INL/CON-11-24105
PREPRINT

Metrics for Assessment of Smart Grid Data Integrity Attacks

IEEE Power & Energy Society General Meeting: Energy Horizons - Opportunities and Challenges

Annarita Giani
Russell Bent
Mark Hinrichs
Miles McQueen
Kameshwar Poolla

July 2012

The INL is a
U.S. Department of Energy
National Laboratory
operated by
Battelle Energy Alliance

Metrics for Assessment of Smart Grid Data Integrity Attacks

Annarita Giani*, Russell Bent†, Mark Hinrichs†, Miles McQueen‡, Kameshwar Poolla§

*CNLS, Los Alamos National Laboratory
†D-4, Los Alamos National Laboratory
‡Idaho National Laboratory
§University of California at Berkeley

***Abstract*—There is an emerging consensus that the nation's electricity grid is vulnerable to cyber attacks. This vulnerability arises from the increasing reliance on using remote measurements, transmitting them over legacy data networks to system operators who make critical decisions based on available data.**

Data integrity attacks are a class of cyber attacks that involve a compromise of information that is processed by the grid operator. This information can include meter readings of injected power at remote generators, power flows on transmission lines, and relay states. These data integrity attacks have consequences only when the system operator responds to compromised data by re-dispatching generation under normal or contingency protocols. These consequences include (a) financial losses from sub-optimal economic dispatch to service loads, (b) robustness/resiliency losses from placing the grid at operating points that are at greater risk from contingencies, and (c) systemic losses resulting from cascading failures induced by poor operational choices.

This paper is focussed on understanding the connections between grid operational procedures and cyber attacks. We first offer an example to illustrate how data integrity attacks can cause economic and physical damage by misleading operators into taking inappropriate decisions. We then focus on unobservable data integrity attacks involving power meter data. These are coordinated attacks where the compromised data is consistent with the physics of power flow, and is therefore passed by any bad data detection algorithm. We develop metrics to assess the economic impact of these attacks under operator re-dispatch decisions using optimal power flow methods. These metrics can be used to prioritize the adoption of appropriate countermeasures including PMU placement, encryption, hardware upgrades, and advanced detection algorithms.

I. Introduction

Cybersecurity of critical infrastructures in general, and the electricity grid in particular, is a subject of increasing research interest [1], [2]. The economic consequences of successful cyberattacks on the electricity grid are potentially staggering. Energy Management Systems [EMS] are ubiquitous in electric grid operations and present potential targets for cyberattacks. These systems are based on SCADA [Supervisory Control and Data Acquisition] hardware and software components and are used to supervise, control, optimize, and manage electricity generation and transmission systems. As the grid evolves, legacy SCADA systems will co-exist and inter-operate with new components [ex: smart meters], networks [ex: NASPInet] [3], sensors [ex: phasor measurement units or PMUs] [4], and control devices [ex: intelligent relays] [5], [6]. Tomorrow's Smart Grid will incorporate increased sensing, communication, and distributed control to accommodate renewable generation, EV [Electric Vehicle] loads, storage, and many other technologies. This substantial increase in actionable data transfers will make the Smart Grid more vulnerable to cyber attacks and is, in turn, driving the urgency of cybersecurity research for electricity grids.

An important class of cyber attacks are *data integrity* attacks. These consist of a set of compromised sensors (ex: power meters, relays) whose readings are altered by the attacker. Much of the research on data integrity attacks in power systems has been on studying taxonomy, developing detection algorithms, and devising various countermeasures. In particular, many recent papers have explored various aspects of data integrity attacks on SCADA/EMS systems that impact the key function of state estimation. These include computation and characterization of the attacks, and various detection and mitigation strategies based on secure PMU placement [7], [8], [9], [10], [11].

Data integrity attacks are of consequence only when the system operator reacts to the compromised data and is misled into taking uneconomical or even catastrophic decisions. There is some research on analysing integrity attacks in the context of subsequent operator actions. A detailed two-year study by Sandia [12] investigated the possible impacts of cyber attack on grid control systems using novel cyber-to-physical (C2P) bridge concepts. However, there is little work (to our knowledge) on *quantifying the consequences of data integrity attacks*. This is the essential focus of our work, and it is important in order to *prioritize* the adoption of cyber security countermeasures including PMU placement, encryption, hardware upgrades, and advanced detection algorithms. In this paper, we devise metrics to assess the economic impact of data integrity attacks under operator re-dispatch decisions based on optimal power flow methods.

The remainder of this paper is organized as follows: In Section II we summarize key results on unobservable attacks and their countermeasures, and in Section III we survey grid operations under normal and contingency conditions. Following this, in Section IV we present an example that illustrates consequences of unobservable attacks in the context of operator actions. Section V contains our main results: metrics to assess the economic impact of unobservable attacks using optimal power flow methods. We illustrate our method using

empirical studies in Section VI, and then draw conclusions and close with a discussion of future research directions.

II. Unobservable Attacks

Data integrity attacks whose compromised meter readings are *consistent* with the physical power flow constraints are called *unobservable* [11]. Unobservable attacks require coordination - compromised meter readings must be carefully orchestrated to fall on a low dimensional manifold in order for the attack to be unobservable. Unobservable attacks will pass any bad data detection algorithm. As a consequence, unobservable attacks can cause significant errors in state estimation. In [13], we address sparse unobservable attacks which involve the compromise of a modest number of meters. Specifically, we offer efficient algorithms to find all unobservable attacks involving the compromise of exactly two power injection meters and an arbitrary number of power meters on lines. Applying these algorithms to a synthetic 2383 bus power system, we identify 685 possible unobservable attacks that involve the compromise of 4 or fewer meters [13]. Other examples produce similar statistics. The conclusion is inescapable: common power systems are vulnerable to a large number of unobservable data integrity attacks.

Phasor measurement units (PMUs) have recently attracted a great deal of interest in the context of cyber security applications. The driving hypothesis is that PMUs are networked on the modern NASPInet architecture which is designed for security. We can thus assume that PMU measurements are *a priori* known to be secure [14]. Emami and Abur [15] have shown that with the introduction of a few extra PMUs, bad data detection and identification capabilities of EMS systems can be dramatically improved. Known secure PMU placement problems have been studied by Bobba *et al.* [16] who have investigated heuristic algorithms for mitigation of unobservable data integrity attacks. In [13] we have developed a method to resist such attacks while maintaining the robustness and reliability of the system. In our work [13], we have shown that $p+1$ PMUs are sufficient to thwart a collection of p unobservable attacks and we offer an algorithm to determine their placement. While these countermeasure strategies using known-secure PMU's are effective, they are extremely expensive because of the number of possible attacks that require defense in realistic power systems.

Given limited resources for protection against cyber attacks, it becomes necessary to quantitatively prioritize investments. There are two components to this prioritization: (a) determining prior probabilities that an attack occurs in some event horizon, and (b) assessing the economic consequences of operator decisions that are taken after an attack occurs. The first component could be developed on the basis of assessing component security (ex: is encryption used, how secure is the installation). This paper focusses on the second component: quantifying the economic consequences of data integrity attacks. More precisely, the operator schedules generation to meet load to minimize some economic cost function J subject to various constraints (ex: line limits, generator ramping and rate constraints, $N-1$ security constraints). In the pre-attack state, the cost function has value J^0. In the post-attack state, the operator is misled into believing that loads have changed, and that the current generation schedule is no longer economically optimal. As a result, the cost function is again minimized using the (compromised) load data, which leads to a (possibly) larger cost J^1. The increase in cost $\Delta J = J^1 - J^0$ is the attack consequence metric we develop in this paper. Interestingly, a decrease in cost ΔJ indicates that a constraint violation will occur. In this paper, a decrease indicates a violation of the thermal limits of a power line, however, in other contexts this could indicate a violation in a security constraint, such as $N-1$.

III. Grid Operations

Independent System Operators (ISOs) and Regional Transmission Organizations (RTOs) are responsible for reliable operation of the electric power system in a region. They dispatch generation, schedule for economic advantage, identify equipment outages, redirect power to manage congestion, coordinate with the neighbouring areas, facilitate effective markets, and promote infrastructure expansion. In order to maintain system reliability with equal treatment of all market entities, these organizations are independent of utilities or other market participants [17].

Control centers are designed to assist system operators take decisions. Advanced software and visualization tools are used to provide the operator with the timeliest and most accurate grid data. System operators follow a set of operating procedures that establish criteria for actions during particular events.

A. Data

Grid operators rely on an enormous amount of real time and historical grid information. The ISO monitors data from the buses and substations in the region to maintain reliable operations and determine what energy source will be the most economical for any given location at any given time. The grid data available includes, at minimum, the apparent, real and reactive power, voltage, current and frequency at every bus and line terminal, and the power flows that each transmission line is carrying. Operators constantly monitor critical system parameters, on numerous computer display screens. Data arrives at the SCADA/EMS master stations from numerous Remote Terminal Units (RTU) that collect field data from substations and other remote power system locations.

B. Software Tools

Automated modelling tools give the operator a comprehensive view of the grid and how it evolves from dynamic occurrences. A state estimator analyses real-time conditions of the grid. Tens of thousands of data points from the power grid are fed into computer algorithms to develop a series of contingency analyses for potential events that could compromise system reliability so that the operator knows how the grid evolves in real time. As an example the Midwest ISO state estimator collect data from 30,000 buses and 87,000 control points every

30 seconds [18]. Video projection systems, alarming display systems show real-time power-grid data from thousands of endpoints that assist the operator in decision-making to ensure safety and reliability of the transmission system. Power flow models describe the physics of the system and include real and reactive power, voltage angles and magnitudes. They are used to check the feasibility of a dispatch and to optimize real and reactive power dispatch. Other important software tools are load forecasting, unit dispatch and economic commitment, voltage and transient stability analysis, intermittent and renewable resources modeling. Each ISO has information about day-ahead real time markets through tools like the real time market look ahead and the day-ahead market to schedule generation with lengthy start-up times.

C. Dispatch Under Contingency

When faced with unexpected circumstances, the power system operator first relies upon automated control sequences programmed into the numerous levels of system dynamic control. The automation is intended to rescue the power system network from an unexpected contingency that occurs faster than a human can respond. After the automated control sequences achieve a new stable system operating point, the operating personnel step in with pre-defined manual operating procedure intervention. The system operator necessarily coordinates with system operators of other portions of the interconnected network to coordinate restructuring the overall power system network to the desired configuration.

D. Data Integrity Attacks

Power system data can be compromised. The attack can take place at the analog measurement level or during digital transmission through the communications circuits. Signals can be compromised at the generation or substation level. The physical quantities can be changed so that the sensing tool measures unreliable or corrupted data. For example, voltage or current can be modified before being measured. The corrupted data is then transmitted to the RTU in the field and then the control room. If the data alteration is done wisely it can pass the bad data detection algorithms and is provided to the operator as if it were reliable. He/she acts consequently and, given the fact that the real grid conditions are different from the corrupted information, potentially serious grid problems can be generated. In the same way breaker and relay status can be altered. Another means to compromise the signals that the SCADA master receives consists in disturbing the data format while on travel. The communication channel from the substation to the control room could be fiber optics, telephone wire, radio frequency or the message might be carried by the power line.

In the next section we give a concrete example of how a data integrity attack forces the operator to take dispatch decisions that have serious consequences on the power grid.

IV. An Example

As discussed above, grid operators critically rely on data in their decision making processes. Compromised data can lead to economically sub-optimal dispatch choices, congestion, and even failures of transmission lines. In this section we offer a simple example that illustrates the damage that can be induced by data integrity attacks through misinformed operator decisions.

Consider an unobservable attack in which exactly two power injection meters and the line connecting the two buses are compromised [13]. The connecting line T is a cutset of the power system graph. Loads L_1 and L_2 are served by power generated by G_1 and G_2. Generator G_1 and load L_1 are in the same island, while G_2 and L_2 are in a second island. These islands are connected by the tie-line T which has a thermal loadability limit of 200 MW. Generations and loads have real power meters that transmit their readings over a SCADA network to the system operator. Power flow on the tie-line is not metered. The situation we consider is illustrated in Figure 1.

The relevant pre-attack operating conditions are:

- generation: $G_1 = 100$ MW, $G_2 = 400$ MW
- loads: $L_1 = 300$ MW, $L_2 = 200$ MW
- tie-line flow $T = 200$ MW

At a certain time, a data integrity attack takes place. This attack involves the compromise of the power meters at L_1 and L_2. The post-attack (compromised) readings of these meters are

$$L_1 = 200\text{MW}, \text{L}_2 = 300\text{MW}$$

This attack is unobservable as the compromised meters readings are entirely consistent with the standard DC load flow model. The operator perceives this attack as corresponding to an *unanticipated* reduction in load at L_1, and a simultaneous increase in load at L_2. Let us assume generation at G_2 is substantially less expensive than at G_1. In response to this load change, the operator may choose to reduce generation at G_1 and increase it at G_2 to serve the new (compromised) load conditions most economically.

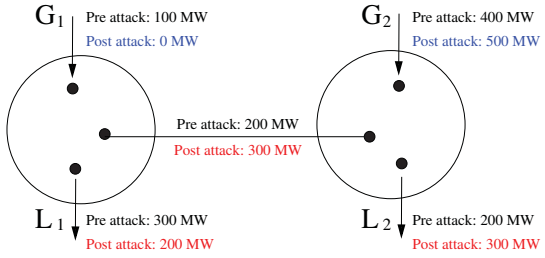

Fig. 1. Data integrity attack causing line overloading.

The resulting post attack operating conditions (calculated with the true loads) are:

- generation: $G_1 = 0$ MW, $G_2 = 500$ MW
- loads: $L_1 = 300$ MW, $L_2 = 200$ MW
- tie -line flow $T = 300$ MW

It is therefore apparent that this attack has misled the operator into a re-dispatch decision that overloads (and possibly damages) the tie-line. In this example, we could also reasonably assume that power-flow on the tie-line is metered in the SCADA network. In this case, we note that the attacker would have to simultaneously compromise three meters (L_1, L_2, T) to keep the attack unobservable. If the attack becomes observable, bad data detection algorithms run by the system operator would produce warning flags and intervene in any re-dispatch operations. We stress that the consequences of this data integrity attack occurs only after the operator responds to the compromised data.

V. Main Results

In this section we discuss an analytical approach to measuring the consequence of the unobservable attacks discussed in [13]. Assessment of consequences is important when resource limitations do not allow full deployment of countermeasures to cover all unobservable attacks. To measure consequence, we consider the DC Optimal Power Flow (DCOPF) as a model of operator behavior and operator response to data integrity attacks. More formally, the DCOPF used in this paper is stated as follows[1]:

$$\begin{aligned}
\min \quad & \textstyle\sum_{i\in\mathcal{B}} c_i g_i && && (1)\\
\text{such that} \quad & G_i^- \le g_i \le G_i^+ && \forall i \in \mathcal{B} && (2)\\
& l_i = L_i && \forall i \in \mathcal{B} && (3)\\
& \textstyle\sum_{j\in\mathcal{B}} b_{i,j}(\theta_i - \theta_j) = g_i - l_i && \forall i \in \mathcal{B} && (4)\\
& b_{i,j}(\theta_i - \theta_j) \le Q_{i,j} && \forall i \forall j \in \mathcal{B} && (5)
\end{aligned}$$

where $\mathcal{B}$ is the set of all buses in the power system, l_i is the load served at bus i and g_i is the generation at bus i. c_i is the cost to produce power at bus i. G_i^- and G_i^+ are the minimum and maximum generation at bus i. L_i is the amount of electric power demanded by bus i. θ_i is the phase angle at bus i. $b_{i,j}$ is the susceptance between buses i and j and $Q_{i,j}$ is the capacity between buses i and j. Equation 1 provides the objective function, which minimizes the cost of generation. Equation 2 constrains the generation to be within operating limits. Equation 3 ensures the specified amount of load is served at each bus.[2] We do not allow load shedding in this model, as a data integrity attack that indicates a shedding requirement to the operator would likely invoke a different response protocol than is assumed here. However, it is possible to incorporate load shedding by changing constraint 3 into an inequality constraint and adding the cost of shedding to the objective function. Equation 4 ensures conservation of flow at each bus. Equation 5 constrains the amount of flow on each line in the network. For simplicity, we denote the flow on a line i, j as $f_{i,j} = b_{i,j}(\theta_i - \theta_j)$. We also use σ to denote the solution to the DCOPF and $\sigma(x)$ to denote the value of variable x in solution σ.

In this section we consider 3-sparse attacks [13] where an attacker may falsify demand information such that net demand remains constant. For example, given buses i and j with demand l_i and l_j, the attack, $A_\Delta(i,j)$, may falsify the demands as $l_i + \Delta$ and $l_j - \Delta$, for some value Δ.

The linear program solution to the DCOPF provides important insight into the sensitivity of the power system to data integrity attacks. In the solution, the shadow price (dual variable) of the constraints measures how the objective function changes in response to a change to the righthandside of the constraints. In this context, the shadow price measures the economic impact to the system when demand data is falsified. Given a shadow price on l_i, denoted by $\tilde{l_i}$ and an attack of size Δ, the economic impact of $A_\Delta(i,j)$ is calculated as

$$\tilde{l_i}\Delta - \tilde{l_j}\Delta$$

The second piece of information in the solution is the range of the righthand side for which a shadow price is valid. The boundaries of the range are the points where a constraint becomes tight or loose. In the physical system, it represents the point where the operator will change its behavior. More importantly, perhaps, within this range, the variation, ρ, of all decision variables can be described with a single linear function.

For the load constraints (3), we denote the upper and lower bounds of the shadow prices range as l^+ and l^-, respectively. The shadow price range is only valid for a single variation of a constraint's righthandside, however, there exists a conservative bound for simultaneous variations. As long as the sum of all the ratios of righthandside deviation to max deviations is ≤ 1 then the shadow prices hold. More formally, for an attack $A_\Delta(i,j)$, the shadow price does not change if Δ is smaller than

$$\arg\max_{\delta_i} |\frac{l_i^+ - (l_i + \delta_i)}{l_i^+ - l_i}| + |\frac{l_j^- - (l_j - \delta_j)}{l_j^- - l_j}| \le 1$$

and larger than

$$\arg\min_{\delta_i} |\frac{l_i^- - (l_i + \delta_i)}{l_i^- - l_i}| + |\frac{l_j^+ - (l_j - \delta_j)}{l_j^- + -l_j}| \le 1$$

where $\delta_i = -\delta_j$ This range is denoted by Δ^- and Δ^+.

A. Operator Response

To compute the ρ for each decision variable during attack $A_\delta(i,j)$, we choose a δ_i that falls within the shadow price range and compute the solution to a new DCOPF, σ_δ:

$$\begin{aligned}
\min \quad & \textstyle\sum_{i\in\mathcal{B}} c_i g_i && && (6)\\
\text{such that} \quad & G_i^- \le g_i \le G_i^+ && \forall i \in \mathcal{B} && (7)\\
& l_k = L_k + \delta_k && \forall k \in \mathcal{B} && (8)\\
& \textstyle\sum_{j\in\mathcal{B}} b_{i,j}(\theta_i - \theta_j) = g_i - l_i && \forall i \in \mathcal{B} && (9)\\
& b_{i,j}(\theta_i - \theta_j) \le Q_{i,j} && \forall i \forall j \in \mathcal{B} && (10)
\end{aligned}$$

[1]The approach generalizes to other DCOPF models that include security constraints such as $N-1$ and other controls such as load shedding.

[2]The DCOPF does not need this constraint, as the constant L_i can replace the l_i variable everywhere in the formulation. However, we include this as a constraint as it allows us to compute the shadow price of the load and measure the consequence of a data integrity attack at the loads.

TABLE I
GENERATOR OPERATIONS COST ($ PER MWH)

Bus	Cost	Bus	Cost
1	142.0	16	101.0
2	142 .0	18	110.0
7	300.0	21	110.0
13	300.0	22	58.5
15	156.0	23	101.0

where $\delta_k = \delta_i$ when $i = k$, δ_k = -δ_i when $j = k$, and 0 otherwise.

This model represents how the operator will respond to an unobserved data integrity attack on the loads. The ρ values are derived by computing the ratio between the original solution and this solution. For example, $\rho(g_i) = \frac{\sigma(g_i) - \sigma_\delta(g_i)}{\delta_i}$.

B. System Response

The system response to actions taken by the operator is computed using the following DCOPF, σ_ψ:

$$\begin{aligned} \min \quad & \textstyle\sum_{i\in\mathcal{B}} c_i g_i && (11)\\ \text{such that} \quad & g_i = \sigma_\delta(g_i) && \forall i \in \mathcal{B} \quad (12)\\ & l_k = \sigma_\delta(l_k) && \forall k \in \mathcal{B} \quad (13)\\ & \textstyle\sum_{j\in\mathcal{B}} b_{i,j}(\theta_i - \theta_j) = g_i - l_i && \forall i \in \mathcal{B} \quad (14) \end{aligned}$$

Thus, the system remains feasible if $\forall_i \forall_j$

$$|f_{i,j}| + |\Delta^+ \rho(f_{i,j})| \leq Q_{i,j}$$

and

$$|f_{i,j}| + |\Delta^- \rho(f_{i,j})| \leq Q_{i,j}$$

In short, if at (Δ^-, Δ^+) the system remains feasible, it will remain feasible throughout the shadow price range. This process can be repeatedly calculated by finding new shadow prices at the boundaries.

VI. EMPIRICAL STUDIES

In order to evaluate shadow prices as a consequence measure we consider two different case studies. The cases adopt the 24 bus IEEE RTS-79 problem [19]. The fuel types for each generator are discussed in [20]. Based on these fuel types, costs are calculated based on reference [21]. These numbers are reported in Table I. In the case of multiple generators at a bus, without loss of generality, we average cost weighted by generation capacity.

In this model there is one unobservable 3-attack based on the approach by [13]. This attack occurs at buses 7 and 8 and the power line between them. Bus 7 has generation with maximum capacity 300 MW and a cost of $300 per MWH. There is no generation at Bus 8. Bus 7 has 125 MW of load and bus 8 has 171 MW of load. The power line between 7 and 8 has capacity 175 MVA. Given that generation at bus 7 is expensive and there is enough load at bus 7 and capacity between 7 and 8 to accommodate all of 7's generation it is not expected that a data integrity attack on the loads at 7 and 8 will have much impact. However, we must analytically determine

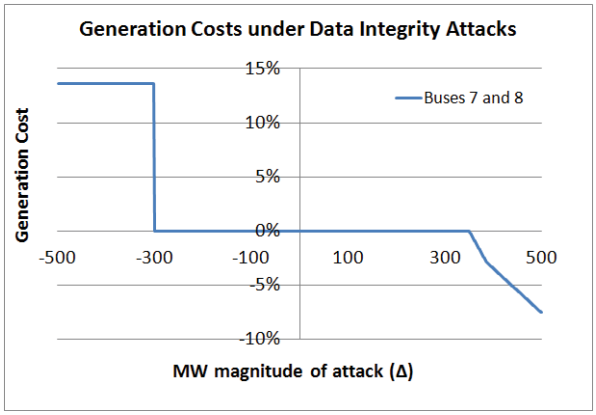

Fig. 2. Impact of data integrity attacks at buses 7 and 8 on the cost to produce power.

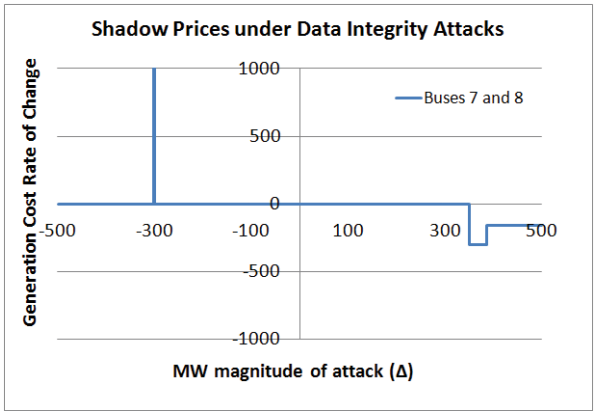

Fig. 3. The shadow price for data integrity attacks at buses 7 and 8.

this. The shadow price on the loads for both 7 and 8 is $300, as the only unused generation has cost $300. The shadow price range for the load at bus 7 is (-9, 30) and at bus 8 is (-171, 13). The change in price (as a % of the original price) is plotted in Figure 2. Here it can be seen that even beyond that range, the price of generation does not change (generation is shifted from one $300 generator to another $300 generator as $\hat{l_i} = \hat{l_j}$). Thus, in order to find a consequence we resolve the DCOPF at each of these boundaries, and recompute the shadow prices and ranges. Once we have done this successive times, as seen in Figure 2, we see economic consequences. Finally, Figure 3 plots the rate of change (shadow price) for attacks of size $\Delta = \pm 500$. Transitions in both plots indicate where attacks cause generation of different costs to be swapped.

This model provides an example of a low impact data integrity attack. The attacker has to launch a substational data integrity deviation (> 300 MW) in order to achieve any changes in the price for power[3] and is unable to have a physical impact to the system within the range provided.

We next consider a variation of the RTS-79 that constrains the network in the region of buses 7 and 8 to present a case where the shadow prices detect larger consequences. Bus 7's

[3]Indeed, this level of load deviation may raise red flags in other parts of the security system, as it requires of the loads to report negative power demands.

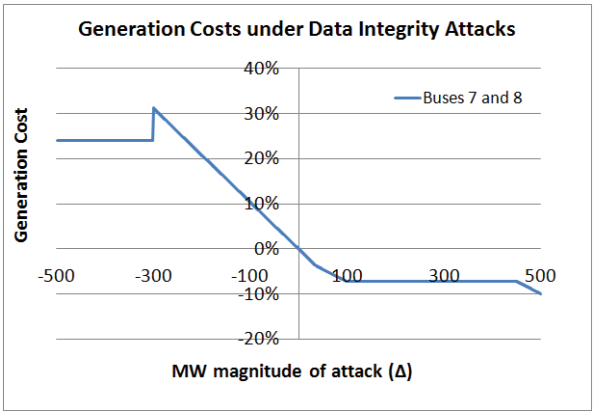

Fig. 4. Impact of data integrity attacks at buses 7 and 8 on the cost to produce power under constrained conditions.

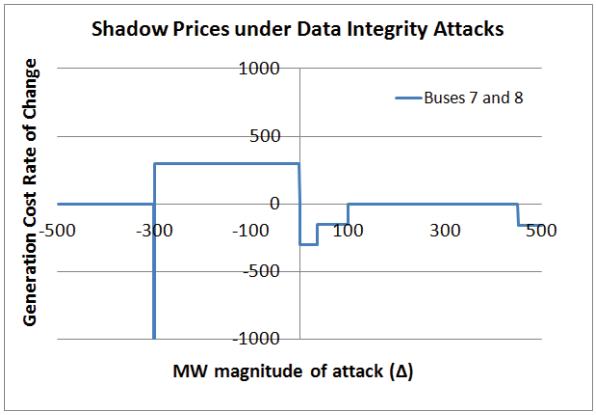

Fig. 5. The shadow price for data integrity attacks at buses 7 and 8 under constrained conditions.

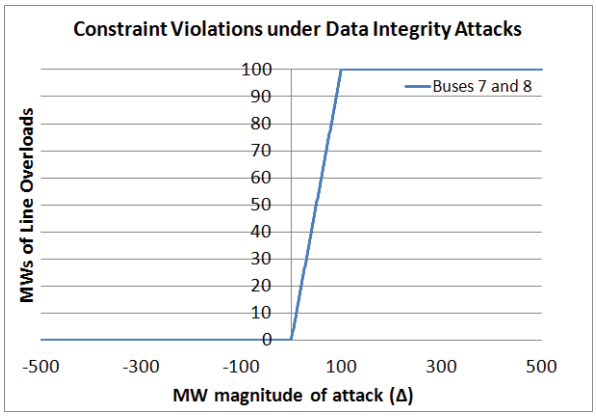

Fig. 6. Impact of data integrity attacks at buses 7 and 8 on physical constraints.

generation capacity is increased to 400 MW and its generation cost is dropped to \$1. The shadow price on the load at bus 7 is now \$1 as it can obtain up to 100MW of additional power from the generator at bus 7. The shadow price for the load at bus 8 is \$300 as the power line from 7 to 8 is congested, so it can only obtain generation from other parts of the network. The shadow price ranges for the loads at bus 7 and 8 are (-4, 100) and (-6, 330), respectively. Given the differences in shadow prices, there is now an immediate economic impact for a data integrity attack (Figures 4 and 5). In addition, in this model, $\sigma(f_{7,8}) = 175$ and $\rho(f_{7,8}) = 1$. Thus, within these shadow price ranges, a physical violation will be observed. This effect is seen in Figure 6, which plots the amount of flow that violates thermal limits on a line as δ is varied. This is not unlike the example seen earlier in Figure 1.

Intuitively the physical violation occurs when the data integrity attack increases load at bus 7 (decreasing load at bus 8). This causes the operator to think it can cheaply dispatch generation at bus 7 to satisfy the extra load at bus 7. As this extra load does not actually exist, the excess generation is shipped on the already saturated line (7, 8), causing an overload. In this case, the consequence does not go beyond the physical damage to the line. Even if the line were to fail, there is enough available generation and capacity in this system to fully satisfy all loads without this line. However, this will not be the case in general.

In short, given a DCOPF model of operator behavior, the shadow prices and shadow price ranges of unobservable attack vectors are a reasonable mechanism for determining the consequence of an attack. The key contribution of this result is to show that under linear response models, physical changes and violations in a system under data integrity attacks can be determined analytically by iteratively calculating the shadow prices and their ranges. Though we focus on the DCOPF, the techniques described here can be generalized to other models of operator behavior, especially linear models. It remains for future work to show how to use these measurements to prioritize the deployment of countermeasures. Possible approaches include worst-case consequence within a specified range of data integrity attacks or minimum attack that causes a physical problem in the system.

VII. Conclusions

Recent years have seen increased interest in a desire to understand the vulnerabilities of electric power grids to cyber attacks. Indeed, recent work by [13] has shown that it is possible for an attacker to falsify information sent to the grid operator so that the incorrect information remains consistent with other measurements reported to the operator. However, though a power grid may contain a large number of possible unobservable data integrity attack vectors, it is clear that they are not all equal in possible severity. This paper has shown that under the linear DC dispatch model of grid operations, shadow pricing information can be used to assess the economic and physical impacts of data integrity attacks to power systems. The approach is straightforward, can be adopted by many existing operations models, is a necessary step for assessing the consequences of attacks discovered by [13], and, to the best of our knowledge, no one has suggested the use of shadow prices in this way.

Though this paper has demonstrated how shadow price information can be used to measure the consequence of data integrity attacks, there remain a number of interesting directions for future work. First, this paper has focused on

data integrity attacks related to metering information (the amount of load demanded by parts of the power grid). There are other types of data integrity attacks that need to be considered, including the on/off status of a power lines (either from direct measurements or state estimation [22], [23], [24]), the output of generators, the states of control devices, etc. Second, this work needs to be extended to sparse attacks of size greater than 3. Third, additional work needs to be done to turn the shadow price measurements into a methodology for prioritizing the deployment of countermeasures, such as PMU place or hardware upgrades. For example, we could posit a prioritization based on a certain level of attack and ranking based on consequence severity within that threshold. Or we could rank by minimum attack that violates physical constraints in the system. Finally, it will be important to develop analytical methods for assessing consequence in non-linear operations models, as many of the important possible physical problems (such as voltage and frequency) only occur in such models.

ACKNOWLEDGMENT

This work was partially supported by the U.S. Department of Energy under DOE Idaho Operations Office Contract DE-AC07-05ID14517, performed as part of the *Known Secure Sensor Measurements* and *Experimental Security* projects at Idaho National Laboratory, the Los Alamos National Laboratory LDRD project *Optimization and Control Theory for Smart Grids*, the Center for Nonlinear studies at Los Alamos National Laboratory, EPRI and CERTS under sub-award 09-206, NSF under Grants EECS-0925337 and 1129001, and Robert Bosch LLC through its Bosch Energy Research Network funding program.

REFERENCES

[1] Department of Energy, "www.oe.energy.gov/documentsandmedia/02-1-11_oe_press_release_risk_management.pdf," Office of Electricity, 2011.

[2] T. Flick and J. Morehouse, "Securing the Smart Grid: Next Generation Power Grid Security," *Syngress*, 2010.

[3] National Institute of Standards and Technology, "NIST Framework and Roadmap for Smart Grid Interoperability Standards," *NIST Special Publication 1108, January*, 2010.

[4] H. Wu, "PMU Impact on State Estimation Reliability for Improved Grid Security," *IEEE Power and Energy Society General Meeting, PES*, vol. 25, no. 1, pp. 1349–1351, 2006.

[5] T. J. Overbye and J. Weber, "The Smart Grid and PMUs: Operational Challenges and Opportunities," *IEEE Power and Energy Society General Meeting, PES*, pp. 1–5, 2010.

[6] North American Synchrophasor Initiative, "http://www.naspi.org/naspinet.stm."

[7] O. Kosut, L. Jia, R. Thomas, and L. Tong, "Malicious Data Attacks on Smart Grid State Estimation: Attack Strategies and Countermeasures," *IEEE SmartGridComm*, 2010.

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

[9] G. Dan and H. Sandberg, "Stealth Attacks and Protection Schemes for State Estimators in Power Systems," *IEEE SmartGridComm*, 2010.

[10] A. Teixeira, G. Dan, H. Sandberg, and K. H. Johansson, "A Cyber Security Study of a SCADA Energy Management System: Stealthy Deception Attacks on the State Estimator," *Proc. IFAC World Congress*, 2011.

[11] Y. Liu, P. Ning, and M. K. Reiter, "False Data Injection Attacks against State Estimation in Electric Power Grids," *Proc. of the 16th ACM Conference on Computer and Communications Security*, pp. 21–32, 2009.

[12] J. Stamp, R. Laviolette, L. Phillips, and B. Richardson, "Final Report: Impacts Analysis for Cyber Attack on Electric Power Systems (National SCADA Test Bed FY08)," *SANDIA Report, SAND2009-1673*, 2009.

[13] A. Giani, E. Bitar, Garcia, M. M., McQueen, P. Khargonekar, and K. Poolla, "Smart Grid Data Integrity Attacks: Characterizations and Countermeasure," *IEEE SmartGridComm*, 2011.

[14] M. McQueen and A. Giani, "'Known Secure Sensor Measurement' for Critical Infrastructure Systems: Detecting Falsification of System State," *Proc. of the 3rd International Workshop on Software Engineering for Resilient Systems, SERENE*, 2011.

[15] R. Emami and A. Abur, "Placement of PMUs to Enable Bad Data Detection in State Estimation," *IEEE Transactions on Power Systems*, vol. 21, no. 4, pp. 1608–1615, 2006.

[16] R. B. Bobba, Rogers, Q. K. M., Wang, H. Khurana, K. Nahrstedt, and T. J. Overbye, "Detecting false data injection attacks on dc state estimation," *First Workshop on Secure Control Systems (SCS 2010)*, 2010.

[17] W. Hogan, C. Hitt, and J. Schmidt, "Governance Structure for an Independent System Operator (ISO)," *WP, center for Business and Government John F. Kennedy School of Government Harvard University*, 1996.

[18] MIDWEST ISO, Improved State Estimator Gives Midwest ISO Most Comprehensive View of Power Grid, "www.midwestiso.org," January 2004.

[19] Reliability Test System Task Force of the Application of Probability Methods Subcommittee, "IEEE reliability test system," *IEEE Transactions on Power Apparatus and Systems*, vol. PAS-98, no. 6, pp. 2047–2054, 1979.

[20] Reliability Test System Task Force, "The IEEE reliability test system - 1996," *IEEE Transactions on Power Systems*, vol. 14, no. 3, pp. 1010–1020, 1996.

[21] United States Energy Information Administration, "Annual energy outlook," Department of Energy, Tech. Rep., 2011.

[22] H. Singh and F. Alvarado, "Network Topology Determination using Least Absolute Value State Estimation," *IEEE Transactions on Power Systems*, vol. 10, no. 3, pp. 1159–1165, 1995.

[23] D. Singh, J. Pandey, and D. Chauhan, "Topology Identification, Bad Data Processing, and State Estimation Using Fuzzy Pattern Matching," *IEEE Transactions on Power Systems*, vol. 20, no. 3, pp. 1370–1379, 2005.

[24] R. Singh, E. Manitsas, B. Pal, and G. Strbac, "A Recursive Bayesian Approach for Identification of Network Configuration Changes in Distribution System State Estimation," *IEEE Transactions on Power Systems*, vol. 25, no. 3, pp. 1329–1336, 2010.

Annarita Giani received her Laurea (Master's degree) in Mathematics from the Universita' di Pisa, Italy. In 2001 she moved to the United States to commence a Ph.D in Computer Engineering at Dartmouth College's Thayer School of Engineering in Hanover, New Hampshire. While at Dartmouth, she participated in the Process Query System (PQS) project sponsored by the Advanced Research and Development Activity (ARDA). Her dissertation addressed issues relating to computer security, anomaly tracking and cognitive attacks. From 2007 to 2011, she was a postdoctoral fellow at the Department of Electrical Engineering and Computer Science at the University of California, Berkeley, where she commenced work on critical infrastructure protection. She currently works at the Los Alamos National Laboratory where she continues her research on power system cyber security.

Russell Bent received his PhD in Computer Science from Brown University in 2005 and is currently a staff scientist at LANL in the Energy and Infrastructure Analysis Group. His publications include deterministic optimization, optimization under uncertainty, infrastructure modeling and simulation, constraint programming, algorithms, and simulation. Russell has published 1 book and over 30 articles in peer-reviewed journals and conferences in artificial intelligence and operations research.

Mark Hinrichs is currently a staff R&D Engineer at LANL in the Energy and Infrastructure Analysis Group. Mark Hinrichs received his BSEE from the University of Minnesota Institute of Technology in 1975. He received his MSEE in Power Systems from Georgia Institute of Technology in 1991. He has completed the curriculum for post graduate studies in Pulse Power and Plasmas at the University of New Mexico in 1995. He is a Registered Professional Engineer (PE). He is a Certified Power Quality (CPQ) Professional in the Association of Energy Engineers (AEE). He is a member of IEEE's Power and Energy, Power Electronics, Nuclear and Plasma Sciences, and Antennas and Propagation Societies. He is a member of the National Society of Professional Engineers. He has 36 years of experience in all aspects of power system planning, operation and management. He has held memberships in a number committees within several NERC Regions. His competencies include experimental proficiency in High Voltage Engineering, Pulse Power, RF Systems, Optics, Power Electronics, SVCs, Generation, Transmission, Power System Analysis, Switching Transients , EMP, Geomagnetic Effects, and more.

Miles McQueen is a Principal Investigator in the Cyber Security R&D department at INL and graduate faculty at the University of Idaho. Miles has been the Director of the University of Idaho's Computer Science Program at the Idaho Falls Center for Higher Education. With well over 20 peer reviewed scientific publications, Miles is currently leading research teams investigating cyber threat attack propagation and consequence modeling for multiple infrastructure simulation efforts; and investigating and estimating aspects of software and human vulnerabilities, and their impacts to the security posture and responsible disclosure processes for control systems. Previously, Miles investigated novel, first of a kind, 0-Day vulnerability estimation techniques. The 0-Day research supported the situational awareness needs of the Department of Homeland Security Control System Security Program. Other less recent work includes research of survivable systems, fault-tolerant agreement algorithms applied to specialized distributed networked monitoring and control systems.

Kameshwar Poolla received the Ph.D. degree from the University of Florida, Gainesville in 1984. He has served on the faculty of the University of Illinois, Urbana from 1984 to 1991. Since then, he has been with the University of California, Berkeley where he is the Cadence Distinguished Professor of Mechanical Engineering and Electrical Engineering and Computer Sciences. He currently serves as the Director of the IMPACT center for Integrated Circuit manufacturing at the University of California. In 1999, Dr. Poolla co-founded OnWafer Technologies which offers metrology based yield enhancement solutions for the semiconductor industry. OnWafer was acquired by KLA-Tencor in 2007. He has also serves as a technology and mergers/acquisitions consultant for Cadence Design Systems. Dr. Poolla has been awarded a 1988 NSF Presidential Young Investigator Award, the 1993 Hugo Schuck Best Paper Prize, the 1994 Donald P. Eckman Award, the 1998 Distinguished Teaching Award of the University of California, the 2005 and 2007 IEEE Transactions on Semiconductor Manufacturing Best Paper Prizes, and the 2009 IEEE CSS Transition to Practice Award. Dr. Poolla's research interests include Renewable Integration, Smart Grid Cybersecurity, Sensor Networks, and Semiconductor Manufacturing.