Dynamic Attacks on Power Systems Economic Dispatch

Jinsub Kim
School of Electrical Engineering and Computer Science
Oregon State University, Corvallis, OR 97331
Email: {jinsub.kim}@oregonstate.edu

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

***Abstract*—A dynamic data attack on a power system aimed at making the real time economic dispatch infeasible is considered. As a man-in-the-middle attack, the attack modifies part of sensor measurements such that the control center is misled with an incorrect system state estimate, which affects the computation of real time economic dispatch. Two attack mechanisms are considered. The first is an opportunistic approach where the attacker waits for a chance of a successful attack and launches an attack in a single state estimation period. The second is a dynamic attack strategy where the attacker gradually drifts the system state toward the infeasible region for real time economic dispatch. The efficacy of the proposed attacks is demonstrated by numerical experiments with the IEEE 14-bus network.**

***Index Terms*—Power systems economic dispatch, dynamic data attack, denial-of-service attack, cyber security of smart grid.**

I. Introduction

Incorporating real-time data processing and control, a future smart grid is expected to operate in a more efficient and reliable manner. However, heavy reliance on data communications exposes grids to possible cyber attacks that may disrupt grid operations. This paper focuses on a man-in-the-middle *data attack* in which an adversary is capable of replacing part of sensor data with “malicious data.”

It was shown in [1] that an adversary controlling a small subset of sensor data may perturb the state estimate by an arbitrary degree without being detected. This result revealed the potential vulnerability of power systems operations that use the state estimate as an input.

Power system *economic dispatch* is one of the most important functions that rely on the state estimate. Economic dispatch determines real-time *generation adjustments* to meet the future demand, subject to operational constraints, such that the generation-load balance can be maintained in a reliable and economic way. A data attack on state estimation may disrupt the dispatch operation that controls the system state trajectory.

In this paper, we study how a data attack may affect the system state trajectory by perturbing the economic dispatch solution throughout multiple state estimation periods. In particular, we present data attack mechanisms that drive the state estimate into the region where economic dispatch has no solution. This is a *denial-of-service* (DoS) attack on economic dispatch. If such an attack succeeds, the control center will mistakenly believe that the system is not capable of meeting the future demand. The most intuitive action that the control center may take is to introduce additional fast-ramping units to make economic dispatch feasible. However, such a decision will result in a considerably higher cost of generation.

A. Summary of contributions

We demonstrate that by exploiting the role of state estimate in economic dispatch, a multi-period data attack can drift the system state toward a certain direction to achieve its objective. In particular, we exploit the geometric structure of the economic dispatch problem to design concrete attack mechanisms. While this paper focuses on the attack objective of making economic dispatch infeasible, the main ideas are general enough to be applicable to a broader range of objectives (*e.g.*, see [2] for an attack aiming to cause a certain type of contingency.)

Two types of strategies are presented for DoS attack: an opportunistic attack and a dynamic attack. The *opportunistic attack* waits for the best timing and launches an attack in a single state-estimation period. In contrast, the *dynamic attack* perturbs the economic dispatch solution persistently in consecutive periods such that the state estimate will quickly enter the infeasibility region for economic dispatch. We present a greedy approach of dynamic attack based on convex optimization.

The proposed attacks were tested on the IEEE 14-bus network, and they demonstrated high success rates even when the compromised sensor data are modified by a small degree.

B. Related works and organization

Following [1], several works studied feasibility of an unobservable attack on state estimation and cost-effective attacks. Unobservable attacks with small attack resources were studied under various scenarios in [1], [3], [4]. In [3], [4], based on a linearized model, feasibility of an unobservable attack is characterized as a classical network observability condition. To take into account the nonlinearity of power systems, unobservable attacks on nonlinear state estimation were studied in [5]. The idea of data framing was exploited in [6] to enable a successful attack on state estimation with a half number of the adversary-controlled sensors required for an unobservable attack. Adversarial effects of data attack on economic dispatch and electricity pricing were also studied in

This work is supported in part by the National Science Foundation under Grant CNS-1135844.

[7]–[9]. The majority of works on data attack, including the aforementioned papers, focused on single-period attacks.

Some research works considered an attack on a cyber physical system that spans multiple state-estimation periods. Mo and Sinopoli in [10] studied a multi-period data attack that aims to destabilize a linear control system. Pasqualetti *et al.* in [11] studied identifiability and detectability of a multi-period attack. While the linear control system models used in [10], [11] are generic, the power system control based on economic dispatch cannot be modeled as a simple linear model.

The rest of the paper is organized as follows. Section II introduces the mathematical models of power system state estimation and economic dispatch. The data attack model and its effect on economic dispatch are described in Section III. Section IV presents an opportunistic approach of DoS attack on economic dispatch. A dynamic approach of DoS attack is presented in Section V. Section VI demonstrates the simulation performance of the proposed attacks, and Section VII provides concluding remarks.

II. Mathematical models

Throughout the paper, we use a boldface lowercase letter (*e.g.*, $\mathbf{x}$) to denote a vector, and x_i denotes the ith entry of $\mathbf{x}$. A boldface uppercase letter (*e.g.*, $\mathbf{H}$) denotes a matrix, and H_{ij} denotes the entry of $\mathbf{H}$ at the ith row and the jth column. A superscript $(\cdot)^{(t)}$ (*e.g.*, $\mathbf{x}^{(t)}$) is used to denote a vector or a matrix defined for the tth period. The m-dimensional vector having all entries equal to 1 is denoted by $\mathbf{1}_m$.

A. Power systems measurement model

For real-time state estimation at the tth period, the control center of a power grid collects real-time measurements $\mathbf{z}^{(t)}$ from sensors deployed throughout the grid. The measurements are related to the system state $\mathbf{x}^{(t)}$ by the nonlinear AC measurement function $h(\cdot)$ as follows [12]:

$$\mathbf{z}^{(t)} = h(\mathbf{x}^{(t)}) + \tilde{\mathbf{e}}^{(t)}, \tag{1}$$

where $\tilde{\mathbf{e}}^{(t)}$ is a Gaussian measurement noise with a covariance matrix $\mathbf{\Sigma}_0$.

In analyzing the impact of data attack on state estimation, we adopt the DC model obtained by linearizing the AC model at the nominal operating point [1], [4], [12]:

$$\mathbf{z}^{(t)} = \mathbf{H}\mathbf{x}^{(t)} + \mathbf{e}^{(t)}, \tag{2}$$

where $\mathbf{z}^{(t)} \in \mathbb{R}^m$ is the vector consisting of real parts of line flow and bus injection measurements[1], the state $\mathbf{x}^{(t)} \in \mathbb{R}^n$ is the vector of the voltage phase angles at all buses except the reference bus, $\mathbf{H} \in \mathbb{R}^{m\times n}$ is the proper submatrix of the Jacobian of h, and $\mathbf{e}^{(t)}$ is a Gaussian measurement noise with a covariance matrix $\mathbf{\Sigma}$. A power network is said to be *observable* if a state $\mathbf{x}$ can be uniquely identified from $\mathbf{H}\mathbf{x}$, *i.e.*, $\mathbf{H}$ has full column rank. Practical power networks are equipped with a sufficient number of sensors such that observability can be guaranteed.

B. Power systems state estimation

Once the sensor measurements $\mathbf{z}^{(t)}$ are collected, nonlinear weighted least squares (WLS) estimation is typically employed to obtain the state estimate $\hat{\mathbf{x}}^{(t)}$:

$$\hat{\mathbf{x}}^{(t)} = \arg\min_{\mathbf{x}} [\mathbf{z}^{(t)} - h(\mathbf{x})]^T \mathbf{\Sigma}_0^{-1} [\mathbf{z}^{(t)} - h(\mathbf{x})]. \tag{3}$$

In practice, the above minimization can be conducted numerically by the Newton-Raphson method or the quasi-Newton method [12].

Based on $\hat{\mathbf{x}}^{(t)}$, a bad data detector checks whether $\mathbf{z}^{(t)}$ contains any biased measurement. A popular bad data detector is a threshold rule based on the residue magnitude [13]:

$$\begin{cases} \text{bad data} & \text{if } [\mathbf{z}^{(t)} - h(\hat{\mathbf{x}}^{(t)})]^T \mathbf{\Sigma}_0^{-1} [\mathbf{z}^{(t)} - h(\hat{\mathbf{x}}^{(t)})] > \tau; \\ \text{good data} & \text{otherwise} \end{cases}, \tag{4}$$

where τ is a threshold predetermined to satisfy the false alarm constraint. If the detector declares the presence of bad data, a bad data filtering mechanism is invoked to identify and remove the bad data entries from $\mathbf{z}^{(t)}$. Then, state estimation is conducted with the updated measurements (see [12] for the details.)

In analyzing the impact of data attack on state estimation, we assume that state estimation is conducted based on the DC model (2):

$$\begin{aligned} \hat{\mathbf{x}}^{(t)} &= \arg\min_{\mathbf{x}} [\mathbf{z}^{(t)} - \mathbf{H}\mathbf{x}]^T \mathbf{\Sigma}^{-1} [\mathbf{z}^{(t)} - \mathbf{H}\mathbf{x}] \\ &= (\mathbf{H}^T \mathbf{\Sigma}^{-1} \mathbf{H})^{-1} \mathbf{H}^T \mathbf{\Sigma}^{-1} \mathbf{z}^{(t)}. \end{aligned} \tag{5}$$

The attack analysis based on the DC model is more tractable, and it provides a useful insight into how practical power systems will react to the attacks. Nevertheless, to verify the efficacy of the attacks, we need to test them using the nonlinear AC model (1) and nonlinear state estimation (3). To this end, section VI will demonstrate the performance of the proposed attacks on nonlinear power systems.

C. Power systems economic dispatch

In the tth period, economic dispatch receives the vector of generation estimates, denoted by $\hat{\mathbf{g}}^{(t)}$ and calculated based on $\hat{\mathbf{x}}^{(t)}$, and the load forecast for the $(t+1)$st period as inputs. Based on the inputs, economic dispatch solves the following optimization to determine the lowest-cost generation schedule that can meet the demand in the $(t+1)$st period while satisfying operational constraints.

$$\begin{aligned} \min_{\mathbf{g}} \quad & \mathbf{c}^T \mathbf{g} \\ \text{subj.} \quad & \textstyle\sum_{i\in\mathcal{G}} g_i = \sum_{j\in\mathcal{D}} d_j^{(t+1)} \\ & g_i^{min} \le g_i \le g_i^{max}, \quad i \in \mathcal{G} \\ & \left| \textstyle\sum_{i\in\mathcal{G}} S_{ki} \cdot g_i - \sum_{j\in\mathcal{D}} S_{kj} \cdot d_j^{(t+1)} \right| \le L_k^{max}, \ k \in \mathcal{L} \\ & -\underline{\Delta g_i} \le g_i - \hat{g}_i^{(t)} \le \overline{\Delta g_i}, \quad i \in \mathcal{G} \end{aligned} \tag{6}$$

The variable $\mathbf{g}$ is a vector consisting of the generation levels for the $(t+1)$st period. The objective is to minimize the

[1] This model can easily incorporate other types of measurements, *e.g.*, synchrophasor measurements. To make the presentation concise, we focus on line flow and bus injection measurements.

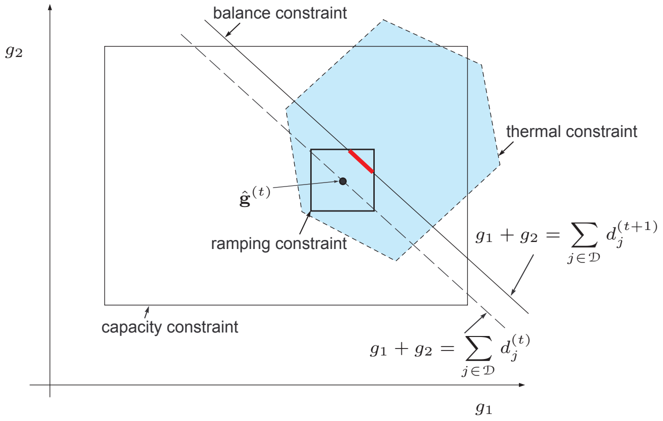

Fig. 1. The feasible set of economic dispatch: the thick red line segment, which is the intersection of all constraints, is the feasible set.

incremental cost of generation. The vector $\mathbf{c}$ consists of the marginal costs of generation at $\hat{\mathbf{g}}^{(t)}$. The incremental cost is $\mathbf{c}^T(\mathbf{g} - \hat{\mathbf{g}}^{(t)})$, and minimizing it is equivalent to minimizing $\mathbf{c}^T\mathbf{g}$ as the second term is fixed. In the following, the four types of constraints are explained in order.

1) *Balance* constraint: the set $\mathcal{G}$ is the set of the bus indices for generator buses, and g_i ($i \in \mathcal{G}$) is an entry of $\mathbf{g}$ corresponding to the generation level at bus i. The set $\mathcal{D}$ is the set of bus indices for the load buses, and $d_j^{(t+1)}$ ($j \in \mathcal{D}$) is the load forecast at bus j for the $(t+1)$st period. The balance constraint requires that the total generation has to match the total load.
2) *Capacity* constraints represent the minimum and the maximum generation output of each generator.
3) *Thermal* constraint: $\mathcal{L}$ is the set of transmission line indices, and S_{ki} denotes the shift factor[2], which is the increase in the line flow through line k when the power injection at bus i increases by 1 p.u. The thermal constraint implies that the line flow through line k cannot be larger than its thermal limit, denoted by L_k^{max}.
4) *Ramping* constraint: the ramping constraints imply that for each generator, there exist upper and lower bounds on generation adjustment within a single period.

The feasible set is described in Fig. 1 for the example of a power network with two generators. The balance constraint is a hyperplane, the capacity constraints are represented as a box, and the thermal constraints give a polytope. The ramping constraints form a box centered at $\hat{\mathbf{g}}^{(t)}$, which we refer to as the *ramping box*. Note that the ramping constraints are the only constraints that depend on the state estimate because $\hat{\mathbf{g}}^{(t)}$ is calculated from $\hat{\mathbf{x}}^{(t)}$.

Real-time electricity prices are set in a way that generators have financial incentives to adjust their generation following the economic dispatch solution (*e.g.*, see [14] for PJM case.) Therefore, we assume that the generation in the $(t+1)$st period will be equal to the solution g^* of (6). Under this assumption, the economic dispatch solution serves as a control signal that, together with the load profile, will determine the state trajectory.

III. Adversary model

A data attack in the tth period is modeled as follows.

$$\bar{\mathbf{z}}^{(t)} = \mathbf{z}^{(t)} + \mathbf{a}^{(t)}, \quad \mathbf{a}^{(t)} \in \mathcal{A}, \; \|\mathbf{a}^{(t)}\|_1 \leq P \tag{7}$$

where $\mathbf{a}^{(t)}$ represents the data modification introduced by the attack. The subspace $\mathcal{A} \subset \mathbb{R}^m$ consists of vectors that have nonzero entries only at the rows corresponding to the adversary-compromised sensors. The l_1-norm constraint is there to prevent an attack that will obviously raise suspicion.

A. Unobservable attack and network observability

Using the DC model, it was shown in [1] that if the attack vector lies in $\mathcal{R}(\mathbf{H})$, the column space of $\mathbf{H}$, then the attack is *unobservable*. To see this, suppose that $\mathbf{a}^{(t)} = \mathbf{H}\mathbf{y}$ for some nonzero state $\mathbf{y}$. Then,

$$\bar{\mathbf{z}}^{(t)} = (\mathbf{H}\mathbf{x}^{(t)} + \mathbf{e}^{(t)}) + \mathbf{a}^{(t)} = \mathbf{H}(\mathbf{x}^{(t)} + \mathbf{y}) + \mathbf{e}^{(t)}. \tag{8}$$

Therefore, the resulting $\bar{\mathbf{z}}^{(t)}$ appears to be a normal measurement vector with the state $\mathbf{x}^{(t)} + \mathbf{y}$. Hence, the attack can perturb the state estimate by $\mathbf{y}$ without being detected.

It was shown in [4] that an unobservable attack exists if and only if after removing the adversary-controlled sensors, the power network becomes unobservable. Throughout the paper, we assume that the attacker controls a proper subset of sensors such that an unobservable attack is feasible. This assumption means that the dimension of the subspace of unobservable attack vectors, which is $\mathcal{A} \cap \mathcal{R}(\mathbf{H})$, is nonzero.

B. Attack impact on economic dispatch

Recall that among the operational constraints of economic dispatch (6), only the ramping constraints depend on $\hat{\mathbf{x}}^{(t)}$ through $\hat{\mathbf{g}}^{(t)}$. This implies that a data attack can affect the economic dispatch solution only through changing the ramping constraints by perturbing $\hat{\mathbf{g}}^{(t)}$.

If a data attack perturbs the generation estimate from $\hat{\mathbf{g}}^{(t)}$ to $\hat{\mathbf{g}}_a^{(t)}$, then the ramping box is translated by the vector $\hat{\mathbf{g}}_a^{(t)} - \hat{\mathbf{g}}^{(t)}$. If the perturbation is significant, the economic dispatch solution will change due to the change in the feasible set. Therefore, our assumption that generators follow the dispatch solution implies that the system state in the $(t+1)$st period will be affected by the attack. If such an attack persists for multiple state-estimation periods, the state trajectory will be affected.

C. Denial-of-service attack on economic dispatch

We consider a DoS attack on economic dispatch, which aims to make economic dispatch have no solution. This attack objective is equivalent to making the feasible set of economic dispatch *empty*, *i.e.*, making the intersection of all constraints empty. The attacker is allowed to inject false data at any time and as many times as he or she wants. Nevertheless, it is

[2] Shift factors are calculated typically based on the DC model (2) [14].

desirable that the attack can succeed within a small number of periods. Because, the longer the attack lasts, the larger the probability that the attack will be detected. In the following sections, we introduce two types of DoS attack mechanisms.

IV. Opportunistic DoS attack

In the opportunistic attack, an attacker waits for a chance of successfully *making the ramping constraints disjoint with the balance constraint* and launches a single-period data attack.

From Fig. 1, one can see that the further $\hat{\mathbf{g}}^{(t)}$ is from the balance hyperplane, the easier it is to make the ramping box disjoint with the balance hyperplane by perturbing $\hat{\mathbf{g}}^{(t)}$. Note that the Euclidean distance from $\hat{\mathbf{g}}^{(t)}$ to the balance hyperplane is proportional to the difference between $\sum_{j\in\mathcal{D}} d_j^{(t)}$ and $\sum_{j\in\mathcal{D}} d_j^{(t+1)}$. Because, $\sum_{i\in\mathcal{G}} \hat{g}_i^{(t)}$ has to be equal to $\sum_{j\in\mathcal{D}} d_j^{(t)}$ (if we ignore the estimation and forecasting errors.) Therefore, the best timing for the opportunistic attack is the time $\bar{t}$ at which $\left|\sum_{j\in\mathcal{D}} d_j^{(\bar{t})} - \sum_{j\in\mathcal{D}} d_j^{(\bar{t}+1)}\right|$ is maximized. In practice, the attacker can infer the best timing based on the day-ahead forecast of the aggregate load.

Once the attacker decides to launch an attack at the tth period, the attack vector can be decided by solving the following convex optimization to maximize the distance from $\hat{\mathbf{g}}_a^{(t)}$ to the balance hyperplane, where $\hat{\mathbf{g}}_a^{(t)}$ denotes the perturbed generation estimate:

$$\begin{array}{ll} \max_{\mathbf{a}\in\mathcal{A}\cap\mathcal{R}(\mathbf{H})} & \mathbf{u}^T\mathbf{G}\mathbf{a} \\ \text{subj.} & \|\mathbf{a}\|_1 \le P \end{array} \tag{9}$$

where $\mathbf{u}$ is $\frac{1}{\sqrt{|\mathcal{G}|}}\mathbf{1}_{|\mathcal{G}|}$ if $\sum_{i\in\mathcal{G}} \hat{g}_i^{(t)} \le \sum_{j\in\mathcal{D}} d_j^{(t+1)}$; otherwise, $\mathbf{u}$ is $-\frac{1}{\sqrt{|\mathcal{G}|}}\mathbf{1}_{|\mathcal{G}|}$. Note that $\mathbf{u}$ is orthogonal to the balance hyperplane and is the direction to move $\hat{\mathbf{g}}^{(t)}$ toward if we want to increase the distance from $\hat{\mathbf{g}}^{(t)}$ to the hyperplane. The $|\mathcal{G}|$-by-m matrix $\mathbf{G}$ is such that for any state $\mathbf{x}$, $\mathbf{GHx}$ is the generation level corresponding to the state $\mathbf{x}$ under the DC model. Then, for $\mathbf{a} \in \mathcal{A}\cap\mathcal{R}(\mathbf{H})$, $\mathbf{Ga}$ corresponds to the perturbation introduced to the generation estimate by the unobservable attack $\mathbf{a}$[3]. Therefore, $\mathbf{u}^T\mathbf{Ga}$ corresponds to the increase in the distance from $\hat{\mathbf{g}}^{(t)}$ to the hyperplane due to the unobservable attack $\mathbf{a}$.

V. Dynamic DoS attack

The first step of the dynamic attack is to select a certain *target constraint*, say $\mathbf{w}^T\mathbf{g} \le w_0$. It can be a half space that represents a thermal constraint of a transmission line or an upper or lower capacity constraint of a generator. Let $\mathcal{T}$ denote $\{\mathbf{g} : \mathbf{w}^T\mathbf{g} \le w_0\}$ and $\mathcal{F}$ the intersection of the ramping box and the balance hyperplane. Then, the dynamic attack perturbs the generation estimate in every state estimation period (thereby perturbing the ramping box and $\mathcal{F}$) such that $\mathcal{F}$ *will gradually move into* $\mathcal{T}^c$. Because the feasible set of economic dispatch is a subset of $\mathcal{F}\cap\mathcal{T}$, $\mathcal{F}\subset\mathcal{T}^c$ means that the feasible set is empty.

We propose a greedy approach to designing attack vectors. In every attack period, the greedy approach aims to *minimize* $\max_{\mathbf{g}\in\mathcal{F}\cap\mathcal{T}} d(\mathbf{g})$ where $d(\mathbf{g}) \triangleq w_0 - \mathbf{w}^T\mathbf{g}$. Note that for $\mathbf{g}\in\mathcal{T}$, $d(\mathbf{g})$ is non-negative, and it is proportional to the Euclidean distance from $\mathbf{g}$ to the target hyperplane ($\mathbf{w}^T\mathbf{g} = w_0$.) The closer $\mathcal{F}$ is to the hyperplane, the smaller $\max_{\mathbf{g}\in\mathcal{F}\cap\mathcal{T}} d(\mathbf{g})$ is.

The attack affects $\max_{\mathbf{g}\in\mathcal{F}\cap\mathcal{T}} d(\mathbf{g})$ by perturbing $\mathcal{F}$ through moving the ramping box. In each attack period, the dynamic attack finds $\mathbf{a}$ that minimizes $\max_{\mathbf{g}\in\mathcal{F}\cap\mathcal{T}} d(\mathbf{g})$ by solving the following convex optimization:

$$\begin{array}{ll} \max_{\mathbf{a}\in\mathcal{A}\cap\mathcal{R}(\mathbf{H})} & \alpha\cdot\mathbf{s}^T\mathbf{Ga} + \mathbf{w}^T(\mathbf{I}-\mathbf{ss}^T)\mathbf{Ga} \\ \text{subj.} & \|\mathbf{a}\|_1 \le P \end{array} \tag{10}$$

where $\mathbf{G}$ was defined in (9). The unit vector $\mathbf{s}$ is chosen between $\frac{1}{\sqrt{|\mathcal{G}|}}\mathbf{1}_{|\mathcal{G}|}$ and $-\frac{1}{\sqrt{|\mathcal{G}|}}\mathbf{1}_{|\mathcal{G}|}$ such that moving $\hat{\mathbf{g}}^{(t)}$ by $\mathbf{s}$ will reduce $\max_{\mathbf{g}\in\mathcal{F}\cap\mathcal{T}} d(\mathbf{g})$. The real constant α is the decrease in $\max_{\mathbf{g}\in\mathcal{F}\cap\mathcal{T}} d(\mathbf{g})$ when $\hat{\mathbf{g}}^{(t)}$ is perturbed by $\mathbf{s}$. In the second term of the objective function, $(\mathbf{I}-\mathbf{ss}^T)\mathbf{Ga}$ is the component of $\mathbf{Ga}$ that is parallel to the balance hyperplane.

The intuition is as follows. We can decompose $\mathbf{Ga}$ (the perturbation of the generation estimate due to the unobservable attack $\mathbf{a}$) into the orthogonal and parallel components with respect to the balance hyperplane. The orthogonal component changes the shape of $\mathcal{F}$. The parallel component translates $\mathcal{F}$ within the balance hyperplane without affecting the shape. Hence, we can understand the effect of $\mathbf{Ga}$ on $\mathcal{F}$ as a two-step procedure: the orthogonal component first changes the shape of $\mathcal{F}$, and then the parallel component translates $\mathcal{F}$ within the balance hyperplane without affecting the shape. The first term and the second term of the objective function characterize the decrease in $\max_{\mathbf{g}\in\mathcal{F}\cap\mathcal{T}} d(\mathbf{g})$ due to the orthogonal component and the parallel component respectively.

VI. Simulation results

We tested the proposed attacks on the IEEE 14-bus network using the AC model (1) and the nonlinear state estimator (3). As described in Fig. 2, the network was assumed to have three generators with quadratic cost functions, and the attacker controlled the sensors associated with the two cuts of the network (denoted by the blue dashed lines.) Under this setting, $\mathcal{A}\cap\mathcal{R}(\mathbf{H})$ has dimension 2 (see [4] for details), so the perturbation that an unobservable attack can introduce to $\hat{\mathbf{g}}^{(t)}$ has two degrees of freedom. In each Monte Carlo simulation, we generated a random load profile for 100 periods, the mean of which is linearly increasing until the 50th period and then linearly decreasing. A random load profile was generated by adding an AR(1) noise process to the mean profile. Once the load profile was generated, we conducted state estimation and economic dispatch for each period and let the system state change according to the economic dispatch solutions.

Tabel. I shows the probability of attack success versus the amplitude constraint, when we restricted the attack to happen within a fixed window of 100 state estimation periods.

[3] Recall that if $\mathbf{a}\in\mathcal{A}\cap\mathcal{R}(\mathbf{H})$, then $\mathbf{a} = \mathbf{Hy}$ where $\mathbf{y}$ is the perturbation introduced to the state estimate by the attack $\mathbf{a}$. Then, $\mathbf{Ga} = \mathbf{GHy} = \mathbf{GH}(\hat{\mathbf{x}}^{(t)} + \mathbf{y}) - \mathbf{GH}\hat{\mathbf{x}}^{(t)}$. Hence, $\mathbf{Ga}$ corresponds to the perturbation of the generation estimate caused by the attack $\mathbf{a}$.

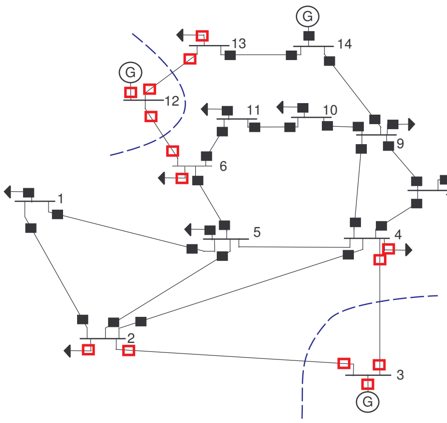

Fig. 2. IEEE 14-bus network with three generators: rectangles denote the locations of bus injection and line flow sensors. Especially, the red empty rectangles represent the sensors that are assumed to be controlled by the attacker.

TABLE I
PROBABILITY OF ATTACK SUCCESS WITHIN 100 ATTACK PERIODS: 200 MONTE CARLO RUNS WERE USED.

Attack magnitude	7%	9%	11%	13%	15%	17%
Opportunistic attack	0	0.01	0.07	0.12	0.34	0.40
Dynamic attack	0	0.03	0.44	0.86	1	1

The dynamic attack began its attack from the first period and continued until economic dispatch becomes infeasible. In contrast, the opportunistic attack selected the best attack timing based on the aggregate load profile and launched a data attack only in the selected period. The attack magnitude in the table denotes the ratio $\frac{P}{\mathbb{E}\|\mathbf{z}_a\|_1}$ where P is the upper bound on $\|\mathbf{a}\|_1$ in (9) and (10), and $\mathbf{z}_a$ is the subvector of $\mathbf{z}^{(t)}$ that consists of the measurements from the adversary-controlled sensors (before adversarial modification); 9% means that the attack can modify the adversary-controlled sensor data at most by 9% of $\mathbb{E}\|\mathbf{z}_a\|_1$, in l_1-norm. The results show that the dynamic attack has much higher probability of success than the opportunistic attack. In addition, the higher the attack magnitude is, the higher the success rate is.

Fig. 3 demonstrates the empirical cumulative distribution functions of the attack duration (until economic dispatch becomes infeasible) for dynamic attacks with different amplitude constraints. The plots imply that the larger the attack magnitude is, the earlier the dynamic attack can succeed.

VII. CONCLUSIONS

DoS data attacks on power systems economic dispatch were presented. The opportunistic attack and the dynamic attack were proposed to reveal vulnerability of economic dispatch to DoS attacks. The simulation results demonstrated that the proposed attacks can succeed with high probability even when the magnitudes of the injected false data are small.

Besides the DoS attacks, our results demonstrate that a dynamic data attack can possibly drift the system state toward a certain point of the attacker's interest by exploiting the role of state estimate in economic dispatch. Potential damages from such attacks are more diverse and detrimental than single-period attacks. Therefore, further study on dynamic data attacks is of immediate importance.

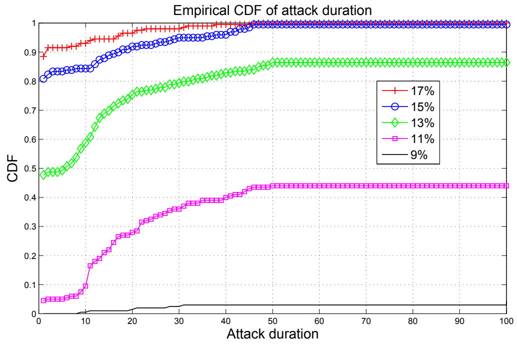

Fig. 3. The empirical CDFs of the attack duration for dynamic attacks with different attack magnitudes: 200 Monte Carlo runs were used

REFERENCES

[1] 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, pp. 21–32.

[2] J. Kim, L. Tong, and R. J. Thomas, "Dynamic Attacks on Power Systems Economic Dispatch," to be submitted to *IEEE Transactions on Smart Grid*.

[3] 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.

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

[5] J. Liang, O. Kosut, and L. Sankar, "Cyber attacks on AC state estimation: Unobservability and physical consequences," in *2014 IEEE PES General Meeting*, July 2014, pp. 1–5.

[6] J. Kim, L. Tong, and R. J. Thomas, "Data Framing Attack on State Estimation," *IEEE Journal on Selected Areas in Communications*, vol. 32, no. 7, July 2014.

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

[8] D.-H. Choi and L. Xie, "Ramp-induced data attacks on look-ahead dispatch in real-time power markets," *IEEE Transactions on Smart Grid*, vol. 4, no. 3, pp. 1235–1243, Sept 2013.

[9] L. Jia, J. Kim, R. Thomas, and L. Tong, "Impact of data quality on real-time locational marginal price," *IEEE Transactions on Power Systems*, vol. 29, no. 2, pp. 627–636, March 2014.

[10] Y. Mo and B. Sinopoli, "False data injection attacks in control systems," in *First Workshop on Secure Control Systems, CPS Week*, 2010.

[11] F. Pasqualetti, F. Dorfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," *IEEE Transactions on Automatic Control*, vol. 58, no. 11, pp. 2715–2729, Nov 2013.

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

[13] 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.

[14] 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.