Quickest Detection of False Data Injection Attack in Wide-Area Smart Grids

Shang Li, Yasin Yılmaz, and Xiaodong Wang, *Fellow, IEEE*

***Abstract*—We consider the sequential (i.e., online) detection of false data injection attacks in smart grid, which aims to manipulate the state estimation procedure by injecting malicious data to the monitoring meters. The unknown parameters in the system, namely the state vector, injected malicious data and the set of attacked meters pose a significant challenge for designing a robust, computationally efficient, and high-performance detector. We propose a sequential detector based on the generalized likelihood ratio to address this challenge. Specifically, the proposed detector is designed to be robust to a variety of attacking strategies, and load situations in the power system, and its computational complexity linearly scales with the number of meters. Moreover, it considerably outperforms the existing first-order cumulative sum detector in terms of the average detection delay and robustness to various attacking strategies. For wide-area monitoring in smart grid, we further develop a distributed sequential detector using an adaptive sampling technique called level-triggered sampling. The resulting distributed detector features single bit per sample in terms of the communication overhead, while preserving the high performance of the proposed centralized detector.**

***Index Terms*—Cyber security, distributed algorithm, generalized CUSUM, level-triggered sampling, smart grid quickest detection, wide-area monitoring.**

I. Introduction

UNDER THE smart grid concept, the power system is tightly integrated with the cyber-infrastructure, such as computer and communication networks, which makes it vulnerable to cyber-attacks. Cyber-security is a critical issue in smart grid since cyber-attacks may eventually cause catastrophic consequences such as blackouts in large geographic areas. Furthermore, it is far more difficult to detect malicious data attacks than to detect random errors in the power systems because the adversary can choose the site of attack judiciously and design attack data carefully. Consequently, cyber-security for smart grid has drawn significant interest in [1]–[4].

Manuscript received May 9, 2014; revised September 2, 2014; accepted November 19, 2014. Date of publication December 11, 2014; date of current version October 17, 2015. This work was supported in part by the U.S. National Science Foundation under Grant CIF1064575, and in part by the U.S. Office of Naval Research under Grant N000141410667. Paper no. TSG-00398-2014.

S. Li is with the Department of Electrical Engineering, Columbia University, New York, NY 10027 USA. (e-mail: shang@ee.columbia.edu).

Y. Yılmaz is with the Electrical Engineering and Computer Science Department, University of Michigan, Ann Arbor, MI 48109 USA (e-mail: yasiny@umich.edu).

X. Wang is with the Department of Electrical Engineering, Columbia University, New York, NY 10027 USA; and also with the King Abdulaziz University, Jeddah, Saudi Arabia (e-mail: wangx@ee.columbia.edu).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TSG.2014.2374577

State estimation is a fundamental task for power grid [5]–[7]. Meter measurements are used to estimate state variables such as bus voltages and phase angles. Then, various power grid components are controlled based on the state estimates. Cyber-attacks in the power system monitoring, is defined as the attacks that aim to cause erroneous state estimates by manipulating meter measurements. Thus, they are also known as false data injection attacks. In the conventional centralized setup, meter readings are transmitted to a control center, and stored in a supervisory control and data acquisition (SCADA) system. Due to the deregulation of modern power grids, wide-area monitoring recently draws extensive attention. In wide-area monitoring, there is a number of sub-areas, each of which only has access to its own meter measurements, and communicates with others and the control center through the wireless medium. The centralized setup may not be practically feasible in wide-area monitoring because of the power and bandwidth constraints of the wireless communication systems. Thus, distributed detection is of interest, in which a primary objective is to minimize the communication overhead.

The naive approach to distributed detection samples the meter readings uniformly in time, and then synchronously transmits samples from sub-areas to the control center. Fortunately, for detecting the false data injection attacks, since only the post-attack measurements bear information, we can considerably decrease the communication overhead, compared to the naive approach, by transmitting only the informative measurements from sub-areas to the control center. The random nature of the attacking time constitutes the challenge here. An adaptive sampling technique called level-triggered sampling, that decides whether to transmit or not each time a new measurement is taken, can effectively handle this challenge. In [8] and [9], it was shown that level-triggered sampling enables efficient information transmission under stringent communication and energy constraints. Specifically, as opposed to the naive uniform-in-time sampling, it allows the sampling times to be determined by the signal to be sampled, hence censors uninformative measurements and enables the changes in the signal level to be easily tracked at a remote place using a few bits of message passing. Hence, it is well suited to distributed cyber-attack detection in wide-area smart grids.

Most of the existing works on distributed detection consider fixed-sample-size (also known as one-shot) schemes, which aim to reach a satisfactory balance between the detection probability and false alarm probability. This type of schemes is useful when there is no strict latency constraint. On the other

hand, strict latency constraints apply to cyber-attack detection since such attacks are judiciously designed, and if not timely detected, can cause catastrophic consequences. The sequential detection framework, and in particular, sequential change detection (also known as quickest detection), which minimizes the average detection delay subject to certain performance constraint, enables online (i.e., real-time) monitoring for smart grid, hence suits well to cyber-attack detection.

Sequential detection (or quickest detection) of false data injection attacks is yet to be more carefully designed. The well-known Cumulative Sum (CUSUM) algorithm is minimax optimum under the centralized setup if the probability distributions before and after the attack are known [10]. However, typically there are several unknowns in cyber-attack detection for smart grid, namely the state vector, the injected malicious data, and the subset of meters compromised by the attackers. In [11], an adaptive CUSUM algorithm is proposed, which assumes a Gaussian prior with some fixed mean and covariance for the state vector, and also assumes that the injected data is small and positive in magnitude so that the first-order approximation to the decision statistic can be used. That scheme, as a result, becomes inefficient for large attacking data, which could be more detrimental to the network, and also for negative data, as shown in Section V.

In this paper, we propose new CUSUM-type algorithms based on the generalized likelihood ratio (GLR) for centralized and distributed cyber-attack detection. With the proposed algorithms, we establish, under the centralized and distributed setups, an online (i.e., real-time) monitoring framework, that is robust to arbitrary load situations in the power system and malicious data, and also computationally efficient. Our contributions are listed as follows.

1) The proposed algorithms are robust to arbitrary state variables (due to different load situations in the power system), arbitrary malicious data injected to the meter readings.
2) The computational complexity of the proposed algorithms scales linearly with the number of meters in the system.
3) The proposed algorithms significantly outperform the existing methods in the literature in terms of the average detection delay, as shown in Section V.
4) The proposed distributed detector leads to a very low communication overhead and energy consumption by censoring the uninformative measurements before the attack and transmitting a single bit per sample to the control center, thanks to the adaptive level-triggered sampling technique.

The remainder of this paper is organized as follows. In Section II, we briefly introduce the power grid monitoring system model and the associated false data injection attack detection problem. Then, we propose the centralized attack detector in Section III. Section IV treats the distributed attack detection in wide-area power grid by drawing on the novel level-triggered sampling scheme. In Section V, we provide extensive numerical experiments to demonstrate the advantages of the proposed detectors over the existing methods. Finally, Section VI concludes this paper.

II. Background and Problem Statement

Consider M meters in an $(N+1)$-bus power system. In this paper, we use the direct current (dc) power flow model, in which the N phase angles (one reference angle), denoted by the state vector $\mathbf{x} \triangleq [\theta_1, \ldots, \theta_N]^\intercal$, are to be estimated. Suppose, we collect all measurements of the power flows and power injections at time t in the vector $\mathbf{y}_t$, then we have the following linear system model [2], [27]:

$$\mathbf{y}_t = \mathbf{H}\mathbf{x}_t + \mathbf{e}_t \tag{1}$$

where $\mathbf{y}_t$ consists of the meter readings at time t, $\mathbf{H} \in \mathbb{R}^{M\times N}$ is the measurement matrix, and $\mathbf{e}_t \sim \mathcal{N}(\mathbf{0}, \sigma^2\mathbf{I}_M)$ is the measurement noise vector. Typically, the number of measurements is greater than that of the unknown parameters in order to provide necessary redundancy against the noise effect, i.e., $M > N$. In addition, aiming at a general application, we consider the dynamic state model, where the state vector evolves over time.

A. Problem Statement

Suppose the malicious attack strikes at time τ and intentionally manipulates the meter readings by $\mathbf{u}_t$. Accordingly, we write the attack-incurred measurement change as

$$\begin{cases} \mathbf{y}_t = \mathbf{H}\mathbf{x}_t + \mathbf{e}_t, & t < \tau \\ \mathbf{y}_t = \mathbf{H}\mathbf{x}_t + \mathbf{u}_t + \mathbf{e}_t = \mathbf{H}(\mathbf{x}_t + \mathbf{c}_t) + \mathbf{b}_t + \mathbf{e}_t, & t \geq \tau. \end{cases} \tag{2}$$

Note that here the aggregate injected false data (i.e., $\mathbf{u}_t$) has been decomposed into two parts $\mathbf{H}\mathbf{c}_t$ and $\mathbf{b}_t$, where $\mathbf{H}\mathbf{c}_t$ represents the component that lies in the column space of $\mathbf{H}$ [i.e., $\mathbf{H}\mathbf{c}_t \in \mathcal{R}(\mathbf{H})$], while $\mathbf{b}_t$ lies in the corresponding complementary space [i.e., $\mathbf{b}_t \in \mathcal{R}^\perp(\mathbf{H})$ and $\mathbf{H}(\mathbf{H}^\intercal\mathbf{H})^{-1}\mathbf{H}^\intercal\mathbf{b}_t = \mathbf{0}$]. As pointed out by [12], $\mathbf{b}_t$ is the only informative part that is detectable while $\mathbf{H}\mathbf{c}_t$ would seemingly bypass the monitoring system since it is indistinguishable from $\mathbf{H}\mathbf{x}_t$ *per se*. Hence, attackers intend to make the best use of their knowledge and resources to prevent detection, i.e., they try to hide attack vectors in the column space of $\mathbf{H}$. If attackers perfectly knew the network information (that is the value of matrix $\mathbf{H}$, including the topology and the line parameters, i.e., line admittances and transformer tap ratio), and could manipulate any meter they want, then they would be able to design stealth attacks that completely lie in $\mathcal{R}(\mathbf{H})$, i.e., $\mathbf{b}_t = \mathbf{0}$, hence bypass the security system [12]. Fortunately, in practice, this is not the case in a wide-area smart grid due to the following factors. First, most attackers gain network information by long-term off-line learning, whereas the power grid configuration could change over time (for example, the environment fluctuation can alter the line admittances); thus the attackers are unlikely to possess the real-time network information. Second, the attackers may have limited resources to access/manipulate sufficient set of smart meters. Notably, Liu and Li [13] put forth a local load redistribution [14] that constructs perfect attack with regional network information, efficiently lowering the information requirement. Nevertheless, such an attack could be prevented by securing sufficient meters according to [3], where the fundamental limit of perfect attack was investigated. Therefore, assuming that there is always a trace of the

attack vector (i.e., some components of $\mathbf{b}_t$ are nonzeros), we further write the change event of interest as

$$\begin{cases} b_t^m = 0, & m = 1, 2, \ldots, M, \quad t < \tau \\ |b_t^m| > \gamma, \, m \in \Omega, & t \geq \tau \end{cases} \tag{3}$$

where γ is a prescribed value, setting the lower bound for the measurement change that draws security attentions and the set Ω contains the significant components in the informative vector $\mathbf{b}_t$, referred to as attacked meters thereafter.

As such, our goal here is to detect the attack vector $\mathbf{b}_t$ as soon as possible after its occurrence at τ. The quickest detection, that exploits the statistical difference before and after the change-point, provides a suitable framework to achieve this goal.

B. Quickest Detection

In quickest detection, we sequentially observe samples in time, and then stop according to a predesigned rule to declare a change. Unlike the fixed-sample-size schemes that focus on the detection power, the sequential change detector aims at minimizing the average detection delay after the change-point. The commonly used performance measure is the worst-case average detection delay, proposed by Lorden [15]

$$J(T) = \sup_{\tau} \operatorname{ess\,sup}_{\mathcal{F}_\tau} \mathbb{E}_\tau \left[(T - \tau)^+ | \mathcal{F}_\tau \right]. \tag{4}$$

Here, T is a stopping time variable, corresponding to a certain detection scheme; $\mathcal{F}_\tau$ is the filtration, which can be understood as all the observations up to τ, $\mathbf{y}_1, \ldots, \mathbf{y}_\tau$. Thus, the expectation $\mathbb{E}_\tau$ is evaluated with respect to the post-change probability measure conditioned on the change-point τ and the past samples up to τ. The essential supremum is obtained over $\mathcal{F}_\tau$, yielding the least favorable situation for the detection delay.[1] The supremum in (4) is obtained over τ, meaning that the change occurs at such a point that the detection delay is maximized. To summarize, $J(T)$ characterizes the average detection delay for the worst possible history of observations before the change-point. While the small average detection delay under attack results in timely alarmed reaction, the running length under normal data, on the other hand, needs to be controlled to avoid frequent false alarms. Hence, the sequential change detection problem is formulated as follows:

$$\inf_T J(T) \quad \text{subject to} \quad \mathbb{E}_\infty[T] \geq \alpha. \tag{5}$$

Note that $\mathbb{E}_\infty$ corresponds to the case where the change never happens, i.e., $\tau = \infty$. To proceed with our cyber-attack detection problem, we denote the pre and postattack probability density functions (PDF) of the meter readings as p_0 and p_1, respectively. If all parameters in the PDFs can be specified, the quickest detection problem in (5) is optimally solved by the well-known CUSUM test [10]

$$T_c \triangleq \min \left\{ k : \max_{1 \leq j \leq k} \sum_{t=j}^{k} \log \frac{p_1(\mathbf{y}_t | \mathbf{x}_t, \mathbf{c}_t, \mathbf{b}_t)}{p_0(\mathbf{y}_t | \mathbf{x}_t)} \geq h \right\}. \tag{6}$$

[1] Simply put, $\operatorname{ess\,sup}_{\mathcal{F}_\tau}$ can be understood as the least upper bound of the objective function for all possible values of $\mathbf{y}_1, \mathbf{y}_2, \ldots, \mathbf{y}_\tau$.

Note that, to fully specify the test statistic in (6), the values of $\mathbf{x}_t$, $\mathbf{c}_t$, and $\mathbf{b}_t$ must be known. However, in reality, acquiring such information is hardly practical, rendering the CUSUM test infeasible. For example, $\mathbf{x}_t$ is unknown and needs to be estimated, as it is the essential task of the power grid monitoring system. In light of this, as we mentioned before, $\mathbf{c}_t$ will be completely mistaken as a part of the state vector in this estimation procedure and becomes indistinguishable from $\mathbf{x}_t$. In addition, considering the diverse nature of the attacking behaviors, $\mathbf{b}_t$ cannot be specified beforehand when designing the security system. Alternatively, in [11], the first-order approximation is proposed by assuming that $\mathbf{b}_t$ is element-wise positive and small. It deviates from the optimal solution as $\mathbf{b}_t$ becomes significant, which, in fact, is the regime of most interest. To address these issues, this paper resorts to the GLR method, that provides asymptotically optimal performance by replacing the unknown parameters with their maximum likelihood estimates (MLE) [16, Sec. 5.3]. We next propose novel centralized and distributed sequential attack detectors based on the GLR statistic.

III. Centralized Sequential Attack Detection

In this section, we consider the cyber-attack detection problem in a centralized setup. That is, all meter readings across the network are collected at a control center and processed together. We first derive a GLR-based change detector, namely generalized CUSUM, which is asymptotically optimal in theory, but its computational complexity is exponential in the number of meters, making it infeasible in large-scale networks. Then, we propose a modified detector whose computational complexity is linear in the number of meters.

A. Generalized CUSUM Detector

Based on the change event modeled by (3), upon replacing the unknown parameters with their MLEs in (6), the generalized CUSUM takes the form given by (7) (shown at the top of next page). Note that $\mathbf{c}_t$ is indistinguishable from $\mathbf{x}_t$, thus we combine them together as $\mathbf{x}_t$ under p_1. Compared to the method in [11], this sequential detector possesses the following advantages.

1) The state vector $\mathbf{x}_t$, which holds the bus phase angles, is not assumed to be a stationary Gaussian process, which is unrealistic for modeling a time-varying workload. Instead, $\mathbf{x}_t$ is estimated over time, providing robustness to arbitrary load situations in the power system.
2) The attacking vector $\mathbf{b}_t$ is neither assumed to be small, nor presumed in the first orthant (i.e., element-wise positive). Like $\mathbf{x}_t$, estimating $\mathbf{b}_t$ results in robustness to significant magnitude and direction changes in the attacking vector.
3) The uncertainty in the subset of attacked meters is incorporated into the detector.

We first compute the GLR s_t^Ω at time t conditioned on the set Ω. Given that $\mathbf{e}_t$ is white Gaussian noise, $\sup_{\mathbf{x}_t}$ yields the least-squares estimators under the two probability measures, that is

$$\hat{\mathbf{x}}_t^0 = \left(\mathbf{H}^\intercal \mathbf{H}\right)^{-1} \mathbf{H}^\intercal \mathbf{y}_t, \quad \hat{\mathbf{x}}_t^1 = \left(\mathbf{H}^\intercal \mathbf{H}\right)^{-1} \mathbf{H}^\intercal \left(\mathbf{y}_t - \mathbf{b}_t\right). \tag{8}$$

$$T_g \triangleq \min\left\{k:\ \max_{1\le j\le k}\sup_{\Omega}\sum_{t=j}^{k}\underbrace{\log\frac{\sup_{\mathbf{x}_t,|b_t^m|\ge\gamma,m\in\Omega}p_1\left(\mathbf{y}_t|\mathbf{x}_t,\mathbf{b}_t\right)}{\sup_{\mathbf{x}_t}p_0\left(\mathbf{y}_t|\mathbf{x}_t\right)}}_{s_t^{\Omega}}\ge h\right\} \tag{7}$$

Noting that $\hat{x}_t^1=\hat{x}_t^0-(\mathbf{H}^\intercal\mathbf{H})^{-1}\mathbf{H}^\intercal\mathbf{b}_t$, we have

$$\begin{aligned}s_t^{\Omega}&=\log\sup_{|b_t^m|\ge\gamma,m\in\Omega}p_1\left(\mathbf{y}_t\mid\hat{\mathbf{x}}_t^1,\mathbf{b}_t\right)-\log p_0\left(\mathbf{y}_t\mid\hat{\mathbf{x}}_t^0\right)\\&=\sup_{|b_t^m|\ge\gamma,m\in\Omega}\left[-\frac{1}{2\sigma^2}\left\|\mathbf{y}_t-\mathbf{H}\hat{\mathbf{x}}_t^1-\mathbf{b}_t\right\|_2^2+\frac{1}{2\sigma^2}\left\|\mathbf{y}_t-\mathbf{H}\hat{\mathbf{x}}_t^0\right\|_2^2\right]\\&=\sup_{|b_t^m|\ge\gamma,m\in\Omega}\left[\frac{1}{\sigma^2}\mathbf{b}_t^\intercal\mathbf{P}^\intercal\left(\mathbf{y}_t-\mathbf{H}\hat{x}_t^0\right)-\frac{1}{2\sigma^2}\mathbf{b}_t^\intercal\mathbf{P}^\intercal\mathbf{P}\mathbf{b}_t\right]\\&=\sup_{|b_t^m|\ge\gamma,m\in\Omega}\left[\frac{\mathbf{b}_t^\intercal\mathbf{P}\mathbf{y}_t}{\sigma^2}-\frac{\mathbf{b}_t^\intercal\mathbf{b}_t}{2\sigma^2}\right]\end{aligned} \tag{9}$$

where $\mathbf{P}\triangleq\mathbf{I}-\mathbf{H}(\mathbf{H}^\intercal\mathbf{H})^{-1}\mathbf{H}^\intercal$. Note that in (9), we used the assumption that $\mathbf{b}_t$ bears the complete information of detectability [i.e., $\mathbf{H}(\mathbf{H}^\intercal\mathbf{H})^{-1}\mathbf{H}^\intercal\mathbf{b}_t=\mathbf{0}$] to give $\mathbf{P}\mathbf{b}_t=\mathbf{b}_t$. In the centralized setup, all measurements are collected at the control center, thus $\widetilde{\mathbf{y}}_t\triangleq\mathbf{P}\mathbf{y}_t$, which is the projection of the measurement vector on $\mathcal{R}^{\perp}(\mathbf{H})$, is readily obtained. Then the GLR in (9) is explicitly expressed as

$$s_t^{\Omega}=\sup_{|b_t^m|\ge\gamma,\ m\in\Omega}\left(\frac{\mathbf{b}_t^\intercal\widetilde{\mathbf{y}}_t}{\sigma^2}-\frac{\mathbf{b}_t^\intercal\mathbf{b}_t}{2\sigma^2}\right) \tag{10}$$

$$=\sum_{m\in\Omega}\underbrace{\sup_{|b_t^m|\ge\gamma}\left(b_t^m\widetilde{y}_t^m-\frac{\left(b_t^m\right)^2}{2}\right)\Big/\sigma^2}_{s_t^m} \tag{11}$$

where

$$s_t^m=\begin{cases}\frac{\left(\widetilde{y}_t^m\right)^2}{2\sigma^2}, & |\widetilde{y}_t^m|\ge\gamma\\ \frac{|\widetilde{y}_t^m|}{\sigma^2}\gamma-\frac{1}{2\sigma^2}\gamma^2, & |\widetilde{y}_t^m|<\gamma.\end{cases} \tag{12}$$

With s_t^{Ω} available in closed-form, the GLR-based detector T_g in (7) can be implemented by exchanging the $\max_{1\le j\le k}$ and $\sup_{\Omega}$

$$T_g=\min\left\{k:\ \sup_{\Omega}\max_{1\le j\le k}\sum_{t=j}^{k}\sum_{m\in\Omega}s_t^m\ge h\right\} \tag{13}$$

$$=\min\left\{T_n,\ n=1,2,\ldots,\sum_{q=1}^{M}\binom{M}{q}=2^M-1\right\} \tag{14}$$

with $T_n\triangleq\min\{k:\max_{1\le j\le k}\sum_{t=j}^{k}\sum_{m\in\Omega_n}s_t^m\ge h\}$, where Ω_n represents a specific subset of all meters. Note that the equality between (13) and (14) holds true thanks to the discrete value of Ω (see [17] and a special case where the sup is evaluated over binary values has been discussed as two-sided CUSUM in [16, Sec. 2.2]). Consequently, following [17], (14) suggests that T_g can be implemented as a multichart scheme, where one GLR-based test is performed for each Ω_n, and the detection procedure stops as soon as one of these tests raises an alarm. This multichart scheme has a computational complexity that is linear in the number of meters, i.e., $O(M)$, only when we know that there is only a single attacked meter, i.e., $q=1$. In this specific case, T_g amounts to the single-bit change detector proposed in [18], i.e., each meter runs its local GLR-based test and the global detection procedure stops whenever a meter raises an alarm. However, in general, when the number of attacked meters is unknown, then (14) has a computational complexity exponential in the number of meters, i.e., $O(2^M)$.

B. Proposed Detector With Linear Complexity

We next propose an efficient detector that is linearly scalable to the number of attacked meters, and robust to the changes in the attacking vector. Note that the operator $\max_{1\le j\le k}$ in T_g implies that all the attacked meters are stricken at the same time, i.e., they share the same estimated change-point $j^\star=\arg\max_{1\le j\le k}\sum_{t=j}^{k}\sum_{m\in\Omega}s_t^m$. It is this underlying assumption that leads to T_m's that have to be run for all combinations, hindering us from further simplifying the detection procedure. To that end, we relax the constraint on simultaneous attack and modify the decision statistic of T_g in (13) by allowing each meter to search its own change-point, that is

$$\sup_{\Omega}\max_{1\le j\le k}\sum_{t=j}^{k}\sum_{m\in\Omega}s_t^m\Rightarrow\sup_{\Omega}\max_{1\le j_m\le k,\ m\in\Omega}\sum_{t=j_m}^{k}\sum_{m\in\Omega}s_t^m \tag{15}$$

which can be further expressed as

$$\sup_{\Omega}\sum_{m\in\Omega}\max_{1\le j_m\le k}\sum_{t=j_m}^{k}s_t^m=\sum_{m=1}^{M}\max\left\{\max_{1\le j_m\le k}\sum_{t=j_m}^{k}s_t^m,0\right\}. \tag{16}$$

Through the above derivation, the relaxation (i.e., individual search for change-point at each meter) on the GLR statistic of T_g has transformed the combinatorial search $\sup_{\Omega}$ into the operation of sum. This modification turns out to significantly simplify the original general CUSUM test T_g, given that the number of meters in the modern power system is in the order of hundreds or thousands. In addition, in the case where the attack strikes each meter asynchronously (e.g., there are time skews), searching the change-point at each meter is expected to be more effective. Consequently, following (13) and (16), we arrive at the resulting change detector:

$$T_p\triangleq\min\left\{k:\ \sum_{m=1}^{M}W_k^m\ge h\right\} \tag{17}$$

$$\text{where}\quad W_k^m\triangleq\max\left\{\max_{1\le j_m\le k}\sum_{t=j_m}^{k}s_t^m,0\right\} \tag{18}$$

can be computed recursively as follows.

Proposition 1: At meter m, the statistic W_k^m is recursively computed as

$$W_{k+1}^m = \max\left\{W_k^m + s_{k+1}^m, 0\right\} \tag{19}$$

where s_{k+1}^m is given by (12).

Proof:

$$\begin{aligned} W_{k+1}^m &= \max\left\{\max_{1\le j_m\le k+1}\sum_{t=j_m}^{k+1} s_t^m, 0\right\} \\ &= \max\left\{\max\left\{\max_{1\le j_m\le k}\sum_{t=j_m}^{k+1} s_t^m, s_{k+1}^m\right\}, 0\right\} \\ &= \max\left\{\max\left\{\max_{1\le j_m\le k}\sum_{t=j_m}^{k} s_t^m, 0\right\} + s_{k+1}^m, 0\right\} \\ &= \max\left\{W_k^m + s_{k+1}^m, 0\right\}. \end{aligned} \tag{20}$$

■

Combining (17) and (19) implies that the global decision statistic is obtained by summing up the local CUSUM-type recursive processes. As a matter of fact, using the sum of multiple CUSUM processes as the test statistic was studied in [19]. By the virtue of the analysis therein, we know that the detection delay of the proposed detector T_p shares the similar asymptotic optimality with T_g. In particular, they deviate from the optimal (which is only feasible when all parameters are known) by $O(\log\log\alpha)$ and $O(\text{constant})$, respectively, recalling that α is the false alarm period as defined in (5). Therefore, for practical scenarios where $\alpha = 10^2 \sim 10^6$, T_p performs as effectively as T_g, yet at a much lower implementation complexity. In a nutshell, the proposed detector in (17) features the following merits.

1) Its computational complexity scales linearly with the network size, i.e., $O(M)$, even when there is no prior knowledge about the set of attacked meters, as opposed to generalized CUSUM, which is $O(2^M)$.
2) It is robust, like the generalized CUSUM, to the changes in the distribution of the state vector $\mathbf{x}_t$, the magnitude, and direction changes in the attacking vector $\mathbf{b}_t$, and the uncertainty in the set of attacked meters.
3) It also greatly facilitates the decentralization of cyber-attack monitoring in wide-area power grids, which will be discussed in next section.

We summarize the proposed sequential attack detector [see (17)] in Algorithm 1. Before performing this algorithm, the parameters γ and h need to be prescribed. To be specific, the lower bound γ is decided according to the designer's tolerance on the attacking impact. A larger γ emphasizes interest in the malicious data with a higher impact, whereas a smaller γ implies sensitivity to small distortions. The decision threshold h is tailored to meet a certain performance requirement, i.e., the average detection delay $J(T_p)$ or the false alarm period α (owing to the diversity of attacks, the worst-scenario detection delay could be considered). Correspondingly, an off-line simulation suffices to fix the value of h, which only needs to be updated when the system setting is altered, for example, the noise level changes.

Algorithm 1 Centralized Sequential Cyber-Attack Detector

1: Initialization: $k \leftarrow 0, s_m \leftarrow 0, W_m \leftarrow 0,\ m = 1, \ldots, M$
2: **while** $\sum_{m=1}^{M} W_m < h$ **do**
3: $k \leftarrow k + 1$
4: Collect meter readings $\mathbf{y}_k$ and compute $\widetilde{\mathbf{y}}_k = \mathbf{P}\mathbf{y}_k$
5: Compute s_m according to (12) and update $W_m = \max\{W_m + s_m, 0\}$ for $m = 1, \ldots, M$
6: **end while**
7: Stop and raise the cyber-attack alarm

IV. Wide-Area Cyber-Attack Detection

In the previous section, the proposed sequential detector is developed under the centralized setup, where all the raw meter readings in the network are collected synchronously at each time by the control center. This induces a significant communication overhead in wide-area networks. As a matter of fact, communication across wide areas has become a critical concern in modern power grids, where wireless communication infrastructure (e.g., WiMax, Cellular, WiFi, Zigbee, Bluetooth) plays an important role [20]–[23]. In particular, [22] demonstrated the use of code division multiple access technology for power system SCADA, by providing cellular communication between sub-area remote terminal unit and SCADA server. Similarly, general packet radio service technology can also be applied to sub-area-to-SCADA communication [24]. On the other hand, the power industry deregulation has divided the large interconnected power system into increasingly many sub-areas [4], [5], [25]. In many cases, sub-areas are geographically separated, spanning over a vast area, which renders the communications and coordinations in the network challenging. All these have called for a more distributed setup in which sub-areas collect and manage their local meter readings, and then communicate with the control center for collaborative wide-area monitoring. In light of this practice, we proceed to propose a novel distributed sequential detector based on the proposed centralized detector T_p and a nonuniform sampling technique called level-triggered sampling. The resulting distributed detector remarkably decreases the communication overhead, yet preserves the high detection performance.

A. System Model and Background

Suppose there are L sub-areas and M meters in an $(N+1)$-bus network. As such, the meter readings $\mathbf{y}_t$ are divided into L sub-vectors, i.e., $\mathbf{y}_t = [\mathbf{y}_t^{(1)\mathsf{T}}, \mathbf{y}_t^{(2)\mathsf{T}}, \ldots, \mathbf{y}_t^{(L)\mathsf{T}}]^{\mathsf{T}}$, where $\mathbf{y}_t^{(\ell)}$ represents the measurements in sub-area ℓ. Similarly, sub-areas confront the attack vector $\mathbf{b}_t = [\mathbf{b}_t^{(1)\mathsf{T}}, \mathbf{b}_t^{(2)\mathsf{T}}, \ldots, \mathbf{b}_t^{(L)\mathsf{T}}]^{\mathsf{T}}$ and compute the projection $\widetilde{\mathbf{y}}_t = [\widetilde{\mathbf{y}}_t^{(1)\mathsf{T}}, \widetilde{\mathbf{y}}_t^{(2)\mathsf{T}}, \ldots, \widetilde{\mathbf{y}}_t^{(L)\mathsf{T}}]^{\mathsf{T}}$. The first issue that arises in the distributed setup is computing the projection $\widetilde{\mathbf{y}}_t = \mathbf{P}\mathbf{y}_t = \mathbf{y}_t - \mathbf{H}\hat{\mathbf{x}}_t^0$, which is readily available at the control center in the centralized setup. However, in the distributed setup, $\widetilde{\mathbf{y}}_t$ needs to be computed in a distributed fashion. Note that, in general, sub-areas are interconnected, and thus $\mathbf{H}$ is not perfectly block diagonal [though usually nearly so, e.g., the measurement matrix of the IEEE-14 bus system given by (32)], meaning that (1) cannot be directly decoupled into L sub-systems.

Consequently, the projection matrix $\mathbf{P} = \mathbf{I} - \mathbf{H}(\mathbf{H}^\intercal\mathbf{H})^{-1}\mathbf{H}^\intercal$ is not block diagonal, preventing a simple expression for $\widetilde{\mathbf{y}}_t^{(\ell)}$.

To resolve this issue, we first write the measurement model for each sub-area

$$\mathbf{y}_t^{(\ell)} = \mathbf{H}_\ell \mathbf{x}_t^{(\ell)} + \mathbf{b}_t^{(\ell)} + \mathbf{e}_t^{(\ell)}, \quad \ell = 1, \ldots, L \tag{21}$$

where $\mathbf{b}_t^{(\ell)} = 0$ before attack, $\mathbf{x}^{(\ell)} \in \mathbb{R}^{N_\ell}$, N_ℓ is the number of local buses and $\mathbf{H}_\ell \in \mathbb{R}^{M_\ell \times N_\ell}$, M_ℓ is the number of local meter readings. Note that here the neighboring sub-areas may share some state parameters, i.e., $\mathbf{x}_t^{(\ell)}$ and $\mathbf{x}_t^{(i)}$, $i \in \widetilde{\mathcal{N}}_\ell$, where $\widetilde{\mathcal{N}}_\ell$ denotes the set of neighboring sub-areas to ℓ, overlap partially owing to the meters deployed at their cross-links (usually termed as tie-line). In the global estimator vector $\hat{\mathbf{x}}_t^0 = (\mathbf{H}^\intercal\mathbf{H})^{-1}\mathbf{H}^\intercal\mathbf{y}_t$, denote the estimates of the state parameters associated to sub-area ℓ with $\hat{\mathbf{x}}_t^{(\ell)}$. Then, we can write

$$\widetilde{\mathbf{y}}_t^{(\ell)} = \mathbf{y}_t^{(\ell)} - \mathbf{H}_\ell \hat{\mathbf{x}}_t^{(\ell)}. \tag{22}$$

Hence, each sub-area ℓ needs to compute the local estimator vector $\hat{\mathbf{x}}_t^{(\ell)}$, which is a function of all measurements related to $\mathbf{x}_t^{(\ell)}$ in the network. In other words, due to interconnectedness, $\hat{\mathbf{x}}_t^{(\ell)}$ is not only a function of the measurements taken at sub-area ℓ. Performing several iterations of data fusion between neighboring sub-areas, we can compute $\hat{\mathbf{x}}_t^{(\ell)}$ at sub-area ℓ via the alternating direction method of multipliers (ADMM). The more iterations we have in ADMM, the closer it is to the global solution. Distributed state estimation using ADMM is well studied in [7] and we briefly summarize the procedure here. At each time t (we neglect the index t for notational convenience in (23)–(25), and the subscript i is used for the index of iteration, i.e., $\hat{\mathbf{x}}_i^{(\ell)}$ is the state estimate of $\mathbf{x}^{(\ell)}$ at time t after ith iteration of ADMM), the following recursive computation of $\hat{\mathbf{x}}_t^{(\ell)}$ is performed.

1) Local partial data exchange with neighbors

$$f_i^\ell[j] \triangleq \frac{1}{|\omega_\ell^j|} \sum_{k \in \omega_\ell^j} \hat{x}_i^{(k)}[j] \tag{23}$$

where $a[j]$ denotes the jth entry of vector $\mathbf{a}$, and j is the index for the state parameter in sub-area ℓ that are shared with others and ω_ℓ^j is the set of the sub-areas sharing the variable $\hat{x}^{(\ell)}[j]$ with sub-area ℓ. Depending on the overlapping level of the network, j can take multiple values for each sub-area. In a word, $f_i^\ell[j]$ is the average of the counterparts of $\hat{x}^{(\ell)}[j]$ from the neighbors that share it.

2) Incorporating with local measurements and evaluating the local state estimate

$$\hat{\mathbf{x}}_{i+1}^{(\ell)} = \left(\mathbf{H}_\ell^\intercal\mathbf{H}_\ell + c\mathbf{D}_\ell\right)^{-1}\left(\mathbf{H}_\ell^\intercal\mathbf{y}^{(\ell)} + c\mathbf{D}_\ell\mathbf{p}_i^\ell\right) \tag{24}$$

with $\mathbf{p}_i^\ell$ defined in the following recursive way:

$$p_{i+1}^\ell[j] = p_i^\ell[j] + f_{i+1}^\ell[j] - \frac{\hat{x}_i^\ell[j] - f_i^\ell[j]}{2}, \ \mathbf{p}_0^\ell = \mathbf{0}. \tag{25}$$

Where $\mathbf{D}_\ell \in \mathbb{N}^{N_\ell \times N_\ell}$ is a diagonal matrix defined for each sub-area ℓ with the (j,j)th entry equal to $|\omega_\ell^j|$ (i.e., the number of elements in set w_ℓ^j), and c is a small constant which can be adjusted for convergence consideration. Here, $\mathbf{f}^\ell$ and $\mathbf{p}^\ell$ are auxilliary variables for expressing the data fusion process. Note that the local partial data exchange between neighboring sub-areas in ADMM is much more efficient in terms of communication resources than the global data fusion in the centralized setup. However, we still need to devise a resource-efficient method to combine the local statistics $\{W_k^m\}$ for sequential attack detection as in (17).

As a result, with the local projection vector $\widetilde{\mathbf{y}}_t^{(\ell)}$ available through ADMM, we can implement the sequential detector T_p [see (17)] as

$$T_p \triangleq \min\left\{k : \sum_{\ell=1}^{L} g_k^\ell \geq h\right\} \tag{26}$$

where $g_k^\ell \triangleq \sum_{m \in \mathcal{N}_\ell} W_k^m$ denotes the local statistic of sub-area ℓ at time k, and W_k^m is given by (12) and (18). Nonetheless, transmitting multibit quantized sub-area statistics to the control center at every sampling instant still imposes demanding communication requirements. Next, we propose a level-triggered sampling scheme in which sub-areas sporadically transmit single-bit information to the control center to report the changes in their local statistics, thus significantly decreasing the communication overhead.

B. Distributed Sequential Attack Detector

In the conventional approach, each sub-area ℓ samples its local statistic g_k^ℓ uniformly over time, and transmits quantization bits to the control center for each sample. Alternatively, level-triggered sampling, adapting the sampling (and thus communication) times to g_k^ℓ, requires significantly less number of bits for accurate representation of each sample. Moreover, adaptive sampling (communication) suits very well to the nonuniform nature of g_k^ℓ, which hovers around zero before the attack and steadily increases after the attack.

Specifically, in level-triggered sampling, a sample is taken when the change in the signal with respect to its most recent approximation exceeds a certain level, say Δ. Define k_n^ℓ as the nth sampling time at sub-area ℓ, and $\widetilde{g}_{k_n^\ell}^\ell$ as the approximation to $g_{k_n^\ell}^\ell$ due to the accumulation of single-bit change information at sampling times until k_n^ℓ. Given $\widetilde{g}_{k_{n-1}^\ell}^\ell$, the next sampling is triggered at time

$$k_n^\ell \triangleq \inf\left\{k > k_{n-1}^\ell : g_k^\ell - \widetilde{g}_{k_{n-1}^\ell}^\ell \notin (-\Delta, \Delta)\right\}. \tag{27}$$

The single-bit change information

$$\phi_n^\ell \triangleq \operatorname{sign}\left(g_{k_n^\ell}^\ell - \widetilde{g}_{k_{n-1}^\ell}^\ell\right) \tag{28}$$

is then transmitted to the control center at time k_n^ℓ. Here, Δ is a positive constant, selected to control the frequency of transmission (i.e., the transmission frequency decreases with increasing Δ) and is known to the control center. The control center can recursively compute the approximation

$$\widetilde{g}_{k_n^\ell}^\ell = \widetilde{g}_{k_{n-1}^\ell}^\ell + \phi_n^\ell \Delta. \tag{29}$$

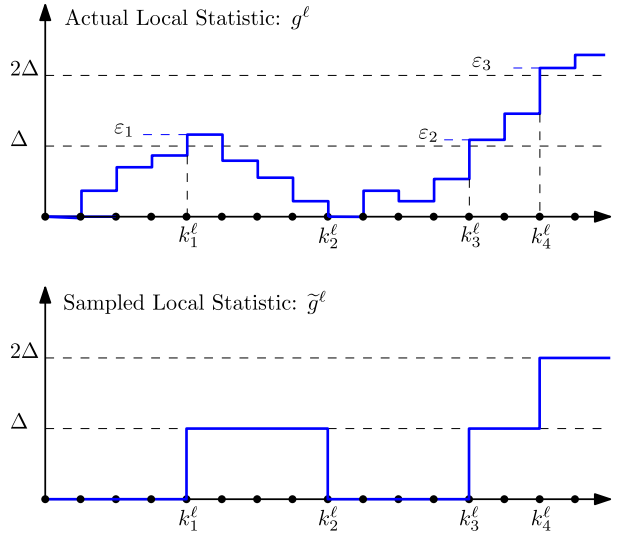

Fig. 1. Illustration for the level-triggered sampling scheme at sub-area ℓ.

Note that at each sampling time k_n^ℓ, the control center misses only the overshoot information of how much the change at time k_n^ℓ exceeded Δ, i.e., $\left|g_{k_n^\ell}^\ell - \widetilde{g}_{k_{n-1}^\ell}^\ell\right| - \Delta$. In general, such missing information is small compared to Δ (and very small compared to $g_{k_n^\ell}^\ell$), since it is caused by the last single increment that triggers sampling, and g_k^ℓ, being a likelihood-ratio-based statistic, does not experience abrupt increments. Most importantly, the discrepancy does not propagate over time since each overshoot is compensated at the next sampling time. This is illustrated in Fig. 1, where ε_i is the overshoot at each level-triggered sampling instant. It can be seen that ε_2 at k_3^ℓ is included in the next update of the increment Δ at k_4^ℓ, and similarly, the new overshoot ε_3 at k_4^ℓ will be updated to the control center in the upcoming sampling instant. We summarize the implementation of level-triggered sampling at sub-area ℓ as Algorithm 2.

On the other hand, to realize the detection scheme T_p in (26), the wide-area control center receives information bits from all sub-areas asynchronously and updates the global running statistic as follows:

$$\begin{aligned}\widetilde{g}_k &= \widetilde{g}_{k-1} + \sum_{\ell=1}^{L}\Big(\ _{\{k=k_n^\ell,\ \phi_n^\ell=1\}}\Delta - \ _{\{k=k_n^\ell,\ \phi_n^\ell=-1\}}\Delta\Big)\\ &= \sum_{\ell=1}^{L}\sum_{n:\ k_n^\ell<k}\Big(\ _{\{\phi_n^\ell=1\}}\Delta - \ _{\{\phi_n^\ell=-1\}}\Delta\Big) \qquad (30)\end{aligned}$$

where $_{\{A\}}$ is the indicator function, taking the value 1 if A is true and 0 otherwise. The distributed sequential detector based on level-triggered sampling at the control center is summarized in Algorithm 3. Every time the global decision statistic is updated, the control center compares it with the prescribed threshold h to determine whether to raise an alarm or to continue receiving information from sub-areas.

In summary, the level-triggered sampling scheme features an inherent data compression and adaptive communication between the distributed sub-areas and control center, thus provides significant savings in bandwidth and energy consumption.

Algorithm 2 Distributed Sequential Cyber-Attack Detector (at Sub-Area ℓ)

1: Initialization: $k \leftarrow 0$, $g \leftarrow 0$, $\lambda \leftarrow 0$, $s_m \leftarrow 0$, $W_m \leftarrow 0$, $m \in \mathcal{N}_\ell$
2: **while** $g - \lambda \in (-\Delta, \Delta)$ **do**
3: $k \leftarrow k + 1$
4: Collect local meter readings $\mathbf{y}_k$ and compute projection $\widetilde{\mathbf{y}}_k$ via ADMM given by (23)–(25)
5: Compute s_m using (12) and update $W_m = \max\{W_m + s_m\}$, for $m \in \mathcal{N}_\ell$
6: $g \leftarrow g + \sum_{m\in\mathcal{N}_\ell} W_m$
7: **end while**
8: Send $\phi = \text{sign}(g - \lambda)$ to the control center
9: $\lambda \leftarrow \lambda + \phi\Delta$ and go to step 2.

Algorithm 3 Distributed Sequential Cyber-Attack Detector (at Control Center)

1: Initialization: $g \leftarrow 0$
2: **while** $g < h$ **do**
3: Wait to receive information bits, say, r_1 "+1"s and r_2 "−1"s
4: $g \leftarrow g + (r_1 - r_2)\Delta$
5: **end while**
6: Raise the attack alarm

V. Numerical Results

In this section, we examine the proposed cyber-attack detectors numerically based on the IEEE 14-bus system (Fig. 2). Voltage magnitudes are set to be equal and normalized to 1. Line admittances are set to be $j1$. All the meters are placed in the same way as [5], [7], and [26]. The network is partitioned into four sub-areas, whose buses are grouped with dashed lines in Fig. 2. As such, the measurement matrix $\mathbf{H}$ is given by (32), where the columns are arranged such that the structure of overlapped states between neighboring sub-areas is revealed and the sub-area measurement matrices $\mathbf{H}_\ell$, $\ell = 1, 2, 3, 4$ are highlighted by blue dashed boxes. Throughout this section, $\gamma = 0.02$ and all meters readings are contaminated independently by AWGN with variance $\sigma^2 = 10^{-4}$. We examine the proposed detectors both in centralized and distributed scenarios. The dynamic state parameters are generated by running the MATPOWER "case14" dc power-flow algorithm with linear load increase at some randomly selected buses [27]. Bus 6 is presumed as the reference bus. First, using an example of $\mathbf{b}_t$, we compare the decision statistics of the proposed centralized detector and the "first-order CUSUM" in [11]. Then, we apply the proposed detector and first-order CUSUM to a large group of randomly generated $\mathbf{b}_t$ to examine their robustness for unknown $\mathbf{b}_t$. We also illustrate that the distributed detector based on level-triggered sampling yields well-approximated decision statistic at the control center. Finally, the average detection delay performance is plotted against the false alarm period to show the effectiveness of the distributed detector compared to its centralized counterpart.

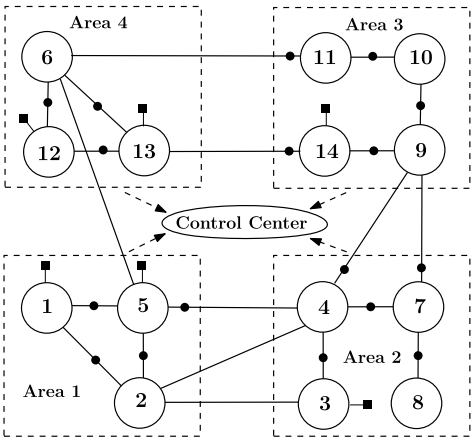

Fig. 2. IEEE 14-bus power system partitioned into four sub-areas that communicate with the control center. The small filled circles on the branches refer to power-flow measurements between two buses, and the squares refer to power injection measurements.

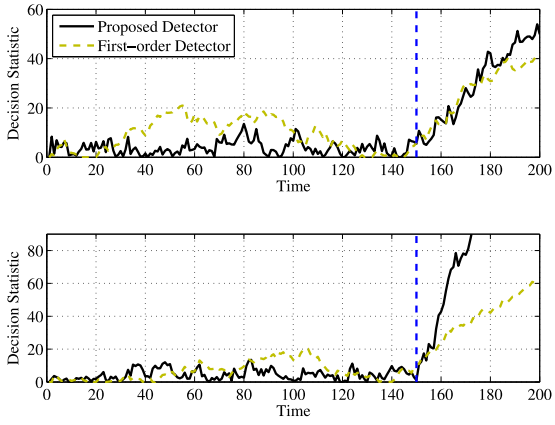

Fig. 3. Decision statistics of the proposed centralized detector and the first-order CUSUM detector [11] under attack $\mathbf{b}_t^*$ (top) and $1.5\mathbf{b}_t^*$ (bottom), respectively.

A. Centralized Detector Versus First-Order Detector

We begin by demonstrating the decision statistics of the proposed centralized detector and the first-order CUSUM approach [11] before and after the attack occurs. Suppose the attack occurs at $\tau = 150$ (marked by blue dashed lines in the figures). The attacking vector is generated as

$$\mathbf{b}_t^* = [0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, -1, 1, \\ -6, -5, -48, 43, -23, 47, 132, -21] \times 10^{-4}$$

and $\mathbf{b}_t \in \mathcal{R}^{\perp}(\mathbf{H})$. Fig. 3 depicts how the decision statistics react to the attacking behavior (the top plot is under the attack of $\mathbf{b}_t$ and bottom plot is under the attack of $1.5\mathbf{b}_t$). As seen from the top plot, the first-order CUSUM exhibits more fluctuation than the proposed detector, indicating a higher false alarm rate/smaller false alarm period $\mathbb{E}_{\infty}[T]$. Both methods show abrupt increase after the attack occurs at τ although only a fraction of $\mathbf{b}_t$ is nonzero. However, it is shown in the bottom plot that the proposed detector experiences a considerably steeper change in the decision statistic, hence is more sensitive to the magnitude increase of attacking vector than the first-order CUSUM. This is expected since the first-order CUSUM test builds on the small $\mathbf{b}_t$ assumption, and is prone to efficiency loss for larger $\mathbf{b}_t$.

Next, to demonstrate the robustness of the proposed detector to arbitrary attacking vector, we randomly generate a large group of $\mathbf{b}_t$ and examine the successful rates of both detectors within a fixed time window after the occurrence of attack. For each group of $\mathbf{b}_t$, 10^5 instances are generated to cover more diverse attacking behaviors. By successful rate, we mean the fraction of $\mathbf{b}_t$ out of 10^5 that are successfully detected within the selected time window. The decision thresholds are chosen such that both detectors meet the constraint $\mathbb{E}_{\infty}[T] \cong 10^3$. The following groups of $\mathbf{b}_t$ and time window are used.

1) $\mathbf{b} = \mathbf{Pu}$, $u_i \sim \mathcal{U}(0.00, 0.02)$, Window=10, 20.
2) $\mathbf{b} = \mathbf{Pu}$, $u_i \sim \mathcal{U}(-0.02, 0.02)$, Window=20, 100.

From the first to the second group of $\mathbf{b}_t$, we increase the number of negative components by decreasing the lower limit of the uniform distribution. Also, to exhibit the robustness of the proposed detector, we plot the success rate along with different number of attacked meters, whose corresponding $\mathbf{b}_t$ entries admit $|b_t^m| \geq \gamma$. As seen from Figs. 4 and 5, the successful detection rate of the proposed detector always stays above that of first-order CUSUM detector, indicating its robustness to a wide range of $\mathbf{b}_t$. In particular, the following observations can be made.

1) The more the attacked meters are, the higher proportion of the attacking vectors can be detected within the fixed window, implying a smaller detection delay. This is particularly true when the window is small, for example, Window = 10 in Fig. 4.
2) In general, if we increase the window size, successful detection increases for both methods.

In both groups of $\mathbf{b}_t$, the success rate of the proposed method approaches 100%, regardless of the number of attacked meters. However, the first-order CUSUM deteriorates severely in the second group, where more negative $\mathbf{b}_t$ is generated. For example, in Fig. 5, even though the window size is set to be 100, which is impractically large, the first-order CUSUM detects only less than 50% of generated $\mathbf{b}_t$, indicating lack of robustness.

B. Centralized Detector Versus Distributed Detector

In this section, we examine the performance of the proposed distributed detector, both with and without level-triggered sampling. Instead of randomly choosing the attacking vector, we consider one that is deliberately designed by the attacker with partial/inaccurate network information. To this end, we assume that the attacker perceives the measurement matrix $\mathbf{H}$ as $\mathbf{H}_a$, and $\mathbf{H} = \mathbf{H}_a + \boldsymbol{\delta}$, where $\boldsymbol{\delta}$ captures the misinformation at the attacker's side. Nevertheless, the attacker intends to launch the perfect attack, that would supposedly bypass the security system as proposed in [12]. This is also the attacking strategy that maximizes the impact on state estimation and minimizes the detectable energy. Denote $\mathbf{c}$ as the state estimate error that the attacker aims to cause, then the injected data is $\mathbf{u}_t = \mathbf{H}_a\mathbf{c}_t$ [12], and $\mathbf{b} = \mathbf{Pu}_t$. Note that

$$\mathbf{b}_t = \mathbf{PH}_a\mathbf{c}_t = \mathbf{P}\left(\mathbf{H} - \boldsymbol{\delta}\right)\mathbf{c}_t = -\mathbf{P}\boldsymbol{\delta}\mathbf{c} \tag{31}$$

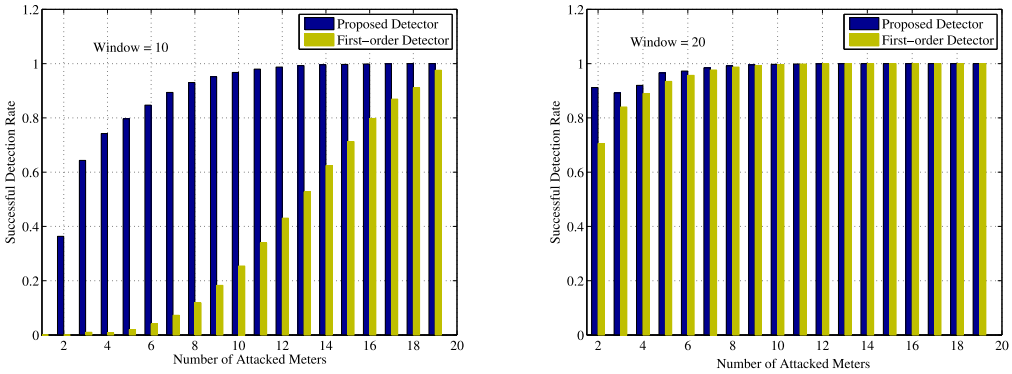

Fig. 4. Comparison of the proposed detector and the first-order CUSUM detector based on the first group of generated $\mathbf{b}_t$.

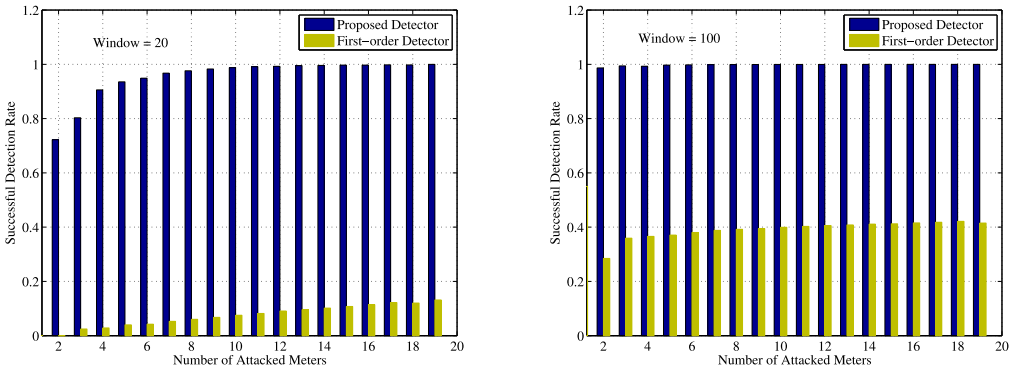

Fig. 5. Comparison of the proposed detector and the first-order CUSUM detector based on the second group of generated $\mathbf{b}_t$.

thus the attacker has made best use of their available information to limit the detectable $\mathbf{b}$, with no knowledge of $\boldsymbol{\delta}$ at all. In the simulation below, we assume the case where $\mathbf{H}_a$ characterizes the correct network topology, but the branch parameters deviate from true values by a zero-mean Gaussian variable with variance $\sigma^2 = 0.1$ (recalling that all branches are assumed to have unit reactance), which could be induced by real-time environment change, or measurement error. Note that the attacker does not know the deviation values or their statistical properties.

The level-triggered sampling threshold is chosen as $\Delta = 6$. Fig. 6 depicts the decision statistics of proposed centralized detector and its associated distributed implementation (with and without level-triggered sampling) under the attack that occurs at $\tau = 250$. The distributed detector without level-triggered sampling refers to the detector (26) based on ADMM only, i.e., the local statistics are transmitted to the control center with infinite bits of quantization at every time, as opposed to the level-triggered sampling where they are transmitted with single-bit message every random period of time. The ADMM is implemented with number of iterations equal to 10 and $c = 0.4$. We see that the decision statistics of the distributed detectors well approximate the centralized statistic. Notably, before the attack, the global statistic of the distributed detector with level-triggered sampling is rarely updated, indicating small sub-area to control center communication; while after the attack, frequent updates take place. This demonstrates the adaptiveness of the level-triggered sampling scheme to the local information, that is, only necessary information

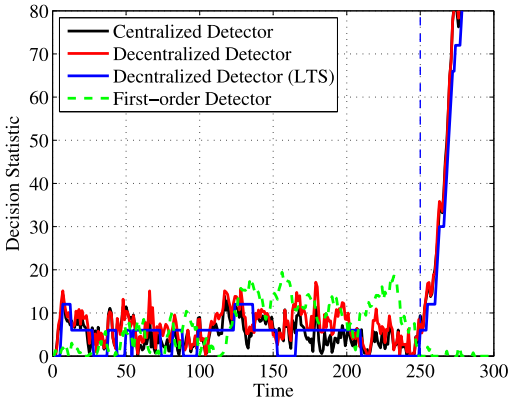

Fig. 6. Comparison of the decision statistics of the centralized, distributed (with and without level-triggered sampling scheme) detectors, and the first-order detector.

is transmitted to the control center. We also plot the statistic of the first-order detector, which fails to react to the attack, showing no abrupt change of statistic after τ.

Next, we compare the proposed centralized and distributed detectors with the sequential detectors in the literature in terms of average detection delay as false alarm period increases. In Fig. 7, the conventional fixed-sample-size scheme (black line with diamond marks) corresponds to repeatedly applying one-shot false data detector, which is accomplished by the classical largest normalized residue (LNR) test [28]. It is seen that the repeated LNR test degrades remarkably as the false alarm period increases, compared to the other methods

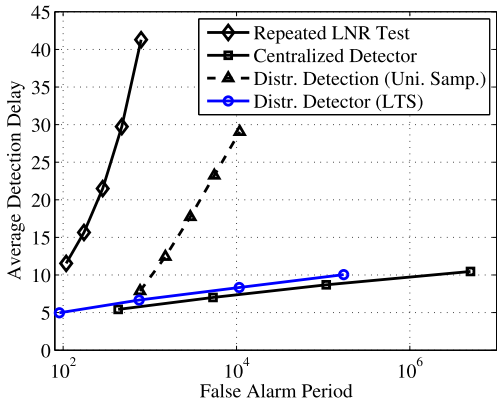

Fig. 7. Comparison of the fixed-sample detector, and the proposed centralized detector, level-triggered-sampling-based detector, and uniform sampling detector.

because it disregards the accumulative effect of the attacking behavior. The black line with squares corresponds to the centralized detector, which yields the best performance. The distributed detectors are implemented with the number of ADMM iterations equal to 10. We again have $\Delta = 6$. Note that the distributed detector based on level-triggered sampling performs similarly to the centralized detector, showing a slight degradation in the detection delay performance while significantly reducing the communication overhead. Specifically, for the four sub-areas, the average communication intervals are $[37.5, 94.7, 68.2, 24.4]$ under normal condition, and $[1.9, 22.1, 25.4, 17.9]$ under attack. As expected, before the attack, communication resources are saved by censoring uninformative data; and after the attack, informative data is transmitted more frequently. Throughout the procedure, the information update is realized by single-bit message transmission. To demonstrate the efficiency of the level-triggered sampling scheme, we also give the performance of the proposed distributed detector based on conventional uniform sampling (dashed line with triangle marks), in which single-bit quantized local statistics are transmitted with a period $V = 2$ (approximately match the minimum average transmission interval of level-triggered sampling, i.e., that of sub-area 3 under attack). The following simple one-bit quantization scheme is used: $\varphi = \text{sign}(g_k^{(\ell)} - g_{k-V}^{(\ell)})\ Q$, where we choose $Q = 3$. We see that the uniform sampling scheme deviates from the centralized detector considerably due to the coarse single-bit quantization. Moreover, the communication intervals are fixed at $V = 2$, thus lacking the adaptiveness to the nonuniform information characteristics before and after the attack. Note that frequent transmission of local statistics to the control center wastes the valuable communication resources.

VI. Conclusion

We have considered the sequential detection problem of false data injection attack in smart grid. We have proposed a centralized detector based on GLR, and showed that it is robust to various attacking data compared to the existing methods, and also computationally efficient. For wide-area monitoring in smart grid, we have further developed a distributed sequential cyber-attack detector using an adaptive sampling technique called level-triggered sampling. The distributed detector considerably reduces the communication overhead in the system, compared to naive approaches, yet preserves the robustness and high performance of the proposed centralized detector. Numerical results have demonstrated the considerable advantages of the proposed centralized and distributed detectors over existing methods in terms of robustness and average detection delay performance.

$$
\begin{array}{c}
\\
P_{1,2}\\P_{1,5}\\P_{2,5}\\P_{1}\\P_{5}\\P_{4,5}\\
\\
P_{3}\\P_{3,4}\\P_{4,7}\\P_{7,8}\\P_{4,9}\\P_{7,9}\\
\\
P_{9,10}\\P_{6,11}\\P_{10,11}\\P_{9,14}\\P_{14}\\P_{13,14}\\
\\
P_{13}\\P_{6,13}\\P_{6,12}\\P_{12,13}\\P_{12}
\end{array}
\begin{pmatrix}
\theta_1 & \theta_5 & \theta_2 & \theta_4 & \theta_3 & \theta_8 & \theta_7 & \theta_9 & \theta_{10} & \theta_{11} & \theta_{14} & \theta_{13} & \theta_{12}\\
1 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & -1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
2 & -1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
-1 & 4 & -1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & -1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
\\
0 & 0 & -1 & -1 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & -1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 1 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & -1 & 1 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 & 0 & 0 & 0 & 0 & 0\\
\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & -1 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 2 & -1 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 1 & 0\\
\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 3 & -1\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 1\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 2
\end{pmatrix}
\begin{array}{l}
\\
\\
\\
\\
\\
\\
\mathbf{H}_1\\
\\
\\
\\
\\
\\
\\
\mathbf{H}_2\\
\\
\\
\\
\\
\\
\mathbf{H}_3\\
\\
\\
\\
\\
\mathbf{H}_4
\end{array}
\tag{32}
$$

References

[1] A. G. Tartakovsky, B. L. Rozovskii, R. B. Blažek, and H. Kim, "A novel approach to detection of intrusions in computer networks via adaptive sequential and batch-sequential change-point detection methods," *IEEE Trans. Signal Process.*, vol. 54, no. 9, pp. 3372–3382, Sep. 2006.

[2] S. Cui *et al.*, "Coordinated data-injection attack and detection in the smart grid: A detailed look at enriching detection solutions," *IEEE Signal Process. Mag.*, vol. 29, no. 5, pp. 106–115, Sep. 2012.

[3] O. Kosut, L. Jia, R. Thomas, and L. Tong, "Malicious data attacks on the smart grid," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 645–658, Dec. 2011.

[4] Y.-F. Huang, S. Werner, J. Huang, N. Kashyap, and V. Gupta, "State estimation in electric power grids: Meeting new challenges presented by the requirements of the future grid," *IEEE Signal Process. Mag.*, vol. 29, no. 5, pp. 33–43, Aug. 2012.

[5] G. N. Korres, "A distributed multiarea state estimation," *IEEE Trans. Power Syst.*, vol. 26, no. 1, pp. 73–84, Feb. 2011.

[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] V. Kekatos and G. B. Giannakis, "Distributed robust power system state estimation," *IEEE Trans. Power Syst.*, vol. 28, no. 2, pp. 1617–1626, May 2013.

[8] Y. Yilmaz, G. Moustakides, and X. Wang, "Cooperative sequential spectrum sensing based on level-triggered sampling," *IEEE Trans. Signal Process.*, vol. 60, no. 9, pp. 4509–4524, Sep. 2012.

[9] Y. Yilmaz and X. Wang, "Sequential decentralized parameter estimation under randomly observed Fisher information," *IEEE Trans. Inf. Theory*, vol. 60, no. 2, pp. 1281–1300, Feb. 2014.

[10] G. Moustakides, "Optimal stopping times for detecting changes in distributions," *Ann. Statist.*, vol. 14, no. 4, pp. 1379–1387, 1986.

[11] 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. 45th Annu. Conf. Inf. Sci. Syst.*, Baltimore, MD, USA, Mar. 2011, pp. 1–6.

[12] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," in *Proc. 16th ACM Conf. Comput. Commun. Security*, Chicago, IL, USA, Nov. 2009, pp. 21–32.
[13] X. Liu and Z. Li, "Local load redistribution attacks in power systems with incomplete network information," *IEEE Trans. Smart Grid*, vol. 5, no. 4, pp. 1665–1676, Jul. 2014.
[14] Y. Yuan, Z. Li, and K. Ren, "Modeling load redistribution attacks in power system," *IEEE Trans. Smart Grid*, vol. 2, no. 2, pp. 382–390, Jun. 2011.
[15] G. Lorden, "Procedures for reacting to a change in distribution," *Ann. Math. Statist.*, vol. 42, no. 6, pp. 1897–1908, 1971.
[16] M. Basseville and I. V. Nikiforov, *Detection of Abrupt Changes: Theory and Application*. Englewood Cliffs, NJ, USA: Prentice Hall, 1993.
[17] A. G. Tartakovsky and A. S. Polunchenko, "Quickest changepoint detection in distributed multisensor systems under unknown parameters," in *Proc. 11th Int. Conf. Inf. Fusion*, Cologne, Germany, Jun./Jul. 2008, pp. 1–8.
[18] O. Hadjiliadis, H. Zhang, and H. V. Poor, "One shot schemes for decentralized quickest change detection," *IEEE Trans. Inf. Theory*, vol. 55, no. 7, pp. 3346–3359, Jul. 2009.
[19] Y. Mei, "Efficient scalable schemes for monitoring a large number of data streams," *Biometrika*, vol. 97, no. 2, pp. 419–433, 2010.
[20] V. Terzija *et al.*, "Wide-area monitoring protection, and control of future electric power networks," *Proc. IEEE*, vol. 99, no. 1, pp. 80–93, Jan. 2011.
[21] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A survey on smart grid communication infrastructures: Motivations, requirements and challenges," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 1, pp. 5–20, Apr. 2013.
[22] X. Zhang, Y. Gao, G. Zhang, and G. Bi, "CDMA2000 cellular network based SCADA system," in *Proc. Int. Conf. Power Syst. Technol.*, Kunming, China, 2002, pp. 1301–1306.
[23] P. P. Parikh, M. G. Kanabar, and T. S. Sidhu, "Opportunities and challenges of wireless communication technologies for smart grid applications," in *Proc. IEEE Power Energy Soc. Gen. Meeting*, Minneapolis, MN, USA, Jul. 2010, pp. 1–7.
[24] L. Kong, J. Jin, and J. Cheng, "Introducing GPRS technology into remote monitoring system for prefabricated substations in China," in *Proc. Int. Conf. Mobile Technol.*, Guangzhou, China, Nov. 2005, p. 6.
[25] A. Gómez-Expósito, A. de la Villa Jaén, and C. Gómez-Quiles, "A taxonomy of multi-area state estimation methods," *IEEE Trans. Power Syst.*, vol. 81, no. 4, pp. 1060–1069, Apr. 2011.
[26] L. Xie, D.-H. Choi, S. Kar, and H. V. Poor, "Fully distributed state estimation for wide-area monitoring systems," *IEEE Trans. Power Syst.*, vol. 3, no. 3, pp. 1154–1169, Sep. 2012.
[27] R. D. Zimmerman and C. E. Murillo-Sánchez. (Dec. 2011). *MATPOWER 4.1 User's Manual*. [Online]. Available: http://www.pserc.cornell.edu/matpower/manual.pdf.
[28] E. Handschin, F. C. Schweppe, J. Kohlas, and A. Fiechter, "Bad data analysis for power system state estimation," *IEEE Trans. Power App. Syst.*, vol. PAS-94, no. 2, pp. 329–337, Mar./Apr. 1975.

Shang Li received the B.Sc. degree in electronics from Peking University, Beijing, China, and the M.Phil. degree in electronic and computer engineering from the Hong Kong University of Science and Technology, Hong Kong, in 2010 and 2012, respectively. He is currently pursuing the Ph.D. degree in electrical engineering from Columbia University, New York, NY, USA.

His current research interests include random matrix theory with application in multi-antenna communication systems and statistical signal processing with applications in social networks and smart grids.

Yasin Yılmaz received the B.Sc. degree from Middle East Technical University, Ankara, Turkey; the M.Sc. degree from Koc University, Istanbul, Turkey; and the Ph.D. degree from Columbia University, New York, NY, USA, in 2008, 2010, and 2014, respectively, all in electrical engineering.

He is currently a Post-Doctoral Research Fellow with the University of Michigan, Ann Arbor, MI, USA. His current research interests include statistical signal processing, sequential detection and estimation, event-based systems, cyber-physical systems, correlation mining, and anomaly detection.

Xiaodong Wang (S'98–M'98–SM'04–F'08) received the Ph.D. degree in electrical engineering from Princeton University, Princeton, NJ, USA, in 1998.

He is a Professor of Electrical Engineering at Columbia University, New York, NY, USA. His current research interests include the general areas of computing, signal processing, communications wireless communications, statistical signal processing, and genomic signal processing, and has published extensively in the above areas. He has authored a recent book entitled *Wireless Communication Systems: Advanced Techniques for Signal Reception* (Prentice Hall, 2003).

Dr. Wang was the recipient of the 1999 National Science Foundation CAREER Award, the 2001 IEEE Communications Society and Information Theory Society Joint Paper Award, and the 2011 IEEE Communication Society Award for Outstanding Paper on New Communication Topics. He has served as an Associate Editor of the IEEE TRANSACTIONS ON COMMUNICATIONS, the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, the IEEE TRANSACTIONS ON SIGNAL PROCESSING, and the IEEE TRANSACTIONS ON INFORMATION THEORY.