Modeling of Local False Data Injection Attacks With Reduced Network Information

Xuan Liu, Zhen Bao, Dan Lu, and Zuyi Li, *Senior Member, IEEE*

***Abstract*—Modern power grids are becoming more prone to cyberattacks. Even worse, an attacker without the full topology and parameter information of a power grid can still execute a false data injection attack without being detected by the state estimator. This paper proposes an efficient strategy for determining the optimal attacking region that requires reduced network information. The effectiveness of the proposed algorithm is verified through extensive simulations. This paper introduces a new front in the study of smart grid cyber security: determination of a feasible attacking region by obtaining less network information. This paper is also essential and significant for finding effective protection strategies against false data injection attacks based on the deep understanding of the mechanisms and strategies of the attacks.**

***Index Terms*—False data injection attacks, incomplete information, local load redistribution, optimal attacking strategy, power systems**

NOMENCLATURE

Regions

A	Attacking region.
N	Nonattacking region.
S	Searching region.

Indices

b, i, j	Subscript: index for buses.
d	Subscript: index for loads.
l	Subscript: index for lines.

Constants

K	Maximum number of lines in the searching region.
M_1	Given large value.
N_D	Number of load buses.
N_G	Number of generators.
x_l	Reactance of line l.
α	Given value for incremental phase angle.
τ	Given maximum percentage of change for load measurement attack.

Variables

D_b	Load at bus b.
D_d	Load d.
ΔD_b	False data injection vector into load measurement at bus b.
ΔD_d	False data injection vector into load d measurement.
ΔF_l	False data injection into line l measurement.
m	Number of feasible initial attacking regions.
n_i	Number of neighboring buses of bus i.
p	Percentage of feasible initial attacking regions.
Q_b	Maximum attacking amount of load bus b.
r	Residual in bad data detection.
$\Delta\theta_i$	Incremental phase angle at bus i.
γ_b	Given threshold value for the attacking amount of load bus b.
δ_i	Indicator variable: $\delta_i = 1$ if bus i is a nonboundary bus in the attacking region; $\delta_i = 0$ otherwise.
v_i	Indicator variable: $v_i = 1$ if bus i is a boundary bus in the attacking region; $v_i = 0$ otherwise.
w_l	Indicator variable: $w_l = 1$ if line l is within the attacking region; $w_l = 0$ otherwise.
σ_d	Indicator variable: $\sigma_d = 1$ if $\Delta D_d \neq 0$; $\sigma_d = 0$ otherwise.
φ_l	Indicator variable: $\varphi_l = 1$ if $\Delta F_l \neq 0$; $\varphi_l = 0$ otherwise.

Sets

Ω_i	Set of neighboring buses of bus i.
Ω_A	Set of buses in region A.
Ω_N	Set of buses in region N.
Ω_{AD}	Set of loads in region A.
Ω_{BA}	Set of boundary buses in region A.
Ω_{BS}	Set of boundary buses in region S.
Ω_{SB}	Set of buses in region S.
Ω_{SD}	Set of loads in region S.
Ω_{SL}	Set of lines in region S.

Vectors and Matrices

$\boldsymbol{a}$	Attacking vector.
$\boldsymbol{B}$	Bus susceptance matrix.
$\boldsymbol{B}_{A'}$	Bus susceptance matrix in region A excluding tie lines.
$\boldsymbol{B}_{S'}$	Bus susceptance matrix in region S excluding tie lines.
$\boldsymbol{B}^{\boldsymbol{0}}_{S'}$	Bus susceptance matrix in region S excluding tie lines when the reactance of lines is set to arbitrary values.
$\boldsymbol{c}$	Measurement error injected by the attacking vector $\boldsymbol{a}$.

Manuscript received February 12, 2014; revised July 7, 2014 and October 16, 2014; accepted November 28, 2014. This work was supported by the U.S. Department of Energy under Grant DE-FC26-08NT02875 and Grant DE-OE-0000449. Paper no. TSG-00067-2014.

The authors are with the Electrical and Computer Engineering Department, Illinois Institute of Technology, Chicago, IL 60616 USA (e-mail: lizu@iit.edu).

Digital Object Identifier 10.1109/TSG.2015.2394358

$\Delta \boldsymbol{D_A}$	False data injection vector into load measurements in region A.
$\Delta \boldsymbol{D_S}$	False data injection vector into load measurements in region S.
$\Delta \boldsymbol{D}$	False data injection vector into load measurements.
$\boldsymbol{E_D}$	Unity matrix of N_D by N_D.
$\boldsymbol{E_G}$	Unity matrix of N_G by N_G.
$\Delta \boldsymbol{F_A}$	Incremental generator output vector in region A.
$\Delta \boldsymbol{F_S}$	Incremental generator output vector in region S.
$\Delta \boldsymbol{G}$	Incremental generator output vector.
$\boldsymbol{H}$	Jacobian matrix of the power grid.
$\boldsymbol{S}$	Shift factor matrix of the power grid.
$\boldsymbol{U}$	Bus-generator incidence matrix.
$\boldsymbol{U_A}$	Bus-generator incidence matrix in region A.
$\boldsymbol{U_S}$	Bus-generator incidence matrix in region S.
$\boldsymbol{V}$	Bus-load incidence matrix.
$\boldsymbol{V_A}$	Bus-load incidence matrix in region A.
$\boldsymbol{V_S}$	Bus-load incidence matrix in region S.
$\boldsymbol{W_A}$	Bus-line incidence matrix in region A.
$\boldsymbol{W_S}$	Bus-line incidence matrix in region S.
$\widehat{\boldsymbol{x}}$	Estimate of the state variables.
$\Delta \boldsymbol{x}$	State variation vector.
$\boldsymbol{X_A}$	Branch reactance matrix in region A.
$\boldsymbol{X_S}$	Branch reactance matrix in region S.
$\boldsymbol{z}$	Measurement vector.
$\Delta \boldsymbol{z}$	False data injection vector.
$\Delta \boldsymbol{\theta}$	Incremental phase angle vector.
$\widehat{\boldsymbol{\theta}}$	Estimate of incremental phase angle vector.
$\Delta \boldsymbol{\theta_A}$	Incremental phase angle vector in region A.
$\Delta \boldsymbol{\theta_S}$	Incremental phase angle vector in region S.

Note that Δ represents incremental change and symbols in bold represent vectors or matrices.

I. Introduction

THE SMART evolution of traditional power systems highly relies on communication networks and information technology, which raise a great concern about cyber security of the smart grid. State estimation is being subject to the threat of bad data. The impact of bad data on state estimation was studied early by Merrill and Schweppe [1] in the 1970s. Recently, Liu *et al.* [2] demonstrated that an attacker can compromise the state estimation by injecting the predesigned false data into meters without being detected if the full topology and parameter information of a power gird is assumed to be known. Based on the corrupted data, the control center may make wrong decisions that lead to economic loss or insecure operations.

False data injection attack has attracted intensive research interest. Kosut *et al.* [3] proposed a heuristic algorithm to determine the worst attacking strategy, which made a trade-off between the probability of being detected and damaging effects to the state estimation. Xie *et al.* [4] showed that the locational marginal prices can be manipulated by injecting false data. Kim and Tong [5] proposed a state-preserving model for a single line attack. The authors showed that an attacker can mask the topology of a power grid without being detected by injecting false power at the terminal buses of a line.

Yuan *et al.* [6] considered the physical characteristics of power systems and transformed the general false data injection attacks into a load redistribution (LR) attacking model. A bi-level mixed integer linear programming (MILP) model was built to determine the worst attacking strategy that would maximize the operation cost. Recently, a delayed LR attacking model which considered the delay effect after outages had been proposed in [7]. More researches about false data injection attacks can be found in [8]–[12].

In [2]–[12], an attacker must know the full network topology and parameter information of the entire power grid. In reality, such sensitive and important information is usually strongly guarded in the control center. It is very difficult for an attacker to get access to these information. However, an attacker can obtain the parameters of lines by nonintrusive methods. In other word, we can take the corresponding measurements to calculate line parameters. For example, an attacker can take the bus voltage and line current to compute the resistance of the line. In general, the more network information that must to be known, the more cost and efforts an attacker should pay. In the context of limited resources, an attacker aims to obtain less necessary network information to launch a successful attack.

It is very difficult or impossible for an attacker to have that knowledge due to limited resources. Unfortunately, an attacker with incomplete network information of a power grid can still launch a successful false data injection attack without being detected. Ashfaqur-Rahman and Mohsenian-Rad [13] made the first attempt to model false data injection attacks with incomplete information, by injecting false data making all the state variables in two subnetworks divided by a cut change the same. Similarly, Giani *et al.* [14] defined an observable island and proposed an unobservable attack in which all the buses in the same observable island share the same change of state under the attack. The buses in different observable islands may have different phase angles. However, it should be noted that the models in [13] and [14] share two disadvantages.

1) The attacking region is limited in the cut, so the selection of the attacking region is not flexible.
2) No feasible attacking vector can be constructed if there are zero-injection boundary buses in the cut.

To overcome the disadvantages in [13] and [14], we proposed a more general and effective false data injection model [15] based on incomplete network information: local LR attacks. In our model, an attacker only needs to obtain the topology and parameter information of the local attacking region to design the false data which can avoid being detected by the state estimator, without knowing any network information of the nonattacking region. This is done by making sure that the variations of phase angles of all boundary buses connected to the same island of the nonattacking region are the same. We also showed that there always exists a nonzero attacking vector as long as the number of nonload buses in the attacking region is no greater than the number

of nonboundary buses in the attacking region minus one. The local LR attacking model reveals the vulnerability of power grids to false data injection attack since an attacker with weak capacity can launch a successful local attack.

In this paper, we continue [15] to investigate the local attacking mechanisms. The main contributions of this paper are listed as follows.

1) We study the topological characteristics of an attacking region and summarize them into three observations. All the observations are translated into linear constraints, making it possible to determine the local attacking region based on MILP method.
2) To the best of our knowledge, this paper is the first to consider the practical issue that an attacker can only obtain the parameter information of a limited number of lines and thus introduce a new front in the study of smart grid cyber security: the determination of a feasible attacking region by obtaining less network information. This paper relaxes the very strong yet unrealistic assumption in previous studies that the attacker must obtain the full network information of the entire power grid. That assumption has made the study on attacking mechanisms impractical.
3) We show that if a bus is LR-attackable in an attacking region with all line reactances set to an arbitrary value, it is highly likely that the bus is still LR-attackable and effectively LR-attackable if all line reactances in the attacking region are set to their true values. This observation is of great help to determine a feasible attacking region by obtaining less line parameter information.
4) We propose a simple yet effective strategy to determine the optimal attacking region that requires the minimum network parameter information.
5) This paper lays the foundation for developing effective protection strategies and detection approaches by deeply investigating the local attacking mechanisms of an attacker.

The rest of this paper is organized as follows. Section II reviews the scheme of local LR attacks. Section III analyzes the topological characteristics of an attacking region and proposes a strategy to determine the optimal attacking region. Section IV demonstrates the proposed model with various testing systems. Section V concludes this paper.

II. Local LR Attacking Model

In state estimation based on dc power flow, the measurement vector $\boldsymbol{z}$ refers to bus power injections and line power flows, and the state vector $\boldsymbol{x}$ refers to bus phase angles. The estimated state vector $\hat{\boldsymbol{x}}$ can be obtained by the least square method

$$\mathbf{min}\|z - \boldsymbol{H}\boldsymbol{x}\|_{\boldsymbol{2}}. \tag{1}$$

In (1), $\boldsymbol{H}$ is the Jacobian matrix and can be constructed according to the topology and line reactances of a power grid.

The residue r is

$$r = \|z - \boldsymbol{H}\hat{\boldsymbol{x}}\|_{\boldsymbol{2}} \tag{2}$$

where $\boldsymbol{H}\hat{\boldsymbol{x}}$ are the estimated values of measurements. The residue r is represented by the two-norm of the error between the real measurements and the estimates.

In the traditional bad data detection, if the residue is less than a given threshold value, the estimated state $\hat{\boldsymbol{x}}$ is acceptable. Otherwise, there exist bad data among the measurements. From (2), we can see that if the false data injection vector $\Delta\boldsymbol{z}$ and the state variation vector $\Delta\boldsymbol{c}$ satisfy (3), the residue r will not increase, and, accordingly, false data injection attacks on measurements can bypass the traditional bad data detection [2]

$$\Delta z = \boldsymbol{H}\Delta\boldsymbol{c}. \tag{3}$$

When (3) is satisfied, $\Delta\boldsymbol{z}$ will never increase the residue $\boldsymbol{r}$. In this paper, we only consider the case in which the injected false data will not increase the original r. That is, (3) is strictly satisfied and the injected false data follows Kirchhoff's Current Law (KCL) and Kirchhoff's Voltage Law (KVL).

Equation (3) indicates that if the injected false data obey the physical laws (KCL and KVL) of power systems, these data can pass the traditional residual test. In [15], we showed that (3) can be equivalently transformed

$$\begin{bmatrix} \Delta\boldsymbol{G} \\ \Delta\boldsymbol{D} \\ \Delta\boldsymbol{F} \end{bmatrix} = \begin{bmatrix} \boldsymbol{E_G} & \boldsymbol{0} \\ \boldsymbol{0} & \boldsymbol{E_D} \\ \boldsymbol{S}\cdot\boldsymbol{U} & -\boldsymbol{S}\cdot\boldsymbol{V} \end{bmatrix} \cdot \begin{bmatrix} \Delta\boldsymbol{G} \\ \Delta\boldsymbol{D} \end{bmatrix}. \tag{4}$$

Yuan *et al.* [6] made the assumptions that generator output measurements cannot be attacked, i.e., $\Delta\boldsymbol{G} = \boldsymbol{0}$, and load measurements $\Delta\boldsymbol{D}$ can be attacked within certain ranges. Then, the false data injection attack is transformed into a LR attack [6]. That is, the attacker aims to modify the bus load measurements by injecting a false data vector $\Delta\boldsymbol{D}$, while keeping the sum of all injected false data zero. Any false data injection vector $[\Delta\boldsymbol{G}\ \Delta\boldsymbol{D}\ \Delta\boldsymbol{F}]^{\boldsymbol{T}}$ that satisfies (4) can pass the residual test.

In [15], we divided the buses of a power grid into three types: nonboundary buses in the attacking region A, boundary buses in the attacking region A, and buses in the nonattacking region N, and proved that the power flows in the nonattacking region will not change if additional power injection into the attacking region makes the phase angles of all boundary buses in the attacking region connected to the same nonattacking region increase or decrease by the same amount. So, if the attacker designs the false data vector $[\Delta\boldsymbol{D}\ \Delta\boldsymbol{F}]^{\boldsymbol{T}}$ such that the variations of phase angles of the boundary buses in the attacking region A are the same, then the false data injection would not impact the power flows in the nonattacking region. Thus, any arbitrary nonzero false injection power vector $[\Delta\boldsymbol{D}\ \Delta\boldsymbol{F}]^{\boldsymbol{T}}$ that satisfies (5)–(8) can be used to launch a successful local LR attack

$$\boldsymbol{B}_{\boldsymbol{A}'}\Delta\boldsymbol{\theta}_{\boldsymbol{A}} = -\boldsymbol{V}_{\boldsymbol{A}}\Delta\boldsymbol{D}_{\boldsymbol{A}} \tag{5}$$

$$\Delta\boldsymbol{F}_{\boldsymbol{A}} = \boldsymbol{X}_{\boldsymbol{A}}{}^{-\boldsymbol{1}}\boldsymbol{W}_{\boldsymbol{A}}{}^{\boldsymbol{T}}\Delta\boldsymbol{\theta}_{\boldsymbol{A}} \tag{6}$$

$$-\tau D_d \le \Delta D_d \le \tau D_d \quad \forall d \in \Omega_{AD} \tag{7}$$

$$\Delta\theta_b = \alpha \ \forall b \in \Omega_{BA}. \tag{8}$$

Equations (5) and (6) indicate that the injected false data obey KCL and KVL. Equation (7) ensures that load measurements can be attacked within certain ranges. Equation (8)

ensures that boundary buses in the attacking region must have the same phase angle. Boundary buses in the attacking region connected to different islands do not have to have the same incremental phase angle. In fact, they may have different incremental phase angles [15]. In the local attacking model, all the information that the attacker must know is the full network information of the attacking region, rather than that of the entire network.

In the local LR attacking model (5)–(8), an attacker needs to obtain the following three types of information to achieve an effective attack:

1) network topology, i.e., the connection information among buses in a power grid;
2) network parameter, i.e., line reactances under dc power flow network model;
3) load level, i.e., amount of load at each load bus.

Of the three types of information, it is much more difficult to obtain the network parameter information of a grid. This is because the reactance of a line is usually stored and strongly guarded in the control center and not transmitted outside of the control center. In addition, the reactance of a line is influenced by a set of factors, and thus is hard to be determined. Thus, considering the difficulty of obtaining the network parameter information, the focus of this paper is to minimize the required network parameter information and reduce the required topology and load level information for determining a small attacking region.

III. Optimal Attacking Region

The goal of an attacker is to determine an attacking region that requires the minimum amount of network information. However, it is a challenging issue for a practical-size network. Reference [15] lays the theoretical foundation on cyberattacks with only local information and provides clues to identify a small attacking region. We assume that all line flows are measured in both directions. In this section, we present a strategy to determine the optimal attacking region for one load bus built upon the local LR attack theory in [15]. For the convenience of discussion, we first define several terms. We then study the topological characteristics of an attacking region, followed by detailed steps for determining the optimal attacking region.

Definition 1 (LR-Attackable and nonLR-Attackable): A measurement is LR-attackable if its reading can be changed according to (5)–(8). A measurement is nonLR-attackable if its reading cannot be changed to satisfy (5)–(8). A network element (bus or line) is LR-attackable if its measurement can be LR-attackable. A network element is nonLR-attackable if its measurement is nonLR-attackable.

Note that, in LR attack, nonload buses (generator buses and zero-injection buses) are nonLR-attackable, and load buses and lines could be LR-attackable or nonLR-attackable.

Definition 2 (Effectively LR-Attackable): A network element is effectively LR-attackable if it is LR-attackable and the attacking amount exceeds a given threshold value.

Reference [6] stated that if the attacking amount at a bus is too large, the attack could be detected by the state estimator with a high probability. This is because the control center usually has preknowledge and experiences of the load distribution at buses. In this paper, we assume that the maximum error of load forecast could reach 10%–15% and, without loss of generality, the maximum allowable attacking amount (τ) of a load bus b is set to 15% of its load value. However, the attacking amount should not be too small either. Otherwise, the impact of the attacks on power systems operation could be insignificant. In this paper, the threshold attacking amount of a load bus b (γ_b) is set to 2.5%–10% of its load value.

Definition 3 (Attacking Region): The attacking region of a load bus is defined as the region that satisfies the following conditions.

1) The load bus is included in the attacking elements.
2) If no line connected to a bus is attacked, then the bus is excluded from the attacking region. All lines connected to the bus are also excluded from the attacking region.
3) If the two terminal buses of a line are included in the attacking region, then this line is also included in the attacking region.
4) If a line is included in the attacking region, then its terminal buses are also included in the attacking region.

Definition 4 (Optimal Attacking Region): The optimal attacking region of a load bus b is defined as a region that requires the minimum network parameter information, reduced topology and load level information, and the minimum number of measurements to be attacked to achieve an effective attack on bus b.

Based on the above definitions, the optimal attacking region of a load bus b should satisfy the following characteristics.

1) Bus b is in the attacking region and LR-attackable. That is, the measurement at bus b can be changed to satisfy (5)–(8).
2) The attacking amount on load bus b in the attacking region is no smaller than a given threshold (e.g., 10% of its load). This is to ensure that the damaging effect of the attack is significant.
3) The number of lines whose parameter information needs to be obtained is minimized and the required topology and load-level information is reduced.
4) The number of measurements that an attacker must attack in the attacking region is minimized.

It should be pointed out that if the attacker has the information of the entire power grid, the global optimality can be achieved. However, as discussed before, in practice it is very hard for an attacker to have the full network information of a power grid. Under the context of incomplete network information, the global optimality cannot be ensured, so we are seeking a suboptimal solution. In this paper, we first determine a feasible attacking region by satisfying 3), and then determine the optimal attacking region in the feasible attacking region.

Definition 5 (Feasible Attacking Region): An attacking region that satisfies the above characteristics 1) and 2) is defined as a feasible attacking region.

Definition 6 (Primary Attacking Region): The primary attacking region of a load bus b is defined as the region that includes bus b, all its neighboring buses and lines connected to bus b.

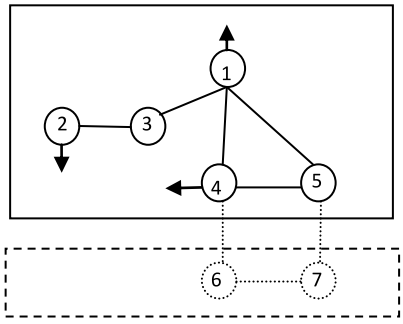

Fig. 1. Illustrative of topological characteristics of attacking regions.

A. Topological Characteristics of Attacking Regions

According to the definition of the attacking region, we can obtain three observations on the topological characteristics.

Observation 1: If bus i is a nonboundary bus in the attacking region, then all its neighboring buses and all lines connected to bus $i$must be included in the attacking region.

Proof: We prove the observation by contradiction. Suppose that there exists at least one neighboring bus j not included in the attacking region. According to the definition of the attacking region, line $i-j$ is not in the attacking region, so bus i is either a boundary bus in the attacking region or a bus in the nonattacking region, which contradicts the fact that bus i is a nonboundary bus in the attacking region. Similarly, we assume that one line $i-j$ is not included in the attacking region, then at least one terminal bus of the line is not included in the attacking region. If bus i is not in the attacking region, then, we obtain the contradiction. If bus j is in the nonattacking region, then bus i cannot be a nonboundary bus in the attacking region. ■

Observation 2: Suppose that bus i is a boundary bus in the attacking region. Line $i-j$ is included in the attacking region if bus j is a nonboundary bus or boundary bus in the attacking region.

Proof: The proof is trivial. Since line $i-j$ is included in the attacking region, according to Definition 3, buses i and j are also included in the attacking region as a nonboundary bus or boundary bus. ■

Observation 3: If bus i is in the nonattacking region, then all lines connected to bus i are excluded from the attacking region.

Proof: The proof is trivial. Since bus i is in the nonattacking region, it is not attacked. So, bus i and all lines connected to bus i are excluded from the attacking region. Observation 3 has been proved.

We use Fig. 1 to illustrate Observations 1–3. The attacking region is circled by the solid rectangle in Fig. 1. ■

Observation 1: Bus 1 is a nonboundary bus in the attacking region, so its neighboring buses 3–5 and lines 1-3–1-5 are all included in attacking region. Note that neighboring bus 5 is a boundary bus and nonattackable since it is a zero-injection bus, and neighboring bus 3 is a nonboundary bus and nonattackable since it is a zero-injection bus.

Observation 2: Bus 4 is a boundary bus in the attacking region. Lines 4-1 and 4-5 are included in the attacking region since buses 1 and 5 are in the attacking region. Line 4-6 is not included in the attacking region since bus 6 is in the nonattacking region.

Observation 3: Bus 6 is in the nonattacking region, so both lines connected to bus 6, i.e., lines 6-4 and 6-7, are excluded from the attacking region.

Observations 1–3 summarize the topological characteristics of an attacking region. These observations can be transformed into corresponding logic constraints such that an MILP model can be built to represent the topological characteristics.

Observation 1 can be divided into two parts.

Part 1: If bus i is a nonboundary bus in the attacking region, then all its neighboring buses must be included in the attacking region.

Part 2: If bus i is a nonboundary bus in the attacking region, then all the lines connected to bus i must be included in the attacking region.

Part 1 is translated into the following "if-then" condition:
If $\delta_i = 1$, then $\delta_j = 1$ or $v_j = 1\ \forall j \in \Omega_i$
which can be modeled as

$$\delta_i \le \delta_j + v_j\ \forall j \in \Omega_i \tag{9}$$

$$\delta_j + v_j \le 2 - \ \delta_i\ \forall j \in \Omega_i. \tag{10}$$

Part 2 is translated into the following "if-then" condition:
If $\delta_i = 1$, then $w_{ij} = 1\ \forall j \in \Omega_i$
which can be modeled as

$$\sum_{j\in\Omega_i} w_{ij} \ge n_i\delta_i. \tag{11}$$

Observation 2 is equivalent to the following "if-then" conditions:
If $v_i = 1$ and $\delta_j + v_j = 1$, then $w_{ij} = 1\ \forall j \in \Omega_i$
If $v_i = 1$ and $\delta_j + v_j = 0$, then $w_{ij} = 0\ \forall j \in \Omega_i$
which can be modeled as

$$w_{ij} \ge v_i + \left(\delta_j + v_j\right) - 1\ \forall j \in \Omega_i \tag{12}$$

$$w_{ij} \le \left(\delta_j + v_j\right) - v_i + 1\ \forall j \in \Omega_i. \tag{13}$$

Since bus i cannot be both a nonboundary bus and a boundary bus in the attacking region, for all the buses in a power grid, we have

$$\delta_i + v_i \le 1. \tag{14}$$

It should be pointed out constraint (10) can be discarded due to constraint (14).

Observation 3 can be described using the following "if-then" condition:
If $\delta_i + v_i = 0$, then $w_{ij} = 0\ \forall j \in \Omega_i$
which can be modeled as

$$\sum_{j\in\Omega_i} w_{ij} \le n_i(\delta_i + v_i). \tag{15}$$

As discussed in Section II, in the local LR attacking model, an attacker does not need to know all the topology and parameters of the entire power grid. In this paper, we design the attacking vector by making all the boundary buses in the attacking regions increase or decrease the same, that is, the nonattacking regions are treated as a connected network

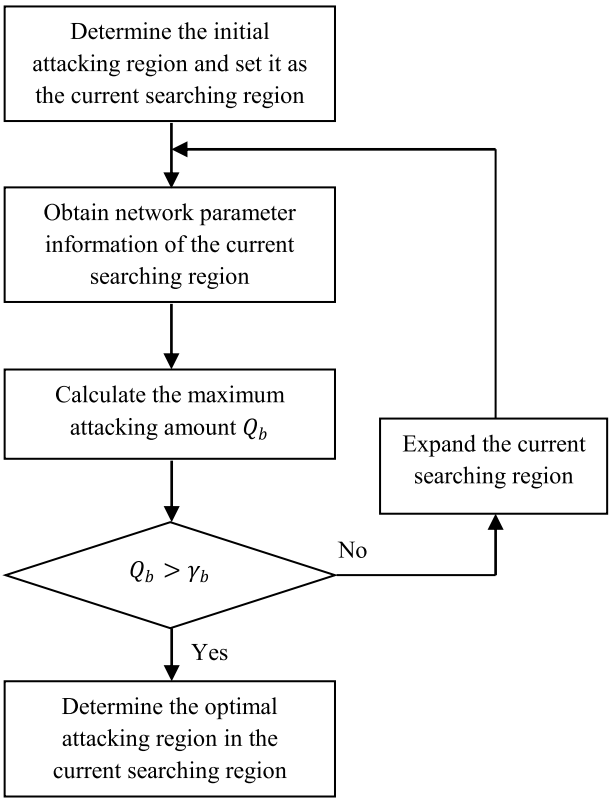

Fig. 2. Flowchart for determining the optimal attacking region.

whether they are really connected or disconnected. In this case, the attacker does not need to know the topology information of the nonattacking region since it does not need to determine the connectivity of the nonattacking region(s).

The condition that all the boundary buses in the attacking region have the same incremental phase angle, e.g., α, can be modeled as

$$\Delta\theta_i + (M_1 + \alpha)(1 - v_i) \geq \alpha \ \forall i \in \Omega_{BA} \tag{16}$$

$$\Delta\theta_i - (M_1 - \alpha)(1 - v_i) \leq \alpha \ \forall i \in \Omega_{BA}. \tag{17}$$

According to [15, Th. 1], all the buses in the nonattacking regions also have the same incremental phase angle α. This can be modeled as

$$\Delta\theta_i + (M_1 + \alpha)(\delta_i + v_i) \geq \alpha \ \forall i \in \Omega_N \tag{18}$$

$$\Delta\theta_i - (M_1 - \alpha)(\delta_i + v_i) \leq \alpha \ \forall i \in \Omega_N. \tag{19}$$

B. Strategy to Determine Optimal Attacking Region

Based on the local attacking principle in [15], we adopt a heuristic algorithm to determine the optimal attacking region for a load bus b. The principle of the entire algorithm is described in Fig. 2. First, we determine an initial attacking region for bus b and set it as the searching region. To ensure that the attacker only needs to obtain the reactances of the minimum number of lines, the number of lines in the searching region is minimized. Next, we obtain the true reactances of all the lines in the searching region. Then, we calculate the maximum attacking amount Q_b. If $Q_b \geq \gamma_b$, we begin to determine the optimal attacking region in the current searching region; otherwise we need to expand the searching region until the condition $Q_b \geq \gamma_b$ is satisfied. The details of determining the initial attacking region, expanding the searching region, determining the maximum attacking amount, and determining the optimal attacking region are presented in the next sections. The reason that we gradually expand the searching region is to reduce the load and topology information required. In each expansion, an attacker only needs to obtain the load and topology information of all boundary buses in the previous searching region.

C. Determination of Initial Attacking Regions

The determination of an initial attacking region in this paper is based on the following two observations.

Observation 4: It is highly likely that if bus b is LR-attackable in an attacking region with all the line reactances set to an arbitrary value, then bus b is still LR-attackable if the reactances of all the lines in the attacking region are set to their true values.

Observation 5: It is very likely that if bus b is LR-attackable in an attacking region, then bus b can be effectively LR-attackable in the region.

Observations 4 and 5 are made as a result of extensive experiments. In particular, Observation 4 is valid for all the experiments we have performed; Observations 5 is valid for over half of the experiments. According to Observations 4 and 5, if we determine an initial attacking region of bus b by setting the reactances of all lines to an arbitrary value, then there is a high probability that the initial attacking region would be a feasible attacking region. Thus, by doing so, for most load buses we do not need to expand the initial attacking region to make it feasible. For the remaining load buses whose initial attacking regions are not feasible, the initial attacking regions are expanded until they are feasible.

Based on Observation 4 and without loss of generality, we can set the reactance of all the lines in the current searching region to one and calculate the susceptance matrix. Then, according to [15, Th. 1], we have

$$\boldsymbol{B}^{\boldsymbol{0}}_{\boldsymbol{S'}} \Delta\boldsymbol{\theta_S} = -\boldsymbol{V_S}\Delta\boldsymbol{D_S}. \tag{20}$$

The algorithm for determining the initial attacking region for a load bus b is summarized as follows.

We can see that the proposed algorithm is very simple yet very effective and has the following advantages.

1) The determination of the initial attacking region does not require the true values of line reactance. The required network information is topology and load level information of the searching region.
2) The initial attacking region is very efficient since it is also a feasible attacking region for most load buses.

D. Expansion of the Current Searching Region

The searching region can be expanded by including all the neighboring buses of the boundary buses in the current searching region and the lines connecting the neighboring buses and boundary buses. In this process, the neighboring buses and the lines connecting the neighboring buses and boundary

Algorithm 1 Determination of Initial Attacking Region

Step 1: Obtain the topology and load level information of the primary attacking region. The searching region starts from the primary attacking region of the load bus.

Step 2: Set the reactances of all lines in the searching region to an arbitrary value.

Step 3: Set the incremental phase angles of all boundary buses, which include the buses in the searching region connected to the nonsearching region, to be the same as α.

Step 4: Determine an attacking region by solving

$$\min \sum_{l \in \Omega_{SL}} w_l \tag{21}$$

subject to

$$-\tau D_d \leq \Delta D_d \leq \tau D_d \quad \forall d \in \Omega_{SD} \tag{22}$$

$$\Delta\theta_j = \alpha \ \forall j \in\in \Omega_{BS} \tag{23}$$

$$\Delta D_b \neq 0. \tag{24}$$

Equations (9)–(19) $\forall i \in \Omega_{SB}$, (20)

The objective function in (21) is to minimize the number of lines whose parameters need to be known. Constraint (22) limits the attacking amount at buses. Constraint (23) ensures that all the boundary buses have the same incremental phase angle. Constraint (24) indicates that false data is injected into the measurement at bus b. Constraints (9)–(19) model the topological characteristics of the attacking region. Constraint (20) ensures that the injected false data obey KCL and KVL.

The optimization problem (21) is an MILP problem. If (21) is feasible, we find an initial attacking region, stop. Note that the initial attacking region may have less number of buses and lines than the current searching region. Otherwise, if (21) is infeasible, go to step 5.

Step 5: Expand the current searching region.

buses represent the topology information the attacker needs to obtain. In addition, the load-level information of newly added buses is also required. Considering the limited capacity of an attacker, it is reasonable to assume that an attacker can obtain the parameters of at most K lines. Thus, during the expansion of the search region, we need to count the number of lines whose true parameters have been obtained. If it is greater than the given value K, the expansion will be stopped. Note that if the searching region cannot be further expanded and the attacking amount of load bus b has not been satisfied yet, then we can tell that load bus b is not effectively attackable by the attacker with limited attacking capacity.

E. Determination of Maximum Attacking Amount

The maximum attacking amount of load bus b is needed to determine whether the current searching region needs to be expanded. It can be obtained by solving the following linear programming (LP) problem given the true reactances of all lines in the current searching region:

$$Q_b = \max \Delta D_b \quad \text{subject to.} \tag{25}$$

Equations (5)–(8) for the current searching region.

F. Determination of the Optimal Attacking Region

In determining the optimal attacking region, we need to minimize the number of measurements that an attacker needs to attack. We can count the number of attacked measurements using the following models:

If $\Delta D_d \neq 0$, then $\sigma_d = 1$
which is equivalent to
If $\sigma_d = 0$, then $\Delta D_d = 0$
which can be modeled as

$$\Delta D_d + (\tau D_d)\,\sigma_d \geq 0 \tag{26}$$

$$\Delta D_d - (\tau D_d)\,\sigma_d \leq 0 \tag{27}$$

If $\Delta F_l \neq 0$, then $\varphi_l = 1$
which is equivalent to
If $\varphi_l = 0$, then $\Delta F_l = 0$
which can be modeled as

$$\Delta F_l + M_1 \varphi_l \geq 0 \tag{28}$$

$$\Delta F_l - M_1 \varphi_l \leq 0. \tag{29}$$

The optimal attacking region for a load bus b in the current searching region can be obtained by solving the MILP optimization problem

$$\min \sum_{d \in \Omega_{SD}} \sigma_d + 2 \sum_{l \in \Omega_{SL}} \varphi_l \tag{30}$$

subject to

$$\Delta \boldsymbol{F_S} = \boldsymbol{X_S}^{-1} \boldsymbol{W_S}^{\boldsymbol{T}} \Delta \boldsymbol{\theta_S} \tag{31}$$

$$\boldsymbol{B_{S'}} \Delta \boldsymbol{\theta_S} = -\boldsymbol{V_S} \Delta \boldsymbol{D_S} \tag{32}$$

$$\Delta D_b \geq \gamma_b. \tag{33}$$

Equations (22), (23), (26), (27) $\forall d \in \Omega_{SD}$, (28), (29) $\forall l \in \Omega_{SL}$.

The objective function in (30) is to minimize the number of attacking measurements. Note that there are two measurements for each line. Constraints (31) and (32) ensure that the injected false data obey KCL and KVL. Constraint (33) ensures that the attack is effective. Constraint (23) represents the boundary condition. Constraints (26)–(29) count the number of attacking components.

IV. Case Study

In this section, we first use the modified IEEE 14-bus system to illustrate the proposed procedure to find the optimal attacking region of a load bus. We then present our extensive experiments that verify Observations 4 and 5. Lastly, we demonstrate that an attacker only needs to obtain the network information of a small number of lines to launch an effective attack.

A. Illustration of the Proposed Strategy

We test the proposed optimal attacking region model using the IEEE 14-bus system. Bus 1 is changed from a nonattackable bus to a load bus. Loads at some buses are also modified for the purpose of illustrating the concepts in this

paper. Line reactances are the same as those in [16]. The system is composed of 14 buses and 20 transmission line. The bus data can be found in the Appendix. We assume that this system is fully measured. That is, we need one meter to measure the injection power for each bus and two meters to measure the power flow passing through each transmission line. Thus, 54 measurements are needed in total. The attacking magnitude for a load bus is limited at $\tau = \pm 15\%$ of the actual load. To ensure that the attacks can bring significant damages to power system, the attacking amount at a load bus must be greater than 10% of its load, that is, $\gamma_b = 0.1\ D_b$. Considering the limited capacity of an attacker, at most $K = 10$ lines are allowed in the searching region. We pick load bus 1 and load bus 12 to illustrate the detailed procedure.

1) Case 1: The Attacker Intends to Attack Load Bus 1: The searching region of bus 1 starts from its primary attacking region, which is composed of buses 1, 2, 5, and lines 1-2, 1-5, 2-5. Buses 2 and 5 are boundary buses between the searching region and the nonsearching region. According to [15, Th. 1], to guarantee that there are no additional power flows exchanges between these two regions, the following boundary condition must hold:

$$\Delta\theta_2 = \Delta\theta_5 = \alpha.$$

Obtain the loads of buses 1 and 5 and set the reactances of lines 1-2, 1-5, 2-5 to one, and then solve the optimization problem (21). Since (21) is infeasible and there are 3 lines in the current searching region, which is less than $K = 10$, we need to expand the current searching region.

The new searching region consists of buses 1, 2, 3, 5 as nonboundary buses, buses 4, 6 as boundary buses, and lines 1-2, 1-5, 2-3, 2-4, 2-5, 3-4, 4-5, 5-6 whose reactances are set one. The loads of newly added buses 4 and 6 are obtained. According to [15, Th. 1], in order to make sure there are no power flows in or out of the searching region, the following boundary condition holds for buses 4 and 6, which are the boundary buses in the searching region:

$$\Delta\theta_4 = \Delta\theta_6 = \alpha.$$

Again, we solve (21), which is feasible now. The solution to (21) determines the initial attacking region, which is composed of buses 1, 2, 3 as nonboundary, buses 4, 5 as boundary buses, and lines 1-2, 1-5, 2-3, 2-4, 2-5, 3-4, 4-5. Note that the initial attacking region is not the same as the new search region.

Then, in order to calculate the maximum attacking amount of bus 1, we need to obtain the reactances of all lines in the initial attacking region, which is now the current searching region. The maximum attacking amount of bus 1 is determined by solving the following LP:

$$Q_1 = \max \Delta D_1$$

subject to

$$\begin{bmatrix} 21.3840 & -16.9005 & 0 & 0 & -4.4835 \\ -16.9005 & 33.3743 & -5.0513 & -5.6715 & -5.7511 \\ 0 & -5.0513 & 10.8982 & -5.8469 & 0 \\ 0 & -5.6715 & -5.8469 & 41.8457 & -23.7473 \\ -4.4835 & -5.7511 & 0 & -23.7473 & 37.9499 \end{bmatrix} \begin{bmatrix} \Delta\theta_1 \\ \Delta\theta_2 \\ \Delta\theta_3 \\ \Delta\theta_4 \\ \Delta\theta_5 \end{bmatrix}$$

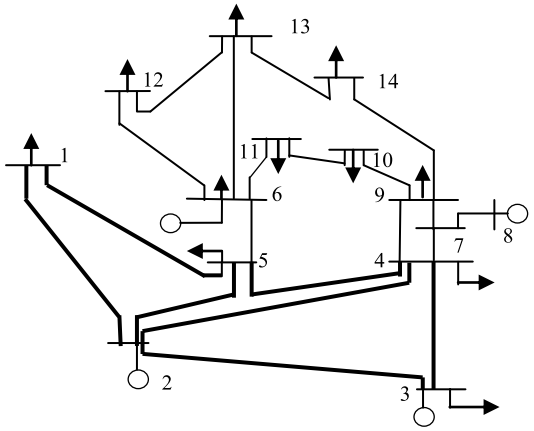

Fig. 3. Case 1.

$$= \begin{bmatrix} \Delta D_1 \\ 0 \\ \Delta D_3 \\ \Delta D_4 \\ \Delta D_5 \end{bmatrix} \qquad -2.265 \le \Delta D_1 \le 2.265$$

$$-3.33 \le \Delta D_3 \le 3.33$$

$$-1.815 \le \Delta D_4 \le 1.815$$

$$-1.14 \le \Delta D_5 \le 1.14$$

$$\Delta\theta_4 = \Delta\theta_5.$$

Solving the above LP, we get the maximum attacking amount of bus 1

$$Q_1 = 2.2650 \text{ MW} > 1.5100 \text{ MW}.$$

Thus, the current searching region is a feasible attacking region as it satisfies the attacking amount requirement. It can be seen that to determine the feasible searching region, an attacker needs to obtain the parameter information of 7 lines marked in bold in Fig. 3, instead that of all 20 lines in the entire power grid.

Solving (30), we get the optimal attacking region which is the same as the feasible searching region and the corresponding false injection data at load buses are

$$\Delta D_1 = 1.5100 \text{ MW};\ \ \Delta D_3 = -2.5748 \text{ MW}$$
$$\Delta D_4 = 1.3814 \text{ MW};\ \ \Delta D_5 = -0.3166 \text{ MW}.$$

2) Case 2: The Attacker Intends to Attack Load Bus 12: The primary attacking region of bus 12 consists of buses 6, 12, 13 and lines 6-12, 6-13, 12-13. The following constraint holds for boundary buses 6 and 13 according to [15, Th. 1]:

$$\Delta\theta_6 = \Delta\theta_{13} = \alpha.$$

Obtain the loads of buses 6, 12, 13 and set the reactances of lines 6-12, 6-13, 12-13 to one and solve the optimization problem (21). Since (21) is feasible and there are 3 lines in the current attacking region, which is less than $K = 10$, we get the initial attacking region, which is the same as the current searching region. We then obtain the true reactances of

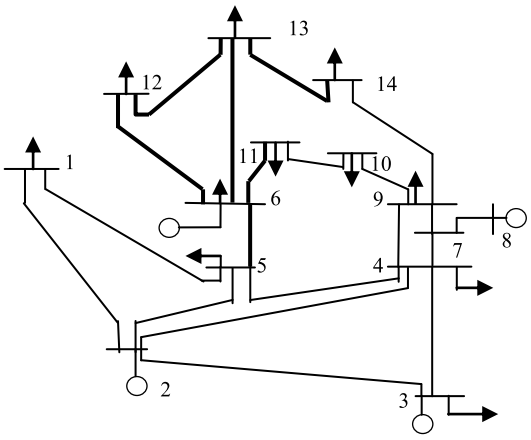

Fig. 4. Case 2.

lines 6-12, 6-13, 12-13 to calculate the maximum attacking amount of bus 12 by solving (30)

$$Q_{12} = 1.3679 \text{ MW} < 1.5000 \text{ MW}.$$

Thus, the initial attacking region does not satisfy the attacking amount requirement and needs to be expanded. Buses 6 and 13 are boundary buses in the initial attacking region, so we add neighboring buses 5, 11, 14 and lines 5-6, 6-11, 13-14 into the initial attacking region to form the new searching region. According to [15, Th. 1], the following boundary condition holds for buses 5, 11, 14, which are the boundary buses in the new searching region:

$$\Delta\theta_5 = \Delta\theta_{11} = \Delta\theta_{14} = \alpha.$$

Obtain the true reactances of the newly added lines 5-6, 6-11, 13-14. Solving (21) again, we get the maximum attacking amount of bus 12

$$Q_{12} = 1.6314 \text{ MW} > 1.5000 \text{ MW}.$$

The attacking amount of bus 12 is increased and satisfies the condition of $Q_{12} > \gamma_{12}$. Thus, the expanded searching region is feasible. We can see that to determine the feasible searching region, an attacker needs to obtain the network parameter information of 6 lines marked in bold in Fig. 4, much less than the number of lines (20) in the entire power grid.

Solving (30), we get the optimal attacking region, which is composed of buses 6, 12, 13, 14 and lines 6-12, 6-13, 12-13, 13-14. Note that the optimal attacking region is only a subnetwork of the feasible searching region with bus 5 and lines 5-6, 6-11 being excluded.

Accordingly, the false injection data at load buses are

$$\Delta D_6 = -0.6000 \text{ MW}; \ \Delta D_{12} = 1.5000 \text{ MW}$$
$$\Delta D_{13} = -0.9169 \text{ MW}; \ \Delta D_{14} = 0.0169 \text{ MW}.$$

3) Verification of the Effectiveness of the Proposed Strategy: Next, we calculate the post-attack power flows using (36) in [15] and compare it with the original power flows. If power flows in the nonattacking region do not change, the proposed method is verified. Table I lists the power flows before and after attacks. The third column represents the original line power flows before attacks, and the last two columns give the line power flows for cases 1 and 2, respectively. The changed power flows are marked in bold. It can be seen that the power flows in the nonattacking region do not change and there are no additional power flows in or out of the attacking region. Thus, the local attacking scheme is successful and will not be detected by the traditional bad data test procedure.

TABLE I
POWER FLOW CHANGES BEFORE AND AFTER ATTACKS

Index	Line	Original Flows(MW)	Case 1 (MW)	Case 2 (MW)
1	1-2	-22.6712	**-23.8647**	-22.6712
2	1-5	7.5712	**7.2547**	7.5712
3	2-3	3.2987	**2.1053**	3.2987
4	2-4	16.6034	16.6034	16.6034
5	2-5	17.4267	17.4267	17.4267
6	3-4	13.2987	**14.6801**	13.2987
7	4-5	2.4373	2.4373	2.4373
8	4-7	9.7629	9.7629	9.7629
9	4-9	5.6019	5.6019	5.6019
10	5-6	19.8352	19.8352	19.8352
11	6-11	-1.6965	-1.6965	-1.6965
12	6-12	9.0144	9.0144	**9.6594**
13	6-13	8.5173	8.5173	**8.4723**
14	7-8	0.0000	0.0000	0.0000
15	7-9	9.7629	9.7629	9.7629
16	9-10	7.6965	7.6965	7.6965
17	9-14	5.5683	5.5683	5.5683
18	10-11	5.1965	5.1965	5.1965
19	12-13	-5.9856	-5.9856	**-6.8406**
20	13-14	-4.5683	-4.5683	**-4.5514**

TABLE II
PERCENTAGES OF FEASIBLE INITIAL ATTACKING REGIONS

System	Percentage			
	$\gamma_b = 0.1$	$\gamma_b = 0.05$	$\gamma_b = 0.025$	$\gamma_b > 0$
IEEE 24	70.59%	82.35%	94.12%	100%
IEEE 30	45.00%	65.00%	80.00%	100%
IEEE 39	47.62%	61.90%	71.43%	100%
IEEE 57	54.76%	73.81%	76.19%	100%
IEEE 118	60.61%	78.79%	88.89%	100%
Polish 2383	60.87%	77.66%	88.00%	100%

B. Verification of Observations 4 and 5

Comparing cases 1 and 2, we find that the initial attacking region obtained using Algorithm 1 could be feasible (case 1) or not feasible (case 2). Next, we want to make further investigation and find the percentage of initial attacking regions that are also feasible. The verifying method is straightforward. Suppose that there are *ND* load buses in a power grid and set $m = 0$. For each load bus b, first determine the initial attacking region by Algorithm 1, then calculate the maximum attacking amount of bus b in the initial attacking region based on true line reactances and increase counter m by one if $Q_b \geq \gamma_b$. Then, the percentage of feasible initial attacking regions is given by

$$p = \frac{m}{ND} \times 100\%.$$

Table II gives the percentages of feasible initial attacking regions for the IEEE 24-bus system, IEEE 30-bus system, IEEE 39-bus system, IEEE 57-bus system, IEEE 118-bus system, and the Polish 2383-bus system [16]. It can be

TABLE III
AVERAGE NUMBER OF LINES IN THE OPTIMAL ATTACKING REGION

System	Percentage			
	$\gamma_b = 0.1$	$\gamma_b = 0.05$	$\gamma_b = 0.025$	$\gamma_b > 0$
IEEE 24	6.06 (20.2%)	4.88 (16.3%)	3.71 (11.0%)	3.29 (11.0%)
IEEE 30	10.60 (25.9%)	7.70 (18.8%)	5.80 (14.2%)	3.60 (8.8%)
IEEE 39	8.52 (18.5%)	6.38 (15.6%)	5.71 (12.4%)	3.86 (8.4%)
IEEE 57	8.40 (10.5%)	5.79 (7.2%)	5.31 (6.6%)	3.29 (4.1%)
IEEE 118	9.09 (4.9%)	6.39 (3.4%)	4.34 (2.3%)	3.00 (1.6%)
Polish 2383	9.98 (0.34%)	6.80 (0.23%)	5.18 (0.18%)	2.56 (0.09%)

observed that the initial attacking regions of about 45% or more load buses have an attacking amount exceeding the required amount when $\gamma_b = 0.1$. As γ_b decreases, more initial attacking regions of load buses are feasible, which indicates that for most load buses, an attacker does not need to expand the initial attacking regions by obtaining the true line reactances of extra lines. Thus, the number of lines whose reactances the attacker must know is minimized. Moreover, if the strict requirement on the attacking amount of load buses is relaxed, i.e., $\gamma_b > 0$, all the initial attacking regions determined by Algorithm 1 are also feasible attacking regions. So, Observations 4 and 5 are verified.

C. Number of Lines to Determine the Optimal Attacking Region

In this section, we investigate the number of lines whose parameter information is needed to determine the optimal attacking region based on the proposed strategy, i.e., the minimum number of lines to launch a successful local false data injection attack without being detected. The average numbers n for different systems are given in Table III. The value in the bracket denotes n as a percentage of the total number of lines. It can be seen that n is much smaller than the total number of lines in a system. Moreover, as the size of a system increases, n remains almost unchanged and accordingly the percentage would decrease. For instance, the value of n falls between 6 and 11 when $\gamma_b = 0.1$, between 4 and 8 when $\gamma_b = 0.05$. When $\gamma_b > 0$, an attacker only needs to obtain the parameters of three lines on the average to attack a load bus. An attacker needs to obtain the parameters of average 20.2% lines to attack a load bus for IEEE 24-bus system when $\gamma_b = 0.1$. However, for the large-scale Polish system, only the parameters of 0.34% lines are needed. In addition, n decreases when the given threshold value γ_b becomes smaller. This is because the attacking amount requirement of a load bus can be satisfied more easily when γ_b gets smaller.

V. CONCLUSION

Cyber security has emerged as a critical issue in smart grid development. In this paper, we proposed the optimal attacking region model under the context of local LR attack. We investigated the topological characteristics of an attacking region and build the corresponding MILP model. Based on the understanding of the topological characteristics of the attacking region, we took the first attempt to propose a strategy to determine the optimal attacking region of a single load bus by obtaining less network information.

As the extension of this paper, we will next explore the strategies of determining the optimal attacking region(s) for multiple load buses. The simplest approach is to determine the optimal attacking region for each load bus independently and then combine the optimal attacking regions of all load buses as the final attacking region. However, this may lead to the unnecessary efforts of obtaining the parameters of more lines. Thus, more effective methods need to be explored in the future. Possible directions are to develop better heuristic rules, consider the connectivity of attacking regions, or adopt distributed attacking schemes and so on. Another extension of this paper is to apply the optimal local attacking model, which is currently based on linear dc state estimation, to nonlinear ac state estimation.

Furthermore, it is expected that this paper will motivate more research in investigating the local attacking mechanisms of an attacker. All of these works will be of great help to develop practical and effective protection strategies and detection methods. As discussed in this paper, it is reasonable to assume that the attacker has a limited capability and can obtain partial network information of a power grid. Hence, if a defender could increase the attacking cost by increasing the minimum number of measurements that needs to be attacked and the amount of topology and parameter information that an attacker must obtain to launch an attack, the damaging effects caused by the attacker can be reduced. Based on the above intuition, one potential solution is to identify the optimal protection strategy that increases an attacker's attacking cost as much as possible by protecting the least number of measurements.

APPENDIX

The bus data of the modified 14-bus system are listed in Tables IV and V.

TABLE IV
LOAD BUS DATA

Index	Bus	Load (MW)
1	1	15.1
2	3	22.2
3	4	12.1
4	5	7.6
5	6	4.0
6	9	2.1
7	10	2.5
8	11	3.5
9	12	15.0
10	13	7.1
11	14	1.0

TABLE V
GENERATOR BUS DATA

Index	Bus	Generation (MW)
1	2	60.0
2	3	32.2
3	6	0.0
4	8	0.0

REFERENCES

[1] H. M. Merrill and F. C. Schweppe, "Bad data suppression in power system static state estimation," *IEEE Trans. Power App. Syst.*, vol. PAS-90, no. 6, pp. 2718–2725, Nov. 1971.

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

[3] O. Kosut, L. Jia, R. Thomas, and L. Tong, "Malicious data attacks on the smart grid," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 645–658, Dec. 2011.

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

[5] 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. 1294–1304, Jul. 2013.

[6] Y. Yuan, Z. Li, and K. Ren, "Modeling load redistribution attacks in power systems," *IEEE Trans. Smart Grid*, vol. 3, no. 3, pp. 382–390, Jun. 2011.

[7] Y. Yuan, Z. Li, and K. Ren, "Quantitative analysis of load redistribution attacks in electric grid," *IEEE Trans. Parallel Distrib. Syst.*, vol. 23, no. 9, pp. 1731–1738, Sep. 2012.

[8] G. Dan and H. Sandberg, "Stealth attacks and protection schemes for state estimators in power systems," in *Proc. IEEE Conf. Smart Grid Commun.*, Oct. 2010, pp. 214–219.

[9] A. H. Mohsenian and A. Leon-Garcia, "Distributed internet-based load altering attacks against smart power grids," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 667–674, Dec. 2011.

[10] M. Ozay, I. Esnaola, F. Vural, S. Kulkarni, and H. Poor, "Sparse attack construction and state estimation in the smart grid: Centralized and distributed models," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 7, pp. 1306–1318, Jul. 2013.

[11] Z. Zhang, S. Gong, A. Dimitrovski, and H. Li, "Time synchronization attack in smart grid: Impact and analysis," *IEEE Trans. Smart Grid*, vol. 4, no. 1, pp. 87–98, Mar. 2013.

[12] S. Mousavian, J. Valenzuela, and J. Wang, "Real-time data reassurance in electrical power systems based on artificial neural networks," *Elect. Power Syst. Res.*, vol. 96, pp. 285–295, Mar. 2013.

[13] M. Ashfaqur-Rahman and H. Mohsenian-Rad, "False data injection attacks with incomplete information against smart power grids," in *Proc. IEEE Conf. Global Commun. (GLOBECOM)*, Anaheim, CA, USA, 2012, pp. 3153–3158.

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

[15] X. Liu and Z. Li, "Local load redistribution attacks in power systems with incomplete network parameters," *IEEE Trans. Smart Grid*, vol. 5, no. 4, pp. 1665–1676, Jul. 2014.

[16] 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.

Xuan Liu received the B.S. and M.S. degrees from Sichuan University, Chengdu, China, in 2008 and 2011, respectively, both in electrical engineering. He is currently pursuing the Ph.D. degree from the Electrical and Computer Engineering Department, Illinois Institute of Technology, Chicago, IL, USA.

His current research interests include smart grid security, operation, and economics of power systems.

Zhen Bao received the B.S. degree from North China Electric Power University, Beijing, China, and the M.S. degree from the Illinois Institute of Technology (IIT), Chicago, IL, USA, in 2007 and 2013, respectively, both in electrical engineering. He is currently pursuing the Ph.D. degree from the Electrical and Computer Engineering Department, IIT.

His current research interests include demand response, operation, and economics of power systems.

Dan Lu received the B.S. degree from North China Electric Power University, Beijing, China, and the M.S. degree from the Illinois Institute of Technology (IIT), Chicago, IL, USA, in 2007 and 2013, respectively, both in electrical engineering. She is currently pursuing the Ph.D. degree from the Electrical and Computer Engineering Department, IIT.

Her current research interests include operation planning, security, and economics of electric power systems.

Zuyi Li (SM'09) received the B.S. degree from Shanghai Jiaotong University, Shanghai, China; the M.S. degree from Tsinghua University, Beijing, China; and the Ph.D. degree from the Illinois Institute of Technology (IIT), Chicago, IL, USA, in 1995, 1998, and 2002, respectively, all in electrical engineering.

He is currently a Professor with the Electrical and Computer Engineering Department, IIT. His current research interests include economic and secure operation of electric power systems, cyber security in smart grid, renewable energy integration, electric demand management of data centers, and power system protection.