# On the Nonlinearity Effects on Malicious Data Attack on Power System

Liyan Jia, Robert J. Thomas, and Lang Tong
School of Electrical and Computer Engineering
Cornell University
Ithaca, NY 14853, USA
Email:{lj92,rjt1,lt35}@cornell.edu.

***Abstract*—There has been a growing literature on the malicious data attack (or data injection attack) on power systems. Most existing work focuses on the DC (linear) model with linear state estimators. This paper examines the effects of nonlinearity in the power systems on the effectiveness of malicious data attack on state estimation and real-time market. It is demonstrated that attack algorithms designed for the DC model may not be effective when they are applied to nonlinear system with nonlinear state estimators. Discussion and experiments results about nonlinearity are provided.**

***Index Terms*—State Estimation, Malicious Data Attack, Bad Data Detection, Electricity Market, Nonlinear System**

## I. Introduction

### A. Background

Sophisticated cyber infrastructures are being integrated into power system operations. With the advanced development of sensing, communications, and actuation technology, future smart grid can provide more reliable real-time control, more flexible demand options, and more efficiency to the system operation.

However, the increasing reliance on networking for wide area situation awareness comes with the risk of cyber attack through the information network for the grid. An adversary may break into the communication network, obtain vital system information, and launch intelligent attacks that can influence covertly the real-time operation of the power system. While there is no publicized incidents of such attacks, it is of significant value to assess the potential impacts of such attacks. Such analysis may also reveal the vulnerability of the network topology, the inadequacy of meter placement, and potential security enhancement solutions. North American Reliability Council (NERC) also publishes its Critical Infrastructure Protection (CIP) requirements to guide the regulated entity to secure the electric system operation [1].

Since first published paper on the potential of data attack in [2], there has been considerable interests on this subject. The properties of the sensitivity matrix has been examined along with intelligent attacking strategies and counter measures have been proposed [3], [4], [5], [6]. However, an important and nontrivial simplification in existing analysis is the use of simple DC model. Such an approach, though significantly simplifying the analysis, may not accurately characterize the effect of attacks. For example, the rank condition of the sensitivity matrix plays a crucial role in most linear analysis. For nonlinear system, no single rank condition can capture all operating conditions. Also, the linear model makes certain strategies unnecessary thus potentially masks certain more insidious attacks.

Two important usages of the real-time state estimation are estimating the state itself [3] and clearing the real-time electricity market price[7]. If the attacker can alter the measurements and affect indirectly state estimates, the adversary can influence the decision by the system operator and potentially profit in the real-time market. Perhaps more importantly, with more active demand side participation, the price changes caused by an adversary potentially can trigger instability as generators react to price changes.

### B. Summary of Results

In this paper, we examine system nonlinearity and the use of nonlinear state estimation on the effectiveness of malicious data attack. To our knowledge, this analysis is the first of this kind in the literature. We demonstrate that near optimal strategies designed for the linear model are not necessarily effective under the nonlinear system model, even if the attacker tracks the factor matrix. The interpretation of this result is twofold. On the one hand, strategies developed using simplifying linear assumption are not effective if applied directly, and the nonlinearity of the power system seems to provide a certain robustness against such attacks. On the other hand, the results presented here should perhaps not be misconstrued as data attacks are ineffective in general. A more appropriate interpretation is that the linear assumption may lead to incomplete and possibly misleading conclusion on the potential risks of data attack.

This work is supported in part by the NSF TRUST (The Team for Research in Ubiquitous Secure Technology) center under award CCF-0424422, the National Science Foundation under Grant CNS-1135844 and DoE CERTS research program.

### C. Related work

Although the detection of bad data is a classic subject, see [8] and references therein, the problem of malicious data attack and its detection has only attracted attention recently, due in large part by the work of Liu, Reiter and Ning [9]. They have shown that, by compromising enough meters, the adversary can perturb the state estimate arbitrarily in some subspace. Kosut *et al.* found that the condition for the existence of such attacks is equivalent to the network observability condition [10], and a graph theoretic approach is developed to characterize the so-called *security index*—the smallest set of attacked meters that will cause unobservability [3]. When the attacker has only limited access to meters in the weak attack regime, algorithms for detecting malicious attack have been considered [10].

As a counterpart, the detection schemes for malicious attack are also proposed. [3] shows that Generalized Likelihood Ratio Detector performs much better than the traditional two-norm detector and maximum residue detector. [5] points out that in order to avoid being attacked by unobserved attack vectors, a set of basic measurements must be protected.

The attack problem in electricity market was first studied in [11], [6]. In [6], the authors use a heuristic way to find the profitable attack in virtual transaction. [7] points out the idea of price region and formulates an optimization problem to gain profit in real-time market, considering the price and estimated generation level at the same time.

All the papers above fall into the DC network assumption, even though they may start from a nonlinear model. In essential, the power system is nonlinear, and the modern nonlinear state estimation methods are efficient and widely used in practice [8]. So how these algorithms perform in a nonlinear setting is an interesting topic to study.

The structure of the rest of the paper is as follows. In Section (II), we will set up the system model and the attack framework. Both nonlinear and linear models are presented, and the difference between the two is stressed. In Section (III), we briefly describe two applications of the attack, to disturb the state estimates and to change real-time electricity market price. The optimal strategies for attack under DC model are shown. Then we discuss the nonlinearity issue in Section (IV). We try to explain why it is a different story if the model is nonlinear rather than linear. Section (V) gives the simulation result based on IEEE 14bus system, and conclusion is in Section (VI)

## II. System and attack models

### A. System model

Consider a standard power system model with $n$ buses. At bus $i$, the voltage is $V_i = |V_i|e^{j\delta_i}$, where $|V_i|$ is the voltage magnitude and $\delta_i$ is the phase. The network state is given by the bus voltages, $V = (V_1, V_2, ..., V_n)$. We can define two real vectors, $X_v = (|V_1|, ..., |V_n|)$ and $X_\delta = (\delta_1, ..., \delta_n)$, and form the real state vector $X = (X_\delta^T, X_v^T)^T$. Note the entry of $X_\delta$ corresponding to the reference bus can be removed. Then $X$ has $2n-1$ dimensions.

Let $Z$ be the $k$-dimension measurement vector that includes a subset of power injection, power flow, voltage magnitude, PMU value, etc. as its entries. The measurement model is given by

$$Z = h(X) + W \tag{1}$$

where $h : \mathcal{R}^{2n-1} \rightarrow \mathcal{R}^k$ is the measurement function for a network with $n$ nodes and $k$ meters, and $W$ is the additive Gaussian noise, with covariance matrix, $R$.

For lossless power network (assuming the admittance in the network is zero everywhere), the measurement model can be reduced to DC model, given by

$$\tilde{Z} = \tilde{H}X_\delta + \tilde{W} \tag{2}$$

where $\tilde{Z}$ is the part in $Z$ corresponding to real values (such as, real injections, real flows), $\tilde{H}$ is the sensitivity matrix, and $\tilde{W}$ is the corresponding measurement noises, with covariance matrix $\tilde{R}$.

Linearization, on one hand gives us much convenience for analysis and computation, on the other, brings lots of inaccuracy into the result. Currently, most of the research papers of attack problem are based on the DC model, regardless what the system parameters are. In this paper, we want to emphasize the importance of nonlinearity, and what is the effect of neglecting nonlinearity.

### B. State estimation and bad data detector

One simple way to do the state estimation is to find the state minimizing the weighted square error. The estimated state is given by

$$\hat{X} = \arg\min_X (h(X) - Z)^T R^{-1}(h(X) - Z). \tag{3}$$

To find the solution, we need to use Newton-Raphson iteration until the result converges. This method is quite time consuming and does not guarantee convergence to the global optimal value. But in general, it works well. For simplicity, we will use it to get our simulation results.

If we approximate the system by the DC model, then the WLS (Weighted Least Square) estimation of the state has a simple form as below,

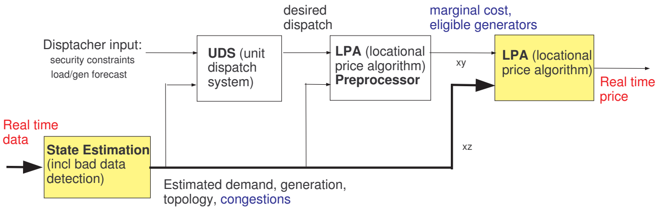
$$\hat{X_\delta} = K\tilde{z}, \quad K \stackrel{\Delta}{=} (\tilde{H}^T\tilde{R}^{-1}\tilde{H})^{-1}\tilde{H}^T\tilde{R}^{-1}, \tag{4}$$

Sometimes, bad data appears when errors occur due to meter malfunctions, bad communications, topological changes, etc. Bad data detection determines if some of the $Z_i$'s are caused by bad data. Once detected, bad data can be removed from the actual state estimation.

A general approach for bad data detection is to compute the residue after state estimation. Given the values of measurements and corresponding estimated state, $Z$ and $\hat{X}$, the residue is given by

$$r = Z - h(\hat{X})$$

Fig. 1: PJM real-time LMP model


Disptacher input:
security constraints
load/gen forecast
UDS (unit dispatch system)
desired dispatch
LPA (locational price algorithm) Preprocessor
marginal cost, eligible generators
xy
LPA (locational price algorithm)
Real time price
Real time data
State Estimation (incl bad data detection)
xz
Estimated demand, generation, topology, congestions

In DC model, the mapping from measurement $Z$ to residue $r$ has a close form solution as below

$$r = \tilde{Z} - \tilde{H}\hat{X}_\delta = G\tilde{Z}, \quad G \stackrel{\Delta}{=} I - \tilde{H}(\tilde{H}^T\tilde{R}^{-1}\tilde{H})^{-1}\tilde{H}^T\tilde{R}^{-1}.$$

The two-norm residue detector $\delta$ is a threshold detector of $r$:

$$\delta(z) = \begin{cases} 1 & \text{if } ||r||^2 > \tau \\ 0 & \text{if } ||r||^2 \leq \tau \end{cases} \tag{5}$$

where $\tau$ is the threshold calculated from a certain false alarm probability. In DC model, according to [12], it is shown that if $\tilde{W}$ is normal, $r$ has a $\chi^2$-distribution with $\tilde{k} - n + 1$ degrees of freedom, where $\tilde{k}$ and $n - 1$ are the row and column dimensions of $\tilde{H}$ respectively.

### C. Electricity market operation

One of the important applications of state estimation is clearing the real-time price in electricity market. Nowadays, the deregulated electricity market in the U.S. consists of two components, a day-ahead market and a real-time market. In the day-ahead market, given the load forecast $L$, an optimal power flow (OPF) problem is solved under the security constraint.

The solution $P^*$ of the OPF is called the *economic dispatch*. The locational marginal price (LMP) is defined as the cost of supplying an additional MW of load at a particular location.

As for the real-time market, fig. (1) shows the PJM real-time LMP model [13] with four main parts, State Estimator (SE), Unit Dispatch System (UDS), Locational Price Algorithm (LPA) and LPA preprocessor. State estimator takes the real-time measurements to make state estimate. UDS makes the real-time re-dispatch for the next 5 minutes according to the current system state. LPA preprocesser takes the result of SE and UDS, generating the available set of generators and their real-time offer in real-time LMP calculation. For simplicity and tractability, we only consider the the effect of state estimator on real-time LMP. We assume UDS doesn't execute the real-time re-dispatch and LPA preprocesser always gives the same set of available generators in real-time and the same real-time offer.

The function of the LPA is to determine the real-time price in every bus. An ex-post formulation (adopted by PJM, ISO-NE, and etc.) is used to solve the following incremental linear programming problem [13],

$$\begin{array}{ll} \text{minimize} & \sum C_i \Delta P_i - \sum C_j \Delta L_j \\ \text{subjcet to} & \sum \Delta P_i = \sum \Delta L_j \\ & \Delta P_i^{\min} \leq \Delta P_i \leq \Delta P_i^{\max} \\ & \Delta L_j^{\min} \leq \Delta L_j \leq \Delta L_i^{\max} \\ & \sum_i A_{ki}\Delta P_i + \sum_j A_{kj}\Delta L_j \leq 0, \text{for all } k \in \hat{\mathcal{C}} \end{array}$$

where $A_{ki}$ is the shift factor of branch $k$ to bus $i$. The set $\hat{\mathcal{C}}$ is the set of estimated congested lines on which the estimated flows are equal or above the flow limits. We call $\hat{\mathcal{C}}$ as congestion pattern in the following discussion. Since the estimated flows are determined by the state estimate, the estimated congested pattern $\hat{\mathcal{C}}$ is also a function of the state estimate. In practice, the upper and lower bound of $\Delta p_i$ are chosen as 0.1MW and -2MW [14].

The real-time LMP is calculated as

$$\hat{\lambda}_i := \hat{\lambda} - \sum_{j \in \hat{\mathcal{C}}} A_{ji}\hat{\mu}_j \tag{6}$$

where $\hat{\lambda}$ and $\hat{\mu_j}$ are the dual variable corresponding to the linear constraint and line flow constraints, respectively.

Since the state estimation is the result of real-time measurement values, the real-time price is naturally a function of meter values, which can be affected by the attack scheme introduced in the next subsection.

### D. Attack model

Assume there exists an adversary who has access to a subset of the measurement values in real-time operation. Denote the set of meters that can be observed in real-time as $\mathcal{B}$, the set that can be manipulated in real-time as $\mathcal{A}$. We call $\mathcal{B}$ and $\mathcal{A}$ as observation set and attack pattern respectively. Additionally, we take a strong assumption that the adversary knows exactly the topology and system parameters of the system. Then based on the prior knowledge of the operating state and the real-time observation $Z_o$, the adversary can inject an attack vector, $A$ into the system. Note that $A$ has only nonzero values on the set of $\mathcal{A}$. The attack model can be represented by

$$Z_a = h(X) + W + A(Z_o)$$

Here, we use $A(Z_o)$ to emphasize that the attack vector is indeed a function of real-time observation.

Usually, the goals of the adversary may include disturbing the system (enlarging the mean square error of estimated state), making profit (disturbing the price in real-time market), and so on. However, due to the existence of the bad data detector, the adversary faces trade-off between achieving the goals and avoiding being detected, especially when the adversary knows only part of the measurement values or no real-time information at all.

To the control center, the measurement data received is $Z_a$. Then the state estimation is made based on this attacked data, and also the residue bad data detector. If the attack vector triggers the bad data detector, the system operator will check the system manually. We simply assume the attack attempt fails in this case.

## III. Attack strategy for the adversary under DC model

### A. How to disturb the state estimation

The following attack strategy first appeared in [3]. Now we apply the strategy to the case that the adversary may have access to part of the real-time measurement values. With this additional information, the attack vector now is a function of the real-time observation values.

In this section, we assume the system model is DC. Also, by historical data, the system state follows a Gaussian distribution, $X_\delta \sim \mathcal{N}(X_0, \Sigma_x)$, which is known to the adversary.

First, let's set up the goal of the adversary. Given the observation $Z_o$, under the existence of the attack vector $A$, the conditional MSE(Mean Square Error) of the state estimation is

$$\begin{aligned}\mathbb{E}[\|\hat{X}_\delta - X_\delta\|^2|Z_o] &= \mathbb{E}[\|K(\tilde{H}X_\delta + W + A) - X_\delta\|^2|Z_o]\\ &= \mathbb{E}[\|K\tilde{W} + KA\|^2|Z_o]\end{aligned} \tag{7}$$

In order to disturb the system operation, the adversary can set the goal as maximizing this conditional MSE, subject to the detection probability constraint. Then, we want to examine the detection part. After attack injection, the conditional expected squared value of the residue vector with attack, $r_a$, can be represented as,

$$\begin{aligned}\mathbb{E}[\|r_a\|^2|Z_o] &= \mathbb{E}[\|GZ_a\|^2|Z_o]\\ &= \mathbb{E}[\|G\tilde{W} + GA\|^2|Z_o]\end{aligned} \tag{8}$$

For a specific attack pattern $\mathcal{A}$, let $\Gamma(\mathcal{A})$ denote the set of attack vectors that have nonzero values only on $\mathcal{A}$. Then to the adversary, the attack problem can be viewed as solving

$$\begin{array}{ll}\min_{A\in\Gamma(\mathcal{A})} & \|G(a + \mathbb{E}[W|Z_o])\|^2\\ \text{subject to} & \|K(a + \mathbb{E}[W|Z_o])\|^2 \geq C\end{array} \tag{9}$$

where $C$ is the constant control the conditional MSE value.

In [3], it is shown that the optimal attack vector can be solved easily by calculating the smallest generalized eigenvalue of the characteristic function. Also, $\mathbb{E}[W|Z_o]$ can also be easily solved since $W$ and $Z_o$ are jointly Gaussian distributed.

After finding the optimal attack vector, the adversary will inject it into the system. In our simulation part, we test this algorithm on the IEEE-14 bus system. We try both DC model and nonlinear model (AC model). We want to show that even though the performance of this algorithm is good for the DC model, it can hardly achieve anything when the real model is nonlinear.

### B. Gaining profit in the real-time market

From the calculation of the real-time LMP, we can see that if the set of available generators in real-time remains the same, the real-time LMP only depends on the congestion pattern.

Our approach relies on a geometric characterization of the state space. Let $\mathcal{X} \subset \Re^M$ be the set of possible state vectors. Given a realization of meter data $z$, the control center obtains the state estimate $\hat{X}(Z)$ (we shall drop the dependency of $Z$ when no confusion arises). From $\hat{X}$, one obtains the estimated congestion pattern $\hat{\mathcal{C}}$ (also a function of $Z$). From the estimated congestion pattern $\hat{\mathcal{C}}$, a real-time price $\hat{\lambda}$ is obtained.

Since the state estimate $\hat{X}$ is taken as a sufficient statistic, we can drop the original data $z$. As a result, each $X \in \mathcal{X}$ is associated with a congestion pattern $\mathcal{C}$ thus a real-time price $\lambda(X)$, as shown in Fig. (III-B). Define $\pi(\mathcal{C})$ as the region of $X$'s which give the congestion pattern as $\mathcal{C}$. Notice that we have dropped the ”hat” on the corresponding variables to indicate that the relation between $X \in \mathcal{X}$ and real-time price $\lambda$ is not a function of real-time data.

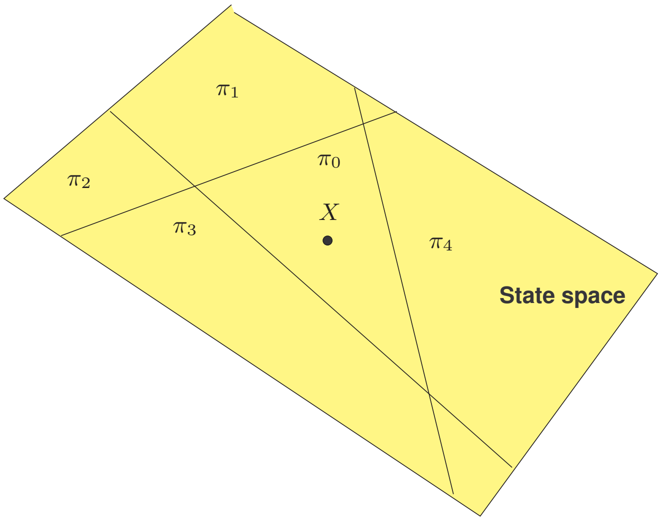


Fig. 2: Partition of the state space by real-time price

Based on the linear DC model and this concept of partition, [15] described a method to increase the price in real-time market by injecting attack vector. The estimated flow, $\hat{F}$, has linear relationship with the measurement values as in Eq.(4). So after injecting the attack vector $A$,

$$\hat{F} = H_F\hat{X}_a = H_F K\tilde{Z} + H_F KA$$

where $H_F$ is the matrix factor between state and flow under linear model.

The basic idea is first estimating the state based on the real-time observation, then starting from the estimated state, moving the estimated state with attack injection to the center of highest price region with the power constraint of the attack vector. We will also compare the result under linear and nonlinear models for this algorithm.

## IV. Discussion about nonlinearity

To handle a research problem, we always start from an easy scenario, such as using DC model in this power attack problem. Linearization here gives us a bunch of theoretical results and intelligent attack strategies. It is the time to pause and think about how far we are now from solving the actual problem under AC model.

In the early study of state estimation on power system [16], it was shown that decomposition of real and reactive power is valid in most of the normal cases, due to the reasons such as the reactance is much larger than the resistance, the voltage on each bus is quite close to each other and so on. Linear state estimation is based on this argument and has achieved great success in actual power system control, optimal power flow analysis and economic dispatch calculation. Following this path, almost all of recent research work on power system attack problem is formulated and solved based on the linear system assumption, such as [2], [6], [3], as our discuss in section III. We'd like to ask in the following whether this assumption is valid or not.

At least four things are in doubt. The first is the undetected attack vector. In [2] and other related work, effort is put to find the null space of the linear system factor matrix, $H$. By using DC model, they claimed that if there exists a sparse vector living in the null space, then a sparse undetected attack vector is found. As long as the original set of measurement values passes the bad data detector, such an attack can not be detected.

However, this argument no longer holds for nonlinear system. Assume the system equation is $Z = f(X) + W$ (same as eq. 1). The state estimate is $\hat{X}$ given the measurement $Z$. By injecting attack vector $A = \bigtriangledown f(X)\Delta X$, the adversary hopes the control center will get state estimates as $\hat{X} + \Delta X$, without increasing the residue value.

We do second order approximation of the system,

$$f(\hat{X} + \Delta X) \approx f(\hat{X}) + \bigtriangledown f(X)\Delta X + (\Delta X)^T \bigtriangledown^2 f(X)\Delta X \tag{10}$$

We can see that even though we make the local nonlinearization, when the curvature of the system function is large, a small perturbation of the measurement values may cause big inconsistence in the nonlinear weighted least square estimation. The added residue value is $(\Delta X)^T \bigtriangledown^2 f(X)\Delta X$. We need to evaluate this value first before claiming the effect of so-called undetected attack.

The second is the detection probability, which is much larger under AC model. When the attack is sparse, doing iteration can effectively reduce the effect of the attack vector and get the state estimate much closer to the actual one than linear estimator, which makes the residue obvious to be identified as abnormal. So, if the adversary designs the attack vector based on the linear model, it can hardly avoid being detected while making effect to the system, as we'll see in the simulation part.

The third is the state estimation result. We point out earlier that to disturb the system, the adversary faces the trade-off between enlarging the state estimate MSE and avoiding being detected. However, under nonlinear system model, not only it is easier to detect the attack, the effect of disturbing the state estimate is waken. To some extent, iteration will correct the error in the measurement. This means that each point on the trade-off curve of attack under linear system moves inward under nonlinear system.

The fourth is the effect of attack vector on the system. In [6], [3], no matter what metrics are used in the analysis, the effects after injecting an attack vector are evaluated by the linear model. In linear model, linear relationship can be established between the value change of estimated states and attack vector. This consequence is very helpful for analysis and algorithm design but unrealistic for nonlinear system. Since nonlinear estimator is much more powerful than the linear counterpart, the effect of attack is largely alleviated. Especially in the electricity market we study, only when the estimated states are moved far enough into another congestion pattern region, the attack vector can change the price as the adversary wants. The actual movement of estimated states is much shorter than the linear model gives. This means on one hand, the adversary needs to take much higher risk to achieve the same effect as in the linear model; on the other hand, the evaluation of attack vector is much less accurate. The adversary doesn't actually know what will happen after injecting attack vector, or at least by current method, the adversary cannot find the optimal attack vector.

As we can see from the simulation part, our results are very pessimistic. The algorithms considered in Section V is very successful under linear assumption, but can affect the nonlinear system little, although we try local linearization based on the observation and prior knowledge of the system states.

## V. Simulation results

We use IEEE 14 bus system to illustrate the effect of using nonlinear system instead of linear system. Here, all the data, including the branch parameters, quantity of loads, generation marginal price and so on. The measurements include all the real power injections and real branch flows for both directions. The false alarm probability of the detector is set to be 0.1.

First we will check the optimal attack to maximizing the conditional MSE. We plot the curve of detection probability versus the percentage change of MSE. Fig.(3) and Fig.(4) show the performance of the MSE attack algorithm under linear system and nonlinear system. In Fig.(3), only the power injection meter at bus 1 is available to the adversary to attack, while in Fig.(4), power injection meters at bus 1-4 are all available to the adversary to attack. Here this 4-sparsity attack is still observable in DC model.

From the result, we can see that under detection probability 0.5, under two different attack scenarios, the adversary can achieve about $150\%$ and $250\%$ percent increase of MSE, while the numbers are only about $40\%$ and $60\%$ for nonlinear system. These two curves show that even though the adversary thinks the attack can achieve great disturbance to the system, the actual impact will be greatly discounted due to the more powerful nonlinear state estimation.

Then we try the attack on electricity market. Still we use the IEEE 14 bus system, only setting the real line flow limit

Fig. 3: MSE increase versus Detection probability, one meter to attack

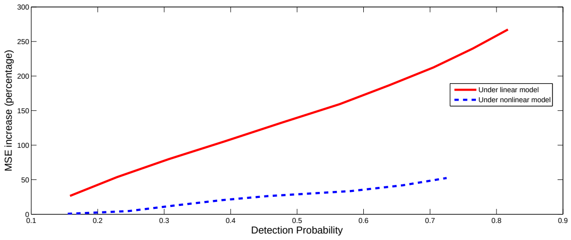
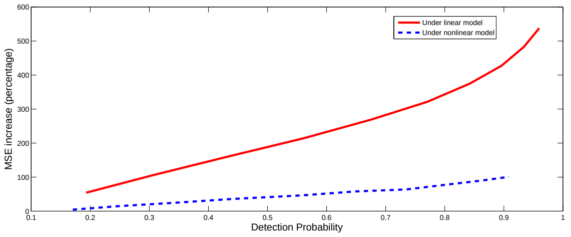


Fig. 4: MSE increase versus Detection probability, four meters to attack



to be 350MW for every line. We assume the the variance of states is 6MW, and the variance of the measurements is 3MW.

Fig.(5) is the percentage change of real-time price versus the detection probability with arbitrary 5 meters to attack under DC model. Here we mean that we assume the actual physical law is given by the DC model, and the algorithm is designed based on the DC model. The three curves represent three different scenarios, knowing all real-time measurement values (black), knowing half of the measurement values in real-time (blue), knowing nothing about the actual measurement values (red).

Then we add 5 more meters for the attack to attack in the nonlinear system. Fig.(6) shows the percentage change of real-time price versus the detection probability. We use the AC power flow equation to generate the measurement values with random measurement noises. The attack vector is still designed based on linear model with the local linearization. The black line represent the full information scenario. Here, since the adversary is using the DC model to design, so there is still a chance for the vector to be detected. The red line denote the scenario with no real-time information.

Fig. 5: Real-time price percentage change at bus 1, with 5 meters to attack, linear model

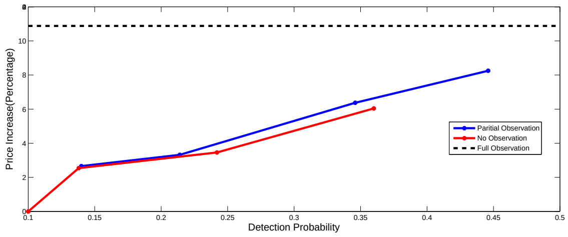
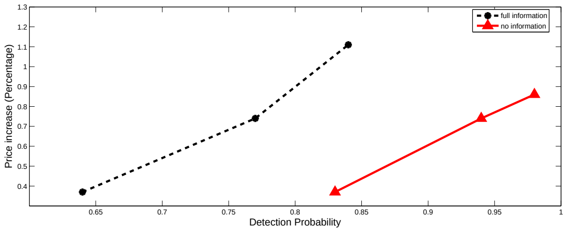


Fig. 6: Real-time price percentage change at bus 1, with 10 meters to attack, nonlinear model



As we can see from the results, although in the nonlinear case has much more meters to attack, the performance is very poor. With very high detection probability, the adversary can achieve little in real-time market.

## VI. Conclusion

With the development of smart grid, security has become a serious problem to the power system operator. Many researchers put their effort on the effect of malicious attack and the corresponding protection methods. To the authors' knowledge, almost all of them are based on DC model, which makes the problem tractable. As the first step of handling the attack problem, under linearization assumption, lots of clever attack strategies and detection schemes are proposed and proved effective by simulation results. Although we have good reasons to make linear assumption since the decomposition of state estimation is valid in most of the normal operation scenarios, we still need to proceed to the realistic setting, nonlinear system model. Then, naturally a question comes out, "is the lineariztion assumption really valid?". If so, we don't need to do much change to the current results. Otherwise, we need to take nonlinearity more seriously and cannot just stay in the DC model, doing those "fancy" things to linear system.

In this paper, we briefly discussed two types of malicious attack, increasing state estimates MSE and disturbing the real-time electricity market price. According to our simulation results, significant difference under the two system models can be observed. We can roughly claim that the ability of malicious attack designed for DC model is largely alleviated by using more accurate AC state estimation.

The purpose of this paper is to serve as a beginning study of attack on nonlinear power system. It is far from being comprehensive. The NERC cyber security criteria [1] provides a excellent guide for responsible entity(RE) to follow. Many of the standards require the RE to take a specific security assessment on the system. Simulating the attack under DC model may prevent the RE from finding the worst case. It is quite interesting for us to study in the future how the compliant utility could be affected by using a realistic model. On the other hand, since nonlinearity cannot be simply neglected, we need to take the effort to design attack strategy under AC model to find the worst effect or the most vulnerable location of the system.

# References

[1] "NERC Standards CIP-002 through CIP 009 – Cyber Security (Draft 3)," January 16th 2006.

[2] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," in *ACM Conference on Computer and Communications Security*, 2009, pp. 21–32.

[3] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Malicious data attacks on smart grid state estimation: attack strategies and countermeasures," in *Proc. IEEE 2010 SmartGridComm*, Gaithersburg, MD, USA, Oct 2010.

[4] A. Teixeira, S. Amin, H. Sandberg, K. Johansson, and S. Sastry, "Cyber Security Analysis of State Estimators in Electric Power Systems," in *Proc. of the 49th IEEE Conference on Decision and Control*, Atlanta, GA, December 2010.

[5] R. B. Bobba, K. M. Rogers, Q. Wang, H. Khurana, K. Nahrstedt, and T. J. Overbye, "Detecting false data injection attacks on dc state estimation," in *First Workshop on Secure Control Systems,CPSWEEK 2010*, Stockholm, Sweeden, Apr 2010.

[6] L. Xie, Y. Mo, and B. Sinopoli, "False data injection attacks in electricity markets," in *Proc. IEEE 2010 SmartGridComm*, Gaithersburg, MD, USA., Oct 2010.

[7] L. Jia, R. J. Thomas, and L. Tong, "Malicious data attack on real-time electricity market," in *Proceedings of 2011 International Conference on Acoustics, Speech and Signal Processing*, May 2011.

[8] A. Abur and A. G. Expósito, *Power System State Estimation: Theory and Implementation*. CRC, 2000.

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

[10] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "On malicious data attacks on power system state estimation," in *Proc. 45th Intl. Univ. Power Engineering Conf.*, Cardiff, Wales, UK, Aug 2010.

[11] R. J. Thomas, L. Tong, L. Jia, and O. E. Kosut, "Some economic impacts of bad and malicious data," in *PSerc 2010 Workshop*, vol. 1, Portland Maine, July 2010.

[12] E. Handschin, F. C. Schweppe, J. Kohlas, and A. Fiechter, "Bad data analysis for power system state estimation," *IEEE Trans. Power Apparatus and Systems*, vol. PAS-94, no. 2, pp. 329–337, Mar/Apr 1975.

[13] A. L. Ott, "Experience with pjm market operation, system design, and implementation," *IEEE Trans. Power Systems*, vol. 18, no. 2, pp. 528–534, May 2003.

[14] D. Patton and P. Van Schaick, "2007 assessment of the electricity markets in new england," *Potomac Economics*, 2008.

[15] L. Jia, R. J. Thomas, and L. Tong, "Impacts of malicious data on real-time price of electricity market operations," in *to be appeared in 45th Hawaii Intl. Conf. on System Sciences*, January 2012.

[16] F. C. Schweppe, J. Wildes, and D. P. Rom, "Power system static state estimation, Parts I, II, III," *IEEE Tran. on Power Appar. & Syst.*, vol. PAS-89, pp. 120–135, 1970.