False Data Injection Attacks against State Estimation in Smart Grids: Challenges and Opportunities

El-Nasser S. Youssef
Electrical and Computer Engineering Department
McGill University
Montréal, Canada
elnasser@ieee.org

Fabrice Labeau
Electrical and Computer Engineering Department
McGill University
Montréal, Canada
fabrice.labeau@mcgill.ca

***Abstract*—Static-State Estimation has been a key function of electric power grids for almost 50 years. During that time, power system engineers have been depending on it to monitor and control power networks, optimize power flow, and perform contingency analysis. State Estimation has always been vulnerable to cyberattacks targeting the availability and integrity of the grid. Nowadays, with the rapid expansion of ICT integration into power systems towards a Smart Grid, this cybersecurity threat is even more pronounced. In order to prepare for the new cybersecurity challenges brought upon by Smart Grids, this paper serves as a concentrated summary of the research on stealth false data injection attacks against Static-State Estimation.**

Keywords—Smart Grid, Cybersecurity, Static State Estimation, Stealth False Data Injection Attacks.

I. Introduction

In power networks, the Supervisory Control and Data Acquisition (SCADA) system gathers two types of meter readings, namely, the real and reactive power injection and power flow measurements, and the status of breakers and switches. The control center of a power grid then uses these readings to carry out Static-State Estimation (SSE) which provides utilities with an update about the current grid state. Without SSE, a power grid would not be observable, and addressing operational issues would not be possible. For the SSE to be valid, measurement inaccuracies have to be kept below a certain level. Gross measurement errors render SSE invalid, as the estimated state would be significantly deviated from the actual one. For this reason, each state estimator is equipped with a Bad Data Detection (BDD) unit whose function is to detect these situations. Because the process of communicating with meters and collecting measurements takes place over ICT networks, it is vulnerable to cyberattacks. In addition, due to SSE's vitality to the grid, it becomes a specially-attractive target for this kind of attacks. Furthermore, over the last decade, researchers have developed a class of malicious cyberattacks, known as stealth false data injection (FDI), which is capable of circumventing conventional BDD while causing significant distortions to the measurements, and thus, ruining SSE. This paper focuses on this class of cyberattacks by surveying the relevant literature. We discuss the different aspects of the subject: the theory, modelling, synthesis, requirements, targets, and detection strategies of stealth FDI attacks against SSE.

This work was supported by Hydro-Quebec, the Natural Sciences and Engineering Research Council of Canada, and McGill University in the framework of the NSERC/Hydro-Quebec Industrial Research Chair in Interactive Information Infrastructure for the Power Grid (IRCPJ406021-14).

The rest of the paper is organized as follows. In section II, an overview of SSE and BDD is given. Section III discusses the different aspects of stealth FDI attacks, and section IV highlights the main research directions in the detection strategies. Finally, the discussion is concluded in section V.

II. Static State Estimation and Bad Data Detection

AC Static State Estimation (SSE) [1], [2] is the process of solving the power flow equations of a power grid to estimate state variables at all grid buses, or nodes, given a number of meter measurements and the electric impedance of each transmission line in the grid. The roles of some state variables and measurements interchange according to the type of a bus. For load buses, meters monitor the injected real and reactive powers. Thus, the state variables in that case are the voltage magnitudes and phase angles. In case of generator buses, the injected real power and voltage magnitude are measured, whereas the injected reactive power and voltage phase angle are estimated [3]. Meters can also be placed on transmission lines to monitor transmitted power so as to provide measurement redundancy, which is used to validate the collected dataset and identify and – possibly – eliminate bad data points. Within the power flow model, Kirchoff's current and voltage laws and the grid's electric admittance matrix govern the nonlinear relationship between measurements and state variables. Let $\mathbf{f}(\mathbf{x}) = [f_1(\mathbf{x}), f_2(\mathbf{x}), \dots, f_m(\mathbf{x})]^T$ denote these nonlinear functions, where $\mathbf{x} = [x_1, x_2, \dots, x_n]^T$ is the vector of state variables. Then, according to the AC power flow model, the measurements vector, $\mathbf{z} = [z_1, z_2, \dots, z_m]^T$, can be expressed as:

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

where m and n are the number of measurements and state variables, respectively, with $m \geq n$ due to measurement redundancy. The vector $\mathbf{e} = [e_1, e_2, \dots, e_m]^T$ is composed of zero-mean, random variables representing the measurement errors. Such errors reflect the combined impact of imperfect meter precision, quantization noise, and communication errors on the accuracy of the collected measurements [1]. Thus, the SCADA system communicates with meters and collects measurements. Then, the control center runs the SSE algorithm to solve (1) and estimate the vector of state variables. This vector, which represents the grid's static-state, is then used to

optimize power flow across generation, transportation, and distribution domains, and to perform contingency analysis in which utilities try to anticipate operational issues and plan corrective measures [4]. However, the AC SSE is a computationally-demanding, iterative process involving an overdetermined system of nonlinear equations which is not guaranteed to converge. Therefore, Schweppe and Rom [2] proposed an approximate linearized model, based on the DC load flow model, that does not require an iterative algorithm to solve. Using a first-order, Taylor expansion of the power flow equations, the so-called DC SSE breaks down the AC SSE into two separate linear regression problems, one relates voltage phase-angles to real power and the other relates voltage magnitudes to reactive power, of the form:

$$\mathbf{z} = \mathbf{H}\mathbf{x} + \mathbf{e}, \tag{2}$$

where the matrix $\mathbf{H}$ carries the information about grid topology and transmission lines' impedances. The DC SSE leverages four principal assumptions: a transmission line impedance is dominated by its reactance, voltage magnitudes at all buses approach unity, phase-angle differences tend to zero, and measurement errors resulting from monitoring real power are uncorrelated with the measurement errors stemming from gauging voltage magnitude and reactive power. Weighted Least Squares (WLS) has been widely used in the context of SSE to solve (2), providing an estimate for the state variables given by:

$$\hat{\mathbf{x}} = [\mathbf{H}^{\boldsymbol{T}}\mathbf{K}^{-\mathbf{1}}\mathbf{H}]^{-\mathbf{1}}\mathbf{H}^{\boldsymbol{T}}\mathbf{K}^{-\mathbf{1}}\mathbf{z} = \mathbf{M}\,\mathbf{z}, \tag{3}$$

where $\mathbf{K}$ is the covariance matrix of the measurement errors, $\mathbf{e}$, and $\mathbf{M} = [\mathbf{H}^{\boldsymbol{T}}\mathbf{K}^{-\mathbf{1}}\mathbf{H}]^{-\mathbf{1}}\mathbf{H}^{\boldsymbol{T}}\mathbf{K}^{-\mathbf{1}}$. After estimating a grid's state, the control center performs BDD to verify it. Bad data points refer to large measurement errors arising from the grid's unexpected operational problems such as meter or communications failures, topology errors, or false data injection attacks [5], [6]. In contrast to the measurement errors modelled in (1), which are expected to introduce a controlled level of inaccuracy to the estimated states, bad data points result in significant deviation from the true states which renders the estimated states unsuitable for contingency analysis. BDD utilizes a statistical hypothesis test using a statistic derived from the measurement residual – defined as: $\mathbf{r} = \mathbf{z} - \mathbf{H}\hat{\mathbf{x}}$. The choice of a specific test statistic depends on the regularization term used to solve (2) and the modeling of the measurement error vector, $\mathbf{e}$ [5]. The earliest, and most commonly-used, test statistic for WLS framework in SSE is the normalized residual [2]. Define $\mathbf{\Sigma}$ as the covariance matrix of the residual, then one can write the normalized residual at the k^{th} measurement as:

$$\Delta_k = \frac{1}{\sqrt{\mathbf{\Sigma}_{kk}}}[\mathbf{z} - \mathbf{H}\hat{\mathbf{x}}]_k; \quad k = 1,2,\dots,m, \tag{4}$$

where $\mathbf{\Sigma}_{kk}$ is the k^{th} entry on the main diagonal of $\mathbf{\Sigma}$, and $[\mathbf{z} - \mathbf{H}\hat{\mathbf{x}}]_k$ is the k^{th} entry in the residual vector. The absolute values of normalized residuals are then compared against thresholds which are determined based on the covariance matrix, $\mathbf{K}$, of the measurement errors, and the desired balance between detection sensitivity and false alarm rate. A value of $|\Delta_k|$ exceeding the threshold indicates the presence of bad data in that k^{th} measurement. If enough measurement redundancy exists for this particular measurement, then it can be removed and the SSE can be repeated yielding a more accurate state. Thus, the level of measurement redundancy available in the system determines the ease of detection, identification, and removal of bad data points. In the next section, we discuss a class of FDI attacks that can circumvent BDD algorithms.

III. Stealth False Data Injection Attacks

FDI attacks occur when an adversary attempts to inject false measurements into the system. Let $\mathbf{a} \in \mathbb{R}^m$ denotes the attack vector, which represents the deviations in true measurements caused by FDI. Thus, the observed measurement vector can be written as: $\mathbf{z}_a = \mathbf{z} + \mathbf{a}$. Plugging $\mathbf{z}_a$ into (3), we obtain the following estimated state and measurement residuals:

$$\hat{\mathbf{x}}_{FDI} = \hat{\mathbf{x}} + \mathbf{M}\,\mathbf{a}, \tag{5}$$

$$\mathbf{r}_{FDI} = \mathbf{z}_a - \mathbf{H}\hat{\mathbf{x}}_{FDI} = \mathbf{r} + (\mathbf{I} - \mathbf{H}\mathbf{M})\,\mathbf{a}. \tag{6}$$

Thus, the FDI attack causes a change in measurement residuals which can be spotted with BDD. However, if an attacker is able to launch an FDI attack that causes little or no change to the measurement residual, then such attack would go unnoticed through conventional BDD algorithms. In the following subsections, we consider the different aspects of this class of FDI attacks, called stealth attacks, by providing a comprehensive survey of the literature on the topic.

A. Perfect versus Imperfect FDI Attacks

Depending on the amount of knowledge an adversary can acquire about the grid prior to launching an attack, stealth FDI attacks can be classified into perfect or imperfect attacks. In perfect FDI attacks, introduced by Y. Liu *et al.* [6], [7], the adversary is assumed to have acquired complete knowledge of the system matrix, $\mathbf{H}$, and thus, is able to create attack vectors that lie in the column space of $\mathbf{H}$. Consider an attack vector of the form $\mathbf{a} = \mathbf{H}\mathbf{c}$. Substituting this expression in (5) and (6) will lead to an erroneous estimated state given by: $\hat{\mathbf{x}}_{FDI} = \hat{\mathbf{x}} + \mathbf{c}$, but to an unchanged residual: $\mathbf{r}_{FDI} = \mathbf{r}$. Thus, if the true measurements, $\mathbf{z}$, would pass the BDD test, so would the false measurements, $\mathbf{z}_a$, as well.

Obtaining real-time, perfect knowledge of the constantly-evolving grid topology is a nontrivial task, and it requires substantial resources on the attacker's part. Therefore, more plausible scenarios prompt the study of imperfect FDI attacks where only partial knowledge of $\mathbf{H}$ is assumed. In these cases, instead of completely avoiding perturbing the measurement residual, attackers use the available incomplete information about $\mathbf{H}$ to launch significant FDI attacks while supressing their impact on the residual – making them harder to detect with conventional BDD. Modeling of imperfect FDI attacks is studied in [8], [9]. In [8], Teixeria *et al.* show that the magnitude of undetectable FDI attacks that attackers can launch against a grid is directly proportional to the accuracy of the grid's model available to them. In addition, they derive conditions on the

attack magnitude under which it is undetectable by BDD schemes. Rahman and Mohsenian-Rad prove in [9] that adversaries still can launch perfect FDI attacks with only partial knowledge of $\mathbf{H}$, given that they have access to complete knowledge of the topology of at least one cut of the grid. A cut is a "set of transmission lines that divides the grid into two disjoint islands" [9]. However, there are constraints on the attack vector that can be launched undetected in this case, so attackers do not have complete freedom to tailor an FDI attack according to their objectives. In addition, the authors study imperfect FDI attacks from the point of view of both attackers and utilities. From attackers' perspective, the authors formulate the task of designing imperfect FDI attacks into a stochastic convex optimization with the objective of maximizing the attack's magnitude while minimizing its impact on the residual. From utilities perspective, the authors propose an analytical measure that estimates the vulnerability of a grid to imperfect FDI attacks which can be used by utilities to improve the resiliency of their networks against cyberattacks of this kind.

B. State versus Topology FDI Attacks

FDI attacks can be further classified – according to which system parameters they target – into state and topology attacks. State FDI attacks take place when adversaries fulfill their objectives by manipulating the state variables [6]–[9]. The manner in which intruders perturb the state variables is determined by their end goals. This fact is highlighted in two, widely-studied, state-attack scenarios: the load-redistribution (LR) attack and the replay attack. In LR attacks [10]–[14], adversaries attempt to falsify individual consumption profiles without changing the aggregated load profile as seen by the utility. They do this by injecting false measurements to make loads appear lower at certain buses – and higher at others – than they really are, so that the total load is unchanged as seen by the network operator. Following the conditions laid out by [6]–[9], attackers can launch perfect or imperfect LR attacks that bypass conventional BDD associated with SSE. However, LR attacks require attackers to have access to more information; not only do attackers need to have – complete or partial -- knowledge of system topology, but also they must have access to state variables in order to be able to keep the aggregated load profile unchanged.

Yuan *et al.* developed the concept of LR attacks and demonstrated its short- and long-term dangers to a power grid in [10]. In addition, they establish an optimization model, from attackers' perspective, to design the LR attack that would inflict the most damage on a utility. The optimization model maximizes the operational costs of the grid under the assumption that the operators will be forced to implement feasible, corrective actions – in an attempt to minimize operational costs – as a consequence of performing contingency analysis using a false SSE of the power network. Moreover, the authors discuss how utilities can use the same optimization model to their advantage by determining the most vulnerable meters that need protection in order to stop this type of attacks. The work in [11] considers a different motive for attackers to launch LR attacks which is to cheat utilities into reducing their electricity bill. The authors of [11] formulate the attack as an optimization problem that minimizes the number of compromised meters while satisfying the constraints of stealth FDI attacks, achieving a certain level of unlawful, financial gain, and keeping the aggregated load profile unaltered. Moreover, they propose an iterative algorithm using graph theory to determine the number and locations of secure grid sensors needed to ensure sufficient network observability and detection of LR attacks.

A number of studies [12]–[14] utilize the concept introduced in [9] to establish models of imperfect LR attacks. X. Liu and Li present an LR attack model in [12] which requires attackers to have access to the topology and state variables only of the boundary buses of an attacked region rather than the whole grid. In [13], the same authors extend their work by further relaxing the conditions on the amount of knowledge required by attackers for a successful attack. Assuming that attackers are able to acquire only the voltage magnitudes of the boundary buses of an attacked region, they propose a method to estimate the voltage phase-angle differences prior to launching an LR attack. Zhao *et al.* study the possibility of using forecasted instead of actual state variables to launch imperfect LR attacks in [14]. The authors derive an expression that demonstrates the trade-off between forecasting error and the achievable magnitudes of undetectable attacks.

Replay attacks are another form of state FDI attacks, which were developed by Mo and Sinopoli in [15]. While this type of attacks does not require the same level of sophistication required in LR attacks, its consequences still could be as catastrophic. In a typical replay attack, attackers seize control of meters in an attacked region, record the readings of these meters over a period of time, and then start broadcasting these readings again in place of the actual, updated measurements. This kind of attacks does not demand knowledge about network topology or state variables, and is sure to circumvent residual-based BDD. The only requirement for this attack to be successful is that the grid remains in steady state during the eavesdropping stage. Replay attacks render the attacked region of the grid unobservable which could mask the impact of a physical attack on the grid while it is taking place in order to delay a response by authorities. In addition to modeling this form of attacks, Mo and Sinopoli [15] analyze the effectiveness and cost of adding authentication signals to meters' measurements in order to detect replay attacks.

Topology attacks [16], [17] refer to a class of FDI attacks in which adversaries target a grid's topology information to realize their malicious objectives. In parallel to gathering power measurements from meters for SSE, SCADA systems collect measurements of network topology parameters, the status of breakers and switches, for topology estimation. Topology estimation is the process of estimating the bus-branch network topology matrix, $\mathbf{H}$, from the measured status of breakers and switches [18]. It acts as a first step to, and has the same underlying concept as, SSE. For instance, gross errors in topology measurements trigger alarms in the BDD unit. In addition, similar to SSE, topology estimation is vulnerable to stealth FDI attacks which can go undetected through BDD. Using a false topology matrix, $\mathbf{H}$, in SSE could lead to either a significantly-erroneous grid state or no state at all as the SSE might fail to converge [5]. Ashok and Govindarasu study perfect topology FDI attacks in [16]; they propose a way to create such attacks and demonstrate their potential dangers to the grid. In

[17], Kim and Tong derive a condition to successfully launch perfect, topology, FDI attacks, and introduce a heuristic method to assemble imperfect, topology attacks. The authors also study the impact of this form of attacks on real-time locational marginal pricing. In addition, they consider mitigation strategies in which if a select-group of critical meters is protected, topology attacks cannot be realized.

IV. Detection Strategies

Since conventional residual-based BDD are incapable of detecting stealth FDI attacks, new detection techniques had to be devised to address this threat. In this section, we discuss a number of articles that highlight the research directions in this area which mainly emerge from three signal processing fields: statistical anomaly detection [19]–[22], machine learning [23]–[25], and graph theory [26]. Despite stemming from different origins, all detection techniques share the same underlying principle: any FDI attack would disrupt the density distribution of authentic measurements and state variables. Thus, researchers working on developing a suitable detector for a certain type of FDI attacks have to address the following three questions. How to define, model, or estimate the original density distribution of legitimate grid data? How will the studied cyberattack change this density distribution? What is the best way to detect such change?

Statistical anomaly detection methods rely on modeling the density distribution of the authentic grid measurements and states using historical data, forecasting, and/or secure measurements, and then using a statistical hypothesis test to detect changes to the regular density distribution as a result of a suspected attack. For instance, in [19], [20], *Kosut et al.* propose a detector for imperfect FDI attacks based on a generalized likelihood ratio test (GLRT) in which they assume that both measurements and state variables have a multivariate, zero-mean, Gaussian density distribution. They use historical data to learn the covariance matrix of both distributions. Then, they compute the GLRT statistic by solving an optimization problem seeking the attack vector – given a specific sparsity level – that best describes the distribution of the observed measurements. There is a number of limitations with this framework. First, it assumes that state variables maintain the same density distribution at all times, whereas one would expect them to behave differently in different operating conditions of the grid. As we pointed out at the beginning of this section, defining the state of an uncompromised grid is very challenging due to the fact that it entails several modes of operation ranging from transient- to steady-state. An effective detector should be able to distinguish between, on the one hand, several, different, normal states, and, on the other, all possible attacked states. Another limitation of the GLRT detector is that it assumes prior knowledge of the number of compromised meters which is not a reasonable assumption in real-life settings. Furthermore, since the detector has to solve an optimization problem each time to compute the GLRT statistic, another challenge emerges in terms of the scalability of this method if it is to be applied to distribution-side SSE where the number of smart meters involved is projected to be enormous.

Another example of statistical anomaly detection techniques is the work of Zhao *et al.* [22], in which they use short-term state forecasting to detect anomalies in the distribution of the SCADA measurements due to imperfect FDI attacks. This work attempts to model some inherent structure in power grids' state variables that would be broken in case an attacker attempts to inject false data into the system. In this case, the authors seek such structure in the form of correlation of injected powers at load buses which could result from the fact that power consumption is significantly affected by local weather conditions. Thus, loads are expected to exhibit time-series behaviour with inter- and intra-bus correlation of state variables. At this point, one should point out that even stealth FDI attacks that keep measurement residuals unchanged would damage such correlation structure. Hence, if this structure can be modelled properly, and if the damage to correlation due to an FDI attack is significant enough to be observed, then it is possible to detect even perfect FDI attacks. In [22], the authors use a first-order, auto-regressive (AR) process to model the temporal evolution of measurements. They use historical data to learn the AR state-transition matrix which they expect would implicitly-encompass the correlation structure. Afterwards, the authors use this AR model to forecast the subsequent set of measurements and compare it to the observed measurements. If the normalized ℓ_∞–norm of the deviation between the two vectors is larger than a certain threshold, the detector triggers an alarm. If not, the estimated state is deemed valid and is then used to update the AR state-transition matrix.

Although detection methods along this line of research are expected to be effective against stealth FDI attacks in which attackers do not consider these innate correlation structures in the data, such as the LR, replay, and topology attacks, the attack model proposed in [27] could prove very challenging for this detection strategy. In [27], Esmalifalak *et al.* propose a technique using which adversaries can acquire the knowledge, about network topology and correlation of state variables, needed to launch stealth FDI attacks. They show, within the framework of DC SSE, that attackers can use independent component analysis (ICA) to estimate the network topology matrix, **H**, multiplied by the eigenvectors of the state variables, from intercepted power measurements. In this case, the attack carried out by the adversaries would hold the same correlation structure as the true measurements, and could prove very challenging for statistical anomaly detection techniques.

Machine learning techniques train classifiers to discriminate between normal and attacked states of a power grid. Learning methods can be classified into supervised and unsupervised. Supervised learning requires expert-labeled examples of both normal and attacked states, while unsupervised learning searches for structures in unlabeled data. While unsupervised learning remains, to the best of our knowledge, an uncharted territory for detection of stealth FDI attacks, Esmalifalak *et al.* proposed a supervised-learning approach, using a Support-Vector Machine (SVM), to detect stealth FDI attacks in [25]. The authors utilize principal component analysis (PCA) to reduce the dimensionality of the power measurements, and thus, address the curse-of-dimensionality issue raised by the scale of Smart Grids.

The accuracy of machine-learning-based classifiers heavily depends on the quality of the training dataset available, which should comprise a comprehensive dictionary of all different,

normal states and all possible, attack models. The construction of such dataset requires studying and emulating a wide range of normal operating conditions of the grid as well as different models of stealth FDI attacks. This remains an open-ended research challenge. For this reason, machine learning algorithms tend to outperform other methods in detecting known models of attacks, but perform poorly on unknown attacks [24].

Graph-theory-based methods employ graphical model selection techniques to fit the grid's state variables into a graphical model which, under normal operating conditions, is expected to follow the grid topology. Thus, by checking the obtained graph of state variables and the output of the topology estimator for mismatches, stealth FDI attacks can be detected. The detection depends on the assumption that in case of an FDI attack, the graph changes and deviates from network topology. In [26], Sedghi and Jonckheere model the bus voltage phase angles using a Gaussian Markov Random Field. Then, they use a Gaussian graphical model selection technique called the Conditional Covariance Test (CCT) to find the Markov graph between the bus voltage phase angles. The authors show that, in normal conditions, the Markov graph follows the grid structure. Afterwards, they compare the obtained graph to the network topology, and raise a flag whenever there is a mismatch between the two. One can observe a major limitation with this approach which is the fact that it assumes that utilities have access to accurate topology information, and therefore, treats the output of the topology estimator as its ground truth. This makes this family of detectors blind to stealth topology FDI attacks.

V. Conclusion

In this paper, we have presented a survey on stealth FDI attacks against SSE. We discussed the theoretical principle behind this class of cyberattacks. In addition, we classified these attacks according to two different criteria: the amount of information available to the attacker and the targeted network parameters. Finally, we highlighted some of the challenges in existing research directions in the detection strategies of these attacks.

References

[1] F. Schweppe and J. Wildes, "Power System Static-State Estimation, Part I: Exact Model," *IEEE Trans. Power Appar. Syst.*, vol. PAS-89, no. 1, pp. 120–125, Jan. 1970.

[2] F. Schweppe and D. Rom, "Power System Static-State Estimation, Part II: Approximate Model," *IEEE Trans. Power Appar. Syst.*, vol. PAS-89, no. 1, pp. 125–130, Jan. 1970.

[3] A. R. Bergen and V. Vittal, *Power Systems Analysis*, 2 edition. Upper Saddle River, NJ: Pearson, 1999.

[4] Y. F. Huang, S. Werner, J. Huang, N. Kashyap, and V. Gupta, "State Estimation in Electric Power Grids: Meeting New Challenges Presented by the Requirements of the Future Grid," *IEEE Signal Process. Mag.*, vol. 29, no. 5, pp. 33–43, Sep. 2012.

[5] A. Abur and A. G. Expósito, *Power System State Estimation: Theory and Implementation*, 1 edition. New York, NY: CRC Press, 2004.

[6] Y. Liu, P. Ning, and M. K. Reiter, "False Data Injection Attacks Against State Estimation in Electric Power Grids," *ACM Trans Inf Syst Secur*, vol. 14, no. 1, p. 13:1–13:33, Jun. 2011.

[7] Y. Liu, P. Ning, and M. K. Reiter, "False Data Injection Attacks Against State Estimation in Electric Power Grids," in *Proceedings of the 16th ACM Conference on Computer and Communications Security*, New York, NY, USA, 2009, pp. 21–32.

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

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

[10] 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.

[11] C.-H. Lo and N. Ansari, "CONSUMER: A Novel Hybrid Intrusion Detection System for Distribution Networks in Smart Grid," *IEEE Trans. Emerg. Top. Comput.*, vol. 1, no. 1, pp. 33–44, Jun. 2013.

[12] X. Liu and Z. Li, "Local Load Redistribution Attacks in Power Systems With Incomplete Network Information," *IEEE Trans. Smart Grid*, vol. 5, no. 4, pp. 1665–1676, Jul. 2014.

[13] X. Liu and Z. Li, "False Data Attacks Against AC State Estimation With Incomplete Network Information," *IEEE Trans. Smart Grid*, vol. 8, no. 5, pp. 2239–2248, Sep. 2017.

[14] J. Zhao, G. Zhang, Z. Y. Dong, and K. P. Wong, "Forecasting-Aided Imperfect False Data Injection Attacks Against Power System Nonlinear State Estimation," *IEEE Trans. Smart Grid*, vol. 7, no. 1, pp. 6–8, Jan. 2016.

[15] Y. Mo and B. Sinopoli, "Secure control against replay attacks," in *2009 47th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, Monticello, IL, USA, 2009, pp. 911–918.

[16] A. Ashok and M. Govindarasu, "Cyber attacks on power system state estimation through topology errors," in *2012 IEEE Power and Energy Society General Meeting*, San Diego, CA, USA, 2012, pp. 1–8.

[17] J. Kim and L. Tong, "On Topology Attack of a Smart Grid: Undetectable Attacks and Countermeasures," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 7, pp. 1294–1305, Jul. 2013.

[18] F. F. Wu and W.-H. E. Liu, "Detection of topology errors by state estimation (power systems)," *IEEE Trans. Power Syst.*, vol. 4, no. 1, pp. 176–183, Feb. 1989.

[19] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Malicious Data Attacks on Smart Grid State Estimation: Attack Strategies and Countermeasures," in *2010 First IEEE International Conference on Smart Grid Communications*, 2010, pp. 220–225.

[20] 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.

[21] J. Zhao, G. Zhang, and R. A. Jabr, "Robust Detection of Cyber Attacks on State Estimators Using Phasor Measurements," *IEEE Trans. Power Syst.*, vol. 32, no. 3, pp. 2468–2470, May 2017.

[22] J. Zhao, G. Zhang, M. La Scala, Z. Y. Dong, C. Chen, and J. Wang, "Short-Term State Forecasting-Aided Method for Detection of Smart Grid General False Data Injection Attacks," *IEEE Trans. Smart Grid*, vol. 8, no. 4, pp. 1580–1590, Jul. 2017.

[23] M. Esmalifalak, Nam Tuan Nguyen, Rong Zheng, and Zhu Han, "Detecting stealthy false data injection using machine learning in smart grid," in *2013 IEEE Global Communications Conference (GLOBECOM)*, Atlanta, GA, USA, 2013, pp. 808–813.

[24] Y. Chakhchoukh, S. Liu, M. Sugiyama, and H. Ishii, "Statistical outlier detection for diagnosis of cyber attacks in power state estimation," in *2016 IEEE Power and Energy Society General Meeting (PESGM)*, Boston, MA, USA, 2016, pp. 1–5.

[25] M. Esmalifalak, L. Liu, N. Nguyen, R. Zheng, and Z. Han, "Detecting Stealthy False Data Injection Using Machine Learning in Smart Grid," *IEEE Syst. J.*, vol. 11, no. 3, pp. 1644–1652, Sep. 2017.

[26] H. Sedghi and E. Jonckheere, "Statistical structure learning of smart grid for detection of false data injection," in *2013 IEEE Power & Energy Society General Meeting*, Vancouver, BC, Canada, 2013, pp. 1–5.

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