LA-UR- 11-06812

Approved for public release;
distribution is unlimited.

Title:	Smart Grid Data Integrity Attacks and Grid Operations
Author(s):	Annarita Giani Russell Bent Mark Hinrichs Miles McQueen Kameshwar Poolla
Intended for:	Power Engineering Society General Meeting

Los Alamos
NATIONAL LABORATORY
EST.1943

Los Alamos National Laboratory, an affirmative action/equal opportunity employer, is operated by the Los Alamos National Security, LLC for the National Nuclear Security Administration of the U.S. Department of Energy under contract DE-AC52-06NA25396. By acceptance of this article, the publisher recognizes that the U.S. Government retains a nonexclusive, royalty-free license to publish or reproduce the published form of this contribution, or to allow others to do so, for U.S. Government purposes. Los Alamos National Laboratory requests that the publisher identify this article as work performed under the auspices of the U.S. Department of Energy. Los Alamos National Laboratory strongly supports academic freedom and a researcher's right to publish; as an institution, however, the Laboratory does not endorse the viewpoint of a publication or guarantee its technical correctness.

Form 836 (7/06)

Smart Grid Data Integrity Attacks and Grid Operations

Annarita Giani, Russell Bent and Mark Hinrichs
Los Alamos National Laboratories
Los Alamos, NM, 87545

Miles McQueen
Idaho National Laboratories
Idaho Falls, ID, 83501

Kameshwar Poolla
Mechanical Engineering
University of California at Berkeley
Berkeley, CA, 94705

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 two examples 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 are consistent with the physics of power flow, and are therefore passed by any bad data detection algorithm. We develop metrics to assess the economic impact of these attacks under re-dispatch decisions using optimal power flow methods. These metrics can be use to prioritize the adoption of appropriate countermeasures including PMU placement, encryption, hardware upgrades, and advance attack detection algorithms.

I. Introduction

Cybersecurity of critical infrastructures in general, and the electricity grid in particular, is a subject of increasing research interest [9], [10]. 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] [11], sensors [ex: phasor measurement units or PMUs] [14], and control devices [ex: intelligent relays] [13], [12]. Tomorrow's Smart Grid will incorporate increased sensing, communication, and distributed control to accommodate renewable generation, EV 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.

Many recent papers have explored various aspects of cyber attacks on SCADA/EMS systems that impact the key function of state estimation. These include computation and characterization of the attacks, minimization of the number of compromised meters, and various detection and mitigation strategies [18], [16], [19], [17], [15].

It was shown in [18] that the attack strategy identified in [21] can be equivalently characterized by the property that the power system becomes unobservable by the removal of the compromised meters. See [20], [22] for a comprehensive discussion of power system observability.

Much of this research has been focussed on identifying and classifying cyber vulnerabilities, and developing countermeasures. There is a very limited body of work (to our knowledge) on *measuring* the consequences of these attacks.

It is important to develop approaches to measuring the consequence of the unobservable attacks when resource limitations do not allow full deployment to cover all unobservable attacks. Available countermeasure resources must be used to thwart the most damaging attacks. This paper is a first attempt to understand the consequences of different unobservable cyber attacks.

This paper is focussed on understanding these connections and developing quantitative methods to classify cyber attacks on the basis of their consequence. We first offer two examples to illustrate how data integrity attacks can cause economic and physical damage by misleading operators into taking inappropriate decisions. We then focus on data integrity attacks involving power meter data. Of particular importance are unobservable attacks. There are coordinated data integrity attacks In this paper we first survey existing approaches to smart grid cyber attacks, summarize grid operational procedures that are relevant in the context of these attacks, and offer examples of how the procedures can cause economic and/or physical damage. We then focus on data integrity attacks involving power meter data, and develop metrics to assess their economic

impact under re-dispatch decisions. These metrics can be used to prioritize the adoption of appropriate countermeasures including PMU placement, encryption, hardware upgrades, and advance attack detection algorithms. Our approach to security assessments goes beyond the standard n-1 model which assures the normal operation under the failure of one grid element.

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 two examples that illustrate 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 draw conclusions and close with a discussion of future research directions.

II. Security Attacks and Countermeasures

Our paper [3] address unobservable attacks where the number of meters compromised is low. We offer an efficient algorithm to find all unobservable attacks involving the compromise of exactly two power injection meters and an arbitrary number of power meters on lines. We call these type of attack $k-$sparse when they involve k meters. Our approach differs from all previous approach since it only consider the underlying network graph so it can be applied in the case of DC or AC. We then give canonical forms for 3, 4, 5-sparse unobservable attacks in term of the topology of the graph of the power system. We consider strategic placement of Phasor Measurement Units (PMUs) as countermeasure.

The advantages of PMUs have been investigated in many articles. For example [5] considers the placement of Phasor measurement Unit to improve state estimation results in terms of minimizing the state estimation errors. Optimal location of PMUs using genetic algorithm for complete and incomplete observability have been formulated in [6]. A comprehensive literature review on PMU placement effort can be found in [7]. Comparison between different placement algorithms have been studied. In [8] Integer Linear programming and Matrix Manipulation are considered. They conclude that ILP is the best option since converges to the optimal solution very quickly both for small or big networks.

We assume that data coming from these device is reliable, for this reason they are considered known secure sensors [4]. We show that $p+1$ PMus are sufficient to thwart a collection of p attacks and we give an algorithm to determine their placement.

If the number of PMUs available is limited we need to make the choice on which are the attacks to neutralize first. This choice depends on which attacks cause more damage. So we want to assign a metric to attacks based on consequences. Data integrity attacks do not cause any immediate physical or economic consequence since they consist of manipulation of data. But compromised data are part of the information available to the operator to dispatch loads and generation. Bad decisions, based on bad data, can cause line congestions, loads not met or generators to run over their nominal capacity. A comprehensive analysis of cyber security threats to power grid must therefore include operating practice, both under normal and contingency operations.

The following sections describe how grid operators take actions and how they can be misled by corrupted data.

III. Grid Operations

ISOs and Regional Transmission Organizations (RTOs) are not-for-profit organizations responsible for the day to day 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 neighboring areas, facilitate effective markets and promote infrastructure expansion. In order to maintain system reliability, achieving equal treatment of all market entities, these organizations are independent of utilities or other market participants [1].

An American ISO or RTO is under the direction of the Federal Energy Regulatory Commission (FERC). The North American Electric Reliability Corporation (NERC) is a larger organization that also includes a Mexican utility and several Canadian utilities [2]. The configuration of the generation and transmission companies has changed over time and now there are 10 distinct member-regions in NERC. The Western Electricity Coordinating Council (WECC) covers the western part of the United States including California.

Control centers are designed to help system operators make 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 Available

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 to the Supervisory Control And Data Acquisition (SCADA) and Enegy Management System (EMS) master stations from the numerous Remote Terminal Units (RTU) including other master stations and RTUs that collect data from the field located in the substations and other remote power system locations.

B. Software Tools Available

Automated modeling tools give the operator a comprehensive view of the grid and how it evolves from dynamic occurrences. A state estimator analyzes 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 [*Add citation*]. 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. Integrity attacks to grid data

However, 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 way 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.

If the data alteration is done wisely it can pass the bad data detection algorithms and is provided to the operator. He/she acts consequently and, given the fact that the real grid conditions are different, potentially serious grid problems can be generated.

The following section shows a set of data integrity attacks that cause damage to the normal grid operation only after the grid operator takes action.

IV. Examples of attacks and their consequences

As seen in the previous section grid operators strongly rely on grid data to make decisions. If the data is corrupted their decision can lead to enormous problem to grip operation. In this section we show how data integrity attacks can be used to force the grid operator to take apparently good decisions (based on the data he/she sees) but that instead create damage to devices or expected loads.

A. Line

This is an example of data integrity attack in which the attacker forces the operator to congest a power line.

Let us consider an unobservable attack [3] in which exactly two power injection meters and the line connecting the two buses are compromised. The line is a cutset of the power system graphic. Consider that the goal of the attacker is to overload the line due to excessive current flow. He/she cannot under normal circumstances force more current to flow through the line but the launched attack can cause the grid operator unknowingly to overload the line.

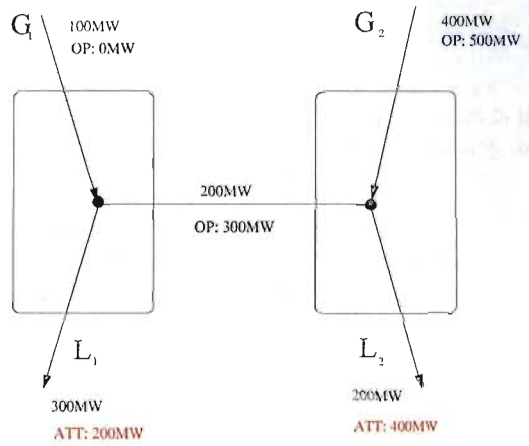

Fig. 1. Attack to a line.

Consider that loads L_1 and L_2 are served by the power generated by G_1 and G_2. G_1 is in the same island as L_1 and G_2 is in the same island as L_2. Suppose that G_2 is much cheaper than G_1 for example G_2 is a coal power plant and G_1 is a nuclear power plant. The maximum capacity of the

transmission line connecting the two buses is 200MW. Under the following grid situation:

- G_1 produces 100 MW
- G_2 produces 400 MW
- L_1 demands 300 MW
- L_2 demands 200 MW

200MW of power is carried through the transmission line. The line is running at maximum capacity.

Let us suppose that an attacker want to overheat the line causing it to trip off the system. He modifies the data the grid operator sees so that he/she does not know the real grid variables. The corrupted data are in red.

- L_1 demands 200 MW
- L_2 demands 400 MW

Since G_2 costs less than G_1 the new generation dispatch, given the corrupted data is the following:

- G_1 produces 0 MW
- G_2 produces 500 MW

But the real variables are such that 300MW of power flows through the transmission line. This is above its capacity so that it overheats.

Usually there are protection devices at the extremity of the line that trip off the line from the grid if the power exceed the limit. We suppose the attacker hacks those devices also.

This is an example of an attack that has consequences only after the grid operator takes action based on the manipulated data.

B. Generator

We give now an example of a data integrity attack that forces the grid operator to damage a nuclear power plant.

Suppose a nuclear power Plant $G-1$ generates at the maximum capacity of 200 MW. Suppose the attacker falsify the reading and the grid operator thinks that the plant generates only 150MW. To make the plant run at the maximum capacity increases generation of 50 MW to get to 200MW. The AGC is told to increase generation and the nuclear power plant tries now to generate 250MW which is over its capabilities.

V. Main Results

In this section we discuss an analytical approach to measuring the consequence of the unobservable attacks discussed in [3]. 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 is stated as follows:

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

where $\mathcal{B}$ is the set of all buses in the power system, l_i is the load 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 load served at 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 is to maximize the amount of load and second, minimize 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.[1] 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 protocal than assumed here. However, we could encorporate load shedding by changing constraint 3 into an inequality constraint and add 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 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 provide the degree to which the objective value changes should the righthandside of the constraint be modified. In this context, the shadow price provides a measure of the economic impact to the system should demand data be 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 bound 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

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

the ratios of righthandside deviation to max deviations is $\leq$ 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

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

or larger than

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

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

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:

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

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. The ρ values are derived by computing the ratio between the original solution and this solution. For example, $\rho(g_i) = \frac{\sigma(g_i) - \sigma_\delta(g_i)}{\delta_i}$.

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

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

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 the boundaries of the shadow price range the system remains feasible, it will remain feasible throughout the shadow price range. This process can be iterated by finding new shadow prices at the boundaries.

Empirical Studies In order to evaluate shadow prices we consider two different case studies. The cases adopt the 24 bus IEEE RTS-79 problem [?]. The fuel types for each generator are discussed in [?]. Based on these fuel types, costs are calculated based on reference [?]. 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 capacity.

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

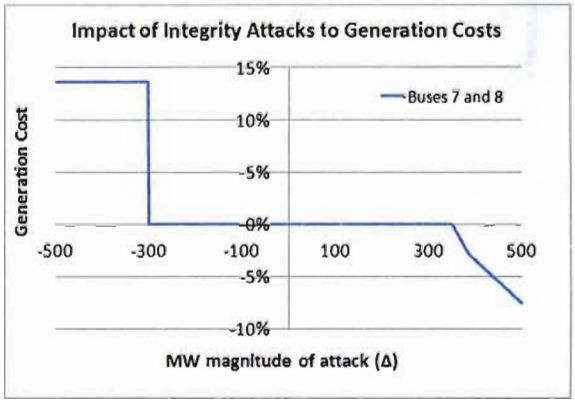

Fig. 2. Impact of data integrity attacks at buses 7 and 8 on the cost to produce power.

In this model there is one unobservable 3-attack based on the approach by [3]. 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. 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 determine 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). Thus, we must 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 start to see economic consequences. Figure ?? plots the rate of change (shadow price) for attacks of size $\Delta = \pm 500$.

This model provides an example of what could be a low impact data integrity attack. The attacker has to launch a substational data integrity deviation ($< 300MW$) in order to achieve any changes in the price for power[2] and is unable to have a physical impact to the system.

We next consider a variation of the RTS-79 that constrains

[2]Indeed, this level of load deviation may raise red flags in other parts of the security system

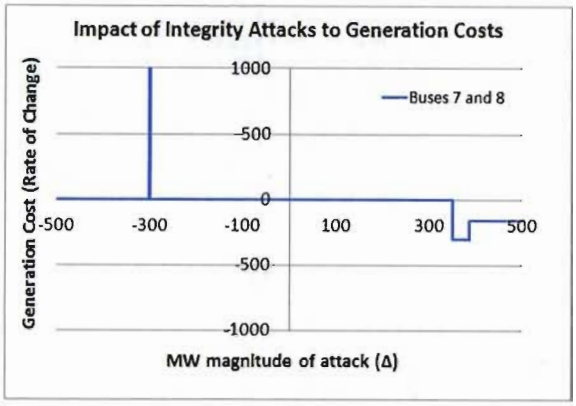

Fig. 3. The shadow price for data integrity attacks at buses 7 and 8.

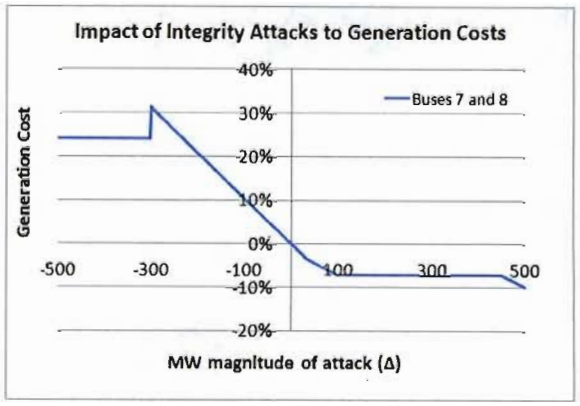

Fig. 4. Impact of data integrity attacks at buses 7 and 8 on the cost to produce power.

the network in the region of buses 7 and 8 to present a case where the shadow prices detect larger consequences. Bus 7's generation capacity is increased to 400 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 3 and **??**). 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 4, which tracks 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.

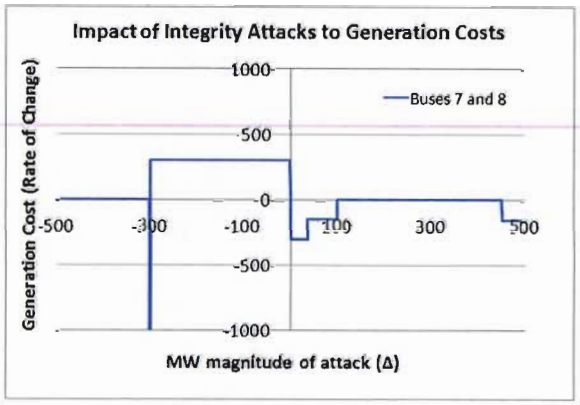

Fig. 5. The shadow price for data integrity attacks at buses 7 and 8.

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 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 a capacity 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 load without this line.

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 point 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 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

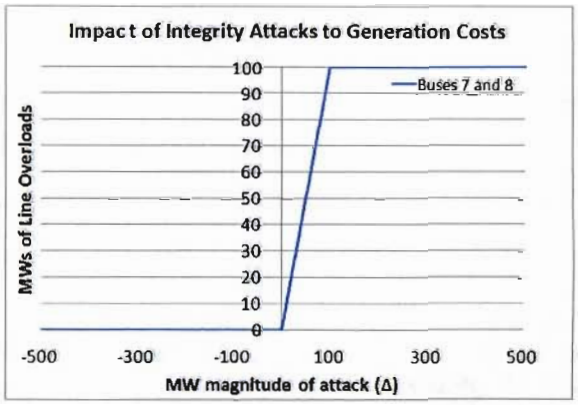

Fig. 6. Impact of data integrity attacks at buses 7 and 8 on physical violations.

worst-case consequence within a specified range of integrity attacks or minimum attack that causes a physical problem in the system.

VI. Conclusions

Recent years have seen increased interest in understanding the vulnerabilities of electric power grids to cyber attacks. Indeed, recent work by [3] 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 possibilities, it is clear that they are not all equal in 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.

Though this paper has demonstrated how shadow price information can be used 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 part 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 [?], [?], [?]), the output of generators, the states of control devices, etc. Second, additional work needs to be done to turn the 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 physical issues (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*, 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] Hogan, W., Hitt, C. And Schmidt, J., *Governance Structure for an Independent System Operator (ISO)'*, WP, center for Business and Government John F. Kennedy School of Government Harvard University, 1996.

[2] FERC, *Recent ISO Software Enhancements and Future Software and Modeling Plans'*, 2011.

[3] Giani, A., Bitar, E., Garcia, M., McQueen, M., Khargonekar, P., Poolla, K., *Smart Grid data Integrity Attacks: Characterizations and Countermeasure'*, Smart Grid Comm, 2011.

[4] McQueen, M., Giani, *'Known Secure Sensor Measurement' for Critical Infrastructure Systems: Detecting Falsification of System State'*, SERENE, 2011.

[5] Li, Q., Negi, R., Ilic, M., *'Phasor Measurement Units Placement for Power System State Estimation: A Greedy Approach'*, PES, 2011.

[6] Sajan, K., Tyagu, B., *'Optimal Placement of PMU with Optimal Branch Current Phasor for Complete and Incomplete Observability'*, PES, 2011.

[7] Yuill, W., Edwards, A., Chowdhury, S., Chowdhury, S., *'Optimal PMU Placement: A comprehensive literature review'*, PES, 2011.

[8] Fish, A., Chowdhury, S., Chowdhury, S., *'Optimal PMU Placement in a Power Network for Full System Observability'*, PES, 2011.

[9] Department of Energy, Office of Electricity, http://www.oe.energy.gov/DocumentsandMedia/02-1-11_OE_Press_Release_Risk_Management.pdf

[10] Flick, T., Morehouse, J., *'Securing the Smart Grid: Next Generation Power Grid Security'* Syngress, 2010.

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

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

[13] Overbye, T. J., Weber, J.D., *'The Smart Grid and PMUs: Operational Challenges and Opportunities'* IEEE 2010 Power and Energy Society General Meeting, pp.1–5, July 2010.

[14] Wu, H., *'PMU Impact on State Estimation Reliability for Improved Grid Security'* IEEE PES , vol.25, no.1, pp.1349–1351 , May 2006.

[15] Pasqualetti, F., Dörfler, F., Bullo, F. *'Cyber-Physical Attacks in Power Networks: Models, Fundamental Limitations and Monitor Design'* arXiv:1103.2795v1, 2011

[16] Teixeira, A., Amin, S., Sandberg, H., Johansson, K. H., Sastry, S., *'Cyber-security Analysis of State Estimators in Electric Power Systems'* Proceedings of the 2010 IEEE Conference on Decision and Control, March 2010.

[17] A. Teixeira, G. Dan, H. Sandberg, K. H. Johansson *'A Cyber Security Study of a SCADA Energy Management System: Stealthy Deception Attacks on the State Estimator'* ArXiv e-prints, Nov. 2010.

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

[19] Dan, G., Sandberg, H., *'Stealth Attacks and Protection Schemes for State Estimators in Power Systems'* Proceedings of the IEEE SmartGridComm , Oct. 2010.

[20] Abur, A., Exposito, A. G., *'Power System State Estimation: Theory and Implementation'* CRC Press, 2004.

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

[22] Monticelli, A., *'State Estimation in Electric Power Systems: A Generalized Approach'* Springer, 1999.