Vulnerability Assessment of AC State Estimation With Respect to False Data Injection Cyber-Attacks

Gabriela Hug, *Member, IEEE*, and Joseph Andrew Giampapa

***Abstract*—This paper introduces new analytical techniques for performing vulnerability analysis of state estimation when it is subject to a hidden false data injection cyber-attack on a power grid's SCADA system. Specifically, we consider ac state estimation and describe how the physical properties of the system can be used as an advantage in protecting the power system from such an attack. We present an algorithm based on graph theory which allows determining how many and which measurement signals an attacker will attack in order to minimize his efforts in keeping the attack hidden from bad data detection. This provides guidance on which measurements are vulnerable and need increased protection. Hence, this paper provides insights into the vulnerabilities but also the inherent strengths provided by ac state estimation and network topology features such as buses without power injections.**

***Index Terms*—Cyber security, false data injection attacks, graph theory, SCADA systems, state estimation.**

I. Introduction

A cyber-security SCADA (Supervisory Control and Data Acquisition) attack matrix that is reported in a National Communications System bulletin [1] lists attacks with the highest impact as those that gain control of the SCADA system. A means to carry out such an attack is known as a *false data injection* attack, which corresponds to modifying stored or transmitted data and can be directed against the data communications infrastructure, data stores in the control center, or even against the SCADA remote terminal units (RTUs). As smart power grid evolution extends the cyber- part of electric power systems and therefore increases the number of possible threat vectors for false data injection attacks, it becomes increasingly important to identify the vulnerabilities of existing SCADA systems and processes. In this paper, we focus our investigations on assessing the vulnerabilities of ac state estimation, the part of an energy management system that processes and uses SCADA data.

False data injection (FDI) attacks modify the data that is generated by the SCADA system and can potentially provoke two negative consequences:

- If the data is altered in a way that is not detectable as false by state estimation schemes, the perceived *observable* state of the system will be wrong and may lead to actions by the grid operator that may endanger the security of the system.
- The malicious intent might not be to hide the attack. Even if the attack is detected, part of the system may become *unobservable*, which means that the state estimator cannot estimate state values (e.g., voltage magnitudes and voltage angles), and thus the transmission grid would be vulnerable to a local physical attack. By the time the consequences of the physical attack have propagated into the rest of the system where the state is observable, it may already be too late to avoid an outage of a larger part of the system.

While there is a growing body of work on this topic, the analysis of the vulnerability of the SCADA system is usually based on a dc model for the state estimation, which has no concept of reactive power flows and therefore has the potential for introducing detectable errors. In this paper, we review the dc model approach to assessing a false data injection attack on a SCADA system, introduce techniques for more accurate vulnerability assessments via topographical analysis and an ac model of the transmission grid, and present empirical results that illustrate the performance of these analytical models. We also analyze the amount of effort that is required to hide an FDI attack on the IEEE 57 bus test system, and by way of this example, illustrate some of the properties of grid design that render an attack either detectable or not. These results can be used to provide insights to transmission grid planners to understand how grid design can render them in/vulnerable to SCADA attacks, as well as provide insights on how such attacks would appear to control center operators.

The structure of the paper is as follows: Section II describes related work and provides the context for this paper. Section III defines the type of cyber-attack which will be studied. Section IV gives a short introduction to state estimation, bad data detection, and briefly discusses the difference between dc and ac state estimation. Section V presents techniques for performing a hidden false data injection vulnerability analysis on state estimation. Section VI presents simulation results and Section VII concludes the paper.

II. Related Work

Research on power system vulnerabilities to cyber-attacks has been published by the *power systems*, *control theory*, and *information technology* communities, and can be classified into three categories:

1) *Vulnerability Analysis of State Estimation:* The inherent weaknesses of state estimation bad data detection to detect malicious alterations to SCADA data are investigated from

Manuscript received September 12, 2011; revised January 20, 2012; accepted March 21, 2012. Date of current version August 20, 2012. This work was supported by the U.S. Department of Energy (DoE) and the U.S. Department of Defense (DoD) via Federal Government Contract FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. Paper no. TSG-00542-2011.

G. Hug is with the Department of Electrical and Computer Engineering, Carnegie Mellon University, Pittsburgh, PA 15213 USA (e-mail: ghug@ece.cmu.edu).

J. A. Giampapa is with the Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA 15213 USA (e-mail: garof@sei.cmu.edu).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TSG.2012.2195338

the perspective of an attacker [2]–[5], i.e., *Which SCADA measurements need to be altered and by how much in order to render the attack undetectable by bad data detection?*

2) *Consequence Analysis:* Multiple functions such as optimal power flow calculations, congestion analysis and management, and automatic generation control use data received from state estimation as input to determine control settings. This research area [6]–[9] investigates what the resulting consequences on those functions would be if a false data attack were to remain undetected and how an attacker could take advantage of such a vulnerability.
3) *Development of Countermeasures:* The key question of this research area is how to detect malicious attacks and protect the power system. Most research [10]–[12] in this area focuses on improving bad data detection schemes or improving the security of the communication system via, for example, isolated physical transmission media, access barriers, and data encryption.

This paper focuses on the vulnerability analysis of state estimation, particularly with respect to ac state estimation. Hence, it completes the research of the first research category.

III. Threat Model

The electric power system, especially in view of its transition to the smart grid, is commonly referred to as a cyberphysical system. Hence, an attacker who maliciously wants to do harm to the electric power system, may attack either the physical system or the cyber system. The reason why the community is becoming increasingly concerned about cyber attacks is that it does not require any physical presence or intrusion of the attacker into the physical system. A cyber attack could be carried out from a distant location and basically only requires specific knowledge about how the system is operated and how data is communicated and hacking skills.

In [13], a classification of cyber attacks is given. Five types of classes are presented including attacks on sensed data sent by RTUs which can either happen directly at the RTU level or on the communication lines to the control center. Higher level attacks correspond to attacks at the SCADA or the energy management system level.

In this paper, we focus on attacks at the RTU level and we concentrate on false data injection attacks. We define such an attack as an attack in which data to be sent by the RTU to the control center is maliciously altered to values specified by the attacker, i.e., the control center does not receive the actually measured values but the values which the attacker has sent instead. The data received from RTUs is used in the state estimator to determine the state of the system and based on that state to make operational decisions with possibly far-ranging consequences.

False or inaccurate data sent by the RTUs has been an issue since the initiation of SCADA systems, not because of cyber attacks but due to the fact that measurements have limited accuracy. Sometimes measurement equipment also completely fails. This is being dealt with using bad data detection (see also the following section) in which the physical properties of the system are used to filter false or extensively inaccurate data. The difference of a false data injection attack to this naturally occurring errors is that the data may be altered in an intelligent way such that it still fulfills the physical laws and will not be detected by bad data detection.

IV. State Estimation

SCADA RTUs forward sensor measurements from points of the transmission grid to a control center so that the state of the system, given by voltage magnitudes and angles at the buses of the system, can be estimated. Measurement errors are to be expected under normal operating conditions, but since there are more measurements than are needed to determine the state variables, it is possible to remove those measurements whose errors exceed expectations. The process of detecting exceptional errors is called *bad data detection*. If there are enough measurements to calculate the values of state variables after those measurements with exceptional errors have been removed, then the system is considered to be *observable*; if so many measurements have been removed due to exceptional errors that the values of state variables cannot be calculated, then the system is considered to be *unobservable*. Our analysis is concerned with an observable system under a false data injection (FDI) attack.

Successfully hiding an FDI attack requires knowing parameters and topology of a grid so that measured values from RTUs can be modified to give a convincing, though misleading, perception of system state. In addition, the attacker also needs knowledge of the state estimation process.

Most state estimation programs use weighted least square minimization to determine the most probable actual state variable values [14]. These programs take into account the full nonlinear power flow equations, but are computationally intensive for an attacker to use, and they require access to a significant amount of system data. In [2] and [5], it is assumed that the problem for an attacker could be much easier: an FDI attacker can use a simplified version of state estimation which corresponds to using the linear dc power flow equations [15]. We provide a short review of both ac and dc state estimation.

A. AC State Estimation

In full ac power flow state estimation, the power flows are nonlinearly dependent on voltage magnitudes and angles, which results in the following nonlinear mathematical dependencies:

$$\mathbf{z} = \mathbf{h}(\mathbf{x}) + \mathbf{e} \tag{1}$$

where:

- $\mathbf{z}$ vector of measured values (active and reactive power flows, active and reactive power injections, voltage magnitudes and angles);
- $\mathbf{x}$ vector of state variables (voltage magnitudes and angles);
- $\mathbf{e}$ vector of measurement errors (unknown but with known distribution);
- $\mathbf{h}(\mathbf{x})$ function vector that establishes dependencies between measured values and state variables.

The state variables are determined from the following weighted least square optimization problem:

$$\min F(\mathbf{x}) = (\mathbf{z} - \mathbf{h}(\mathbf{x}))^T \cdot \mathbf{W} \cdot (\mathbf{z} - \mathbf{h}(\mathbf{x})) \tag{2}$$

where $\mathbf{W}$ is the weighting matrix whose elements correspond to the inverse of the accuracy of the individual measurements. The functions in the function vector $\mathbf{h}$ depend on the type of measurement, i.e., active or reactive power flow on lines or as injections, voltage magnitudes and angles.

The standard approach to solve (2) is the iterative normal equation method [14]. The first order optimality condition of this unconstrained optimization problem is formulated:

$$\frac{\partial F(\mathbf{x})}{\partial \mathbf{x}}|_{\mathbf{x}=\hat{\mathbf{x}}} = -2\mathbf{J}_h^T(\hat{\mathbf{x}})\mathbf{W}(\mathbf{z} - \mathbf{h}(\hat{\mathbf{x}})) = 0 \tag{3}$$

where $\mathbf{J}_h$ is the Jacobian matrix derived from the function vector $\mathbf{h}(\mathbf{x})$ and $\hat{\mathbf{x}}$ is the estimated state vector. The result is a nonlinear equation system which can then be solved using an iterative process [14].

B. DC State Estimation

DC power flow leads to significantly simplified expressions: the voltage magnitudes are assumed to be constant and equal to one at all buses, the shunt susceptances and series resistances in the lines are neglected and the angle differences between buses are small. Hence, reactive power is completely neglected and state variables only consist of voltage angles. This leads to linear relationships between measurements and state variables, i.e.,

$$\mathbf{z} = \mathbf{H}\mathbf{x} + \mathbf{e} \tag{4}$$

where:

$\mathbf{z}$	vector of measured values (active power flows, active power injections, voltage angles);
$\mathbf{x}$	vector of state variables (voltage angles);
$\mathbf{e}$	vector of measurement errors (unknown but with known distribution);
$\mathbf{H}$	matrix providing dependencies between measured values and state variables.

The objective function for the least square minimization in this case results in

$$F(\mathbf{x}) = (\mathbf{z} - \mathbf{H}\mathbf{x})^T \cdot \mathbf{W} \cdot (\mathbf{z} - \mathbf{H}\mathbf{x}) \tag{5}$$

and using

$$\frac{dF(\mathbf{x})}{d\mathbf{x}}|_{\mathbf{x}=\hat{\mathbf{x}}} = 0 \tag{6}$$

leads to

$$\hat{\mathbf{x}} = (\mathbf{H}^T\mathbf{W}\mathbf{H})^{-1}\mathbf{H}^T\mathbf{W}\mathbf{z}. \tag{7}$$

Hence, there is a closed form solution to the least square minimization problem.

C. Bad Data Detection

Faulty measurements can lead to significant errors in determining the state of a system, hence bad data detection schemes are used to detect them. There are various algorithms for bad data detection [14] which are mostly based on the residual

$$\mathbf{r} = \mathbf{z} - \mathbf{h}(\hat{\mathbf{x}}) \tag{8}$$

which corresponds to the difference between the received measurement and the value for this measurement as a function of the estimated state.

The largest normalized residual method uses the following condition to determine if there is a faulty measurement. If

$$\|\mathbf{r}\| < \tau, \tag{9}$$

where τ, a predetermined threshold, is violated, then there is at least one faulty measurement. The key is to choose an appropriate value for τ. Using the known error distributions and the theory of χ^2 testing, this value can be determined such that faulty measurements are identified if they exceed the expected probability distributions [14].

V. Analytic Techniques for Hidden FDI Vulnerability Analysis

It is important to understand the characteristics of hidden FDI attacks in order to provide countermeasures for them. For example, in order to minimize the effort required to: attack a SCADA system, avoid detection, and maintain the deception, an attacker would likely search the transmission grid for attack points with the least number of measurements that need to be modified or minimal required alterations of measurement values. He will also need information so that he can modify the measurement values in such a way as to avoid detection and elimination by bad data detection. These concerns are investigated in [2] and [5] by considering the matrix $\mathbf{H}$—that is, the dc model of the grid for state estimation. We provide a method to find attack points that satisfy the above attack criteria, based on analysis of the grid topology and on the implications given by the power balance equations that can be applied to both dc and ac state estimation.

A. Topographical Attack Analysis

The general rule for a hidden attack is that the attacker must alter the data so that the measurements can plausibly correspond to the physical properties of the system. If there is no feasible solution to the power flow equations, then bad data detection will detect the FDI as values that exceed a certain acceptable limit, and an investigation will be launched into why those values are being detected.

The proposed analysis is based on the following two properties:

- Power injections at bus i representing generation (positive) as well as loads (negative) are functions of the state variables, i.e., voltage magnitudes and angles, at bus i and all adjacent buses $j \in \Omega_i$.

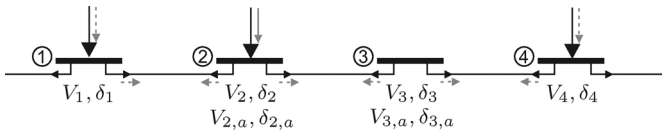

Fig. 1. Illustration of an attack including a bus with no generation or load.

- Power flows on the line connecting buses i and j are functions of the state variables at buses i and j.

Consequently, if the attacker's goal is to change the perceived value of any of the power injections or power flow measurements z_k, he needs to adjust the estimated value of at least one state variable x_p which appears in the function of this measurement, i.e., $z_k = h_k(\ldots, x_p, \ldots)$. In order to achieve compliance of all measurements with the power flow equations, he must adjust all measurements which are a function of this state variable x_p.

Assuming that the attacker has chosen to alter the perceived value of measurement z_k by changing the estimated value for x_p at bus p, the minimum number of measurements the attacker needs to alter depends on the following factors:

- the number of adjacent buses to bus p;
- the number of measurements at bus p, at the adjacent buses, and on the lines connecting bus p with its adjacent buses;
- the presence of adjacent buses at which the power injection is zero, i.e., buses with no load or generation.

For buses with no load or generation connected, the attacker must ensure that power flows on lines connected to this bus sum to zero. This implies that if one of these line flows is adjusted then at least another one needs to be adjusted, as well. Consequently, either the estimated values of the state variables at this bus or the estimated values for the state variables at one other connecting bus will be influenced, which again has consequences for the line flows going out of this connecting bus.

For clarification, consider the example illustrated in Fig. 1. The goal of the attacker is to change the perceived power injection at bus 2 (indicated by the bold gray line) without the system operator noticing the attack. The dashed gray lines at buses 1 and 4 indicate measurements that need to be changed to hide the attack. Assuming that he achieves this by influencing the estimated values for the state variables at bus 2 (indicated by the subscript a), he will need to adjust the power flows on the connecting lines 1-2 and 2-3. The line flows on the line connecting buses 3 and 4 must be adjusted as well, modifying also the power injections at bus 4. This will lead to a change in the estimated value of the state variables at bus 3 (indicated by the subscript a).

Three conclusions can be drawn from the above derivations:

Conclusion 1: Assuming that all power flows on lines and power injections are measured, the attacker needs to attack all measurements in the subgraph that is bounded by buses with power injections, in order to hide his attack.

Conclusion 2: The sum in power flow injection alterations plus changes in power losses must add to zero, i.e.,

$$\sum_i \Delta P_i + \Delta P_{loss} = 0 \tag{10}$$

$$\sum_i \Delta Q_i + \Delta Q_{loss} = 0. \tag{11}$$

Conclusion 3: The minimum number of measurements that an attacker must alter to hide the attack is heavily dependent on the network topology, the composition of types of buses (buses with and without power injections), the existing measurements, their respective location and the specific values the attacker wants the perceived measured values to be.

B. Procedure for Determining the Minimum Subgraph of a Topographical Analysis

As concluded in the previous section, the number of measurements that need to be altered by an attacker for an attack to be hidden can be derived by finding the smallest subgraph with the following properties: a) it must contain the bus for which the state variables are to be changed, we will use the term "center" for this bus, plus b) at least all buses connected to this bus, and c) it must be bounded only by buses with power injections (e.g., generation or loads).

The procedure to determine the minimal number of attacked measurements is as follows:

1) Represent the power grid as a weighted graph in which an edge represents a transmission line and a node a bus.
2) Assign the weight on an edge equal to the number of measurements on this line, i.e.,
$$w_e(e_{ij}) = \#m_{ij}. \tag{12}$$
3) Assign type to each node according to:
   - if power injection present (even if not measured) $t(n_i) = t_1$;
   - if no power injection present $t(n_i) = t_2$.
4) Assign a weight $w_n(n_i)$ to each node which is equal:
   - to the number of power injections measured at this bus if $t(n_i) = t_1$,
   - to the number of state variables (voltage magnitude, voltage angle) that are measured if $t(n_i) = t_2$.
5) Determine nodes n_C at which a change in the state variable value leads to a change in the attacked measurement according to:
   - Attacked measurement is line flow F_{ij}: n_C includes the nodes i and j at the ends of the line, i.e.,
   $$n_C = \{i, j\}. \tag{13}$$
   - Attacked measurement is bus injection F_i: n_C includes bus i and all buses connected to bus i, i.e.,
   $$n_C = \{i, j \in \Omega_i\}. \tag{14}$$
6) Find subgraph $\mathcal{S}_p$ with node $p \in n_C$ as starting point as follows:
   a) Include all nodes $k \in \Omega_p$ and edges connecting these buses to p in subgraph.
   b) Go through all buses $k \in \Omega_p$:
      - if $t(n_k) = t_1$, then no further actions for this node needed;
      - if $t(n_k) = t_2$, start inner loop with node k as starting point and add all nodes $q \in \Omega_k$ and connecting edges to subgraph.

c) Set $w_p = 1$, if all state variables are measured at bus p; set $w_p = 0$, if only part of the state variables are measured.

7) If one of the nodes $p \in n_C$ is of type t_2, add nodes $k \in \mathcal{S}_p$ of type t_1 to n_C, ignore $\mathcal{S}_p$ as possible subgraph and repeat 6) for the new nodes in n_C.

8) Choose node $p \in n_C$ and corresponding subgraph for which

$$\#m_{UB} = \min_{\mathcal{S}_p} \left(\sum_{e_{ij} \in \mathcal{S}_p} w_e(e_{ij}) + \sum_{n_i \in \mathcal{S}_p} w_n(n_i) + w_p \right) \tag{15}$$

which will provide the upper bound on the minimum number of measurements which the attacker needs to attack.

If this number is equal to the actual number of measurements which needs to be attacked depends on which measurements are taken. If the system is in normal state, then it is observable and the upper bound of (15) will indicate the number of measurements that the attacker will need to alter in order for them to avoid discovery by the bad data detection algorithms of state estimation.

In step 8), it is conceivable that not the subgraph which results in the least measurements is chosen but the one which will result in the smallest changes of the manipulated measurements and/or state variables. In this case, the method is used to determine possible sets of measurements $\mathcal{S}_p$ which need to be manipulated for a hidden attack guaranteeing a low number of manipulated measurements and a "cost of attack function" would determine which set to choose. However, in this case the choice of $\mathcal{S}_p$ is dependent on the specific generation and loading situation and by how much the attacked measurement is to be altered.

Step 7) accounts for the fact that buses without power injections have the constraint that the total power flowing into the network has to be equal to zero. Consequently, the number of influenceable state variables is equal to the number of constraints at such a bus. In order to have enough freedom in the resulting system of equations to set the attacked measurement to the desired value, at least one state variable at a bus with power injections needs to be adjusted. This will increase the size of $\mathcal{S}_p$.

C. DC Attack Analysis

An upper bound on the minimum number of measurements that need to be compromised in order to hide the attack from the state estimator, assuming that there is a power injection at each bus, can be derived by considering matrix $\mathbf{H}$ in (4) [5]: to hide an attack on measurement k, only the columns in $\mathbf{H}$ that have a nonzero value in row k, need to be considered. For each of these columns, the number of nonzero elements is determined. The minimum number of measurements to compromise is equal to the smallest number of nonzero elements in any of these columns. This minimum number will become the actual number of measurements which must be compromised if all power injections and power flows on lines are measured, and if there is a power injection at each bus.

This analysis is consistent with the derivations in Section V-B, above. A column in $\mathbf{H}$ corresponds to a voltage angle. Consequently, choosing a column and measurements which have nonzero elements in this column corresponds to choosing which state variable (voltage angle) will be adjusted. Since there are no losses in the dc model of the system, the following must be fulfilled in order to hide an attack:

$$\sum_i \Delta P_i = 0. \tag{16}$$

Bad data detection in the dc analysis corresponds to

$$\|\mathbf{z} - \mathbf{H}\hat{\mathbf{x}}\| > \tau. \tag{17}$$

Hence, in order for an attack to be undetectable, it can be derived from

$$\|\mathbf{z_a} - \mathbf{H}\hat{\mathbf{x}}_{\mathbf{bad}}\| = \|\mathbf{z} + \mathbf{a} - \mathbf{H}(\hat{\mathbf{x}} + \mathbf{c})\| \tag{18}$$

$$= \|\mathbf{z} - \mathbf{H}\hat{\mathbf{x}} + (\mathbf{a} - \mathbf{H}\mathbf{c})\| \tag{19}$$

$$= \|\mathbf{z} - \mathbf{H}\hat{\mathbf{x}}\| \leq \tau \tag{20}$$

where the following equality constraint:

$$\mathbf{a} - \mathbf{H}\mathbf{c} = 0 \tag{21}$$

must hold [2], where $\mathbf{a}$ is the vector of changes in measurements and $\mathbf{c}$ is the vector of changes in the estimated state variables.

D. AC Attack Analysis

In this section, we will follow the approach described in the previous section, Section V-C, and extend it to ac state estimation. The first step is to determine which measurements need to be manipulated if a hidden attack is to be directed against one specific measurement; in a second step, the values for these measurements are determined.

In order to hide a manipulation of the attacked measurement, the value resulting from state estimation for at least one state variable needs to be influenced. This, in turn, requires a manipulation of all the measurements which are directly dependent on this state variable. In dc state estimation, the $\mathbf{H}$ matrix provides the information of which measurement is dependent on which state variable, i.e., a nonzero value of element ij indicates that the value z_i is a direct function of state x_j. In ac state estimation, the relation between state variables and measurements is nonlinear and is given by (1). However, the Jacobian matrix of $\mathbf{h}(\mathbf{x})$

$$\mathbf{J}_h = \begin{bmatrix} \frac{\partial h_1}{\partial x_1} & \frac{\partial h_1}{\partial x_2} & \cdots & \frac{\partial h_1}{\partial x_{n-1}} & \frac{\partial h_1}{\partial x_n} \\ \frac{\partial h_2}{\partial x_1} & \frac{\partial h_2}{\partial x_2} & \cdots & \frac{\partial h_2}{\partial x_{n-1}} & \frac{\partial h_2}{\partial x_n} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \frac{\partial h_{m-1}}{\partial x_1} & \frac{\partial h_{m-1}}{\partial x_2} & \cdots & \frac{\partial h_{m-1}}{\partial x_{n-1}} & \frac{\partial h_{m-1}}{\partial x_n} \\ \frac{\partial h_m}{\partial x_1} & \frac{\partial h_m}{\partial x_2} & \cdots & \frac{\partial h_m}{\partial x_{n-1}} & \frac{\partial h_m}{\partial x_n} \end{bmatrix} \tag{22}$$

provides the information with regards to which measurement is dependent on which state variable, i.e., whenever a measurement is directly dependent on a certain state variable, the specific element in the row that corresponds to the measurement and in the column that corresponds to the state variable must be

nonzero. Otherwise, if the measurement is not directly dependent on the state variable, then its corresponding element in the matrix is equal to zero. Hence, the algorithm used in the dc analysis to identify the measurements that need to be altered can be applied to the Jacobian matrix: By considering the row associated with the targeted measurement and the columns for which this row has nonzero elements, the upper bound on the minimum number of measurements which need to be altered can be found. Namely, this upper bound is equal to the minimum number of nonzero elements in any of these columns. Again, the assumption here is that there is a power injection at each bus. As soon as there is a bus with no power injections, the situation changes with the implications described in Section V-A, above.

Having determined which measurements have to be altered, the question arises what values they need to be changed to. The equations for power flows on lines are given by

$$\begin{aligned} P_{ij} &= V_i^2 \cdot g_{ij} - V_i V_j \cdot g_{ij} \cos(\theta_i - \theta_j) \\ &\quad - V_i V_j \cdot b_{ij} \sin(\theta_i - \theta_j) \qquad (23) \\ Q_{ij} &= -V_i^2 \cdot (b_{ij} + b_{ij}^{sh}) + V_i V_j \cdot b_{ij} \cos(\theta_i - \theta_j) \\ &\quad - V_i V_j \cdot g_{ij} \sin(\theta_i - \theta_j) \qquad (24) \end{aligned}$$

where V_i is the voltage at bus i and g_{ij}, b_{ij} and b_{ij}^{sh} are line parameters. The active and reactive power injected into bus i are given by

$$P_i = \sum_{j \in \Omega_i} P_{ij} \qquad (25)$$

$$Q_i = \sum_{j \in \Omega_i} Q_{ij}. \qquad (26)$$

Similar to the dc analysis, the choice of the column and measurements to be adjusted determine the state variable—in this case voltage magnitude or voltage angle—for which the estimated value will be changed.

Assuming that the attacker wants to alter the power flow on the line connecting bus i and j and has chosen V_i as the state variable to be impacted, then the following equation must be solved in order to find the voltage magnitude which will yield the desired power flow:

$$\begin{aligned} P_{ij} &= V_{i,a}^2 \cdot g_{ij} - V_{i,a} V_j \cdot g_{ij} \cos(\theta_i - \theta_j) \qquad (27) \\ &\quad - V_{i,a} V_j \cdot b_{ij} \sin(\theta_i - \theta_j) \qquad (28) \end{aligned}$$

where the subscript a indicates the state variable which will be influenced by the attacker. It is a quadratic equation for which multiple solutions exist. In most of the cases, however, only one of the solutions makes physical sense. While in the dc analysis, the attacker did not need to know the values of the state variables, this is no longer the case in the ac analysis. In order to solve the above equation, he needs to know or estimate the values V_j and $\theta_i - \theta_j$. Having determined the value $V_{i,a}$ the values for the other measurements are calculated using (23)–(26).

Another option is to choose θ_i as the state variable to be impacted. Since the sensitivity of active power flows and injections on voltage angles is significantly higher than for voltage magnitudes, a larger impact on power flows should be expected for smaller changes in voltage angles. If both the voltage magnitude and angle are chosen as variables to be defined, the possible set of solutions becomes even larger.

A necessary condition for how the measurement which have been identified in the first step to guarantee a hidden attack can be derived as follows from bad data detection:

$$\begin{aligned} \|\mathbf{z_a} - \mathbf{h}(\hat{\mathbf{x}}_{\mathbf{bad}})\| &= \|\mathbf{z} + \mathbf{a} - \mathbf{h}(\hat{\mathbf{x}} + \mathbf{c})\| \\ &= \left\| \begin{pmatrix} \mathbf{z_1} \\ \mathbf{z_2} + \mathbf{a_2} \end{pmatrix} - \begin{pmatrix} \mathbf{h_1}(\hat{\mathbf{x}}_1) \\ \mathbf{h_2}(\hat{\mathbf{x}}_1, \hat{\mathbf{x}}_2 + \mathbf{c}) \end{pmatrix} \right\| \\ &= \left\| \begin{pmatrix} \mathbf{z_1} \\ \mathbf{z_2} \end{pmatrix} - \begin{pmatrix} \mathbf{h_1}(\hat{\mathbf{x}}_1) \\ \mathbf{h_2}(\hat{\mathbf{x}}_1, \hat{\mathbf{x}}_2) \end{pmatrix} \right\| \\ &= \|\mathbf{z} - \mathbf{h}(\hat{\mathbf{x}})\| < \tau. \qquad (29) \end{aligned}$$

Variables with the subscript of 1 correspond to the measurements and state variables which are not altered by the attacker, whereas those with the subscript of 2 correspond to those that were maliciously altered (which measurements these are have been determined in the first step). The vectors $\mathbf{a}$ and $\mathbf{c}$ correspond to the required changes in the attacked measurements and the changes in estimated state variables, respectively.

From (29) it follows that the requirement to ensure that the attack is hidden is given by

$$\mathbf{a_2} = \mathbf{h_2}(\hat{\mathbf{x}}_1, \hat{\mathbf{x}}_2 + \mathbf{c}) - \mathbf{h_2}(\hat{\mathbf{x}}_1, \hat{\mathbf{x}}_2). \qquad (30)$$

It can be seen from this equality that, at difference with the dc analysis, an attacker using an ac analysis must also know the estimated value for the set of state variables that appear in $\mathbf{h_2}$.

VI. Simulation Results

In the following simulations we illustrate how to determine the number of measurements an attacker needs to alter in order to hide an attack. This will also provide a system operator an intuitive indication of the measurements that can be easily subverted. We also simulate ac versus dc analysis for determining an attack vector for the purposes of: 1) illustrating the two methods; 2) evaluating the effectiveness of the dc analysis to subvert ac state estimation; and 3) to provide insight into some of the security characteristics that can defeat stealthy FDI attacks by virtue of the power grid design.

We use the IEEE 57 bus system as the test system. It is assumed that the measurements taken in the system are the following:

- active power flows on all lines at both ends of the line;
- reactive power flows on all lines at both ends of the line;
- voltage magnitudes at all buses;
- voltage angles at all buses;
- active power injection at buses with loads and/or generation;
- reactive power injection at buses with loads and/or generation;

i.e., for all of the following simulations, the actual measurements taken is the same and equal to 518.

The following simulations are carried out:

1) *Minimum Number of Attacked Measurements*: Using the subgraph method described in Section V-B, we determine the minimum number of measurements that an attacker needs to corrupt in order to attack any line or bus injection measurement, without being detected.

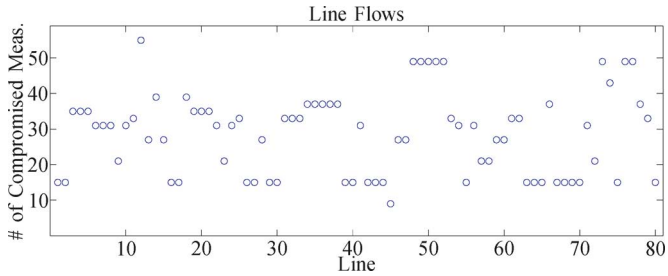

Fig. 2. The minimum number of adjusted measurements for a hidden attack on active or reactive power flows on either side of line ij.

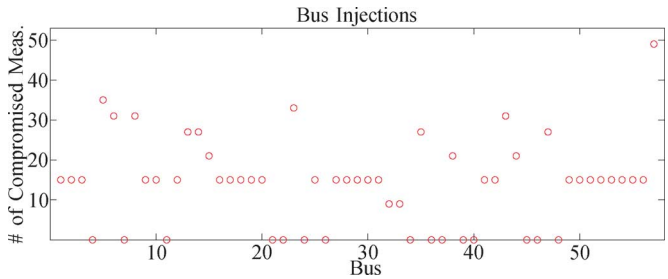

Fig. 3. The minimum number of adjusted measurements for a hidden attack on active or reactive power injections at bus i.

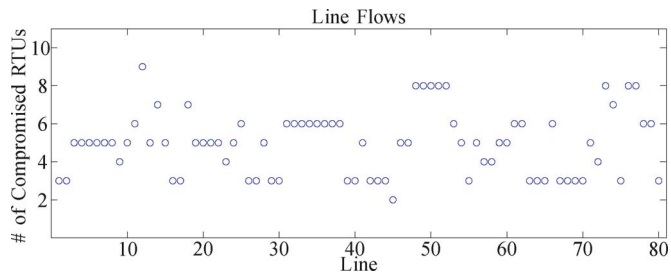

Fig. 4. The minimum number of RTUs that must be compromised to attack active or reactive power flows on either side of line ij.

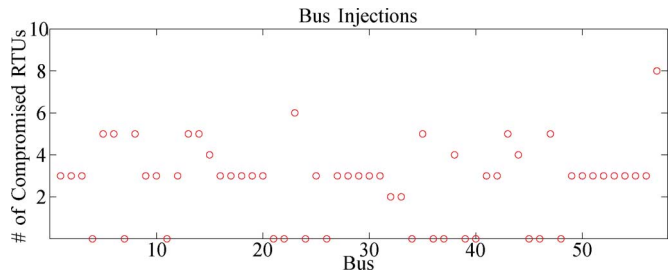

Fig. 5. The minimum number of RTUs that must be compromised to attack active or reactive power injections at bus i.

2) *ΔV, $\Delta\theta$ via AC Analysis*: The changes in voltage angles and magnitudes required to hide an attack on a line flow are determined. We assume that the perceived line flow should be 50% higher than the actual line flow.
3) *Comparison of AC vs. DC Analyses*: Changes in the voltage angle to hide an attack on line flows are determined using a dc analysis and compared to the values determined with the ac analysis. The resultant errors in adjustment of measurements are evaluated.

A. Minimum Number of Attacked Measurements

Based on the topology of the system and according to the method described in Section V, the upper bound on the minimum number of measurements which the attacker needs to corrupt in order to hide an attack on a line flow or a bus injection is determined. Since it is assumed that all possible measurements are taken, this upper bound is equal to the minimum number and is given by (15). The results for line flows are given in Fig. 2. The line number of the x-axis indicates the line that is attacked, i.e., the attacker wants to change the perceived value of one of the measurements on this line, and the results provide the number of measurements which the attacker needs to manipulate in order to hide this attack. For example, in order to change the perceived value of one of the measurements of line 1, he needs to adjust a total of 15 measurements.

The results for bus injection measurements are given in Fig. 3. The explanation for the representation of the results is the same as for the line flow measurements. Zero measurements in Fig. 3 indicate a bus with no load or generation. Consequently, the power injections at this bus must equal zero. Whenever an attacker tries to change the perceived value of this injection, the operator will immediately know that this is not correct. Hence, *it is impossible to execute a hidden attack for such buses.*

Fig. 3 shows that the number of measurements to be compromised ranges from approximately 10 to 50. Multiple measurements may be transmitted via one single remote terminal unit (RTU), however, which will allow the attacker to manipulate multiple measurements by compromising just one RTU. Assuming that there is one RTU per bus and that the measurements of power injections, voltage magnitude and angle, as well as all power flows out of the bus, are transmitted via this RTU, then the number of RTUs that need to be compromised is significantly lower—from 2 to 9 RTUs—and is shown in Fig. 4 for line flow measurements, and for bus injection measurements—from 2 to 8 RTUs—shown in Fig. 5.

B. ΔV, $\Delta\theta$ Via AC Analysis

Compromised measurements lead to changes in the estimated values for voltage magnitudes and angles at buses in the subgraph at which no load or generation is connected, and at the bus which has been chosen as the center bus (cf. Section V-B, above). Often there are two free variables (voltage magnitude and voltage angle, except for the buses with a generator for which the voltage magnitude is fixed) but only one measurement to adjust, which results in an overdetermined system. Consequently, we formulate the problem as an optimization problem:

$$\min \quad \sum_{i\in\mathcal{S}_C} (\Delta V_i^2 + \Delta\theta_i^2) \tag{31}$$

$$s.t. \quad P_{ij} = (1+\gamma)\cdot P_{ij}^m \tag{32}$$

$$P_i = \sum_{j\in\Omega_i} P_{ij}, \;\; i \in \mathcal{S}_C \tag{33}$$

$$Q_i = \sum_{j\in\Omega_i} Q_{ij}, \;\; i \in \mathcal{S}_C \tag{34}$$

with the angle given in radians and the voltage in p.u. (per unit normalization [15]), to determine the changes in voltage magnitudes ΔV_i and voltage angles $\Delta\theta_i$ that will lead to the desired hidden attack changing the measurement P_{ij} by γ with respect to the actually measured value P_{ij}^m.

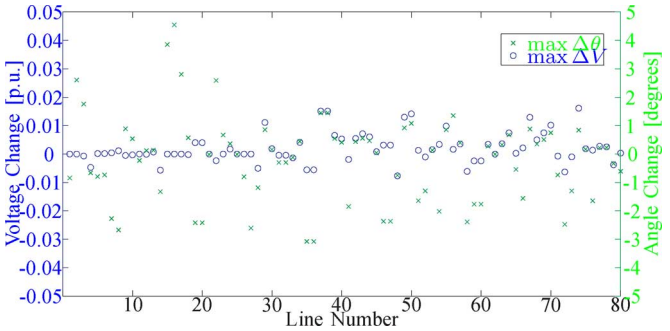

Fig. 6. Changes in voltage magnitude and angle to increase the perceived line flow by 50%.

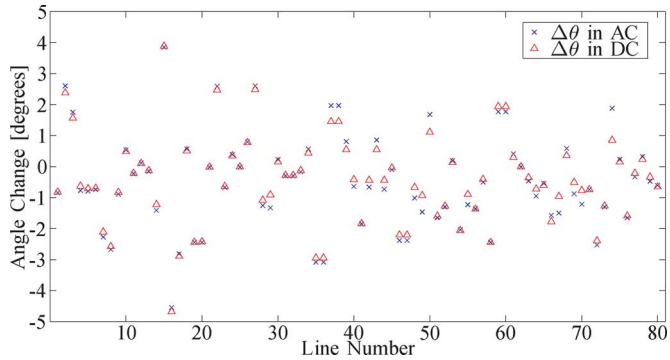

Fig. 7. Comparison of enforced changes in voltage angle for a 50% increase in perceived active line flow using ac and dc model.

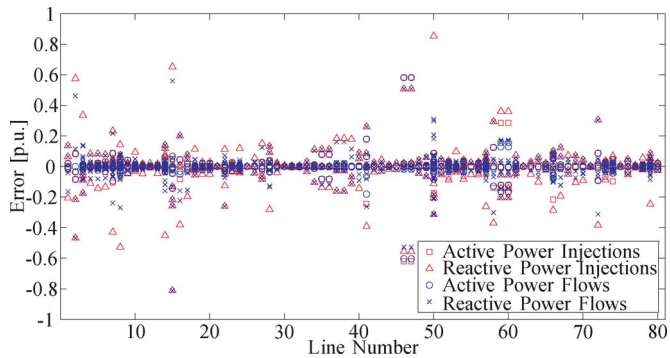

Fig. 8. Errors in adjusted values of power flow and injection measurements when using dc model.

Subgraph $\mathcal{S}_C$ corresponds to one of the subgraphs $\mathcal{S}_p$ identified by the method described in Section V-B up to step 7). Each of these subgraphs provides a possible set of measurements the attacker needs to modify in order to hide his attack. In step 8), the subgraph with the least number of measurements to be adjusted is determined. However, rather than choosing the one that yields the least measurements to be adjusted, the subgraph that results in the smallest changes in voltage magnitude and angle was chosen for this simulation as the worst case vulnerability. It should be noted that the subgraph with the smallest number of measurements to be influenced is not necessarily a good choice, because in some instances the changes in voltage and/or angle are so high that they will be easily detected by state estimation.

Fig. 6 shows the resulting voltage magnitude and angle changes for the specific bus at which the changes are the largest for a change in line flow of $+50\%$. E.g. in order to change the perceived active power flow on line 1, the largest change in voltage angle (and in this case, this is the only change because no bus without power injections is included in the subgraph) is $\approx 0.9°$. The reader should be aware of the different scales for voltage magnitude and angle. Since the dependency of active power flows on voltage angles is significantly larger than on voltage magnitude, usually the $\Delta\theta_i$ is comparably large if compared to ΔV_i. The angle changes are within a range of $\pm 5°$ and the voltage magnitude changes within ± 0.02 p.u.

C. Comparison of AC and DC Analyses

The point of this comparison is to determine the feasibility of planning an attack on an ac transmission grid, based solely on the use of a dc model of that system. In order to use an ac attack analysis, the attacker needs significantly more system data. Using a dc model requires less data to determine by how much the measurements should be adjusted but will also result in errors that potentially could trigger bad data detection of the FDI. In this simulation, the results from an ac attack analysis and from a dc attack analysis are compared. For directly comparable results, only the voltage angle at the chosen center bus has been adjusted and the voltage magnitude is kept constant for the ac case. The results of the changes in the voltage angle are given in Fig. 7 for a change in the perceived line flow of 50%. The deviations between the angle changes resulting from the dc model and the angle changes resulting from the ac model are fairly close for many of the cases. This is only part of the entire story, however. It is even more important to determine the errors which the attacker makes when adjusting the measurements sent to the control center.

Having determined the angle, the attacker would derive by how much he needs to change the power flow and injection measurements using these angle changes. Consequently, the error from the voltage angles propagates into the power flow and injection measurements sent by the attacker to the control center. An even more important factor is that the attacker completely neglects reactive power flows. Consequently, he will not know how to adjust these values and possibly leave them unchanged.

Fig. 8 shows the errors in power injections and line flows determined by using the dc model with respect to the values that the ac model provides, i.e., the reference values are determined by the ac model and are fully compliant with the power flow equations. In the figure, values for the errors are given in p.u.: the active power flows range up to 1.78 p.u., reactive power flows up to 0.75 p.u., active power injections up to 4.24 p.u. and reactive power injections up to 1.12 p.u. Consequently, the errors introduced by the dc model for many cases are quite significant.

VII. Conclusion

Analyses of the implications of a hidden false data injection attack at the RTU level on ac state estimation have been derived and a method has been presented that determines the number of measurements an attacker needs to modify in order to prevent the detection of those modifications, for any given system (including buses with no power injections) and available measurements. The number of attacked measurements for a hidden

attack is dependent on the topology of the system and the presence of buses with no power injections. In fact, buses with no power injections increase the security of the system with respect to false data injection attacks due to the fact that the power injections at these buses must equal zero. The method has been derived for a single attack but is extendable to multiple attacks which will be part of future work.

Comparing the results from a dc attack analysis with the results from an ac attack analysis indicates that an attacker using a dc model for this specific type of false data injection attack at the RTU level has a greater chance of introducing errors in the measurements, which in turn, will trigger bad data detection. Consequently, it can be concluded that the nonlinearity of the power flow equations provide advantages to the system operator with regards to this type of attack, however, only if the attacker does not have knowledge of the system data which would allow him to use an ac attack analysis. If the attacker is in possession of this data, then he could be able to execute an attack which would pass unnoticed through ac state estimation.

Acknowledgment

This information was prepared as an account of work sponsored by an agency of the U.S. Government. Neither the U.S. Government nor any agency thereof, nor any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness, of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the U.S. Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the U.S. Government or any agency thereof.

References

[1] Office of the Manager, National Communications System, *Supervisory Control and Data Acquisition (SCADA) Systems,*TIB 04-1 ed. Arlington, VA, 2004.

[2] Y. Liu, M. K. Reiter, and P. Ning, "False data injection attacks against state estimation in electric power grids," in *Proc. 16th ACM Conf. Comput. Commun. Security*, 2009.

[3] G. Dan and H. Sandberg, "Stealth attacks and protection schemes for state estimators in power systems," in *Proc. 1st IEEE Int. Conf. Smart Grid Commun. (SmartGridComm)*, 2010, pp. 214–219.

[4] A. Teixeira, S. Amin, H. Sandberg, K. H. Johansson, and S. S. Sastry, "Cyber security analysis of state estimators in electric power systems," in *Proc. 49th IEEE Conf. Decision Control (CDC)*, 2010, pp. 5991–5998.

[5] H. Sandberg, A. Teixeira, and K. H. Johansson, "On security indices for state estimators in power networks," in *Proc. 1st Workshop Secure Control Syst.*, 2010.

[6] P. Mohajerin Esfahani, M. Vrakopoulou, K. Margellos, J. Lygeros, and G. Andersson, "Cyber attack in a two-area power system: Impact identification using reachability," in *Proc. Amer. Control Conf. (ACC)*, 2010.

[7] P. M. Esfahani, M. Vrakopoulou, K. Margellos, J. Lygeros, and G. Andersson, "A robust policy for automatic generation control cyber attack in two area power network," in *Proc. 2010 49th IEEE Conf. Decision Control (CDC)*, pp. 5973–5978.

[8] S. Sridhar and G. Manimaran, "Data integrity attacks and their impacts on SCADA control system," in *Proc. Power Energy Soc. Gen. Meet.*, 2010.

[9] L. Xie, Y. Mo, and B. Sinopoli, "False data injection attacks in electricity markets," in *Proc. 1st IEEE Int. Conf. Smart Grid Commun. (SmartGridComm)*, 2010.

[10] O. Kosut, J. Liyan, R. J. Thomas, and T. Lang, "Malicious data attacks on smart grid state estimation: Attack strategies and countermeasures," in *Proc. 1st IEEE Int. Conf. Smart Grid Commun. (SmartGridComm)*, 2010.

[11] R. B. Bobba, K. M. Rogers, Q. Wang, H. Khurana, K. Nahrstedt, and T. Overbye, "Detecting false data injection attacks on DC state estimation," in *Proc. 1st Workshop Secure Control Syst.*, 2010.

[12] T. T. Kim and H. V. Poor, "Strategic protection against data injection attacks on power grids," *IEEE Trans. Smart Grid*, vol. 2, no. 2, pp. 326–333, 2011.

[13] 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. Resilient Control Syst.*, 2009, pp. 31–35.

[14] A. Monticelli, "Electric power system state estimation," *Proc. IEEE*, vol. 88, no. 2, pp. 262–282, 2000.

[15] P. Schavemaker and L. van der Sluis*, Electrical Power System Essentials*. New York: Wiley, 2009.

Gabriela Hug (S'05–M'08) was born in Baden, Switzerland. She received the M.Sc. and Ph.D. degrees in electrical engineering from the Swiss Federal Institute of Technology (ETH), Zurich, in 2004 and 2008, respectively.

After her Ph.D., she worked in the Special Studies Group of Hydro One, Toronto, ON, Canada, and since 2009 she is an Assistant Professor at Carnegie Mellon University, Pittsburgh, PA. Her research is dedicated to control and optimization of electric power systems.

Joseph Andrew Giampapa received the M.Sc. degree from Carnegie Mellon University, Pittsburgh, PA, in 1998.

He is a Senior Member of the Technical Staff at the Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA. He leads research and development efforts that leverage his expertise in autonomous agents and multi-agent systems, robotics, agent-based modeling and simulation, artificial intelligence, and language technologies, for the purposes of achieving understanding, control, predictability, and justified confidence in the behavior of distributed, autonomous, cyber-physical, and socio-technical systems.