Defending False Data Injection Attack On Smart Grid Network Using Adaptive CUSUM Test

Yi Huang
ECE Department
University of Houston
Houston, TX 77004, USA

Husheng Li
EECS Department
University of Tennessee
Knoxville, TN 37996, USA

Kristy A. Campbell
ECE Department
Boise State University
Boise, ID 83725, USA

Zhu Han
ECE Department
University of Houston
Houston, TX 77004, USA

***Abstract*—In modern smart grid networks, the traditional power grid is enabled by the technological advances in sensing, measurement, and control devices with two-way communications between the suppliers and customers. The smart grid integration helps the power grid networks to be smarter, but it also increases the risk of adversaries because of the currently obsoleted cyber-infrastructure. Adversaries can easily paralyzes the power facility by misleading the energy management system with injecting false data. In this paper, we proposes a defense strategy to the malicious data injection attack for smart grid state estimation at the control center. The proposed "adaptive CUSUM algorithm", is recursive in nature, and each recursion comprises two interleaved stages: Stage 1 introduces the linear unknown parameter solver technique , and Stage 2 applies the multi-thread CUSUM algorithm for quickest change detection. The proposed scheme is able to determine the possible existence of adversary at the control center as quickly as possible without violating the given constraints such as a certain level of detection accuracy and false alarm. The performance of the proposed algorithm is evaluated by both mathematic analysis and numerical simulation.**

I. Introduction

The smart grid has been improved the robustness and efficiency of traditional power grid networks via the aid of the modern communication technologies. It is enabled by the technological advances in sensing, measurement, and control devices with two-way communications to electricity production, transmission, distribution and consumption parts [1] of power grids by exchanging information about the grid states to system users, operators, and automated devices. Such important integration helps the power grid networks to be smarter, but it also endangers this newly constructed network by increasing the risk of adversaries around the world because of its cyber-infrastructure. It has been warned in [2] [3] that the utility companies recklessly scramble to install such integration (smarter meters, sub control stations, etc.) into current power grid without heeding security risks.

In the smart grid networks, the objective of adversaries are not only obtaining the unauthorized information but also paralyzing the power facility by misleading the energy management system with injecting false data. The energy management system in the control center mainly work on estimation of system states (power-flow, reactance, voltage, phase angle, etc) by collecting the data from remote meters at every period of time. If the adversaries are able to penetrate into the power grid network and inject the malicious data, the energy management system may produce the false state estimation, which potentially results wrong decisions on billing, power dispatch and erroneous analysis, and even causes a generator self-destruct. Thus, the smart grid network must try to prevent the hackers' attacks such as false data injection, disrupt network operations, or denial-of-service attack. The energy management system in the control center has to efficiently execute real-time analysis to detect a change (the intruder) in statistical behavior of state estimation as little delay as possible in order to prevent further damage to the entire network. Similar issues arise in the monitoring of cardiac patients [4], image analysis, or econometrics [5], [6] that require to perform on-line (e.g. in real time) detection of such changes in a way that minimizes the delay between the time a change occurs and the time it is detected. This type of problem is known as the quickest detection (QD) problem [7].

The idea of QD attempts to determine a change as quickly as possible based on real-time observations such that the user-defined condition is satisfied while maintaining a certain level of detection accuracy. The strict term of the user-defined condition is known as the decision rules, which optimize the tradeoff between the stopping time and decision accuracy (i.e. pre-defined error probability, initial prior probability of each hypothesis occurring, etc. [7]). The classification of QD includes: (1) Bayesian framework, which detects the distribution changes between two known distribution at random times. It requires the full knowledge about the prior distributions of changing time. (2) non-Bayesian framework (e.g. CUSUM test), which detects a change of unknown distribution to known/unknown distributions at random times. It is executable with unknown distributions of changing time. Page's CUSUM test [8] is one of most powerful tool for such QD in real-time process. It rises a great variety of applications [7] such as the intrusion detection in network, seismology, quality control in speech and image processing, and biomedical signal processing.

Furthermore, QD technique becomes a powerful tool with combining "statistical hypotheses test (SHT)" [9]. The mechanism of SHT is that the receiver classifies a sequence of observations into one hypothesis among multiple hypotheses based on some knowledge of the statistical distributions. By doing that, one true hypothesis, which is actually transmitted, can be determined in real time. If only two possible hypotheses exist, it is known as "binary hypotheses test (BHT)" [9]. There are a lot of recent literature to apply QD and SHT to a variety of networks. The authors in [10] applied the modified CUSUM test to detect an abrupt distribution change with an unknown time varying parameter. In [11], the authors modified the sequential probability ratio test (SPRT) to detect

978-1-4244-9848-2/11$26.00©2011 IEEE

the occupancy of the unknown primary user (PU) in a licensed spectrum band for a cognitive radio application. The cognitive radio spectrum sensing with unknown parameters of PU was described in [12]. The authors in [13] used the CUSUM tests as a collaborative QD for detecting a distribution change in ad hoc networks. However, little existing work has considered the unique environment of smart grid networks.

In this paper, we consider a counter-measurement strategy of the data injection attack at the control center in the form of adversary detection. The problem formulation of detecting the false data injection is based on the bad data detection (BDD) on smart grid state estimation. The proposed algorithm, "adaptive CUSUM Test", is recursive in nature, and each recursion comprises two interleaved stages: Stage 1 introduces the linear unknown parameter solver technique, and Stage 2 applies the multi-thread CUSUM algorithm for quickest change detection. The proposed scheme is able to determine the possible existence of adversary at the control center as quickly as possible without violating the given constraints such as a certain level of detection accuracy and false alarm. The performance of the proposed algorithm is evaluated by both mathematic analysis and numerical simulation.

The remainder of this paper is organized as follows. The system model is given in Section II. The proposed scheme - adaptive CUSUM algorithm is given and analyzed mathematically in Section III. The numerical results are provided in Section IV, and the conclusion is given in Section V.

II. Problem Formulation

A. Active Power Flow Models

A power system is composed by a collection of power flow meters, transmission lines, and buses. Assuming the power system has $n+1$ buses, we consider model of active power-flow P_{ij}, active power injections P_i, and bus phase angles θ_i, where $i = 1, \cdots, n+1$. Assuming the power network has reached a steady state, and the resistance in the transmission line connecting buses i and j is small compared to its reactance, the active power-flow model [14] from bus i to bus j can be described as:

$$P_{ij} = \frac{V_i V_j}{X_{ij}} \sin(\theta_i - \theta_j), \tag{1}$$

where V_i is the voltage level at bus i, and X_{ij} is the reactance between bus i and bus j. At bus i, active power P_i can also be injected through a generator. A negative P_i represents the power load. Without lost of generality, no energy is loss or dissipated, and the conservation of energy yields that for all buses it holds that:

$$P_i = \sum_{k \in \nu_i} P_{ik}, \ \forall i \tag{2}$$

where ν_i is the set of all buses connected to bus i.

B. State Estimation

We consider the state-estimation problem as estimating n phase angles θ_i, by observing the real-time measurements of active power-flow. The initial phase angle θ_1 is known as reference angle, and therefore only n angles have to be estimated. The voltage level of each bus and reactance of each transmission line are assumed to be known.

At time t, the control center observes a vector $\mathbf{Z}_t$ of actual power-flow measurements for m active power-flow branches. Each active branch is composed by two meters and one transmission-line. The observation can be described as follows:

$$\mathbf{Z}_t = \mathbf{P}_t + \mathbf{e} = \mathbf{h}(\mathbf{x}) + \mathbf{e}, \tag{3}$$

where $\mathbf{Z}_t = [Z_{t,1}, \cdots, Z_{t,m}]^T$ is the vector power-flow measurement, $\mathbf{h}(\mathbf{x})$ is the actual power-flow model derived using (1) and (2), the system state $\mathbf{x}$ is the vector of n bus phase angles θ_i, and $\mathbf{e} = (e_1, \cdots, e_m)^T$ is the Gaussian measurement noise with zero mean and covariance matrix $\mathbf{\Sigma}_e$. If we temperately neglect the time index t, to estimate the unknown bus phase angles from the power flow measurements $\mathbf{Z}$, the Gauss-Newton method is applied [15]:

$$\hat{\mathbf{x}}^{k+1} = \hat{\mathbf{x}}^k + (\mathbf{H}_k^T \mathbf{\Sigma}_e^{-1} \mathbf{H}_k)^{-1} \mathbf{H}_k^T \mathbf{\Sigma}_e^{-1} [\mathbf{Z} - \mathbf{h}(\hat{\mathbf{x}}_k)], \tag{4}$$

where the estimated system state $\hat{\mathbf{x}}^k \in \mathbb{R}^n$, k is iteration number, and $\mathbf{H}_k \in \mathbb{R}^m$ is Jacobian evaluated at $\hat{\mathbf{x}}^k$,

$$\mathbf{H}_k = \frac{\partial \mathbf{h}(\hat{\mathbf{x}}^k)}{\partial \mathbf{x}}, \tag{5}$$

If the phase differences $(\theta_i - \theta_j)$ in (1) is small, then the linear approximation model of (3) can be described as:

$$\mathbf{Z} = \mathbf{H}\mathbf{x} + \mathbf{e} \tag{6}$$

where $\mathbf{H} \in \mathbb{R}^m$ is the constant Jacobian matrix, and the estimated system state $\hat{\mathbf{x}}$ is:

$$\hat{\mathbf{x}} = (\mathbf{H}^T \mathbf{\Sigma}_e^{-1} \mathbf{H})^{-1} \mathbf{H}^T \mathbf{\Sigma}_e^{-1} \mathbf{Z}, \tag{7}$$

For the bad-date detection (BDD) system (e.g. sensor faulty, topological error), we compare the power-flow measurements $\mathbf{Z}$ with the estimated active power-flow $\hat{\mathbf{Z}}$ by the phase angle estimate $\hat{\mathbf{x}}$. $\hat{\mathbf{Z}}$ can be written as:

$$\hat{\mathbf{Z}} = \mathbf{H}\hat{\mathbf{x}} = \mathbf{H}(\mathbf{H}^T \mathbf{\Sigma}_e^{-1} \mathbf{H})^{-1} \mathbf{H}^T \mathbf{\Sigma}_e^{-1} \mathbf{z} = \Im \mathbf{Z}, \tag{8}$$

where $\Im$ is known as "hat matrix" [15]. However, if the adversary performs an unobservable attack by injecting the malicious data like described in [16], BDD system is unable to detect the unobservable attack due to the insignificance in comparison with arbitrarily large estimation error. According to [16], if the nonzero k-sparse $\mathbf{a}$ is existed in the system, where vector $\mathbf{a} = \mathbf{H}\mathbf{c}$ is the malicious data injected by an adversary, no detector can distinguish $\mathbf{x}$ from $\mathbf{x} + \mathbf{c}$ as shown in (9).

$$\mathbf{Z} = \mathbf{H}\mathbf{x} + \mathbf{a} + \mathbf{e} = \mathbf{H} \cdot (\mathbf{x} + \mathbf{c}) + \mathbf{e}, \tag{9}$$

where $\mathbf{a} = [a_l, l = 1, 2, \cdots, m]^T$. When the adversary's malicious data is injected at the true state $\mathbf{x}$ in the system, the $\mathbf{x}$ leads the control center to believe that true state is $\mathbf{x} + \mathbf{c}$, and $\mathbf{c}$ can be in any form such as scaled or vectored arbitrarily. Therefore, it is so-called stealth (unobservable) attack.

978-1-4244-9848-2/11$26.00©2011 IEEE

III. Adaptive CUSUM Algorithm

In this paper, we propose an adaptive CUSUM algorithm for quickest change detection with a linear unknown parameter solver. The unknown parameter exists in the post-change distribution and may changes over the detection process. The proposed scheme does not require the Maximum Likelihood (ML) estimate of the unknown parameter thereby making the computation process much simpler. To formulate the detection problem at the control center, the non-Bayesian approach is applied because of the unknown prior probability of the adversary and unknown statistical model for the adversary vector.

we consider the control center monitors a subdivision of a smart grid network with n active buses. $z_{t,m}$ represents the observation at the m^{th} measurement at time t. When the system is at the normal state (no adversary), we assume a Bayesian model of the random state variables with multivariate Gaussian distribution $\mathcal{N}(\mu_z, \mathbf{\Sigma}_z)$ and $\mu_z = 0_m$ without loss of generality. The adversary is assumed inactive initially; At randomly unknown time τ, it becomes active to inject the malicious data. Under observation of (9), the binary hypothesis can be formulated:

$$\begin{cases} \mathcal{H}_0: & \mathbf{Z}_t \sim \mathcal{N}(0, \mathbf{\Sigma}_z), \\ \mathcal{H}_1: & \mathbf{Z}_t \sim \mathcal{N}(\mathbf{a}_t, \mathbf{\Sigma}_z), \end{cases} \tag{10}$$

where $\mathbf{a}_t = [a_{t,1}, a_{t,2}, \cdots, a_{t,m}]^T, \in \mathbb{R}^m$ is the unknown attacker vector to inject malicious data at time t , and $\mathbf{\Sigma}_z$ is $\mathbf{H}\mathbf{\Sigma}_x\mathbf{H}^T + \mathbf{\Sigma}_e$. In other words, a change of the distribution from $\mathcal{N}(0, \mathbf{\Sigma}_z)$ to $\mathcal{N}(\mathbf{a}_t, \mathbf{\Sigma}_z)$ at the unknown time τ.

Let T_h donate the stopping time, which the change is detected. If $T_h < \tau$, then it is the false alarm, and the average run length (ARL) is $T_f = E_0[T_h]$, where E_0 is the average before the change. If $T_h > \tau$, then $T_h - \tau$ is the detection delay and T_d donate the ARL of detection delay. Based on Lorden's formulation [7], we minimize the worst case of detection delay, which can be described as:

$$T_d = \sup_{\tau \geq 1} E_\tau[T_h - \tau | T_h \geq \tau] \tag{11}$$

To solve the minimum T_d, Page's CUSUM algorithm is the best-known technique to tackle this type of problem [8]. However, most of CUSUM-based models assume the perfect knowledge of the likelihood functions. In the scenario of intrusion detection, the parameters of $\mathcal{H}_1$ distribution can not be completely defined because of the unknown attacker parameters and statical model. Thus, we need employ the technique to solve the unknown parameter issue in Page's CUSUM detection scheme.

The proposed quickest detection algorithm, adaptive CUSUM Test, is recursive in nature, and each recursion comprises two interleaved steps: i) linear unknown parameter solver and ii) multi-thread CUSUM. The proposed multi-thread CUSUM test is modified and based on Page's CUSUM algorithm. The multi-thread CUSUM test considers and co-operates the likelihood ratio term of m measurements at time t in order to determine the stopping time T_h, which can be described as follows:

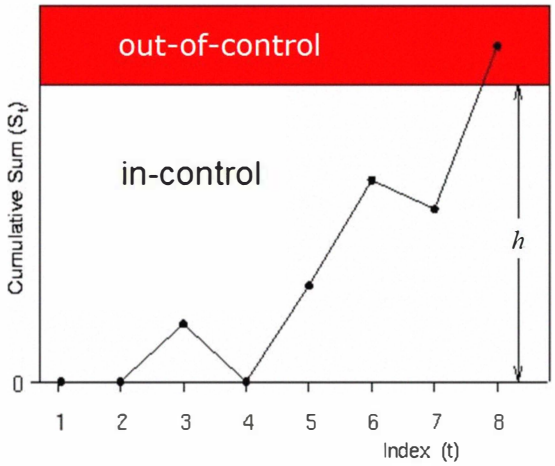

Fig. 1. An illustration of the CUSUM test with the decision interval.

$$T_h = \inf\{t \geq 1 | S_t > h\}, \tag{12}$$

in which the detection threshold h is a function of FAR, MDR, and the process variance, with cumulative statistic at time t:

$$S_t = \max_{1 \geq k \geq T_h} \sum_{t=k}^{T_h} L_t, \tag{13}$$

and

$$L_t(\mathbf{Z}_t) = \sum_{l=1}^{m} \log \frac{f_1(\mathbf{Z}_t)}{f_0(\mathbf{Z}_t)}, \tag{14}$$

where L_t is the sum of likelihood ratio function for all measurements $(z_{t,l}, l \in 1, 2, \cdots, m)$ of the vector $\mathbf{Z}_t$ at time t, $f_1(\mathbf{Z}_t)$ is the $\mathcal{H}_1$ multi-variate normal distribution while the adversary actively injects malicious data, and $f_0(\mathbf{Z}_t)$ is the $\mathcal{H}_0$ multi-variate normal distribution at the normal state. At time t, the cumulative statistic S_t can be solved recursively and described as:

$$S_t = \max(S_{t-1}, 0) + L_t(\mathbf{Z}_t), \tag{15}$$

where $S_0 = 0$. Hence, the test based on T_h accumulates the likelihood ratio term, resetting the accumulation to zero whenever the alarm rises. The control center declares the alarm when the accumulation crosses a certain threshold h. Figure 1 illustrates the decision interval (time) is displayed as a horizontal line on the CUSUM chart. As shown in Figure 1, a shift or out-of-control condition is signaled, the cumulative process is terminated, and ARL is equivalent to T_h, which is from S_0 to S_{T_h}. The optimality of the stopping time based on the first exist of S_t from the interval [0,h).

Due to the unknown adversary statistic model, the author in [17] proposed to implement the generalized likelihood ratio test (GLRT) in Page's CUSUM algorithm with the unknown parameters. The idea is to apply LRT by replacing the unknown parameter with the ML estimation. The GLRT approach is asymptotically minimax in the sense of minimizing $\max_{\mathbf{a} \in \mathbb{R}} f_e(\mathbf{Z}_t | \mathbf{a})$, which $\mathbf{a}$ is the uncertain parameter as shown in (16). In the other words, we minimize the effect of

978-1-4244-9848-2/11$26.00©2011 IEEE

the unknown while considering the worst case of the unknown parameter, which is potentially maximized. Thus, by applying GLRT in CUSUM algorithm, we can ensure a certain level of detection accuracy for QD, while minimizing the potential effect from the unknown in the system. We test-drive and formulate this idea into our detection problem. At time t, the cumulative statistic in (13) can be re-written for our problem as :

$$S_t = \max_{1\geq k\geq T_h} \max_{a_{t,l}} \sum_{t=1}^{T_h} \sum_{l=1}^{m} \log \frac{f_1(\mathbf{Z}_t|a_{t,l})}{f_0(\mathbf{Z}_t)}, \tag{16}$$

where $a_{t,l}$ represents l^{th} unknown element in unknown adversary vector $\mathbf{a}$ under the current time t. However, the recursive expression of (16) for CUSUM Test is no longer available as shown in (15). It is because GLRT needs to compute every unknown element of $\mathbf{a}$ for each measurement at time t by estimating from the observations up to the current time t. In other words, GLRT approach on CUSUM requires storing the observation and ML-estimating the unknown parameter at every point. Thus, in reality, GLRT is too difficult to be applied into quickest detection model from the view points of hardware and software implementation.

For multi-thread CUSUM algorithm with unknown parameters, the better approach is to solve recursively, avoiding complex ML estimation, and implemented in practice. Thus, we consider the Rao test [18], which is the asymptotically equivalent test model of GLRT. The derivation of Rao test is similar to the locally most powerful (LMP) test but only much simpler; Rao test has the straight-forward calculation by taking derivative with respect to the unknown parameter evaluated at the unknown parameter equal to zero. Thus, for $\mathbf{a}_t$ near $\hat{\mathbf{a}}_t^0$, we can achieve approximate maximum outcome with a certain level of FAR by maximizing $\frac{\partial f_e(\mathbf{Z}_t|\mathbf{a}_t)}{\partial \mathbf{a}_t}$ as shown in (17). In addition, the Rao test also doesn't involve the complex computation like the ML estimation does. The statistic [18] of the Rao test for the observations can be modified and rewritten as follows at time t:

$$\mathcal{R}(\mathbf{Z}_t) = \frac{\partial \log[f_1(\mathbf{Z}_t|\mathbf{a}_t)]}{\partial \mathbf{a}_t}\bigg|_{\mathbf{a}_t=\hat{\mathbf{a}}_t^0}^{T} \times [\mathbf{J}^{-1}(\hat{\mathbf{a}_t}^0_t)]_{\mathbf{a}} \frac{\partial \log[f_1(\mathbf{Z}_t|\mathbf{a}_t)]}{\partial \mathbf{a}_t}\bigg|_{\mathbf{a}_t=\hat{\mathbf{a}}_t^0}, \tag{17}$$

where $\hat{\mathbf{a}}_0$ is set to zero for our problem, and $\mathbf{J}(\hat{\mathbf{a}}_t^0)$ is the Fisher information matrix [19] evaluated at $\mathbf{a}_t = \hat{\mathbf{a}}_t^0$. By inspecting (17), We know that the Rao test is two-side test, therefore it is in quadratic form. The computation of the inverse fisher information matrix is usually demanded in multi-parameter environment. In our problem, the unknown a is always positive. Thus, the necessity of the quadratic form can be omitted. At time t, the linear model of (17) can be described as:

$$\varphi(\mathbf{Z}_t) = \sum_{l=1}^{m} \frac{\partial \log[f_1(\mathbf{Z}_t|\mathbf{a}_t)]}{\partial \mathbf{a}_t}\bigg|_{\mathbf{a}_t=0_m}, \tag{18}$$

and

$$\begin{aligned} \mathbf{Z}_t &= [z_{t,l} : \quad z_{t,1}, z_{t,2}, \cdots, z_{t,m}]^T \\ \mathbf{a}_t &= [a_{t,l} : \quad a_{t,1}, a_{t,2}, \cdots, a_{t,m}]^T, \end{aligned} \tag{19}$$

that is not in a quadratic form, and no need to store the observation and re-calculate the unknown parameter at every time internal. By setting $\mathbf{a}_t$ to 0_m, the unknown matrix can be minimized in the system. The linear unknown parameter solver in (18) is also allowed the multi-thread CUSUM algorithm with unknown parameters to compute recursively for test statistic. Now, we can apply the linear unknown parameter solver (18) into the multi-thread CUSUM algorithm.

Based on (10), we can write the binary hypothesis $\{\mathcal{H}_0, \mathcal{H}_1\}$ by expanding the multivariate normal distributions:

$$\begin{cases} \mathcal{H}_0 : \quad f_0(\mathbf{Z}_t) = \frac{\exp\left[-0.5(\mathbf{Z}_t)^T \mathbf{\Sigma}_z^{-1}(\mathbf{Z}_t)\right]}{(2\pi)^{0.5m} \det(\mathbf{\Sigma}_z)^{0.5}}, \\ \mathcal{H}_1 : \quad f_1(\mathbf{Z}_t) = \frac{\exp\left[-0.5(\mathbf{Z}_t-\mathbf{a}_t)^T \mathbf{\Sigma}_z^{-1}(\mathbf{Z}_t-\mathbf{a}_t)\right]}{(2\pi)^{0.5m} \det(\mathbf{\Sigma}_z)^{0.5}}. \end{cases} \tag{20}$$

So, the multi-thread CUSUM statistic with unknown parameter can be derived as:

$$\begin{aligned} S_t = \max_{1\geq k\geq T_h} \sum_{t=k}^{T_h} \sum_{l=1}^{m} \\ \log\left[\exp\left(\mathbf{Z}_t^T \mathbf{\Sigma}_z^{-1} \mathbf{a}_t + \mathbf{a}_t^T \mathbf{\Sigma}_z^{-1} \mathbf{Z}_t - \mathbf{a}_t^T \mathbf{\Sigma}_z^{-1} \mathbf{a}_t\right)\right], \end{aligned} \tag{21}$$

Next, we apply the linear unknown parameter solver from the result of (18) to each m^{th} log likelihood ratio term in (21) by taking its derivative with respect to a_l evaluated at $a_l = 0$ in the unknown vector $\mathbf{a}_t$ at time t. We can rewrite (15) and then formulate the linear-based multi-thread CUSUM statistic by recursion as follows:

$$\begin{aligned} S_t = \max(S_{t-1}, 0) + \\ \sum_{l=1}^{m} \frac{\partial \log\left[\exp\left(\mathbf{Z}_t^T \mathbf{\Sigma}_z^{-1} \mathbf{a}_t + \mathbf{a}_t^T \mathbf{\Sigma}_z^{-1} \mathbf{Z}_t - \mathbf{a}_t^T \mathbf{\Sigma}_z^{-1} \mathbf{a}_t\right)\right]}{\partial \mathbf{a}_t}\bigg|_{\mathbf{a}_t=0_m}. \end{aligned} \tag{22}$$

From the visional inspection of (22), we know $\frac{\partial \log \exp(\mathbf{ab})}{\partial \mathbf{a}} = \frac{\partial \mathbf{ab}}{\partial \mathbf{a}} = \mathbf{b}$, and we can rewrite (22) as follows:

$$S_t = \max(S_{t-1}, 0) + \sum_{l=1}^{m} \left[(\mathbf{Z}_t^T \mathbf{\Sigma}_z^{-1})^T + \mathbf{\Sigma}_z^{-1} \mathbf{Z}_t\right]. \tag{23}$$

Notes that the control center observes a vector $\mathbf{Z}_t$ of actual power-flow measurements for m active power-flow branches at time t, $\mathbf{Z}_t \in \{z_{t,l}\}$, and $\mathbf{a}_t \in \{a_{t,l}\}$ where $l = 1, 2, \cdots, m$. With these two interleaved steps: the linear unknown parameter solver and multi-thread CUSUM test, we construct the proposed scheme, which is named the "adaptive CUSUM algorithm". The control center is able to tackle with the unobservable attack (malicious data injection) by examining adaptive CUSUM statistic in (22) against the threshold h in (13) at time t; h is the detection threshold to be set according to the desired value of the false alarm rate (FAR) and miss detection rate (MDR); the alarm rise as little delay as possible when the CUSUM statistic S_t excess the threshold h while maintaining a certain level of detection accuracy.

A decision is made at each time t for whether continue sampling, or terminate the test and declare the true hypothesis.

978-1-4244-9848-2/11$26.00©2011 IEEE

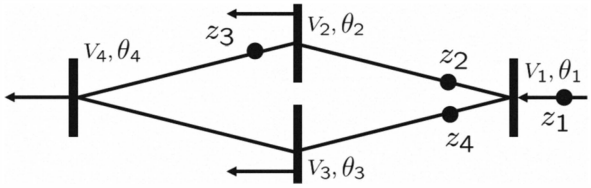

Fig. 2. An experimental setup of IEEE 4-bus power network with four available active power-flow measurements.

If either S_t excesses the threshold h, the hypothesis decision is made and the process is terminated. The framework of the adaptive CUSUM algorithm of the proposed scheme is shown in Table 1.

Algorithm 1 Adaptive CUSUM algorithm

$t \leftarrow (1, 2, 3 \cdots)$
$\mathbf{a} \leftarrow$ The unknown adversary vector ($\mu_z \in \mathcal{R}^m$ for $\mathcal{H}_1$)
repeat
  compute the the covariance matrix $\mathbf{\Sigma}_z$, $\mathbf{\Sigma}_e$
  Linear Unknown Parameter Solver:
  solve $\mathbf{a}$ by taking its derivative with respect $\mathbf{a}_t$ evaluated to $\mathbf{a}_t = 0_m$ based on the Rao test
  Multi-thread CUSUM test:
  compute recursively S_t with the sum of L_t for all m measurements at current time t
  Update of: $t \leftarrow t + 1$
  continues the observation
until $T_h = \inf\{t \geq 1 | S_t > h\}$ is determined
Terminate the adaptive CUSUM process
Report the true hypothesis and T_h as the ARL

IV. Numerical Results

In this section, we present the numerical simulations to demonstrate the performance of the proposed scheme with the following setup. The simulation performs under IEEE 4-bus test system for the power network as shown in Figure 2. Each bus has its corresponded voltage (V_i) and phase angle (θ_i); the dots represents available active power-flow measurements. The total number of the measurements from this IEEE 4-bus test system is four, which are $\mathbf{P} = [P_1, P_{12}, P_{24}, P_{13}]^T$. The bus phase angle θ_1 is set to zero as the reference angle. The normal state in the power system is assumed to be initially drawn from the multivariate normal distribution $\mathcal{N}(0, \mathbf{\Sigma}_z)$. $\mathbf{\Sigma}_z$ is in term of $\mathbf{\Sigma}_e$, which sets equivalently to the identify matrix. After passing the unknown period of time, the adversary start to inject the malicious data at time τ that are drawn from $\mathcal{N}(\mathbf{a}, \mathbf{\Sigma}_z)$. The detector has none information about the matrix $\mathbf{a}$'s statistical model, distribution, or prior probabilities. The adversary manipulates and injects the false data into the system at the random time.

The simulation of the adaptive CUSUM algorithm is shown in Figure 3 with the constant probability of detection error. We consider that Case 1 with FAR of 1% and Case 2 with FAR of

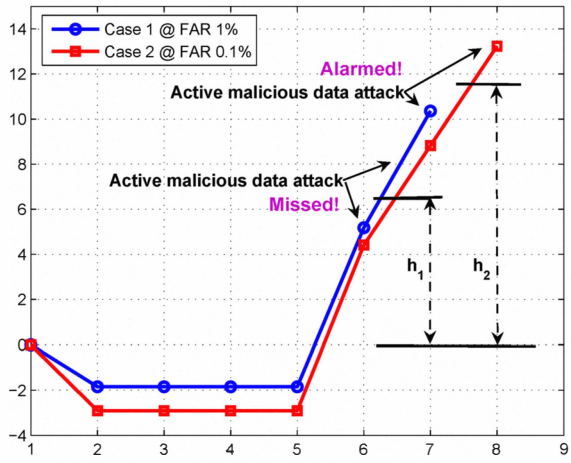

Fig. 3. The simulation of the adaptive CUSUM algorithm. The x-axis is the time (t), and y-axis is the recursive CUSUM statistic (S_t). Case 1 with FAR of 1% corresponds to h_1 , and Case 2 with FAR of 0.1% corresponds to h_2. The proposed algorithm signals the alarm and then terminates the process at $T_h = 7$ and 8, respectively.

0.01%. The adversary becomes active and injects the malicious data at time $t = 6$. In other words, a change distribution is at $\tau = 6$ from $\mathcal{N}(0, \mathbf{\Sigma}_z)$ to $\mathcal{N}(\mathbf{a}, \mathbf{\Sigma}_z)$, where $\mathbf{a}$ is unknown. For both cases, the curve of adaptive CUSUM statistic (S_t) shows the sudden increase right after a change of distributions. The proposed algorithm quickly responses the abnormal event by signaling an alarm of out-of-control. At time 7, the threshold parameters h_1 and h_2 are corresponded to Case 1 and Case 2, respectively. As a result in Figure 3, h_1 is less than h_2, because of the different FARs. For the higher successful rate of detection, the stricter constraint (smaller FAR) causes increasing the threshold, which sets the higher requirement for system to declare the decision from the observation. The above statement is corresponded to the simulation results in Figure 4 and Figure 5, which are explained in the next paragraph. ARL (T_h) of adaptive CUSUM algorithm is 7 and 8 at S_t of 6.23 (Case 1) and 11.49 (Case 2), respectively. ARL (T_d) of detection delay is 1 for cases 1 and 2 for the Case 2 in this simulation. The proposed algorithm is able to signal the alarm and terminates the process after the active malicious date attack; the detection delay occurs because of the missing detection at time 6 as shown in Figure 3. The system continues the detection process until the CUSUM statistic S_t, which excesses the threshold. However, the detection accuracy of the proposed scheme is comparable high while maintaining a certain level of detection error rate.

Both Figure 4 and Figure 5 shows the characteristics of the proposed algorithm by varying FAR for the detection probability P_D and the expectional ARL ($E(T_d)$) of detection delay. To compute P_D and $E(T_d)$, we run 5000 realizations for the simulation. MDR is set to the constant 1%, and FAR is vary from 10^{-10} to 10^{-2}. The change τ of distribution is randomly selected. $E(T_d)$ of detection delay is computed by subtracting τ from $E(T_h)$. The simulation result shows that the algorithm maintains the fairly good detection accuracy of 67% and 1

978-1-4244-9848-2/11$26.00©2011 IEEE

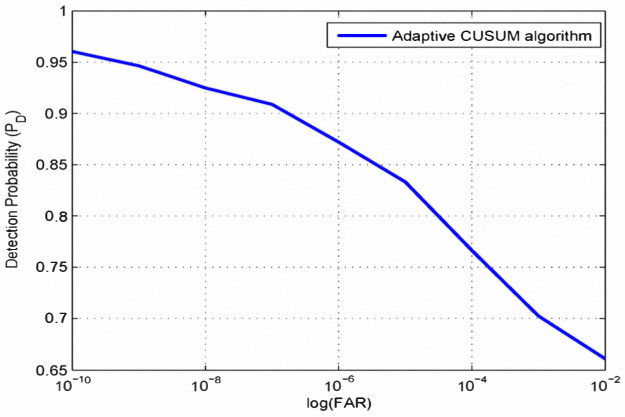

Fig. 4. The performance analysis for the adaptive CUSUM algorithm. The y-axis is P_D, the probability of detection, and x-axis is the probability of the false alarm.

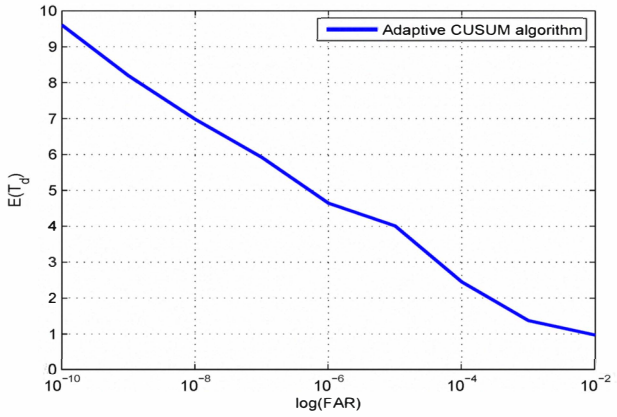

Fig. 5. The performance analysis for the adaptive CUSUM algorithm. The y-axis is $E(T_d)$, and x-axis is the probability of the false alarm.

unit of $E(T_d)$ at the worst case of FAR 1% From both Figure 4-5, we know the tradeoff between the detection accuracy and ARL; the higher detection accuracy (the smaller FAR) causes higher ARL (the higher $E(T_d)$), i.e., the system needs to spend more time for making a decision. $E(T_d)$ decreases as FAR increases, of course, the P_D decreases because of the loss of constraints; in this case, the constraint is FAR. The loss of constraints also benefits the quicker detection (less detection delay) but may degrading the accuracy of detection. Therefore, the tradeoff between the constraints and the detection accuracy needs to be addressed carefully since it may have the great impact on the output parameters.

V. Conclusion

In this paper, we have studied malicious node quickest detection in smart grid networks. We propose the adaptive CUSUM algorithm for defending false data injection attack in smart grid networks. Our proposed scheme for smart grid state estimation composes two interleaved stages: Stage 1 introduces the linear unknown parameter solver technique, and Stage 2 applies the multi-thread CUSUM algorithm for determining the possible existence of adversary at the control center as quickly as possible without violating the given constraints while maintaining a certain low level of detection error rate. The analysis and numerical simulation results have shown that the proposed scheme achieved good performance while maintaining a certain level of detection accuracy and detection delay. The proposed adaptive CUSUM algorithm is not only simple but also efficient in term of detection accuracy and minimum ARL. The numerical simulation of FAR verses $E(T_d)$ and P_D also helps us to understand the characteristics of the proposed scheme. Finally, the proposed scheme in this paper is able to achieve the important objectives of smart grid security in term of the real-time operation and security requirement.

References

[1] P. Marken, J. Marczewski, and R. D'Aquila, "A smart transmission technology that is compatible with the existing and future Grid," *in Proceedings of IEEE Power Systems Conference and Exposition*, Seattle, WA, March 2009.

[2] McClatchy Newspapers, "Smart grid technology vulnerable to attack," Internet: http://www.statesman.com/news/local/smart-grid-technology-vulnerable-to-attack-expert-says-826545.html, Accessed: December 2010.

[3] Homeland Security Newswire group, "Smart grid attack," Internet: http://homelandsecuritynewswire.com/smart-grid-attack-likely, Accessed: December 2010.

[4] M. Petzold, C. Sonesson, E. Bergman, and H. Kieler, "Surveillance in longitudinal models: Detection of intrauterine growth restriction," *Biometrics*, Vol. 60, No. 4, pp. 1025-1033,2004.

[5] E. Andersson, D. Bock, and M. Frisen, "Some statistical aspects of methods for detection of turning points in business cycles," *Journal of Applied Statistics*, Vol. 33, No. 3, pp. 257-278, 2006.

[6] E. Andreou and E. Ghysels, "The impact of sampling frequency and volatility estimators on change-point tests," *Journal of Financial Econometrics*, Vol. 2, No. 2, pp. 290-318, 2004.

[7] H. V. Poor and Q. Hadjiliadis, *Quickest Detection*, Cambridge University Press, 2008.

[8] E. S. Page, "Continuous inspection schemes," *Biometrika*, vol. 41, pp. 100-115, 1954.

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

[10] C. Li, H. Dai, and H. Li, "Adaptive quickest detection with unknown parameters," *in Proceedings of IEEE International Conference on Acoustics, Speech, and Signal Processing 2009*, pp. 3241 - 3244, Taipei, Taiwan, April 2009.

[11] Y. Xin, H. Zhang, and S. Rangarajan, "SSCT: A simple sequential spectrum sensing scheme for cognitive radio," *in Proceedings of IEEE Global Communications Conference 2009*, Honolulu, HI, Nov. 2009.

[12] H. Li, C. Li, and H. Dai, "Quickest spectrum sensing in cognitive radio," *IEEE Information Sciences and Systems 2008*, pp. 203 - 208, Princeton, NJ, March 2008.

[13] H. Li, C. Li, and H. Dai, "Collaborative quickest detection in ad hoc networks with delay constraint Part I: Two-node network," *IEEE Information Sciences and Systems 2008*, pp. 594 - 599, Princeton, NJ, March 2008.

[14] J. Casazza and F. Delea, *Understanding Electric Power Systems*, IEEE Press Understanding Science and Technology Series, A John Wiley and Sons, Inc., 2010.

[15] A. Abur and A. G. Exposito, *Power System State Estimation: Theory and Implementation*, Marcel Dekker, Inc., 2004.

[16] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *in Proceedings of ACM Conference on Computer and Communications Security*, Chicago, IL, November 2009.

[17] G. Lorden, "Procedures for reacting to a change in distribution," *Annals of Mathematical Statistics*, vol. 42, no. 6, pp. 1897-1908, 1971

[18] A. D. Maio, "Rao test for adaptive detection in Haussian interference with unknown covariance matrix," *IEEE transactions on signal processing*, vol. 55, no. 7, pp. , July 2007

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

978-1-4244-9848-2/11$26.00©2011 IEEE