LPAttack: Leverage Point Attacks against State Estimation in Smart Grid

Song Tan*, Wen-Zhan Song*, Michael Stewart†, and Lang Tong‡
*Department of Computer Science, Georgia State University, GA, USA
†Department of Mathematics and Statistics, Georgia State University, GA, USA
‡School of Electrical and Computer Engineering, Cornell University, NY, USA
stan,songwz@cs.gsu.edu, mastewart@gsu.edu, ltong@ece.cornell.edu

***Abstract*—A novel class of malicious data attacks, LPAttack, are presented against the state estimation process in Smart Grid. Here LP represents leverage points, which are the outliers in the factor space of the regression model for Smart Grid state estimation. The attacker strategically manipulates the parameter data in Smart Grid to mislead the control center with incorrect system parameter information, such that leverage points are created within the factor space of the state estimation regression model. As a result, the attacker can freely inject arbitrary errors into the meter measurements corresponded with the leverage points, while bypassing the existing bad data detection mechanism. We first introduce the fundamental principles and strategies of launching LPAttack in Smart Grid. Then the potential countermeasure based on robust Schweppe-Huber Generalized-M estimator is proposed. Finally, we evaluate the LPAttack principles and its countermeasure through simulations in IEEE test system, and examine in particular the effect of the attacks on Locational Marginal Prices in real-time pricing power market.**

I. Introduction

Smart Grid is envisioned to improve the efficiency of the legacy power system by integrating cyber infrastructure for sensing, control, computation and communication. State estimation is a key system monitoring process deployed in power control center to estimate the unknown state variables based on meter measurement data, power network topology data and parameter data [1]. The output of state estimation lays the foundation for a series of subsequent critical control processes, such as contingency analysis, security constrained power analysis, and real-time pricing in power market, etc.

Due to the strong dependency on the cyber infrastructure for data collection, transmission and storage in Smart Grid, it becomes more likely for malicious attackers to compromise meters, intercept data, or even gain access to the databases to mislead the state estimation process with tampered data, which could lead to serious unstable power operating conditions or even blackout. Therefore, the data security of state estimation for Smart Grid is a key concern with increasing urgency for cyber security research.

Quite a few of existing works have already addressed the issue. In [2], Liu *et al.* are firstly introduced the concept of false data attacks against Smart Grid state estimation. Assuming the attackers keep the original network topology data and parameter data intact, the authors shows that the attacker can inject errors to the meter measurement data in certain ways while without being detected by the existing bad data detectors. Inspired by the work in [2], extensive further developments are made in [3] [4] [5] [6], etc. Different undetectable attacks and defence strategies are presented. However, all the above works only consider the manipulations of meter measurement data, and the errors introduced by the attacker to the meter measurements have to be in the column space of the Jacobian matrix of the state estimation regression model. In [7], the authors at first introduce another kind of malicious data attack, called topology attack. The key innovation is that the manipulations of power network topology data are also considered.

In this paper, we present a novel class of malicious data attack against Smart Grid state estimation, called LPAttack. Here LP represents *leverage points*, which are the outliers in the factor space of the regression model for state estimation [8]. Different from the previous works, we present a brand new approach to launching undetectable data attacks by strategically manipulating the parameter data, such that leverage points are created within the factor space of the state estimation regression model. The key feature about leverage point is that the residual of the measurement corresponded with the leverage point will be very small even when it is contaminated with a very large error [8]. Based on this key feature, the attacker can freely introduce arbitrary errors into the meter measurements while without being detected by the existing bad data detection mechanisms. The concept of leverage point is not new in power system state estimation, however, as far as we know, we are the **first** to explore the potentials of cyber attacks employing this feature. The key contributions in the paper are:

- We present and rigorously prove the validity of the fundamental principles and strategies for launching LPAttacks.
- We propose a potential countermeasure against the attacks based on robust Schweppe-Huber Generalized-M estimator.
- We evaluate the attacking principles and countermeasure in IEEE test system, and examine in particular the effects of attacks on the real time pricing in power market.

This research is supported by NSF grant (NSF-CPS-1135814) to Sensorweb Research Laboratory at Georgia State University.

978-1-4799-3512-3/14/$31.00 ©2014 IEEE

II. Preliminaries

State estimation: Figure 1 demonstrates the typical state estimation process in control center. State estimation takes three kinds of data as input:

- z: The meter measurement data, including power injections at buses and power flows across branches.
- t: The network topology data, indicating the on/off status of power network switches between buses.
- p: The parameter data, typically including: 1) the branch susceptance data and 2) the variances of meter measurement errors, etc.

Typically, z, t and p are either sent wirely/wirelessly from meters to control center, or kept in databases.

After taking the input, the topology processing and observability analysis process would generate the regression model equation, in which:

- 1) The matrix H depends on the topology data t and the branch susceptance data in p;
- 2) The variances of each meter measurement error e_i in vector e, denoted by σ_i^2, are part of data in p.

Then the weighted least-square state estimator is used to get the best estimates of the unknown state variables x, which are the voltage magnitude and phase angle at each bus.

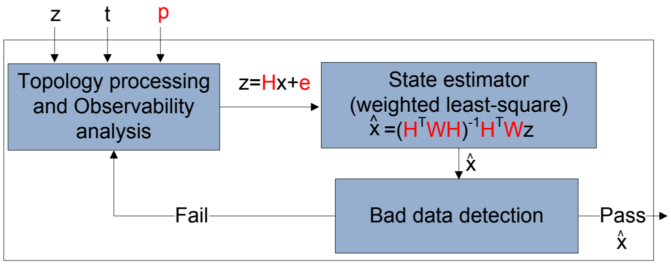
z
t
p
Topology processing and Observability analysis
z=Hx+e
State estimator (weighted least-square)
x̂ =(H^TWH)^-1H^TWz
x̂
Bad data detection
Fail
Pass
x̂

Fig. 1. State estimation process in control center

Mathematically, a precise definition of state estimation is given as follows [1]. Let $x = (x_1, x_2, ..., x_n)^T$ and $z = (z_1, z_2, ..., z_m)^T$ denote state variables and meter measurements, respectively, where n is the number of unknown state variables, m is the number of meter measurements, and $m \geq n$. Further let $e = (e_1, e_2, ..., e_m)^T$ denote meter measurement errors, which are assumed to be normally distributed with zero mean. The state variables are related to the measurements by:

$$z = h(x) + e \tag{1}$$

where $h(x) = (h_1(x_1, x_2, ..., x_n), ..., h_m(x_1, x_2, ..., x_n))^T$, and $E(e) = 0$ and $cov(e) = W$, and W is defined as:

$$W = \begin{bmatrix} \sigma_1^{-2} & 0 & \cdots & 0 \\ 0 & \sigma_2^{-2} & \cdots & \vdots \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & \cdots & \sigma_m^{-2} \end{bmatrix} \tag{2}$$

where σ_i^2 is the variances of e_i.

The state estimation problem is formulated as the following Weighted Least Square (WLS) format:

$$\begin{aligned} \underset{x}{\text{minimize}} \quad & \frac{1}{2} r^T W r \\ \text{subject to} \quad & z = h(x) + r \end{aligned} \tag{3}$$

For state estimation in standard DC power flow [1], the Equation (1) can be represented by a linear regression model:

$$z = Hx + e \tag{4}$$

where H is an $m \times n$ full rank Jacobian matrix of the measurement model. Then the WLS state estimator will give the following solution:

$$\hat{x} = (H^T W H)^{-1} H^T W z \tag{5}$$

Bad data detection: Measurement residuals are employed by the bad data detection techniques in Smart Grid to protect state estimation process against abnormality in measurement data, which are usually caused by nature or faulty sensors. The measurement residual is represented as:

$$r = z - \hat{z} = z - H\hat{x} \tag{6}$$

The objective function for bad data detection is defined as:

$$J(\hat{x}) = \sum_{i=1}^{m} \frac{(z_i - H_i \hat{x})^2}{\sigma_i^2} = \sum_{i=1}^{m} \frac{r_i^2}{\sigma_i^2} \tag{7}$$

where H_i is the ith row of H. Then in the $J(\hat{x})$ test:

$$J(\hat{x}) = \begin{cases} \text{Bad data ,} & \text{if } J(\hat{x}) > \varepsilon \\ \text{Good data ,} & \text{if } J(\hat{x}) \leq \varepsilon \end{cases}$$

where ε is an empirical detection threshold defined in control center. If no bad data is detected, the state estimation resulted $\hat{x}$ would be accepted by the subsequent control processes. Otherwise, an alarm is fired and new data must be incorporated to start over the whole process.

III. LPAttack:Leverage point attack

We assume that the attackers can access and manipulate the data z, t, and p as needed to launch the attacks.

Let $\bar{z} = W^{\frac{1}{2}} \cdot z$, $\bar{r} = W^{\frac{1}{2}} \cdot r$, $\bar{H} = W^{\frac{1}{2}} \cdot H$ and $\bar{e} = W^{\frac{1}{2}} \cdot e$, from (4):

$$\bar{z} = \bar{H} \cdot x + \bar{e} \tag{8}$$

where $E[\bar{e}] = 0$ and $cov[\bar{e}] = I_m$. Then the WLS solution for x in (5) can be rewritten as:

$$\hat{x} = (\bar{H}^T \bar{H})^{-1} \bar{H}^T \bar{z} \tag{9}$$

and the residual,

$$\bar{r} = \bar{z} - \bar{H}\hat{x} = (I_m - K)\bar{z} \tag{10}$$

where I_m is the m dimensional identity matrix and K is defined as:

$$K = \bar{H}(\bar{H}^T \bar{H})^{-1} \bar{H}^T \tag{11}$$

Since K is both symmetric $(K = K^T)$ and idempotent $(K \cdot K = K)$, then K_{ii} can also be written as:

$$K_{ii} = K_{ii}^2 + \sum_{j=1, j \neq i}^{m} K_{ij}^2 \tag{12}$$

It follows from the above equation that $0 \leq K_{ii} \leq 1$.

A. Principles of LPAttack

In the above regression model, the row vector $\bar{H}_i = (\bar{H}_{i1}, \bar{H}_{i2}, ..., \bar{H}_{in})$ defines a factor point in the n dimensional factor space of the regression. The outliers which are far away from the bulk of the factor points in this space are called ***leverage points*** and the corresponding measurements are called ***leverage measurements*** [8]. Geometrically, K_{ii} gives a measure of the distance from the factor point $\bar{H}_i$ to the bulk of the remaining $(m-1)$ factor points. Therefore, a larger K_{ii} would simply indicate a leverage point.

A large value of K_{ii} will also imply that there is a strong influence of the ith measurement z_i on its estimated $\hat{z}_i$, such that the estimated value is essentially determined by its measured value [1]. Thus we call the value of K_{ii} as ***the leverage of measurement*** z_i. As we can see from (10) and (12), as K_{ii} becomes closer to 1, the residual r_i would be very small, no matter how much error is introduced into measurement z_i. Since the bad data detection process depends solely on the measurement residual, it would fail to reject the measurement data even when it is contaminated with a very large error. In other words, **the larger the attackers can increase the value of K_{ii}, the less likely the perturbation of measurement z_i can be detected by the bad data detection process.** This is the key idea of LPAttack. Theorem 1 gives the general relationship between any set of measurements z and the values of K_{ii} when it can pass the $J(\hat{x})$ test.

Theorem 1: Let ε be the threshold and $\sigma_{i=1,...,m}$ be the variances of errors in the $J(\hat{x})$ test. Given any set of measurements z, it is guaranteed to pass the $J(\hat{x})$ test when $\sum_{i=1}^{m}(1 - K_{ii}) \sum_{j=1}^{m}(z_j^2/\sigma_j^2) \leq \varepsilon$.

Proof: From (10), we have,

$$\bar{r_i} = (\sum_{j=1, j \neq i}^{m} -K_{ij}\bar{z}_j) + (1 - K_{ii})\bar{z}_i \tag{13}$$

From Cauchy-Schwarz inequality and (12),

$$\begin{aligned} \bar{r_i}^2 &= ((\sum_{j=1, j \neq i}^{m} K_{ij}\bar{z}_j) + (1 - K_{ii})\bar{z}_i)^2 \\ &\leq [\sum_{j=1, j \neq i}^{m} K_{ij}^2 + (1 - K_{ii})^2][\sum_{j=1}^{m} \bar{z}_j^2] \\ &= [K_{ii} - K_{ii}^2 + (1 - K_{ii})^2][\sum_{j=1}^{m} \bar{z}_j^2] \\ &= (1 - K_{ii})[\sum_{j=1}^{m} \bar{z}_j^2] \end{aligned}$$

Since $\bar{r}_i = r_i/\sigma_i$ and $\bar{z}_i = z_i/\sigma_i$, we can rewrite as:

$$\frac{r_i^2}{\sigma_i^2} \leq (1 - K_{ii}) \sum_{j=1}^{m}(z_j^2/\sigma_j^2) \tag{14}$$

then from $J(\hat{x})$ definition, when

$$\sum_{i=1}^{m}(1 - K_{ii}) \sum_{j=1}^{m}(z_j^2/\sigma_j^2) \leq \varepsilon \tag{15}$$

The measurement z is guaranteed to pass the $J(\hat{x})$ test. ■

Theorem 1 suggests a loosely bound condition for the attacker to launch a successful attack in general. From a pragmatic point of view, it is more worth investigating how the perturbation of a particular measurement z_i, can be marked by the only change of K_{ii}.

Theorem 2: Suppose the original set of measurements z can bypass the $J(\hat{x})$ test. When the measurement z_i in z is perturbed into z'_i by the attacker, there always exists a new value $K'_{ii} \in (K_{ii}, 1]$, such that the new measurement set z' is guaranteed to bypass the $J(\hat{x})$ test.

Proof: Since the original measurements z can bypass the $J(\hat{x})$ test, from (10), we have:

$$J(\hat{x}) = \bar{r}^T\bar{r} = \bar{z}^T(I_m - K)^T(I_m - K)\bar{z} \leq \varepsilon \tag{16}$$

Since matrix $I_m - K$ is idempotent, from the above we have:

$$\bar{z}^T(I_m - K)\bar{z} \leq \varepsilon \tag{17}$$

Let $\tau = \varepsilon - \bar{z}^T(I_m - K)\bar{z}$, $\bar{z'} = W^{\frac{1}{2}} \cdot z'$, $\triangle\bar{z} = \bar{z'} - \bar{z}$, in order for z' to pass the test, it must also satisfy:

$$(\bar{z}^T + \triangle\bar{z}^T)(I_m - K)(\bar{z} + \triangle\bar{z}) \leq \varepsilon \tag{18}$$

Expand (18) and compare with (17), we have:

$$\triangle\bar{z}^T(I_m - K)(\bar{z'} + \bar{z}) \leq \tau \tag{19}$$

Note $\triangle\bar{z}$ only has one nonzero element $\triangle\bar{z}_i$ since only the ith measurement is perturbed. So, the above is equivalent to:

$$\triangle\bar{z}_i[(\sum_{j=1, j \neq i}^{m} -K_{ij}c_j) + c_i(1 - K_{ii})] \leq \tau, \tag{20}$$

where $c_j = z'_j + z_j$, for $j = 1, 2, ..., m$. Combined with (12), it can be seen that for any value of $\triangle\bar{z}_i$, equation (20) is guaranteed to be satisfied when increasing the value K_{ii} to a particular value $K'_{ii} \in (K_{ii}, 1]$. In particular, when $K'_{ii} = 1$, $\triangle\bar{z}_i$ can be infinity. ■

Theorem 2 demonstrates how much the attacker has to increase the value K_{ii} after the perturbation of a single measurement z_i. Note that in cases when the attacker wants to perturb multiple measurements, he would perturb the measurement one at a time and Theorem 2 is applied repeatedly to each targeted measurement with the most updated K_{ii} and z. One last question for the attacker would be how to actually increase the value of K_{ii}. The following theorem gives the answer.

Theorem 3: Let K_{ii} be the ith diagonal element of hat matrix K defined in (11), then,

$$(1-K_{ii})^2 \le \frac{\left\| \begin{bmatrix} \bar{H}_p \\ \bar{H}_f \end{bmatrix} \right\|_2^2}{\| \bar{H}_i^T \|_2^2}$$

where $\bar{H}_i$ is the ith row of $\bar{H}$, and $\bar{H}$ is partitioned as:

$$\bar{H} = [\bar{H}_p \bar{H}_i \bar{H}_f]^T$$

Proof: Since K is both symmetric $(K = K^T)$ and idempotent $(K \cdot K = K)$, then K is the orthogonal projector for $col(\bar{H})$, which is the column space of $\bar{H}$. For any vector v, the projection of v gives the closest vector in $col(\bar{H})$ to v, where closest is measured in Euclidean norm. That is,

$$\| v - Kv \|_2^2 \le \| v - u \|_2^2 \tag{21}$$

for all $u \in col(\bar{H})$.

Let $\hat{y} = Ke_i$ be the projection of e_i on the $col(\bar{H})$, where e_i is the m dimensional vector with ith element equals to 1 and all the other elements are zeros. Then there exists a vector $\hat{t}$ such that

$$\hat{y} = \bar{H}\hat{t} = \begin{bmatrix} \bar{H}_p\hat{t} \\ \bar{H}_i\hat{t} \\ \bar{H}_f\hat{t} \end{bmatrix} \tag{22}$$

Note $\hat{y}$ is the closest vector to e_i in $col(\bar{H})$, and for any t,

$$\| e_i - \bar{H}\hat{t} \|_2^2 \le \| e_i - \bar{H}t \|_2^2 \tag{23}$$

or equivalently,

$$\begin{aligned} &\| \bar{H}_p\hat{t} \|_2^2 + \| \bar{H}_f\hat{t} \|_2^2 + (1-\bar{H}_i\hat{t})^2 \le \\ &\| \bar{H}_p t \|_2^2 + \| \bar{H}_f t \|_2^2 + (1-\bar{H}_i t)^2 \end{aligned} \tag{24}$$

Note that since $\hat{y} = Ke_i$, then with (22), we get $\bar{H}_i\hat{t} = K_{ii}$. Also set $t = \bar{H}_i^T / \| \bar{H}_i^T \|_2^2$, then $(1-\bar{H}_i t)^2 = 0$. From (24),

$$\begin{aligned} (1-K_{ii})^2 &\le \| \bar{H}_p t \|_2^2 + \| \bar{H}_f t \|_2^2 - \| \bar{H}_p\hat{t} \|_2^2 - \| \bar{H}_f\hat{t} \|_2^2 \\ &\le \frac{\| \bar{H}_p\bar{H}_i^T \|_2^2}{\| \bar{H}_i^T \|_2^4} + \frac{\| \bar{H}_f\bar{H}_i^T \|_2^2}{\| \bar{H}_i^T \|_2^4} = \frac{\left\| \begin{bmatrix} \bar{H}_p \\ \bar{H}_f \end{bmatrix} \bar{H}_i^T \right\|_2^2}{\| \bar{H}_i^T \|_2^4} \\ &\le \frac{\left\| \begin{bmatrix} \bar{H}_p \\ \bar{H}_f \end{bmatrix} \right\|_2^2 \| \bar{H}_i^T \|_2^2}{\| \bar{H}_i^T \|_2^4} = \frac{\left\| \begin{bmatrix} \bar{H}_p \\ \bar{H}_f \end{bmatrix} \right\|_2^2}{\| \bar{H}_i^T \|_2^2} \end{aligned}$$

■

From Theorem 3, it can be seen that the attacker can increase the value of K_{ii} by just increasing the l_2-norm of $\bar{H}_i^T$. Since $\bar{H}_i = 1/\sigma_i \cdot H_i$, then mathematically it gives three rules to increase the value of K_{ii}:

- **Rule 1**: Increase the absolute values of elements in H_i.
- **Rule 2**: Decrease the value of σ_i.
- **Rule 3**: Increase the number of non-zero elements in H_i.

B. LPAttack strategies in Smart Grid

In this part, we introduce the specific attacking strategies in Smart Grid by applying the above principles.

1) Attacking power flow measurement

Power flow measurement is the one placed between buses to monitor the power flow across the connecting branch. If an entry z_i of z is the measurement of the power flow from bus k to m, then $z_i = B_{km}(x_k - x_m)$, where B_{km} is the branch susceptance between bus k and m and x_k, x_m are the unknown voltage phase angles at bus k and m. The corresponding ith row of H is:

$$H_i = [0, ..., \overbrace{B_{km}}^{kth \text{ entry}}, 0, ..., 0, \overbrace{-B_{km}}^{mth \text{ entry}}, ..., 0] \tag{25}$$

If the attacker intends to alter the measurement from z_i to z_i' without being detected, he should apply Theorem 2 first to figure out how much he has to increase the value of K_{ii}, then applies rule 1 and rule 2, which requires increasing the value of B_{km} and decreasing the value of σ_i.

2) Attacking power injection measurement

Power injection measurement is placed at bus to monitor the power injection of the particular bus, typically from a load or synchronized generator. If z_i is the measurement of power injection at bus i, it is the sum of all the power flows along incident branches to that bus: $z_i = \sum_{j \in N_i} z_{ij}$, where N_i is the set of buses incident to i, e.g. , $k, m \in N_i$. Therefore, the corresponding ith row of H is the sum of all the row vectors corresponding to the incident branch power flows, which is:

$$H_i = [0, ..., \overbrace{\sum_{j \in N_i} B_{ij}}^{ith \text{ entry}}, ..., \overbrace{-B_{ik}}^{kth \text{ entry}}, ..., \overbrace{-B_{im}}^{mth \text{ entry}}, ..., 0] \tag{26}$$

If the attacker intends to alter the measurement from z_i to z_i' without being detected, he applies Theorem 2 first to figure out how much he has to increase the value of K_{ii}, then he can apply rule 1 and rule 2 in this case. In addition, since the number of nonzero elements is related to the physical connections of buses in power network, rule 3 cannot be applied directly. However, it is still valuable since it suggests that the power injection measurements at buses with more incident branches are more vulnerable since they already have a large leverage in normal condition.

C. Remarks

Several facts are worth pointing out from the above analysis. First, since σ_i is the standard deviation of measurement error e_i, a smaller σ_i indicates a higher accuracy of the measurement z_i. This implies that high accuracy measurement is more likely to become a leverage point and attacking a higher accuracy device will actually have better chance of success. Second, increasing the susceptance of branches should be the first choice of the attacker since it can affect the branch flow measurement and the power injection measurements at incident buses simultaneously. Third, the existences of leverage points in actual power system are very common. For instance, the IEEE 118-bus system has 7.2% of branches with relatively large susceptance(13 over 179) and 28% of buses with at least 4 incident branches (33 over 118) [8]. This suggests that even without the explicit creations of leverage points, the attacker can still launch LPAttack against the corresponding measurements.

IV. Countermeasure

Since all the attacking strategies are based on the creation of leverage points, the straightforward countermeasure would be first evaluating the leverages of measurements to identify leverage points, then discard corresponding measurements before entering WLS state estimator. However, since the ubiquitous existence of leverage points in power system and the leverage measurements could be good when there is no cyber attacks, the above approach would destroy a large amount of useful information and could even make the system unobservable. Therefore, a better solution should be replacing the WLS with a more robust state estimator, which is designed to automatically detect leverage points and suppress the influence of corresponding measurements on the state estimation.

Inspired by the works in [9] [10], we present the countermeasure based on the robust Schweppe-Huber Generalized-M (SHGM) estimator. We modified SHGM such that it possesses good robustness and efficiency against leverage-point attacks. ω_i is specifically designed as the penalty factor to suppress the effects of leverage measurements. The details are as follows:

$$\begin{array}{ll} \underset{x}{\text{minimize}} & \rho(r) = \sum_{i=1}^{m} \rho(r_i) \\ \text{subject to} & z = h(x) + r \end{array}$$

where $z, h(x)$ are the same as in (1), and $\rho(r_i)$ is a function of the measurement residual r_i, which is defined as:

$$\rho(r_i) = \begin{cases} \frac{1}{2} r_i^2/\sigma_i^2 & |r_i/\sigma_i| \le a \cdot \omega_i \\ a \cdot \omega_i |r_i/\sigma_i| - \frac{1}{2} a^2 \cdot \omega_i^2 & otherwise \end{cases}$$

where a is a constant ranging from 1 to 3 and ω_i is defined as:

$$\omega_i = \min\{1, [\frac{1 - K_{ii}}{K_{ii}}]\} \tag{27}$$

Note that when a is infinity, the SHGM is equivalent to WLS.

We propose a solution algorithm based on numerically stable iteratively re-weighted least squares method [11]. Writing the KKT necessary conditions for a minimum of $\rho(r)$:

$$\frac{\partial \rho}{\partial x} = \frac{\partial \rho}{\partial r} \cdot \frac{\partial r}{\partial x} = 0 \Rightarrow \sum_{i=1}^{m} \frac{\partial \rho}{\partial r_i} \cdot \frac{\partial r_i}{\partial x} = 0$$

$$\Rightarrow \sum_{i=1}^{m} \Upsilon(r_i) \cdot H_i = 0 \Rightarrow \sum_{i=1}^{m} \frac{\Upsilon(r_i)}{r_i} \cdot r_i \cdot H_i = 0$$

where $\Upsilon(r_i) = \frac{\partial \rho}{\partial r_i}$. Write the above in matrix form, we have:

$$H^T \cdot Q \cdot r = 0 \tag{28}$$

where Q is a m dimensional diagonal matrix and $Q_{ii} = \frac{\Upsilon(r_i)}{r_i}$, defined as:

$$Q_{ii} = \begin{cases} \frac{1}{\sigma_i^2} & |r_i/\sigma_i| \le a \cdot \omega_i \\ \frac{a \cdot \omega_i}{r_i \sigma_i} \cdot \text{sign}(r_i) & otherwise \end{cases} \tag{29}$$

Also, from the first order Taylor approximation, we have:

$$h(x) \approx h(x^k) + H \cdot \triangle x^k \tag{30}$$

where k means the kth iteration. Since $r = z - h(x)$, $r^k = z - h(x^k)$, combined with (28), we get the kth iteration equation:

$$H^T \cdot Q \cdot H \triangle x^k = H^T \cdot Q \cdot r^k \tag{31}$$

Note that matrix Q is keeping updated based on the residual r of current iteration. Given an initial guess, equation (31) would generate the final solution.

V. Evaluation

We evaluate the proposed attacking strategy and countermeasure using IEEE 14 test system in Figure 2. It is provided with 12 power injection measurements and 13 power flow measurements in normal steady state. In the following, IN i denotes a power injection measurement at Bus i and FL $i-j$ denotes a power flow measurement from Bus i to Bus j. We extract configurations and parameters of the IEEE test systems from MATPOWER.

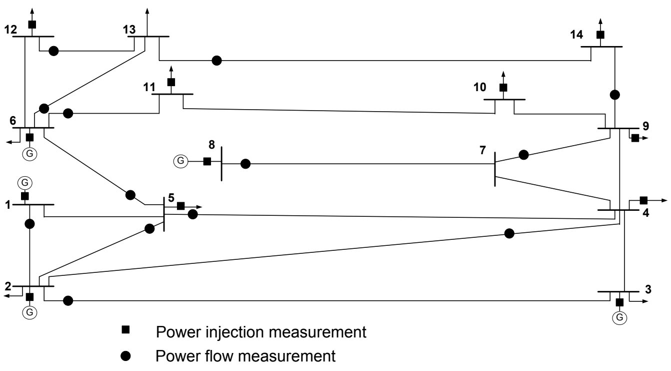

Fig. 2. IEEE 14 bus test system

We first investigate the LPAttack principle in Theorem 2 by demonstrating the relationship between the perturbation of power measurement z_i and the corresponding required minimum increase of K_{ii}. Table I lists the results for several chosen power measurements in IEEE 14 test system. Note $\triangle z_i = \mid z_i' - z_i \mid$ and $\triangle K_{ii} = K_{ii}' - K_{ii}$. $\triangle z_i$ is set to be $0.5, 1, 2,$ respectively. All numerical values of the measurements are in per-unit system with base value 100MVA(pu).

TABLE I
Leverage-Point Attack in IEEE 14 bus system

Meas.	IN1	FL1-2	IN4	IN5	IN6	FL4-5	FL5-6
Normal z_i	125.48	84.70	-27.39	-4.36	-6.42	-35.38	24.52
Original K_{ii}	0.3969	0.2171	0.6043	0.5536	0.5902	0.2179	0.1967
$\triangle K_{ii}(\triangle z_i$=0.5)	0.0637	0.0413	0.0140	0.0053	0.0034	0.0181	0.0126
$\triangle K_{ii}(\triangle z_i$=1)	0.1275	0.0864	0.0283	0.0101	0.0070	0.0364	0.0254
$\triangle K_{ii}(\triangle z_i$=2)	0.2553	0.1733	0.0567	0.0319	0.0151	0.0738	0.0518

The results from Table I imply some interesting facts. First, we discover that in general, when the original magnitude of measurement is large, the corresponding required $\triangle K_{ii}$ is relatively large. This indicates that the attack against measurements with smaller magnitude is easier to succeed. Second, when the original value of K_{ii} is large, such as IN4 and IN5, the perturbations of corresponding measurements only require small increase in K_{ii}. This suggests that the attacks against measurements with larger K_{ii} are more prone to success.

Next we will study how the changes in parameters of branch susceptance and measurement error variances will affect the leverages of measurements. Figure 3 gives the result for IN5.

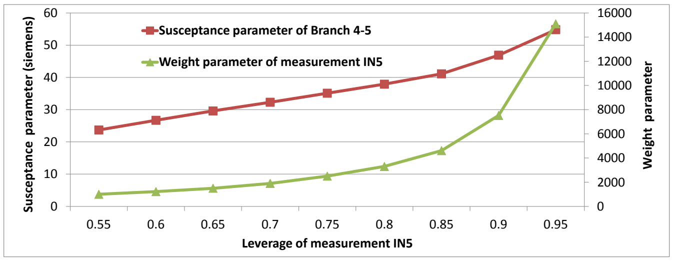

Fig. 3. Relations between leverage of IN5 and value of parameters

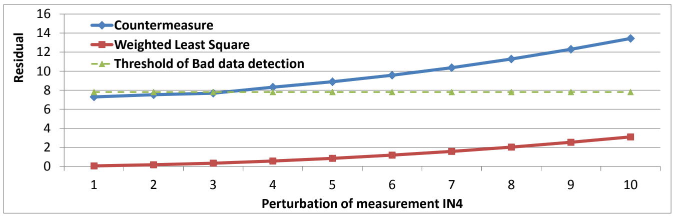

Fig. 4. Residual in conventional WLS and our proposed countermeasure

Figure 4 shows the residuals after measurement perturbation in both WLS and our countermeasure. We can see that the residual in countermeasure is significantly larger than in WLS and can fire the bad data detection alarm correspondingly in most cases.

Finally, the effects of LPAttacks on power market, particularly on the Locational Marginal Price (LMP), are examined. LMP is the core variable in market operations and obtained through the real-time pricing models. The real-time pricing models are built on the power flow measurements given by the state estimation process, thus our proposed leverage-point attacks would directly affect the LMPs. We adopt the Ex-post pricing model in [12] and conduct the sensitivity analysis of LMP at each of the 14 buses with respect to perturbations in different power flow measurements. Figure 5 shows the LMP sensitivities of all 14 buses with respect to the changes in three measurements: IN1, IN4 and FL5-6. The unit on vertical axis is (\$/MWh)/(puMVA). We can see that the perturbation in measurements would have greater impact on the LMPs of nearby buses than other buses. For example, perturbation of IN4 has larger impact on LMPs of bus 4,5 and almost no impact on bus 13,14, either positive or negative.

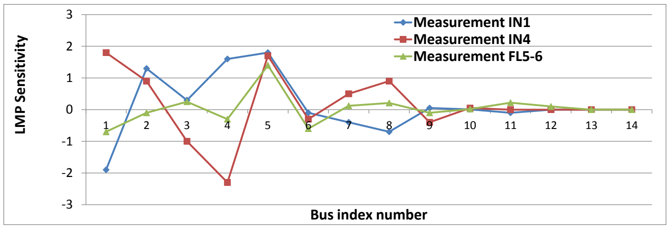

Fig. 5. LMP sensitivities of all buses with respect to measurements

VI. Conclusion and Future Work

In this paper, we present and rigorously prove the validity of the principles and strategies of LPAttacks, the novel data integrity attacks against state estimation in Smart Grid. Countermeasure based on robust state estimation is proposed. Our current attacking principles require the attacker to have a global knowledge of the targeting Smart Grid system. Future work would explore the possibility of conducting attacks only using local information. Meanwhile, potential countermeasures based on secure meter placement would also be studied.

References

[1] A. Abur and A. Expósito, *Power System State Estimation: Theory and Implementation*, 2004.

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

[3] O. Kosut, L. Jia, R. Thomas, and L. Tong, “Malicious data attacks on smart grid state estimation: Attack strategies and countermeasures,” in *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*, 2010, pp. 220–225.

[4] S. Cui, Z. Han, S. Kar, T. Kim, H. Poor, and A. Tajer, “Coordinated data-injection attack and detection in the smart grid: A detailed look at enriching detection solutions,” *Signal Processing Magazine, IEEE*, vol. 29, no. 5, pp. 106–115, 2012.

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

[6] Y. Huang, M. Esmalifalak, H. Nguyen, R. Zheng, Z. Han, H. Li, and L. Song, “Bad data injection in smart grid: attack and defense mechanisms,” *Communications Magazine, IEEE*, vol. 51, no. 1, pp. 27–33, 2013.

[7] J. Kim and L. Tong, “On topology attack of a smart grid: Undetectable attacks and countermeasures,” *Selected Areas in Communications, IEEE Journal on*, vol. 31, no. 7, pp. 1294–1305, 2013.

[8] L. Mili, V. Phaniraj, and P. Rousseeuw, “Least median of squares estimation in power systems,” *Power Systems, IEEE Transactions on*, vol. 6, no. 2, pp. 511–523, May 1991.

[9] L. Mili, M. Cheniae, N. S. Vichare, and P. Rousseeuw, “Robust state estimation based on projection statistics [of power systems],” *Power Systems, IEEE Transactions on*, vol. 11, no. 2, pp. 1118–1127, May 1996.

[10] R. A. S. Benedito, L. F. C. Alberto, N. G. Bretas, and J. B. A. London, “Power system state estimation: Undetectable bad data,” *International Transactions on Electrical Energy Systems*, 2013.

[11] P. J. Green, “Iteratively reweighted least squares for maximum likelihood estimation, and some robust and resistant alternatives,” *Journal of the Royal Statistical Society. Series B (Methodological)*, vol. 46, no. 2, pp. 149–192, 1984.

[12] T. Zheng and E. Litvinov, “On ex post pricing in the real-time electricity market,” *Power Systems, IEEE Transactions on*, vol. 26, no. 1, pp. 153–164, Feb 2011.