Real-Time Detection of False Data Injection in Smart Grid Networks: An Adaptive CUSUM Method and Analysis

Yi Huang, *Student Member, IEEE*, Jin Tang, *Member, IEEE*, Yu Cheng, *Senior Member, IEEE*,
Husheng Li, *Member, IEEE*, Kristy A. Campbell, and Zhu Han, *Fellow, IEEE*

***Abstract*—A smart grid is delay sensitive and requires the techniques that can identify and react on the abnormal changes (i.e., system fault, attacker, shortcut, etc.) in a timely manner. In this paper, we propose a real-time detection scheme against false data injection attack in smart grid networks. Unlike the classical detection test, the proposed algorithm is able to tackle the unknown parameters with low complexity and process multiple measurements at once, leading to a shorter decision time and a better detection accuracy. The objective is to detect the adversary as quickly as possible while satisfying certain detection error constraints. A Markov-chain-based analytical model is constructed to systematically analyze the proposed scheme. With the analytical model, we are able to configure the system parameters for guaranteed performance in terms of false alarm rate, average detection delay, and missed detection ratio under a detection delay constraint. The simulations are conducted with MATPOWER 4.0 package for different IEEE test systems.**

***Index Terms*—Abnormal detection, CUSUM, false data injection attack, network security, signal detection and estimation, smart grid, quickest detection.**

I. Introduction

THE smart grid has improved the robustness and efficiency of traditional power grid networks by exploiting the modern technologies. In particular, information exchange among users, operators, and control devices significantly improves the efficiency in production, transmission, and distribution. However, integration of intelligence into the power grid needs to act punctually on abnormal situations (i.e., system fault, attacks, shortcut, etc.) [1].

Indeed, the smart grid is delay sensitive and requires the techniques that can identify and react on the abnormal changes in a timely manner. If the detection and responses are not made promptly, the grid may become unstable and further cause the catastrophic failures over the entire network. For example, in the control center of the smart grid, an essential task of the energy management system (EMS) is to estimate the system states by collecting data from remote meters periodically. If the adversaries are able to inject malicious data, EMS may produce the false state estimation, which potentially results in wrong decisions on billing, power dispatch, erroneous analysis, and even blackout [2]. Thus, the smart grid network must incorporate the protection mechanism, which has the capability of detecting the abnormal change and then making the decision as quickly as possible. Such an issue strongly motivates us to propose the quick detection-based detection scheme.

There are many studies on smart grid security in the literature. A framework for analyzing the impact of cyber-attacks in a smart grid was presented in [3] and [4]. The work in [5], [6], and [8] formulated the attacks that are able to evade the conventional detection in smart grids. The false data injections are studied in [9]–[11] as one type of the cyber-attacks in the power system. The authors in [12] discovered the microgrid vulnerability in the smarter power system under the false data injection attack. In [13], the false data injection attacks are shown to interrupt the energy-routing process. In this paper, we would like to focus on studying in the observable context with the proposed detection scheme that can be an interesting practical contribution for smart grid networks.

To address the false data injection attacks in the smart grid, EMS in the control center needs to be equipped with the capability of real-time detection of malicious attacks by analyzing the statistical behavior of the state estimation process. According to the quickest detection (QD) framework [14], the cumulative sum (CUSUM) based approach fits well to this type of detection problems because of its non-Bayesian properties. Such a framework aims to determine a change of the observed statistics as quickly as possible based on the online observations, the user-defined decision rules, and the requirement of detection accuracy. The decision rules should be properly designed to optimize the tradeoff between the stopping time and decision accuracy.

The QD technique is normally combined with the *statistical hypotheses test (SHT)* [15], [16]. The mechanism of SHT is that the receiver classifies a sequence of observations into one of the candidate hypotheses; a hypothesis normally represents a type of distributions. The QD and SHT have been applied to a variety

Manuscript received July 22, 2013; revised January 14, 2014; accepted May 8, 2014. Date of publication November 6, 2014; date of current version May 30, 2016. This work was supported in part by U.S. National Science Foundation CNS-0953377, CNS-0905556, CNS-0910461, ECCS-1028782, and CNS 1117560.

Y. Huang and Z. Han are with the Department of Electrical and Computer Engineering, University of Houston, Houston, TX 77204-4005 USA (e-mail: yhuang23@uh.edu; zhan2@uh.edu).

J. Tang and Y. Cheng are with the Department of Electronics and Computer Engineering, Illinois Institute of Technology, Chicago, IL 60616-3793 USA.

H. Li is with the Department of Electrical Engineering and Computer Science, University of Tennessee, Knoxville, TN 37996-2250 USA.

K. A. Campbell is with the Department of Electronics and Computer Engineering, Boise State University, Boise, ID 83725-2075 USA (e-mail: krisCampbell@boisestate.edu).

Digital Object Identifier 10.1109/JSYST.2014.2323266

of networks. The authors in [17] used the CUSUM tests as a collaborative QD for detecting a distribution change in *ad hoc* networks. The authors in [18] utilized the CUSUM test to address the real-time backoff misbehavior problem in IEEE 802.11 based wireless networks. However, not much existing work has considered the unique environment of smart grid networks.

In this paper, a countermeasure strategy of the false data injection attack is considered in the form of adversary detection. The problem formulation of detecting the false data injection is based on the bad data detection (BDD) for the smart grid state estimation. The proposed scheme is able to determine the existence of adversary as quickly as possible without violating the given constraints such as a certain level of detection accuracy in terms of the false alarm rate (FAR) and missed detection rate. In [19], we studied some preliminary works that include the basic mathematic derivation and numerical simulations; without loss of generality, one in conference version is motivated on the straightforward approach by directly evaluating the likelihood of load for detection decision, instead of formulating the algorithm based on the likelihood of residual in this paper, i.e., state estimation in power systems is based on measurement of residual, and therefore, the derivation and result from this journal can be more accurate and practical for real-world applications. In addition, the conference one measured a limited range of the unknown by utilizing one-side Rao test for simplicity, while this paper considers the quadratic equivalence of Rao test for solving the unknown. Essentially, this journal focuses on the thorough examination of the proposed algorithm in terms of analytical model and performance simulations. The development of an analytical model in this paper for the proposed algorithm provides theoretical guidance for quantitative performance analysis, and it further makes available the precious insight on system parameter configuration for guaranteed performance in terms of fundamental performance metrics. The main contributions are as follows.

1) We develop a framework for real-time detection of false data injection attacks in the smart grid network, under certain detection quality constraints. While the conventional state estimation [20], [21] for BDD focuses on balancing between the FAR and missing detection ratio, our approach aims to minimize the detection delay under the error probability constraint. In addition, the conventional approach makes decisions based on snapshot measurements only, but the proposed framework analyzes a sequence of samples for more reliable decisions over time.
2) The proposed algorithm is able to detect the presence of false data attacks in that the probability density function of the postchange is unknown due to the unknown parameters. However, the classical CUSUM test assumes the perfect knowledge of the likelihood functions. While the existing generalized likelihood ratio test (GLRT) approach can resolve the unknown parameters, it has high complexity. This paper proposes a new low-complexity approach with shorter decision delay and more accurate decision, which is asymptotically equivalent to the GLRT test.

TABLE I
DESCRIPTION OF SOME IMPORTANT SYMBOLS AND ABBREVIATIONS

Notation	Description
EMS	energy management system
QD	quickest detection
CUSUM	cumulative sum
SHT	statistical hypothesis test
BDD	bad data detection
AGC	automatic generation control
OPF	optimal power flow
ARL	average run length
GLRT	generalized likelihood ratio test
TPM	transition probabilities matrix
FAR	false alarm rate
MDR	misssed detection ratio
B	number of buses in power system
C	detection delay constraint
$\mathcal{H}_e$	hypothesis e in SHT
V_q	voltage measurement at the bus q
θ_q	phase measurement at the bus q
X_{qr}	reactance between bus q and r
M_{qr}	power flow measurement from bus q to r
M_q	power injection measurement at bus q
h	detection threshold, a function of error probability
n	observation index
m	total number of active power measurement
$\mathbf{Z}$	a vector of power measurement (M_qr,M_q, or both)
$\mathbf{x}$	the unknown state vector for state estimation
$\mathbf{e}$	a vector of measurement noise
$\mathbf{H}$	Jacobian matrix
T_D	detection delay for the proposed algorithm
T_h	the moment when detector raises the alarm
τ	the moment when adversary initializes the attack
S_n	CUSUM statistic at observation index n
$\mathbf{P}$	the transition probability matrix for Markov chain
π_i^0	the steady state probability that a detector starts from a normal state i
π_i	the steady state probability that a detector is at state i

3) An analytical model for the proposed algorithm is developed, which provides the theoretical guidance for quantitative performance analysis. With the analytical model, it gives the insight on system parameter configuration for the online detection of false data injection attacks. System parameters can also be computed for guaranteed performance in terms of three fundamental performance metrics: the FAR, average detection delay, and missed detection ratio under a detection delay constraint. In other words, our analytical model can guide us to configure a detection system based on some detection performance requirements.
4) The performance of the proposed algorithm is evaluated by both mathematical analysis and simulations. Note that simulations are conducted under MATPOWER 4.0 package [22] for different IEEE test systems to ensure the experimental accuracy and proficiency.

The remainder of this paper is organized as follows. Section II describes the system model. Section III presents and analyzes the newly proposed scheme, the *adaptive CUSUM algorithm*. Section IV develops the Markov-chain-based analytical model. Section V presents extensive numerical and simulation results for performance evaluation. Section VI gives the concluding remarks. Table I includes some important notations used in this paper.

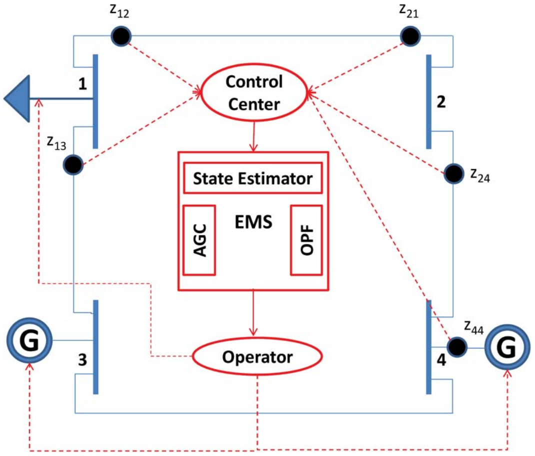

Fig. 1. Illustration of the four-bus power network, control center, few main functions (AGC, OPF, and EMS), and operator. Note that "G" represents the generators, the black dot represents the available active power flow measurements, and the triangle on the bus represents the load of the region or city.

II. Problem Formulation

Fig. 1 illustrates the IEEE four-bus test system with two generators. Each bus has its corresponding voltage (V_q) and phase angle (θ_q). The control center sends the power measurement data (z_{qr}) to the state estimator which generates an estimate of system state to be used in different functions such as the automatic generation control (AGC), optimal power flow (OPF), or EMS. The operator makes the final decision on generator control and load management.

As an essential role in the power system, the state estimator uses the steady-state system model to estimate the system status (i.e., the voltages at all buses over the time) [23]. Speaking in general, state estimation with a total of B active buses in a practical power system can be described as

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

where $\mathbf{Z}$ denotes the measurement data, $\mathbf{x}$ represents the unknown state including the voltage level V_q and the phase angle θ_q of each bus $q \in B$, and $\mathbf{e}$ is the Gaussian measurement noise with a zero mean and a covariance matrix $\boldsymbol{\Sigma}_e$. Noticing that a nonlinear $\mathbf{h}(\mathbf{x})$ is determined by the network topology, the real power flow from bus q to bus r can be expressed as

$$\begin{aligned} M_{qr} &= V_q^2(g_{sq} + g_{qr}) - V_q V_r (g_{qr}\cos\theta_{qr} + b_{qr}\sin\theta_{qr}) \\ \tilde{M}_{qr} &= -V_q^2(b_{sq} + b_{qr}) - V_q V_r (g_{qr}\cos\theta_{qr} - b_{qr}\sin\theta_{qr}) \end{aligned} \tag{2}$$

where the admittance of the series branch between buses q and r is $(g_{qr} + jb_{qr})$ and the admittance of the shunt branch at bus q is $(g_{sq} + jb_{sq})$. The formulations of real and reactive power injection can be constructed in the same way as that described in (2).

For simplicity, the linear state estimation model is applied in this paper. Notice that all shunt elements, bus, branch, and reactive power flow are neglected, and the bus voltage magnitude is known [20]. The power flow and power injection can be linearized and described as

$$\begin{aligned} M_{qr} &= \frac{\theta_{qr}}{X_{qr}} \\ M_q &= \sum_{r \in B_q} M_{qr} \end{aligned} \tag{3}$$

where M_q is denoted as the power injection, B_q is the set of bus numbers that are directly connected to bus q, and X_{qr} is the reactance between bus q and bus r. Furthermore, we can simplify[1] (1) to

$$\mathbf{Z}_n = \mathbf{H}\mathbf{x} + \mathbf{e}_n \tag{4}$$

where $\mathbf{H}$ is the constant Jacobian matrix, $\mathbf{Z}_n = [Z_{n,1}, \ldots, Z_{n,m}]^T$ with m measurements at the observation index $n \in 1, 2, 3, \ldots,$ and $\mathbf{x} = [\theta_2, \ldots, \theta_B]^T$. Notice that phase angle θ_0 for bus 0 is assumed known as a reference angle, and the size of $\mathbf{Z}_n$ is normally greater than that of $\mathbf{x}$ [20], [24]. One objective of (4) is to determine the $\hat{\mathbf{x}}$ which can minimize

$$(\mathbf{Z}_n - \mathbf{H}\hat{\mathbf{x}})^T \boldsymbol{\Sigma}_e^{-1} (\mathbf{Z}_n - \mathbf{H}\hat{\mathbf{x}}).$$

By applying the weighted least square, the estimated system state $\hat{\mathbf{x}}$ is

$$\hat{\mathbf{x}} = \left(\mathbf{H}^T \boldsymbol{\Sigma}_e^{-1} \mathbf{H}\right)^{-1} \mathbf{H}^T \boldsymbol{\Sigma}_e^{-1} \mathbf{Z}_n. \tag{5}$$

For BDD systems, we compare the power flow measurements $\mathbf{Z}_n$ with the estimated active power flow $\hat{\mathbf{Z}}_n$ by the phase angle estimate $\hat{\mathbf{x}}$. $\hat{\mathbf{Z}}_n$ can be written as

$$\hat{\mathbf{Z}}_n = \mathbf{H}\hat{\mathbf{x}} = \mathbf{H}\left(\mathbf{H}^T \boldsymbol{\Sigma}_e^{-1} \mathbf{H}\right)^{-1} \mathbf{H}^T \boldsymbol{\Sigma}_e^{-1} \mathbf{Z}_n = \Im \mathbf{Z}_n \tag{6}$$

where $\Im$ is known as the *hat matrix*. Define the residue vector as

$$\mathbf{R}_n = \mathbf{Z}_n - \hat{\mathbf{Z}}_n. \tag{7}$$

The expected value and the covariance of residual $\mathbf{R}_n$ are

$$E(\mathbf{R}_n) = \mathbf{0} \tag{8}$$

$$\boldsymbol{\Sigma}_{\mathbf{R}} = \left[\mathbf{I} - \mathbf{H}\left(\mathbf{H}^T \boldsymbol{\Sigma}_e^{-1} \mathbf{H}\right)^{-1} \mathbf{H}^T \boldsymbol{\Sigma}_e^{-1}\right] \boldsymbol{\Sigma}_e \tag{9}$$

respectively. The system can perform BDD by analyzing $\mathbf{R}_n$ [20].

In brief, the conventional state estimation for false data injection detection uses only snapshot measurements, and therefore, we like to apply the online QD technique using a sequence of measurements for more reliable decisions.

III. Adaptive CUSUM Algorithm

In this paper, we propose an adaptive CUSUM algorithm for real-time detection of false data attacks in smart grid state estimation. The proposed scheme evaluates the measurements before the potential bad data are removed by BDD. The detection system formulation as presented in [14] and [26] is no longer useful in the scenario under our consideration because

[1] The DC model is adopted due to practical security constraint unit commitment and market operations. Most of the control centers use a linear power model for state estimation because of two reasons. First, the phase differences are relatively small so that a linear model can be employed. Second, due to the complexity of computing the AC model, the linear model is used for real-time analysis in the power system operation [25].

unknown parameters exist in the postchange distribution and may dynamically change over the detection process. Our main motivation is to derive a detection model considering the existence of the unknown and then develop an analytical model that can guide us configure the detection system for guaranteed performance. The proposed scheme does not require the maximum likelihood (ML) estimate of the unknown, thereby making the computation process much simpler.

Under a false data injection attack, the false data $\mathbf{b}_n$ is maliciously injected into the power flow measurement vector as

$$\mathbf{Z}_n = \mathbf{H}\mathbf{x} + \mathbf{b}_n + \mathbf{e}_n. \tag{10}$$

Residual vector $\mathbf{R}_n$ can be well approximated by a Gaussian random variable because of Gaussian thermal measurement noise $\mathbf{e}_n$ [7], [27]. When there is no attack, the residual vector $\mathbf{R}_n$ follows Gaussian distribution $\mathcal{N}(\mathbf{0}, \mathbf{\Sigma_R})$. Under attack, $\mathbf{R}_n$ follows $\mathcal{N}(\mathbf{a}_n, \mathbf{\Sigma_R})$, where

$$\mathbf{a}_n = \mathbf{K}\mathbf{b}_n \tag{11}$$

where $\mathbf{K} = (\mathbf{I} - \mathfrak{S})$. Notice that $\mathbf{a}_n = [a_{n,1}, a_{n,2}, \ldots, a_{n,m}]^T$, $\in \mathbb{R}^m$ is not known *a priori* (i.e., the adversary's statistical model, attack patterns, or mathematical distributions cannot be known in advance. This issue will be addressed later in this section.). Then, we have the binary hypothesis as

$$\begin{cases} \mathcal{H}_0: & \mathbf{R}_n \sim \mathcal{N}(\mathbf{0}, \mathbf{\Sigma_R}) \\ \mathcal{H}_1: & \mathbf{R}_n \sim \mathcal{N}(\mathbf{a}_n, \mathbf{\Sigma_R}) \end{cases} \tag{12}$$

and assume that the false data injection becomes active at random-time moment τ, in other words a change of the distribution from $\mathcal{N}(\mathbf{0}, \mathbf{\Sigma_R})$ to $\mathcal{N}(\mathbf{a}_n, \mathbf{\Sigma_R})$ at τ. Note that we process the measurement data before a BDD removes the potential residual.

We denote T_h as the stopping time for declaring the best arm under current observation. τ is a change time. In other words, it is the switch point from one distribution that belongs to the normal state to another distribution under the attack. Based on the Lorden's formulation [14], we minimize the worst case of detection delay, which can be described as

$$T_D = \inf\nolimits_{T_h \in \mathcal{T}} \text{ sup esssup } E_\tau \left[(T_h - \tau + 1)^+ | \mathcal{F}_{\tau-1} \right] \tag{13}$$

where $\tau > 1$, $\mathcal{F}_\tau$ denotes the smallest α-field with respect to the observations, $\mathcal{T}$ is the set of all stopping time with respect to $\mathcal{F}_\tau$, and E_τ is the expectation that the change time is τ. However, most CUSUM-based models assume the perfect knowledge of the likelihood functions [26]. In the scenario of intrusion detection in smart grid state estimation, the variable from the $\mathcal{H}_1$ distribution cannot be completely defined because of the unknown. The detection also needs to address the issue that multiple measurements are correlated each together in a single online observation. Thus, we need to employ the technique to solve the issues for real-time detection of false data injection in smart grid networks.

The proposed QD algorithm is recursive in nature, and each recursion comprises two interleaved steps: 1) unknown variable solver based on Rao test and 2) multithread CUSUM test. The proposed CUSUM algorithm updates a likelihood ratio term based on a series of power measurements with a stopping time T_h, described as

$$T_h = \inf\{n \geq 1 | S_n > h\} \tag{14}$$

where the detection threshold h is a function of FAR and its value is determined numerically. We will discuss how to determine the value of h in Section IV. At nth, the cumulative statistic S_n can be solved recursively and described as

$$S_n = \max[\,0, S_{n-1} + L_n] \tag{15}$$

where S_n returns to zero for statistical accuracy if its value is negative, $S_0 = 0$ initially, and

$$L_n = \log \frac{f_1(\mathbf{R}_n)}{f_0(\mathbf{R}_n)} \tag{16}$$

being the likelihood ratio function based on the nth round of measurement denoted as the observation vector $\mathbf{R}_n$ $(R_{n,l}, l \in 1, 2, \ldots, m)$. In (16), $f_1(\mathbf{R}_n)$ is the distribution associated with the hypothesis $\mathcal{H}_1$ with false data injection, and $f_0(\mathbf{R}_n)$ is the distribution associated with the hypothesis $\mathcal{H}_0$ in the normal state. Therefore, the control center is able to declare the alarm when the accumulation crosses a certain threshold h, the cumulative process is terminated, and average run length (ARL) is equivalent to T_h.

As the value of $\mathbf{a}_n$ in (11) is unknown, the author in [28] proposed to implement the GLRT in the Page's CUSUM algorithm with the unknown. The idea is to apply likelihood ratio test (LRT) by replacing the unknown with the ML estimation. The GLRT approach is asymptotically minimax and can be written as

$$S_n = \min_{1 \leq n \leq T_h} \max_{a_n} \sum_{i=n}^{T_h} \log \frac{f_1(\mathbf{R}_i | \mathbf{a}_i)}{f_0(\mathbf{R}_i)}. \tag{17}$$

In other words, we minimize the effect of the unknown while considering the worst case situation (i.e., the second maximization in (17)). Thus, by applying GLRT in the CUSUM algorithm, we can ensure a certain level of detection accuracy for QD while minimizing the potential effect from the unknown in the system. However, the recursive expression of (17) for the CUSUM test is no longer available, as shown in (15). It is because GLRT needs to compute every unknown element of $\mathbf{a}_n$ based on samples up to the current observation n. In other words, the GLRT approach requires storing the estimated data and ML-estimating the unknown at every point. Thus, in practice, the GLRT is too difficult from the viewpoints of hardware and software implementation. Moreover, the work in [29] states that Rao test might be more robust but less complex than the GLRT real operating situations. In [30], the performance of Rao-test-based detectors is better than GLRT in parameter estimation and handling training-free scenarios.

For the multithread CUSUM algorithm, the desired approach is to solve the unknown recursively, avoiding ML estimation. Thus, we consider the Rao test [31], which is asymptotically equivalent to the GLRT. The derivation of the Rao test is similar to the locally most powerful test but much simpler. The Rao test has the straightforward calculation by taking the derivative of L_n with respect to the unknown evaluated around the region of interests. In our case, we analyze the case where the region is around zero because the hypothesis $\mathcal{H}_0$ has zero mean. The statistic [31] of the Rao test for detection can be modified and rewritten as follows at observation n:

$$\mathcal{I}(\mathbf{R}_n) = \frac{\partial L_n}{\partial \mathbf{a}_n}\bigg|_{\mathbf{a}_n=\mathbf{0}}^{T} \left[\mathbf{J}^{-1}(\mathbf{a}_n)\big|_{\mathbf{a}_n=\mathbf{0}}\right] \frac{\partial L_n}{\partial \mathbf{a}_n}\bigg|_{\mathbf{a}_n=\mathbf{0}} \tag{18}$$

where $\mathbf{J}$ is the Fisher information matrix [32]. By inspecting (18) and evaluating (11) and (12), we notice that the computation of the inverse Fisher information matrix can be simplified and equivalent to the covariance of residual.

Based on (12), we can write the binary hypothesis $\{\mathcal{H}_0, \mathcal{H}_1\}$ by expanding the multivariate normal distributions. Next, we apply (18) to (16) by taking its derivative with respect to $\mathbf{a}_n$ evaluated at $\mathbf{a}_n = \mathbf{0}$. Finally, by recursion, the multithread CUSUM-based statistic can be described as follows:

$$S_n = \max\{0, S_{n-1} + \mathcal{I}(\mathbf{R}_n)\} \tag{19}$$

where $\mathcal{I}(\mathbf{R}_n) = [(\mathbf{R}_n^T \boldsymbol{\Sigma}_{\mathbf{R}}^{-1})^T + \boldsymbol{\Sigma}_{\mathbf{R}}^{-1}\mathbf{R}_n]^T \boldsymbol{\Sigma}_{\mathbf{R}} [(\mathbf{R}_n^T \boldsymbol{\Sigma}_{\mathbf{R}}^{-1})^T + \boldsymbol{\Sigma}_{\mathbf{R}}^{-1}\mathbf{R}_n]$. Notice that the cumulative statistic is now independent from the unknown variable, and (19) becomes a scalar quantity once it is computed. In summary, the control center observes actual power flow measurements and generates the vector of residual from m measurement samples taken in the nth round of observation. The proposed scheme is composed of two interleaved steps: the unknown variable solver and the multithread CUSUM test. The control center will monitor the CUSUM statistic in (19) against the threshold to detect the false data injection attacks. The alarm rises when the CUSUM statistic S_n exceeds the threshold. The framework of the adaptive CUSUM algorithm of the proposed scheme is shown in Algorithm 1.

Algorithm 1 Adaptive CUSUM algorithm

```
    $n \leftarrow (1, 2, 3 \cdots)$
    $\mathbf{R}_n \leftarrow$ compute the difference between $\hat{\mathbf{Z}}$ and $\mathbf{Z}$.
    **repeat**
        **Update of**: $n \leftarrow n + 1$
        continues the observation
        **Unknown solver based on Rao test**:
        eliminate $\mathbf{a}_n$ by taking derivative of $L_n$ with respect $\mathbf{a}_n$ evaluated at $\mathbf{0}$
        **Multithread CUSUM test**:
        compute recursively $S_n$ for all $m$ measurements at current $n$ as shown in (19)
    **until** $T_h = \inf\{n \geq 1 | S_n > h\}$ is determined
    Terminate the adaptive CUSUM process
    Report the determined hypothesis and ARL
```

IV. Markov-Chain-Based Analytical Model

In this section, we develop the Markov-chain-based analytical model to systematically examine the proposed scheme for the false data injection attack. The Markov-chain-based model produces quantitative performance analysis and provides theoretical guidance on the system configuration for performance guarantee in terms of three fundamental performance metrics: the expectation of FAR, the expectation of missing-detection rate, and the expectation of detection delay.

A. Analysis Model

For analysis purposes, we discretize $\mathbb{R}^+ \bigcup 0$ into the finite sets $\{U_1, \ldots, U_{F-1}, U_F\}$, where $U_1 = 0$ and U_F is the set whose value is greater than or equal to h. In other words, F is the total number of transition from 0 to the state that has the value greater than or equal to h. There are several approaches for discretization [33], [34]. In this paper, we employ uniform sampling without loss of generality. Alternative discretization methods can also be employed, like the μ-law or A-law in the pulse-code modulation. Moreover, from (19), we know that the sequence exhibits the Markov property, where the current state $j = S_n$ at observation n only depends on the previous state $i = S_{n-1}$ at $n - 1$ but not on the past history [35].

The transition probabilities of the Markov chain for the proposed scheme from state i at $(n - 1)$ to state j at n can be described as

$$\begin{aligned} P_{ij} &= P(S_n = j | S_{n-1} = i), \text{under } \mathcal{H}_0;\\ \hat{P}_{ij} &= P(S_n = j | S_{n-1} = i), \text{under } \mathcal{H}_1. \end{aligned} \tag{20}$$

Note that the Markov-chain-based analytical model for the proposed scheme involves two different transition probability matrices (TPMs): one is under the normal state environment, and the other one is under the false data attack. The normal TPM can help in determining the initial state as well as FAR. With the initial states, the average detection delay and detection delay can be analyzed by using the TPM under attack. We can calculate TPMs: $\mathbf{P}$ and $\hat{\mathbf{P}}$ with the size of $(F + 1) \times (F + 1)$, under the hypothesis $\mathcal{H}_0$ and $\mathcal{H}_1$ according to $f_0(\mathbf{R}_n)$ and $f_1(\mathbf{R}_n)$, respectively. Here, we assume that the attacker's strategy is stationary. If the attackers' attack has zero mean but nonzero variance, the hypothesis test problem becomes detecting the different variances with versus without attack. If the attackers' attack has nonzero mean and nonzero variance, the hypothesis test has two dimensions (mean and variance). Both cases can be investigated by a similar way to our current analysis (attacker has nonzero mean and zero variance). Due to page limitation, we leave this for the future study.

The initial steady-state probability of the Markov chain, where the process starts from a normal state, can be determined as

$$\pi_j^0 = \frac{\pi_j}{\sum_{i=0}^{F-1} \pi_j}, \quad \text{given} \quad j \in \{0, U_1, \ldots, U_{F-1}\} \tag{21}$$

and the steady-state probability can be determined

$$\pi_j = \sum_{i=0}^{F} P_{ij}\pi_i \tag{22}$$

where $j \in \{0, U_1, \ldots, UF\}$ and $\sum_{j=0}^{F} \pi_j = 1$.

Next, based on the Markov chain model, we study the theoretical performance analysis of detection delay, FAR, and missed detection ratio expectations, respectively, in the following sections.

B. Expectation of Detection Delay

To determine the expectation $(E_{\hat{\mathbf{P}}}[T_D])$ of detection delay, we utilize the weighted average of the expected number of transitions from every initial state $(\pi_0^0, \pi_1^0, \ldots, \pi_{F-2}^0, \pi_{F-1}^0)$ to state U_F based on $\hat{\mathbf{P}}$. We set $\Omega_{gF},\ g \in \{0, U_1, \ldots, U_{F-1}\}$, as the expected number of transitions for state g to state U_F. Following the derivation from [35], the numerical value of Ω_{iF} can be determined as follows:

$$\Omega_{iF} = 1 + \sum_{g \neq F} \hat{P}_{ig} \Omega_{gF} \tag{23}$$

where the transition probability $\hat{P}_{ig} \in \hat{\mathbf{P}}$ is from state i to state g. The expectation of detection delay can be obtained from the results of (21) and (23)

$$E_{\hat{\mathbf{P}}}[T_D] = \sum_{i=0}^{F-1} \pi_i^0 \Omega_{iF}. \tag{24}$$

C. Expectation of FAR

The expectation $(E_{\mathbf{P}}[\text{FAR}])$ of FAR is the probability that the proposed CUSUM statistic S_n reaches to the state U_F when there is no attacker in the network. As described in [35], $E_{\mathbf{P}}[\text{FAR}]$ is equivalent to the probability that S_n stays at state U_F (i.e., exceeding threshold h) under hypothesis $\mathcal{H}_0$.

According to [35], it states the TPM $\mathbf{P}$ always has a special eigenvector with only one eigenvalue $\lambda = 1$ and the rest is zero. Thus, we can obtain the solution by re-elaborating (22) into the matrix form as

$$\begin{bmatrix} P_{00}-1 & P_{01} & \cdots & P_{0F} \\ P_{10} & P_{11}-1 & \cdots & P_{0F} \\ \vdots & \vdots & \ddots & \vdots \\ P_{F0} & P_{F1} & \cdots & P_{FF}-1 \\ 1 & 1 & \cdots & 1 \end{bmatrix} \begin{bmatrix} \pi_0 \\ \pi_1 \\ \vdots \\ \pi_F \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 1 \end{bmatrix}. \tag{25}$$

By least squares estimation, the average FAR can be determined by

$$E_{\mathbf{P}}[\text{FAR}] = \pi_F. \tag{26}$$

D. Expectation of Missed Detection Ratio

We define the missing detection probability as the probability that the detection delay is greater than or equal to a detection delay constraint C. The expectation $(E_{\hat{\mathbf{P}}}[\text{MDR}])$ of the missing detection probability is, starting from the initial state, the summation of probabilities that S_n stays at a state other than state U_F at time C. Let $p_i(s)$ denote the probability of the state variable at time s and at state i. We set the initial condition for the transition probabilities as

$$p_i(0) = \pi_i^0 \tag{27}$$

where $i \in \{0, U_1, \ldots, U_{F-1}\}$ and $p_F(0) = 0$. By the iteration, at each s, the state probability vector is updated by the previous state probability vector in a matrix form as

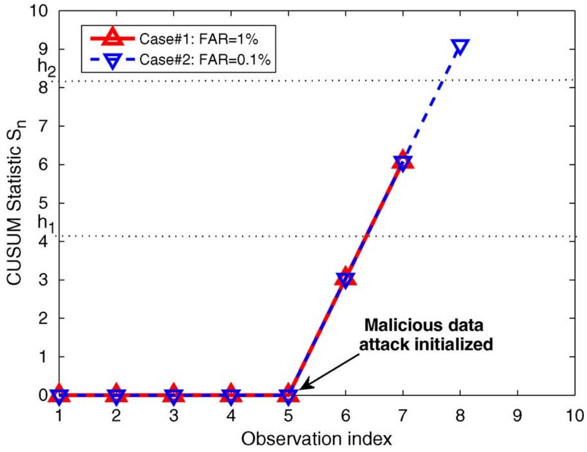

Fig. 2. Simulation of the adaptive CUSUM algorithm. The x-axis is the observation index (n), and the y-axis is the recursive CUSUM statistic (S_n). Case 1 with FAR of 1% corresponds to h_1, and case 2 with FAR of 0.1% corresponds to h_2. The proposed algorithm signals the alarm and then terminates the process at $T_h = 7$ and 8, respectively.

$$\begin{bmatrix} p_0(s) \\ p_1(s) \\ \vdots \\ p_{F-1}(s) \\ p_F(s) \end{bmatrix}^T = \begin{bmatrix} p_0(s-1) \\ p_1(s-1) \\ \vdots \\ p_{F-1}(s-1) \\ p_F(s-1) \end{bmatrix}^T \hat{\mathbf{P}} \tag{28}$$

$$p_F(s) = 0, \quad s \in \{0, C-1\}. \tag{29}$$

Here, the $p_F(s)$ at every s of state U_F is reset to zero for the next iteration since we only concern the missing detection case only. The expectation of missed detection ratio under the given delay constraint C can be obtained as

$$E_{\hat{\mathbf{P}}}[\text{MDR}] = \sum_{i=0}^{F-1} p_i(C). \tag{30}$$

V. Performance Analysis

In this section, we present the analytical and numerical simulations to demonstrate the performance of the proposed scheme. This section is composed of two main sections. The first section demonstrates the performance of the proposed scheme from the simulated data. In other words, we heuristically configure the parameter and analyze the detection performance. The second section involves both analytical and numerical results under the realistic power test systems by MATPOWER 4.0 package [22]. Without loss of generality, we assume that the simulation has normalized sample rate[2] and the static system.[3] Note that the adversary is able to inject the false power flow measurement at the random time.

[2] Since the measured noise is white Gaussian (independent over time), the performance of the QD depends on the number of observations. In other words, the decision time is related to the sampling rate, and the decision time is equivalent to the number of observation divided by the sampling rate.

[3] The reason that we have a steady-state or quasi-steady-state system is that our algorithm can converge in a very short time. For the PJM network, it is able to have state estimation for measurement of more than 2000 buses per minute [25]. From the simulation, we can see that our algorithm converges around 100 samples. In other words, our algorithm can converge within a couple of seconds, during which the states can be considered at least quasi-steady.

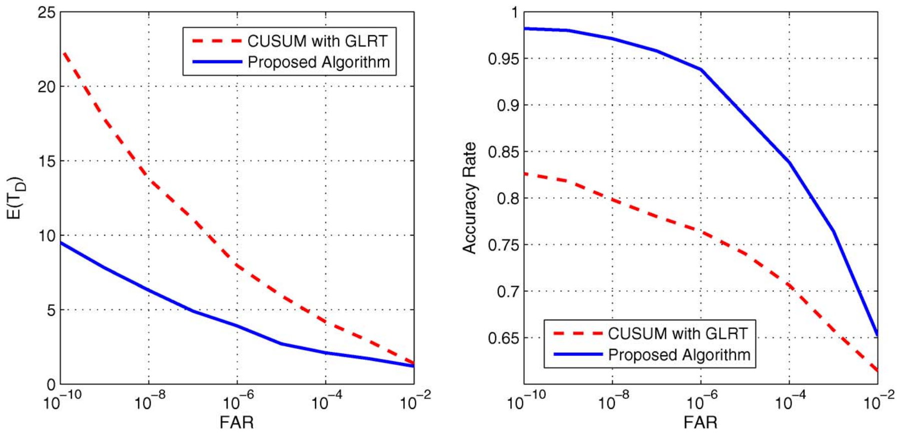

Fig. 3. Performance analysis of the adaptive CUSUM algorithm in comparison with CUSUM GLRT.

A. *Simulation Results With Simulated Data*

Fig. 2 illustrates the relation between the detection parameters (S_n, h) and performance metrics (FAR and T_D). The number of measurements $m = 4$. On the detector side, the detector has no information about the adversary statistical model, distribution, or any unknown. The adversary manipulates and injects the false data into the system at the random time. As shown in Fig. 2, we consider that case 1 has a FAR of 0.01 and case 2 has a FAR of 0.0001. The adversary becomes active and injects the false data at $n = 6$. In other words, a change distribution is at $\tau = 6$ from $\mathcal{N}(0, \mathbf{\Sigma_R})$ to $\mathcal{N}(\mathbf{a}_n, \mathbf{\Sigma_R})$, where $\mathbf{a}_n$ is unknown. For both cases, the curve of adaptive CUSUM statistic (S_n) shows the sudden increase right after a change of distributions. The proposed algorithm quickly responses the abnormal event by signaling an alarm when S_n passes the threshold. At observation index 7, the threshold parameters h_1 and h_2 correspond to case 1 and case 2, respectively. As a result, h_1 is less than h_2 because of the different FARs. For the smaller FAR, the stricter constraint that causes increasing the threshold, the higher requirement for system to declare the decision. The ARLs (T_h) of the adaptive CUSUM algorithm are 7 and 8 at S_n of 6.07 (case 1) with $h = 5.97$ and 9.11 (case 2) with $h = 8.19$, respectively. The ARL (T_D) of detection delay is 1 for cases 1 and 2 for case 2 in this simulation. The proposed algorithm is able to signal the alarm and terminates the process after the active false date attack.

Fig. 3 shows the characteristics of the proposed algorithm by varying FAR for the accuracy rate and expected $(E[T_D])$ of detection delay in comparison to that of the CUSUM GLRT. We run 5000 realizations for the simulation. FAR varies from 10^{-10} to 10^{-2}. The false data injection begins at the sixth observation index. The accuracy rate in Fig. 3 (right) represents the ratio of successful detection that the algorithm terminates the process and declares the existence of adversary after the sixth observation index (the actual attack index). As shown in the figure for both the proposed scheme and the CUSUM GLRT, the stricter FAR is, the greater expected detection delay and higher detection accuracy we have. The expected detection delay of CUSUM GLRT seems to increase exponentially, while that of the proposed scheme steadily rises as FAR decreases. $E[T_D]$ of the proposed scheme has the average 50% less than that of CUSUM GLRT. We also obtain the better accuracy rate as FAR decreases. By giving the sufficiently low FAR, the proposed scheme is able to reach the accuracy above 95%, while CUSUM GLRT struggles it below 83%. Therefore, the proposed scheme outperforms the CUSUM GLRT in terms of shorter decision time and higher detection accuracy. The simulation result also shows the tradeoff between the detection delay, false alarm, and accuracy rate. The smaller FAR causes higher delay but better accuracy, i.e., the system needs to spend more observations for making a decision.

B. *Simulation Results With MATPOWER 4.0*

For the experimental setup of this section, we first apply the analytical model to theoretically analyze the performance of the detection system for guiding the system parameter configuration. Then, we use the parameter from the theoretical analysis to confirm the accuracy of the analysis in the first half of the section and then demonstrate the performance of the detection system in the second half of the section.

1) Accuracy of the Analytical Model: In this section, the power flow data for all simulations are generated by MATPOWER 4.0 instead of random independent variables in the previous section. MATPOWER 4.0 is a MATLAB simulation tool for solving power flow and OPF problems. It provides realistic power flow data and test systems that are used widely in research-oriented studies as well as in practice. We consider four popular IEEE test systems from the MATPOWER 4.0 package. Case 1 is the IEEE four-bus test system, which has two generators for four measurements; case 2 is the IEEE 57-bus test system, which has 7 generators for 80 measurements; case 3 is the IEEE 118-bus test system, which has 54 generators for 186 measurements; and case 4 is the IEEE 2383-bus test system, which has 326 generators for 2896 measurements. The analytical performance measures and the simulation results are compared under the same setting and input data to examine. Hence, by using power flow data sets with four different study cases from MATPOWER 4.0, the performance indices $(E[\text{FAR}], E[\text{MDR}], E[T_D])$ comparisons between the analytical and simulation results can be conducted. With the parameter from the theoretical analysis, the performance indices are

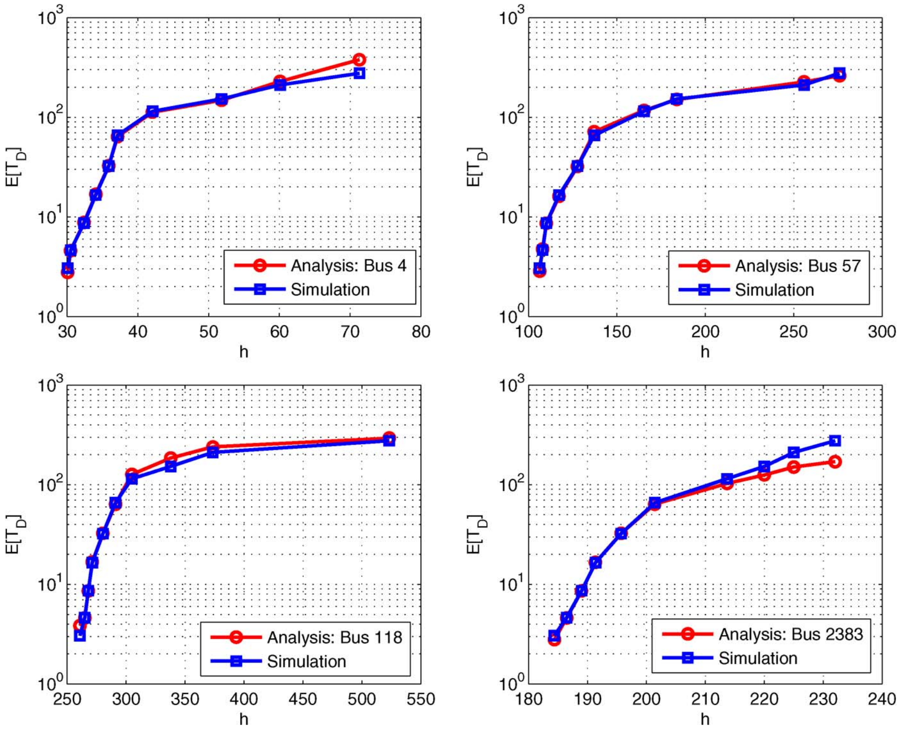

Fig. 4. Expectation $E[T_D]$ of detection delay for different IEEE bus test systems.

simulated so that we can properly configure the proposed algorithm for the guaranteed performance. Notice that both theoretical analysis and simulation are plotted together to confirm the accuracy of the analysis and demonstrate the performance.

Fig. 4 gives us an insight of the relationship between the system parameters h and the detection delay $E[T_D]$ of the proposed scheme. The higher the threshold, the larger the delay. Also, shown in Fig. 4, both analytical and simulation results are matched closely in all IEEE 4-bus, 57-bus, and 118-bus test systems. The maximum difference between the analysis and simulation is around 2% in the case of the IEEE 2383-bus test system.

The numerical examination is presented to understand the impact of the fundamental performance metric FAR on system parameters h of the proposed scheme. As shown in Fig. 5, the analytical and simulation results are close. Note that the logarithmic scale is used in the figure for the vertical axis. In cases of IEEE 4-bus and 57-bus test systems, the difference percentage between the analysis and simulation is very small and near zero. However, as the number of buses increases (the total number of active power flow measurement increases, too), the maximum difference percentage is about 8% in the IEEE 2383-bus test system. More measurements can cause the larger variance when we try to calculate the covariance for computing $\mathbf{R}$. From the figure, we also can observe that a larger h yields a smaller FAR as expected.

The analytical result of $E[\mathrm{MDR}]$ is demonstrated under two scenarios of the delay constraints, in which $C = 7$ and $C = 18$. The result is shown in Fig. 6, which helps us study the impact of the missed detection ratio on h of the proposed scheme. The logarithmic scale is used in the figure for the vertical axis. From the figure, the larger constraint C results to a smaller expectation of missed detection ratio as expected. In other words, the probability of detection rises if we allow to increase the cost of longer delay. We also compute the mean of expected missed detection ratio as the baseline, in comparison with the analytical results for four different IEEE test systems. The trend of analysis follows the baseline closely. However, as the number of active power flow measurement increases, the gap between them becomes obvious, particularly, in case of the IEEE 2383-bus test system, the maximum difference percentage is obtained around 10%. More measurements can cause the larger variance when we try to calculate the covariance for computing $\mathbf{R}$. In addition, the smaller h is, the better the expectation of missed detection ratio that corresponds to the result of expected FAR in Fig. 5 as the tradeoff.

2) Detection With Performance Guarantee: From Figs. 4–6, we demonstrate the performance metrics with different h. It also helps us to configure the system parameter h for guaranteed performance under three fundamental metrics. For each different IEEE test system, we can select the proper configuration of h from the reasonable range to satisfy the desired performance constraints. For example, the configuration of h is set to 135 for the IEEE 57-bus test system; the analytical model of the proposed scheme shows the expectation of the FAR of 0.001, the expectation of the detection delay of 20, and the expectation of the missed detection ratio of 0.00005 under the delay constraint $C = 18$. In addition, if we wish to have a certain level of detection probability, we can compute the numerical value of detection probability from Fig. 4; with its corresponding h, we can explicitly determine the cost of detection delay from Fig. 4 and the tradeoff for the FAR from Fig. 5. The aforementioned analysis can be extended to other IEEE power systems in a similar way.

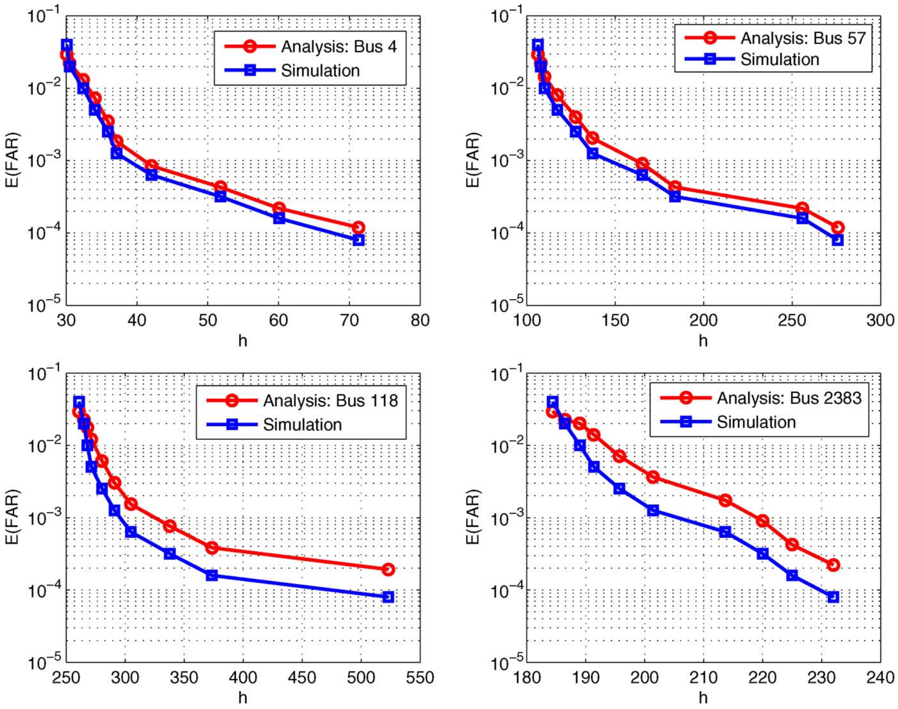

Fig. 5. Expectation $E[\text{FAR}]$ of FAR for different IEEE bus test systems.

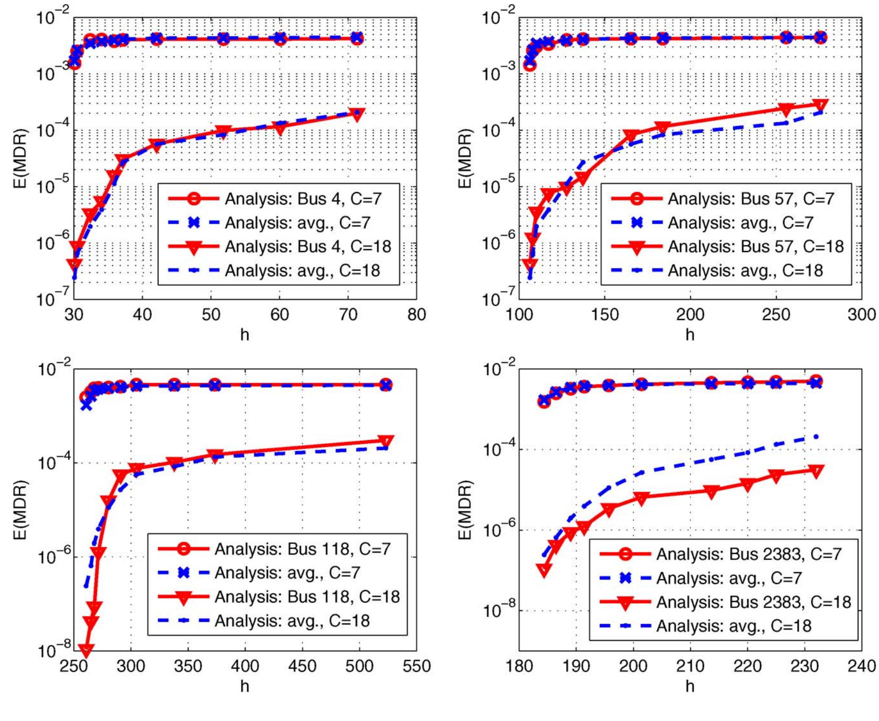

Fig. 6. Expectation $E[\text{MDR}]$ of missed detection ratio for different IEEE bus test systems.

In Fig. 7, we show the CUSUM statistics S_n over observation index n for the IEEE 4-bus, 57-bus, and 118-bus test systems. For the simulation setup, we consider that the FAR of 0.01 is presented, and the active false data injection attack is initialized after observation index 15. For the simulation results, in the IEEE four-bus test system, the system is alarmed after 24 observations with the corresponding detection threshold of 34.51; the detection delay is 9. In the IEEE 57-bus test system, the system is alarmed after 37 observations with the corresponding detection threshold of 133.52 and the detection delay of 22. In the IEEE 118-bus test system, the system is alarmed after 45 observations with the corresponding detection threshold of 283.14; the detection delay in this test system is 30. As expected, the simulation also shows that the detector needs more observations to make the decision when the number of the power flow measurements and buses increases. Notice that the numerical results of each IEEE test system in Fig. 7 correspond to our analytical results, which are presented in Figs. 4–6.

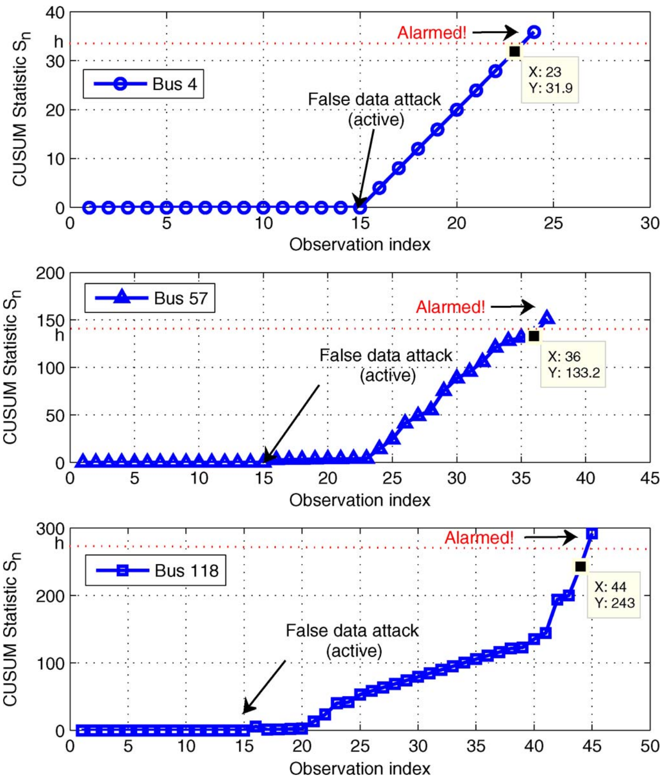

Fig. 7. Detection simulation of the adaptive CUSUM algorithm with MATPOWER 4.0 power flow measurements for the IEEE 4-bus test system, IEEE 57-bus test system, and IEEE 118-bus test system. The x-axis is the observation (n), and the y-axis is the recursive CUSUM statistic (S_n). The proposed algorithm signals the alarm and then terminates the process at $T_h = 24, 37,$ and 45, respectively.

VI. Conclusion

In this paper, we have proposed the adaptive CUSUM algorithm for defending false data injection attacks in smart grid networks. We have successfully derived a detection model by considering the existence of the unknown and then developed an analytical model that can guide us configure the detection system for performance guarantee based on the fundamental detection requirements. Our proposed scheme for smart grid state estimation is composed of two interleaved steps: 1) introduces the unknown variable solver technique based on the Rao test and 2) applies the multithread CUSUM algorithm for determining the possible existence of adversary as quickly as possible without violating the given constraints. Furthermore, we have developed the Markov-chain-based analytical model to characterize the behavior of our proposed scheme. We can quantitatively study the system parameters to achieve the guaranteed detection performance in terms of three fundamental metrics (E[FAR], E[MDR], and $E[T_D]$). The analytical and numerical simulation results have shown that the proposed scheme is efficient in terms of detection accuracy and minimum detection delay. Overall, the proposed scheme is able to achieve the important objectives of smart grid security in terms of real-time operation and security requirement.

In future work, we further investigate the optimality of a joint attack detection and state estimation in smart grid. When an attacker occurs in the power network, the ultimate objective of the network operator is beyond a reliable detection of the attack. In fact, detecting the attack will be used as an intermediate step toward obtaining a reliable estimate about the injected false data, which, in turn, facilitates eliminating the disruptive effects of the false data. Assuring good estimation performance is the core of the estimation and detection problem in the smart grid networks. To account for the significance of estimation quality, we can define an estimation performance of measure and seek to optimize it while ensuring satisfactory detection performance. The objective is to minimize the estimation-related cost subject to appropriate constraints on the tolerable levels of detection errors. This approach can provide the operator with the freedom to strike desired balance between estimation and detection qualities. Other future work can include the analysis of load/generation disruption and joint consideration with PMU.

References

[1] *The Smart Grid: An Introduction*, U.S. Department of Energy (DOE), Washington, DC, USA, Sep. 2012, U.S. Department of Energy Book: Smart Grid Series.

[2] E. Hossain, Z. Han, and V. Poor, *Smart Grid Communications and Networking*. Cambridge, U.K.: Cambridge Univ. Press, 2012.

[3] D.-H. Choi and L. Xie, "Ramp-induced data attacks on look-ahead dispatch in real-time power markets," *IEEE Trans. Smart Grid*, vol. 4, no. 3, pp. 1235–1243, Sep. 2013.

[4] D. Kundur, X. Feng, S. Liu, T. Zourntos, and K. L. Butler-Purry, "Towards a framework for cyber attack impact analysis of the electric smart grid," in *Proc. IEEE Conf. Smart Grid Commun.*, Oct. 2010, pp. 244–249.

[5] S. McLaughlin, B. Holbert, A. Fawaz, R. Berthier, and S. Zonouz, "A multi-sensor energy theft detection framework for advanced metering infrastructures," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 7, pp. 1319–1330, Jul. 2013.

[6] M. Ozay, I. Esnaola, F. T. Y. Vural, S. R. Kulkarni, and H. V. Poor, "Sparse attack construction and state estimation in the smart grid: Centralized and distributed models," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 7, pp. 1306–1318, Jul. 2013.

[7] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Malicious data attacks on smart grid state estimation: Attack strategies and countermeasures," in *Proc. IEEE Conf. Smart Grid Commun.*, Oct. 2010, pp. 220–225.

[8] C.-H. Lo and N. Ansari, "NSUMER: A novel hybrid intrusion detection system for distribution networks in smart grid," *IEEE Trans. Emerging Topics Comput.*, vol. 1, no. 1, pp. 33–44, Jun. 2013.

[9] I. Matei, J. S. Baras, and V. Srinivasan, "Trust-based multi-agent filtering for increased smart grid security," in *Proc. 20th Mediterranean Conf. Control Autom.*, Jul. 2012, pp. 716–721.

[10] Y. Huang *et al.*, "Adaptive quickest estimation algorithm for smart grid network topology error," *IEEE Syst. J*, vol. 8, no. 2, pp. 430–440, Jun. 2014.

[11] Y. Huang *et al.*, "Bad data injection in smart grid: Attack and defense mechanisms," *IEEE Commun. Mag.*, vol. 51, no. 1, pp. 27–33, Jan. 2013.

[12] M. Talebi, C. Li, and Z. Qu, "Enhanced protection against false data injection by dynamically changing information structure of microgrids," in *Proc. IEEE 7th Sensor Array Multichannel Signal Process. Workshop*, Jun. 2012, pp. 393–396.

[13] J. Lin, W. Yu, X. Yang, G. Xu, and W. Zhao, "On false data injection attacks against distributed energy routing in smart grid," in *Proc. IEEE/ACM 3rd Int. Conf. Cyber-Phys. Syst.*, Apr. 2012.

[14] H. V. Poor and Q. Hadjiliadis, *Quickest Detection*. Cambridge, U.K.: Cambridge Univ. Press, 2008.

[15] Y. Huang, L. Lai, H. Li, W. Chen, and Z. Han, "Online quickest multi-armed bandit algorithm for distributive renewable energy resources," in *Proc. IEEE Conf. Smart Grid Commun.*, Nov. 2012, pp. 558–563.

[16] M. Basseville and I. Nikiforov, *Detection of Abrupt Changes: Theory and Applications*. Englewood Cliffs, NJ, USA: Prentice-Hall, Apr. 1993.

[17] H. Li, C. Li, and H. Dai, "Collaborative quickest detection in *ad hoc* networks with delay constraint—Part I: Two-node network," in *IEEE Inf. Sci. Syst.*, Princeton, NJ, USA, Mar. 2008, pp. 594–599.

[18] J. Tang, Y. Cheng, and W. Zhuang, "An analytical approach to real-time misbehavior detection in IEEE 802.11 based wireless networks," in *Proc. IEEE Int. Conf. Comput. Commun.*, Apr. 2011, pp. 1638–1646.

[19] Y. Huang, H. Li, K. A. Campbell, and Z. Han, "Defending false data injection attack on smart grid network using adaptive CUSUM test," in *Proc. IEEE Conf. Inf. Sci. Syst.*, Mar. 2011, pp. 1–6.

[20] A. Abur and A. G. Exposito, *Power System State Estimation: Theory and Implementation*. New York, NY, USA: Marcel Dekker, 2004.

[21] A. J. Wood, B. F. Wollenberg, and G. B. Sheblé, *Power Generation, Operation, Control*. New York, NY, USA: Wiley, 1996.

[22] R. D. Zimmerman , C. E. Murillo-Schnchez , and R. J. Thomas, "MATPOWER steady-state operations, planning and analysis tools for power systems research and education," *IEEE Trans. Power Syst.*, vol. 26, no. 1, pp. 12–19, Feb. 2011.

[23] F. C. Schweppe, J. Wildes, and D. B. Rom, "Power system static state estimation," *IEEE Trans. Power App. Syst.*, vol. PAS-89, no. 1, pp. 120–135, Jan. 1970.

[24] J. Casazza and F. Delea, *Understanding Electric Power Systems*. Hoboken, NJ, USA: Wiley, 2010, ser. IEEE Press Understanding Science and Technology Series.

[25] A. L. Ott, "Experience with PJM market operation, system design, implementation," *IEEE Trans. Power Syst.*, vol. 18, no. 2, pp. 528–534, May 2003.

[26] E. S. Page, "Continuous inspection schemes," *Biometrika*, vol. 41, no. 1/2, pp. 100–115, Jul. 1954.

[27] M. He and J. Zhang, "Fault detection and localization in smart grid: A probabilistic dependence graph approach," in *Proc. IEEE Conf. Smart Grid Commun.*, Oct. 2010, pp. 43–48.

[28] G. Lorden, "Procedures for reacting to a change in distribution," *Ann. Math. Statist.*, vol. 42, no. 6, pp. 1897–1908, Jul. 1971.

[29] A. De Maio and S. Iommelli, "Coincidence of the Rao test, Wald test, GLRT in partially homogeneous environment," *IEEE Lett. Signal Process.*, vol. 15, no. 1, pp. 385–388, Apr. 2008.

[30] K. J. Sohn, "Parametric Tests for Multichannel Adaptive Signal Detection," Ph.D. Dissertation, Stevens Inst. Technol., Hoboken, NJ, USA, Dec. 2007.

[31] A. D. Maio, "Rao test for adaptive detection in Gaussian interference with unknown covariance matrix," *IEEE Trans. Signal Process.*, vol. 55, no. 7, pp. 3577–3584, Jul. 2007.

[32] S. M. Kay, *Fundamentals of Statistical Signal Processing: Detection Theory*. Englewood Cliffs, NJ, USA: Prentice-Hall, 1998.

[33] M. R. Chmielewski and J. W. Grzymala-BusseJ, "Global discretization of continuous attributes as preprocessing for machine learning," *Int. J. Approx. Reasoning*, vol. 15, no. 4, pp. 319–331, Nov. 1996.

[34] Y. Q. Chen and K. L. Moore, "Discretization schemes for fractional-order differentiators and integrators," *IEEE Trans. Circuits Syst. I, Fundam. Theory Appl.*, vol. 49, no. 3, pp. 363–367, Mar. 2002.

[35] D. Gamerman and H. F. Lopes, *Markov Chain Monte Carlo: Stochastic Simulation for Bayesian Inference*. Boca Raton, FL, USA: CRC, 2006.

Yi Huang (S'11) received the B.S. degree in electrical engineering from the University of Arizona, Phoenix, AZ, USA, in 2007 and the M.S. degree in electrical engineering from the University of Southern California, Los Angeles, CA, USA, in 2008.

Prior to joining the University of Houston, Houston, TX, USA, he was a Graduate Research Assistant under the supervision of USC Professor K. K. Shung. He joined Ph.D. program in 2009 under the supervision of Prof. Z. Han at the University of Houston. His current research works include the application of quickest detection, data mining, machine learning, and signal processing in wireless networks, cognitive radio networks, and smart grids.

Mr. Huang is the author of the paper that won the Best Paper Award of IEEE SmartGridComm 2012.

Jin Tang (S'10–M'13) received the B.S. degree in computer science from Fudan University, Shanghai, China, in 2004 and the Master's degree in information technology and management and the Ph.D. degree in computer engineering from Illinois Institute of Technology, Chicago, IL, USA, in 2007 and 2012, respectively.

He is currently with AT&T Labs. His current research interests include wireless network security, security in VoIP applications, and intrusion detection.

Dr. Tang received the Best Paper Award of IEEE ICC 2011.

Yu Cheng (S'01–M'04–SM'09) received the B.E. and M.E. degrees in electronic engineering from Tsinghua University, Beijing, China, in 1995 and 1998, respectively, and the Ph.D. degree in electrical and computer engineering from the University of Waterloo, Waterloo, ON, Canada, in 2003.

From September 2004 to July 2006, he was a Postdoctoral Research Fellow with the Department of Electrical and Computer Engineering, University of Toronto, Toronto, ON, Canada. Since August 2006, he has been with the Department of Electrical and Computer Engineering, Illinois Institute of Technology, Chicago, IL, USA, where he is now an Associate Professor. His research interests include next-generation Internet architectures and management, wireless network performance analysis, network security, and wireless/wireline interworking.

Dr. Cheng received the Best Paper Award from the conferences QShine 2007 and ICC 2011. He received the National Science Foundation (NSF) CAREER AWARD in 2011 and IIT Sigma Xi Research Award in the junior faculty division in 2013. He served as a Cochair of the Wireless Networking Symposium of IEEE ICC 2009, a Cochair of the Communications QoS, Reliability, and Modeling Symposium of IEEE GLOBECOM 2011, a Cochair of the Signal Processing for Communications Symposium of IEEE ICC 2012, a Cochair of the *Ad Hoc* and Sensor Networking Symposium of IEEE GLOBECOM 2013, and a Technical Program Committee (TPC) Cochair of WASA 2011. He is the founding Vice Chair of the IEEE ComSoc Technical Subcommittee on Green Communications and Computing. He is an Associate Editor of the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY and the New Books & Multimedia Column Editor of IEEE NETWORK.

Husheng Li (S'00–M'05) received the B.S. and M.S. degrees in electronic engineering from Tsinghua University, Beijing, China, in 1998 and 2000, respectively, and the Ph.D. degree in electrical engineering from Princeton University, Princeton, NJ, USA, in 2005.

From 2005 to 2007, he was a Senior Engineer with Qualcomm Inc., San Diego, CA, USA. In 2007, he joined the EECS Department, University of Tennessee, Knoxville, TN, USA, as an Assistant Professor, where he became an Associate Professor in 2013. He is also an International Scholar of Kyung Hee University, Seoul, Korea. His research is mainly focused on wireless communications and smart grid.

Dr. Li was the recipient of the Best Paper Award of *the EURASIP Journal of Wireless Communications and Networks*, 2005 (together with his Ph.D. advisor Prof. H. V. Poor), the best demo award of GLOBECOM 2010. and the Best Paper Awards of ICC 2011 and SmartGridComm 2012.

Kristy A. Campbell received the Ph.D. degree from the University of California, Davis, CA, USA.

She is an Associate Professor with the Department of Electrical and Computer Engineering, Boise State University, Boise, ID, USA. Her research interests are focused on new electronic memory technologies, reconfigurable electronics, and resistance variable devices based on chalcogenide ion-conducting materials. She has over 100 pending/issued patents in the area of chalcogenide materials as used in electronic memory. She has published more than 20 papers in peer-reviewed journals, three book chapters, and papers for several conference proceedings.

Zhu Han (S'01–M'04–SM'09–F'14) received the B.S. degree in electronic engineering from Tsinghua University, Beijing, China, in 1997 and the M.S. and Ph.D. degrees in electrical engineering from the University of Maryland, College Park, MD, USA, in 1999 and 2003, respectively.

From 2000 to 2002, he was an R&D Engineer with JDSU, Germantown, MD. From 2003 to 2006, he was a Research Associate with the University of Maryland. From 2006 to 2008, he was an Assistant Professor with Boise State University, Boise, ID, USA. He is currently an Associate Professor with the Department of Electrical and Computer Engineering, University of Houston, Houston, TX, USA. His research interests include wireless resource allocation and management, wireless communications and networking, game theory, wireless multimedia, security, and smart grid communication.

Dr. Han has been an Associate Editor of the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS since 2010. He was the recipient of IEEE Fred W. Ellersick Prize 2011. He was the recipient of an NSF CAREER award in 2010.