This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JESTPE.2019.2936587, IEEE Journal of Emerging and Selected Topics in Power Electronics



# Quickest Detection of False Data Injection Attacks in Smart Grid with Dynamic Models

Samrat Nath*, *Student Member, IEEE*, Israel Akingeneye†, *Member, IEEE*, Jingxian Wu*, *Senior Member, IEEE*, and Zhu Han‡, *Fellow, IEEE*

***Abstract*—A quickest intrusion detection algorithm is proposed to detect false data injection attacks (FDIA) in smart grids with time-varying dynamic models. The quickest detection algorithm aims at minimizing the worst-case detection delays of cyber-attacks, subject to an upper bound of the false alarm rate. Since power grid state transitions could be caused by either cyber-attacks or sudden change in loads or grid configurations, we propose to distinguish between FDIA and sudden system change by using a time-varying dynamic model, which can accurately capture the dynamic state transitions due to changes in system configurations. A dynamic state estimation algorithm is developed to estimate and track the time-varying and non-stationary power grid states. The quickest detection algorithm is developed by analyzing the statistical properties of dynamic state estimations, such that the algorithm minimizes the worst-case detection delay while accurately distinguishing FDIA from sudden system changes. A Markov-chain-based analytical model is used to identify the detector's parameter and quantify its performance. Simulation results demonstrate that the proposed algorithm can accurately detect and remove false data injections or system faults with minimum delays. The proposed algorithm can be implemented to harden intelligent electronic devices or supervisory control and data acquisition systems to improve their resilience to cyber-attacks or system faults, thus improving the cyber-security of smart grids.**

***Index Terms*—False data injection, cyber-attack, dynamic state estimation, dynamic load change, power system.**

## I. Introduction

A smart grid is a combination of electrical power infrastructure, smart meters, and a network of computers [1]. It uses information technologies to make intelligent decisions about the control and state of electrical power systems. Compared to conventional power grids, smart grid is more robust and efficient due to the advancement in system monitoring, energy management, and operation control. However, due to its dependence on cyber-infrastructure, a smart grid is prone to cyber-attacks [1]. Cyber-attacks can be performed by hacking into the communication network of smart grids, or by remotely accessing the remote terminal units (RTUs) installed at the substations [2]. For example, the supervisory control and data acquisition (SCADA) system of Iran's Natanz nuclear fuel-enrichment facility was attacked by a Stuxnet worm in July 2010 [3]. An adversary can launch cyber-attacks by compromising the measurement results obtained by the SCADA system or phasor measurement units (PMUs), such as the power injected into different buses or power flowing into the lines between the buses. False data injected in the measurement results will affect the real-time control of grid operations, thus cause significant damages to power grids. A comprehensive review of false data injection attack (FDIA) against modern power systems is given in [4]. To improve the cyber-security of smart grids, it is critical to ensure the integrity and confidentiality of the intelligent electronic devices (IEDs) in the network such as smart meters, RTUs, PMUs through hardware or software hardening [5]. Tamper-proof hardware platforms can reduce avenues for FDIA.

A large number of algorithms have been developed to detect various forms of cyber-attacks in smart grids [6]–[10]. Most methods assume a static system model, where the system is in steady state and its measurements are quasi-static over time. However, in reality, the state of a power system varies with time due to the dynamic nature of system loads [11]. So, state estimation and FDIA detection algorithms require a dynamic model to track the time evolution of the system states, which can be utilized to detect and replace corrupted measurements in the system. A dynamic state estimator can capture the system transients due to sudden system changes in a faster and more accurate manner compared to its static counterpart. This is possible because of the dynamic state estimator's ability of using past state estimations to predict future state of the system one step ahead. A mismatch between newly collected measurements and their predicted values indicates that there have been sudden changes in the system such as loss of a large load, changes in network configurations, system faults, or malicious attacks that have modified some system measurements. It is vital to detect and identify these attacks as soon as possible in order to replace the corrupted measurements before they are processed by the state estimator.

Dynamic state estimation is important for the control and operations of a power grid [11]–[17]. Dynamic state estimation in many existing works is performed by using different versions of an extended Kalman filter (EKF) to filter predicted state variables [11]–[13]. In [16], FDIA is detected by tracking the dynamics of measurement variations in terms of the Kullback-Leibler divergence [18] between two probability distributions under normal and abnormal conditions. In [17], an online FDIA detection method is developed by analyzing

*S. Nath and J. Wu are with the Department of Electrical Engineering, University of Arkansas, Fayetteville, AR 72701 USA. †I. Akingeneye is with Intel Corporation, San Diego, CA 92131, USA. ‡Z. Han is with the Department of Electrical and Computer Engineering, University of Houston, Houston, TX 77204 USA, and also with the Department of Computer Science and Engineering, Kyung Hee University, Seoul, South Korea, 446-701. Corresponding author: Jingxian Wu (wuj@uark.edu)

This work was supported in part by the U.S. Department of Energy under Grant DE-OE0000779, by the National Science Foundation under Grant ECCS-1711087, and by US MURI AFOSR MURI 18RT0073, NSF CNS-1717454, CNS-1731424, CNS-1702850, CNS-1646607.

temporally consecutive estimated system states using wavelet transform and deep neural network, which can effectively capture deviations in temporal data correlations of state vectors due to FDIA scenarios. Most works utilize the estimation residual, which is the difference between the newly collected measurements and their corresponding predictions, to test the presence of FDIA. If the residual magnitude exceeds a certain threshold, a flag is raised indicating that either there is a sudden system change or FDIA. FDIA is distinguished from sudden system changes by analyzing correlated measurements in the location near the abnormality. In [11], if the measurements from neighboring buses fail the detection test simultaneously, a sudden change is declared. But, such a method might not be effective if false data are simultaneously injected into several neighboring buses with correlated measurements. This may lead to a mischaracterization of the attacks as sudden changes.

Most existing FDIA detection methods are developed to improve detection accuracy, with little or no attention given to detection delay. Detection delay is defined as the time difference between the launch and detection of a cyber-attack. Reducing detection delay is critical for improving cybersecurity [19]. A lower detection delay can shorten the response time so that remedial actions can be taken in a timely manner to significantly reduce the damages and economic losses caused by cyber-attacks. Detection delay can be reduced by employing algorithms from the quickest change detection (QCD) framework [20], which aims at minimizing the average or worst-case detection delays while ensuring high detection accuracy. One of the most commonly used QCD procedure is the cumulative sum (CUSUM) procedure [20], [21]. It has been shown in [22], [23] that the CUSUM algorithm is asymptotically optimum, that is, it can asymptotically minimize the worst-case detection delay (WDD) when the false alarm rate goes to 0. However, implementation of CUSUM requires knowledge of the exact statistical distribution of the measurement under attack, which is usually unknown in practical applications [24]. An adaptive Rao-CUSUM test is proposed in [6] for false data detection in smart grid, where the unknown distribution of data under attack is summarized by using the Rao test statistic [25]. In [19], an orthogonal matching pursuit CUSUM (OMP-CUSUM) algorithm is proposed to identify the buses under attack while minimizing the detection delay. Both [6] and [19] are developed under highly simplified linear static system models and they cannot capture the time-varying transient of power grids.

In this paper, we develop a quickest intrusion detection algorithm for detecting FDIA in smart grids by using dynamic state estimations. This algorithm can be used to harden IEDs, PMUs, or SCADA system to improve their resilience to cyber-attacks or system faults. The detection method is designed to minimize the worst-case detection delay of FDIA subject to an upper bound of the false alarm rate, which is defined as the probability of falsely detecting an FDIA while the system is under normal operating conditions. One of the main challenges faced by FDIA detection is to distinguish power grid state changes caused by FDIA from those caused by a sudden system change, such as sudden load changes on certain buses. To address this challenge, we propose to use a locally linear but globally non-linear dynamic state model to represent the dynamic state transitions in power grids. The dynamic state evolution of the power grid is estimated and tracked by using an EKF-based dynamic state estimator, which estimates the current state by using both current measurements and predictions from past states. A sudden system change will affect the dynamic state transitions on all buses based on the physical model of the grid, and such state transitions can be accurately estimated by the dynamic state estimator based on SCADA or PMU measurements. On the contrary, FDIA or system faults might violate the dynamic state transitions determined by the model, and this may result in large residuals in estimation. Thus the employment of the dynamic state models can help distinguish FDIA from sudden system change.

The quickest intrusion detection algorithm is developed by analyzing the statistical properties of the results obtained from dynamic state estimations. The problem is formulated as a hypothesis test performed on the residuals between the estimated and actual measurements. Since the false data attack vector is unknown at the detector, we propose a new normalized Rao-CUSUM test, which summarizes the unknown statistics of post-attack distributions by using a normalized Rao test statistic. Simulation results show that the normalization of Rao test statistic yields significantly lower FAR compared to un-normalized Rao test statistic under the same detection delay. The design parameter of the test is identified by using a Markov-chain based model of the test statistics through offline calculations. Once FDIA is detected, corrupted measurements are identified and replaced with their predicted values to ensure normal operations of the grid.

To summarize, this work has two main contributions. First, the detection algorithm aims at minimizing the worst-case detection delay of FDIA while ensuring high detection accuracy. The quickest detection algorithm is developed by using a new normalized Rao-CUSUM test that can accurately detect FDIA in a timely manner. Second, with a dynamic model and dynamic state estimations, the quickest detection algorithm can distinguish state transitions caused by FDIA from those caused by sudden system change, thus ensure the normal operations of the grid under both conditions.

The remainder of this paper is organized as follows. Section II describes the system model and problem formulation. The dynamic model and dynamic state estimation are presented in Section III. In Section IV, we develop the quickest detection algorithm by analyzing the statistical properties of the results from dynamic state estimations. In Section V, a Markov-chain-based model is introduced to analytically evaluate the proposed false data detector. Simulation results are given in Section VI, and Section VII concludes this paper.

## II. System Model

A power system with $N$ buses is considered. Without loss of generality, the first bus is assumed to be the reference. Define the set of buses connected to bus $i$ as $\mathcal{X}_i$ with cardinality $c_i = |\mathcal{X}_i|$. Denote the active and reactive power injections into bus $i$ as $P_i$ and $Q_i$, respectively. Similarly, the active and reactive power flows from bus $i$ to bus $j$ are denoted $P_{ij}$ and $Q_{ij}$, respectively, $\forall\ j \in \mathcal{X}_i$.

The power system collects measurements of both active and reactive power flows on different buses. The measurements are collected in such a way that the system becomes observable, i.e. all the state variables can be determined from the measurements. There are many optimal approaches for sensor placement in order to make the system completely observable through collected measurements [26]. The power system provides a total of $m = m_1 + m_2 + 1$ measurements, where $m_1 = 2N$ is the number of active and reactive power injections, $m_2 = \sum_{i=1}^{N} |\mathcal{X}_i|$ is the number of active and reactive power flows. In addition to the power measurements, the measurement of the voltage magnitude at the reference bus is also available. Define the measurement vector as $\mathbf{z} = [z_1, z_2, \cdots, z_m]^T \in \mathcal{R}^{m\times 1}$, where $(\cdot)^T$ is the matrix transpose operator and $\mathcal{R}$ is the set of real numbers.

Define the state vector as $\mathbf{x} = [x_1, x_2, \ldots, x_n]^T \in \mathcal{R}^{n\times 1}$ for $n = 2N - 1$, where the first $N - 1$ elements of $\mathbf{x}$ are the voltage angles of $N - 1$ non-reference buses and the last $N$ elements are the voltage magnitudes of $N$ buses.

The relationship between the measurement vector $\mathbf{z}_k$ and the state vector $\mathbf{x}_k$, at an instant of time $k$ is expressed as

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

where $\mathbf{h}(\mathbf{x}_k) = [h_1(\mathbf{x}_k), \ldots, h_m(\mathbf{x}_k)]^T$ is a nonlinear function between the measurement vector $\mathbf{z}_k$ and the system state vector $\mathbf{x}_k$, and $\mathbf{e}_k \in \mathcal{R}^{m\times 1}$ is the measurement error vector at the sampling instant $k$. As shown in [11], we assume that the measurement noise $\mathbf{e}_k$ is zero-mean Gaussian distributed with covariance matrix $\mathbf{R}_k$.

Based on the observations in (1), the state estimator can obtain an estimate $\hat{\mathbf{x}}_k$ of the state variable $\mathbf{x}_k$. The state estimation results can be used to facilitate the detection of FDIA or system faults.

## III. Dynamic State Estimation

In this section, we present a dynamic state estimation algorithm, which relies on previous estimates to predict future states of the system. The predicted states can, in turn, be used by the system operator for timely anomaly detection and other control decisions such as economic dispatch.

Consider the following state transition model, which describes the time behavior of the state vector, as

$$\mathbf{x}_{k+1} = \mathbf{F}_k\mathbf{x}_k + \mathbf{G}_k + \mathbf{w}_k, \tag{2}$$

where $\mathbf{F}_k \in \mathcal{R}^{n\times n}$ is a non-zero diagonal matrix, $\mathbf{G}_k \in \mathcal{R}^{n\times 1}$ is a non-zero column vector, and $\mathbf{w}_k \in \mathcal{R}^{n\times 1}$ is a white Gaussian noise vector with 0 mean and covariance matrix $\mathbf{Q}_k$.

The parameters $\mathbf{F}_k$ and $\mathbf{G}_k$ can be identified according to the Holt's exponential smoothing method [11]. The Holt's method performs smoothing over an original time series with two smoothing parameters, $\alpha$ and $\beta$, with values between 0 and 1. Denote the predicted state vector at time $k$ as $\tilde{\mathbf{x}}_k$. The Holt's method is expressed as

$$\tilde{\mathbf{x}}_{k+1} = \mathbf{a}'_k + \mathbf{b}'_k, \tag{3}$$

$$\mathbf{a}'_k = \alpha\mathbf{x}_k + (1-\alpha)\tilde{\mathbf{x}}_k, \tag{4}$$

$$\mathbf{b}'_k = \beta\left[\mathbf{a}'_k - \mathbf{a}'_{k-1}\right] + (1-\beta)\mathbf{b}'_{k-1}. \tag{5}$$

Combining (3)-(5) yields

$$\tilde{\mathbf{x}}_{k+1} = \mathbf{F}_k\mathbf{x}_k + \mathbf{G}_k, \tag{6}$$

where

$$\mathbf{F}_k = \alpha(1+\beta)\mathbf{I}_n,$$
$$\mathbf{G}_k = (1+\beta)(1-\alpha)\tilde{\mathbf{x}}_k - \beta\mathbf{a}'_{k-1} + (1-\beta)\mathbf{b}'_{k-1}.$$

The time-varying linear dynamic model in (2) can then be obtained by adding a zero mean Gaussian noise $\mathbf{w}_k$ to (6) to account for model uncertainties.

The proposed dynamic state estimator contains two steps: state forecasting and state estimation.

### A. State Forecasting

One main advantage of the dynamic state estimator is its ability to use past state estimates to predict future system states. Let $\hat{\mathbf{x}}_k$ be the estimated state vector at time $k$ and $\mathbf{\Sigma}_k$ its error covariance matrix. The predicted state vector $\tilde{\mathbf{x}}_{k+1}$ and its error covariance matrix $\mathbf{M}_{k+1}$ at time $k$ can be obtained by performing the conditional expectation on (2) as follows

$$\tilde{\mathbf{x}}_{k+1} = \mathbb{E}\left[\mathbf{x}_{k+1} \mid \mathbf{x}_k = \hat{\mathbf{x}}_k\right] = \mathbf{F}_k\hat{\mathbf{x}}_k + \mathbf{G}_k, \tag{7}$$

$$\begin{aligned}\mathbf{M}_{k+1} &= \mathbb{E}\left[\left(\mathbf{x}_{k+1} - \tilde{\mathbf{x}}_{k+1}\right)\left(\mathbf{x}_{k+1} - \tilde{\mathbf{x}}_{k+1}\right)^T \mid \mathbf{x}_k = \hat{\mathbf{x}}_k\right] \\ &= \mathbf{F}_k\mathbf{\Sigma}_k\mathbf{F}_k + \mathbf{Q}_k,\end{aligned} \tag{8}$$

where $\mathbb{E}[.]$ is the expectation operator.

### B. State Estimation

The state estimation, also known as state filtering, seeks to estimate the state at time $k+1$ by using both the predicated state vector, $\tilde{\mathbf{x}}_{k+1}$, obtained at the preceding step $k$, and the newly received measurement vector $\mathbf{z}_{k+1}$ at time $k+1$. During this stage, a new estimate $\hat{\mathbf{x}}_{k+1}$ along with its error covariance matrix $\mathbf{\Sigma}_{k+1}$ are obtained at time $k+1$ by minimizing the objective function

$$\begin{aligned}J\left(\mathbf{x}_{k+1}\right) = &\frac{1}{2}\left[\mathbf{z}_{k+1} - \mathbf{h}(\mathbf{x}_{k+1})\right]^T\mathbf{R}_{k+1}^{-1}\left[\mathbf{z}_{k+1} - \mathbf{h}(\mathbf{x}_{k+1})\right] \\ &+ \frac{1}{2}\left[\left(\mathbf{x}_{k+1} - \tilde{\mathbf{x}}_{k+1}\right)^T\mathbf{M}_{k+1}^{-1}\left(\mathbf{x}_{k+1} - \tilde{\mathbf{x}}_{k+1}\right)\right].\end{aligned} \tag{9}$$

The estimate $\hat{\mathbf{x}}_{k+1}$ that minimizes the objective function in (9) can be obtained through an iterative extended Kalman filter (EKF) [11] as

$$\begin{aligned}\mathbf{x}^{(i+1)} = \mathbf{x}^{(i)} + \mathbf{\Sigma}^{(i)}\{&\mathbf{H}^T(\mathbf{x}^{(i)})\mathbf{R}^{-1}[\mathbf{z} - \mathbf{h}(\mathbf{x}^{(i)})] \\ &- \mathbf{M}^{-1}[\mathbf{x}^{(i)} - \tilde{\mathbf{x}}]\},\end{aligned} \tag{10}$$

where $i$ denotes the iteration counter, $\mathbf{H}(\mathbf{x}) = \frac{\partial\mathbf{h}(\mathbf{x})}{\partial\mathbf{x}}$ is the Jacobian matrix, and

$$\mathbf{\Sigma}^{(i)} = \left[\mathbf{H}^T(\mathbf{x}^{(i)})\mathbf{R}^{-1}\mathbf{H}(\mathbf{x}^{(i)}) + \mathbf{M}^{-1}\right]^{-1}. \tag{11}$$

It should be noted that the subscript $k+1$ was omitted in (10) and (11) for simplicity. The proof for (10) is given in Appendix A.

One main benefit of the state forecasting stage is to provide the initial states to the iterative EKF algorithm in (10). Thus, the convergence of the EKF algorithm partly depends on the accuracy of the forecast state vector. A high state forecasting accuracy leads to a faster convergence of the EKF algorithm.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JESTPE.2019.2936587, IEEE Journal of Emerging and Selected Topics in Power Electronics



## IV. False Data Detection and Identification

The problems of detecting false data injections in the measurement vector and identifying the buses under attack are studied in this section.

Results of the dynamic state estimation will be used in the detection and identification of FDIA. To facilitate the development of the FDIA detection algorithm, let the initial guess $\mathbf{x}^{(i)} = \tilde{\mathbf{x}}$ at time $k+1$ and by performing only one iteration in (10), the estimated state vector is approximated as

$$\hat{\mathbf{x}}_{k+1} = \tilde{\mathbf{x}}_{k+1} + \mathbf{K}_{k+1}\mathbf{v}_{k+1}, \tag{12}$$

where

$$\mathbf{v}_{k+1} = \mathbf{z}_{k+1} - \mathbf{h}(\tilde{\mathbf{x}}_{k+1}) \tag{13}$$

is the residual vector,

$$\mathbf{K}_{k+1} = \mathbf{\Sigma}_{k+1}\mathbf{H}^T(\tilde{\mathbf{x}}_{k+1})\mathbf{R}_{k+1}^{-1} \tag{14}$$

is the gain matrix, and

$$\mathbf{\Sigma}_{k+1} = \left[\mathbf{H}^T(\tilde{\mathbf{x}}_{k+1})\mathbf{R}_{k+1}^{-1}\mathbf{H}(\tilde{\mathbf{x}}_{k+1}) + \mathbf{M}_{k+1}^{-1}\right]^{-1}. \tag{15}$$

To facilitate analysis, write the Taylor series expansion of $\mathbf{h}(\mathbf{x}_{k+1})$ around a linearization point $\tilde{\mathbf{x}}_{k+1}$ as

$$\mathbf{h}(\mathbf{x}_{k+1}) = \mathbf{h}(\tilde{\mathbf{x}}_{k+1}) + \mathbf{H}(\tilde{\mathbf{x}}_{k+1})(\mathbf{x}_{k+1} - \tilde{\mathbf{x}}_{k+1}), \tag{16}$$

where $\mathbf{H}(\tilde{\mathbf{x}}_{k+1}) = \frac{\partial \mathbf{h}(\mathbf{x})}{\partial \mathbf{x}}|_{\mathbf{x}=\tilde{\mathbf{x}}_{k+1}}$.

The higher order terms of (16) are omitted by assuming that the difference $(\mathbf{x}_{k+1} - \tilde{\mathbf{x}}_{k+1})$ is very small.

Combining (1), (13), and (16) gives

$$\mathbf{v}_{k+1} = \mathbf{H}(\tilde{\mathbf{x}}_{k+1})(\mathbf{x}_{k+1} - \tilde{\mathbf{x}}_{k+1}) + \mathbf{e}_{k+1}. \tag{17}$$

The covariance matrix, $\mathbf{S}_{k+1}$, of the residual vector, $\mathbf{v}_{k+1}$, can then be calculated as

$$\mathbf{S}_{k+1} = \mathbf{H}(\tilde{\mathbf{x}}_{k+1})\mathbf{M}_{k+1}\mathbf{H}^T(\tilde{\mathbf{x}}_{k+1}) + \mathbf{R}_{k+1}. \tag{18}$$

Based on (12), the estimated state vector $\hat{\mathbf{x}}_{k+1}$ is a function the residual vector $\mathbf{v}_{k+1}$, the difference between newly received measurements at time $k+1$ and its corresponding predictions $\mathbf{h}(\tilde{\mathbf{x}}_{k+1})$. The newly received measurement vector $\mathbf{z}_{k+1}$ may deviate from its predicated value $\mathbf{h}(\tilde{\mathbf{x}}_{k+1})$. This mismatch between the measured and predicted measurements may be a result of several factors: a sudden change in the system's operating point due to a loss of a large load [12], system faults such as sensor failure or line-to-ground faults, or false data injections in the measurements. The change in the system's operating point is considered as a normal event. However, presence of false data injections is abnormal and can be very harmful to the system. Hence, it is vital to distinguish between state changes due to sudden load change or FDIA, such that false data injections can be detected and removed from the measurements $\mathbf{z}_{k+1}$ before performing state estimations.

We propose a new quickest change detection method by analyzing the statistical properties of the residual vector $\mathbf{v}_{k+1}$. The design criterion of the quickest change detection algorithm is to minimize the worst-case detection delay, subject to the constraint on an upper-bound of the false alarm rate. Specifically, a sudden load change will affect the measurements on all buses based on the physical model of the system. On the other hand, FDIA will only affect the measurements on a few buses. Thus we propose to distinguish between sudden load change and FDIA by analyzing the statistical correlations of signals from different buses.

### A. Formulation of the Hypothesis Test

Define the null hypothesis $\mathcal{H}_0$, which corresponds to the measurements without false data at time $k+1$, and the alternative hypothesis $\mathcal{H}_1$, which corresponds to the measurements with false data at time $k+1$, as

$$\begin{aligned} \mathcal{H}_0 &: \mathbf{z}_{k+1} = \mathbf{h}(\mathbf{x}_{k+1}) + \mathbf{e}_{k+1}, \\ \mathcal{H}_1 &: \mathbf{z}_{k+1} = \mathbf{h}(\mathbf{x}_{k+1}) + \mathbf{e}_{k+1} + \mathbf{a}, \end{aligned} \tag{19}$$

where $\mathbf{a}$ is a vector of false data injected in the measurements.

From (13), (17), and (19), the hypothesis test on the residual vector $\mathbf{v}_{k+1}$ can be written as

$$\begin{aligned} \mathcal{H}_0 &: \mathbf{v}_{k+1} = \mathbf{H}(\tilde{\mathbf{x}}_{k+1})(\mathbf{x}_{k+1} - \tilde{\mathbf{x}}_{k+1}) + \mathbf{e}_{k+1}, \\ \mathcal{H}_1 &: \mathbf{v}_{k+1} = \mathbf{H}(\tilde{\mathbf{x}}_{k+1})(\mathbf{x}_{k+1} - \tilde{\mathbf{x}}_{k+1}) + \mathbf{e}_{k+1} + \mathbf{a}. \end{aligned} \tag{20}$$

The residual vector $\mathbf{v}_{k+1}$ under the null hypothesis $\mathcal{H}_0$ is generally assumed to be a zero mean Gaussian vector [11] and [14]. With the dynamic state estimator presented in this paper, the covariance matrix $\mathbf{S}_{k+1}$ of the residual vector is given in (18). Assuming that the attack vector $\mathbf{a}$ is a deterministic vector, under the alternate hypothesis $\mathcal{H}_1$, $\mathbf{v}_{k+1}$ is Gaussian with mean $\mathbf{a}$ and covariance matrix $\mathbf{S}_{k+1}$.

As in (18), the elements in $\mathbf{z}_{k+1}$ are correlated based on the physical model of the power grid. To simplify the analysis, we propose to perform a whitening transformation on $\mathbf{v}_{k+1}$. The covariance matrix of the residual vector can be decomposed as $\mathbf{S}_{k+1} = \mathbf{U}_{k+1}^T\mathbf{D}_{k+1}\mathbf{U}_{k+1}$, where $\mathbf{D}_{k+1}$ is a diagonal matrix with the eigenvalues of $\mathbf{S}_{k+1}$ on its main diagonal and $\mathbf{U}_{k+1}$ is the corresponding orthonormal eigenvector matrix at time instant $k+1$. The whitening transformation of the residual vector $\mathbf{v}_{k+1}$ is $\bar{\mathbf{v}}_{k+1} = \mathbf{W}_{k+1}\mathbf{v}_{k+1}$, where the whitening matrix $\mathbf{W}_{k+1} = \mathbf{D}_{k+1}^{-\frac{1}{2}}\mathbf{U}_{k+1}$. With the whitening operator, it can be easily shown that the covariance matrix of $\bar{\mathbf{v}}_{k+1}$ is $\mathbf{I}_m$, which is an $m \times m$ identity matrix.

Following the Gaussian distribution of $\mathbf{v}_{k+1}$ given in (20), the hypothesis test on $\bar{\mathbf{v}}_{k+1}$ is

$$\begin{aligned} \mathcal{H}_0 &: \bar{\mathbf{v}}_{k+1} = \mathbf{W}_{k+1}\mathbf{v}_{k+1} \quad \sim \mathcal{N}(\mathbf{0}, \mathbf{I}_m), \\ \mathcal{H}_1 &: \bar{\mathbf{v}}_{k+1} = \mathbf{W}_{k+1}\mathbf{v}_{k+1} \quad \sim \mathcal{N}(\boldsymbol{\mu}, \mathbf{I}_m), \end{aligned} \tag{21}$$

where $\boldsymbol{\mu} = \mathbf{W}_{k+1}\mathbf{a}$.

### B. Proposed False Data Detector

A QCD-based false data detection method is proposed in this section to detect cyber-attacks. We assume that the false data is injected at a random time $\tau$, and the attack was detected at time $\hat{\tau}$. Based on the design criteria of quickest change detection, the problem can be formulated as

$$\text{(P1)} \qquad \begin{aligned} &\text{minimize} \quad \text{WDD} = \sup_k \mathbb{E}_k[(\hat{\tau} - k)^+] \\ &\text{subject to} \quad \text{FAR} = \frac{1}{\mathbb{E}_\infty[\hat{\tau}]} \leq \zeta. \end{aligned}$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JESTPE.2019.2936587, IEEE Journal of Emerging and Selected Topics in Power Electronics



where WDD is the worst-case detection delay, FAR is the false alarm rate, $(a)^+ = a$ if $a \geq 0$ and 0 otherwise, $\mathbb{E}_k$ is the expectation assuming the attack becomes active at $\tau = k$, and $\mathbb{E}_\infty$ denotes the expectation when there is no attack. The solution of the problem is a quickest detection algorithm in that it aims at minimizing the worst-case detection delay, subject to an upper bound of the false alarm rate.

The above problem can be solved by using the well-known CUSUM algorithm [21]

$$\hat{\tau} = \inf\{k \geq 1 | C_k \geq A\}, \tag{22}$$

where $A$ is a threshold obtained by the FAR upper bound $\zeta$,

$$C_{k+1} = \max(0, C_k + L_k), \tag{23}$$

and $L_k = \log \frac{f_1(\bar{\mathbf{v}}_k)}{f_0(\bar{\mathbf{v}}_k)}$ is the log-likelihood ratio (LLR), with $f_1(\bar{\mathbf{v}}_k)$ and $f_0(\bar{\mathbf{v}}_k)$ being the probability density functions (pdfs) associated with hypotheses $\mathcal{H}_1$ and $\mathcal{H}_0$, respectively. The CUSUM algorithm is the asymptotically optimum solution to (P1) because it can asymptotically minimize the WDD when the FAR goes to 0 [22], [23].

Under the assumption that $\bar{\mathbf{v}}_k$ is Gaussian distributed, the LLR can be calculated as

$$L_k = \mathbf{a}^T \mathbf{W}_k^T \bar{\mathbf{v}}_k - \frac{1}{2} \mathbf{a}^T \mathbf{W}_k^T \mathbf{W}_k \mathbf{a}. \tag{24}$$

The calculation of the LLR $L_k$ requires the knowledge of the attack vector $\mathbf{a}$, which is unknown at the detector. Thus we cannot directly apply the CUSUM algorithm. In order to resolve the unknown parameters, the detection method in [23] utilizes the generalized likelihood ratio test (GLRT) approach by replacing the unknown parameter with the maximum likelihood estimation (MLE) as

$$\hat{\tau} = \inf\{k \geq 1 | \max_{1 \leq t \leq k} \sup_{\mathbf{a}} \sum\nolimits_{i=t}^{k} L_i \geq A\}. \tag{25}$$

This approach is proven to be asymptotically optimal in terms of minimum detection delay [27]. However, the test statistic cannot be computed recursively as the CUSUM test, because GLRT needs to compute every unknown element of $\mathbf{a}$ for each observation at sampling time $1 \leq t \leq k$. In other words, GLRT needs to store the observations and perform MLE of $\mathbf{a}$ at every sampling instant. As a result, this approach has very high complexity, and it might not be feasible for real-time FDIA detection in power grids.

A low-complexity adaptive-CUSUM algorithm is proposed in [6] based on Rao test [25], which is asymptotically equivalent to the GLRT test [28]. The Rao test statistic can be computed by taking the derivative of $L_k$ with respect to the unknown parameter $\mathbf{a}$ evaluated around the region of interests. In our case, the region of interest is considered to be around zero because the hypothesis $\mathcal{H}_0$ has zero mean. According to (21), the statistic [25] of the Rao test for detection at time $k$ can be written as follows:

$$Y(\bar{\mathbf{v}}_k) = \frac{\partial L_k}{\partial \mathbf{a}}^T \Big|_{\mathbf{a}=0} \left[\mathcal{I}^{-1}(\mathbf{a})\big|_{\mathbf{a}=0}\right] \frac{\partial L_k}{\partial \mathbf{a}}\Big|_{\mathbf{a}=0} = \bar{\mathbf{v}}_k^T \bar{\mathbf{v}}_k, \tag{26}$$

where $\mathcal{I}(\mathbf{a})$ is the Fisher information matrix [18]. The proof for (26) is given in Appendix B.

Under the null hypothesis $\mathcal{H}_0$, the Rao test statistic follows Chi-square distribution, that is, $Y(\bar{\mathbf{v}}_k) \sim \chi^2_m$, where $m$ is the degree-of-freedom corresponding to the dimension of the measurement vector. If we directly replace the LLR $L_k$ in (23) with the Rao test statistic $Y(\bar{\mathbf{v}}_k)$ in the CUSUM test defined in (22), the CUSUM test statistic $C_k$ will increase monotonically under both the null and alternative hypothesis because $Y(\bar{\mathbf{v}}_k) \geq 0$. This is undesirable for CUSUM because it is a threshold test. To address this issue, we introduce a normalized version of the test statistic in (26) with respect to the mean and standard deviation of $Y(\bar{\mathbf{v}}_k)$ under $\mathcal{H}_0$, which are, $m$ and $\sqrt{2m}$, respectively. Based on the normalized test statistic, we propose a new detection rule as follows.

**Definition 1.** *(Normalized Rao-CUSUM Detector) Given a whitened residual vector $\bar{\mathbf{v}}_{k+1} = \mathbf{W}_{k+1}\mathbf{v}_{k+1}$ at time $k+1$, an FDIA is detected at time $\hat{\tau}$ with*

$$\hat{\tau} = \inf\{k \geq 1 | T_k \geq A\}, \tag{27}$$

*where*

$$T_{k+1} = \max\left(0, T_k + \frac{Y(\bar{\mathbf{v}}_{k+1}) - m}{\sqrt{2m}}\right) > A, \tag{28}$$

*with $T_0 = 0$. The threshold $A$ is determined by the FAR upper bound $\zeta$.*

The normalized Rao-CUSUM detector is developed by modifying the asymptotically optimum GLRT-CUSUM detector to balance the tradeoff between complexity and performance. The proposed normalized Rao-CUSUM algorithm might have a bit higher WDD than the GLRT-CUSUM algorithm, but offers much lower complexity.

It should be noted that the above test can distinguish between sudden load change from FDIA because the formulation of the null hypothesis $\mathcal{H}_0$ includes sudden load change as a special case. In case of a sudden load change, the system dynamics still follow the physical model of the power grid. As a result, the residual vector can still be modeled as zero-mean Gaussian distributed with covariance matrix $\mathbf{S}_{k+1}$. Yet this is no longer true when there is false data injected into the power grid, which is modeled as the alternative hypothesis $\mathcal{H}_1$. Since the test in Definition 1 is designed to distinguish between the null and alternative hypothesis by minimizing the worst-case detection delay, it is able to distinguish between load change and FDIA. On the other hand, system faults, such as sensor failures or line faults, will also cause the measurements to deviate from those predicted by the physical model of the system. In that case, the proposed algorithm will be able to detect the presence of sensor failures or system faults. However, it will not be able to differentiate FDIA from sensor failures or system faults. Thus the algorithm will treat FDIA, sensor failure, or other system faults in a similar manner.

In case false data are detected, we can identify the buses under attack by using the power of the residuals at different buses. That is, if the residual power or amplitude on a given bus is above a certain threshold, then it is considered that the corresponding bus is under attack. Similar to [11], the amplitude test can be expressed as

$$|\mathbf{v}_{k+1}(i)| > \gamma \sigma_{S_i}, \tag{29}$$

where $|\mathbf{v}_{k+1}(i)|$ is the absolute value of the $i$-th element of $\mathbf{v}_{k+1}$, $\sigma_{S_i}$ is the standard deviation of the $i$-th element of $\mathbf{v}_{k+1}$, and $\gamma$ defines the limit of confidence. If a bus is detected as under attack, we replace the estimated states with the predicted states to ensure the normal operations of the power grid.

The normalized Rao-CUSUM detector proposed in Definition 1 is a simple threshold test, and the test statistic $T_k$ can be recursively calculated based on (28). As a result, the proposed test has low complexity and can be easily implemented. The implementation of the detector in (27) requires a threshold $A$, which in turn depends on the FAR upper bound $\zeta$. In the next section, we will provide a theoretical guideline for choosing the threshold value $A$ in terms of FAR with the help of a Markov-chain-based analytical model.

### C. Computation Complexity Analysis

In this subsection, we study the effects of the size of system on the computation complexity of the proposed algorithm. The size of the system can be defined by two parameters:

- The dimension of state vector: $n = 2N - 1$, where $N$ is the number of buses in the system,
- The dimension of measurement vector: $m$, which depends on the number of buses and lines.

It is easily observed that $m > n$. To determine the effect of size of the system on the performance, we present the complexity analysis of the proposed algorithm in a single sampling instant $k$ with respect to these two parameters separately.

The proposed algorithm has two stages: 1) false data detection and 2) dynamic state estimation. With respect to $m$, computation in stage 1 is dominated by the eigenvalue decomposition process which has a cubic complexity $\mathcal{O}(m^3)$, and stage 2 is dominated by the matrix inversion of $\mathbf{R}_k$ which also has a cubic complexity $\mathcal{O}(m^3)$. So, total complexity of the proposed algorithm scales cubically with $m$ as $\mathcal{O}(m^3)$.

With respect to $n$, stage 2 computation is dominated by the computations of $\mathbf{M}_k$ in (8) and $\mathbf{\Sigma}_k$ in (11), both of which have a cubic complexity $\mathcal{O}(n^3)$. Comparatively, complexity of stage 1 scales quadratically with $n$. So, total complexity of the proposed algorithm scales cubically with $n$ as $\mathcal{O}(n^3)$.

## V. Markov-chain-based Analytical Model

In this section, we present a Markov-chain-based model to analyze the proposed false data detector. The Markov-chain-based model provides theoretical guidelines on the choice of the detection threshold in (27) based on the FAR upper bound. For a given FAR upper bound, we can obtain the optimum detection threshold by using offline Monte-Carlo simulations. Once the optimum threshold is obtained offline, the online normalized Rao-CUSUM detector can then be performed to detect FDIA or system faults in real time.

To facilitate analysis, $\mathbb{R}^+ \cup 0$ is discretized into a finite set of intervals representing the states $\{U_0, U_1, \cdots, U_M\}$ such as

$$U_0 = 0, \quad U_1 = (0, \Delta], \quad U_2 = (\Delta, 2\Delta],$$
$$U_3 = (2\Delta, 3\Delta], \quad \cdots\cdots, \quad U_M = (A, +\infty),$$

where $\Delta = \frac{A}{M-1}$ and $M$ represents the total number of transitions from 0 to the state that has the value greater than the threshold $A$.

It can be easily observed from (28) that the sequence exhibits the property of a first-order Markov chain, where the future state $T_{k+1}$ at time index $k+1$ depends only on the current state $T_k$, but not on past states [29].

The transition probabilities of the Markov chain under $\mathcal{H}_0$ for the proposed algorithm from state $U_i$ at $k$ to state $U_j$ at $k+1$ can be described as

$$P_{ij} = P(T_{k+1} \in U_j | T_k \in U_i). \tag{30}$$

The transition probability $P_{ij}$ can be computed numerically using Monte-Carlo simulations according to the distribution of $\bar{\mathbf{v}}$ under the null hypothesis $\mathcal{H}_0$. The values of the transition probabilities are uniquely determined by the threshold $A$ and the number of discretization levels $M$. Since the calculations of the transition probabilities are performed offline, we can achieve arbitrary precision of the transition probability by increasing the number of Mote-Carlo trials without affecting the complexity of the online portion of the algorithm. As a result, we can establish a very accurate numerical relationship between $A$ and the transition probabilities.

Define the transition probability matrix (TPM) $\mathbf{P}$ as an $(M+1) \times (M+1)$ matrix with the $(i,j)$-th element being $P_{i-1,j-1}$. It is clear that $\mathbf{P}$ is a Markov matrix, that is, all elements of $\mathbf{P}$ are non-negative and the sum of each row vector is 1. The steady-state probability $\pi_j$ of each state $U_j$ can be determined by

$$\pi_j = \sum\nolimits_{i=0}^{M} P_{ij}\pi_i, \ \forall\ j \in \{0, \cdots, M\}, \tag{31}$$

$$\sum\nolimits_{j=0}^{M} \pi_j = 1. \tag{32}$$

The transition probability of the Markov chain can be written in a matrix format as

$$\mathbf{P}^T \boldsymbol{\pi} = \boldsymbol{\pi} \tag{33}$$

where $\boldsymbol{\pi} = [\pi_0, \pi_1, \cdots, \pi_M]^T$. The steady-state probability vector $\boldsymbol{\pi}$ can then be obtained by finding the eigenvector corresponding to the eigenvalue 1 of the TPM $\mathbf{P}$. Since $\mathbf{P}$ is a Markov matrix, it always has an eigenvalue of 1.

The steady-state probability can be used to calculate the FAR, which can be equivalently evaluated as the probability that $T_k$ crosses the threshold $A$ when there is no attack in the network. As in [29], the FAR can be equivalently calculated as the steady-state probability $\pi_M$, that is, the probability that $T_k$ stays at state $U_M$ under the null hypothesis

$$\text{FAR} = \pi_M. \tag{34}$$

Since $\pi_M$ is determined by the eigenvector of $\mathbf{P}$, which in turn depends on the choice of threshold $A$, there is an optimum threshold value for a given FAR. Enabled by the Markov-chain model, we can numerically obtain a very accurate estimate of the optimum threshold based on the FAR.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JESTPE.2019.2936587, IEEE Journal of Emerging and Selected Topics in Power Electronics



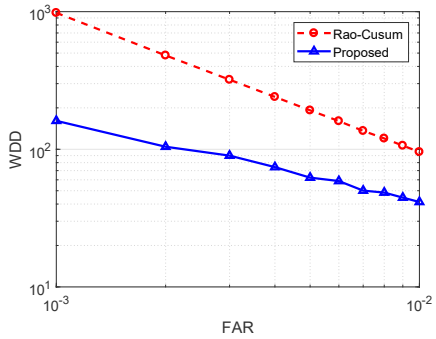


Fig. 1. Performance analysis of the proposed algorithm in comparison with Rao-CUSUM test [6].

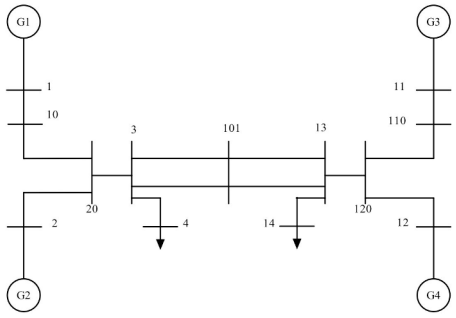


Fig. 2. Single Line Diagram Two Area System [31].

## VI. Simulation Results

In this section, we present numerical simulations results to illustrate the performance of the proposed algorithm. The first subsection demonstrates the performance in terms of FAR and WDD using simulated data. The second subsection presents numerical results based on simulations of the 13-bus system using MATLAB Power System Toolbox (PST v3.0) [30], [31].

### A. WDD v.s. FAR

Fig. 1 shows the tradeoff between WDD and FAR of the proposed algorithm and the Rao-CUSUM test presented in [6]. In the simulation, the data are generated by following the model in (21) with $m = 55$ and $\boldsymbol{\mu} = [1, 1, 0, \cdots, 0]$. The false data injection time $\tau$ follows discrete uniform distribution between $[1, 100]$. Every point on the curves is obtained by averaging over $10,000$ Monte-Carlo trials. For a given FAR, the corresponding threshold $A$ is chosen by following the Markov-chain analysis in Section V. As expected, the WDD is a decreasing function of the FAR. The proposed detection algorithm outperforms the Rao-CUSUM test used in [6]. At FAR = $10^{-2}$, the WDD of the proposed algorithm and the Rao-CUSUM test is 42 and 95 samples, respectively.

### B. FDIA Detection in Power Systems

In this section, we present the simulation results performed on a 13-bus system with two areas as shown in Fig. 2. Bus 1 is used as the reference bus. The measurement vector consists of $m = 55$ components: the voltage magnitude of bus 1, the active and reactive power injections at all 13 buses, the active and reactive power flows at all 14 lines. The state vector consists of $n = 25$ components: the voltage magnitudes at all 13 buses and the phase angles at the 12 non-reference buses.

Using MATLAB Power System Toolbox (PST v3.0), the system dynamics is simulated by increasing the active load at bus 4 by 0.5 per unit (p.u.) and the resulting measurement and state vectors are considered as the true values of the system. The noisy measurement vector $\mathbf{e}_k$ in (1) is obtained by adding a zero mean Gaussian noise with a diagonal covariance matrix $\mathbf{R}_k$ to each of the true measurements. The noise variances, which are the diagonal elements of $\mathbf{R}_k$, are $10^{-5}$ for the voltage magnitude of reference bus and $10^{-6}$ for the active and reactive power measurements. The matrix $\mathbf{Q}_k = 10^{-6}\mathbf{I}_n$ is kept constant at every sampling time $k$. The parameters $\mathbf{F}_k$ and $\mathbf{G}_k$ are obtained according to the Holt's exponential smoothing method with $\alpha = 0.95$ and $\beta = 0.001$ [11].

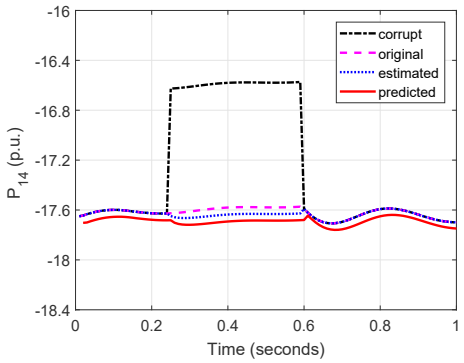


Fig. 3. The real power at bus 14 vs time $t$ with false data at $0.25 \leq t < 0.6$, load change at $t = 0.6$, and the detector in (28).

The sampling rate in our simulation is set as $\Delta t = 0.01$ seconds. Thus the $k$-th time index corresponds to a time value of $t = k\Delta t$ seconds. In order to evaluate the performance of the proposed detector, two scenarios are simulated: false data and sudden load change conditions. The false data condition is simulated by injecting errors of $-1.5$ and 1 p.u. into the active power measurements at buses 13 and 14, respectively, during a time period $0.25 \leq t < 0.6$ seconds unless specified otherwise. The sudden load change condition is simulated by cutting the active power injection of bus 4 by 1 p.u at $t = 0.6$ seconds. In each of the following figures, every point on the curves is obtained by averaging over $1,000$ Monte-Carlo trials.

Fig. 3 shows the active power at bus 14 with false data injected into the active power measurements at buses 13 and 14. In addition, the active power injection of bus 4 is cut by 1 p.u. at $t = 0.6$ seconds to simulate sudden load change. The threshold of the proposed detector is set at $A = 200$, which corresponds to FAR of $2.5 \times 10^{-5}$ according to the Markov-chain analysis. Once an FDIA is detected, the residual amplitudes are compared to a threshold as in (29) to identify the buses under attack, with $\alpha = 3.5$ used in this paper. The measurements at the buses under attack are then replaced with their predicted values. When there is no attack, the power calculated from the estimated states is almost identical to its actual value. When false data is injected between $0.25 \leq t < 0.6$ seconds, the proposed detector successfully detects the presence of FDIA and replaces the corrupted measurement

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JESTPE.2019.2936587, IEEE Journal of Emerging and Selected Topics in Power Electronics



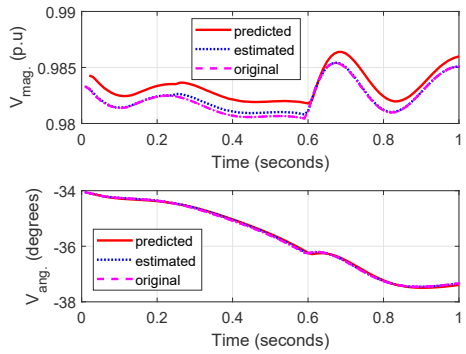


Fig. 4. The voltage magnitude (top) and phase angle (bottom) at bus 13 vs time $t$ with false data at $0.25 \leq t < 0.6$, load change at $t = 0.6$, and the detector in (28).

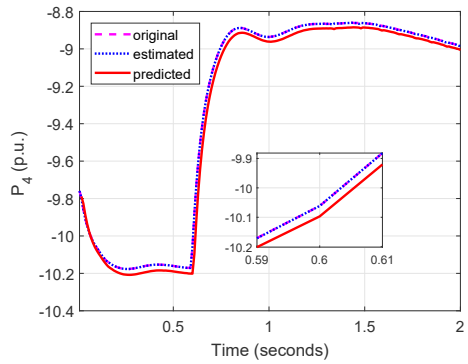


Fig. 6. The real power at bus 4 vs time $t$ with false data at $0.25 \leq t < 0.6$, load change at $t = 0.6$, and the detector in (28).

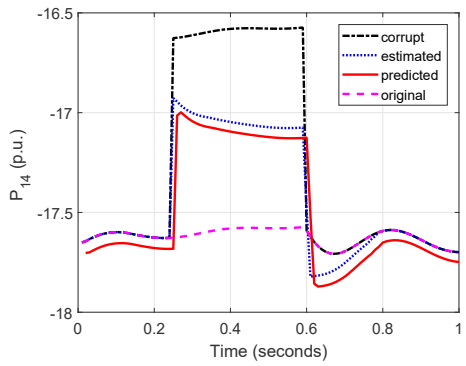


Fig. 5. The real power at bus 14 vs time $t$ with false data at $0.25 \leq t < 0.6$ and the detector in [11].

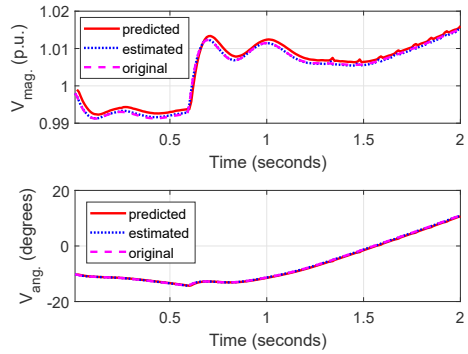


Fig. 7. The voltage magnitude (top) and phase angle (bottom) at bus 4 vs time $t$ with false data at $0.25 \leq t < 0.6$, load change at $t = 0.6$, and the detector in (28).

with the predicted values. In this case, the power calculated by using state estimation is slightly different from its true value, with a difference less than 0.33%. When there is a sudden change at $t = 0.6$ seconds, the detector correctly recognizes it as a normal operating condition and achieves correct state estimates. In addition, there is a one sample lag between the predicted value and the actual value.

Fig. 4 shows the voltage magnitude (top) and phase angle (bottom) at bus 13 under the same configuration of Fig. 3. The voltage amplitude and phase are estimated with high accuracy despite the presence of FDIA, mainly because the false data are correctly identified and replaced with predicted values. In addition, the state estimator correctly adapts to the dynamic change at $t = 0.6$ seconds.

Fig. 5 shows the performance of an existing residual-based detector that was proposed in [11], under the same configuration as in Fig. 3. Since the false data are injected into the correlated measurements of adjacent buses 13 and 14, the detector in [11] is unable to distinguish the false data from the sudden changes in the system. The FDIA is erroneously detected as a sudden change. As a result, during the FDIA, the power calculated from the estimated and predicted states deviate significantly from its actual value. The performance of the estimator yields in an estimation error of as high as 0.7 p.u at $t = 0.25$ seconds.

To further illustrate the ability of the proposed detector to distinguish between FDIA and sudden change, Fig. 6 shows the active power measurement at bus 4. The active load at bus 4 is increased by 0.5 p.u. at $t = 0.6$ seconds. The load change caused a gradual change of the active power. Since the load change affects power measurements on all buses based on the physical model of the power grid, the proposed detector successfully recognizes it as a load change instead of FDIA. Thus the dynamic state estimator can accurately track and estimate the state change caused by the load change. The power calculated from the estimated states is almost identical to its original value. Again a one sample lag is observed between the predicted value and actual value. Similarly, in Fig. 7, the voltage magnitude (top) and phase angle (bottom) at bus 4 are estimated with high accuracy.

The proposed algorithm assumes that the topology of the system remains unchanged. However, in the event of a system fault, the topology of the system might change. As a result, the proposed algorithm will detect the deviation of system's behavior due to system fault in a similar manner as FDIA detection. To further illustrate the performance of proposed algorithm under system faults, Fig. 8 shows the active power at bus 14 under the influence of a single line-to-ground fault, which is applied to the line connecting bus 3 and bus 101 at $t = 0.2$ seconds. The fault is cleared at bus 3 at $t = 0.35$ seconds and at bus 101 at $t = 0.4$ seconds. It can be observed that throughout the duration of the line-to-ground fault, the proposed algorithm detects the fault and replace the measurement value by using the predicted values. Thus

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JESTPE.2019.2936587, IEEE Journal of Emerging and Selected Topics in Power Electronics



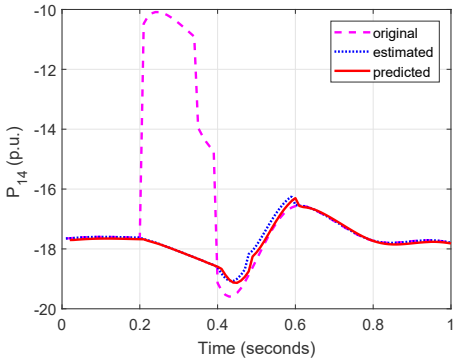


Fig. 8. The real power at bus 14 with single line-to-ground fault at the line connecting bus 3 and bus 101 during $0.2 \leq t \leq 0.4$.

the algorithm can detect the presence of fault, but it cannot differentiate fault from cyber-attacks.

## VII. Conclusion

A quickest intrusion detection algorithm has been developed for the detection and removal of false data injected into smart grids. The algorithm was developed to minimize the worst-case detection delay subject to an upper bound of false alarm rate. To distinguish between FDIA and sudden system change, a time-varying dynamic model was used to represent the dynamic state transitions. A dynamic state estimator was then developed to estimate and track the time-varying and non-stationary state transitions. Based on the statistical properties of the state estimation results, a new normalized Rao-CUSUM detector was developed to minimize the detection delay of FDIA while separating FDIA from sudden system changes. Unlike existing algorithms that rely on measurement correlation to discriminate false data from sudden system changes, the proposed algorithm can detect any false data including those injected into correlated measurements. Simulation results have shown that the proposed algorithm can accurately and timely detect and remove FDIA. In addition, the algorithm can also detect system faults such as sensor failures or line outages. However, it cannot differentiate system faults from FDIA. The algorithm can be used to harden IEDs or SCADA systems to improve the security and resilience of smart grids.

## Appendix A
## Proof of (10)

The point $\mathbf{x}$, which minimizes (9) can be obtained by calculating the first derivative of $J(\mathbf{x})$ and setting it to zero. Define the first derivative of $J(\mathbf{x})$ as

$$\mathbf{g}(\mathbf{x}) = \frac{\partial \mathbf{J}(\mathbf{x})}{\partial \mathbf{x}} = -\frac{\partial \mathbf{h}^{\mathbf{T}}(\mathbf{x})}{\partial \mathbf{x}} \mathbf{R}^{-1} [\mathbf{z} - \mathbf{h}(\mathbf{x})] + \mathbf{M}^{-1}(\mathbf{x} - \tilde{\mathbf{x}}). \tag{35}$$

The minimum point $\hat{\mathbf{x}}$ of $J(\mathbf{x})$ is calculated by solving

$$\mathbf{g}(\hat{\mathbf{x}}) = \mathbf{0}. \tag{36}$$

Given the non-linearity of (35), (36) is solved by iterative methods such as the Newton-Raphson method.

The Taylor series expansion of $\mathbf{g}(\mathbf{x})$ for $\mathbf{x} = \mathbf{x}^{(0)} + \Delta_{\mathbf{x}}$ is

$$\mathbf{g}(\mathbf{x}) = \mathbf{g}(\mathbf{x}^{(\mathbf{0})}) + \frac{\partial \mathbf{g}(\mathbf{x})}{\partial \mathbf{x}} \mid_{\mathbf{x}=\mathbf{x}^{(0)}} \Delta_{\mathbf{x}}, \tag{37}$$

where $\mathbf{x}^{(0)}$ is the initial point and

$$\frac{\partial \mathbf{g}(\mathbf{x})}{\partial \mathbf{x}} = \mathbf{g}^{'}(\mathbf{x}) = \mathbf{H}^{T}(\mathbf{x})\mathbf{R}^{-1}\mathbf{H}(\mathbf{x}) + \mathbf{M}^{-1}, \tag{38}$$

where $\mathbf{H}(\mathbf{x}) = \frac{\partial \mathbf{h}(\mathbf{x})}{\partial \mathbf{x}}$.

According to the Newton-Raphson method, by setting (37) to zero, the increment $\Delta_{\mathbf{x}}$ is obtained as

$$\Delta_{\mathbf{x}} = -\left[\mathbf{g}^{'}(\mathbf{x}^{(0)})\right]^{-1} \mathbf{g}(\mathbf{x}^{(\mathbf{0})}). \tag{39}$$

Thus,

$$\mathbf{x} = \mathbf{x}^{(0)} - \mathbf{\Sigma}^{(0)}\mathbf{g}(\mathbf{x}^{(\mathbf{0})}), \tag{40}$$

where

$$\mathbf{\Sigma}^{(0)} = \left[\mathbf{g}^{'}(\mathbf{x}^{(0)})\right]^{-1} = \left[\mathbf{H}^{T}(\mathbf{x}^{(0)})\mathbf{R}^{-1}\mathbf{H}(\mathbf{x}^{(0)}) + \mathbf{M}^{-1}\right]^{-1}. \tag{41}$$

Combining (35), (40), and (41) at the $(i+1)$-th iteration with an initial point $\mathbf{x}^{(i)} = \mathbf{x}^{(i+1)} - \Delta_{\mathbf{x}}$, the $(i+1)$-th point becomes

$$\mathbf{x}^{(i+1)} = \mathbf{x}^{(i)} + \mathbf{\Sigma}^{(i)}\{\mathbf{H}^{T}(\mathbf{x}^{(i)})\mathbf{R}^{-1}[\mathbf{z} - \mathbf{h}(\mathbf{x}^{(i)})] - \mathbf{M}^{-1}(\mathbf{x}^{(i)} - \tilde{\mathbf{x}})\}. \tag{42}$$

This completes the proof.

## Appendix B
## Proof of (26)

Combining the definition of LLR in (24) with the hypotheses in (21), we obtain

$$\frac{\partial L_k}{\partial \mathbf{a}} = \mathbf{W}_k^T \bar{\mathbf{v}}_k - \mathbf{W}_k^T \mathbf{W}_k \mathbf{a}. \tag{43}$$

Next, substituting the value $\mathbf{a} = 0$ yields in

$$\frac{\partial L_k}{\partial \mathbf{a}}\Big|_{\mathbf{a}=0} = \mathbf{W}_k^T \bar{\mathbf{v}}_k. \tag{44}$$

Using the definition of Fisher information matrix [18], we get

$$\mathcal{I}(\mathbf{a}) = -\mathbb{E}\left[\frac{\partial}{\partial \mathbf{a}}\left(\frac{\partial L_k}{\partial \mathbf{a}}\right)\right] = \mathbf{W}_k^T \mathbf{W}_k. \tag{45}$$

Combining (44) and (45) results in the Rao test statistic $Y(\bar{\mathbf{v}}_k) = \bar{\mathbf{v}}_k^T \bar{\mathbf{v}}_k$. This completes the proof.

## References

[1] S. Cui, Z. Han, S. Kar, T. T. Kim, H. V. Poor, and A. Tajer, "Coordinated data-injection attack and detection in the smart grid: A detailed look at enriching detection solutions," *IEEE Signal Processing Magazine*, vol. 29, no. 5, pp. 106–115, Sep. 2012.

[2] D. Wei, Y. Lu, M. Jafari, P. M. Skare, and K. Rohde, "Protecting smart grid automation systems against cyberattacks," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 782–795, Dec. 2011.

[3] R. Langner, "Stuxnet: Dissecting a cyberwarfare weapon," *IEEE Security & Privacy*, vol. 9, no. 3, pp. 49–51, May 2011.

[4] G. Liang, J. Zhao, F. Luo, S. R. Weller, and Z. Y. Dong, "A review of false data injection attacks against modern power systems," *IEEE Transactions on Smart Grid*, vol. 8, no. 4, pp. 1630–1638, Jul. 2017.

[5] A. J. McBride and A. R. McGee, "Assessing smart grid security," *Bell Labs Technical Journal*, vol. 17, no. 3, pp. 87–103, Dec. 2012.

[6] Y. Huang, J. Tang, Y. Cheng, H. Li, K. A. Campbell, and Z. Han, "Real-time detection of false data injection in smart grid networks: an adaptive cusum method and analysis," *IEEE Systems Journal*, vol. 10, no. 2, pp. 532–543, Jun. 2016.

[7] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Transactions on Information and System Security*, vol. 14, no. 1, pp. 13:1–13:33, May 2011.

[8] Z.-H. Yu and C. Wen-Long, "Blind false data injection attack using pca approximation method in smart grid," *IEEE Trans. Smart Grid*, vol. 6, no. 3, pp. 1219–1226, May 2015.

[9] J. Liang, O. Kosut, and L. Sankar, "Cyber attacks on ac state estimation: Unobservability and physical consequences," in *IEEE PES General Meeting— Conference & Exposition*. National Harbor, MD, USA: IEEE, Jul. 2014.

[10] M. A. Rahman and H. Mohsenian-Rad, "False data injection attacks against nonlinear state estimation in smart power grids," in *IEEE PES General Meeting*, Vancouver, BC, Canada, Jul. 2013, pp. 1–5.

[11] A. L. Da Silva, M. Do Coutto Filho, and J. De Queiroz, "State forecasting in electric power systems," in *IEE Proceedings C (Generation, Transmission and Distribution)*, vol. 130, no. 5, Sep. 1983, pp. 237–244.

[12] M. B. Do Coutto Filho and J. C. S. de Souza, "Forecasting-aided state estimation—part i: Panorama," *IEEE Transactions on Power Systems*, vol. 24, no. 4, pp. 1667–1677, Nov. 2009.

[13] A. Jain and N. Shivakumar, "Power system tracking and dynamic state estimation," in *IEEE/PES Power Systems Conference and Exposition*, Seattle, WA, USA, Mar. 2009.

[14] K. Nishiya, J. Hasegawa, and T. Koike, "Dynamic state estimation including anomaly detection and identification for power systems," in *IEE Proceedings C (Generation, Transmission and Distribution)*, vol. 129, no. 5, Sep. 1982, pp. 192–198.

[15] Q. Yang, L. Chang, and W. Yu, "On false data injection attacks against kalman filtering in power system dynamic state estimation," *Security and Communication Networks*, vol. 9, no. 9, pp. 833–849, Jun. 2016.

[16] G. Chaojun, P. Jirutitijaroen, and M. Motani, "Detecting false data injection attacks in ac state estimation," *IEEE Transactions on Smart Grid*, vol. 6, no. 5, pp. 2476–2483, Sep. 2015.

[17] J. James, Y. Hou, and V. O. Li, "Online false data injection attack detection with wavelet transform and deep neural networks," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 7, pp. 3271–3280, Jul. 2018.

[18] S. M. Kay, *Fundamentals of statistical signal processing*. Prentice Hall PTR, 1993.

[19] I. Akingeneye and J. Wu, "Low latency detection of sparse false data injections in smart grids," *IEEE Access*, vol. 6, pp. 58 564–58 573, Oct. 2018.

[20] H. V. Poor and O. Hadjiliadis, *Quickest detection*. Cambridge University Press Cambridge, 2009, vol. 40.

[21] G. V. Moustakides *et al.*, "Optimal stopping times for detecting changes in distributions," *The Annals of Statistics*, vol. 14, no. 4, pp. 1379–1387, Dec. 1986.

[22] G. Lorden, "Procedures for reacting to a change in distribution," *The Annals of Mathematical Statistics*, pp. 1897–1908, 1971.

[23] T. L. Lai, "Information bounds and quick detection of parameter changes in stochastic systems," *IEEE Transactions on Information Theory*, vol. 44, no. 7, pp. 2917–2929, Nov. 1998.

[24] S. Nath and J. Wu, "Bayesian quickest change point detection with multiple candidates of post-change models," in *IEEE Global Conference on Signal and Information Processing*, Anaheim, CA, USA, Nov. 2018.

[25] A. De Maio, "Rao test for adaptive detection in gaussian interference with unknown covariance matrix," *IEEE transactions on signal processing*, vol. 55, no. 7, pp. 3577–3584, Jul. 2007.

[26] X. Li, A. Scaglione, and T.-H. Chang, "Optimal sensor placement for hybrid state estimation in smart grid," in *2013 IEEE International Conference on Acoustics, Speech and Signal Processing*, Vancouver, BC, Canada, May 2013.

[27] T. L. Lai and J. Z. Shan, "Efficient recursive algorithms for detection of abrupt changes in signals and control systems," *IEEE Transactions on Automatic Control*, vol. 44, no. 5, pp. 952–966, 1999.

[28] A. De Maio and S. Iommelli, "Coincidence of the rao test, wald test, and glrt in partially homogeneous environment," *IEEE Signal Processing Letters*, vol. 15, pp. 385–388, Apr. 2008.

[29] D. Gamerman and H. F. Lopes, *Markov chain Monte Carlo: stochastic simulation for Bayesian inference*. Chapman and Hall/CRC, 2006.

[30] J. H. Chow and K. W. Cheung, "A toolbox for power system dynamics and control engineering education and research," *IEEE transactions on Power Systems*, vol. 7, no. 4, pp. 1559–1564, Nov. 1992.

[31] G. Rogers, *Power system oscillations*. Springer Science & Business Media, 2012.