This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2015.2495133, IEEE Transactions on Smart Grid

A Review of False Data Injection Attacks Against Modern Power Systems

Gaoqi Liang, *Student Member, IEEE,* Junhua Zhao, *Member, IEEE,* Fengji Luo, *Member, IEEE,* Steven R. Weller, *Member, IEEE,* and Zhao Yang Dong, *Senior Member, IEEE*

***Abstract*— With rapid advances in sensor, computer and communication networks, modern power systems have become complicated cyber-physical systems. Assessing and enhancing cyber-physical system security is therefore of utmost importance for the future electricity grid. In a successful false data injection attack (FDIA), an attacker compromises measurements from grid sensors in such a way that undetected errors are introduced into estimates of state variables such as bus voltage angles and magnitudes. In evading detection by commonly employed residue-based bad data detection tests, FDIAs are capable of severely threatening power system security. Since the first published research on FDIAs in 2009, research into FDIA-based cyber-attacks has been extensive. This paper gives a comprehensive review of state-of-the-art in FDIAs against modern power systems. The paper first summarizes the theoretical basis of FDIAs, and then discusses both the physical and economic impacts of a successful FDIA. The paper presents the basic defense strategies against FDIAs, and discusses some potential future research directions in this field.**

***Index Terms*— Cyber physical security, false data injection attacks, state estimation, power system**

I. INTRODUCTION

Power systems are critical societal infrastructures. Reliable electricity supply via the modern power grid is fundamentally supported by the underlying cyber systems. Consequently, security has become a crucial factor for modern power system operation.

Power system security involves two main aspects: physical security and cyber security. Physical security represents the ability of a power system to maintain a normal working state in the presence of severe disturbances. Cyber security refers to the security of the communication networks and computer systems which support the power system operation. In recent years, cyber security has been become a significant threat to modern power system due to the pervasive application of information technologies. Moreover, weaknesses in cyber security can also

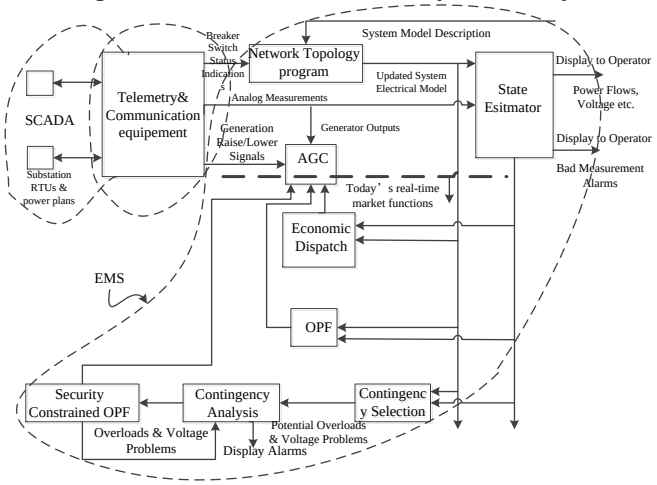

Fig. 1. EMS/SCADA/SE system diagram [8]

threaten the physical security of the power systems due to the deep integration of the physical and cyber systems [1-6].

Cyber-attacks are capable of undermining or even totally disrupting the control systems underlying electric power grids. It was traditionally believed that cyber-attacks were incapable of threatening the security of industrial systems. However, cyber-attacks have resulted in many security problems in recent years, and have become a critical concern for both industrial control system users and vendors [7]. For example, in 2000, the Supervisory Control and Data Acquisition (SCADA) system of the sewage control system in Maroochy Shire, Australia, was compromised. In 2003, a cyber-attack penetrated a computer network at the Davis-Besse nuclear power plant in the U.S. In 2008, the public transport system in Poland was hacked remotely, while in 2010 the Stuxnet worm attacked Iran's Natanz nuclear fuel-enrichment facility.

As depicted in Fig.1, state estimation plays a very important role in the control center. It calculates the state of every bus, and filters raw measurements by processing the data provided by the SCADA system. A successful attack on a SCADA system typically affects the power system state estimation process. Since many power system applications (such as economic dispatch (ED), contingency analysis, etc.) rely on the results of state estimation [11], [14], falsified state estimation results potentially mislead the operation and control functions of energy management systems (EMSs). In a worst-case situation, such an attack could have catastrophic consequences [12]. It is therefore

This research is partially supported by a China Southern Power Grid Research Grant (WYKJ00000027).

J.H. Zhao is the corresponding author of this paper.

G. Liang, J.H. Zhao and F. Luo are with the Center for Intelligent Electricity Networks (CIEN), University of Newcastle, Callaghan, NSW, 2308, Australia (e-mails: gaoqi.liang@uon.edu.au; andy.zhao@newcastle.edu.au fengji.luo@newcastle.edu.au;).

S.R. Weller is with the School of Electrical Engineering and Computer Science, University of Newcastle, Callaghan, NSW, 2308, Australia (e-mail: steven.weller@newcastle.edu.au).

Z.Y. Dong is with the School of Electrical and Information Engineering, the University of Sydney, Sydney, NSW, 2006, Australia (email: joe.dong@sydney.edu.au).

of great importance to get to know such cyber-attacks, detect them, and develop effective preventive measures. This is

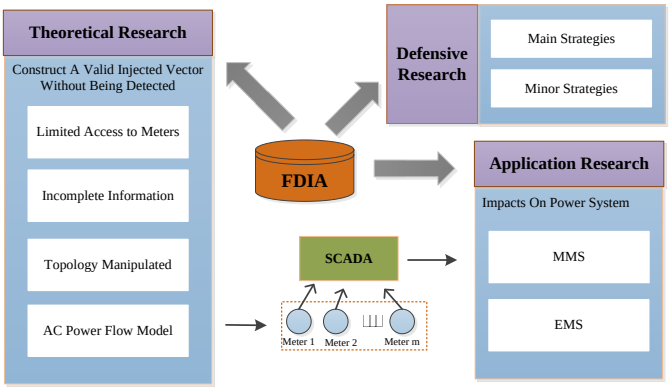

Fig. 2. The Main Research Directions of FDIAs

especially true for the future grid where the physical power system will be deeply integrated with the cyber system.

False data injection attacks (FDIAs) are an important type of cyber-attack capable of disturbing the power system state estimation process. A successful FDIA can cause the state estimator to output erroneous values to the system operator, and thus make either physical or economic impacts on the power system. As depicted in Fig.2, research on FDIAs mainly focuses on the following three aspects: theoretical research, application research, and defensive research. In theoretical research, the key problem is the construction of injected vectors capable of evading detection by the control center under different situations, for example, when the attacker has limited access to meters, incomplete information, false topology, or an AC power flow model is used; the attacker then injects bad data into meters. In application research, the key problem is to analyze the impacts of FDIAs on power system operation, mainly on EMS and MMS (market management systems), for instance, economic dispatch, congestion managements, etc. In defensive research, the key problem is proposing defense strategies from the viewpoint of the system operator.

This paper gives a comprehensive review of the state-of-the-art research in the field of FDIAs against power systems. The existing works can be categorized as shown in Table I. Based on this, this paper is organized as follows: Section II gives some basic theoretical background on state estimation and FDIAs; Section III summarizes the different strategies of constructing a valid FDIA; Section IV discusses the impacts of FDIAs on power systems; Section V summarizes the existing defence strategies against FDIAs; Section VI discusses some potential future research directions in this field. Finally, conclusions are drawn in Section VII.

II. Introduction to False Data Injection Attacks

In an FDIA, the attacker aims to inject malicious measurements to mislead the state estimation process [9]. An attacker can also exploit the small measurement errors which are typically tolerated by the state estimation algorithms to further increase the impact of FDIAs on the power system [10].

In this section, the basic theory of state estimation and bad data detection are first introduced, followed by the FDIAs and generalized FDIAs theories.

TABLE I
Overview of FDIA Researches

FDIA research	Categories	References
Theoretical researches on constructing a valid FDIA	Construct a valid FDIA under certain constraints	[10][12][14][15] [16][17]
	Construct a valid FDIA with incomplete information of matrix	[18][19][20][21]
	Construct a valid FDIA with topology being falsified	[22][28][30]
	Construct a valid FDIA under AC power flow model	[23][24][25]
Application researches on the impacts of FDIAs	Economic attack	[26][27][28][29] [30]
	Load redistribution attack	[31][32]
	Energy deceiving attack	[33]
Defense strategies against FDIAs	Protect a set of basic measurements	[10][14][34][35]
	PMU-based protection	[36][37][38][39]
	Other ways of defending against FDIAs	[40][41][42][43] [44][45][46]

A. State Estimation and Bad Data Detection Theory

1) State Estimation

The basic principle of state estimation is to infer the operational state of the power system from available measurements of the power network equipped with various meters [10]. Meter measurements include bus voltages, bus real and reactive power injections, and branch real and reactive power flows in each subsystem of the grid [10].

The AC-based state estimation model can be formulated as:

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

where the vector $z = (z_1, z_2, ..., z_m)^T$ denotes the measurement data; $x = (x_1, x_2, ..., x_n)^T$ denotes the system states; $e = (e_1, e_2, ..., e_m)^T$ denotes measurement noise, here assumed to be Gaussian distributed, and $h(x)$ denotes the functional dependency between measurements and state variables. The precise form of $h(x)$ is determined by the grid structure and line parameters.

Model (1) is commonly solved by the weighted least squares method. In this method, the vector of estimated state variables $\hat{x}$ is obtained by solving the following optimization problem:

$$\min \quad J(x) = \frac{1}{2}(z - h(x))^T W (z - h(x)) \tag{2}$$

where W is a diagonal matrix represented as $W = diag(\sigma_i^{-2}, 0)$, where σ_i^2 is the variance of the measurement errors associated with the i-th meter ($1 \le i \le m$).

Iterative algorithms can be applied to solve model (2). Since solving the iterative AC-based state estimation problem can be computationally intensive, a DC-based state estimation model can be used to approximate the AC model as follows:

$$z = Hx + e \tag{3}$$

where the vectors $z=(z_1,z_2,...,z_m)^T$, $x=(x_1,x_2,...,x_n)^T$, and $e=(e_1,e_2,...,e_m)^T$ have the same meaning as those in model (1). In (3), H is a constant $m\times n$ Jacobian matrix determined by the grid structure and line parameters.

The DC-based state estimation model can also be solved by the weighted least squares method:

$$\min \quad J(x)=(z-Hx)^T W(z-Hx) \tag{4}$$

where now the solution can be computed in closed-form:

$$\hat{x}=(H^TWH)^{-1}H^TWz \tag{5}$$

2) Bad Data Detection

Bad data detection aims to detect, identify and eliminate measurement errors throughout the system [12], [13]. In power systems, bad data can be detected by two testing hypothesis: the *largest normalized residual* (LNR) and the $J(\hat{x})$ *performance index* [12]. To achieve this, the chi-square test and $J(\hat{x})$ test can be applied:

$$J(\hat{x})<C \tag{6}$$

where $J(\hat{x})$ assumed to follow a chi-square distribution, with threshold C set to some pre-determined significance level.

With the DC model, when $W=I$, the traditional bad data detection approaches often compute the square of the 2-norm of the measurement residual to check whether there exist bad measurements [10]. In this case, $\varepsilon=C$.That is:

$$\left\|z-H\hat{x}\right\|^2<\varepsilon \tag{7}$$

For notational simplicity in the remainder of this paper, the notation LNR will be used to denote the measurement residual, where $LNR=\left\|z-H\hat{x}\right\|$.

B. FDIAs and Generalized FDIAs

In FDIAs, an attacker can compromise the integrity of the state estimator by hacking a subset of meters and sending altered readings without changing the value of LNR [10]. To achieve this, the attacker needs to carefully design his/her actions to fool the estimator to avoid triggering the alarm. Denoting a as the nonzero injected vector which is injected into the measurement data z, the measurement vector after attack can be represented as $z_{bad}=z+a$. Denoting c as the deviation vector of the estimated state variables before and after the attack, the estimated system state vector after attack can be represented as $\hat{x}_{bad}=\hat{x}+c$.

With the DC model, the estimated state variables after FDIAs are as follows:

$$\begin{aligned}\hat{x}_{bad}&=(H^TWH)^{-1}H^TWz_{bad}\\&=(H^TWH)^{-1}H^TW(z+a)\\&=\hat{x}+(H^TWH)^{-1}H^TWa\\&=\hat{x}+c\end{aligned} \tag{8}$$

and the new LNR value can be computed as:

$$\begin{aligned}LNR_{bad}&=\left\|z_{bad}-H\hat{x}_{bad}\right\|\\&=\left\|z+a-H(\hat{x}+(H^TWH)^{-1}H^TWa)\right\|\\&=\left\|z-H\hat{x}+(a-H(H^TWH)^{-1}H^TWa)\right\|\\&=\left\|z-H\hat{x}+(a-Hc)\right\|\end{aligned} \tag{9}$$

If $a=Hc$, then $LNR_{bad}=LNR$, i.e., the attacker can inject bad data into meter measurements whilst keep the measurement residual unchanged. This type of attack is called a *FDIA*. It is noteworthy that the injected vector a can also be obtained without explicitly requiring c. In [10], it is shown that the relationship $a=Hc$ can be transformed into an equivalent form without explicitly using c, and from which a can be generated.

If $a\neq Hc$ but $J(\hat{x}_{bad})<C$, then the attacker can still bypass bad data detection. This type of attack is called a *generalized FDIA*. In a generalized FDIA, the attacker can evade bad data detection by exploiting small measurement errors tolerated by the state estimation algorithms. Both FDIA and generalized FDIA are capable of degrading the economic efficiency and security of the power grid.

III. CONSTRUCTING A VALID FDIA

Theoretically, if an attacker is capable of gaining knowledge of all system configuration information (i.e., grid topology information, system parameters, details of the state estimation algorithm and bad data detection method, etc.) and has the ability to manipulate all meter measurements, it is conceptually straightforward to launch a successful FDIA by constructing the injected vector directly using $a=Hc$. However, in a practical attack, constructing a valid injected vector is always complicated by less-than-perfect system information and constraints, which we now consider. In this section, we summarize four main scenarios, in which the attacker constructs a valid FDIA.

A. Constructing a Valid FDIA under Certain Constraints

When constructing a valid FDIA under certain constraints, it is assumed that the attacker has full knowledge of all relevant system configuration information, (i.e., the Jacobian matrix H is known to the attacker), but he has limited ability to hack into meters.

In this case, the attacker can only access some specific measurements due to different physical protection of the meters. For example, meters located in substations with physical perimeter control might be much more difficult to access than those located in a locked box outside of a building [10].

In this case, it is assumed that the attacker has the ability to compromise at most k out of a possible m meters [14] in constructing the attack vector a, but that the particular meter set is free to be selected by the attacker. If the attacker uses a brute-force approach, i.e., the attacker may try all possible a consisting of k unknown elements and $m-k$ zero elements, then the worst case is to try C_m^k times. This is clearly computationally intractable for large m. To solve the meter selection problem in a feasible time scale, Liu *et al.* [12] proposed a

heuristic-based approach based on column transformations of H. The approach is potentially slow for general H, but efficient when H is sparse, as is typical in practical power systems. Limitations of the approach in [10] are that it cannot guarantee the construction of a even if it exists; and also that it cannot guarantee the construction of a with the minimum possible number of nonzero elements [10].

The limited access to meter problem leads to a subset of researches on FDIAs: constructing a valid FDIA by minimizing the number of attacked meters.

For the attacker, minimizing the number of attacked meters can significantly reduce the risk and cost of an attack. For defenders, knowing the minimum attacked meter number of the attacker is helpful in identifying vulnerable measurements [15]. The objective of attacked meter minimization problem can be formulated as:

$$\alpha_k = \min_c \|Hc\|_0 \tag{10}$$

where α_k denotes the minimum objective value; $\|\cdot\|_0$ denotes the cardinality of a vector. The constraints to this optimization problem vary according to different requests.

The problem is known to be NP-hard for arbitrary H, but is often solved using the mixed-integer linear programming (MILP) method [15], matching pursuit [16], or LASSO algorithm [17]. Exploiting the fact that H exhibits special structure in power systems (i.e., H is a sparse matrix on account of physical topology and measurement structure), Sou *et al.* [15] proposed a min-cut polynomial time algorithm which is shown to be as accurate as MILP yet faster than either matching pursuit or LASSO.

B. Constructing a Valid FDIA with Incomplete Information of matrix H

Most research on FDIAs is based on the assumption that the attacker knows the complete configuration information of the power network. This assumption implies that if the attacker has no access to the grid configuration, it would be infeasible to launch a successful attack. However, research has established that it is still possible for an attacker to launch a valid attack with incomplete information. The following three scenarios show the different situations under which the attackers can obtain the topology information needed to launch a valid FDIA.

1) By Collecting Offline and Online data

Rahman and Mohsenian-Rad [18] proved that H can be estimated by collecting both offline and online data. For offline data collection, the attacker collects grid topology information manually (e.g. utilizing company employees to get access to such information) before performing the actual attack; for the online data collection, the attacker deploys his/her own meters to access the grid.

2) By Using Market Data

Under the DC model, locational marginal prices (LMPs) correspond to the Lagrange multipliers of the network-constrained economic dispatch problem. The topology related information can be extracted from the LMPs components. Kekatos *et al.* [19] proposed an iterative alternating direction method of multipliers (ADMM) based algorithm to estimate the grid Laplacian matrix from the LMPs using a regularized maximum likelihood estimator (MLE). In [19], the authors solve the problem using an ADMM-based algorithm and demonstrated that the estimated Laplacian matrix is close to the real one.

3) By Utilizing Power Flow Measurements

The idea of speculating the matrix H from power flow measurements to launch an attack is based on the observation that when the system parameters (e.g. active or passive loads) vary within a small range, topology information is in fact embedded into the correlations among power flow measurements [20]. Esmalifalak *et al.* [20] proposed an Independent Component Analysis (ICA) algorithm to obtain this information.

However, due to limited resources and restricted physical access to the grid, the estimated H may be inaccurate, deviating from the true one. Denoting the attacker's estimate of H as $\overline{H} = H + \delta$ (where δ is an $m \times n$ error matrix), then,

$$a = \overline{H}c = Hc + \delta c \tag{11}$$

From Eq. (9), it follows:

$$\begin{aligned} \hat{x}_{bad} &= x + \bar{c} \\ &= \hat{x} + c + (H^T W H)^{-1} H^T W \delta c \end{aligned} \tag{12}$$

and hence,

$$\begin{aligned} LNR_{bad} &= \|z_{bad} - H\hat{x}_{bad}\| \\ &= \|z + a - H(\hat{x} + \bar{c})\| \\ &= \|z - H\hat{x} + \delta c + H(c - \bar{c})\| \\ &= \|z - H\hat{x} + (I - H(H^T W H)^{-1} H^T W)\delta c\| \end{aligned} \tag{13}$$

Eq. (13) shows that the residual test results depend not only on the attacker's modeling error δ, but also some grid-specific parameters (i.e., H and W).

Therefore, if $\delta c = 0$, $LNR_{bad} = LNR$. In this case, the attacker can launch a perfect attack even if the attacker's knowledge about matrix H is inaccurate. Furthermore, if $\delta c \neq 0$, the attacker can use a generalized FDIA, to minimize $\|\delta c\|$ and thereby satisfying the threshold test $J(\hat{x}_{bad}) < C$.

Moreover, instead of trying concentrate on getting to know the whole network information, Liu *et al.* [21] showed that an attacker can launch a valid FDIA in a local region. In [21] it is shown that an attacker only needs to obtain the topology and parameter information of the local attacking region to design the false data. Moreover, it is unnecessary for the attacker to know any network information regarding the non-attacked region [21].

C. Constructing a Valid FDIA with Topology being Falsified

Research integrating a topology attack with FDIA has appeared only very recently. In this type of attack, it is assumed that not only can continuous data (meter measurements) be manipulated by the attacker, but also that discrete data (on-off status of switching devices, reflecting the topology of the power network) can be tampered with. In order to evade being detected by both bad data detection and topology error identification, the attacker needs to simultaneously modify continuous data and discrete data to launch such an attack.

Denoting $\bar{H}$ as the false topology matrix being used by the state estimation, in absence of FDIA, model (3) becomes:

$$\bar{z} = \bar{H}x + \bar{e} \tag{14}$$

where the vectors $\bar{z} = (\bar{z}_1, \bar{z}_2, ..., \bar{z}_r)^T$, $x = (x_1, x_2, ..., x_n)^T$, and $\bar{e} = (\bar{e}_1, \bar{e}_2, ..., \bar{e}_r)^T$ have the same meaning as those in model (1).

In the presence of FDIA, denoting $\bar{z}_{bad} = \bar{z} + a$ as the meter measurements after attack, the objective of the attacker is still to construct a valid injected vector a satisfying $J(\hat{x}_{bad}) < C$.

Kim and Tong [22] were among the first to study this problem. They made theoretical and instance analysis based on DC and AC model considering that the system states stay the same before and after the topology information has been falsified.

D. Constructing a Valid FDIA under AC Power Flow Model

At the present time, there are few published results on AC model-based methods of forming an injected vector that keeps the measurement residual unchanged. With the AC model, it is much more difficult for the attacker to construct an analytical formula of the injected vector a due to the complexity of the nonlinear system. Furthermore, it is impractical to implement DC model based FDIAs in the AC system. Rahman and Mohsenian-Rad [23] have shown that if the attacker implements FDIAs targeted at the DC state estimator but the system operator actually uses the nonlinear state estimator, then the attack will easily be detected.

Rahman and Mohsenian-Rad [23] proved that with the AC model, if $a = h(\hat{x}_{bad}) - h(\hat{x})$, then:

$$\begin{aligned} LNR_{bad} &= \left\| z_{bad} - h(\hat{x}_{bad}) \right\| \\ &= \left\| z + a - h(\hat{x}_{bad}) + h(\hat{x}) - h(\hat{x}) \right\| \\ &= \left\| z - h(\hat{x}) + a - h(\hat{x}_{bad}) + h(\hat{x}) \right\| = LNR \end{aligned} \tag{15}$$

In Eq. (21), $h(\hat{x}_{bad}) - h(\bar{x}) = 0$ needs to be satisfied at each iteration. One limitation of model (15) is that convergence of the Gauss–Newton Method cannot be guaranteed, and nor can the exact fixed point $\bar{x}$ be obtained analytically.

Hug and Giampapa [24] proposed that with the AC model, if $a_2 = h_2(\hat{x}_1, \hat{x}_2 + c) - h_2(\hat{x}_1, \hat{x}_2)$, then:

$$\begin{aligned} LNR_{bad} &= \left\| z_{bad} - h(\hat{x}_{bad}) \right\| \\ &= \left\| z + a - h(\hat{x} + c) \right\| \\ &= \left\| \begin{pmatrix} z_1 \\ z_2 + a_2 \end{pmatrix} - \begin{pmatrix} h_1(\hat{x}_1) \\ h_2(\hat{x}_1, \hat{x}_2 + c) \end{pmatrix} \right\| \\ &= \left\| \begin{pmatrix} z_1 \\ z_2 \end{pmatrix} - \begin{pmatrix} h_1(\hat{x}_1) \\ h_2(\hat{x}_1, \hat{x}_2) \end{pmatrix} \right\| \\ &= \left\| z - h(\hat{x}) \right\| = LNR \end{aligned} \tag{16}$$

where variables with the subscript '1' correspond to the measurements and state variables which are not altered by the attacker; variables with subscript '2' correspond to measurements and state variables that are altered [24]. One limitation of (16) is that this function shows the attacker must also know the estimated values of the state variables that appear in h_2, information about which is not easy to obtain.

Overall, research on false data injection with the AC power flow model is based mainly on generalized FDIAs.

IV. The Impacts of FDIAs on Power System

By launching a valid FDIA, an attacker can either gain economic benefit or disrupt the power system. Recently, some research has been conducted to study the impacts of FDIAs on the electricity market, power system operation, and distributed energy routing, respectively. This section reviews the impact of FDIAs on all three of these aspects.

A. Economic Attack

The economic attack is a type of FDIA proposed by Xie *et al.* [26] and [27] which can affect the operation of the deregulated electricity market.

The electricity market consists of two markets: day-ahead market and real-time market. The specific operation model and settlement method differs according to countries. Xie *et al.* in [26] and [27] analyze the potential for financial misconduct under FDIAs using both ex-ante market and ex-post market, which are the formulations adopted by PJM, ISO New England, in the U.S.

The independent system operator (ISO) in a wholesale electricity market collects data from various market participants. The locational marginal price (LMP) is an index that reflects the electricity price at each node. Based on state estimation obtained via the SCADA system, the ISO calculates the ex-post LMPs using the DC optimal power flow model.

The attacker under the aforementioned electricity market environment makes his/her profit by the following three steps: i) in the ex-ante market, the attacker buys and sells the virtual power P at locations j_1 and j_2 with prices λ_{j1}^{DA} and λ_{j2}^{DA}, respectively; ii) the attacker injects a to manipulate the nodal prices of the ex-post market; iii) in the ex-post market, the attacker sells and buys the virtual power P at j_1 and j_2 with prices λ_{j1} and λ_{j2}, respectively [26]. It can be formulated as:

$$\begin{aligned} \mathrm{Pr}ofit &= (\lambda_{j1} - \lambda_{j1}^{DA})P + (\lambda_{j2}^{DA} - \lambda_{j2})P \\ &= (\lambda_{j1} - \lambda_{j2} + \lambda_{j2}^{DA} - \lambda_{j1}^{DA})P \end{aligned} \tag{17}$$

The objective of an attacker in attacking the electricity market is to gain financial profit. In an economic attack, the attacker intends to buy virtual power at the lower priced node and sells at the higher priced node. Nevertheless, in this case, the attacker cannot always guarantee the non-negativity of the profit. References [26] and [27] develop a heuristic-based method for the attacker to improve the attack efficiency.

Furthermore, since the calculation of real-time LMPs is based on both real-time measurements of meters and on-off status of switching devices, some researchers have studied the impacts of integrated generalized FDIA and topology attacks (see Section. III) on LMPs. Jia *et al.* in [28] proposed serval ways to calculate the injected vector a on the purpose of causing congestion pattern which affect the LMP most. Choi and Xie in [29] studied the impacts of topology errors on LMPs. Since the LMP is a by-product of OPF, Rahman *et al*. in [30] described a formal verification-based framework to systematically analyse the

impact of topology attacks on the integrity of OPF and economic operation.

B. Load Redistribution Attack

The load redistribution (LR) attack is a type of FDIA proposed by Yuan *et al.* [31] which can affect the power grid operation by attacking the security-constrained economic dispatch (SCED).

In [31], the authors analyzed the damage of the LR attack on power systems and classified it into the immediate attack and delayed attack, based on the different attacking consequences.

The objective of SCED is to minimize the total system operation cost (generation cost, load shedding cost, etc.) by re-dispatching the generation outputs [31]. Once the estimated state is manipulated by an LR attack, the falsified SCED solution may drive the system to an uneconomic operating state. In a worst-case situation, this could lead to immediate load shedding or even wider load shedding in a delayed time without immediate corrective actions [31], [32]. In [31] and [32], the authors propose a bi-level model and tri-level model to model the immediate LR attack and delayed attack, respectively.

The main attacking processed is as follows. In the immediate attack, the attacker determines the injected vector and injects it into the targeted meters to maximize the operation cost of the system; the system operator then optimally reacts to the false state estimation that has been successfully manipulated by the injected vector. As a consequence of a successful immediate attack, the actual operation cost will increase no matter whether there is load shedding action or not.

In the delayed attack, the attacker determines the injected vector and injects it into the targeted meters; the control center performs the first round of SCED function based on the false state estimation, which would lead to the occurrence of the line overloading without being noticed; the control center then performs the second round of SCED after the tripping of the overload lines. A successful delayed attack results in line overloading undetected by the control center, which can lead to physical damage to the power system.

C. Energy Deceiving Attack

The energy deceiving attack is a type of FDIA proposed by Lin *et al.* [33], which affects the distributed energy routing process.

In [33], the authors proposed a distributed energy routing scheme which determines the optimal energy route for transmitting energy among the nodes of the grid. It is assumed that each node can act both as the energy consumer and producer. The measuring component at the node (e.g., smart meter) determines whether the node is a producer-node or consumer-node. The nodes communicate with each other to share the measurements, demands, and requests. In the energy deceiving attack, the attacker is assumed to be capable of injecting either the forged energy information or forged link state information into the energy request and response message among nodes [33]. Once the memory of a measuring component is manipulated by the attacker, erroneous energy demand and supply messages can be injected into the grid.

Based on the proposed scheme, the authors studied the energy deceiving attack that manipulated the quantity of energy supply, the quantity of energy response, and the link state information of the energy transmission, respectively. It is concluded in [33] that the energy deceiving attack can create an imbalance between power demand and supply, and can therefore further increase the cost of the energy distribution and disrupt the effectiveness of the energy distribution process.

V. Defense Strategies against FDIAs

As FDIAs can severely threaten the economic and physical securities of the power system, it is important for the system operator to design proper defensive measures to protect the power grid. In this section, two main defense strategies and many other strategies against FDIAs are introduced.

A. Protecting a set of Basic Measurements

A set of basic measurements is a minimum set of measurements whose corresponding rows in H are linearly independent and sufficient to solve for the corresponding state variables.

Liu *et al.* [10] demonstrated that if an attacker can compromise k meter measurements, where $k \geq m-n+1$, there always exist successful attack vectors that can inject false data without being detected. On the other hand, if the number of the meters that the attacker can manipulate is less than $m-n+1$, the attack will then be detected. Therefore, the size of the basic measurements based on DC state estimation model is n, the number of state variables. Bobba *et al.* [14] proved that it is necessary and sufficient to protect a set of basic measurements in order to be able to detect FDIAs.

This problem leads to another research direction on defences against FDIAs: how to locate and protect the set of basic measurements. Bi and Zhang [34] considered the location of protected meter problem using graphical methods. Anwar *et al.* [35] expanded the FDIA problem from the power transmission system to power distribution systems, and utilized a voltage stability index and improved constriction factor particle swarm optimization (CF-PSO) based hybrid cluster technique to rank each node according to vulnerability, from most- to least-vulnerable. The meter measurements on the node belonging to the least vulnerable group that needs to be protected are then located. In respect to the ways of protecting basic measurements, methods range from simple physical security (e.g. locking each meter in a box) through enhance communication security, to replacing meters with PMUs [36], etc.

B. PMU-based Protection

Phasor measurement units (PMUs) are measurement devices equipped with the global positioning system (GPS) technology for precise timing. By synchronizing to GPS time, PMUs have the capability of providing accurate synchronous phasor measurements for geographically dispersed nodes in power grids [36]. It is much more difficult for an attacker to compromise the measurements which are collected by the PMUs. However, a major impediment to large-scale deployment of PMUs is their high capital cost. Therefore, it is important to find the best locations to place PMUs so that the number of PMUs can be minimized.

Chen and Abur [37] proposed a PMU placement algorithm, formulating it as an integer programming problem. They showed that extra PMUs can help improve the bad data detection and identification capability of a given system [37]. Similarly, Kim and Poor [36] also proposed a secure PMU placement algorithm to find the appropriate locations for these PMUs. The proposed algorithm has low complexity and is capable of handling different types of PMU measurements. In [36] it is shown it may become infeasible for an attacker to inject bad data without changing the measurement residual if approximately 1/3 of the buses are protected with PMUs.

References [36] and [37] show that by placing PMUs, the power system can effectively protect itself. However, Gong *et al.* [38] proposed a time stamp attack by spoofing the GPS. By sending a forged signal to the GPS receiver, attackers can mount an attack even without access to the communication network. This attack scheme can lead to the failure of the basic application of PMU system [38]. Liu *et al*. [39] also demonstrated that an attacker can mask the outage of a single line by attacking a set of critical measurements, even though PMUs are deployed in the system.

C. Other Defense Strategies against FDIAs

Several other methods have been proposed to defend against FDIAs. Based on the fact that the network topology information is a key prior knowledge for the attacker, Talebi *et al*. [40] proposed a defense strategy against FDIAs by dynamically changing the information structure of micro-grids. Huang *et al*. [41] proposed an adaptive CUSUM algorithm to defend against FDIA in a smart grid. Zhu *et al*. [42] proposed an interleaved hop-by-hop authentication scheme to help the base station detect injected false data packets. Liu *et al*. [43] consider the detection problem as a matrix separation problem, and proposed nuclear norm minimization method and low rank matrix factorization approach. Li *et al*. [44] considered the online detection of FDIA by using a sequential detector based on the generalized likelihood ratio. Chaojun *et al*. [45] proposed a Kullback-Leibler distance (KLD) based method by tracking the dynamics of measurement variations to detect FDIAs under the AC state estimation model. Liu *et al*. [46] expanded meters from the power side to the user side, and proposed an intrusion detection mechanism that can achieve collaborative detection of FDIA by setting spying domain randomly in physical memory in combination with using secret information and event log.

VI. Future Research Directions

Based on existing research, the following areas of research are suggested in the field of FDIAs against the power system:

(1) AC model-based FDIAs for future power system problems need to be more comprehensively studied. Despite the considerable research on DC model-based FDIAs, practical power systems operate under the conditions of the AC model. It would therefore be beneficial to power system operators if the characteristics of AC model-based FDIAs were more intensively studied. For instance, to better understand: i) nonlinear rules for constructing a valid FDIA when the attacker has some states or measurements as predetermined targets; ii) the influence of AC model based FDIAs on system control operation and system stability; and iii) the vulnerability assessment of the practical power system when FDIAs combine with other kinds of cyber-attacks.

(2) For enhancing security defense mechanisms, more work is required to focus on the higher-level security algorithm or structure. As the state estimator may not filter bad data using the existing bad data detection method in the presence of FDIAs, higher-level security algorithms or structures are required. For example, in addition to the existing bad data detection process, if the SCADA system has some other modules which are specially used to detect the false data using a new regulation, it would be much more difficult for any kind of attacks to success.

(3) For enriching the impact analysis of FDIA, more work is required to focus on the distribution system and user side. Besides transmission system, distribution system can also be influenced by using false meter measurements and fake topology information. On the other hand, meters deployed in the user side that transfer user's power consumption and utility company's command can also be manipulated. Therefore, the security of load management and demand side management should draw more attention in the future.

VII. Conclusions

The cyber physical system security of modern power system is of utmost importance for the future grid. Recent research reveals that modern power systems face severe threats from cyber-attacks due to the tight integration of physical and cyber systems. False data injection attacks are an important type of cyber-attack which can disrupt the underlying control system of the electric power grid.

This paper provides a comprehensive review of the state-of-the-art research in the field of FDIAs against modern power systems. Firstly, the theoretical basis of state estimation, bad data detection, FDIAs and generalized FDIAs are introduced. Secondly, in the theoretical research of FDIAs, four main scenarios for constructing valid FDIAs are discussed. Following this, the paper discusses the impacts of FDIAs on different aspects of the power grid operation. Then, two common defense strategies together with many other defense strategies are summarized. This paper also ventures potential research directions in the field. These directions are principally based on extending the framework of FDIAs and defenses to the considerably more challenging case of AC power system models, distribution system, and user side.

References

[1] T. Baumeister, "Literature review on smart grid cyber security," *University of Hawaii at Manoa, Tech. Rep*, 2010.

[2] G.N. Sorebo and M.C. Echols, *Smart Grid Security: An End-to-End View of Security in the New Electrical Grid*, CRC Press, Boca Raton, Florida, 2011.

[3] A.J. Wood and B.F. Wollenberg, *Power Generation, Operation, and Control*, John Wiley & Sons, 2012.

[4] S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber–physical system security for the electric power grid," *Proc. IEEE*, vol. 100, no. 1, pp. 210-224, Jan. 2012.

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

[6] O. Kosut, L. Jia, R.J. Thomas, and L. Tong, "Malicious data attacks on the smart grid," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 645-658, Dec. 2011.

[7] Cybersecurity for Industrial Automation & Control Environments, [Online]. Available: http://www2.schneider-electric.com/documents/support/white-papers/white-paper-cybersecurity-for-industrial-automation-control.pdf

[8] Introduction of State Estimation [Online]. Available: http://home.eng.iastate.edu/~jdm/ee553/SE1.pdf

[9] Q. Yang, J. Yang, W. Yu, D. An, N. Zhang, and W. Zhao, "On false data-injection attacks against power system state estimation: Modeling and countermeasures," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 3, pp. 717-729, Mar. 2014.

[10] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Transactions on Information and System Security (TISSEC)*, vol. 14, no.1, May. 2011.

[11] B.M. Horowitz and K.M. Pierce, "The integration of diversely redundant designs, dynamic system models, and state estimation technology to the cyber security of physical systems," *Systems Engineering*, vol. 16, no. 4, pp. 401-412, Jan. 2013.

[12] M. Giannini, "Improving cyber-security of power system state estimators," Master's Thesis, KTH, Stockholm, Sweden, Feb. 2014.

[13] Y. Huang, M. Esmalifalak, H. Nguyen, R. Zheng, Z. Han, H. Li, and L. Song, "Bad data injection in smart grid: attack and defense mechanisms," *IEEE Commun. Mag.*, vol. 51, no. 1, pp. 27-33, Jan. 2013.

[14] 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 *Preprints of the First Workshop on Secure Control Systems, CPSWEEK*, 2010.

[15] K.C. Sou, H. Sandberg, and K.H. Johansson, "Electric power network security analysis via minimum cut relaxation," in *IEEE 50th Conference on Decision and Control and European Control Conference (CDC-ECC)*, pp. 4054-4059, Dec. 2011.

[16] S.G. Mallat and Z. Zhang, "Matching pursuit with time-frequency dictionaries, " *IEEE Trans. Signal Process*, vol. 41, no. 12, pp. 3397–3415, Dec. 1993.

[17] R. Tibshirani, "Regression shrinkage and selection via the lasso, " *J. Roy. Stat. Soc. B.*, vol. 58, no. 1, pp. 267–288, 1996.

[18] M.A. Rahman and H. Mohsenian-Rad, "False data injection attacks with incomplete information against smart power grids," in *IEEE Global Communications Conference (GLOBECOM)*, pp. 3153-3158, 2012.

[19] V. Kekatos, G.B. Giannakis, and R. Baldick, "Grid topology identification using electricity prices," in *Proc. IEEE Power and Energy Society General Meeting*, pp. 1–5, National Harbor, MD, 27–31 July 2014.

[20] M. Esmalifalak, H. Nguyen, R. Zheng, and Z. Han, "Stealth false data injection using independent component analysis in smart grid," in *IEEE International Conference on Smart Grid Communications (SmartGridComm)*, pp. 244-248, Brussels, Belgium, 17–20 Oct. 2011.

[21] X. Liu, Z. Bao, D. Lu, and Z. Li, "Modeling of local false data injection attacks with reduced network information," *IEEE Trans. Smart Grid*, vol. 6, no.4, pp. 1686-1696, July. 2015.

[22] J. Kim and L. Tong. "On topology attack of a smart grid: Undetectable attacks and countermeasures," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 7, pp. 1294–1305, July 2013.

[23] M. Rahman and H. Mohsenian-Rad, "False data injection attacks against nonlinear state estimation in smart power grids," in *Proc. IEEE Power and Energy Society General Meeting*, pp. 1–5, Vancouver, Canada, 21–25 July 2013.

[24] G. Hug and J. A. Giampapa, "Vulnerability assessment of AC state estimation with respect to false data injection cyber-attacks," *IEEE Trans. Smart Grid*, vol. 3, no. 3, pp. 1362-1370, Sep. 2012.

[25] L. Jia, R.J. Thomas, and L. Tong, "On the nonlinearity effects on malicious data attack on power system," in *Proc. IEEE Power and Energy Society General Meeting*, pp. 1-8, San Diego, CA, 22–26 July 2012.

[26] L. Xie, Y. Mo, and B. Sinopoli, "False data injection attacks in electricity markets," in *IEEE International Conference on Smart Grid Communications (SmartGridComm)*, pp. 226-231, 2010.

[27] L. Xie, Y. Mo, and B. Sinopoli, "Integrity data attacks in power market operations," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 659-666, Dec. 2011.

[28] L. Jia, J. Kim, R.J. Thomas and L. Tong. "Impact of data quality on real-time locational marginal price." *IEEE Trans. Power Syst.*, vo. 29, no. 2, pp. 627-636, Mar. 2014.

[29] D.H. Choi and L. Xie. "Impact analysis of locational marginal price subject to power system topology errors," in *IEEE International Conference on Smart Grid Communications (SmartGridComm)*, 2013.

[30] M.A. Rahman, E. Al-Shaer, and R. Kavasseri. "Impact analysis of topology poisoning attacks on economic operation of the smart power grid," in *IEEE 34th International Conference on Distributed Computing Systems*, 2014.

[31] Y. Yuan, Z. Li, and K. Ren, "Modeling load redistribution attacks in power systems," *IEEE Trans. Smart Grid*, vol. 2, no.2, pp. 382-390, Jun. 2011.

[32] Y. Yuan, Z. Li, and K. Ren, "Quantitative analysis of load redistribution attacks in power systems," *IEEE Trans. Parallel Distrib. Syst.*, vol. 23, no. 9, pp. 1731–1738, Sep. 2012.

[33] J. Lin, W. Yu, X. Yang, G. Xu, and W. Zhao, "On false data injection attacks against distributed energy routing in smart grid," in *IEEE/ACM Third Int. Conf. on Cyber-Physical Systems (ICCPS)*, pp. 183-192, 2012.

[34] S. Bi and Y.J. Zhang. "Graphical methods for defense against false-data injection attacks on power system state estimation," *IEEE Trans. Smart Grid*, vol. 5, no. 3, pp. 1216–1227, May 2014.

[35] A. Anwar, A.N. Mahmood, and Z. Tari. "Identification of vulnerable node clusters against false data injection attack in an AMI based Smart Grid." *Information Systems*, vol. 53, pp. 201–212, Oct.-Nov. 2015.

[36] 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, Jun. 2011.

[37] J. Chen and A. Abur, "Placement of PMUs to enable bad data detection in state estimation," *IEEE Trans. Power Syst.*, vol. 21, no. 4, pp. 1608-1615, Nov. 2006.

[38] S. Gong, Z. Zhang, H. Li, and A.D. Dimitrovski, "Time stamp attack in smart grid: Physical mechanism and damage analysis," preprint: http://arxiv.org/abs/1201.2578, Jan. 2012.

[39] X. Liu, Z. Li and Z. Li, "Impacts of bad data on the PMU based line outage detection." Preprint: http://arxiv.org/abs/1502.04236, 2015.

[40] M. Talebi, C. Li, and Z. Qu, "Enhanced protection against false data injection by dynamically changing information structure of microgrids," in *IEEE 7th Sensor Array and Multichannel Signal Processing Workshop (SAM)*, pp. 393-396, 2012.

[41] Y. Huang, H. Li, K.A. Campbell, and Z. Han, "Defending false data injection attack on smart grid network using adaptive CUSUM test," in *IEEE 45th Annual Conference on Information Sciences and Systems (CISS)*, pp. 1-6, 2011.

[42] S. Zhu, S. Setia, S. Jajodia, and P. Ning, "An interleaved hop-by-hop authentication scheme for filtering of injected false data in sensor networks," *Proc. IEEE Symposium on Security and Privacy*, Oakland, CA, pp. 259–271, May. 2004.

[43] L. Liu, M. Esmalifalak, Q. Ding, V.A. Emesih, and Z. Han "Detecting false data injection attacks on power grid by sparse optimization." *IEEE Trans. Smart Grid*, vol. 5, no. 2, pp. 612-621, Mar. 2014.

[44] S. Li, Sinan, Y. Yilmaz, and X. Wang. "Quickest detection of false data injection attack in wide-area smart grids," *IEEE Trans. Smart Grid* 2014.

[45] G. Chaojun, P. Jirutitijaroen, and M. Motani. "Detecting false data injection attacks in AC state estimation," *IEEE Trans. Smart Grid*, 2015.

[46] X. Liu, P. Zhu, Y. Zhang and K. Chen "A collaborative intrusion detection mechanism against false data injection attack in advanced metering infrastructure," *IEEE Trans. Smart Grid*, 2015.

Gaoqi Liang (M'13) obtained the B.S. degrees in automation from the North China Electric Power University, Baoding, China, in 2012. She is currently towards her Ph.D. degree in electrical engineering from the University of Newcastle, Australia. Her research interests include cyber physical system, power system security, and electricity market.

Junhua Zhao (M'07) received his Ph.D. degree from the University of Queensland, Australia. Currently he is a senior lecturer at the University of

Newcastle, Australia. His research interests include power system analysis and computation, smart grid, cyber physical system, electricity market, data mining and its applications.

Fengji Luo (M'13) obtained the B.S. and M.S. degrees in software engineering from Chongqing University, Chongqing, China, in 2006 and 2009, respectively. He received the Ph.D. degree in electrical engineering from the University of Newcastle, Australia, in 2013. Currently, he is the research associate of the Centre for Intelligent Electricity Networks, Australia. His research interests include demand side management, computational intelligence applications, distributed computing, and power system operation & planning.

Steven R. Weller (S'88–M'94) received the B.E. (Hons.I.) degree in computer engineering in 1988, the M.E. degree in electrical engineering in 1992, and the Ph.D. degree in electrical engineering in 1994, all from the University of Newcastle, Australia. During 1994–1997, he was a Lecturer in the Department of Electrical and Electronic Engineering, University of Melbourne, Australia. In 1997, he joined the University of Newcastle, where he is currently an Associate Professor and Deputy Head of Faculty, Engineering, and Built Environment. His research interests lie in the areas of control theory and its application to energy systems and climate. Dr. Weller was the recipient of the IET Control Theory and Applications Premium Award.

Zhao Yang Dong (M'99–SM'06) obtained his Ph.D. degree from the University of Sydney, Australia in 1999, where he is now Professor and Head of the School of Electrical and Information Engineering. He is immediate Ausgrid Chair Professor and Director of the Centre for Intelligent Electricity Networks (CIEN), University of Newcastle, Australia. He also held academic and industrial positions with the Hong Kong Polytechnic University, the University of Queensland, Australia and Transend Networks, Tasmania, Australia. His research interest includes Smart Grid, power system planning, power system security, load modeling, renewable energy systems, electricity market, and computational intelligence and its application in power engineering. Prof. Dong is an editor of IEEE TRANSACTIONS ON SMART GRID and IEEE POWER ENGINEERING LETTERS.