “Analysis of the Cyber Attack on the Ukrainian Power Grid,” E-ISAC and ICS, Tech. Rep., Mar. 2016. [Online]. Available: https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

[14] Z. Li, M. Shahidehpour, A. Alabdulwahab, and A. Abusorrah, “Bilevel Model for Analyzing Coordinated Cyber-Physical Attacks on Power Systems,” *IEEE Trans. Smart Grid*, vol. 7, no. 5, pp. 2260–2272, Sep. 2016.

[15] 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.

[16] R. Deng and P. Zhuang, “CCPA: Coordinated Cyber-Physical Attacks and Countermeasures in Smart Grid,” *IEEE Trans. Smart Grid*, vol. 8, no. 5, pp. 2420–2430, Sep. 2017.

[17] 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.

[18] 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.

[19] J. Kim and L. Tong, “On Topology Attack of a Smart Grid,” in *Proc. IEEE PES Innovative Smart Grid Technol. (ISGT)*, Washington, DC, Feb. 2013, pp. 1–6.

[20] ——, “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.

[21] X. Liu and Z. Li, “Local Topology Attacks in Smart Grids,” *IEEE Trans. Smart Grid*, vol. 8, no. 6, pp. 2617–2626, Nov. 2017.

[22] M. A. Rahman and H. Mohsenian-Rad, “False Data Injection Attacks Against Nonlinear State Estimation in Smart Power Grids,” in *Proc. IEEE Power Eng. Soc. Gen. Meeting*, Vancouver, BC, Canada, Jul. 2013.

[23] 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.

[24] J. Zhu and A. Abur, “Identification of Network Parameter Errors,” *IEEE Trans. Power Syst.*, vol. 21, no. 2, pp. 586–592, May 2006.

[25] Y. Lin and A. Abur, “A New Framework for Detection and Identification of Network Parameter Errors,” *IEEE Trans. Smart Grid*, to be published.

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

[27] K. C. Sou, H. Sandberg, and K.H. Johansson, "Electric Power Network Security Analysis via Minimum Cut Relaxation," in *Proc. IEEE 50th Conf. Decision & Control & European Control Conf. (CDC-ECC)*, Florida, U.S.A, Dec. 2011, pp. 4054–4059.

[28] Y. Sun, W.-T. Li, W. Song, and C. Yuen, "Joint Cyber and Physical Attacks Against Topology of Electric Grids," in *Proc. IEEE Region 10 conf. (TENCON)*, Singapore, Nov. 2016.

[29] J. Guo, Y. Fu, Z. Li, and M. Shahidehpour, "Direct Calculation of Line Outage Distribution Factors," *IEEE Trans. Power Syst.*, vol. 24, no. 3, pp. 1633–1634, Aug. 2009.

[30] G. Coffrin, H. L. Hijazi, and P. V. Hentenryck, "DistFlow Extensions for AC Transmission Systems," *arXiv*, May 2015. [Online]. Available: http://arxiv.org/abs/1506.04773

[31] S. Bose, S. H. Low, T. Teeraratkul, and B. Hassibi, "Equivalent Relaxations of Optimal Power Flow," *IEEE Trans. Autom. Control*, vol. 60, no. 3, pp. 729–742, Mar. 2015.

[32] H.-W. Chung, W.-T. Li, C. Yuen, W.-H. Chung, and C.-K. Wen, "Local Cyber-physical Attack with Leveraging Detection in Smart Grid," in *Proc. IEEE Intl. Conf. Smart Grid Commun. (SmartGridComm)*, Dresden, Germany, Oct. 2017, pp. 461–466.

[33] R. D. Christie, "Power Systems Test Case Archive," University of Washington, Aug. 1993. [Online]. Available: https://www2.ee.washington.edu/research/pstca/pf14/pg_tca14bus.htm

[34] C. Grigg, P. Wong, P. Albrecht, R. Allan, M. Bhavaraju, R. Billinton, Q. Chen, C. Fong, S. Haddad, S. Kuruganty, et al., "The IEEE Reliability Test System 1996. A Report Prepared by the Reliability Test System Task Force of the Application of Probability Methods Subcommittee," *IEEE Trans. Power Syst.*, vol. 14, no. 3, pp. 1010–1020, Aug. 1999.

[35] Electrical and Computer Engineering Department, "IEEE 118-Bus, 54 Unit, 24-Hour System Unit and Network Data," Illinois Institute of Technology. [Online]. Available: http://motor.ece.iit.edu/data/JEAS_IEEE118.doc

[36] R. D. Zimmerman, C. E. Murillo-Sánchez, and R. J. Thomas, "MATPOWER: Steady-State Operations, Planning and Analysis Tools for Power Systems Research and Education," *IEEE Trans. Power Syst.*, vol. 26, no. 1, pp. 12–19, Feb. 2011.

[37] M. Grant and S. Boyd, "CVX: Matlab software for disciplined convex programming, version 2.1," http://cvxr.com/cvx, Mar. 2014.

[38] H. Ren and I. Dobson, "Using Transmission Line Outage Data to Estimate Cascading Failure Propagation in an Electric Power System," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 55, no. 9, pp. 927–931, Sep. 2008.

Appendix

A. Proof of Selection Criteria in Section III-B

The formulation in (6) can be rewritten as follows using the Lagrange method :

$$\min_{\widehat{\mathbf{v}},P_e} \quad \mathbf{r}^T\mathbf{R}^{-1}\mathbf{r} + \boldsymbol{\lambda}^T P_e \tag{19}$$

The first-order necessary condition of optimality must satisfy the following:

$$\frac{\partial \mathbf{r}^T\mathbf{R}^{-1}\mathbf{r} + \boldsymbol{\lambda}^T P_e}{\partial P_e} = \mathbf{H}_p\mathbf{R}^{-1}\mathbf{r} + \boldsymbol{\lambda} = 0, \tag{20}$$

where $\mathbf{H}_p$ is the Jacobian matrix of the measurement functions, $h\left(P_e, \mathcal{G}, \widehat{\mathbf{v}}\right)$, with respect to the network parameter error vector, P_e. When SE converges, the Lagrange multiplier vector $\boldsymbol{\lambda}$ must be expressed as follows:

$$\boldsymbol{\lambda} = -\mathbf{H}_p\mathbf{R}^{-1}\mathbf{r}. \tag{21}$$

For the system, $\mathbf{R}$ is determined, so $\boldsymbol{\lambda}$ is related to $\mathbf{H}_p$ and $\mathbf{r}$. The $\mathbf{H}_p$ is related to the topology and system states, and $\mathbf{r}$ is caused by the estimation results. Therefore, the residual vector, $\mathbf{r}$, has an important influence on the results of bad data and parameter error detection. When selecting the target lines, if the outage event of one line has a greater influence on the system compared with the outage event of other lines, then the residual can be increased. For this purpose, we apply the LODF matrix to determine the impact when the specific line is disconnected.

B. Proof of the Efficiency of the Proposed Attack

According to [24]–[26], the normalized a-th measurement residual and the corresponding Lagrange multipliers for the l-th line can be represented as

$$\left|\lambda_l^N\right| = \frac{\left|\Lambda_{\{l,l\}}P_{e\{l\}} + H^T_{p\{:,l\}}R^{-1}_{\{a,a\}}S_{\{:,a\}}n_a\right|}{\sqrt{\Lambda_{\{l,l\}}}}, \tag{22a}$$

$$\left|r_a^N\right| = \frac{\left|S_{\{a,a\}}n_a + S_{\{a,:\}}H_{p\{:,l\}}P_{e\{l\}}\right|}{\sqrt{S_{\{a,a\}}R_{\{a,a\}}}}, \tag{22b}$$

where $\Lambda_{\{l,l\}}$ denotes the l-th column and l-th row of the parameter covariance matrix, $\boldsymbol{\Lambda}$, $S_{\{a,a\}}$ is the a-th column and a-th row of the parameter sensitivity matrix, $\mathbf{S}$, $R_{\{a,a\}}$ is the a-th column and a-th row of the noise covariance matrix, $\mathbf{R}$, $H_{p\{:,l\}}$ represents the l-th column of $\mathbf{H}_p$, n_a is the noise interference of a-th measurement, and $P_{e\{l\}}$ is the parameter error of the l-th line.

In this section, we explain how the fake outage position obtains the largest value of the normalized Lagrange multiplier compared with the other lines. The influence of noise is ignored in the derivation. If the m-th line is the fake outage position and has an erroneous parameter, which means $P_{e\{m\}} \neq 0, P_{e\{l\}} = 0 (l \neq m)$, then all measurements are correct. Based on (22a), we obtain

$$\left|\lambda_m^N\right| = \sqrt{\Lambda_{\{m,m\}}}\left|P_{e,\{m\}}\right|, \tag{23a}$$

$$\left|\lambda_l^N\right| = \frac{\Lambda_{\{m,l\}}}{\sqrt{\Lambda_{\{l,l\}}}}\left|P_{e,\{m\}}\right|. \tag{23b}$$

The ratio of $\left|\lambda_l^N\right|$ to $\left|\lambda_m^N\right|$ can be represented as follows:

$$\left|\frac{\lambda_l^N}{\lambda_m^N}\right| = \frac{\left|\Lambda_{\{m,l\}}\right|}{\sqrt{\Lambda_{\{l,l\}}\Lambda_{\{m,m\}}}}. \tag{24}$$

To show that $\left|\lambda_m^N\right|$ is larger than the other normalized Lagrange multipliers, we must prove that the ratio in (24) is lower than 1. Consider an expectation of a square value that must be positive as

$$E\left\{\left[\left(\lambda_l - E\left(\lambda_l\right)\right) - \left(\lambda_m - E\left(\lambda_m\right)\right)\right]^2\right\} \geq 0. \tag{25}$$

From the definition of the covariance matrix, we obtain

$$\Lambda_{\{m,m\}} = E\left\{\left[\lambda_m - E(\lambda_m)\right]^2\right\}, \tag{26a}$$

$$\Lambda_{\{l,l\}} \quad = E\left\{\left[\lambda_l - E(\lambda_l)\right]^2\right\}, \tag{26b}$$

$$\Lambda_{\{m,l\}} \quad = E\left\{\left[\lambda_m - E(\lambda_m)\right]\left[\lambda_l - E(\lambda_l)\right] \quad \right\}. \tag{26c}$$

Eq. (25) can then be rewritten as follows:

$$\Lambda_{\{l,l\}} - 2\Lambda_{\{m,l\}} + \Lambda_{\{m,m\}} \geq 0. \tag{27}$$

To obtain (25), the determinant of (27) must remain non-positive as follows:

$$\left(2\Lambda_{\{m,l\}}\right)^2 - 4\Lambda_{\{l,l\}}\Lambda_{\{m,m\}} \leq 0, \quad (28)$$

which yields

$$\frac{\Lambda^2_{\{m,l\}}}{\Lambda_{\{l,l\}}\Lambda_{\{m,m\}}} \leq 1. \quad (29)$$

After taking the square root for both sides, we obtain $\left|\lambda^N_m\right| \geq \left|\lambda^N_l\right|$ according to (24). Therefore, the normalized Lagrange multiplier of the fake outage position obtains the largest value.

C. Economic Impact of the Attacks

In this section, we discuss the economic impact of the proposed attack strategy. However, some impacts, such as the failures in the system or detecting the failures in the system, cannot be easily quantified as a number. To cope with this situation, we only discuss the cost that we can calculate, and therefore we only compare the operation cost. The operation cost considers the scenario that only the true outage position is disconnected in the system. Specifically, this is the minimum operation cost that the control center can obtain after observing the fake outage event. By contrast, this is also the operation cost that the attackers can *at least* cause to the system.

The operation cost increases from 8297.73$ to 8331.50$, which raises 33.77$, in 14-bus system. In 118-bus system, the cost increases from 129660.70$ to 129726.25$, which raises 65.55$. According to the simulation, the operation cost increases after the attacks. Moreover, if the control center decides to redispatch the flows, the cost can go even higher, and then the failures will happen.

The simulations results reveal that the operation cost slightly increases. This is because we only consider the situation that a true outage line is disconnected and the control center ignores the fake outage event. On the other hand, operational costs for the grid to diagnose the outage event and the delay in recovering the system are not included in the comparison; all these damage created to the system is something hard for us to compute. If we wish to create more economic impact to the system, there are two directions to further interfere the operation of the power grid. First, we can attempt to attack several pairs of target lines, which means several real and fake outage positions, in the system. More specifically, we can have several attackers in the system, and they attempt to jointly attack the power grid. By contrast, we can propose another attack strategy, which mainly focuses on the impact to the operation cost, so that the operation cost can be higher than the results. The abovementioned points can be also regarded as our future research topics.

Hwei-Ming Chung received the B.S. degree in electrical engineering and the M.S. degree in communications engineering from National Sun Yat-sen University in 2014 and 2016, respectively. He wes a research assistant at the Wireless Communications Laboratory, Research Center for Information Technology Innovation, Academia Sinica, Taiwan in 2017. Then, he is currently working toward the Ph.D. degree in Department of Informatics, University of Oslo. His current research interests include power system monitoring, smart grid, and statistical signal processing.

Wen-Tai Li (M'18) received the B.S. and M.S. degrees in optoelectronics and communication engineering from National Kaohsiung Normal University, Kaohsiung, Taiwan, in 2009 and 2011, respectively, and the Ph.D. degree in communications engineering from the Institute of Communications Engineering, National Sun Yat-sen University, Kaohsiung, Taiwan, in 2018.

He was a Research Assistant, from 2015 to 2017, and is currently a Postdoc Fellow with the Singapore University of Technology and Design, Singapore. His research interests include power system monitoring, smart grid, and wireless communications.

Chau Yuen (S'04-M'06-SM'12) received the BEng and PhD degree from Nanyang Technological University (NTU), Singapore, in 2000 and 2004 respectively. Dr Yuen was a Post Doc Fellow in Lucent Technologies Bell Labs, Murray Hill during 2005. During the period of 2006 - 2010, he worked at the Institute for Infocomm Research (I2R, Singapore) as a Senior Research Engineer, where he was involved in an industrial project on developing an 802.11n Wireless LAN system, and participated actively in o Long Term Evolution (LTE) and LTE-Advanced (LTE-A) standardization. He joined the Singapore University of Technology and Design from June 2010, and received IEEE Asia-Pacific Outstanding Young Researcher Award on 2012. Dr Yuen serves as an Editor for IEEE Transactions on Communications and IEEE Transactions on Vehicular Technology.

Wei-Ho Chung received the B.Sc. and M.Sc. degrees in Electrical Engineering from the National Taiwan University, Taipei, Taiwan, and the Ph.D. degree in Electrical Engineering from the University of California, Los Angeles, in 2009. From 2002 to 2005, he was with ChungHwa Telecommunications Company. In 2008, he worked on CDMA systems at Qualcomm, Inc., San Diego, CA. His research interests include communications, signal processing, and networks. Dr. Chung received the Ta-You Wu Memorial Award from Ministry of Science and Technology in 2016, Best Paper Award in IEEE WCNC 2012, and Taiwan Merit Scholarship from 2005 to 2009. He has published over 50 journal articles and over 50 conference papers. Since January 2010, Dr. Chung had been an assistant research fellow, and promoted to the rank of associate research fellow in January 2014 in Academia Sinica. Since 2018, he holds the position of full professor and leads the Wireless Communications Lab at Electrical Engineering, National Tsing Hua University, Taiwan.

Yan Zhang is Full Professor at the Department of Informatics, University of Oslo, Norway. He received a PhD degree in School of Electrical & Electronics Engineering, Nanyang Technological University, Singapore. He is an Associate Technical Editor of IEEE Communications Magazine, an Editor of IEEE Network Magazine, an Editor of IEEE Transactions on Green Communications and Networking, an Editor of IEEE Communications Surveys & Tutorials, an Editor of IEEE Internet of Things Journal, an Editor of IEEE Vehicular Technology Magazine, and an Associate Editor of IEEE Access. He serves as chair positions in a number of conferences, including IEEE GLOBECOM 2017, IEEE VTC-Spring 2017, IEEE PIMRC 2016, IEEE CloudCom 2016, IEEE ICCC 2016, IEEE CCNC 2016, IEEE SmartGridComm 2015, and IEEE CloudCom 2015. He serves as TPC member for numerous international conference including IEEE INFOCOM, IEEE ICC, IEEE GLOBECOM, and IEEE WCNC. His current research interests include: next-generation wireless networks leading to 5G, green and secure cyber-physical systems (e.g., smart grid, healthcare, and transport). He is IEEE VTS (Vehicular Technology Society) Distinguished Lecturer. He is also a senior member of IEEE, IEEE ComSoc, IEEE CS, IEEE PES, and IEEE VT society.

Chao-Kai Wen (S'00–M'04) received the Ph.D. degree from the Institute of Communications Engineering, National Tsing Hua University, Taiwan, in 2004. He was with Industrial Technology Research Institute, Hsinchu, Taiwan and MediaTek Inc., Hsinchu, Taiwan, from 2004 to 2009. Since 2009, he has been with National Sun Yat-sen University, Taiwan, where he is Professor of the Institute of Communications Engineering. His research interests center around the optimization in wireless multimedia networks.