Impacts of Bad Data on the PMU Based Line Outage Detection

Xuan Liu, Member, IEEE, Zhiyi Li, Student Member, Zuyi Li, Senior Member, IEEE

Abstract—An increasing number of Phasor Measurement Unit (PMU) have been deployed in power grids to increase the observability. Recent studies have shown that PMU data can be used to detect the outage of lines. On the other side, modern power system becomes more prone to cyber attacks due to the highly integration of information technology and communication network. In this paper, we demonstrated that an attacker can mask the outage of a single line by attacking a set of critical measurements. A mixed integer linear programming model is proposed to minimize the number of attacked measurements. The IEEE 39-bus system is used to demonstrate the masking scheme.

Index Terms—attacking region, false data injection attacks, line outage, power systems.

NOMENCLATURE

\( M \) sufficiently large value for line power flow
\( \varepsilon \) threshold value for \( r \)
\( r \) residual value
\( \tau \) given maximum percentage of change for load measurement attack

\( b, d, i, j \) subscript: index for buses
\( l, k \) subscript: index for lines

\( ND \) number of loads
\( NG \) number of generators

\( S \) set of PMU buses
\( SD \) set of load buses
\( SL \) set of lines
\( SD_{pmu} \) set of buses with PMUs
\( SL_{pmu} \) Set of lines observed by PMUs

\( \Delta D_i \) false data injection into the measurement at bus \( i \)
\( \Delta F_l \) false data injected into the measurement on line \( l \)
\( f_k^b \) power flow of line \( k \) before attacks
\( \Delta f_k \) additional power flow of line \( k \) due to false data injection

\( \sigma_b \) if \( \delta_b = 1 \), then \( \Delta D_b \neq 0 \)
\( \phi_l \) if \( \nu_l = 1 \), then \( \Delta F_l \neq 0 \)

\( B \) bus susceptance matrix
\( B_{out} \) bus susceptance matrix after line outage
\( D \) load vector

\( \Delta D \) false data injection vector into load measurements
\( F', F'' \) power flow of line \( k \) after attacks
\( F_{out} \) physical line flow vector after line outage’
\( \Delta F \) false data vector of line measurements

\( H \) Jacobian matrix
\( p_{pre} \) power injection vector before attacks
\( p_{out} \) power injection vector
\( p_{post,k} \) equivalent power injection vector after line \( k \) outaged without bad data
\( p'_{post,k} \) equivalent power injection vector after line \( k \) outaged with bad data

\( S \) shift factor matrix of the power grid
\( S_k \) the \( k \)-th row of \( S \)

\( U \) bus-generator incidence matrix
\( V \) bus-load incidence matrix
\( W \) bus-line incidence matrix
\( z \) measurement vector
\( \Delta z \) measurement error injected by the attacking vector
\( \theta \) phase angle vector
\( \Delta \theta \) measurement error injected by the attacking vector \( a \)
\( \theta_{pre} \) phase angle vector before attacks
\( \theta_{post,k} \) phase angle vector after line \( k \) outaged without bad data
\( \theta'_{post,k} \) phase angle vector after line \( k \) outaged with bad data
\( \Delta \theta_{pmu} \) calculated phase angle change vector of PMU buses
\( \Delta \theta'_{pmu} \) calculated phase angle vector of PMU buses after line \( l \) is outaged with bad data

Note that \( \Delta \) represents incremental change and symbols in bold represent vectors or matrices. \( \delta, \nu, w, \gamma \) are binary variables.

I. INTRODUCTION

POWER grid, one of critical infrastructures, is the backbone of a nation’s economy and is critical to the homeland security. In particular, the blackouts around the globe in recent years have raised a great concern about the reliable and safe operation of power systems. In fact, some blackouts are triggered by the failures of a small number of components at the initial stage[1]. However, the control center was not aware of the potential risk or even did not detect such failures, thus no responding measures were taken to mitigate the risk. As a result, the initial failures of the components triggered the
The residue $r$ is
\[ r = \| z - H\hat{\theta} \|_2 \]  

(6)

In the bad data test, if the residue is less than a given threshold value, the estimated state \( \hat{\theta} \) is acceptable. Otherwise, there exit false data among the measurements.

\[
\| z_a - H\hat{\theta}_{\text{bad}} \|_2 = \| z + \Delta z - H(\hat{\theta} + \Delta \theta) \|_2 = \\
\| z - H\hat{\theta} - (\Delta z - H\Delta \theta) \|_2 = \| z - H\hat{\theta} \|_2 
\]

(7)

From (7), we can see that if the injection false data vector \( \Delta z \) and the state variation vector \( \Delta \theta \) satisfy

\[
\Delta z = H\Delta \theta 
\]

(8)

The residue \( r \) will not increase, so false data injection attacks on measurements can bypass the residual test.

The disadvantage of the general false data injection model is the lack of considerations of practical conditions of real power systems. For example, a strong mutual communication is usually built between a power plant and control center, so there is a high risk of being detected if an attacker chooses to attack the measurement at a generator bus. Additionally, the control center would doubt the data if the injecting false data is too large since the state estimator has the preknowledge of the load distribution of a power network and can predict loads using load forecasting techniques.

To make the false data injection attack model more practical, Yuan et al. [6] proposed a load redistribution attack model which sets some constraints on the general attack model: 1) The output reading of a generator cannot be altered; 2) The readings of the measurement at a load bus can be attacked within certain ranges.

The mathematical model can be formulations as

\[
\sum_{d=1}^{ND} \Delta D_d = 0
\]

(9)

\[-\tau D_d \leq \Delta D_d \leq \tau D_d (0 < \tau < 1) \]

(10)

\[
\Delta F = -S \cdot V \cdot \Delta D
\]

(11)

Constraint (9) ensures that summation of injection powers at load buses equals to zero since the readings of generators cannot be changed. Constraint (10) limits the attacking amount within a certain range. Constraint (11) constructs the corresponding attacking vector of line measurements.

III. MATHEMATICAL FORMULATION

In this section, we first review the principle of line outage detection using PMU data, and then reveal that the detection approach will fail due to the interruption of bad data injection.

A. Principle of line outage detection

In real power systems, the topology of a power grid is changing due to natural or malicious attacks and economic operations such as line switching. Thus, to monitor the real-time status of the topology of a power network, it is essential for the control center to detect the outages of lines. The status of breakers will be transmitted to the control center. If a line is in service, 1 will be sent; 0 will be sent otherwise.

Before the outage, the phase angle vector is calculated by

\[
\theta_{\text{pre}} = B^{-1}P_{\text{pre}}
\]

and the post-outage phase angle vector is calculated by

\[
\theta_{\text{post}} = B^{-1}P_{\text{post}}
\]

To avoid recalculating the matrix \( B^{-1} \), it was shown that the line outage can be simulated by injecting additional powers \( \Delta p \), \( -\Delta p \) at the terminal buses of the outaged line while keeping the topology of the power network unchanged[19]. That is, the outaged line is assumed to be in service.

The vector \( e \) as follows,

\[
e = \begin{bmatrix}
0 \\
0 \\
\vdots \\
1 \\
\vdots \\
-1 \\
\vdots \\
0
\end{bmatrix}
\]

By doing so, the post-outage power injection vector becomes

\[
P_{\text{post}} = P_{\text{pre}} - e\Delta p
\]

(13)

The additional power injection \( \Delta p \) is calculated by (14)

\[
\Delta p = \frac{-x_k e_j e^T}{\left( (B^{-1})_i + (B^{-1})_{ij} - 2(B^{-1})_{ij} \right) x_k}
\]

(14)

where

\[
\beta = \frac{x_k}{\left( (B^{-1})_i + (B^{-1})_{ij} - 2(B^{-1})_{ij} \right) x_k}
\]

Accordingly, (12) becomes

\[
\theta_{\text{post}} = B^{-1}P_{\text{post}}
\]

(15)

Then, the phase angle changes at PMU buses are calculated by (16)

\[
\Delta \theta_{\text{pmu}} = (\theta_{\text{post}})_{\text{pmu}} - (\theta_{\text{pre}})_{\text{pmu}}
\]

(16)

To detect if there is line outage and which line is disconnected, we assume that line \( l \) is out of service, then we calculate

\[
r = \| \Delta \theta_{\text{m}} - \Delta \theta_{\text{pmu}} \|_1
\]

(17)

where \( \Delta \theta_{\text{m}} \) is the observed phase angle change vector at PMU buses.

Without the interruption of bad data, the residual \( r \) is attributed to the measuring errors \( e \), of sensors. In the normal condition, it is small. Hence, the line that minimizes the value of \( r \) is identified as the outaged line. If the value of \( r \) is large for all the lines, then the control center is reasonable to think that there are no outaged lines. We will show that the detection principle provides a chance for an attacker to confuse the control center by carefully designing the false data.
B. Determining the optimal attacking region

In section, we investigate the principle of making the outage of a single line. That is, when a line is physically disconnected, however 1 will be sent to the control center to represent the line is connected.

As discussed in Section III, in the normal condition and without bad data interruption, the residual \( r \) in (17) will be small. Thus, to mask the outage of a line, the value of \( r \) must be increased to be greater than a threshold value such that the control center will trust the line still being connected.

\[
r = \|\Delta \theta_m - \Delta \theta_{pmu}\|_1 > \varepsilon \tag{18}
\]

Note that in (18), \( \Delta \theta_m \) is based on the actual physical data and consistent with the case that the line is outaged. And \( \Delta \theta_{pmu} \) is estimated using the received data from sensors. Without the interruption of bad data, the small residual is mainly attributed to the random measuring errors. However, if the data are modified to be consistent with the case that the line is connected, then the residual will be increased since \( \Delta \theta_m \) is consistent with the case that the line is disconnected. The phase angle changes of PMU buses are thought to be caused by load variations.

To ensure the injected bad data can avoid being detected by the state estimator, as discussed in [16], constraints (9)-(11) are satisfied to ensure the injected bad data obey KCL, KVL and attacking amount constraints.

The type of topology attacks could bring in serious consequences to the operation of power systems. Especially, a wise attacker choose a best attacking time, for example, when a system is under heavy load level, the outage of a critical line might lead to cascading failures. If the control center can detect the line outage immediately, corresponding measures will be taken to prevent or mitigate the risk. On the contrary, if such an outage is masked by an attacker and the control center has no way to detect the outage of the line, no actions will be taken. Since a DC power system is linear, it obeys the superstition law. If there is false data \( \Delta D \) injected into the power grid, then \( \Delta p \) in (13) becomes

\[
\Delta p' = \frac{-x_k(b_k^2 + \Delta f_k)}{[(b_k^2 - 2)(b_k^2 - 1) - x_k]} \tag{19}
\]

where \( \Delta f_k \) is attributed to the false injection data \( \Delta D \)

\[
\Delta f_k = -S_k.V.\Delta D \tag{20}
\]

So, the equivalent post-outage power injection vector is

\[
P_{postk} = P_{pre} - e\Delta p' \tag{21}
\]

Then, the phase angle vector after line \( k \) is outaged is calculated as

\[
\theta_{postk}' = B^{-1}P_{postk}' \tag{22}
\]

To ensure the constraints of attacking amounts, for the terminal buses of the target line,

\[
-\tau D_i \leq \Delta p' - \Delta D_l \leq \tau D_i \tag{23}
\]

\[
-\tau D_l \leq -\Delta p' - \Delta D_l \leq \tau D_l \tag{24}
\]

Introducing (22) into (23) and (24), which gives

\[
-\tau D_i + \beta f^S_k \leq \beta S_k.V.\Delta D - \Delta D_l \leq \tau D_i + \beta f^S_k \tag{25}
\]

\[
-\tau D_l - \beta f^S_k \leq -\beta S_k.V.\Delta D - \Delta D_l \leq \tau D_l - \beta f^S_k \tag{26}
\]

For the rest load buses, we have

\[
-\tau D_d \leq \Delta D_d \leq \tau D_d \quad \forall d \in SD, d \neq i, d \neq j \tag{27}
\]

The injected line flow vector becomes

\[
\Delta F = S_i(-V_i.\Delta D - e(-\beta f_i^S)) \tag{28}
\]

Substituting (20) into (28), we have

\[
\Delta F = (-S_i.V - \beta S_i.e_i.S_i.V)\Delta D \tag{29}
\]

In (16), since the residual \( r \) due to the measuring errors \( e \) of sensors in normal operation condition is small, similar to [3], we can assume that \( e_r = 0 \). Thus, the observed phase angle differences at PMU buses before and post the line outage can be approximately expressed as

\[
\Delta \theta_m = \Delta \theta_{pmu} = \left(\theta_{postk}\right)_{pmu} - \left(\theta_{pre}\right)_{pmu} \tag{30}
\]

With bad data, the vector of the change in phase angles at PMU buses is calculated as

\[
\Delta \theta_{pmu} = \left(\theta'_{postk}\right)_{pmu} - \left(\theta'_{pre}\right)_{pmu} \tag{31}
\]

According to the principle of line outage detection discussed in section B, to mask the outage of line \( k \), constraint (32) holds

\[
\|\Delta \theta_m - \Delta \theta_{pmu}\|_1 > \varepsilon \tag{32}
\]

Combining (21), (22), (30) and (31), (32) can be expressed by

\[
\|\Delta \theta_m - \Delta \theta\|_1 = \sum_{i \in SL} \sum_{j=1}^{SD} \alpha_{ij} |\Delta D_j| \geq \sum_{i \in SL} \sum_{j=1}^{SD} \alpha_{ij} |\Delta D_j| \tag{33}
\]

where

\[
a = -B^{-1}.V - \frac{-x_i}{(X_{ii} + X_{ij} - 2X_{ij}) - x_i} e_i.S_i.V
\]

Thus, (33) is translated into

\[
\sum_{j=1}^{SD} \sum_{i \in SL} \alpha_{ij} |\Delta D_j| \geq \varepsilon \tag{34}
\]

Or

\[
\sum_{j=1}^{SD} \sum_{i \in SL} \alpha_{ij} |\Delta D_j| \leq -\varepsilon \tag{35}
\]

So, the entire optimization problem is formulated as

\[
\min \sum_{d \in SD} s_d + 2 \sum_{i \in SL} \varphi_i \tag{36}
\]

subject to

\[
\Delta D_d + (\tau D_d) s_d \geq 0 \tag{37}
\]

\[
\Delta D_d - (\tau D_d) s_d \leq 0 \tag{38}
\]

\[
\Delta F_i + M \varphi_i \geq 0 \tag{39}
\]

\[
\Delta F_i - M \varphi_i \leq 0 \tag{40}
\]

\[
\Delta D_d = 0 \quad \forall d \in SD_{pmu} \tag{41}
\]

\[
\Delta F_l = 0 \quad \forall l \in SL_{pmu} \tag{42}
\]

Constraints (9)-(11), (34)

And

\[
\min \sum_{d \in SD} s_d + 2 \sum_{i \in SL} \varphi_i \tag{43}
\]

Constraints (9)-(11), (35)

It is assumed that the power flow of a line is measured in positive and negative directions, so the second term in the objective function is multiplied by 2. Constraints (37)-(38)
count the number of load buses whose power injections are changed. Constraints (39)-(40) count the number of lines whose power flows are modified. Constraints (41)-(42) ensures that if a PMU is installed at a bus, then the power injection at the bus and the power flows of lines connected to the bus cannot be attacked. The optimization problem is a mixed integer linear programming, which can be solved by available commercial solvers, such as Cplex, Gurobi.

IV. CASE STUDY

In this section, we test the masking scheme using the IEEE 39-bus system [20], which is composed of 39 buses and 46 lines as shown in figure 2. For the purpose of illustration, loads at buses 3 and 27 are modified to 722MW and 381MW, respectively. 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.

In this paper we assume that an attacker can obtain the network information of the entire power network. Without loss of generality, we assume that the maximum attacking amount at a load bus is no more than 50% of the load. The mask of the outage of line 25-26 is used to demonstrate the proposed masking scheme.

![Fig. 2 IEEE 39-bus system](image)

We assume that five PMUs are instated at buses 4, 13, 18, 23 and 24, respectively. Once a PMU is installed at a bus, the power injection and currents of branches connected to the buses are measured. Thus the power injection measurements at buses 4, 18, 23, 24 and line flow measurements on lines 4-5, 4-14, 3-4, 10-13, 13-14, 22-23, 23-24, 23-36, 3-18, 17-18 and 16-24 cannot be attacked.

The original phase angle before attacks is calculated by (11)

\[
\begin{bmatrix}
\theta_{18} \\
\theta_{23} \\
\theta_{24}
\end{bmatrix}
= \begin{bmatrix}
3.76^\circ \\
13.99^\circ \\
6.89^\circ
\end{bmatrix}
\tag{44}
\]

The power flow of line 25-26 before attacks is 2.5094 MW, so after line 25-26 is disconnected, according to (14), the equivalent injected powers at buses 25 and 26 are

\[
\Delta P_{25} = -\Delta P_{26} = -265.8MW
\tag{45}
\]

Then, the phase angles at PMU buses become

\[
\begin{bmatrix}
\theta_{18} \\
\theta_{23} \\
\theta_{24}
\end{bmatrix}^{\text{post}}
= \begin{bmatrix}
1.85^\circ \\
5.98^\circ \\
3.76^\circ \\
13.99^\circ \\
6.89^\circ
\end{bmatrix}
\tag{46}
\]

So, the changes in the bus phase angles are

\[
\Delta \theta_m = \begin{bmatrix}
\Delta \theta_4 \\
\Delta \theta_{13} \\
\Delta \theta_{18} \\
\Delta \theta_{23} \\
\Delta \theta_{24}
\end{bmatrix}
= \begin{bmatrix}
0.91^\circ \\
1.01^\circ \\
1.43^\circ \\
1.73^\circ \\
1.72^\circ
\end{bmatrix}
\tag{47}
\]

Without loss of generality, we assume that the minimum phase angle variations for the five PMUs are chosen as a random number between 0 and 0.1. The threshold value \(\epsilon\) is set to 10. Then, solving the optimization problems (36) and (43), we get the false injection data into the measurements at load buses in table 1. The attacker needs to attack at least 31 measurements which include 7 power injection measurements and 24 line flow measurements. The false injection powers at bus measurements are listed in table 1.

**Table 1: False Injection Data at Load Buses**

| Bus | \(\Delta D_L\) (MW) | \(\tau D_L\) (MW) |
|-----|----------------------|-------------------|
| 8   | -261                |                   |
| 15  | 160.00              |                   |
| 20  | 340                 |                   |
| 25  | 112                 |                   |
| 26  | 69.5                | -69.5             |
| 27  | 140.5               |                   |
| 39  | 552                 |                   |

According to (19), the equivalent injected powers at buses 25 and 26 are

\[
\Delta P_{25} = -\Delta P_{26} = -113.71MW
\tag{48}
\]

When the additional powers -131.79MW, 131.79MW are added into buses 25 and 26, the net additional power injections at buses 25 and 26 become -69.5MW and 68.83MW, respectively. As can been seen, all the false data injections at load buses are summed to zero and limited within \([-\tau D_L, \tau D_L]\). For the purpose of false data injection analysis, buses with negative false data injections are treated as generator buses and buses with positive false data injections are treated as load buses.

Then, the phase angles at PMU buses become
\[
\theta_{\text{post}} = \begin{bmatrix}
\theta_4 \\
\theta_{13} \\
\theta_{18} \\
\theta_{23} \\
\theta_{24}
\end{bmatrix} = \begin{bmatrix}
3.83^\circ \\
7.88^\circ \\
5.36^\circ \\
16.23^\circ \\
9.14^\circ
\end{bmatrix} \tag{49}
\]

So, the bus phase angle changes at buses 4, 13, 18, 23, 24 after the bad data injection are

\[
\begin{align*}
\Delta \theta'_{\text{pmu}} &= \begin{bmatrix}
\Delta \theta_4 \\
\Delta \theta_{13} \\
\Delta \theta_{18} \\
\Delta \theta_{23} \\
\Delta \theta_{24}
\end{bmatrix} = \begin{bmatrix}
2.89^\circ \\
2.91^\circ \\
3.03^\circ \\
3.97^\circ \\
3.97^\circ
\end{bmatrix} \\
\end{align*} \tag{50}
\]

Compared (47) with (50), the residual \( r \) is

\[
 r = \| \Delta \theta_{\text{m}} - \Delta \theta'_{\text{pmu}} \|_1 = 10 \geq 10 \tag{51}
\]

The residual \( r \) is greater than or equal to the threshold value 10, so constraints (34) and (35) are verified. Therefore, the defender cannot detect the outage of line 25-26 using the PMU data. To achieve such an attack, at least 7 bus injection power measurements and 24 line flow measurements must be attacked. The attacking region is a connected region, which includes the measurements at buses 8, 15, 20, 25, 26, 27, 39 and the measurements on lines 1-2, 1-39, 2-25, 8-9, 9-39, 15-16, 16-17, 16-19, 17-27, 19-20, 25-26 and 26-27.

**TABLE 2 POWER FLOWS AFTER LINE OUTAGE**

| From bus | To bus | \( F_{\text{out}} \) (MW) | \( \Delta F_1 \) (MW) | \( \Delta F_2 \) (MW) | \( F' \) (MW) | \( F'' \) (MW) |
|---------|-------|-----------------|------------------|-----------------|-------------|-------------|
| 1       | 2     | -2.07           | -1.12            | -3.19           | -3.19       | -3.19       |
| 1       | 39    | 0.66            | 1.12             | 1.78            | 1.78        | 1.78        |
| 2       | 3     | 4.59            | 0.00             | 4.59            | 4.59        | 4.59        |
| 2       | 25    | -4.16           | -1.12            | -5.28           | -5.28       | -5.28       |
| 2       | 30    | -2.50           | 0.00             | -2.50           | -2.50       | -2.50       |
| 3       | 4     | -0.24           | 0.00             | -0.24           | -0.24       | -0.24       |
| 4       | 3     | -2.39           | 0.00             | -2.39           | -2.39       | -2.39       |
| 4       | 5     | -2.10           | 0.00             | -2.10           | -2.10       | -2.10       |
| 5       | 4     | -3.14           | 0.00             | -3.14           | -3.14       | -3.14       |
| 5       | 6     | -5.51           | 0.00             | -5.51           | -5.51       | -5.51       |
| 5       | 8     | 3.42            | 0.00             | 3.42            | 3.42        | 3.42        |
| 6       | 7     | 4.59            | 0.00             | 4.59            | 4.59        | 4.59        |
| 6       | 11    | -3.42           | 0.00             | -3.42           | -3.42       | -3.42       |
| 6       | 31    | -6.69           | 0.00             | -6.69           | -6.69       | -6.69       |
| 7       | 8     | 2.25            | 0.00             | 2.25            | 2.25        | 2.25        |
| 8       | 9     | 0.45            | 1.21             | 1.66            | 1.66        | 1.66        |
| 9       | 39    | 0.38            | 1.21             | 1.59            | 1.59        | 1.59        |
| 10      | 11    | 3.44            | 0.00             | 3.44            | 3.44        | 3.44        |
| 10      | 13    | 3.06            | 0.00             | 3.06            | 3.06        | 3.06        |
| 10      | 32    | -6.50           | 0.00             | -6.50           | -6.50       | -6.50       |
| 12      | 11    | -0.02           | 0.00             | -0.02           | -0.02       | -0.02       |
| 12      | 13    | 0.06            | 0.00             | 0.06            | 0.06        | 0.06        |
| 13      | 14    | 3.00            | 0.00             | 3.00            | 3.00        | 3.00        |
| 14      | 15    | -0.14           | 0.00             | -0.14           | -0.14       | -0.14       |
| 15      | 16    | -3.34           | 1.60             | -4.94           | -4.94       | -4.94       |
| 16      | 17    | 4.60            | -3.29            | 1.36            | 1.36        | 1.36        |
| 16      | 19    | -3.35           | -3.35            | -3.35           | -3.35       | -3.35       |
| 16      | 21    | -0.45           | 0.00             | -0.45           | -0.45       | -0.45       |
| 17      | 18    | 3.97            | 0.00             | 3.97            | 3.97        | 3.97        |
| 17      | 27    | -2.20           | 1.69             | -0.52           | -0.52       | -0.52       |
| 19      | 20    | 1.72            | -3.29            | -1.57           | -1.57       | -1.57       |

In table 2, the third column represents the line power flows after line 25-26 is disconnected. The fourth column gives the injected false data for line flow measurements, which is calculated using (28). The fifth column gives the injected false data for line flow measurements calculated by keeping line 25-26 connected through injecting corresponding powers at the terminal buses. It can be seen that \( F'' \) and \( F' \) have the same entries except the flow of the target line, which shows that the outage of line 25-26 can be simulated by injecting additional 113.71MW, -113.71MW at the terminal buses 25 and 26, respectively. The difference between the last column and the second column is the injected false data for line measurements, which is equal to \( \Delta F \) calculated by (28). Hence, the correctness of the proposed method is verified. In other words, the attacker can design the false data of line measurements using (28) since the changes in line flows can be determined using (28) after \( \Delta D \) is injected.

V. CONCLUSIONS AND FUTURE WORK

Smart grids are subject to the high risk of cyber attacks due to the highly integrations of information and communication technologies. In this paper, with the consideration of PMU installation, we investigate a novel attack model to mask the outage of a single line by injecting false data into a set of measurements. A mixed integer linear programming is formulated to minimize the number of attacked measurements. In [16], we showed that an attacker only needs to obtain the network information of the attacking region instead of that of the entire power grid. This is done by making sure that the variations of phase angles of all boundary buses connected to the same island of the non-attacking region are the same. In [17], we further presented a heuristic algorithm to find an optimal attacking region which requires the reduced network information. In this paper, we assume that the attacker has the full network information of the power network. In the next work, we will investigate the possibility of launching such an attack based on local network information. Additionally, it is expected to develop effective protection strategies against such topology attacks.

REFERENCES
[1] Y. Liu, M. K. Reiter, and P. Ning, “False data injection attacks against state estimation in electric power grids,” In Proceedings of the 16th ACM Conference on Computer and Communications Security, November 2009.

[2] J. E. Tate and T. J. Overbye, “Line outage detection using phasor angle measurements,” IEEE Trans. on Power Systems, vol. 23, no. 4, pp. 1644–1652, Nov. 2008.

[3] H. Zhu and G. B. Giannakis “Sparse overcomplete representations for efficient identification of power line outages”, IEEE Trans. Power Syst., vol. 27, no. 4, pp.2215–2224 2012

[4] Y. Zhao , A. Goldsmith and H. V. Poor “On PMU location selection for line outage detection in wide-area transmission networks”, In Proc. IEEE Power Energy Soc. General Meeting, pp.1 –8 2012

[5] Y. Liu, M. K. Reiter, and P. Ning, “False data injection attacks against state estimation in electric power grids,” In Proceedings of the 16th ACM Conference on Computer and Communications security, November 2009.

[6] Y. Yuan, Z. Li, and K. Ren, “Modeling load redistribution attacks in power systems,” IEEE Transaction on Smart Grid, vol. 2, no. 2, pp. 382–390, Jun. 2011.

[7] A. H. Mohsenian, A. Leon-Garcia, “Distributed Internet-Based Load Altering Attacks Against Smart Power Grids,” IEEE Transactions on Smart Grid, vol. 2, no. 4, pp. 667-674, Dec. 2011.

[8] 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, 2011.

[9] J. Valenzuela, J. Wang, and N. Bissinger, “Real-time intrusion detection in power system operations”, IEEE Transactions on Power Systems, vol. 28, no.2, pp. 1052-1062, May, 2013.

[10] O. Kosut, L. Jia, R. Thomas, and L. Tong, “Limiting false data attacks on power system state estimation,” In Proceedings of Conference on Information Sciences and Systems, pp. 1-6, Mar. 2010.

[11] G. Dan and H. Sandberg, “Stealth attacks and protection schemes for state estimators in power systems,” IEEE Conf. on Smart Grid Communications, pp. 214-219, Oct. 2010.

[12] S. Bi and Y. J. Zhang, “Defending mechanisms against false-data injection attacks in the power system state estimation”, In Proceedings of IEEE Globecom SG-COMNETS, Houston, TX, Dec. 2011.

[13] A. Giani, E. Bitar, M. Garcia, M. McNell, P. Khargonekar and K. Poolla, “Smart grid data integrity attacks,” IEEE Transaction on Smart Grid, vol. 4, no. 3, pp. 1244–1253, Sep. 2013.

[14] G. Hug and J. A. Giampapa, “Vulnerability Assessment of AC State Estimation With Respect to False Data Injection Cyber-Attacks,” IEEE Trans. on Smart Grid, vol.3, no.3, pp.1362-1370, Sept. 2012.

[15] O. Kosut, L. Jia, R. Thomas, and L. Tong, “Limiting false data attacks on power system state estimation,” In Proceedings of Conference on Information Sciences and Systems, pp. 1-6, Mar. 2010.

[16] X. Liu and Z. Li, “Local load redistribution attacks in power systems with incomplete network information,” IEEE Transactions on Smart Grid, vol.5, no. 4, pp. 1665 -1676, Jul. 2014.

[17] X. Liu, Z. Bao, D. Lu and Z. Li, “Modeling of local false data injection attacks with reduced requirement on network Information,” IEEE Transactions on Smart Grid, accepted for publication, 2015.

[18] Z. Li, S.M. Shahidehpour, “Bilevel Model for Analyzing Coordinated Cyber-Physical Attacks on Power Systems,” 2015.

[19] A. J. Wood, B. F. Wollenberg, and G. B. Sheble, Power Generation, Operation and Control, 3rd edition. Wiley-Interscience, 2013.

[20] 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 Transactions on Power Systems, vol. 26, no. 1, pp. 12-19, Feb. 2011.

Xuan Liu (M’14) received the B.S. and M.S degrees from Sichuan University, China, in 2008 and 2011, respectively. He is currently working toward the Ph.D. degree in the Electrical and Computer Engineering Department, Illinois Institute of Technology. His research interests include smart grid security, operation and economics of power systems.

Zhili Li (GS’14) received the B.S. degree from Xi’an Jiaotong University, Xi’an, China, in 2011 and the M.S. degree from Zhejiang University, China, in 2014. He is currently pursuing the Ph.D. degree in the Electrical and Computer Engineering Department, Illinois Institute of Technology. His research interests include cyber-physical power system and power system optimization.

Zuyi Li (SM’09) received the B.S. and M.S. degrees from Shanghai Jiaotong University, Shanghai, China, in 1995 and 1998, respectively, and the Ph.D. degree from the Illinois Institute of Technology (IIT), Chicago, in 2002, all in electrical engineering. Presently, he is a Professor in the Electrical and Computer Engineering Department at IIT. His 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.