False Data Injection Attacks with Incomplete Information Against Smart Power Grids

Md. Ashfaqur Rahman[†] and Hamed Mohsenian-Rad[†‡]
[†]Department of Electrical and Computer Engineering, Texas Tech University, Lubbock, TX, USA
[‡]Department of Electrical Engineering, University of California, Riverside, CA, USA
e-mails: md.rahman@ttu.edu, hamed@ee.ucr.edu

***Abstract*— False data injection attacks have recently been introduced as an important class of cyber attacks against smart grid's wide area measurement and monitoring systems. These attacks aim to compromise the readings of multiple power grid sensors and phasor measurement units in order to mislead the operation and control centers. Recent studies have shown that if an adversary has complete knowledge on the power grid topology and transmission-line admittance values, he can adjust the false data injection attack vector such that the attack remains undetected and successfully passes the residue-based bad data detection tests that are commonly used in power system state estimation. However, in this paper, we explain that a realistic false data injection attack is essentially an attack with *incomplete information* due to the attackers lack of real-time knowledge with respect to various grid parameters and attributes such as the position of circuit breaker switches and transformer tap changers and also because of the attacker's limited physical access to most grid facilities. We mathematically characterize false data injection attacks with incomplete information from both the attacker's and grid operator's viewpoints. Furthermore, we introduce a novel vulnerability measure that can compare and rank different power grid topologies against such attacks. To the best of our knowledge, this paper is the first study to investigate false data injection attacks with line admittance uncertainty.**

***Keywords*: False Data Injection Attack, Smart Grid Security, Incomplete Information, Transmission Line Admittance Uncertainty, Transformer Tap Position, Topological Vulnerability.**

I. Introduction

The recent advancements in smart grid control and monitoring systems, such as two-way communication capabilities and distributed intelligence, can significantly enhance efficiency and reliability [1]. However, they may also create new vulnerabilities in power infrastructures if they are not accompanied with appropriate security enforcements. In particular, it has recently been shown that cyber attacks against the wide area measurement and supervisory control and data acquisition systems have the potential to significantly damage the power grid and the utilities and consumer equipment [2].

A new and important class of cyber attacks against smart grid's wide area measurement systems is recently identified in [3] as *false data injection attacks* (FDIAs). In FDIA an adversary aims to hack the readings of multiple sensors and phasor measurement units (PMUs) to mislead smart grid's decision making process. In [3] showed that if the false data injection vector fulfils certain conditions, the adversary will be able to inject an arbitrary amount of error in state estimation and yet the FDIA will still successfully pass the commonly used *residue-based bad data detection tests* in power system state estimation [4]. The later studies further revealed that an adversary may even gain some economic advantages by using FDIA against the wholesale electricity market [5].

In [6], the authors showed that one can prevent a false data injection attack against state estimation by protecting a subset of sensors and PMUs. However, the number of sensors that need to be protected can be large, e.g., as many as one third of all sensors connected to the grid buses [7]. Another thread of research seeks to improve the existing residue-based bad data detection methods in state estimation such that they can also detect false data injection attacks. For example, the use of L_∞-norm versus L_2-norm detectors are investigated in [8]. The more advanced generalized likelihood ratio test and the adaptive cumulative sum control chart test are also recently proposed to detect FDIAs in [9] and [10], respectively.

A common assumption in most prior work on FDIAs, e.g., in [3], [5]–[10], is that the attacker has *complete knowledge* about the power grid topology and transmission-line admittances. In fact, such information is implicitly assumed available to the attacker in order to construct the false data injection attack vector. However, an important practical scenario is the case when the attacker has limited information with respect to the power network topology or admittance for some transmission-lines. Therefore, the focus of this paper is to take the first step to investigate the possibilities for implementing a successful false data injection attack with limited information. The contributions of this paper can be summarized as follows.

- We explain that a realistic FDIA is essentially an attack with incomplete information due to the attacker's lack of real-time knowledge with respect to the status of various grid elements such as the position of circuit breaker switches and transformer tap changers and also because of his/her limited physical access to most grid facilities.
- We mathematically characterize FDIAs with limited information and show how the impact of the attack on the power grid as well as the likelihood of the attack being detected can be affected by the attacker's lack of complete knowledge about the grid parameters and attributes.
- We study FDIAs with limited information from both attacker's as well as grid operator's viewpoints. From an attacker's point of view, depending on the uncertainty patterns, we distinguish *perfect* and *imperfect* attacks. From an operator's point of view, we introduce a novel

vulnerability measure that can compare and rank various power grid topologies. This can potentially help building power grids that are less vulnerable against FDIAs.

The rest of this paper is organized as follows. The system model and the background on FDIAs with limited information are given in Section II. We mathematically characterize FDIAs with limited information in Section III. Optimizing such attacks from the attacker's viewpoint is discussed in Section IV. Analyzing the grid vulnerability from the operator's viewpoint are investigated in Section V. Simulation results are presented in Section VI. The paper is concluded in Section VII.

II. System Model and Background

A. State Estimation in Power Systems

Let $\mathbf{z}$ denote an $m\times 1$ vector of all measurements in a power system such as power flows at transmission lines and power injections and loads at buses. The power flow measurements can be taken at one or both ends of a transmission line. In the state estimation problem in power systems, we are interested in using the collected set of measurements to estimate an $n \times 1$ vector of unknown states $\mathbf{x}$, where $n \ll m$. The unknown states can be, for example, the voltage angles at different buses. Let $\mathbf{H}$ denote the $m \times n$ network topology matrix. We have

$$\mathbf{z} = \mathbf{H}\mathbf{x} + \mathbf{e}, \tag{1}$$

where $\mathbf{e}$ denotes measurement noise. In general, there are three criteria that are commonly used to estimate the system states: maximum likelihood, weighted least-square, and minimum variance. When the measurement noise is Gaussian with zero mean, these criteria lead to the same estimator [4]:

$$\hat{\mathbf{x}} = (\mathbf{H}^T\mathbf{W}\mathbf{H})^{-1}\mathbf{H}^T\mathbf{W}\mathbf{z}, \tag{2}$$

where the $m \times m$ noise co-variance matrix $\mathbf{W}$ is diagonal.

Next, we explain how the network topology matrix $\mathbf{H}$ is constructed. Let $\mathbf{A}$ denote the $l \times n$ grid connectivity matrix, where l denotes the number of transmission lines. Without loss of generality we assume an arbitrary direction for each transmission line. For each transmission line i, the element in i^{th} row and j^{th} column is $A_{ij} = 1$, if the direction of link i is from bus j, $A_{ij} = -1$, if the direction of link i is towards bus j, and $A_{ij} = 0$, otherwise. Note that the power flow on a transmission line is assumed positive if it is at the direction of the line and negative if it is at the opposite of the direction of the line. Let $\mathbf{D}$ denote an $l \times l$ diagonal matrix representing the admittance of all transmission lines. For the rest of this paper, we assume that the collected measurements for state estimation comprise of all bus injections and power flows at both directions of all buses. Therefore, we have [11]:

$$\mathbf{H} = \begin{bmatrix} \mathbf{A}^T\mathbf{D}\mathbf{A} \\ \mathbf{D}\mathbf{A} \\ -\mathbf{D}\mathbf{A} \end{bmatrix}. \tag{3}$$

B. False Data Injection Attack with Complete Information

In False Data Injection Attack against smart grid, an adversary aims to hack the readings of sensors such that the vector of measurement $\mathbf{z}$ is replaced by a compromised vector $\mathbf{z}_a = \mathbf{z}+\mathbf{a}$, where $\mathbf{a}$ is an $m\times 1$ false data vector. Clearly, given the false measurement vector $\mathbf{z}_a$, the state estimation solution becomes $\hat{\mathbf{x}}_a \neq \hat{\mathbf{x}}$. As shown in [3], false data injection can sometimes be detected by using bad data detection methods which evaluate the measurement residue:

$$\mathbf{z}_a - \mathbf{H}\hat{\mathbf{x}}_a, \tag{4}$$

and trigger an alarm if the residue becomes greater than a preset limit. However, the results in [3] also show that if the attacker selects the false data injection vector $\mathbf{a}$ to be a linear combination of the rows in matrix $\mathbf{H}$, i.e., $\mathbf{a} = \mathbf{H}\mathbf{c}$ for some arbitrary $n \times 1$ vector $\mathbf{c}$, then the bad data detection methods based on residue test will *not* be able to detect the attack since the injected false data will no longer affect the residue:

$$\mathbf{z}_a - \mathbf{H}\hat{\mathbf{x}}_a = \mathbf{z} + \mathbf{a} - \mathbf{H}(\hat{\mathbf{x}} + \mathbf{c}) = \mathbf{z} - \mathbf{H}\hat{\mathbf{x}}, \tag{5}$$

where

$$\hat{\mathbf{x}}_a = \hat{\mathbf{x}} + (\mathbf{H}^T\mathbf{W}\mathbf{H})^{-1}\mathbf{H}^T\mathbf{W}\mathbf{H}\mathbf{c} = \hat{\mathbf{x}} + c. \tag{6}$$

In other words, if the attacker has *complete knowledge* of the grid topology and line admittances such that he can accurately construct matrix $\mathbf{H}$, then he will be able to implement a false data injection attack which is not detected by a residue test, yet it is able to inject an arbitrary error to the state estimation solution. However, we believe that in practice, the attacker's knowledge can be *limited* and involve *uncertainties*.

C. Obtaining Grid Connectivity and Admittance Matrices

As explained in Section II-B, to implement a false data injection attack, an adversary needs to construct matrix $\mathbf{H}$. From (3), this requires knowledge on connectivity matrix $\mathbf{A}$ and admittance matrix $\mathbf{D}$. Such knowledge can be gained through both *offline* and *online* data collections. Offline data collection can be done weeks, months, or even years before implementing the actual attack and may involve getting access to the *grid topology maps* through intruders or former utility company employees. However, offline data collection may not be enough to implement an attack. On one hand, some offline data could be outdated due to new construction and expansion of the existing transmission lines. On the other hand, in most practical cases, the exact position of *circuit breaker switches*, *transformer tap changers*, etc. can significantly affect the connectivity and admittance matrices, and thus the true value of matrix $\mathbf{H}$. Therefore, an adversary may need to implement some online data collection efforts, e.g., by deploying its own sensors and PMUs. Nevertheless, due to limited resources and restricted physical access to the grid, online data collection may not be feasible and the attack may essentially become an *attack with incomplete information*. Investigating this realistic scenario is the focus of this paper. In particular, we are interested in the case where the adversary has limited information of the line admittance values. This can be due to various practical reasons as we explain next.

First, the position of the transformer tap changers across the power grid may sometimes change to adjust the voltage and current ratios based on the power system operation conditions. An example is shown in Fig. 1. In this figure, the transmission

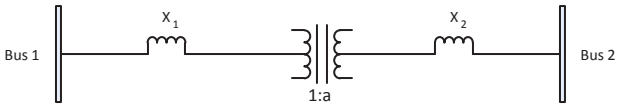

Fig. 1. A transmission line with a transformer. The transformer tap position can change from time to time and affect the line admittance $a^2X_1 + X_2$.

line between bus 1 and bus 2 includes fixed admittance values X_1 and X_2 and a transformer with turns ratio $1 : a$. In this case, the total admittance for the transmission lines between the two buses is $a^2X_1 + X_2$ for the right side. Clearly, while offline data collection can be used to obtain X_1 and X_2, the exact position of the tap changer, i.e., the value of parameter a may only be obtained via online data collection and/or physical access to the transformer site. If such access is not feasible, the uncertainty with respect to parameter a will affect constructing matrix $\mathbf{D}$ and thus $\mathbf{H}$. Second, even for transmission lines without transfer, obtaining the line admittance may require knowledge of the exact length of the transmission line and type of the conductor being used. Finally, even if the adversary can measure line admittance in an offline effort, the values may change by the time of implementing the attack due to weather conditions and changes in temperature [12].

III. False Data Injection Attacks with Incomplete Information

Consider a false data injection attack with incomplete information where the attacker does not have accurate knowledge about matrix $\mathbf{H}$, e.g., because of the issues discussed in Section II-C. Let us denote the attacker's understanding of the topology matrix $\mathbf{H}$ as $\bar{\mathbf{H}} = \mathbf{H} + \boldsymbol{\delta}$, where $\boldsymbol{\delta}$ is an $m \times n$ error matrix. Therefore, the false data injection attack vector implemented by the attacker in this case will be in the following form:

$$\mathbf{a} = \bar{\mathbf{H}}\mathbf{c} = (\mathbf{H} + \boldsymbol{\delta})\,\mathbf{c} = \mathbf{H}\mathbf{c} + \boldsymbol{\delta}\mathbf{c}. \tag{7}$$

Of course, since $\mathbf{a} \neq \mathbf{H}\mathbf{c}$, most existing theorems on FDIAs, e.g., those in [3], [5], are no longer applicable and the attack is no longer guaranteed to pass the residue test in Section II-B. In other words, the adversary's limited information may cause the attack to be detected by the grid operator.

From [3], vector $\mathbf{c}$ in (7) is the *estimation error* that the attacker *intends* to inject into the state estimation solution. Similarly, let $\bar{\mathbf{c}}$ denote the estimation error that the attacker *actually injects* into the solution in case of an attack with incomplete information. Note that, in general, $\bar{\mathbf{c}} \neq \mathbf{c}$. The state estimation solution under attack is obtained as,

$$\begin{aligned}\hat{\mathbf{x}}_a &= (\mathbf{H}^T\mathbf{W}\mathbf{H})^{-1}\mathbf{H}^T\mathbf{W}\,\mathbf{z}_a \\ &= (\mathbf{H}^T\mathbf{W}\mathbf{H})^{-1}\mathbf{H}^T\mathbf{W}(\mathbf{z}+\mathbf{a}) \\ &= (\mathbf{H}^T\mathbf{W}\mathbf{H})^{-1}\mathbf{H}^T\mathbf{W}(\mathbf{z}+\mathbf{H}\mathbf{c}+\boldsymbol{\delta}\mathbf{c}) \\ &= \hat{\mathbf{x}} + \mathbf{c} + (\mathbf{H}^T\mathbf{W}\mathbf{H})^{-1}\mathbf{H}^T\mathbf{W}\boldsymbol{\delta}\mathbf{c}.\end{aligned} \tag{8}$$

By definition, we have

$$\hat{\mathbf{x}}_a = \hat{\mathbf{x}} + \bar{\mathbf{c}}. \tag{9}$$

From (8) and (9), we can conclude that

$$\bar{\mathbf{c}} = \mathbf{c} + (\mathbf{H}^T\mathbf{W}\mathbf{H})^{-1}\mathbf{H}^T\mathbf{W}\boldsymbol{\delta}\mathbf{c}. \tag{10}$$

Next, we can obtain the residue in presence of a false data injection attack with limited information as

$$\begin{aligned}\mathbf{r}_a &= \mathbf{z}_a - \mathbf{H}\hat{\mathbf{x}}_a \\ &= \mathbf{z} + \mathbf{a} - \mathbf{H}(\hat{\mathbf{x}} + \bar{\mathbf{c}}) \\ &= \mathbf{r} + \boldsymbol{\delta}\mathbf{c} + \mathbf{H}(\mathbf{c} - \bar{\mathbf{c}}) \\ &= \mathbf{r} + (\mathbf{I} - \boldsymbol{\Gamma})\boldsymbol{\delta}\mathbf{c},\end{aligned} \tag{11}$$

where

$$\boldsymbol{\Gamma} \triangleq \mathbf{H}(\mathbf{H}^T\mathbf{W}\mathbf{H})^{-1}\mathbf{H}^T\mathbf{W}. \tag{12}$$

Note that $\boldsymbol{\Gamma}$ is a fixed $m \times m$ matrix which only depends on the matrixes $\mathbf{H}$ and $\mathbf{W}$. In presence of *no* false data injection attack, i.e., when $\mathbf{a} = \mathbf{0}$, bad data detection works by evaluating the following residue-related inequality test [4]:

$$J(\hat{\mathbf{x}}) \leq C, \tag{13}$$

where C is a control parameter that is selected based on the choice of false alarm rate. We also have

$$\begin{aligned}J(\hat{\mathbf{x}}) = \sum_{i=1}^{m}\left(\frac{z_i - \hat{z}_i}{\sigma_i}\right) &= \left|\left|\begin{bmatrix}\frac{z_1-\hat{z}_1}{\sigma_1}\\ \vdots \\ \frac{z_m-\hat{z}_m}{\sigma_m}\end{bmatrix}\right|\right|^2 = \left|\left|\begin{bmatrix}\frac{r_1}{\sigma_1}\\ \vdots \\ \frac{r_m}{\sigma_m}\end{bmatrix}\right|\right|^2 \\ &= \left|\left|\begin{bmatrix}\frac{1}{\sigma_1} & 0 & \dots \\ 0 & \frac{1}{\sigma_2} & \vdots \\ 0 & \dots & \frac{1}{\sigma_m}\end{bmatrix}\begin{bmatrix}r_1\\ \vdots \\ r_m\end{bmatrix}\right|\right|^2 = \left|\left|\sqrt{\mathbf{W}}\mathbf{r}\right|\right|^2.\end{aligned} \tag{14}$$

Similarly, for the case of a false data injection attack with incomplete information, the bad data detection test becomes

$$J(\hat{\mathbf{x}}_a) = ||\sqrt{\mathbf{W}}\mathbf{r} + \sqrt{\mathbf{W}}(\mathbf{I} - \boldsymbol{\Gamma})\boldsymbol{\delta}\mathbf{c}||^2 \leq C. \tag{15}$$

Together, (10) and (15) characterize an FDIA false data injection attack with incomplete information. Note that, for an attack with complete information, where $\boldsymbol{\delta} = \mathbf{0}$, from (10) and (15), we have $\bar{\mathbf{c}} = \mathbf{c}$ and $J(\hat{\mathbf{x}}_a) = J(\hat{\mathbf{x}})$. Furthermore, we can see that the amount of injected estimation error in (10) and the residue test outcome in (15) depend on not only the attacker's modeling error $\boldsymbol{\delta}$ but also some grid-specific parameters, i.e., matrixes $\mathbf{H}$ and $\mathbf{W}$. Of course, neither the attacker nor the grid operator are aware of the exact value of attacker's modeling error matrix $\boldsymbol{\delta}$. However, while the attacker does not have an accurate knowledge of $\mathbf{H}$, $\mathbf{W}$, and $\boldsymbol{\Gamma}$, these matrices are indeed known to the power grid operator. Therefore, we investigate the false data injection attacks with limited information first from the attacker's viewpoint and then from the grid operator's viewpoint.

IV. Attacker's View Point

In this section, we will discuss what an attacker can achieve when he has limited information. From (10) and (15) we can distinguish two different scenarios: a) *Perfect Attacks*: the attacks that can assure achieving $\boldsymbol{\delta}\mathbf{c} = \mathbf{0}$ even though $\boldsymbol{\delta} \neq \mathbf{0}$; b) *Imperfect Attacks*: the attacks that cannot assure achieving $\boldsymbol{\delta}\mathbf{c} = \mathbf{0}$. Next, we characterize perfect and imperfect attacks.

A. Perfect Attacks with Limited Information

A perfect attack is a false data injection attack in which $\boldsymbol{\delta}\mathbf{c} = \mathbf{0}$ and consequently $\bar{\mathbf{c}} = \mathbf{c}$ and $J(\hat{\mathbf{x}}_a) = J(\hat{\mathbf{x}})$. A perfect FDIA *cannot* be detected by a residue test, regardless of the fact that the attacker's knowledge about matrix $\mathbf{H}$ is not accurate. The following definition and theorem explain how we can characterize perfect FDIAs under attacks with incomplete information and transmission-line admittance uncertainties.

Definition: A *cut* is a set of transmission lines in a grid that can divide the power network into *two disjoint islands*. In general, each power grid topology may have several cuts.

Theorem 1: We can show that a) An attacker can implement a perfect FDIA under transmission-line admittance uncertainties if it has complete knowledge about the admittance values of *all* transmission lines on at least one cut. b) Let $\mathcal{N}_1$ and $\mathcal{N}_2$ denote the set of buses in the two disjoint islands that are formed by the aforementioned cut, if the attacker selects

$$c_i = c_j \quad \forall\, i, j \in \mathcal{N}_1, \tag{16}$$

$$c_i = c_j \quad \forall\, i, j \in \mathcal{N}_2, \tag{17}$$

then achieving $\boldsymbol{\delta}\,\mathbf{c} = \mathbf{0}$ is guaranteed regardless of the values of the admittances for the rest of the grid transmission lines.

Proof: First, we note that by definition, the summation of all entries in each row of the connectivity matrix $\mathbf{A}$ is zero. That is, for each row $i = 1, \ldots, l$, we always have

$$\sum_{j=1}^{n} A_{ij} = 0. \tag{18}$$

Let $\boldsymbol{\epsilon}$ denote the diagonal matrix of errors in the attacker's knowledge on the lines admittance values. From (3), we have

$$\mathbf{H} + \boldsymbol{\delta} = \begin{bmatrix} \mathbf{A}^T(\mathbf{D}+\boldsymbol{\epsilon})\mathbf{A} \\ (\mathbf{D}+\boldsymbol{\epsilon})\mathbf{A} \\ -(\mathbf{D}+\boldsymbol{\epsilon})\mathbf{A} \end{bmatrix} \quad \Rightarrow \quad \boldsymbol{\delta} = \begin{bmatrix} \mathbf{A}^T\boldsymbol{\epsilon}\mathbf{A} \\ \boldsymbol{\epsilon}\mathbf{A} \\ -\boldsymbol{\epsilon}\mathbf{A} \end{bmatrix}. \tag{19}$$

Thus, a *sufficient condition* to have $\boldsymbol{\delta}\,\mathbf{c} = \mathbf{0}$ is to have

$$\boldsymbol{\epsilon}\mathbf{A}\mathbf{c} = \mathbf{0}. \tag{20}$$

Consider an arbitrary cut for the power network topology and the two constructed disjoint islands of buses $\mathcal{N}_1$ and $\mathcal{N}_2$, as defined in Theorem 1. Next, we reorder the rows of matrix $\mathbf{A}$ such that the first rows correspond to the links in the first island, denoted by $[\mathbf{A}_1\ \mathbf{0}]$, then it comes to the rows corresponding to the links that belong to the cut, denoted by $\mathbf{A}_c$, and finally it comes to the tows corresponding to the links in the second island, denoted by $[\mathbf{0}\ \mathbf{A}_2]$. That is,

$$\mathbf{A} = \begin{bmatrix} \mathbf{A}_1 & & \mathbf{0} \\ & \mathbf{A}_c & \\ \mathbf{0} & & \mathbf{A}_2 \end{bmatrix}. \tag{21}$$

If the attacker knows the admittance values for all the transmission lines on the cut, then we have

$$\boldsymbol{\epsilon} = \begin{bmatrix} \boldsymbol{\epsilon}_1 & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \boldsymbol{\epsilon}_2 \end{bmatrix} \quad \Rightarrow \quad \boldsymbol{\epsilon}\mathbf{A} = \begin{bmatrix} \boldsymbol{\epsilon}_1\mathbf{A}_1 \\ \mathbf{0} \\ \boldsymbol{\epsilon}_2\mathbf{A}_2 \end{bmatrix}, \tag{22}$$

where $\boldsymbol{\epsilon}_1$ and $\boldsymbol{\epsilon}_2$ are diagonal. From (18) and (22), condition (20) holds if vector $\mathbf{c}$ is selected as in (16) and (17). ■

From Theorem 1, knowing the admittance values for all transmission lines in the power grid is *not* necessary for implementing a perfect FDIA with limited information. Instead, the attacker only needs to know the admittance values for only a small group of transmission lines that together can form a cut. That is, having limited information on other transmission lines does not affect the attacker's ability in implementing a successful and effective FDIA. Of course, the attack would still face some limitations in terms of the injected estimation errors into the state estimation solution as such errors cannot be arbitrary and need to follow the conditions in (16) and (17).

B. Imperfect Attacks with Limited Information

Next, assume that the attacker does not have exact knowledge about the transmission line admittance values for any cut in the power grid topology. In that case, reaching $\boldsymbol{\delta}\mathbf{c} = \mathbf{0}$, i.e., implementing a perfect attack, may not be possible. Instead, the attacker may only have some probability distribution of the transmission line admittance values. Such information can be obtained from offline data collection, e.g., the historical data of the position of each transformer's tap changer, etc.

From (10) and (15), the attacker should seek to simultaneously minimize $(\mathbf{H}^T\mathbf{W}\mathbf{H})^{-1}\mathbf{H}^T\mathbf{W}\boldsymbol{\delta}\mathbf{c}$ to achieve $\bar{\mathbf{c}} \approx \mathbf{c}$ and minimize $\sqrt{\mathbf{W}}(\mathbf{I}-\boldsymbol{\Gamma})\boldsymbol{\delta}\mathbf{c}$ to achieve $J(\hat{\mathbf{x}}_a) \approx J(\hat{\mathbf{x}})$. However, these objectives can be reached only if the attacker is accurately aware of matrixes $\mathbf{H}$, $\mathbf{W}$, and $\boldsymbol{\Gamma}$, which is not the case in an attack with limited information. Therefore, an attacker may have no choice but using some offline knowledge on the probability distribution of the elements of matrix $\boldsymbol{\delta}$ as mentioned earlier and rather focus on minimizing $||\boldsymbol{\delta}\mathbf{c}||$. In this regard, the adversary may aim to select vector $\mathbf{c}$ such that it can solve the following stochastic optimization problem:

$$\begin{aligned} &\underset{\mathbf{c}}{\textbf{maximize}} \ \ \underset{i\in\mathcal{N}}{\textbf{minimum}} \ \ c_i \\ &\textbf{subject to} \ \ \mathbb{E}\left\{\|\boldsymbol{\delta}\,\mathbf{c}\|\right\} \le \kappa\sqrt{C} \end{aligned} \tag{23}$$

Here, the objective is to maximize the impact of the attack by maximizing the minimum amount of error to be injected into the state estimation solutions. However, in order to limit the chance of the attack being detected, the solution should be subject to maintaining the *expected* norm of $\boldsymbol{\delta}\mathbf{c}$ below $\kappa\sqrt{C}$, where $0 < \kappa < 1$ is an attack planning parameter. We note that if a perfect attack is feasible, then the optimal solution of problem (23) will automatically become as in (16) and (17) and the optimal objective value will be unbounded regardless of the probability distribution of the unknown transmission line admittance values. Furthermore, we note that one can introduce an auxiliary variable t and replace problem (23) with the following equivalent optimization problem:

$$\begin{aligned} &\underset{\mathbf{c},t}{\textbf{maximize}} \ \ t \\ &\textbf{subject to} \ \ \mathbb{E}\left\{\|\boldsymbol{\delta}\,\mathbf{c}\|\right\} \le \kappa\sqrt{C} \\ &\qquad\qquad c_i \ge t, \quad \forall\, i \in \mathcal{N}. \end{aligned} \tag{24}$$

Problem (24) is a standard stochastic convex program that can be solved, e.g., using scenario generation as explained in [13].

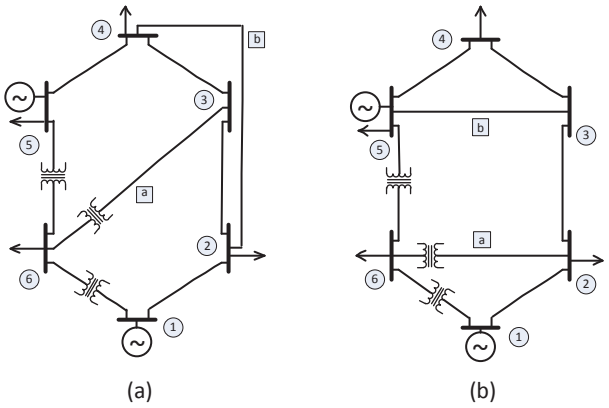

Fig. 2. Two power grids with six buses and eight lines. We can show that the grid on the left is more vulnerable against FDIAs with incomplete information.

V. Grid Operator's view point

Similar to the attacker, the grid operator is not aware of the attacker's modeling mismatch matrix $\boldsymbol{\delta}$. However, unlike the attacker, the grid operator does know the true and up-to-date values of matrices $\mathbf{H}$, $\mathbf{W}$, and $\mathbf{\Gamma}$. Given such knowledge, the grid operator is interested in answering the following two questions: 1) Which power grid topologies, characterized by matrices $\mathbf{H}$, $\mathbf{W}$, and $\mathbf{\Gamma}$, are less vulnerable against FDIAs with incomplete information. 2) Can we slightly change a power grid topology and make it less vulnerable against FDIAs with incomplete information. For example, consider the two partly similar power grid topologies in Fig. 2. From [3], if the attacker has *complete knowledge* about matrix $\mathbf{H}$ corresponding to each of these two topologies, then the two networks are *equally vulnerable* to a FDIA as long as the adversary selects the attack vector as $\mathbf{a} = \mathbf{Hc}$ as discussed in Section II-B. However, as shown next, one can argue that in case of FDIAs with *incomplete information*, the power grid in Fig. 2(b) is less vulnerable compared to the grid in Fig 2(a).

To obtain an analytical measure for vulnerability against FDIAs with limited information, we note that an attack is successful if it is likely to pass the bad data detection test in (15) while it imposes a significant error in power state estimation solution. Thus, given $\mathbf{H}$, $\mathbf{W}$, and $\mathbf{\Gamma}$ for each grid topology and given a probability distribution function for mismatch matrix $\boldsymbol{\delta}$, we can introduce a *vulnerability measure* (VM) specific to the power grid topology of interest as follows:

$$\begin{aligned} VM = \quad & \underset{\mathbf{c},t}{\textbf{maximum}} \quad t \\ & \textbf{subject to} \quad \mathbb{E}\left\{\|\sqrt{\mathbf{W}}(\mathbf{I}-\mathbf{\Gamma})\boldsymbol{\delta}\,\mathbf{c}\|\right\} \leq \sqrt{C} \\ & \qquad\qquad c_i \geq t, \qquad \forall\, i \in \mathcal{N}. \end{aligned} \tag{25}$$

We may note the following remarks. First, the difference between problems (24) and (25) is in the choice of constraints. In (24), the grid operator obtains an estimate on how strong an attack can become while it is not detected, in a stochastic sense, by a bad data detection test. Second, For each topology, the VM in (24) depends on the probability distribution function for matrix $\boldsymbol{\delta}$. Assuming a Gaussian distribution with zero mean for each element of matrix $\boldsymbol{\delta}$, one can expect that the VM decreases, i.e., the grid becomes less vulnerable, as the mismatch variance increases. Finally, the VM in (24) can be used to compare the vulnerability of different power grids with similar probability distribution functions for mismatch matrix $\boldsymbol{\delta}$. As we will explain in detail in Section VI for the case of topologies in Fig. 2, some power grid topologies can be seen to less vulnerable to FDIAs with incomplete information.

VI. Simulation Results

In this section, we assess the efficiency of FDIAs with incomplete information. First, the results on detecting an imperfect FDIA in an IEEE 118 bus test system are shown in Fig. 3. Here, we have plotted the measurement residue under the attack versus 1000 different measurement noise scenarios. The residue test parameter C is set at such a value that 2.5% residue goes up it without attack. We can see that the rate of detecting the attack with the residue test is as low as only 3.5%, which is minor indicating that having incomplete information has not affected the attacker's ability in implementing a successful FDIA attack significantly.

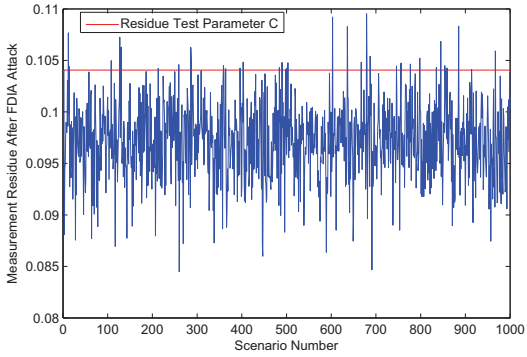

Fig. 3. The measurement residues after an FDIA with incomplete information of transmission line admittance values for 1000 different noise scenarios.

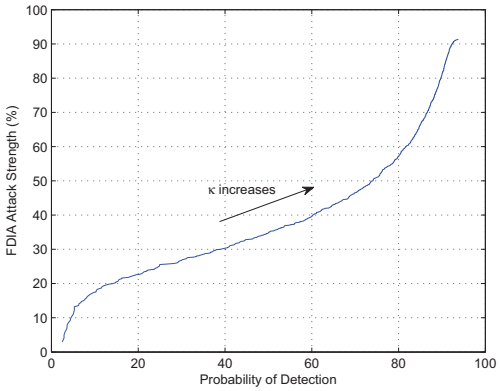

Fig. 4. The trade-off between attack strength and the probability of detection.

From (23), the attacker may increase κ to implement stronger attacks, i.e., attacks with higher values for the entries of vector $\mathbf{c}$. However, higher κ will increase the risk of the FDIA being detected. The trade-off is shown in Fig. 4. Here, the attack strength is defined as the optimal objective value of problem (24). We can see that if the attack strength is limited to 10%, then the probability of detecting the imperfect FDIAs with limited information on transmission line admittance is

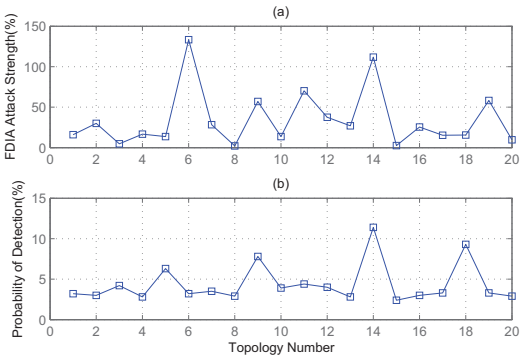

Fig. 5. The strength of an attack and the probability of detecting attack for 20 topology and measurement noise scenarios under admittance uncertainties.

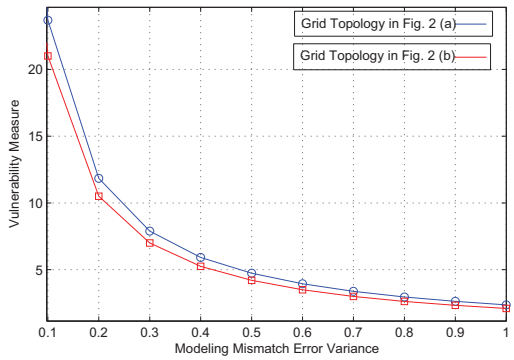

Fig. 6. Comparing the vulnerability measures of the two power grid topologies in Figs. 2(a) and (b). The topology in Fig. 2(b) is less vulnerable.

as small as only 5%. As we increase κ, although the attacks become stronger, the probability of detecting the attacks will increase. Note that, these results are for the cases where the attack is imperfect. Clearly, if the attack is perfect or the attacker has complete information, then the attack strength can arbitrarily increase without affecting the measurement residues, as long as vector $\mathbf{c}$ is selected according to the conditions in (16) and (17) as explained in Theorem 1.

Next, we simulate 20 different attack scenarios under different topologies and different transmission line admittance uncertainties. The results are shown in Fig. 5. In each case, the attack vector $\mathbf{a}$ is calculated based on (7) where $\mathbf{c}$ is chosen according to the solution of problem (24). The probability distribution of the unknown admittance parameters are assumed to be normal and spanned within $\pm 20\%$ of the correct admittance values. We can see that except for scenario 14, the probability of detecting the attack is small and below 10%. On the other hand, in almost all cases the FDIA under uncertainties have significant strengths. For example, in scenario 6, while the minimum injected error in state estimation (i.e., the attack strength) is around 135%, the probability of attack being detected is only 4%. The trade-off between the attack strength and the probability of detecting the attack depends on the configuration of the transmission line admittance uncertainties as explained in Theorem 1.

Finally, we compare the vulnerability measures of the two topologies in Fig. 2. For each topology, we plot the vulnerability measure, as defined in (25), versus the variance in the attacker's modeling error $\boldsymbol{\delta}$. Recall that the vulnerability measure is calculated by the grid operator to assess how vulnerable a topology can become given different uncertainty levels in the attacker's knowledge of the grid. We can see in Fig. 6 that, for all variance levels, the grid in Fig. 2(b) has a lower vulnerability measure than the one in Fig. 2(a). This suggest that the topology in Fig. 2(b) is less vulnerable to FDIAs with *limited information*. It is worth mentioning that if the variance is zero, i.e., in case of an attack with *complete information*, then the two topologies are *equally vulnerable* to an FDIA as long as the adversary selects the attack vector as $\mathbf{a} = \mathbf{Hc}$ as explained in Section II-B.

VII. Conclusions

We addressed the problem of implementing an FDIA when the attacker has incomplete information about the admittances of transmission lines. Such attacks were investigated from both attacker's and grid operator's viewpoints. We introduced two types of attacks. First, *perfect attacks*, where the attacker has complete knowledge of the admittance for all lines on at least one cut on the grid topology. Second, *imperfect attacks*, where such information is not available. We showed that an attacker may construct a probability distribution function for each unknown admittance to design an imperfect attack according to the solution of a stochastic optimization problem. We also introduced a novel vulnerability measure to compare and rank different grid topologies against FDIAs with incomplete information. This measure can potentially help building power grids that are less vulnerable against practical false data injection attacks when the attacker has limited information.

References

[1] A. Ipakchi and F. Albuyeh, "Grid of the future," *IEEE Power and Energy Magazine*, pp. 52–62, Mar. 2009.

[2] D. Kundur, X. Feng, S. Liu, T. Zourntos, and K. Butler-Purry, "Towards a framework for cyber attack impact analysis of the electric smart grid," in *Proc. of IEEE SmartGridComm*, Gaithersburg, MD, Oct. 2010.

[3] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," in *Proc. of ACM CCS*, Chicago, IL, Oct. 2010.

[4] A. Monticelli, *State Estimation in Power Systems*. Boston: Kluwer Academic Publishers, 1999.

[5] L. Xie, Y. Mo, and B. Sinopoli, "False data injection attacks in electricity markets," in *Proc. of IEEE International Conference on Smart Grid Communications (SmartGridComm)*, Gaithersburg, MD, Nov. 2009.

[6] R. B. Bobba, K. M. Rogers, Q. Wang, H. Khurana, K. Nahrstedt, and T. J. Overbye, "Detecting false data injection attacks on dc state estimation," in *Proc. of IEEE SCS*, Stockholm, Sweden, Apr. 2010.

[7] S. Bi and Y. J. Zhang, "Defending mechanisms against false-data injection attacks in the power system state estimation," in *Proc. of IEEE Globecom SG-COMNETS*, 2011.

[8] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Limiting false data attacks on power system state estimation," in *Proc. of IEEE CISS*, Princeton, NJ, Mar. 2010.

[9] ——, "On malicious data attacks on power system state estimation," in *Proc. of IEEE UPEC*, Cardiff, Wales, Aug. 2010.

[10] Y. Huang, H. Li, K. A. Campbell, and Z. Han, "Defending false data injection attack on smart grid network using adaptive cusum test," in *Proc. of IEEE CISS*, Baltimore, MD, Mar. 2011.

[11] K. C. Sou, H. Sandberg, and K. H. Johansson, "Electric power network security analysis via minimum cut relaxation," in *Proc. of IEEE Conference on Decision and Control*, Dec. 2011.

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

[13] K. Marti, *Stochastic Optimization Methods*. New York: Springer, 2005.