2012 American Control Conference
Fairmont Queen Elizabeth, Montréal, Canada
June 27-June 29, 2012

Optimal Power Flow: Closing the Loop over Corrupted Data

André Teixeira, Henrik Sandberg, György Dán, and Karl H. Johansson

***Abstract*—Recently the power system state estimator was shown to be vulnerable to malicious deception attacks on the measurements, resulting in biased estimates. In this work we analyze the behavior of the Optimal Power Flow (OPF) algorithm in the presence of such maliciously biased estimates and the resulting consequences to the system operator. In particular, we characterize the set of attacks that may lead the operator to apply the erroneous OPF recommendation. Such characterization is used to improve a previously proposed security index by also considering the attack impact, which may be used for allocation and prioritization of protective measures. Additionally, we propose an analytical expression for the optimal solution of a simplified OPF problem with corrupted measurements. A small analytical example is discussed to illustrate and motivate our contributions.**

***Index Terms*—Power Systems, Optimal Power Flow, Data Corruption, Security**

I. Introduction

Common IT systems widely used in control application are the Supervisory Control and Data Acquisition (SCADA) systems. In power networks, the SCADA system is combined with application specific components gathered in the so-called Energy Management System. Modern SCADA/EMS systems collect large amounts of measurement data and, using a State Estimator (SE) with detailed models of the network and Bad Data Detection (BDD) schemes, provide the human operator estimates of the current network state. The estimated state information is then used by optimization tools to compute optimal supervisory control actions minimizing the network operation costs while ensuring safety and reliability requirements are met. These control actions are obtained by solving the Optimal Power Flow (OPF) problem and the safety requirements are evaluated by the Contingency Analysis (CA) component. Fig. 1 shows the power network's control loop.

The technological development enabled the implementation of more advanced and fast acting controllers, leading to an increasing need for timely exchange of large amounts of measurement and actuator data. This resulted in having the data transmitted through unencrypted communication channels, making the data and all the components in the control loop vulnerable to cyber attacks, see [1], [2]. In fact, several cyber attacks on SCADA/EMS systems operating power networks have already been reported, see [3], [4], and [5] for a recent example that received considerable media attention.

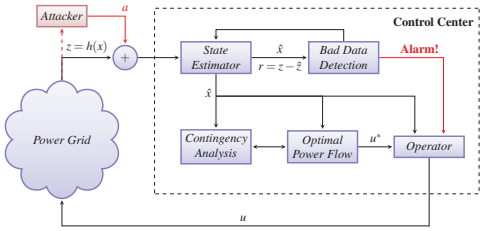

Fig. 1. The state estimator under a cyber attack. We denote the data corruption by a.

In this paper, we analyze the consequences of data attacks on the power network's control loop, namely the OPF algorithm and the human operator. Recent work has characterized a class of data corruption attacks that are undetectable by conventional BDD schemes, assuming both the BDD and the attacker know exactly a simplified linear network model, see [6], [7], [8], [9]. In [10] data attack experiments on a SCADA/EMS testbed were carried out, showing that current SE and BDD implementations with the full nonlinear network model available are also vulnerable to data attacks based on the simplified linear model.

Several countermeasures to these attacks were proposed, from the allocation of encryption [11] and additional protected measuring devices [9], to the implementation of improved BDD schemes, see [8], [12]. Methods to efficiently rank the measurements in terms of their vulnerability and finding sparse attacks requiring the corruption of a low number of measurements were also proposed in [7], [11], [13], [9]. However, these methods only considered the existence of sparse attacks, neglecting their impact on the control loop and the network.

The economic impact of data corruption attacks has been investigated recently for electricity market applications in [14], [15]. These approaches considered the linearized version of the DC-OPF or Economic Dispatch and provided several attack heuristics to tamper with the electricity markets while remaining undetected by conventional BDD schemes. Recently the impact of a more restricted class of data attacks corrupting only load and flow measurements was also analyzed for a linear Security-Constrained Economic Dispatch problem under a game-theoretic perspective in [16]. In these approaches the presence of a human operator was neglected, hence the com-

This work was supported in part by the European Commission through the VIKING project, the Swedish Research Council under Grants 2007-6350 and 2009-4565, and the Knut and Alice Wallenberg Foundation.

The authors are with ACCESS Linnaeus Centre, KTH - Royal Institute of Technology, School of Electrical Engineering, Stockholm, Sweden.
{andretei,hsan,gyuri,kallej}@kth.se

promised control actions were always applied to the system.

Here we analyze the behavior of the DC-OPF, formulated as a Quadratic Programming problem, under corrupted estimates resulting from undetectable attacks. No market application is considered, instead we focus on how the corrupted estimates may affect the operator's decisions and the possible economic consequences. We further consider that the operator makes a binary decision of either closing the loop over the DC-OPF recommendation or not taking any control action.

Our first contribution builds on the KarushKuhnTucker (KKT) conditions and provides an analytical characterization of the perturbed DC-OPF solution given that the corrupted estimates satisfy certain conditions. Using these expressions, we discuss under what conditions a human operator has the incentive to consider and apply the compromised DC-OPF recommendation. The discussion follows by analyzing the economic impact on the network operation if the operator decides to close the control loop over the corrupted measurements. A small analytical example is discussed, illustrating the concepts of the first contribution and motivating our second one.

In our second contribution, we use the novel analytical expressions to improve the security index proposed in [7]. Some computational issues of this index and connections to previous results are briefly discussed. We envision this contribution to be useful to system security designers, namely for secure sensor allocation, as discussed in [8] and [11].

The outline of the paper is as follows. In Section II, the basic formulation of the DC network model is introduced and the DC-OPF problem described and solved. In Section III, the effect of corrupted estimates on the DC-OPF is studied for attacks satisfying mild assumptions. The consequences of applying the compromised DC-OPF recommendation and conditions under which it may happen are also discussed. In Section IV, an illustrative example is considered, and in Section V an impact-aware security index taking in account the attack sparsity and corresponding impact is proposed. A summary of the contributions and conclusions are presented in Section VI.

II. Simplified Optimal Power Flow

We consider a simplified OPF problem, namely the DC-OPF. In this formulation, the network model is simplified by neglecting the losses, the reactive power, and assuming the voltage magnitudes to be constant, usually called the DC network model.

Let N, N_g, and N_b be the number of buses, generator buses, and transmission lines in the power network, respectively. The variables considered in the DC-OPF problem are:

- $P^d \in \mathbf{R}^N$: the active power demand;
- $P^g \in \mathbf{R}^{N_g}$: the active power generation;
- $\theta \in \mathbf{R}^{N-1}$: the phase-angle at each bus, except the reference bus, for which $\theta_1 = 0$;
- $P^f \in \mathbf{R}^{N_b}$: the active power flow on each transmission line.

The active power demand $P^d \leq 0$ is supplied to the DC-OPF as a known parameter, while the power generated at all generator buses, P^g, are the decision variables constrained by $\overline{P^g} \geq P^g \geq 0$. In the DC network model the power balance equations provide a linear relation between the phase-angles and the power demand, generation, and flows:

$$\begin{bmatrix} C_g P^g + P^d \\ P^f \end{bmatrix} = \begin{bmatrix} H_i \\ H_f \end{bmatrix} \theta = H\theta, \tag{1}$$

where $C_g \in \mathbf{R}^{N \times N_g}$ is the bus to generator incidence matrix, mapping the generators to the respective buses and $H \in \mathbf{R}^{(N+N_b)\times(N-1)}$ represents the network model, containing information regarding the network topology and model parameters [17]. To mantain the power balance, a given generator bus can be selected as the slack bus and the corresponding generated power is determined so that the demand is met, namely

$$\mathbf{1}^\top P^g + \mathbf{1}^\top P^d = 0 \tag{2}$$

in the lossless case.

Assuming the power network is connected, by removing the row corresponding to the chosen slack bus from H_i we obtain an invertible matrix $\bar{H}_i = \Pi_s H_i$, where Π_s is the matrix representing the row removal operation. We can then obtain θ as a function of P^g and P^d with $\theta = \bar{H}_i^{-1}\Pi_s(C_g P^g + P^d)$ and the power flows can be written as

$$P^f = H_f(\Pi_s H_i)^{-1}\Pi_s(C_g P^g + P^d) = G_g P^g + G_d P^d. \tag{3}$$

Thermal limitations on the transmission lines introduce operation limits on the power flows, $|P^f| \leq \overline{P^f}$, where $\overline{P^f} \in \mathbf{R}^{N_b}$ contains the power flow limits for each transmission line and $|\cdot|$ is an element-wise operation. At the same time, there is an operation cost associated to each generator k, $c_k(P_k^g) = c_{k2}(P_k^g)^2 + c_{k1}P_k^g + c_{k0}$ with $c_{k2} > 0$. Defining $\bar{c}_i = \begin{bmatrix} c_{1i} & \cdots & c_{N_g i} \end{bmatrix}^\top$ for $i \in \{0, 1, 2\}$, the corresponding total generation cost is given by

$$c(P^g) = \sum_{k=1}^{N_g} c_k(P_k^g) = \frac{1}{2} P^{g\top} Q P^g + R^\top P^g + C_0, \tag{4}$$

with $Q = \operatorname{diag}(2\bar{c}_2)$, $R = \bar{c}_1$, and $C_0 = \mathbf{1}^\top \bar{c}_0$. The purpose of DC-OPF is then to minimize the total generation cost subject to the operation limits of the transmission lines and generators, which can be formulated as the following optimization problem

$$\begin{aligned} \min_{P^g} \quad & c(P^g) \\ \text{s.t.} \quad & h(P^g, P^d) = \mathbf{1}^\top P^g + \mathbf{1}^\top P^d = 0 \\ & f(P^g, P^d) = F_g P^g + F_d P^d + F_0 \leq 0, \end{aligned} \tag{5}$$

with

$$F_g = \begin{bmatrix} G_g \\ -G_g \\ I \\ -I \end{bmatrix}, \quad F_d = \begin{bmatrix} G_d \\ -G_d \\ 0 \\ 0 \end{bmatrix}, \quad F_0 = \begin{bmatrix} -\overline{P^f} \\ -\overline{P^f} \\ -\overline{P^g} \\ 0 \end{bmatrix}.$$

The Lagrangian function for this problem can be written as

$$\begin{aligned} L(P^g, \nu, \lambda) = c(P^g) + \nu(\mathbf{1}^\top P^g + \mathbf{1}^\top P^d) \\ + \lambda^\top(F_g P^g + F_d P^d + F_0), \end{aligned}$$

where ν and $\lambda \geq 0$ are the dual variables. In the following, we assume the DC-OPF problem is always feasible.

A. Optimal Solution

The DC-OPF problem (5) is a strictly convex problem, since the constraints form a convex set and the objective function is quadratic with Q being positive definite given that $c_{k2} > 0 \, \forall k$. Therefore, for given P^d, the DC-OPF admits a unique optimal solution which we denote by

$$P^{g*} = \Omega(P^d), \tag{6}$$

having the associated nominal optimal cost $c^* = c(P^{g*})$ and optimal power flows $P^{f*} = G_g P^{g*} + G_d P^d$. Given that the DC-OPF is a convex problem, a feasible optimal solution satisfies the the KKT conditions:

$$\begin{aligned}
0 &= \nabla c(P^{g*}) + \nabla h(P^{g*}, P^d)^\top \nu^* \\
&\quad + \nabla f(P^{g*}, P^d)^\top \lambda^* \\
0 &= h(P^{g*}, P^d) \\
0 &= \lambda_i^* f_i(P^{g*}, P^d), \quad \forall i = 1, \ldots, N_f \\
0 &\leq \lambda^*,
\end{aligned}$$

where $N_f = 2(N_b + N_g)$ is the number of inequality contraints.

According to the KKT conditions [18], only the dual variables associated with active constraints are nonzero in the optimal solution. We denote the number of active and inactive inequality constraints as N_1 and $N_0 = N_f - N_1$, respectively. Considering the total generation cost (4) and denoting $H_1 \in \mathbf{R}^{N_1 \times N_f}$ and $H_0 \in \mathbf{R}^{N_0 \times N_f}$ as the "selector matrices" selecting the active and inactive constraints at the optimal solution, respectively, the KKT conditions become

$$\begin{bmatrix} Q & F_g^\top & \mathbf{1} \\ \mathbf{1}^\top & 0 & 0 \\ H_1 F_g & 0 & 0 \\ 0 & H_0 & 0 \end{bmatrix} \begin{bmatrix} P^{g*} \\ \lambda^* \\ \nu^* \end{bmatrix} = \begin{bmatrix} -R \\ -\mathbf{1}^\top (P^d) \\ H_1(-F_d P^d - F_0) \\ 0 \end{bmatrix},$$

which we rewrite as

$$K \begin{bmatrix} P^{g*} \\ \lambda^* \\ \nu^* \end{bmatrix} = \begin{bmatrix} -R \\ -\mathbf{1}^\top P^d \\ H_1(-F_d P^d - F_0) \\ 0 \end{bmatrix}. \tag{7}$$

Proposition 1: For any feasible optimal solution $P^{g*} = \Omega(P^d)$, λ^*, and ν^*, the corresponding matrix $K \in \mathbf{R}^{(N_g+N_f+1)\times(N_g+N_f+1)}$ is invertible.

Proof: Since the DC-OPF is a strictly convex optimization problem, there exists a unique optimal solution. Furthermore, since all inequality constraints are linear, strong duality holds and the KKT conditions (7) are necessary and sufficient for any feasible solution to be optimal. Hence (7) has a single solution, which requires K to be invertible. ■

B. Nominal Optimal Operation

In general the full state of the power network is not directly available to the operator. Instead, the network state is estimated based on a large amount of measurements and a known measurement model, as explained in [17].

Denoting $\hat{P}^g$, $\hat{P}^d$, and $\hat{P}^f$ as the estimated power generation, demand, and flows, the current *estimated operation cost* is

$$\hat{c} = c(\hat{P}^g) \tag{8}$$

and the OPF problem solved is in fact

$$\begin{aligned}
\min_{P^g} \quad & c(P^g) \\
\text{s.t.} \quad & \mathbf{1}^\top P^g + \mathbf{1}^\top \hat{P}^d = 0 \\
& F_g P^g + F_d \hat{P}^d + F_0 \leq 0.
\end{aligned}$$

Let us consider a system in which the estimated demand equals the true demand $\hat{P}^d = P^d$ (i.e., measurements are accurate). Applying $P^{g*} = \Omega(\hat{P}^d)$ to the system would then result in $\hat{P}^g = P^{g*}$ and $\hat{P}^f = P^{f*}$. We refer to this system as the system in *nominal optimal operation*.

Assumption 1: The system operates in optimality, that is, $\hat{P}^g = P^{g*}$ and $\hat{P}^f = P^{f*}$ for the given $\hat{P}^d = P^d$.

III. Simplified OPF under a Data Attack

As mentioned in the previous section, the input parameters to the DC-OPF are obtained either from direct measurement or through state estimation and are therefore vulnerable to malicious data corruption of the measurement data.

Now consider the case where the data attack illustrated in Fig. 1 has been performed such that the corrupted estimates become

$$\hat{P}_a^g = P^{g*} + a_g = \hat{P}^g + a_g \tag{9}$$

$$\hat{P}_a^f = P^{f*} + a_f = \hat{P}^f + a_f \tag{10}$$

$$\hat{P}_a^d = P^d + a_d = \hat{P}^d + a_d \tag{11}$$

where a_g, a_d, and a_f are the corrupted data added to the measurements so that they fulfill (1) for some θ. That is, the attack is undetectable using standard bad-data detection based on the DC network model, see [6], [7], [8], [9].

Remark 1: Given the corrupted estimate $\hat{P}_a^g$, the operator believes that the power network is operating at the *estimated operation cost* $c(\hat{P}_a^g)$.

After receiving the corrupted measurements and computing the state estimates $\hat{P}_a^d$, the operator solves the DC-OPF problem and obtains the corresponding optimal solution $\hat{P}_a^{g*} = \Omega(\hat{P}_a^d)$. Before characterizing the DC-OPF solution given the corrupted measurements, we make the following assumption.

Assumption 2: The data corruptions a_g, a_d, and a_f are such that the active constraints for $P^{g*} = \Omega(P^d)$ remain the same for $\hat{P}_a^{g*} = \Omega(\hat{P}_a^d)$.

Conditions enforcing the above assumption to hold may be found in the Appendix.

In the remainder of this section we discuss the consequences of the data corruption attack. First we characterize the data

attack impact on the DC-OPF solution and under what conditions the operator may decide to apply the generation profile recommended by the DC-OPF under data attack. Assuming the operator accepts the DC-OPF recommendation, the discussion then proceeds by examining the true economical losses of that decision.

A. Consequences on the DC-OPF solution

The DC-OPF solution given $\hat{P}_a^d$ can be computed using the KKT conditions in (7). Furthermore, based on Assumption 2, the difference in the optimal solutions $\hat{P}_a^{g*} = \Omega(\hat{P}_a^d)$ and $P^{g*} = \Omega(P^d)$ is given by

$$\begin{bmatrix} \hat{P}_a^{g*} - P^{g*} \\ \hat{\lambda}_a^* - \lambda^* \\ \hat{\nu}_a^* - \nu^* \end{bmatrix} = K^{-1} \begin{bmatrix} 0 \\ -\mathbf{1}^\top \\ -H_1 F_d \\ 0 \end{bmatrix} a_d = \begin{bmatrix} T_g \\ T_\lambda \\ T_\nu \end{bmatrix} a_d, \quad (12)$$

and so we can write

$$\hat{P}_a^{g*} - P^{g*} = T_g a_d. \quad (13)$$

At this point, the operator believes the power network can be operated at the *estimated optimal operation cost* $c(\hat{P}_a^{g*})$ if the DC-OPF recommendation is applied.

Given the corrupted power generation estimates $\hat{P}_a^g$, the current *estimated operation cost* computed by the operator is $c(\hat{P}_a^g)$. Running the DC-OPF based on the corrupted load estimates $\hat{P}_a^d$ will provide the operator with the estimated optimal operation cost $c(\hat{P}_a^{g*})$. The difference between the estimated operation cost $c(\hat{P}_a^g)$ and the estimated optimal operation cost $c(\hat{P}_a^{g*})$ corresponds to the *estimated re-dispatching profit* if the power generation is re-dispatched according to the DC-OPF, which we now define using (9) and (13).

Definition 1 (Estimated Re-Dispatching Profit): The *estimated re-dispatching profit* is defined as

$$\hat{\mathcal{P}}_a \triangleq c(\hat{P}_a^g) - c(\hat{P}_a^{g*}). \quad (14)$$

Since the DC-OPF active and inactive constraints at optimality remain the same after the data corruptions given Assumption 2, from the optimality principle we conclude that $\hat{\mathcal{P}}_a \geq 0$. A large value of $\hat{\mathcal{P}}_a$ can make the operator update the generator set-points, as there seems to be an incentive to do so. Note however that both these cost might be fictitious, since the estimates have been corrupted.

B. Consequences on the physical network

Consider that the operator decides to apply the generation profile $\hat{P}_a^{g*} = \Omega(\hat{P}_a^d)$ recommended by the DC-OPF under attack. In reality, the power demand may be different from the respective estimate, i.e. $P^d \neq \hat{P}^d$. This occurs for any data corruption attack with $a_d \neq 0$. Therefore there might exist a mismatch between the demand and generation, which has to be compensated by the slack generator so that the power balance equation (2) is satisfied. Choosing generator 1 as the slack, the power generated by this bus is then a function of the power imbalance

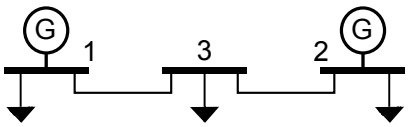

Fig. 2. Three bus network with two transmission lines. The generations are $P_1^g, P_2^g \geq 0$ and the loads are $P_1^d, P_2^d, P_3^d \leq 0$.

$$P_{a,1}^{g*} = -\sum_{i=2}^{N_g} \hat{P}_{a,i}^{g*} - 1^\top P^d. \quad (15)$$

Hence the real generation profile after attack is $P_a^{g*} = [P_{a,1}^{g*}\ \hat{P}_{a,2}^{g*} \cdots \hat{P}_{a,N_g}^{g*}]^\top$, yielding a *true operation cost* $c(P_a^{g*})$.

Assuming the operator applies the DC-OPF recommendation, the *true re-dispatching profit* due to the data corruption attack is defined as follows.

Definition 2 (True Re-Dispatching Profit): The *true re-dispatching profit* is defined as

$$\mathcal{P}_a \triangleq c(P^{g*}) - c(P_a^{g*}). \quad (16)$$

Recalling that there is no actual change on the power demand P^d, P^g is the true unique optimal solution of the DC-OPF problem. Therefore any other feasible solution yields a higher true operation cost and results in a negative $\mathcal{P}_a$. However, note that the true generation profile P_a^{g*} is determined in open-loop by the slack generator, which could drive the power network out of the feasible region and into an unsafe state. The reduced safety in this case would lead to a lower operation cost, resulting in a positive $\mathcal{P}_a$. Hence any non-zero true re-dispatch profit $\mathcal{P}_a$ may indicate negative consequences to the power network operation.

The true power generation difference $P_a^{g*} - P^{g*}$ is of interest to assess both $\mathcal{P}_a$ and the true power network state, which can be computed using (2), (13), and (15)

$$P_a^{g*} - P^{g*} = M T_g a_d \quad (17)$$

with

$$M = \begin{bmatrix} 0 & -\mathbf{1}^\top \\ 0_{N_g-1\times 1} & I_{N_g-1} \end{bmatrix}.$$

Note that M is associated with the type of slack generation in the power network and therefore it may differ, for instance, if a type of distributed slack is considered.

In the next section we consider a simple analytical example to illustrate the discussion in the current section.

IV. Analytical Example

In this section we illustrate the effects of attacks on the DC-OPF problem (5) for the power network in Fig. 2 assuming a scenario where there are no saturated tie lines or generators, namely $|P^{f*}| < \overline{P^f}$ and $0 < P^{g*} < \overline{P^g}$.

Applying the KKT conditions (7) to this case, we obtain the following optimal generation profile

$$P_1^{g*} = \frac{-c_{11} + c_{21} - 2c_{22}(P_1^d + P_2^d + P_3^d)}{2(c_{12} + c_{22})}$$
$$P_2^{g*} = \frac{c_{11} - c_{21} - 2c_{12}(P_1^d + P_2^d + P_3^d)}{2(c_{12} + c_{22})}$$

where we see the generated power depends on the generation costs. We now analyze the consequences of data corruption for this nominal operation scenario under Assumption 2.

Let us now consider that the measurements are corrupted as in (9)–(11). The optimal generation profile, given the corrupted load estimates $\hat{P}_a^d$, is obtained by solving (7). For this scenario the solution is

$$\hat{P}_{a,1}^{g*} = \frac{-c_{11} + c_{21} - 2c_{22}(\hat{P}_{a,1}^d + \hat{P}_{a,2}^d + \hat{P}_{a,3}^d)}{2(c_{12} + c_{22})}$$
$$\hat{P}_{a,2}^{g*} = \frac{c_{11} - c_{21} - 2c_{12}(\hat{P}_{a,1}^d + \hat{P}_{a,2}^d + \hat{P}_{a,3}^d)}{2(c_{12} + c_{22})}$$

and the difference to the previous optimal generation profile P^{g*} is

$$\hat{P}_a^{g*} - P^{g*} = Ta_d = \frac{-1}{(c_{12} + c_{22})} \begin{bmatrix} c_{22} \\ c_{12} \end{bmatrix} \mathbf{1}^\top a_d. \tag{18}$$

To illustrate the previous discussion, we now present two particular data attack scenarios based on the example network in Fig. 2.

Consider P_1 acts as the slack bus and recall Assumption 1, which states that the system operates under optimality before the data attack. Furthermore, assume no lines are saturated and consider the data attack $a = \begin{bmatrix} a_g^\top & a_d^\top & a_f^\top \end{bmatrix}^\top$ and the corresponding attack vector on the power injection and flow measurements $\bar{a} = [a_i^\top \quad a_f^\top]^\top$, where

$$\bar{a} = \begin{bmatrix} C_g & I & 0 \\ 0 & 0 & I \end{bmatrix} \begin{bmatrix} a_g \\ a_d \\ a_f \end{bmatrix} = \Gamma a. \tag{19}$$

1) Scenario 1: ($c_{22} \gg c_{12}$): In this scenario the marginal cost of generator 2 is considered to be much higher than that of generator 1, hence in optimality it would be expected that an increase in the load demand would be compensated mainly by generator 1. Indeed using (18) we have

$$\hat{P}_{a,1}^{g*} - P_1^{g*} = \frac{-c_{22}}{(c_{12} + c_{22})} \mathbf{1}^\top a_d \approx -\mathbf{1}^\top a_d$$
$$\hat{P}_{a,2}^{g*} - P_2^{g*} = \frac{-c_{12}}{(c_{12} + c_{22})} \mathbf{1}^\top a_d \approx 0.$$

meaning that the DC-OPF compensates small load changes solely through the cheapest bus, which happens to be the slack bus. Recalling that in open-loop, i.e., without the DC-OPF, load changes are compensated by the slack bus, a direct consequence is that the true and estimated generator profile after applying the DC-OPF's recommendation are the same, as we can see from (17) and (18):

$$P_a^{g*} - P^{g*} = MT_g a_d = \begin{bmatrix} 0 & -1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} -\mathbf{1}^\top \\ 0 \end{bmatrix} a_d = 0.$$

Hence for all attacks $\mathcal{P}_a = 0$, i.e. there is no economic impact even if the DC-OPF solution is applied.

2) Scenario 2: ($c_{22} \ll c_{12}$): As opposed to the previous scenario, here the marginal cost of generator 2 is the lowest and hence we have

$$\hat{P}_{a,1}^{g*} - P_1^{g*} = \frac{-c_{22}}{(c_{12} + c_{22})} \mathbf{1}^\top a_d \approx 0$$
$$\hat{P}_{a,2}^{g*} - P_2^{g*} = \frac{-c_{12}}{(c_{12} + c_{22})} \mathbf{1}^\top a_d \approx -\mathbf{1}^\top a_d,$$

indicating that small load changes are compensated by DC-OPF through the cheapest generator, which in this case is not the slack bus. Thus the DC-OPF and open-loop load compensations differ, possibly resulting in economic incentives to use the DC-OPF recommendation. In fact, using (9) and (13) we can rewrite the estimated re-dispatching profit as

$$\hat{\mathcal{P}}_a = c(\hat{P}_a^{g*} + a_g - T_g a_d) - c(\hat{P}_a^{g*}),$$

which indicates that

$$a_g - T_g a_d = \begin{bmatrix} a_{g,1} \\ a_{g,2} + \mathbf{1}^\top a_d \end{bmatrix}$$

plays an important role in the estimated re-dispatching profit $\hat{\mathcal{P}}_a$. This is further illustrated for two sparse attack examples.

Suppose that all the power flows, demand, and generation are being measured, except for the demand in bus 3, P_3^d. It can be shown that in this case no $1-$sparse data attacks exist and there are only two $2-$sparse attack patterns, namely attacks on measurements $\{a_{i,1},\, a_{f,13}\}$ and $\{a_{i,2},\, a_{f,23}\}$, where $a_{i,j} = a_{g,j} + a_{d,j}$ is the attack on the injection measurement of bus j. Furthermore, given the DC power flow equations, $P_{13}^f = P_1^g + P_1^d$ and $P_{23}^f = P_2^g + P_2^d$, these attacks are constrained by $a_{i,1} = a_{f,13}$ and $a_{i,2} = a_{f,23}$, respectively.

Consider the $2-$sparse attack on $\{a_{i,1},\, a_{f,13}\}$, $\bar{a}_1 = [a_{i,1} \quad a_{f,13}]^\top$ with $a_{i,1} = a_{f,13} = \epsilon$, $a_{g,1} = \epsilon$, and $a_{d,1} = 0$. Noticing that $P_3^d + P_{13}^f + P_{23}^f = 0$ is also a network equation, we then have that this data attack induces the following bias in $\hat{P}_{a,3}^d$: $a_{d,3} + a_{f,13} + a_{f,23} = 0 \Rightarrow a_{d,3} = -a_{f,13} + 0 = -\epsilon$. Thus for $\bar{a}_1$ we have

$$a_g - T_g a_d = \begin{bmatrix} a_{g,1} \\ a_{g,2} + a_{d,1} + a_{d,3} \end{bmatrix} = \begin{bmatrix} \epsilon \\ -\epsilon \end{bmatrix},$$

which results in a positive estimated re-dispatching profit, $\hat{\mathcal{P}}_a(\bar{a}_1) > 0$.

Considering now the other $2-$sparse attack on $\{a_{i,2},\, a_{f,23}\}$, $\bar{a}_2 = [a_{i,2} \quad a_{f,23}]^\top$ with $a_{i,2} = a_{f,23} = \epsilon$, $a_{g,2} = \epsilon$, and $a_{d,2} = 0$. Similarly as before, this data attack induces a bias in $\hat{P}_{a,3}^d$: $a_{d,3} + a_{f,13} + a_{f,23} = 0 \Rightarrow a_{d,3} = 0 - a_{f,23} = -\epsilon$, resulting in

$$a_g - T_g a_d = \begin{bmatrix} a_{g,1} \\ a_{g,2} + a_{d,2} + a_{d,3} \end{bmatrix} = \begin{bmatrix} 0 \\ \epsilon + 0 - \epsilon \end{bmatrix} = 0.$$

Hence for this attack we conclude $\hat{\mathcal{P}}_a(\bar{a}_2) = 0$ and therefore the attack has no impact on the power network.

From these two examples we conclude that only the data attack $\bar{a}_1$ may lead the operator to re-dispatch the power

generation, while $\bar{a}_2$ will have no impact in the power network. Therefore $\bar{a}_1$ is more dangerous than $\bar{a}_2$, even though they have the same sparsity, which motivates the need for tools to analyze the system vulnerability while evaluating the attack impact.

V. Impact-Aware Security Index

In previous work [7], the vulnerability of each measurement k was evaluated by studying the following problem:

Problem 1: Given a data attack targeting measurement k, what is the minimal number of attacked sensors so that the data attack is undetectable by the Bad Data Detection?

This problem was formulated as an optimization problem

$$\begin{aligned} \alpha_k := \min_{\theta} \quad & \|W\bar{a}\|_0 \\ \text{s.t.} \quad & \bar{a} = H\theta \ , \\ & 1 = e_k^\top \bar{a}, \end{aligned} \tag{20}$$

where $\bar{a} = \Gamma a$ is defined in (19), W is a diagonal matrix of zeros and ones that indicate whether a particular flow or injection is measured or not, and e_k is a vector of zeros with the $k-$th entry set to 1. The resulting optimal value α_k was taken as a security index for measurement k. Defensive actions to secure the state estimator using this security index were then proposed in [11].

Note however the proposed index does not consider the data attack impact on the power network operation. In fact, different data attacks with the same sparsity $\|\bar{a}_k^*\|_0 = \|\bar{a}_j^*\|_0$ are considered equally dangerous, even though they might have considerably different impacts, as seen in Section IV.

In this section we propose a modification to the security index in (20) taking into account the impact of the data attack on the DC-OPF. This modification addresses the following

Problem 2: Given a data attack targeting measurement k, what is the minimal number of attacked sensors such that the data attack is undetectable by the Bad Data Detection, the operator decides to apply the corrupted DC-OPF recommendation, and the power network operation is affected?

This problem is addressed for a given initial demand P^d and the corresponding optimal dispatch P^{g*} using the results in the previous sections. Our goal is to provide to the operator security indices designed to quantify the vulnerability to *and* impact of data attacks on the several measurements. As a result, the measurements with the highest index would be candidates for protection, similarly to the approach in [11].

Recalling the discussion in Section II, we have two measures of the data attack impact, namely the *estimated re-dispatch profit* $\hat{\mathcal{P}}_a$ and the *true re-dispatch profit* $\mathcal{P}_a$. To address Problem 2, the following optimization problem is proposed:

$$\beta_k := \min_{\theta} \quad \|W\Gamma a\|_0 \tag{21a}$$

$$\text{s.t.} \quad \Gamma a = H\theta \tag{21b}$$

$$\epsilon = |e_k^\top \Gamma a| \tag{21c}$$

$$\hat{\xi} \leq \hat{\mathcal{P}}_a \tag{21d}$$

$$\xi \leq |\mathcal{P}_a|. \tag{21e}$$

The constraint $|e_k^\top \Gamma a| = \epsilon$ normalizes the solution and requires the k-th measurement to be attacked. It says the attacker is willing to add or subtract ϵ *per units* of power in that measurement. The parameter $\hat{\xi}$ is a threshold that quantifies how much the estimated re-dispatch profit must be for the operator to decide to re-dispatch the generation. The other threshold ξ quantifies how much the true re-dispatch profit must be for the attack to be considered harmful.

Note that $\hat{\xi}$ and ξ depend on the size of the data corruption ϵ. One could set $\epsilon = 1$ and tune $\hat{\xi}$ and ξ accordingly. Obviously the original security index is recovered for $\hat{\xi} = \xi = 0$. However there are other conditions under which both problems yield the same solution, as discussed below.

A. Connections to Problem 1

Recall the original security index described in (20).

Proposition 2: Given any optimal solution to the security index in (20) a_k^*, there exists a scalar m such that ma_k^* is an optimal solution to the optimization problem (21) if and only if $\hat{\mathcal{P}}_a(a_k^*) \neq 0$ and $\mathcal{P}_a(a_k^*) \neq 0$.

Proof: Assume that $\hat{\mathcal{P}}_a(a_k^*) \neq 0$. Then for a sufficiently large $|m|$, either $|m|a_k^*$ or $-|m|a_k^*$ satisfies (21d). Regarding the constraint (21e), note that it is not affected by the sign of a_k^*, as the constraint depends on the absolute value of $\mathcal{P}_a(a_k^*)$. Hence, assuming $\mathcal{P}_a(a_k^*) \neq 0$ holds, the scaled solution $\pm|m|a_k^*$ satisfying (21d) can be scaled once more so that (21e) holds.

If either $\hat{\mathcal{P}}_a(a_k^*) = 0$ or $\mathcal{P}_a(a_k^*) = 0$, then it is clearly not possible to satisfy both (21d) and (21e). ■

Proposition 3: For any optimal solution a_k^* to the optimization problem (20) satisfying $\hat{\mathcal{P}}_a(a_k^*) \neq 0$ and $\mathcal{P}_a(a_k^*) \neq 0$ there exists a large enough ϵ so that a_k^* is a solution to the optimization problem (21) subject to (21b)–(21e).

Proof: Take the limit $\epsilon \to \infty$ and use Proposition 2. ■

Proposition 3 tells us that choosing ϵ large enough will give the same results as the security index proposed in [7]. However, note that the attack needs to be such that Assumption 2 holds, thus these indices may in fact be different. We refer to the Appendix for conditions enforcing Assumption 2 that can be included in the optimization problem (21). Further analysis of the optimization problem (21) and heuristics to solve it are subject of future work.

VI. Conclusions and Future Work

In this paper we addressed the DC-OPF-based power network operation in the presence of stealthy data corruption attacks on the measurements. Given the biased estimates resulting from the measurement corruption, we derived analytical expressions characterizing the behavior of the DC-OPF for attacks that do not affect the system operating constraints. Based on these expressions, we discussed under what conditions a human operator would have the incentive to close the loop over the corrupted measurements . The economic impact of applying these erroneous control actions was also discussed and analytically characterized.

The above results led to our second contribution: an impact-aware security index for the measurements, quantifying their vulnerability to attacks and the corresponding impact on the network when the attacked control action is accepted and applied by the operator. Efficient methods to compute or approximate the proposed non-convex problem are subject of future work.

The concepts and results in the paper are illustrated using a three bus example, for which some motivating scenarios are also considered.

ACKNOWLEDGEMENTS

The authors would like to thank Dr. Kin Cheong Sou for helpful discussions.

REFERENCES

[1] A. Giani, S. Sastry, K. H. Johansson, and H. Sandberg, "The VIKING project: an initiative on resilient control of power networks," in *Proc. 2nd Int. Symp. on Resilient Control Systems*, Idaho Falls, ID, USA, Aug. 2009.

[2] A. Cárdenas, S. Amin, and S. Sastry, "Research challenges for the security of control systems." in *Proc. 3rd USENIX Workshop on Hot topics in security*, July 2008.

[3] "Electricity grid in U.S. penetrated by spies," *The Wall Street Journal*, p. A1, April 8th 2009.

[4] "Cyber war: Sabotaging the system," *CBSNews*, November 8th 2009. [Online]. Available: http://www.cbsnews.com/stories/2009/11/06/60minutes/main5555565.shtml

[5] Symantech, "Stuxnet introduces the first known rootkit for industrial control systems," August 6th 2010. [Online]. Available: http://www.symantec.com/connect/blogs/stuxnet-introduces-first-known-rootkit-scada-devices

[6] Y. Liu, M. K. Reiter, and P. Ning, "False data injection attacks against state estimation in electric power grids," in *Proc. 16th ACM Conf. on Computer and Communications Security*, New York, NY, USA, 2009.

[7] H. Sandberg, A. Teixeira, and K. H. Johansson, "On security indices for state estimators in power networks," in *Preprints of the First Workshop on Secure Control Systems, CPSWEEK 2010*, Stockholm, Sweden, April 2010.

[8] R. Bobba, K. M. Rogers, Q. Wang, H. Khurana, K. Nahrstedt, and T. Overbye, "Detecting false data injection attacks on DC state estimation," in *Preprints of the First Workshop on Secure Control Systems, CPSWEEK 2010*, Stockholm, Sweden, April 2010.

[9] A. Giani, E. Bitar, M. McQueen, P. Khargonekar, K. Poolla, and M. Garcia, "Smart grid data integrity attacks: Characterizations and countermeasures," in *Proc. of IEEE SmartGridComm*, Brussels, Belgium, Oct. 2011.

[10] A. Teixeira, G. Dán, H. Sandberg, and K. H. Johansson, "Cyber security study of a scada energy management system: stealthy deception attacks on the state estimator," in *Proc. of 18th IFAC World Congress*, Milan, Italy, Aug. 2011.

[11] G. Dán and H. Sandberg, "Stealth attacks and protection schemes for state estimators in power systems," in *Proc. of IEEE SmartGridComm*, Gaithersburg, MD, USA, Oct. 2010.

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

[13] K. C. Sou, H. Sandberg, and K. H. Johansson, "Electric power network security analysis via minimum cut relaxation," in *Proc. of 50th IEEE Conf. on Decision and Control*, Orlando, FL, USA, Dec. 2011.

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

[15] L. Jia, R. J. Thomas, and L. Tong, "Malicious data attack on real-time electricity market," in *Proc. of IEEE ICASSP*, May 2011.

[16] Y. Yuan, Z. Li, and K. Ren, "Modeling load redistribution attacks in power systems," *IEEE Trans. Smart Grid*, no. 2, Jun. 2011.

[17] A. Monticelli, "Electric power system state estimation," in *Proc. IEEE*, vol. 88, no. 2, Feb. 2000.

[18] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge University Press, 2004.

APPENDIX
ENFORCING ASSUMPTION 2

The analysis in Sections III–V remains valid as long as Assumption 2 holds. To strengthen the validity of the analysis, here we discuss on what conditions Assumption 2 holds.

Theorem 1: The necessary and sufficient conditions for Assumption 2 to hold are

$$\begin{bmatrix} -H_1 T_\lambda \\ H_0(F_g T_g + F_d) \end{bmatrix} a_d < \begin{bmatrix} H_1 \lambda^* \\ H_0(-F_g P^{g*} - F_d P^d - F_0) \end{bmatrix}$$
$$\begin{bmatrix} H_0 T_\lambda \\ H_1(F_g T_g + F_d) \end{bmatrix} a_d = \begin{bmatrix} 0 \\ H_1(-F_g P^{g*} - F_d P^d - F_0) \end{bmatrix}.$$

Proof: Consider the set of primal and dual variables computed based on corrupted data using (7) and (12)

$$\begin{bmatrix} \hat{P}_a^{g*} \\ \hat{\lambda}_a^* \\ \hat{\nu}_a^* \end{bmatrix} = \begin{bmatrix} T_g \\ T_\lambda \\ T_\nu \end{bmatrix} a_d + \begin{bmatrix} P^{g*} \\ \lambda^* \\ \nu^* \end{bmatrix}.$$

Note that Assumption 2 is equivalent to the optimality of the primal and dual variables $\begin{bmatrix} \hat{P}_a^{g*\top} & \hat{\lambda}_a^{*\top} & \hat{\nu}_a^{*\top} \end{bmatrix}^\top$ for the DC-OPF problem with corrupted data. Thus the necessary and sufficient conditions for Assumption 2 to hold correspond to the KKT optimality conditions.

By construction, all primal and dual variables computed using (7) satisfy $\nabla L(\hat{P}_a^{g*}, \hat{\nu}_a^*, \hat{\lambda}_a^*) = 0$ and $h(\hat{P}_a^{g*}, \hat{P}_a^d) = 0$. Thus only the inequality constraints need to be considered.

Regarding the dual variables of the inequality constraints, the variables corresponding to active constraints are positive, while the remaining variables are zero, yielding

$$H_1 \hat{\lambda}_a^* = H_1 T_\lambda a_d + H_1 \lambda^* > 0$$
$$H_0 \hat{\lambda}_a^* = H_0 T_\lambda a_d = 0.$$

To conclude the proof, note that the primal variables also need to be constrained so that the active and inactive inequality constraints remain unchanged, leading to the following conditions

$$H_1(F_g T_g + F_d) a_d = H_1(-F_g P^{g*} - F_d P^d - F_0)$$
$$H_0(F_g T_g + F_d) a_d < H_0(-F_g P^{g*} - F_d P^d - F_0).$$

■