Short-term state forecasting-aided method for detection of smart grid general false data injection attacks

Published source: 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," in IEEE Transactions on Smart Grid, vol. 8, no. 4, pp. 1580-1590, July 2017, doi: 10.1109/TSG.2015.2492827.

Short-Term State Forecasting-Aided Method for Detection of Smart Grid General False Data Injection Attacks

Junbo Zhao, *Student Member, IEEE*, Gexiang Zhang, *Member, IEEE*, Massimo La Scala, *Fellow, IEEE*, Zhao Yang Dong, *Senior Member, IEEE*, Chen Chen, *Member, IEEE*, Jianhui Wang, *Senior Member, IEEE*

***Abstract*—Successful detection of false data injection attacks (FDIAs) is essential for ensuring secure power grids operation and control. First, this paper extends the approximate DC model to a more general linear model that can handle both SCADA and PMU measurements. Then, a general FDIA based on this model is derived and the error tolerance of such attacks is discussed. To detect such attacks, a method based on short-term state forecasting considering temporal correlation is proposed. Furthermore, a statistics-based measurement consistency test method is presented to check the consistency between the forecasted measurements and the received measurements. This measurement consistency test is further integrated with ∞-norm and L_2-norm-based measurement residual analysis to construct the proposed detection metric. The proposed detector addresses the shortcoming of previous detectors in terms of handling critical measurements. Besides, the problem of removal of attacked measurements, which may cause the system to become unobservable, is addressed effectively by the proposed method through forecasted measurements. Numerical tests on IEEE 14-bus and 118-bus test systems verify the effectiveness and performance of the proposed method.**

***Index Terms*—False data injection attack, state estimation, cyber security, smart grid.**

I. Introduction

STATE estimation (SE) is extremely important for ensuring power system reliable operation and control. It provides system accurate and continuously updated snapshots of the real-time states, which enable energy management system to perform various important control and planning tasks such as optimal power flows, voltage stability study, and contingency analysis [1]. However, with the development of smart grids, the power systems are facing great challenges. One of them is the cyber attacks against SE, which can mislead the system controls, possibly resulting in catastrophic large geographical blackouts [2].

After the introduction of the false data injection attack (FDIA) into power grids [2], it has been the object of new interests and investigations among researchers and utilities because of the potential hacker attack risks due to the increasing number of links to public networks and the web-based applications in the power industry, etc. The FDIA can successfully bypass the conventional normalized measurement residual-based bad data detection, thus causing serious threats to system operation and control. To date, three kinds of FDIAs have been proposed, i.e., state attack [2]–[4], topology attack [5], and load redistribution attack [6]. In the state attack case, the adversary can introduce arbitrary perturbations into the system state estimation results by altering the measurement values of a set of meters. In the topology attack, the adversary aims to compromise a certain number of meters and break circuit switches to mislead the operator with the incorrect system topology without being detected. In the load redistribution attack scenario, power injection measurements of the load buses and line power flow measurements are attacked and used to change the power flow distributions, i.e., to increase loads at some buses and to reduce loads at other buses without changing the total loads.

To detect and mitigate the FDIA, a number of methods have been proposed [7]– [13]. Two security indices based on the analysis of the sparsity of attack vector and attack vector magnitude are proposed [7]. The least effort needed to launch the FDIA while avoiding detections by the control center is also discussed. In [8], a greedy algorithm-based secure PMU placement method is proposed to defend against FDIA. In [9], the FDIA is formulated as a matrix separation problem while the nuclear norm minimization and low rank matrix factorization methods are used as detection metrics. In [10], known perturbations are applied to the system and then the system is "probed" for any unexpected responses; however, the random known perturbations, i.e., topology, transformer taps, etc., cannot guarantee the fully elimination of the FDIA possibility. For example, it is showed in [11] that the FDIA is still successful if the attacker has imperfect but structured topological information of the system. An alternative group of the FDIA defense methods [12], [13] aims to add protections on many measurements so that the adversary could not get enough measurements to launch attacks. For instance,

This work is partially supported by National Natural Science Foundation (NSFC) under Grants 61170016 and 61373047. The author Junbo Zhao thanks for the financial support from CSC No.201407000013.

Junbo Zhao are with the School of Electrical Engineering, Southwest Jiaotong University, Chengdu, 610031 China and the Bradley Department of Electrical Computer Engineering, Virginia Polytechnic Institute and State University, Northern Virginia Center, Falls Church, VA 22043, USA (e-mail: junbob@vt.edu).

Gexiang Zhang is with the School of Electrical Engineering, Southwest Jiaotong University, Chengdu, 610031 China (e-mail: zhgxdylan@126.com).

Massimo La Scala is with the Department of Electrical Engineering and Computer Science, Politecnico di Bari, 70125 Bari, Italy (e-mail:massimo.lascala@poliba.it).

Zhao Yang Dong is with the School of Electrical and Information Engineering, The University of Sydney, NSW 2006, Australia (e-mail: zydong@ieee.org).

Jianhui Wang and Chen Chen are with Argonne National Laboratory, Argonne, IL 60439 USA (e-mail: jianhui.wang@anl.gov).

in [12], a specific selected measurement-based strategy is adopted against the attacks. The selected measurements are the minimum number of measurements needed to ensure system observability. However, it is economically unattractive to add protection on a large number of measurements. On the other hand, most papers assume hackers can acquire perfect system configuration information, i.e., Jacobian matrix $\boldsymbol{H}$ without biases in order to launch perfect FDIA, which is not practical for real power systems. This is because that the attacker is 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 he/she is restricted to get access to many grid facilities (for example, the hacker may not know the new installed PMU devices while the control center can get access to them). Thus, it is impossible for the hacker to get exactly the same Jacobian matrix $\boldsymbol{H}$ as the control center. In other words, the $\boldsymbol{H}$ that the hacker gets has bias, which would increase the risk of being detected by the control center since the FDIA is not perfect any more. Therefore, how to find the general FDIA model (including perfect and imperfect FDIAs) while maintaining as low probability to be detected by the control center as possible should be investigated.

The measurements for a power system can be broadly classified as critical and non-critical [14]. Critical measurements are measurements that, once removed, will make the system unobservable and the state estimation unavailable. Existence of critical measurements depends on the network topology, as well as the number, type, and location of measurements, instead of the measurement values themselves. The widely used L_2-norm measurements residual-based $J(\boldsymbol{x})$ detector and the largest normalized residue-based (LNR) detector cannot detect bad critical measurements [14], not to mention the intentional false data injection attacks on the critical measurements. To the best of our knowledge, detection of such attacks is not considered in the existing literature. Last but not least, another purpose of detecting the FDIA is to remove the attacked measurements and then re-run the SE to get the most likely system operation states. But sometimes the removal of attacked measurements may cause the system to be unobservable, especially for distribution or transmission systems with low measurement redundancy, leading to SE unavailable. However, this problem has not been completely considered and addressed in the aforementioned FDIA methods.

This paper focuses on mitigating the issues discussed above to a certain degree. The main contributions are:

- Most of the existing FDIAs assume an approximate DC model associated to the SCADA measurements, which is not accurate and comprehensive when the PMU measurements are included. This paper extends the model to a more general linear model which can effectively handle both the SCADA and PMU measurements.
- A general FDIA based on the proposed linear measurement model is derived and the error tolerance of such attacks is analyzed.
- To detect the FDIAs, a short-term state forecasting-based method considering nodal state temporal correlations is proposed. This method exploits the measurement consistency between the forecasted and the received measurements. This measurement consistency test is then integrated with ∞–norm and L_2-norm-based measurement residual analysis to construct the proposed detection metric.
- The ability of the proposed detector for handling the FDIA on critical measurements is discussed and analyzed. Besides, the system observability issue caused by removal of the attacked measurements is addressed.
- Numerical test results on IEEE 14-bus and 118-bus test systems show that the proposed method outperforms the two well-established detection schemes, i.e., $J(\boldsymbol{x})$ detector and the LNR detector.

The rest of this paper is organized as follows. In Section II, the general linear measurement model and its corresponding FDIA are presented. The proposed short-term forecasting-based FDIA detection method is shown in Section III. The effectiveness and performance of the proposed model and detection method are evaluated in Section V. Finally, the paper is concluded in Section VI.

II. Problem Formulation

A. Generic Linear Measurement Derivation

In the literature, the approximate simplified and linearized DC power flow model derived from the complex nonlinear power flow equations is widely used for the FDIA construction. This pure DC model-based FDIA is neither accurate nor general for the following reasons: from the perspective of the operator, inclusion of more accurate PMU measurements into SE will generate more accurate estimation results [15]. Then, the pure SCADA measurement-based SE will be slightly modified because with the increasing installation of PMU devices, part of the Jacobian matrix will be exactly linear for the PMU observable area or even the whole Jacobian matrix will be exactly linear if the number of PMUs is enough for ensuring the entire system observable. In this situation, the linearization errors are reduced. From the adversaries' point, if the pure approximate DC model is still used for the FDIA construction, larger deviations will be produced, thus resulting in being detected with higher probability by the control center since the measurement model used by the control center has been modified. In this section, a more general linear measurement model that can handle both conventional SCADA and PMU measurements is derived. Then, the general FDIA on this model is presented and discussed.

For any linear measurement model, the relationship between the measurement vector $\boldsymbol{z}$ and the state vector $\boldsymbol{x}$ is

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

where $\boldsymbol{H}$ is a matrix that represents the linear relationship between the measurements and the states. For PMU full observable systems, the elements of $\boldsymbol{H}$ are constituted by the system conductance and susceptance without any linearization error, while for PMU partial observable systems, $\boldsymbol{H} = [\boldsymbol{H_c^T}\ \boldsymbol{H_p^T}]^{\boldsymbol{T}}$, where $\boldsymbol{H_c}$ is the approximate DC model related part for the PMU unobservable area, and $\boldsymbol{H_p}$ is the accurate linear model for the PMU observable area. If no PMUs are installed in the

system, $\boldsymbol{H} = \boldsymbol{H_c}$. $\boldsymbol{e}$ is the random measurement error vector and is assumed to be normally distributed, i.e., $\boldsymbol{e} \sim N(\boldsymbol{0}, \boldsymbol{R})$, where $\boldsymbol{R}$ is the error covariance matrix. From (1), we can obtain the estimated state variables $\hat{\boldsymbol{x}}$ by the weighted least square method, i.e.,

$$\hat{\boldsymbol{x}} = (\boldsymbol{H}^T\boldsymbol{R}^{-1}\boldsymbol{H})^{-1}\boldsymbol{H}^T\boldsymbol{R}^{-1}\boldsymbol{z}. \tag{2}$$

B. Generic FDIA and Error Tolerance Analysis

The widely used bad data detection algorithm indicates the existence of bad data as long as $\|\boldsymbol{z} - \boldsymbol{H}\hat{\boldsymbol{x}}\| > \boldsymbol{\tau}$ holds, where $\boldsymbol{\tau}$ is a pre-defined detection threshold. However, [2] discovered that if the attacker vector is $\boldsymbol{a} = \boldsymbol{Hc}$, where $\boldsymbol{c}$ is the nonzero column vector and has the same dimensions as $\boldsymbol{x}$, the injected false data cannot be detected by the bad data detection algorithm, because

$$\begin{aligned}\|\boldsymbol{z} + \boldsymbol{a} - \boldsymbol{H}(\hat{\boldsymbol{x}} + \boldsymbol{c})\| &= \|\boldsymbol{z} - \boldsymbol{H}\hat{\boldsymbol{x}} + (\boldsymbol{a} - \boldsymbol{Hc})\| \\ &= \|\boldsymbol{z} - \boldsymbol{H}\hat{\boldsymbol{x}}\| \le \boldsymbol{\tau}.\end{aligned} \tag{3}$$

The estimated state vector is

$$\begin{aligned}\widehat{\boldsymbol{x}}_{\boldsymbol{a}} &= (\boldsymbol{H}^T\boldsymbol{R}^{-1}\boldsymbol{H})^{-1}\boldsymbol{H}^T\boldsymbol{R}^{-1}(\boldsymbol{z} + \boldsymbol{a}) \\ &= (\boldsymbol{H}^T\boldsymbol{R}^{-1}\boldsymbol{H})^{-1}\boldsymbol{H}^T\boldsymbol{R}^{-1}(\boldsymbol{z} + \boldsymbol{Hc}) \\ &= \widehat{\boldsymbol{x}} + \boldsymbol{c}.\end{aligned} \tag{4}$$

Actually it is impossible to acquire the exact information of $\boldsymbol{H}$ in practical power systems, the assumptions $\boldsymbol{a} = \boldsymbol{Hc}$ should be relaxed to the general conditions.

Proposition 1. *Suppose the original measurement $\boldsymbol{z}$ can bypass the L_2-norm measurement residual-based bad data detection. The malicious measurement $\boldsymbol{z} + \boldsymbol{a}$ can also pass this detector as long as $\varepsilon = \|\boldsymbol{a} - \boldsymbol{Hc}\| \le \boldsymbol{\tau} - \|\boldsymbol{z} - \boldsymbol{H}\hat{\boldsymbol{x}}\|$ holds, where $\boldsymbol{a}$ is the sparse attack vector; $\boldsymbol{c}$ is the nonzero column vector; $\boldsymbol{\varepsilon}$ is the error tolerance of the attack vector; τ is the detection threshold.*

Proof: since $\boldsymbol{z}$ can bypass the L_2-norm measurement residual-based bad data detection, $\|\boldsymbol{z} - \boldsymbol{H}\hat{\boldsymbol{x}}\| \le \boldsymbol{\tau}$ is satisfied. The estimated state vector $\hat{\boldsymbol{x}}_{\boldsymbol{bad}}$ using $\boldsymbol{z_a} = \boldsymbol{z} + \boldsymbol{a}$ is represented by $\hat{\boldsymbol{x}} + \boldsymbol{c}$. Then, the L_2-norm of the measurement residual is

$$\begin{aligned}\|\boldsymbol{z_a} - \boldsymbol{H}\hat{\boldsymbol{x}}_{\boldsymbol{bad}}\| &= \|\boldsymbol{z} + \boldsymbol{a} - \boldsymbol{H}(\hat{\boldsymbol{x}} + \boldsymbol{c})\| \\ &\le \|\boldsymbol{z} - \boldsymbol{H}\hat{\boldsymbol{x}}\| + \|\boldsymbol{a} - \boldsymbol{Hc}\|.\end{aligned} \tag{5}$$

Therefore, as long as $\varepsilon \le \boldsymbol{\tau} - \|\boldsymbol{z} - \boldsymbol{H}\hat{\boldsymbol{x}}\|$ holds, we can obtain

$$\|\boldsymbol{z_a} - \boldsymbol{H}\hat{\boldsymbol{x}}_{\boldsymbol{bad}}\| \le \boldsymbol{\tau}, \tag{6}$$

which means the L_2-norm of the measurement residual with attacks is less than the detection threshold, resulting in undetectable FDIA. It should be noticed that the widely used perfect attack vector in the literature is just a special case of this error tolerance, i.e., $\varepsilon = 0$. ■

1) Proposed Generic FDIA Method: As mentioned in the introduction that due to the limited knowledge of the system real-time operation states and the restricted physical access to to most grid facilities, the hacker to cannot get exactly the same Jacobian matrix $\boldsymbol{H}$ as the control center. In other words, the $\boldsymbol{H}$ the hacker gets has bias, i.e., $\boldsymbol{H} \leftarrow \boldsymbol{H} + \boldsymbol{\delta}$, where $\boldsymbol{\delta}$ is the bias due to the imperfect knowledge of the system information. Thus, the attack vector constructed by the adversary in this scenario will be $\boldsymbol{a} = (\boldsymbol{H} + \boldsymbol{\delta})\boldsymbol{c} = \boldsymbol{Hc} + \boldsymbol{\delta c}$. The estimated state vector under the attack is

$$\begin{aligned}\widehat{\boldsymbol{x}}_{\boldsymbol{a}} &= (\boldsymbol{H}^T\boldsymbol{R}^{-1}\boldsymbol{H})^{-1}\boldsymbol{H}^T\boldsymbol{R}^{-1}(\boldsymbol{z} + \boldsymbol{a}) \\ &= (\boldsymbol{H}^T\boldsymbol{R}^{-1}\boldsymbol{H})^{-1}\boldsymbol{H}^T\boldsymbol{R}^{-1}(\boldsymbol{z} + \boldsymbol{Hc} + \boldsymbol{\delta c}) \\ &= \widehat{\boldsymbol{x}} + \boldsymbol{c} + (\boldsymbol{H}^T\boldsymbol{R}^{-1}\boldsymbol{H})^{-1}\boldsymbol{H}^T\boldsymbol{R}^{-1}\boldsymbol{\delta c}.\end{aligned} \tag{7}$$

By comparing (4) and (7), it is observed that the intended attack magnitude $\boldsymbol{c}$ on the state vector has changed to $\overline{\boldsymbol{c}} = \boldsymbol{c} + (\boldsymbol{H}^T\boldsymbol{R}^{-1}\boldsymbol{H})^{-1}\boldsymbol{H}^T\boldsymbol{R}^{-1}\boldsymbol{\delta c}$ due to the imperfect knowledge of system matrix $\boldsymbol{H}$. This will cause the increased probability of being detected. The residual can be obtained as:

$$\begin{aligned}\boldsymbol{r_a} &= \boldsymbol{z_a} - \boldsymbol{H}\widehat{\boldsymbol{x}}_{\boldsymbol{a}} = \boldsymbol{z} + \boldsymbol{a} - \boldsymbol{H}(\widehat{\boldsymbol{x}} + \overline{\boldsymbol{c}}) \\ &= \boldsymbol{r} + \boldsymbol{a} - \boldsymbol{H}\overline{\boldsymbol{c}} \\ &= \boldsymbol{r} + \boldsymbol{\delta c} + \boldsymbol{H}(\boldsymbol{c} - \overline{\boldsymbol{c}}) \\ &= \boldsymbol{r} + \boldsymbol{\delta c} - \boldsymbol{H}(\boldsymbol{H}^T\boldsymbol{R}^{-1}\boldsymbol{H})^{-1}\boldsymbol{H}^T\boldsymbol{R}^{-1}\boldsymbol{\delta c} \\ &= \boldsymbol{r} + (\boldsymbol{I} - \boldsymbol{M})\boldsymbol{\delta c} = \boldsymbol{r} + \boldsymbol{S}\boldsymbol{\delta c},\end{aligned} \tag{8}$$

where $\boldsymbol{M} = \boldsymbol{H}(\boldsymbol{H}^T\boldsymbol{R}^{-1}\boldsymbol{H})^{-1}\boldsymbol{H}^T\boldsymbol{R}^{-1}$; $\boldsymbol{S} = \boldsymbol{I} - \boldsymbol{M}$; $\boldsymbol{I}$ is the identity matrix.

By combining (5) and (8), we can conclude that if the following condition is satisfied, the FDIA cannot be detected.

$$\varepsilon = \|\boldsymbol{a} - \boldsymbol{H}\overline{\boldsymbol{c}}\| = \|\boldsymbol{I} - \boldsymbol{M}\|\|\boldsymbol{\delta c}\| \le \boldsymbol{\tau} - \|\boldsymbol{z} - \boldsymbol{H}\widehat{\boldsymbol{x}}\| \tag{9}$$

This upper bound of $\|\boldsymbol{\delta c}\|$ represents the tradeoff between attack magnitude and degree of imperfect knowledge of the system information.

2) Analysis of FDIA on Critical Measurements: According to the definition of critical measurement [14], the zero diagonal(s) of $\boldsymbol{S}$ is (are) defined as critical measurement(s). It is interesting to notice that as long as the attacks are imposed on the critical measurements, $\|\boldsymbol{\varepsilon}\| = \|\boldsymbol{I} - \boldsymbol{S}\|\|\boldsymbol{\delta c}\| = \boldsymbol{0} \le \boldsymbol{\tau} - \|\boldsymbol{z} - \boldsymbol{H}\widehat{\boldsymbol{x}}\|$ always holds irrespective of the attack magnitudes.

This paper aims to construct a practical FDIA based on the general linear measurement model. Besides, the short-term state forecasting-aided method is proposed to detect both general FDIA and the FDIA on critical measurements in the following section.

III. Proposed Detection Method

A. Motivation

As indicated in [16], "If a system is controlled by a human being, watching, perhaps, a pen recorder, he will automatically ignore a large random spike that is obviously incorrect." In other words, under system normal operation conditions, if we can get the approximate prior system measurements, the perturbation $\boldsymbol{a}$ on the original measurements introduced by the adversary will make the attacked measurements deviate far from the approximate prior measurements, thus making the attack detectable. On the other hand, the loads vary according to the weather and temperature, showing apparently time series characteristics. It means that with the evolution of system changes, temporal correlation exists among different nodal states. If the FDIA occurs, the deviation $\boldsymbol{c}$ or $\overline{\boldsymbol{c}}$ introduced

by the adversary will break down the temporal correlation, leading to the FDIA detectable.Besides, due to the imperfect knowledge of the system information and the restricted access to the system measurements, the replay attack [17] is impractical for realistic power systems. Thus, the historical state-based system anomaly detection is feasible.

In this paper, a short-term state forecasting method considering the temporal correlation is proposed to calculate the approximate prior system measurements. Then, a statistics-based measurement consistency test method is proposed to check the consistency between the forecasted measurements and the current received measurements. This measurement consistency test is then integrated with the ∞ and the L_2-norm-based measurement residual analysis to construct the proposed detection metric.

B. Short-Term State Forecasting

In the existing forecasting-aided state estimation methods [18], the system is assumed to operate under quasi-static conditions and the state transition matrix $\boldsymbol{F_k}$ in (13) is diagonal and constant. However, due to the continuous variation of loads, a power system is not static, but changes with time. Once the loads of a power system change, the generation has to keep up with the changes and consequently the flows and injections at all the buses will change, resulting in state changes of every bus. On the other hand, due to the load variations caused by the weather and temperature changes, temporal correlation exists among the nodal states and should be carefully considered for better forecasting. This paper takes into account such correlation and uses the time-variant state transition matrix updating method in our earlier work [19] to improve the system state forecasting accuracy.

In this paper, since we are only interested in one-step ahead (short-term) state prediction (using the state at previous time sample, i.e., k-1, to forecast the state at time sample k), the auto-regressive (AR) models, which have comparable performance with auto-regressive moving average (ARMA), are adopted [20]. The time series for system states $\boldsymbol{x_k}$ at time sample k, by the AR(p) model is expressed as,

$$x_k = \sum_{i=1}^{p} \varphi_i \cdot x_{k-i} + \nu_k, \tag{10}$$

where φ_i are the coefficient parameters; $\boldsymbol{\nu_k}$ is the noise, which is usually assumed to have Gaussian distribution, i.e., $N(0, C_k)$. If we define $\boldsymbol{x_k^j}$ the jth zone according to (10), i.e., $\boldsymbol{x_k^j} = [x^j_{k-1}, x^j_{k-2}, ..., x^j_{k-(p-1)}]^T$, the following equation can be derived

$$\begin{bmatrix} x^j_k \\ x^j_{k-1} \\ \vdots \\ x^j_{k-(p-1)} \end{bmatrix} = \begin{bmatrix} \varphi^j_1 & \varphi^j_2 & \cdots & \varphi^j_p \\ 1 & 0 & \cdots 0 & 0 \\ & \ddots & \ddots & \\ 0 & \cdots & 1 & 0 \end{bmatrix} \begin{bmatrix} x^j_{k-1} \\ x^j_{k-2} \\ \vdots \\ x^j_{k-p} \end{bmatrix} + \begin{bmatrix} \nu^j_{k-1} \\ 0 \\ \vdots \\ 0 \end{bmatrix} \tag{11}$$

Let M the total number of zones, the above equation can be rewritten as:

$$\begin{bmatrix} \boldsymbol{x_k^1} \\ \vdots \\ \boldsymbol{x_k^M} \end{bmatrix} = \begin{bmatrix} \boldsymbol{\phi_k^1} & \cdots & 0 \\ 0 & \ddots & \vdots \\ 0 & \cdots & \boldsymbol{\phi_k^M} \end{bmatrix} \begin{bmatrix} \boldsymbol{x_{k-1}^1} \\ \vdots \\ \boldsymbol{x_{k-1}^M} \end{bmatrix} + \begin{bmatrix} \nu^1_k \\ \vdots \\ \nu^M_k \end{bmatrix} \tag{12}$$

where $\boldsymbol{\phi_k^j} = [\varphi^j_{k-1}\ \varphi^j_{k-2}\ ...\varphi^j_{k-(p-1)}]^T, j = (1, ...M)$. In this paper, as most papers did ([18], [19], [21] for example), we assume the order of the AR model is $p = 1$. Thus, one can obtain the following forecasting model:

$$\widetilde{\boldsymbol{x}}_{\boldsymbol{k}} = \boldsymbol{F_k x_{k-1}} + \boldsymbol{\nu_k}, \tag{13}$$

where $\widetilde{\boldsymbol{x}}_{\boldsymbol{k}}$ is the forecasted state vector; the parameter matrix $\boldsymbol{F_k} = \boldsymbol{diag(\phi_k^j)}$ can be estimated by our previous time-variant state transition matrix updating technique [19]. The main idea of this method is to update $\boldsymbol{F_k}$ using the estimated state $\widehat{\boldsymbol{x}}_{\boldsymbol{k}}$ at time sample k and the historical $\boldsymbol{x_{k-1}}$ through least squares estimation, resulting in more accurate parameters estimation. This is because the new system measurements, which can reflect realistic system operation conditions, bring new information to the filtered state. Thus, using both filtered and historical state information to adjust the parameters will make the forecasting model more accurate, leading to more accurate state forecasting results.

The forecasting error matrix can be calculated through $\boldsymbol{\Sigma_k} = \boldsymbol{F_k T_k F_k^T} + \boldsymbol{C_k}$, where $\boldsymbol{T_k}$ is the state forecasting error matrix at time k-1 and usually assumed to have normal distribution [18], [19], [21], i.e., $\boldsymbol{T_k} = \boldsymbol{E}[(\boldsymbol{x_{k-1}} - \widehat{\boldsymbol{x}}_{\boldsymbol{k-1}}) \cdot (\boldsymbol{x_{k-1}} - \widehat{\boldsymbol{x}}_{\boldsymbol{k-1}})^{\boldsymbol{T}}]$, where $\widehat{\boldsymbol{x}}_{\boldsymbol{k-1}}$ is the estimated state vector at previous time sample k-1; $\boldsymbol{C_k} = \boldsymbol{E}(\boldsymbol{\nu_k \nu_k^T})$, where $\boldsymbol{E}(\cdot)$ is the expectation operator. It is easy to prove that $\boldsymbol{\Sigma_k}$ follows normal distribution since $\boldsymbol{x_{k-1}}$ and $\boldsymbol{\nu_k}$ follows normal distributions. A more detailed process of parameter estimation and its associated covariance matrix can be found in [19].

Therefore, the prior system measurements including conventional SCADA and PMU measurements at time sample k can be calculated by the forecasted states as (the index k is omitted for notational simplicity):

$$\widetilde{\boldsymbol{z}} = \boldsymbol{H}\widetilde{\boldsymbol{x}}, \tag{14}$$

and the forecasting error covariance matrix is

$$\mathbf{cov}(\boldsymbol{H}\widetilde{\boldsymbol{x}}) = \boldsymbol{H}\mathbf{cov}(\widetilde{\boldsymbol{x}})\boldsymbol{H^T} = \boldsymbol{H\Sigma H^T}. \tag{15}$$

Thus, the residual between the original received measurement vector $\boldsymbol{z}$ and the forecasted measurement vector is $\widetilde{\boldsymbol{r}} = \widetilde{\boldsymbol{z}} - \boldsymbol{z}$.

Proposition 2. *Ideally, the residual $\widetilde{\boldsymbol{r}} = \widetilde{\boldsymbol{z}} - \boldsymbol{z}$ should be normally distributed with zero mean and covariance $\boldsymbol{N} = \boldsymbol{R} + \boldsymbol{H\Sigma H^T}$.*

Proof: The forecasted measurement vector $\widetilde{\boldsymbol{z}}$ is dependent on the historical measurements, which is independent from the present measurement $\boldsymbol{z}$. Therefore, errors present in each of these measurement sets will be considered uncorrelated. Thus, the error covariance matrix of the residual can be calculated as

$$\boldsymbol{N} = \mathbf{cov}\,(\widetilde{\boldsymbol{z}} - \boldsymbol{z}) = \mathbf{cov}\,(\widetilde{\boldsymbol{z}}) + \mathbf{cov}\,(\boldsymbol{z}) = \boldsymbol{R} + \boldsymbol{H\Sigma H^T} \tag{16}$$

On the other hand, the noise matrix $\boldsymbol{C}$, gross error of SCADA and PMU measurements are usually assumed to be normally distributed with zero mean. So, we can easily derive: $\Im[\widetilde{\boldsymbol{z}} - \boldsymbol{z}] = \boldsymbol{0}$, where $\Im$ is the expectation operator. ■

Remark 1: In this paper, the historical state information come from the previous state estimation results and the enhanced bad data processing methods in the literature, such as that in [22], [23], are assumed to be used to clear the contaminated data. If such enhanced bad data processing methods are not adopted for the previous state estimation, the robust estimation methods in time series analysis can be used for ensuring the accuracy of the forecasting results even contaminated data occur in the historical data. For example, the Median-of-Ratios Estimator (MRE) and the Phase-Phase Correlator (PPC) [24], which have high breakdown points, can be adopted to perform the robust state forecasting. On the other hand, we assume that the hacker do not have the ability to compromise both the real-time data and the historical data . The investigation of detecting FDIA when both real-time and the historical data are compromised by the hacker will be handled in the forthcoming paper.

C. Proposed Detection Metric

The L_2-norm-based measurement residual analysis method has been used in the control center for many years and it has been verified to have good performance in dealing with bad data except for the FDIA. In this paper, we keep this function unchanged and add another back-up high efficient FDIA detection scheme to improve the bad data processing ability including malicious injected data. To be specific, the ∞-norm or L_2-norm-based measurement residual analysis method is integrated into the proposed detector:

$$D_1(\boldsymbol{z}) = \begin{cases} 1 & \text{if} \|\boldsymbol{z} - \boldsymbol{H}\widehat{\boldsymbol{x}}\|_2 \geq \tau_1 \text{ or } \|(\widetilde{\boldsymbol{z}} - \boldsymbol{z})/\boldsymbol{\sigma_N}\|_\infty \geq \tau_2 \\ 0 & \text{otherwise} \end{cases} \tag{17}$$

where $\boldsymbol{\sigma_N} = \boldsymbol{diag(N)}$. Value 1 of $D_1(\boldsymbol{z})$ indicates the existence of bad data or FDIA, whereas, value 0 means no bad data or FDIA. Note that, there are two thresholds in the detector, τ_1 and τ_2, which mark the significance levels of the hypothesis test. In the existing integrated detector-based methods in [4], [25], and [26], the traditional residual-based bad data detection (the detection threshold is τ_1) stays unchanged and τ_1 is fixed to obtain the desired false alarm probability, then, the detection threshold τ_2 for alternative proposed method is varied to test the performance of the detector. In this paper, the performance of the proposed method is tested using the same approach as [4], [25], and [26], i.e., we fix τ_1 to a desired false alarm probability, then vary τ_2 to test our detector.

Remark 2: Two commonly used classical detection schemes: the $J(x)$ detector (marked as $D_2(\boldsymbol{z})$) and LNR detector (marked as $D_3(\boldsymbol{z})$) can be expressed as

$$D_2(\boldsymbol{z}) = \begin{cases} 1 & \text{if } J(\widehat{\boldsymbol{x}}) = (\boldsymbol{z} - \boldsymbol{H}\widehat{\boldsymbol{x}})^T \boldsymbol{R^{-1}} (\boldsymbol{z} - \boldsymbol{H}\widehat{\boldsymbol{x}}) \geq \lambda_1 \\ 0 & \text{otherwise} \end{cases} \tag{18}$$

$$D_3(\boldsymbol{z}) = \begin{cases} 1 & \text{if } \|(\boldsymbol{z} - \boldsymbol{H}\widehat{\boldsymbol{x}})/\boldsymbol{\sigma_W}\|_\infty > \lambda_2 \\ 0 & \text{otherwise} \end{cases} \tag{19}$$

where $\boldsymbol{\sigma_W} = diag(\boldsymbol{W})$ and $\boldsymbol{W}$ is the error covariance matrix of the measurement residue $\widehat{\boldsymbol{r}} = \boldsymbol{z} - \boldsymbol{H}\widehat{\boldsymbol{x}}$ and $\boldsymbol{W} = \boldsymbol{R} - \boldsymbol{H}(\boldsymbol{H^T R^{-1} H})^{-1}\boldsymbol{H^T}$. The probability $\Pr(J(\hat{x}) > \lambda_1)$ and $\Pr(\|(\boldsymbol{z} - \boldsymbol{H}\widehat{\boldsymbol{x}})/\boldsymbol{\sigma_W}\|_\infty > \lambda_2)$ are directly evaluated by the techniques in [27].

It is clear that if the attacks are imposed on the system's critical measurements, both $J(x)$ and LNR detectors will fail for the detection. However, this does not happen in the proposed detector. The reason is that the residue for the critical measurements will always be zeros regardless of attacks. In other words, for those attacked critical measurements, their associated measurement residue vector $\widehat{\boldsymbol{r}} = \boldsymbol{z} - \boldsymbol{H}\widehat{\boldsymbol{x}} = \boldsymbol{0}$, resulting no violations of the detection threshold. However, for the proposed detector, once attacks are imposed on the critical measurements, the forecasted measurements will deviate from the received measurements, i.e., $\widetilde{\boldsymbol{r}} = \widetilde{\boldsymbol{z}} - \boldsymbol{z} \neq \boldsymbol{0}$. This is because under system normal operation conditions, the temporal correlation indicates that the measurement differences between forecasted measurements and received measurements should be consistent. Once the measurements are imposed additional false injected data, the consistency will be broken down, making the attacks detectable.

Remark 3: In this paper, τ_1, λ_1 and λ_2 are designed according to the detection theory in [28]; the corresponding detectors are evaluated by the receive operating characteristic curves (ROC) [4], [28] that characterize the trade-off between the probability of attack detection and the probability of false alarm.

D. FDIA Processing

In the proposed framework, when the historical system state information is available, the short-term state forecasting is performed using the equation (13). The proposed FDIA detection metric is then used to detect whether FDIA exists or not. If no FDIA exists, the state estimation results are reliable and can be used to perform advanced controls and optimizations. Otherwise, the FDIA is detected and the attacked measurements needed to be processed so that the state estimation could be run again to get the accurate estimation results.

In this paper, the normalized residuals, which are larger than the detection thresholds will be remarked as the attacked measurements. One way to process these attacked measurements is to remove them from the measurement set so that they will not affect the final state estimation results. However, removal of the attacked measurements may cause the system to become unobservable, especially for the transmission system with low measurement redundancy, leading to the SE unavailable. In order to handle this problem, instead of removing these attacked measurements, we propose to replace them by the forecasted measurements. To be specific, the corresponding forecasted measurements are used to replace the attacked measurements, then the mixed measurements (original and replaced)-based linear SE is performed again to get the new accurate system operation states. On the other hand, the forecasted measurements can be further regarded as pseudo

measurements to increase the system observability, which is helpful for other measurements-based functions in the control center.

IV. Numerical Results

In this paper, the proposed method is tested on IEEE 14-bus and 118-bus test systems [2]. The PMU installed at a bus can measure the nodal voltage phasors as well as all the current phasors of transmission lines that are connected to this bus. In the simulation, since the PMU measurements are more accurate than the SCADA measurements, their noises are smaller compared with the SCADA measurement noise. Besides, the PMU standard C37.118-2011 [29] specifies that the measurement error requirement in terms of total vector error (TVE) as 0.1%. In this paper, the noise for PMU measurements is assumed to be normally distributed with zero mean and variance, 0.1%, which is widely used in the existing literature [22], [30], [31], while the noise for traditional SCADA measurements is assumed to be normally distributed with zero mean and variance 1%; the power systems are assumed to operate under normal conditions, the scaled aggregated 5-min load data from BPA [32] is used and is linearly filled with 20 data points; then, a normal random variable (noise) with zero mean and standard deviation 1% is added to the load curve and the percent of change in load from one step to another is assumed to be 2%; the fast decoupled power flow program is used to obtain the system states; the total number of zones is set to M=20; the minimum energy attack residue-based attack [4] is used to construct the attack vector. The probability $\Pr(J(\hat{x}) > \lambda_1)$ and $\Pr(\|(\boldsymbol{z} - \boldsymbol{H}\widehat{\boldsymbol{x}})/\boldsymbol{\sigma_W}\|_\infty > \lambda_2)$ are directly evaluated by the techniques in [27]. However, for the proposed detector D_1, we fix τ_1 to gain the desired probability of false alarm and vary τ_2 to test its performance. All the tests are performed in MATLAB environment using Intel Core i5 2.5Hz CPU with 8 GB memory computer.

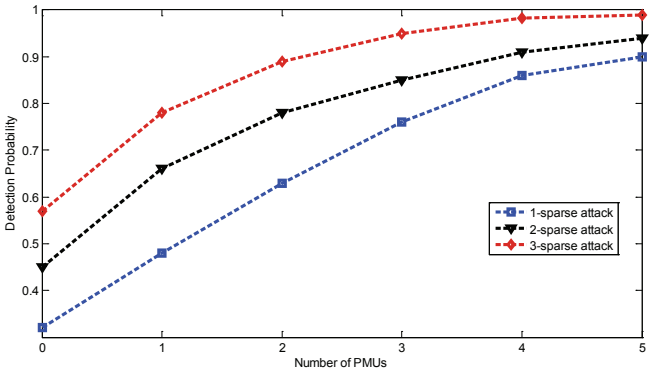
A. Model Validation

To verify the effectiveness of the proposed general linear measurement model and its associated generic FDIAs, the following two cases are considered,

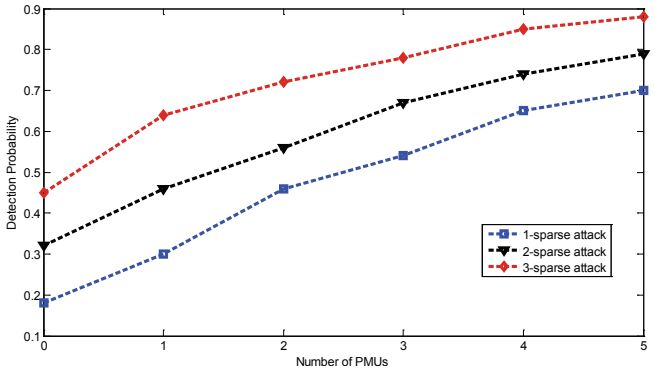
Case 1: The control center is assumed to use the proposed model for SE and bad data detection (LNR detector is used), while the hacker uses a pure DC model to launch FDIA.

Case 2: The strategy for the control center is same as Case 1, but the hacker uses the proposed general model to launch FDIA.

Different numbers of PMUs are installed in the IEEE 14-bus system, i.e., no PMUs installed, one PMU installed at bus 2, two PMUs installed at buses 2 and 4, three PMUs installed at buses 2, 6 and 7, four PMUs installed at buses 2, 6, 7 and 9, and five PMUs installed at buses 2, 6, 7, 9 and 10. Note that the deployment of four PMUs can ensure the system observable. Two false alarm probabilities, 0.05 and 0.1, are considered; several cases of sparsity of the attack,i.e., 1 sparsity case (1-sparse attack), 2 sparsity case (2-sparse attack) and 3 sparsity case (3-sparse attack), defined in [4], are simulated. Simulation results are shown in Fig.1 and



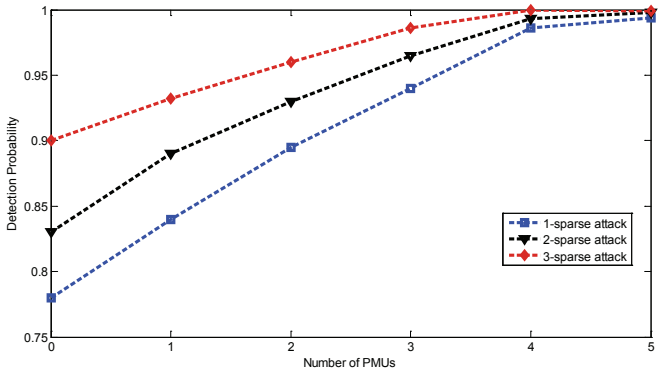
(a) Case 1: DC model based-FDIA



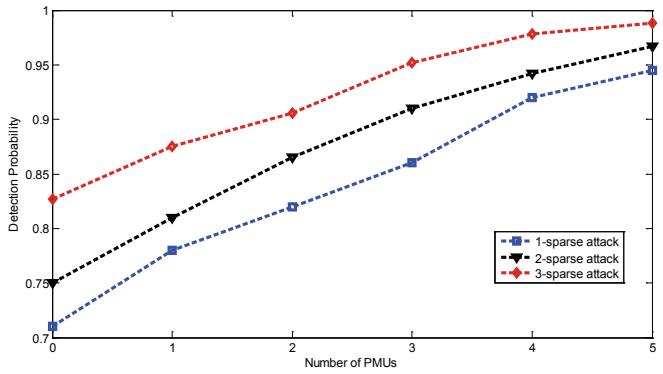
(b) Case 2: Proposed general model based-FDIA

Fig. 1. The detection probability versus different numbers of PMUs under different linear models, where the false alarm probability is 0.05.

Fig.2. As it is expected that with the increase number of the deployed PMUs, the detection probability increases. On the other hand, the growth in the number of the attacked measurements will cause the rise of detection probability. This is because that if more measurements are attacked, the state inconsistences between the forecasted values and the estimated values increase, resulting in higher probability to be detected by the control center. It is interesting to find that thanks to the installation of PMUs, the proposed model-based FDIA has lower probability to be detected by the control center compared with the commonly used pure DC model-based FDIA. Another observation is that when the number of the installed PMUs is able to make the system observable, the attacks are more vulnerable to be detected, e.g., for 3-sparse attack in Fig.1(a), when the deployed number of the PMUs is four, the detection probability is 99.6%, whereas, the value in Fig.1(b) is 87.6%. This indicates that when the PMU measurements are available, the operator can use the slightly modified linear measurement model-based detection method to detect FDIA with higher probability. For the hacker, he should try his best to acquire system PMU configuration information to perform more efficient FDIA. Finally, by the comparisons between Fig.1 and Fig.2, one can find that with the increased false alarm probability, the detection probability rises to a much higher level.



(a) Case 1: DC model based-FDIA



(b) Case 2: Proposed general model based-FDIA

Fig. 2. The detection probability versus different numbers of PMUs under different linear models, where the false alarm probability is 0.1.

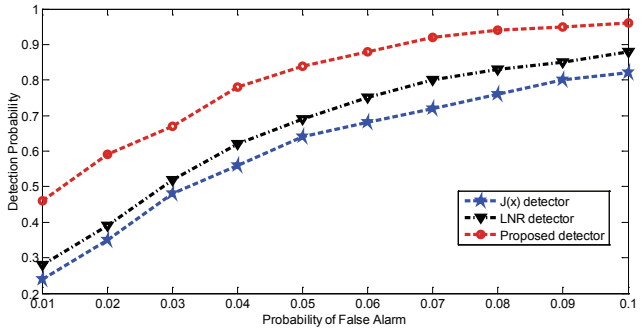


Fig. 3. Scenario 1: ROC performance comparisons results for the three different detectors in IEEE 14-bus system with 2-sparse attack

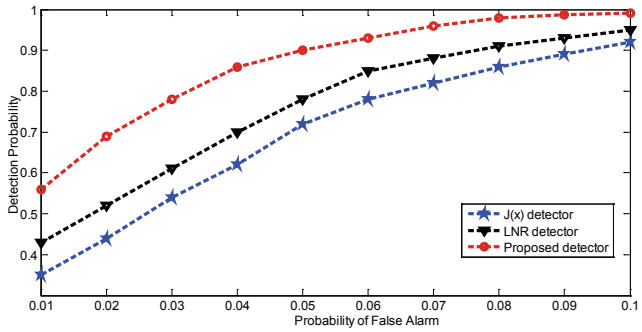


Fig. 4. Scenario 1: ROC performance comparisons results for the three different detectors in IEEE 118-bus system with 10-sparse attack

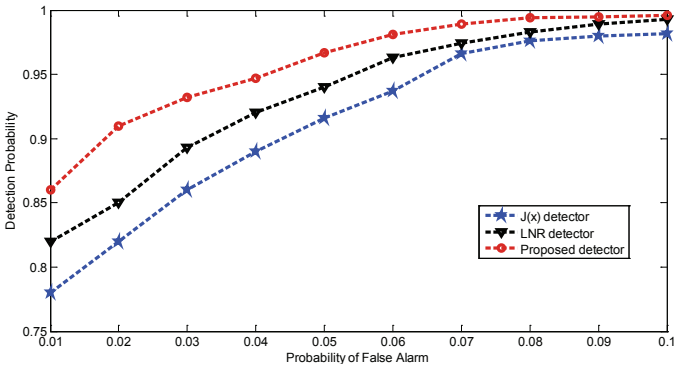


Fig. 5. Scenario 2: ROC performance comparisons results for the three different detectors in IEEE 14-bus system with 2-sparse attack

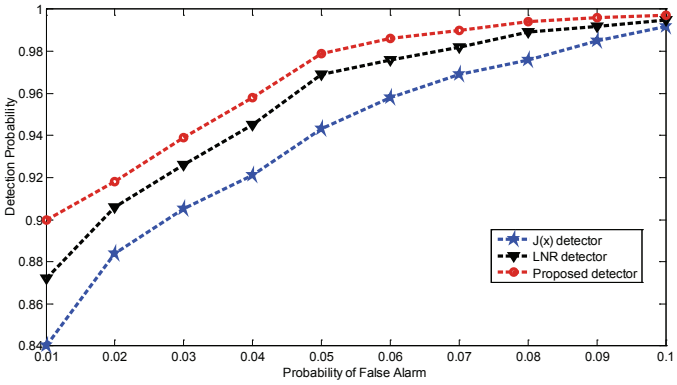


Fig. 6. Scenario 2: ROC performance comparisons results for the three different detectors in IEEE 118-bus system with 10-sparse attack

B. Performance of Proposed Detector

2-sparse attack is simulated on IEEE 14-bus test system, whereas, 10-sparse attack is applied to 118-bus test system, where perturbation 20% is added to the attacked state variables. Both the control center and hacker use the proposed general linear measurement model. The following two scenarios are considered, i.e.,

Scenario 1: two PMUs are installed at buses 2 and 6 for IEEE 14-bus system, while 19 PMUs are installed for IEEE 118-bus system, allowing system partially observable. The detailed measurements placement and topology can be found in [31].

Scenario 2: four PMUs are installed at buses 2, 6, 7 and 9 for ensuring IEEE 14-bus system observability, while 28 PMUs are installed for IEEE 118-bus system, allowing system to be observable [33].

Figures 3–6 show the receive operator characteristic curves (ROC) [4] that characterize the trade-off between the probability of attack detection and the probability of false alarm for the three detectors in IEEE 14-bus and 118-bus test systems, respectively. It can be clearly seen from Figures 3–6 that the proposed detector outperforms the other two classical ones for a wide range of probabilities of false alarm since the prior forecasted measurements and the combined detector can greatly contribute to the FDIAs detection. On the other hand, even under relative small false alarm probability conditions,

the proposed method can effectively detect the attacks with relatively high probability. Comparisons between scenario 1 and scenario 2 indicate that it is very hard for the hacker to launch successful FDIAs when system is observable through PMUs because the measurement model deviations between the hacker and the operator become large. In other words, the operator can get a more accurate linear measurement model through secure PMU measurements whereas the hacker is only able to get limited PMU information (his attack model is the combination of approximate DC model and linear PMU measurement model for PMU observable area), which makes the attacks be detected with higher probability. One more interesting observation here is that the placement of PMUs is helpful for detecting FDIA. But, how many PMUs are needed to maximize the detection probability for a given power network? This is an optimization problem and will be further investigated in the forthcoming paper.

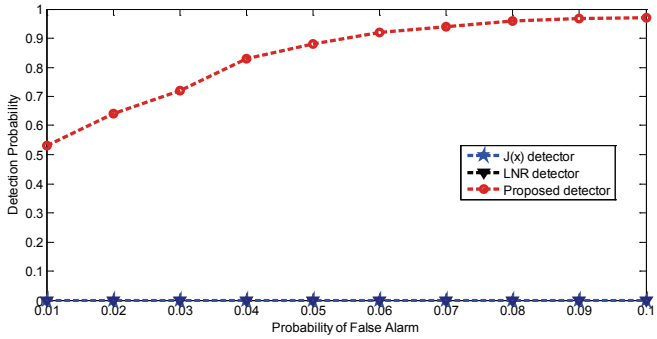
C. Detection of False Critical Measurements Injection Attacks

For the IEEE 14-bus test system, 20 SCADA measurements are used, including 15 power flows, 4 power injections, and 1 bus voltage magnitude at bus 1, whose detailed measurement configuration and topology can be found in [34]. P_{1-2}, P_{7-8} and P_3 are critical measurements through the critical measurements detection method. Two cases are considered:

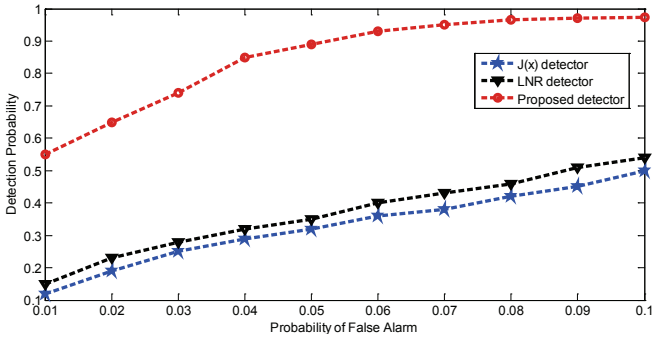
Case 3: No PMU is installed and three critical measurements are compromised;

Case 4: One PMU is installed at bus 1 (the attacker may not realize this situation) and the three critical measurements are compromised.

In both cases, the FDIA and detection are based on the proposed model. Fig.7 shows the detection probability versus false alarm probability for cases 3 and 4. In case 3, both $J(x)$ and LNR detectors fail, as remarked and analyzed in Section III-C. However, the proposed detector is able to handle such attacks with a reasonable detection probability. This is because the injected false data break down the consistency between the forecasted measurements and the received measurements under system normal operation condition, making the attacks detectable. On the other hand, it is worth noting that the detection probability increases when PMUs are installed close to critical measurements buses (i.e. at the same bus or at a bus directly connected to the critical one). To be specific, in case 4, when one PMU is installed at bus 1, critical measurement P_{1-2} becomes noncritical since redundant measurements from PMU are introduced. Thus, the attacks on the critical measurements will be detected with higher probability (the attacker may not know that the control center has installed new PMU devices. Therefore, he may still launch the attacks on critical measurements according to the previous measurement configuration). This motivates the control center to deploy the optimal number of secure PMUs to maximize the FDIA detection probability with some extra investments. In addition, one can observe that under both cases, the detection performance of the proposed detection method is slightly affected. This means that the control center is able to obtain satisfactory FDIA detection probability using the proposed detector without additional PMUs investments.



(a) Case 3: No PMUs



(b) Case 4: One PMU at bus 1

Fig. 7. The detection probability versus false alarm for cases 3 and 4

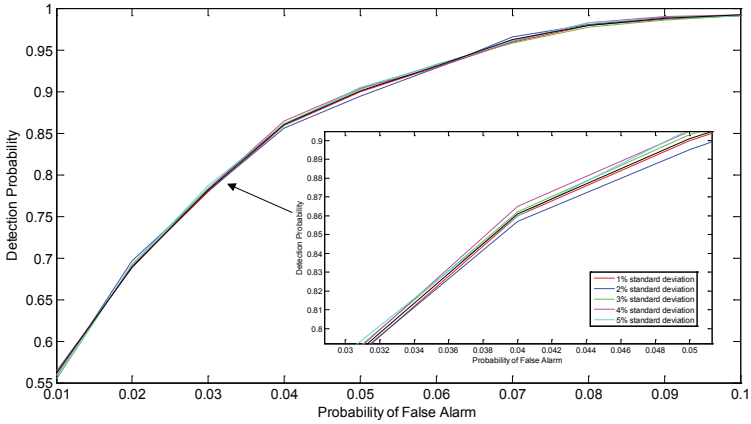


Fig. 8. Sensitivity assessment of proposed method for scenario 1 with 10-sparse attack

D. Sensitivity Assessment

In order to investigate the effects of state forecasting error on detection performance under system normal operation conditions, the sensitivity study is conducted. Instead of adding Gaussian noise with zero mean and 1% standard deviation to the load curve, we vary the standard deviation for the Gaussian noise imposed on the load curve from 1%-5% to test the sensitivity of proposed method. The scenario 1 for IEEE 118-bus test system in Section IV-B is taken as an example. Figure. 8 presents the sensitivity study of proposed method for scenario 1 with 10-sparse attack. It can be observed from this figure that with the increased load variation magnitudes, the FDIA detection probability varies slightly since

TABLE I
COMPUTATION EFFICIENCY FOR PROPOSED METHOD UNDER DIFFERENT SCENARIOS

Scenario	IEEE 14-bus	IEEE 118-bus
Scenario 1	0.095s	0.754s
Scenario 2	0.109s	0.783s

the state forecasting errors change a little bit in different load conditions, resulting in affecting the detection performance. However, the detection performance is excellent and similar to the case where Gaussian noise with zero mean and 1% standard deviation is added for load curve. This confirms that when the system operates under normal conditions, the proposed method can be a good back-up scheme for aiding the conventional residual- based bad data analysis method to detect and process FDIA.

E. Assessment of Computational Efficiency

In this subsection, the computational efficiency of the proposed method in multiple cases are presented. In the proposed method, once the historical system state information from the previous state estimation is available, the short-term state forecasting is performed. The proposed FDIA detection metric is then used to detect whether FDIA exists or not. If no FDIA is detected, the estimation is reliable and used for EMS applications. Otherwise, the FDIA exists and the attacked measurements are replaced by the forecasted measurements, followed by the re-execution of state estimation to get the accurate estimation results. Table I presents the computing times for the scenarios 1 and 2 in Section IV-B including the computing times for state forecasting, FDIA detection and processing, and the final SE execution. As observed from this table, we can find that when the system is PMU observable, the computing time is a little bit larger than the PMU partial observable system since the introduction of additional PMU would increase the dimension of the measurement matrix, thus requires additional computing time. On the other hand, it is obvious that the computing time for the proposed method is considerably acceptable and can be compatible with real-time application.

V. CONCLUSION AND FUTURE WORK

A general linear measurement model is derived to handle both SCADA and PMU measurements. The generic FDIA based on this model is derived and the error tolerance of such attacks is analyzed. Then, the short-term state forecasting method considering temporal correlation is used to exploit the measurement consistency between the forecasted measurements and the received measurements. This measurement consistency test is further integrated with the ∞–norm and the L_2-norm-based measurement residual analysis to construct the proposed detection metric. The shortcoming of previous detectors in terms of handling critical measurements is effectively solved by the proposed detector. In addition, the system observability issue caused by removal of the attacked measurements is addressed. Numerical test results on IEEE 14-bus and 118-bus test systems show that the proposed method outperforms the two well established detection schemes, the $J(\boldsymbol{x})$ detector and LNR detector.

As verified in many papers ([15], [18], [19] for example) that the forecasted information can be used to effectively detect the topology error, it is thus expecting that the proposed method is able to handle the topology attack. Besides, the load redistribution attack changes the power flow distribution while maintaining the whole power flow balanced. However, changing of the specific power flow may also violate the consistency between the forecasted power flow and the measured power flow, resulting in detection of the attack. To investigate the ability and performance of handling these two kinds of attacks will be part of our future work. Besides, as indicated in [35] that the statistic-based anomaly detection may fail in few cases, it is thus important to investigate how to enhance the FDIA detection ability using statistic-based detection method in these cases.

VI. ACKNOWLEDGEMENTS

The authors would like to thank Prof. Lamine Mili, Dr. Srivats, Dr. Marcos at Virginia Tech and Prof. Robson C. Pires at UNIFEI for valuable discussions and suggestions.

REFERENCES

[1] A. Monticelli, "Electric power system state estimation," *Proc. IEEE*, vol. 88, no. 2, pp. 262–282, Feb. 2000.
[2] Y. Liu, P. Ning, M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Trans. Information and System Security*, vol. 14, no. 1, pp. 1-33, 2011.
[3] S. Cui , Z. Han, S. Kar, T. T. Kim, H. V. Poor, and Ali Tajer, "Coordinated data-injection attack and detection in the smart grid: A detailed look at enriching detection solutions," *IEEE Signal Process. Mag.,* vol. 29, no. 5, pp. 106–115, 2012.
[4] O. Kosut, L. Jia, R. J. Thomas, L. Tong, "Malicious data attacks on the smart grid," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 645–658, 2011.
[5] J. Kim, 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, 2013.
[6] Y. Y. Ling, L. Z. Y, R. Kui, "Modeling load redistribution attacks in power systems," *IEEE Trans. Smart Grid*, vol. 2, no. 2, pp. 382–390, 2011.
[7] H. Sandberg, A. Teixeira, K. H. Johansson, "On security indices for state estimators in power networks," presented at the 1stWorkshop Secure Control Syst. (CPSWEEK), Stockholm, Sweden, Apr. 2010.
[8] T. T. Kim , H. V Poor, "Strategic protection against data injection attacks on power grids," *IEEE Trans. Smart Grid*, vol. 2, no. 2, pp. 326–333, 2011.
[9] L. C. Liu, M. Esmalifalak, Q. F. Ding, V. A. Emesih, H. Zhu, "Detecting false data injection attacks on power grid state estimation by sparse optimization," *IEEE Trans. Smart Grid*, vol. 5, no. 2, pp. 612–620, 2014.
[10] K. L. Morrow, E. Heine, K. M. Rogers, R. B. Bobba, T. J. Overbye. Topology perturbation for detecting malicious data injection. In: *The 45th System Science conference*. Hawaii, USA; 2012. p. 2104–13.
[11] M. A. Rahman, H. Mohsenian-Rad, "False data injection attacks within icomplete information against smart power grids," in Proc. IEEE GLOBECOM, 2012.
[12] R. B. Bobba, K. M. Rogers, Q. Wang, H. Khurana, T. J. Overbye. Detecting false data injection attacks on DC state estimation. In: Proceedings of the first workshop on Secure Control Systems. Stockholm, Sweden; 2010. p. 226–231.
[13] A. Giani, E. Bitar, M. Garcia, M. McQueen, P. Khargonekar, K. Poolla. Smart grid data integrity attacks. *IEEE Trans. Smart Grid*, vol. 4, no. 3, pp. 1244–1253, 2013.
[14] A. Abur, A. Gomez Exposito, *Power System State Estimation: Theory and Implementation*. Marcel Dekker, Inc.: New York, 2004.

[15] Y. F. Huang, S. F. Werner, J. Huang, N. Kashyap, V. Gupta, "State estimation in electric power grids," *IEEE Signal Proc Mag.* Vol. 29, no. 5, pp. 33–43, 2012.

[16] H. M. Merrill and F. C. Schweppe, "Bad data suppression in power system state estimation," *IEEE Trans. Power Apparatus and Systems*, vol. PAS-90, pp. 2718–2725, 1971.

[17] Y. Mo, B. Sinopoli, "Secure control against replay attacks," in 47th Annual Conference on Communication, Control, and Computing, 2009, Allerton, pp: 911–918.

[18] M. B. Do Coutto Filho, J. C. Stacchini de Souza, "Forecasting-aided state estimation–Part I: Panorama," *IEEE Trans. Power Syst.,* vol. 24, no. 4, pp. 1667–1678, 2009.

[19] J. B. Zhao, G. X. Zhang, M. L. Scala, "PMU based robust dynamic state estimation method for power systems," in *Proc. IEEE Power Eng. Soc. General Meeting*, 2015: 26–30.

[20] M. D. Ilic, L. Xie, U. A. Khan, J. M. F. Moura. "Modeling Future Cyber-Physical Energy Systems," in *Proc. of Power and Energy Society General Meeting*, 2008.

[21] S. Deshmukh, N. Balasubramaniam, A. Pahwa, "State estimation and voltage/VAR control in distribution network with intermittent measurements," *IEEE Trans. Smart Grid*, vol. 5, no. 1, pp. 200–209, Jan. 2014.

[22] M. B. Do Coutto Filho, J. C. Stacchini de Souza, M . A. R. Guimaraens, "Enhanced bad data processing by phasor-aided state estimation," *IEEE Trans. Power Syst.*, no. 99, pp. 1–10, 2014.

[23] J. B. Zhao, G. X. Zhang, M. L. Scala, J. H. Zhang, "Multistage phasoraided bad data detection and identification," in *Proc. IEEE Power Eng. Soc. General Meeting*, July. 26-30, 2015.

[24] P. Tamburello, L. Mili, "New Robust Estimators of Correlation and Weighted Basis Pursuit," *IEEE Trans. Signal Processing*, Vol. 63, no. 4, pp. 882–894, 2015.

[25] Y. C. Li, Y.L . Wang, "State summation for detecting false data attack on smart grid," *Int J Electr Power Energy Syst*, vol. 57, pp. 156–163, 2014.

[26] O. Kosut, L. Jia, R. J. Thomas, L. Tong, "Limiting false data attacks on power system state estimation," in *Proceedings of the 44th Annual Conference on Information Sciences and Systems*, 2010: 1–6.

[27] J. Sheil and I. O' Muircheartaigh, "The distribution of non-negative quadratic forms in normal variables," *Journal of the Royal Statistical Society, Series C (Applied Statistics)*, Vol. 26, no. I, pp. 92–98, 1977.

[28] H. V. Poor. *An introduction to signal detection and estimation*. Springer Science and Business Media, 2013.

[29] IEEE Std. C37.118.2011–1, *IEEE Standard for Synchrophasor Measurements for Power Systems*, revision of the IEEE Std. C37.118.2005, Dec. 2011.

[30] A. Simoes Costa, A. Albuquerque, and D. Bez, "An estimation fusion method for including phasor measurements into power system real-time modeling," *IEEE Trans. Power Syst.*, vol. 28, no. 2, pp.1910–1920, May 2013.

[31] A. Tarali, A. Abur, "Bad data detection in two-stage state estimation using phasor measurements," in *Proceedings of the 3rd IEEE PES Innovative Smart Grid Technologies Conference*, 2012: 1–8.

[32] Bonneville Power Administration, Wind Generation & Total Load in the BPA Balancing Authority, http://transmission.bpa.gov /business/operations/wind, 2011.

[33] B. Milosevic, M. Begovic, "Non-dominated sorting genetic algorithm for optimal phasor measurement placement," *IEEE Trans. Power Syst.,* vol. 18, no. 1, pp. 69–75, 2003.

[34] A. Aditya, M. Govindarasu, "Cyber attacks on power system state estimation through topology errors," in *Proc. IEEE Power Eng. Soc. General Meeting*, 2012: 1–8.

[35] D. Hadžiosmanović, R. Sommer, E. Zambon, P. H. Hartel, "Through the eye of the PLC: semantic security monitoring for industrial processes," *Proceedings of the 30th Annual Computer Security Applications Conference*, 2014, pp. 126–135.

Junbo Zhao (S'13) is pursuing the Ph.D. degree at the Bradley Department of Electrical Computer Engineering, Virginia Polytechnic Institute and State University, USA. His research interests are in the theoretical and algorithmic studies in power system state estimation, power system operation and control, signal processing.

Gexiang Zhang (M'03), received Ph.D. degree in 2005 from Southwest Jiaotong University, Chengdu, China. Since the year of 2005, he has been a Professor at the School of Electrical Engineering in Southwest Jiaotong University, where he leads the research group of Nature-Inspired Computation and Smart Grid (NICSG).

His research interests include natural computing and smart grid. He has published over 100 scientific papers in international journals or conferences. He was selected as "New Century Excellent Talents in University" from Chinese Ministry of Education.

Massimo La Scala (M'88–SM'99–F'07) received the B.S. and Ph.D. degrees in electrical engineering from the University of Bari, Bari, in 1984 and 1989, respectively.

He is currently Professor of Electrical Energy Systems and Director of Lab ZERO, a lab for the development of sustainable technologies in smart cities, at the Politecnico di Bari, Italy. His research interests are in the area of power system analysis and control, smart grids, sustainable and smart cities.

Zhao Yang Dong (M'99–SM'06) obtained Ph.D. from the University of Sydney, Australia in 1999. He is now a Professor and Head of School of Electrical and Information Engineering, University of Sydney, Australia. His research interest includes Smart Grid, power system planning, power system security, load modeling, electricity market, and computational intelligence and its application in power engineering.

Prof. Dong is an editor of the IEEE TRANSACTIONS ON SMART GRID, the IEEE TRANSACTIONS ON SUSTAINABLE ENERGY, IEEE POWER ENGINEERING LETTERS, and IET Renewable Power Generation.

Jianhui Wang (M'07–SM'12)received the Ph.D. degree in electrical engineering from the Illinois Institute of Technology, Chicago, IL, USA, in 2007.

He is currently a Section Lead for Advanced Power Grid Modeling at the Energy Systems Division, Argonne National Laboratory, Argonne, IL, USA. He is also an Affiliate Professor at Auburn University, Auburn, AL, USA, and an Adjunct Professor at the University of Notre Dame, Notre Dame, IN, USA.

Dr. Wang is the Secretary of the IEEE Power and Energy Society (PES) Power System Operations Committee. He was the Chair of the IEEE PES Power System Operation Methods Subcommittee for six years. He is an Editor-in-chief of IEEE TRANSACTIONS ON SMART GRID and an Editor of the IEEE TRANSACTIONS ON POWER SYSTEMS, an Associate Editor of the *Journal of Energy Engineering*, an Editor of the *IEEE PES LETTERS*, and an Associate Editor of *Applied Energy*. He is an IEEE PES Distinguished Lecturer.

Chen Chen (M'13) received the B.S. and M.S. degrees in electrical engineering from Xi' an Jiaotong University, Xian, China, in 2006 and 2009, respectively, and the Ph.D. degree in electrical engineering from Lehigh University, Bethlehem, PA, USA, in 2013.

He is currently a Post-Doctoral Researcher with the Energy Systems Division, Argonne National Laboratory, Argonne, IL, USA. His current research interests include optimization, communications, and signal processing for smart electricity systems.