Robust Detection of Cyber Attacks on State Estimators Using Phasor Measurements

Junbo Zhao, *Student Member, IEEE*, Gexiang Zhang, *Member, IEEE*, and Rabih A. Jabr, *Fellow, IEEE*

***Abstract*—This letter proposes a statistical consistency check based imperfect false data injection attacks detector that is more effective than the conventional residual-based methods. It is shown that the proposed detector could detect attacks with high probability by using a limited number of secure PMU measurements even if the probability of false alarm is low. Numerical results validate its effectiveness and practicability.**

***Index Terms*—Phasor measurements, power system security, robustness, state estimation.**

I. Introduction

TO defend against false data injection attacks (FDIAs), various measurement protection based methods have been proposed. The aim of protecting a subset of measurements is to make the perfect FDIAs [1] completely impossible [2], [3] and at the same time to increase the cost for a hacker to successfully launch imperfect FDIAs. Note that an imperfect FDIA cannot keep the measurement residual unchanged, thus increasing its possibility of being detected by the control center. However, good imperfect FDIAs do not increase the measurement residual too much and the attacked largest normalized residual does not violate the bad data detection threshold. Thus, imperfect FDIAs are still very challenging for the conventional measurement residual-based bad data detection methods [2], [4], [5].

This letter proposes an imperfect FDIAs detector based on a statistical consistency check using modified projection statistics with a limited number of secure measurements. To accomplish the statistical test, two independent state estimations are performed: (i) the secure PMU measurements based robust state estimation and (ii) the hybrid state estimation that processes the remaining SCADA and PMU measurements. The robust projection statistics algorithm is then used for checking the statistical consistency of the estimation results from the two independent estimators, and consequently to determine whether FDIAs exist or not. To the best of our knowledge, there is little work on developing an effective imperfect FDIAs detector.

II. Method for Attack Detection

A. Problem Formulation

For a power system, the state estimation using a linear or linearized measurement model is:

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

where $\boldsymbol{z}$ and $\boldsymbol{x}$ are the measurement vector and state vector, respectively; $\boldsymbol{H}$ is the Jacobian matrix that relates the measurements to the state variables; and $\boldsymbol{e}$ is a measurement error vector that is assumed to be normally distributed with zero mean and covariance matrix $\boldsymbol{R}$, i.e., $\boldsymbol{e} \sim \mathcal{N}(\boldsymbol{0}, \boldsymbol{R})$. Define $\boldsymbol{W} = \boldsymbol{R}^{-1}$, the state can be estimated by:

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

The commonly used detection algorithms assume the existence of bad measurements as long as the condition $\|\boldsymbol{z} - \boldsymbol{H}\hat{\boldsymbol{x}}\| > \tau$ holds, where τ is a pre-defined detection threshold. However, [1] discovered that if the attack vector $\boldsymbol{a}$ is of the form: $\boldsymbol{a} = \boldsymbol{H}\boldsymbol{c}$ (also called a perfect FDIA), then the attacker will bypass the detection algorithm. The key idea behind perfect FDIAs is to ensure that the measurement residual is unchanged so as to be undetectable by the measurement residual-based detectors. It is almost impossible for any hacker to launch such perfect FDIAs against practical power systems because the hacker is restricted to limited access to system information mainly due to measurement protection schemes and data authentication [3]. However, the imperfect FDIAs [2], [4], [5] still pose great challenges to the conventional bad data detection methods. In this letter, a robust detector that makes use of limited PMU measurements is proposed to handle imperfect FDIAs.

B. The Proposed Detector

Recall that the objective of an attacker is to alter the estimation results by injecting malicious measurements. In other words, once some measurements are compromised, the distribution of the estimated state vector would be perturbed by the attack [6]. If one could find a set of measurements that can produce a close approximation to the true estimated state vector and its distribution, then this statistical information can be further used to double check the estimation results obtained from the remaining measurements. This can be done first by leveraging a small subset of secure PMU measurements, which make the system observable, to obtain the estimation results. A statistical consistency check is then performed between the secure PMU measurements based robust estimation and the hybrid state estimation that uses the remaining SCADA and PMU measurements, to determine whether FDIAs exist or not. Therefore, the challenging issue is how to perform the statistical consistency check effectively.

In this letter, a robust projection statistics algorithm-based detector for the state statistical consistency check is proposed. Note that here, the state estimation model itself is an approximate model with parameter uncertainty, measurement bias, topology uncertainty, etc. Thus, a high measurement redundancy is required to get the system approximate true state. This motivates the need to use and correct the remaining SCADA and PMU measurements that contribute to system measurement redundancy improvement and system visualization.

By partitioning the measurement vector and the Jacobian matrix into two parts, i.e, $\boldsymbol{z} = \left[\boldsymbol{z}_p^T\ \boldsymbol{z}_l^T\right]^T$, $\boldsymbol{H} = \left[\boldsymbol{H}_p^T\ \boldsymbol{H}_l^T\right]^T$, and defining the $\hat{\boldsymbol{x}}_p$ and $\hat{\boldsymbol{x}}_l$ as the estimated state vectors by using secure PMU measurements and the remaining SCADA and PMU measurements, respectively, we obtain the following formulations:

$$\hat{\boldsymbol{x}}_p = \left({\boldsymbol{H}_p}^T\boldsymbol{W}_p\boldsymbol{H}_p\right)^{-1}{\boldsymbol{H}_p}^T\boldsymbol{W}_p\boldsymbol{z}_p, \tag{3}$$

$$\hat{\boldsymbol{x}}_l = \left({\boldsymbol{H}_l}^T\boldsymbol{W}_l\boldsymbol{H}_l\right)^{-1}{\boldsymbol{H}_l}^T\boldsymbol{W}_l\boldsymbol{z}_l, \tag{4}$$

This work was supported in part by the National NSFC under Grants 61170016 and 61373047. The work of J. Zhao was supported by the CSC under Grant 201407000013.*Corresponding author*: Gexiang Zhang

J. Zhao and G. Zhang are with the School of Electrical Engineering, Southwest Jiaotong University, Chengdu 610031, China. J. Zhao is also with 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; zhgxdylan@126.com).

R. A. Jabr is with the Department of Electrical and Computer Engineering, American University of Beirut, Beirut 1107 2020, Lebanon (e-mail: rabih.jabr@aub.edu.lb).

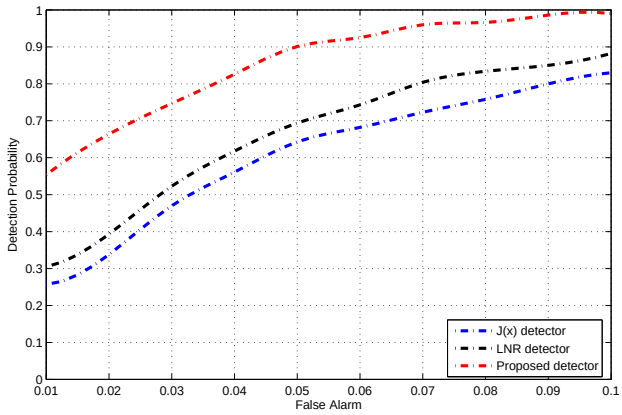

Fig. 1. ROC curves for the proposed robust detector on the IEEE 118-bus test system

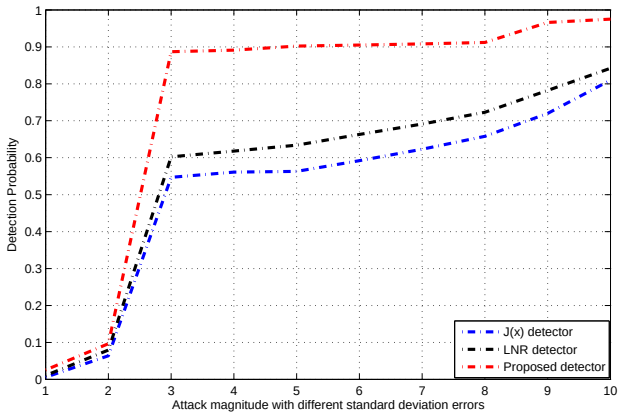

Fig. 2. Sensitivity of the proposed robust detector for different state attack magnitudes

where the subscripts p and l denote the secure PMU measurements and the remaining measurements; the weight matrix $\boldsymbol{W}_l$ is determined from the measurement variances, while $\boldsymbol{W}_p$ is determined using the robust scale and the Huber ψ function [7] for handling the possible occurrence of bad data in secure PMU measurements. The number of secure PMU measurements is determined by the method in [3].

Proposed detector based on robust projection statistics: To effectively perform the statistical consistency check, this paper proposes to apply projection statistics (PS) to the matrix $\boldsymbol{X} = [\widehat{\boldsymbol{x}}_p \ \widehat{\boldsymbol{x}}_l]^T$. The PS of the ith row vector, $\boldsymbol{\ell}_i$ in $\boldsymbol{X}$, is defined as the maximum of the standardized projections of all the $\boldsymbol{\ell}_i$'s on every direction $\boldsymbol{l}$ that originates from the coordinatewise medians that pass through every data point, and where the standardized projections are based on the sample median and the median-absolute-deviation [7]. Formally we have

$$PS_i = \max_{\|\boldsymbol{l}\|=1} \frac{\left|\boldsymbol{\ell}_i^T l - med_j\left(\boldsymbol{\ell}_j^T l\right)\right|}{1.4826\ med_k\left|\boldsymbol{\ell}_k^T l - med_j\left(\boldsymbol{\ell}_j^T l\right)\right|}. \quad (5)$$

The reason why PS is applied to matrix $\boldsymbol{X}$ is that $\widehat{\boldsymbol{x}}_p$ with its associated distribution is close to the SE results using non-attacked measurements, and if there is no attack in the remaining SCADA and PMU measurements, then $\widehat{\boldsymbol{x}}_l$ with its distribution is also close to the SE results; otherwise, the distribution of $\widehat{\boldsymbol{x}}_p$ will deviate from $\widehat{\boldsymbol{x}}_l$. Therefore, by checking the statistics of $\widehat{\boldsymbol{x}}_p$ and $\widehat{\boldsymbol{x}}_l$, the attacks could be identified. In this letter, the states, whose associated PS values satisfy $PS_i > \chi^2_{2,\alpha}$ [7], are marked as attacked states with α confidence in the statistical hypothesis testing; α usually varies between 0.9 and 0.99.

III. Numerical Results

The proposed detector is tested on the 118-bus test system. The number of secure PMUs is chosen according to [3]. The PMU can measure both the bus voltage angles and the power flows on all branches incident to that bus. In the simulation, since it is generally accepted that the precision of PMU measurements is much higher than SCADA measurements, the Gaussian noise for SCADA and PMU measurements are with zero mean and standard deviations 0.01 and 0.001, respectively; it is assumed that the adversary targeted attacking the state variable θ_5 with 8 times standard deviation error (please see [2], [4], [5] for more information about how to construct an imperfect FDIA). The receiver operator characteristic (ROC) curves [4], [6] are used to depict the tradeoff between the two probabilities of attack detection and false alarm. The widely used largest normalized residual (LNR) test based detector and the objective function ($J(\hat{\boldsymbol{x}})$) based detector are employed for comparison; all the tests are based on 100 Monte-Carlo simulations.

Fig. 1 shows the detection probability versus the false alarm probability (ROC curves) for the proposed and classical detectors; it can be observed that the performance of the proposed detector is superior to the traditional ones. Even when the probability of false alarm is low, e.g, 5%, there is more than 90% chance to detect the attacks by using the proposed method. While for the two traditional detectors, even if the probability of false alarm is at 10%, the chance of detecting the attacks does not reach 90%.

To test the sensitivity of the proposed method under different attack scenarios, the attack magnitude is varied from 1 to 10 standard deviations with 0.05 false alarm probability. Fig. 2 presents the simulation results from which it can be observed that the proposed detector has relatively low detection probability to the attacks that introduce less than 3 times standard deviation error, while it has very high detection probability to attacks with more than 3 times standard deviation error. The results of the other two methods have a similar trend, but their detection performances are much lower than the proposed method. The only limitation of the proposed method is that it requires local measurement redundancy to suppress the possible occurrence of bad data in the secure PMU measurements. This is unlikely to be a concern given the high measurement redundancy in transmission networks.

References

[1] Y. Liu, P. Ning, M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Transactions on Information and System Security*, vol. 14, no. 1, pp. 1-33, May 2011.

[2] X. Liu, Z. Li, "False data attacks against AC state estimation with incomplete network information," *IEEE Trans. Smart Grid*, 2016.

[3] 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.

[4] J. B. Zhao, G. X. Zhang, et al, "Short-term state forecasting-aided method for detection of smart grid general false data injection attacks," *IEEE Trans. Smart Grid*, 2015, DOI: 10.1109/TSG.2015.2492827.

[5] J. B. Zhao, G. X. Zhang, Z. Y. Dong, K. P. Wong, "Forecasting-aided imperfect false data injection attacks against power system nonlinear state estimation," *IEEE Trans. on Smart Grid*, Vol. 7, no. 1, pp. 6–8, 2016.

[6] 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.

[7] L. Mili, M. Cheniae, N. Vichare, P. Rousseeuw, "Robust state estimation based on projection statistics," *IEEE Trans. Power Syst.*, vol. 11, no. 2, pp. 1118–1127, May 1996.