Real-Time Nonparametric Anomaly Detection in High-Dimensional Settings

Mehmet Necip Kurt, Yasin Yılmaz, and Xiaodong Wang

Abstract

Timely and reliable detection of abrupt anomalies, e.g., faults, intrusions/attacks, is crucial for real-time monitoring and security of many modern systems such as the smart grid and the Internet of Things (IoT) networks that produce high-dimensional data. With this goal, we propose effective and scalable algorithms for real-time anomaly detection in high-dimensional settings. Our proposed algorithms are nonparametric (model-free) as both the nominal and anomalous multivariate data distributions are assumed to be unknown. We extract useful univariate summary statistics and perform the anomaly detection task in a single-dimensional space. We model anomalies as persistent outliers and propose to detect them via a cumulative sum (CUSUM)-like algorithm. In case the observed data stream has a low intrinsic dimensionality, we find a low-dimensional submanifold in which the nominal data are embedded and then evaluate whether the sequentially acquired data persistently deviate from the nominal submanifold. Further, in the general case, we determine an acceptance region for nominal data via the Geometric Entropy Minimization (GEM) method and then evaluate whether the sequentially observed data persistently fall outside the acceptance region. We provide an asymptotic lower bound on the average false alarm period of the proposed CUSUM-like algorithm. Moreover, we provide a sufficient condition to asymptotically guarantee that the decision statistic of the proposed algorithm does not diverge in the absence of anomalies. Numerical studies illustrate the effectiveness of the proposed schemes in quick and accurate detection of changes/anomalies in a variety of high-dimensional settings.

Index Terms

High-dimensional data, summary statistic, Geometric Entropy Minimization (GEM), principal component analysis (PCA), real-time anomaly detection, nonparametric, cumulative sum (CUSUM).

I. Introduction

A. Background

Anomaly refers to deviation from the expected (regular) behavior. Anomaly detection has been widely studied and to name a few, many distance-based, density-based, subspace-based, support vector machine (SVM)-based, neural networks-based, and information theoretic anomaly detection techniques have been proposed in the literature in a variety of application domains such as intrusion detection in computer and communication networks, credit card fraud detection, industrial damage detection, etc. [1]–[3]. Early and accurate detection of anomalies has a critical importance for safe and reliable operation of many modern

M. N. Kurt and X. Wang are with the Department of Electrical Engineering, Columbia University, New York, NY 10027, USA (e-mail: m.n.kurt@columbia.edu; wangx@ee.columbia.edu).

Y. Yılmaz is with the Department of Electrical Engineering, University of South Florida, Tampa, FL 33620, USA (e-mail: yasiny@usf.edu).

systems such as the power networks (smart grid) and the Internet of Things (IoT) networks that produce high-dimensional data streams. Such sudden anomalies often correspond to changes in the underlying statistical properties of the observed processes. To detect the changes, the framework of quickest detection [4], [5] is quite suitable, where the statistical inference about the monitored process is typically done through observations acquired sequentially over time and the goal is to detect the changes as soon as possible after they occur while limiting the risk of false alarm.

The well-known quickest detection algorithms require the exact knowledge or estimates of the probability density functions (pdfs) of the observed data stream for both the pre- and post-change cases [4], [5]. On the other hand, in high-dimensional settings, e.g., large-scale complex networks that consist of large number of nodes that exhibit complex interactions, it is usually difficult to model or intractable to estimate the high-dimensional multivariate pdfs. Moreover, it is, in general, quite difficult to model all possible types of anomalies. Hence, in a general anomaly detection problem, the post-change (anomalous) pdf is totally unknown. To overcome such difficulties, we propose to extract useful univariate summary statistics from the observed high-dimensional data and perform the anomaly detection task in a single-dimensional space, through which we also aim to make more efficient use of limited computational resources and to speed up the algorithms, that is especially required in time-sensitive online settings.

Although a summary statistic may not completely characterize a random process, it can be useful to evaluate the non-similarity between random processes with different statistical properties. In our problem, there are two main challenges to determine good summary statistics: (i) summary statistics should be well informative to (statistically) distinguish anomalous data from nominal (non-anomalous) data, (ii) since we are in an online setting, computation of the summary statistics should be simple to allow for real-time processing. In this paper, we consider two alternative summary statistics: (i) if the observed nominal data has a low intrinsic dimensionality, firstly finding a representative low-dimensional submanifold in which the nominal data are embedded and then computing a statistic that shows how much the incoming data stream deviates from the nominal submanifold; (ii) in the general case, determining an acceptance region for the nominal data via the Geometric Entropy Minimization (GEM) method [6], [7] and then computing a nearest neighbor (NN) statistic that shows how much the incoming data stream is away from the acceptance region. We propose to firstly compute a set of nominal summary statistics that constitute the baseline in an offline phase and then monitor possible deviations of online summary statistics from the baseline statistics.

Anomaly detection schemes based on parametric models are vulnerable to model mismatch that limits their applicability. For instance, it is common to fit a Gaussian or Gaussian mixture model to the observed data or the data after dimensionality reduction [1], [2], [8], [9] and to assume Gaussian noise or residual terms, see e.g., [10]. Such parametric approaches are powerful only if the observed data perfectly matches with the presumed model. On the other hand, nonparametric data-driven techniques are robust to the data model mismatch, that results in wider applicability of such techniques in a variety of problems. Moreover, in practical high-dimensional settings, the lack of parametric models is common and complicated parameter-laden algorithms generally result in low performance, over-fitting, and bias towards particular anomaly types [11]. Hence, in this paper, we do not make parametric model assumptions for the observed high-dimensional data stream nor for the extracted summary statistics.

Conventional anomaly detection schemes ignore the temporal relation between anomalous data points and make sample-by-sample decisions [1], [2]. Such schemes are essentially outlier detectors that are vulnerable to false alarms since it is possible to observe non-persistent random outliers in a normal system operation (no anomaly) due to e.g., heavy-tailed random noise processes. On the other hand, if a system produces persistent outliers, then this may indicate an actual anomaly. Hence, we define an anomaly as persistent outliers and from the observed data stream, we propose to accumulate statistical evidence for anomaly over time, similarly to the accumulation of log-likelihood ratios (LLRs) in the well-known cumulative sum (CUSUM) algorithm for change detection [Sec. 2.2] [5]. With the goal of making a reliable decision, we declare an anomaly only if we have a strong evidence for that. The sequential decision making based on the accumulated evidence also enables the detection of small but persistent changes, that would be missed by outlier detectors.

B. Related Work

Batch algorithms are widely encountered in the anomaly detection literature [1], [2], that require the entire data before processing. Clearly, such techniques are not suitable in the online settings. For instance, in [12], [13], via the principal component analysis (PCA), the data are decomposed into normal and anomalous components and the data points with large anomalous components are classified as anomalous. The well-known nonparametric statistical tests such as the Kolmogrov-Smirnov test, the Wilcoxon signed-rank test, and the Pearson's chi-squared test are also mainly designed for batch processing. Although several sliding window-based versions of them have been proposed for online anomaly detection, see e.g., [14], [15], the window-based approach has an inherent detection latency caused by the window size. More importantly, such tests are primarily designed for univariate data, with no direct extensions for multivariate data.

Various online anomaly detection techniques for multivariate data streams have also been proposed in the literature. The SVM-based one-class classification algorithms in [16], [17] determine a decision region for nominal data after mapping the data onto a kernel space, where there is no clear control mechanism on the false alarm rate. Moreover, the choice and complexity of computing the kernel functions are among the disadvantages of such algorithms. A similar algorithm is presented in [18] where the training data might contain a small number of anomalous data points or outliers. An extension of the one-class SVM algorithm [16] is proposed in [19] where the objective is to detect anomalies in the presence of multiple classes. Furthermore, in [6], [7], [20], NN graph-based anomaly detection schemes are proposed with sample-by-sample decisions. As discussed earlier, the sequential decision making is more effective and reliable compared to the sample-by-sample decisions. In [21], an online sliding window-based detector is proposed based on NN graphs, where after each observation, a new NN graph needs to be formed, that is prohibitive in terms of computational complexity for real-time processing. In [22]–[24], two-sample tests are proposed to evaluate whether two datasets have the same distribution, where the test statistics are the distance between the means of the two samples mapped into a kernel space in [22] and the relative entropy, i.e., the Kullback-Leibler (KL) divergence, between the two samples in [23], [24]. Such approaches mainly suffer from low time resolution since they need large sample sizes for reliable decisions. More recently, in [25], a new interpretation of the CUSUM algorithm based on the discrepancy theory and the GEM method ~~are~~ presented to detect anomalies in real-time, where the proposed detector asymptotically achieves the CUSUM algorithm under certain conditions.

C. Contributions

In this paper, we propose real-time nonparametric anomaly detection schemes for high-dimensional data streams. We list our main contributions as follows:

- We propose to extract easy-to-compute univariate summary statistics from the observed high-dimensional data streams, where the summary statistics are useful to distinguish anomalous data from nominal data. We do not impose any restrictive model assumptions for both the observed high-dimensional data stream and the extracted summary statistics. Hence, the proposed schemes are completely nonparametric.
- We propose a low-complexity CUSUM-like real-time anomaly detection algorithm that makes use of the summary statistics.
- We provide an asymptotic lower bound on the average false alarm period of the proposed algorithm, where the bound can be controlled by choosing the significance level for outliers and the decision threshold of the proposed algorithm.
- We provide a sufficient condition to (asymptotically) prevent false alarms due to divergence of the decision statistic of the proposed algorithm in the absence of anomalies.

D. Organization

The remainder of the paper is organized as follows. We present the problem description and our solution approach in Sec. II, derivations of the univariate summary statistics in Sec. III, and the proposed real-time anomaly detection schemes in Sec. IV. We then evaluate the proposed schemes in different application settings via simulations in Sec. V. Finally, Sec. VI concludes the paper. Throughout the paper, boldface letters denote vectors and matrices, all vectors are column vectors, and $\cdot^{\mathrm{T}}$ denotes the transpose operator.

II. Problem Description and Solution Approach

A. Problem Description

Suppose that we monitor a system that produces a high-dimensional stationary data stream, where at each time t we observe a new data point $\mathbf{x}_t \in \mathbb{R}^p$ where $p \gg 1$ is the dimensionality of the original data space, also called the ambient dimension, and the data points are independent and identically distributed (i.i.d.) over time. Suppose that an abrupt anomaly, e.g., an unfriendly intervention (attack/intrusion) or an unexpected failure, happens at an unknown time τ, called the change-point, and continues thereafter. That is, the system is under normal operating conditions up to time τ and the system's underlying statistical properties suddenly change at τ due to an anomaly. Denoting the pdfs of $\mathbf{x}_t$ under normal (pre-change) and anomalous (post-change) conditions as $f_0^{\mathbf{x}}$ and $f_1^{\mathbf{x}} \neq f_0^{\mathbf{x}}$, respectively, we have

$$\mathbf{x}_t \sim \begin{cases} f_0^{\mathbf{x}}, & \text{if } t < \tau \\ f_1^{\mathbf{x}}, & \text{if } t \geq \tau. \end{cases}$$

Our goal is to detect changes (anomalies) with minimal possible delays and also with minimal rates of false alarm for a secure and reliable operation of the observed system. In other words, we aim to detect the changes as quickly as possible after they occur. The framework of quickest detection well matches with this purpose. A well-known problem formulation in the quickest detection framework is the minimax problem proposed by Lorden [26]. In the minimax problem, the goal is to minimize the worst-case detection delay subject to false alarm constraints. More specifically, let Γ denote the stopping time at which a change is declared and $\mathbb{E}_\tau$ denote the expectation measure if the change happens at time τ. The Lorden's worst-case average detection delay is given by

$$J(\Gamma) \triangleq \sup_{\tau} \operatorname*{ess\,sup}_{\mathcal{F}_\tau} \mathbb{E}_\tau\left[(\Gamma-\tau)^+ \,|\mathcal{F}_\tau\,\right],$$

where $(\cdot)^+ = \max\{0,\cdot\}$ and $\mathcal{F}_\tau$ is the history of observations up to the change-point τ. $J(\Gamma)$ is called the worst-case delay since it is computed based on the least favorable change-point and the least favorable history of observations up to the change-point. The minimax problem can then be written as follows:

$$\inf_{\Gamma} \; J(\Gamma) \quad \text{subject to} \quad \mathbb{E}_\infty[\Gamma] \geq \beta, \tag{1}$$

where $\mathbb{E}_\infty[\Gamma]$ is the average false alarm period, i.e., the average stopping time when no change occurs at all ($\tau = \infty$), and β is the desired lower bound on the average false alarm period.

If both $f_0^{\mathbf{x}}$ and $f_1^{\mathbf{x}}$ are known, then the well-known CUSUM algorithm is the optimal solution to the minimax problem given in (1) [27]. Let

$$\ell_t \triangleq \log\left(\frac{f_1^{\mathbf{x}}(\mathbf{x}_t)}{f_0^{\mathbf{x}}(\mathbf{x}_t)}\right)$$

denote the LLR at time t. In the CUSUM algorithm, the LLR is considered as a statistical evidence for change and the LLRs are accumulated over time. If the accumulated evidence exceeds a predefined threshold, then a change is declared. Denoting the CUSUM decision statistic at time t by g_t and the decision threshold by h, the CUSUM algorithm is given by

$$\begin{aligned}\Gamma &= \inf\{t : g_t \geq h\},\\ g_t &= \max\{0, g_{t-1} + \ell_t\},\end{aligned} \tag{2}$$

where $g_0 = 0$.

Since it is practically difficult to model all types of anomalies, $f_1^{\mathbf{x}}$ needs to be assumed unknown for a general anomaly detection problem. In that case, if only $f_0^{\mathbf{x}}$ is known and also has a parametric form, slight deviations from the parameters of $f_0^{\mathbf{x}}$ can be detected using a generalized CUSUM algorithm [5, Sec. 5.3], [15], [28]. However, in a general high-dimensional problem, it might be difficult to model or estimate the high-dimensional multivariate nominal pdf $f_0^{\mathbf{x}}$. Hence, in this study, we assume that both $f_0^{\mathbf{x}}$ and $f_1^{\mathbf{x}}$ are unknown. We propose to use an alternative technique in that we extract useful univariate summary statistics from the observed high-dimensional data stream and perform the anomaly detection task in a single-dimensional space based on the extracted summary statistics, as detailed below.

B. Proposed Solution Approach

Firstly, we assume that there is an available set of nominal data points $\mathcal{X} \triangleq \{\mathbf{x}_i : i = 1, 2, \ldots, N\}$, that are free of anomaly. Practically, this is, in general, possible since the monitored system produces a data point at each sampling instant and a set of nominal data points can be obtained under normal system operation (no anomaly). Using $\mathcal{X}$, we aim to extract univariate baseline statistics that summarize the normal system operation such that the summary statistics corresponding to anomalous data deviate from the baseline statistics. To this end, summary statistics should be well informative to distinguish anomalous conditions from the normal operating conditions.

Let the summary statistic corresponding to $\mathbf{x}_t$ be denoted by d_t. Since the statistical properties of $\mathbf{x}_t$ changes at time τ, we assume that the statistical properties of d_t also changes at τ. Denoting the nominal and anomalous pdfs of d_t as f_0^d and $f_1^d \neq f_0^d$, respectively, we then have

$$d_t \sim \begin{cases} f_0^d, & \text{if } t < \tau \\ f_1^d, & \text{if } t \geq \tau, \end{cases}$$

where we assume that f_0^d and f_1^d are both unknown. Nonetheless, extracting a set of nominal summary statistics from $\mathcal{X}$ and using this set as i.i.d. realizations of the nominal pdf f_0^d, we can form an empirical distribution function (edf) of the nominal summary statistics that estimates the nominal cumulative distribution function (cdf) F_0^d of d_t. Then, based on the nominal edf of the summary statistics, for an incoming data point $\mathbf{x}_t$ at time t and its corresponding summary statistic d_t, we can estimate the corresponding tail probability (p-value), denoted with p_t. In statistical outlier detection, a data point $\mathbf{x}_t$ is considered as an outlier with respect to the level of α if its p-value is less than α, i.e., $p_t < \alpha$. Let

$$s_t \triangleq \log\left(\frac{\alpha}{p_t}\right). \tag{3}$$

Then, for an outlier $\mathbf{x}_t$, we have $s_t > 0$ and similarly, for a non-outlier $\mathbf{x}_t$, we have $s_t \leq 0$.

Under normal system operation, we may observe random non-persistent outliers due to e.g., high-level random system noise. However, if a system produces persistent outliers, then this may indicate an actual anomaly. Hence, we can model anomalies as persistent outliers. Considering s_t in (3) as a positive/negative statistical evidence for anomaly at time t, we can accumulate s_t's over time and obtain an accumulated evidence for anomaly. We can then declare an anomaly only if we have a strong (reliable) evidence supporting an anomaly. This gives rise to the following CUSUM-like anomaly detection algorithm where we replace the LLR ℓ_t in the CUSUM algorithm (see (2)) with s_t:

$$\begin{aligned} \Gamma &= \inf\{t : g_t \geq h\}, \\ g_t &= \max\{0, g_{t-1} + s_t\}, \end{aligned} \tag{4}$$

where $g_0 = 0$.

In the following section, we present derivations of the proposed summary statistics. Then, in Sec. IV, we explain the estimation of the tail probability p_t (and hence s_t) based on the nominal summary statistics, that results in the final proposed detection algorithm.

III. Summary Statistics

In this section, we firstly explain our methodology to derive summary statistics for a general high-dimensional data stream. We then explain the derivation of summary statistics in a specific case where the data exhibits a low intrinsic dimensionality.

A. GEM-based Summary Statistics

Given a set of nominal data points $\mathcal{X}$ and a chosen significance level of α, the GEM method [6] determines an acceptance region $\mathcal{A}$ for the nominal data based on the asymptotic theory of random Euclidean graphs such that if a data point falls outside $\mathcal{A}$, it is considered as an outlier with respect to the level α, otherwise considered as a non-outlier. The GEM method is based on the NN statistics that capture the local interactions between data points governed by the underlying statistical properties of the observed data stream.

A computationally efficient GEM method presented in [7] is based on bipartite kNN graphs (BP-GEM). In this method, firstly $\mathcal{X}$ is uniformly randomly partitioned into two subsets $\mathcal{S}_1$ and $\mathcal{S}_2$ with sizes N_1 and $N_2 = N - N_1$, respectively. Then, for each data point $\mathbf{x}_j \in \mathcal{S}_2$, the kNNs of $\mathbf{x}_j$ among the set $\mathcal{S}_1$ are determined. Denoting the Euclidean distance of $\mathbf{x}_j$ to its ith NN in $\mathcal{S}_1$ by $e_j(i)$, the sum of distances of $\mathbf{x}_j$ to its kNNs can be written as follows:

$$d_j \triangleq \sum_{i=1}^{k} e_j(i). \tag{5}$$

After computing $\{d_j : \mathbf{x}_j \in \mathcal{S}_2\}$, d_j's are sorted in ascending order and the $(1-\alpha)$ fraction of $\mathbf{x}_j$'s in $\mathcal{S}_2$ corresponding to the smallest $(1-\alpha)$ fraction of d_j's form the acceptance region $\mathcal{A}$. Then, for a new data point $\mathbf{x}_t$, if its sum of distances to its kNNs among $\mathcal{S}_1$, denoted with d_t, is greater than the smallest $(1-\alpha)$ fraction of d_j's, i.e.,

$$\frac{\sum_{\mathbf{x}_j \in \mathcal{S}_2} \mathbb{1}\{d_t > d_j\}}{N_2} > 1 - \alpha,$$

then $\mathbf{x}_t$ is considered as an outlier with respect to the level of α, where $\mathbb{1}\{\cdot\}$ is an indicator function.

Let $\delta(\cdot)$ be the Lebesgue measure in $\mathbb{R}^p$. As $k/N_1 \to 0$ and $k, N_2 \to \infty$, the acceptance region $\mathcal{A}$ determined by the BP-GEM method almost surely converges to the minimum volume set of level α [7], given by

$$\Lambda_\alpha \triangleq \min \left\{ \delta(\mathcal{A}) : \int_{\mathbf{z} \in \mathcal{A}} f_0^{\mathbf{x}}(\mathbf{z}) d\mathbf{z} \geq 1 - \alpha \right\},$$

where $\delta(\mathcal{A})$ denotes the volume of $\mathcal{A}$. Moreover, if $f_0^{\mathbf{x}}$ is a Lebesgue density, the minimum volume set and the minimum Rényi entropy set are equivalent [7]. Hence, the BP-GEM method asymptotically achieves the minimum entropy set, i.e., the most compact acceptance region for the nominal data.

If $\mathbf{x}_t$ is an outlier, then it falls outside the acceptance region $\mathcal{A}$, i.e., the corresponding NN statistic d_t takes a higher value compared to non-outliers. Moreover, if the observed data stream persistently fall outside the acceptance region, or equivalently if we persistently observe high NN statistics over time, then this may indicate an anomaly. Hence, we can use the GEM-based NN statistic as a summary statistic to distinguish anomalous data from nominal data. Moreover, we can use $\{d_j : \mathbf{x}_j \in \mathcal{S}_2\}$ as a set of GEM-based nominal summary statistics.

A salient feature of extracting summary statistics based on the BP-GEM method is that with the incoming data points in an online setting, there is no need to recompute the NN graph for the entire dataset. This is because for each data point, either newly acquired or belonging to the set $\mathcal{S}_2$, the NNs are always searched among the time-invariant set $\mathcal{S}_1$. Hence, obtaining new data does not alter the NNs of the points in $\mathcal{S}_2$. In the online phase, the main computational complexity is then searching the NNs of incoming data points among the set $\mathcal{S}_1$. To further reduce the complexity, fast NN search algorithms can be employed to approximately determine the NNs, see e.g., [29].

Finally, since we capture local interactions between data points via their kNNs, k should not be chosen too large. On the other hand, since the set $\mathcal{S}_1$ might contain some outliers, an incoming data point might fall geometrically close to a few of such outliers. Then, k should not be chosen too small in order to reduce the risk of evaluating an outlier or anomalous data point as a non-outlier. Therefore, a moderate k value might best fit to our purpose of extracting useful GEM-based summary statistics for anomaly detection.

B. Summary Statistics for High-Dimensional Data Exhibiting Low Intrinsic Dimensionality

In many practical applications, observed high-dimensional data exhibits a sparse structure so that the intrinsic dimensionality of the data is lower than the ambient dimension, and hence the data can be well represented in a lower-dimensional subspace. In such cases, we can model the data as follows:

$$\mathbf{x}_t = \mathbf{y}_t + \mathbf{r}_t, \tag{6}$$

where $\mathbf{y}_t$ is the representation of $\mathbf{x}_t$ in a submanifold and $\mathbf{r}_t$ is the residual term, i.e., the departure of $\mathbf{x}_t$ from the submanifold, mostly consisting of noise.

Suppose that we learn a submanifold that the nominal data are embedded in. Since the learned manifold is mainly representative for the nominal data, anomalous data points are expected to deviate from the nominal submanifold and hence the magnitude of the residual term, i.e., $\|\mathbf{r}_t\|_2$, is expected to take higher values for anomalous data compared to nominal data. Hence, the magnitude of the residual term can be used as a summary statistic to distinguish anomalous data. Given a nominal dataset $\mathcal{X}$, let $\mathcal{S}_1$ and $\mathcal{S}_2$ be two subsets of $\mathcal{X}$, i.e., $\mathcal{S}_1, \mathcal{S}_2 \subset \mathcal{X}$, with sizes N_1 and N_2, respectively, where $N_1, N_2 \leq N$. Firstly, using $\mathcal{S}_1$, we can determine a representative submanifold that the nominal data are embedded in. Then, using $\mathcal{S}_2$, we can compute the magnitude of the residual terms, i.e., $\{\|\mathbf{r}_j\|_2 : \mathbf{x}_j \in \mathcal{S}_2\}$, that can be used as a set of nominal summary statistics.

There are various methods to determine the underlying submanifold of the observed high-dimensional data streams, among which the PCA is a well known method for finding a linear submanifold, called the principal subspace [30, Sec. 12.1]. Next, we explain the PCA and the PCA-based summary statistics.

The PCA is a nonparametric linear submanifold learning technique as it is computed directly from a given dataset without requiring any data model. Given a set of nominal data points $\mathcal{S}_1$, the PCA provides a linear subspace with dimensionality $r \leq p$ such that (i) the variance of the projected data onto the r-dimensional subspace is maximized and (ii) the sum of squares of the projection errors (residual magnitudes) is minimized [30, Sec. 12.1].

In the PCA method, denoting $\bar{\mathbf{x}}$ as the sample mean, i.e.,

$$\bar{\mathbf{x}} \triangleq \frac{1}{N_1} \sum_{\mathbf{x}_i \in \mathcal{S}_1} \mathbf{x}_i \tag{7}$$

and $\mathbf{Q}$ as the sample data covariance matrix, i.e.,

$$\mathbf{Q} \triangleq \frac{1}{N_1} \sum_{\mathbf{x}_i \in \mathcal{S}_1} (\mathbf{x}_i - \bar{\mathbf{x}})(\mathbf{x}_i - \bar{\mathbf{x}})^{\mathrm{T}}, \tag{8}$$

firstly, the eigenvalues $\{\lambda_j : j = 1, 2, \ldots, p\}$ and the eigenvectors $\{\mathbf{v}_j : j = 1, 2, \ldots, p\}$ of $\mathbf{Q}$ are computed, where

$$\mathbf{Q}\,\mathbf{v}_j = \lambda_j \mathbf{v}_j, \quad j = 1, 2, \ldots, p.$$

Then, the dimensionality of the submanifold, r, can be determined based on the desired fraction of data variance retained in the submanifold, given by

$$\gamma \triangleq \frac{\sum_{j=1}^{r} \lambda_j}{\sum_{j=1}^{p} \lambda_j} \leq 1, \tag{9}$$

where the r-dimensional principal subspace is spanned by the orthonormal eigenvectors $\mathbf{v}_1$, $\mathbf{v}_2$, …, $\mathbf{v}_r$ corresponding to the r largest eigenvalues λ_1, λ_2, …, λ_r of $\mathbf{Q}$. Let $\mathbf{V} \triangleq [\mathbf{v}_1, \mathbf{v}_2, \ldots \mathbf{v}_r]$. The representation of $\mathbf{x}_t$ in the linear submanifold can then be determined as follows:

$$\begin{aligned} \mathbf{y}_t &= \bar{\mathbf{x}} + \sum_{j=1}^{r} \mathbf{v}_j \mathbf{v}_j^{\mathrm{T}} (\mathbf{x}_t - \bar{\mathbf{x}}) \\ &= \bar{\mathbf{x}} + \mathbf{V}\mathbf{V}^{\mathrm{T}} (\mathbf{x}_t - \bar{\mathbf{x}}). \end{aligned} \tag{10}$$

Then, the residual term can be computed as

$$\begin{aligned} \mathbf{r}_t &= \mathbf{x}_t - \mathbf{y}_t \\ &= (\mathbf{I}_p - \mathbf{V}\mathbf{V}^{\mathrm{T}})(\mathbf{x}_t - \bar{\mathbf{x}}), \end{aligned} \tag{11}$$

where $\mathbf{I}_p \in \mathbb{R}^{p \times p}$ is an identity matrix.

To obtain the PCA-based nominal summary statistics, firstly, using $\mathcal{S}_1$, we can compute $\mathbf{Q}$ based on (8), and then its eigenvalues and eigenvectors. Then, for a chosen γ (see (9)), we can determine r and the corresponding $\mathbf{V}$. Finally, using $\mathcal{S}_2$ and (11), we can compute $\{\|\mathbf{r}_j\|_2 : \mathbf{x}_j \in \mathcal{S}_2\}$, that forms a set of nominal PCA-based summary statistics.

Note that although here we have only focused on the PCA and the linear submanifolds, using the same data model in (6) and following a similar methodology, summary statistics can be extracted for any (possibly nonlinear) manifold learning algorithm as long as it is appropriate for the observed high-dimensional data stream and it allows for efficient computation of the residual terms $\mathbf{r}_t$ (see (6)) both for a given nominal dataset and also for the sequentially acquired out-of-sample data, without re-running the manifold learning algorithm.

IV. Real-Time Nonparametric Anomaly Detection

A. Proposed Algorithm

We firstly discuss the statistical outlier detection based on a set of nominal summary statistics. Notice that for outliers, both of the proposed summary statistics, d_t and $\|\mathbf{r}_t\|_2$, take higher values compared to non-outliers (see Sec. III). Hence, outliers in fact correspond to the right tail events based on the nominal pdf of the summary statistics. Let us specifically consider d_t. In case the knowledge of the nominal pdf of d_t, i.e., f_0^d, is available, we would compute the corresponding right tail probability as follows:

$$p_t = \int_{d_t}^{\infty} f_0^d(z) dz = 1 - F_0^d(d_t), \tag{12}$$

where F_0^d is the cdf of d_t. If $p_t < \alpha$, we can then consider d_t (correspondingly $\mathbf{x}_t$) as an outlier with respect to the significance level α.

In our problem, although we do not have the knowledge of f_0^d (and F_0^d), using a set of i.i.d. realizations of the nominal summary statistics, we can obtain an edf that estimates F_0^d. Let $\{d_j : \mathbf{x}_j \in \mathcal{S}_2\}$ be the set of nominal summary statistics. Then, the corresponding edf is given by

$$\hat{F}_{0,N_2}^d(z) \triangleq \frac{1}{N_2} \sum_{\mathbf{x}_j \in \mathcal{S}_2} \mathbb{1}\{d_j \leq z\}. \tag{13}$$

Moreover, by the Glivenko-Cantelli theorem, $\hat{F}_{0,N_2}^d$ pointwise almost surely converges to the actual cdf F_0^d as $N_2 \to \infty$ [31]. Then, we can estimate p_t based on $\hat{F}_{0,N_2}^d$ as follows:

$$\begin{aligned} \hat{p}_t &= 1 - \hat{F}_{0,N_2}^d(d_t) \\ &= \frac{1}{N_2} \sum_{\mathbf{x}_j \in \mathcal{S}_2} \mathbb{1}\{d_j > d_t\}. \end{aligned} \tag{14}$$

That is, $\hat{p}_t$ is simply the fraction of the nominal summary statistics $\{d_j : \mathbf{x}_j \in S_2\}$ greater than d_t. If $\hat{p}_t < \alpha$, then we can consider $\mathbf{x}_t$ as an outlier with respect to the level of α.

Let

$$\hat{s}_t \triangleq \log\left(\frac{\alpha}{\hat{p}_t}\right). \tag{15}$$

Notice that for an outlier $\mathbf{x}_t$ with respect to a level of α, we have $\hat{s}_t > 0$ and similarly, for a non-outlier $\mathbf{x}_t$, we have $\hat{s}_t \leq 0$. Then, by replacing $\hat{s}_t$ with s_t in (4), we propose the following model-free CUSUM-like anomaly detection algorithm:

$$\begin{aligned} \Gamma &= \inf\{t : g_t \geq h\}, \\ g_t &= \max\{0, g_{t-1} + \hat{s}_t\}, \end{aligned} \tag{16}$$

Algorithm 1 GEM-based Real-time Nonparametric Anomaly Detection

```
Offline Phase
Uniformly randomly partition the nominal dataset $\mathcal{X}$ into two subsets $\mathcal{S}_1$ and $\mathcal{S}_2$ with sizes $N_1$ and $N_2$, respectively.
for $j : \mathbf{x}_j \in \mathcal{S}_2$ do
    Search for the $k$NNs of $\mathbf{x}_j$ among the set $\mathcal{S}_1$.
    Compute $d_j$ using (5).
end for
Online Detection Phase
Initialization: $t \leftarrow 0$, $g_0 \leftarrow 0$.
while $g_t < h$ do
    $t \leftarrow t + 1$.
    Obtain the new data point $\mathbf{x}_t$.
    Search for the $k$NNs of $\mathbf{x}_t$ among the set $\mathcal{S}_1$ and compute $d_t$ using (5).
    $\hat{p}_t = \frac{1}{N_2} \sum_{\mathbf{x}_j \in \mathcal{S}_2} \mathbb{1}\{d_j > d_t\}$.
    $\hat{s}_t = \log(\alpha / \hat{p}_t)$.
    $g_t \leftarrow \max\{0, g_{t-1} + \hat{s}_t\}$.
end while
Declare an anomaly and stop the procedure.
```

Algorithm 2 PCA-based Real-time Nonparametric Anomaly Detection

```
Offline Phase
Choose subsets $\mathcal{S}_1$ and $\mathcal{S}_2$ of $\mathcal{X}$ with sizes $N_1$ and $N_2$, respectively.
Compute $\bar{\mathbf{x}}$ and $\mathbf{Q}$ over $\mathcal{S}_1$ using (7) and (8), respectively.
Compute the eigenvalues $\{\lambda_j : j = 1, 2, \ldots, p\}$ and the eigenvectors $\{\mathbf{v}_j : j = 1, 2, \ldots, p\}$ of $\mathbf{Q}$.
Based on a desired level of $\gamma$ (see (9)), determine $r$ and form the matrix $\mathbf{V} = [\mathbf{v}_1, \mathbf{v}_2, \ldots \mathbf{v}_r]$.
for $j : \mathbf{x}_j \in \mathcal{S}_2$ do
    $\mathbf{r}_j = (\mathbf{I}_p - \mathbf{V}\mathbf{V}^{\mathrm{T}})(\mathbf{x}_j - \bar{\mathbf{x}})$.
    Compute $\|\mathbf{r}_j\|_2$.
end for
Online Detection Phase
Initialization: $t \leftarrow 0$, $g_0 \leftarrow 0$.
while $g_t < h$ do
    $t \leftarrow t + 1$.
    Obtain the new data point $\mathbf{x}_t$.
    $\mathbf{r}_t = (\mathbf{I}_p - \mathbf{V}\mathbf{V}^{\mathrm{T}})(\mathbf{x}_t - \bar{\mathbf{x}})$ and compute $\|\mathbf{r}_t\|_2$.
    $\hat{p}_t = \frac{1}{N_2} \sum_{\mathbf{x}_j \in \mathcal{S}_2} \mathbb{1}\{\|\mathbf{r}_j\|_2 > \|\mathbf{r}_t\|_2\}$.
    $\hat{s}_t = \log(\alpha / \hat{p}_t)$.
    $g_t \leftarrow \max\{0, g_{t-1} + \hat{s}_t\}$.
end while
Declare an anomaly and stop the procedure.
```

where $g_0 = 0$[1]. Since we model anomalies as persistent outliers, the decision statistic g_t has a positive drift in case of an anomaly and a non-positive drift in the absence of anomalies.

We summarize the proposed GEM-based and PCA-based detection schemes in Algorithms 1 and 2, respectively. Moreover, we present a diagram of the proposed schemes in Fig. 1. The proposed schemes consist of an offline phase for extracting the baseline statistics for a given set of nominal data points and an online phase for anomaly detection. The offline phases are explained in Sec. III. In the online phase, at each time t, a new data point $\mathbf{x}_t$ is observed and using the baseline statistics, the summary statistic corresponding to $\mathbf{x}_t$ is computed and then the tail probability $\hat{p}_t$ and the statistical evidence $\hat{s}_t$ are estimated. The decision statistic g_t is then updated and if it exceeds the predetermined decision threshold h, an anomaly is declared,

[1] In case where $\sum_{\mathbf{x}_j \in \mathcal{S}_2} \mathbb{1}\{d_j > d_t\} = 0$, we have $\hat{p}_t = 0$ (see (14)), and hence $g_t = \infty$. In this case, a small nonzero value, e.g., $1/N_2$, can be assigned to $\hat{p}_t$ in order to prevent the decision statistic to raise to infinity due to a single outlier. This modification can be useful to reduce the false alarm rate especially in the small-sample settings (small N_2).

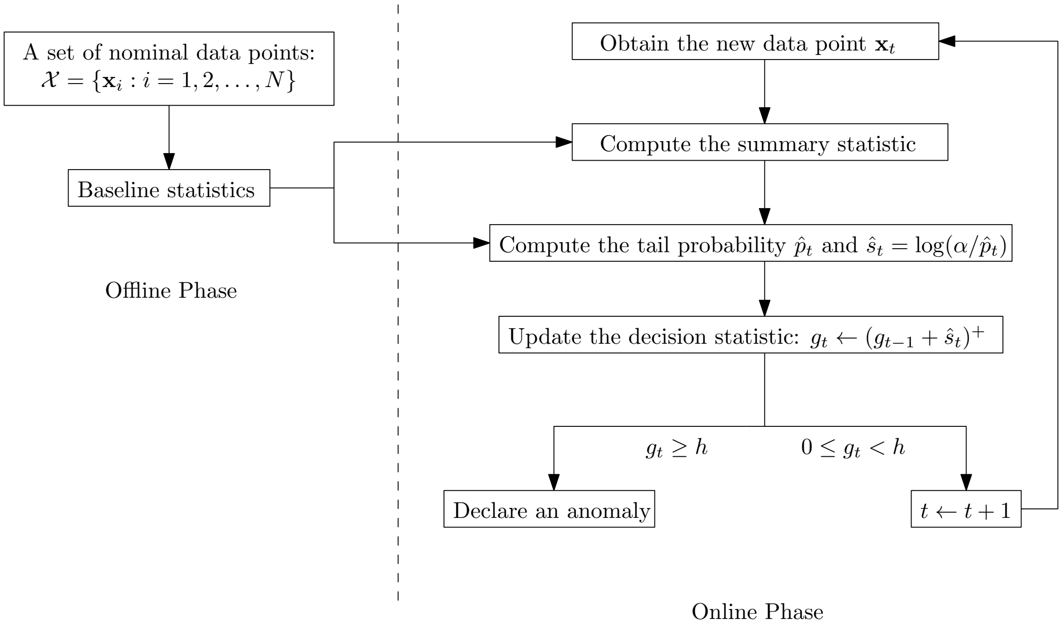
A set of nominal data points: $\mathcal{X} = \{\mathbf{x}_i : i = 1, 2, \dots, N\}$
Baseline statistics
Offline Phase
Obtain the new data point $\mathbf{x}_t$
Compute the summary statistic
Compute the tail probability $\hat{p}_t$ and $\hat{s}_t = \log(\alpha/\hat{p}_t)$
Update the decision statistic: $g_t \leftarrow (g_{t-1} + \hat{s}_t)^+$
$g_t \geq h$
$0 \leq g_t < h$
Declare an anomaly
$t \leftarrow t + 1$
Online Phase

Fig. 1: Diagram of the proposed detection schemes.

otherwise the algorithm proceeds to the next time interval and acquires a further observation. Note that the proposed detection mechanism is generic in the sense that after extracting useful summary statistics for nominal data and computing an edf for the nominal summary statistics, the proposed CUSUM-like algorithm in (16) can be employed for real-time anomaly detection.

B. Analysis

During normal system operation (no anomaly), if the decision statistic g_t exceeds the test threshold h, then a false alarm occurs. In anomaly detection, false alarm is an undesired event and for reliability of an anomaly detection scheme, performance guarantees regarding the false alarm rate are often desirable. With this purpose, firstly the following theorem provides an asymptotic upper bound on the level of α such that in the absence of anomalies, the decision statistic g_t (almost surely) does not diverge in the mean squared sense.

Theorem 1: In the absence of anomalies, i.e., for $t < \tau$, if $\alpha < 1/e$, where e denotes the Euler's number, we have as $N_2 \to \infty$,

$$\mathbb{P}\left(\sup_{t \geq 0} \; \mathbb{E}\left[g_t^2 \,|\, g_0 = 0 \right] < \infty \right) = 1,$$

i.e., the decision statistic does not grow unbounded in the mean squared sense, with the probability 1.

Proof. See Appendix A. □

Theorem 1 provides a guidance to choose the level of α. Specifically, α can be chosen smaller than $1/e$ to asymptotically ensure that the decision statistic of the proposed algorithm stays finite over time under normal operating conditions, that eliminates false alarms due to the divergence of the decision statistic.

In the proposed CUSUM-like algorithm given in (16), the decision statistic at time t, i.e., g_t, is determined by $\{\hat{s}_n : n \leq t\}$ where $\hat{s}_n$'s are i.i.d. over time in the absence of anomalies. Hence, we have actually a random walk driven by $\{\hat{s}_n\}$ with lower threshold 0 and upper (decision) threshold h and our aim is to determine the average false alarm period, i.e., the first time, on the average, the upper threshold h is crossed in the no-anomaly case. In the literature, this problem has been considered in several studies and some approximations and bounds are provided for this quantity as the exact computation is analytically intractable [5, Sec. 5.2.2], [32]–[35]. To be able to provide a performance guarantee regarding the false alarm rate, we prefer to derive a lower bound on the average false alarm period based on [5, Sec. 5.2.2.4]. The following theorem provides an asymptotic lower bound on the average false alarm period of the proposed algorithm for chosen values of α and h.

Theorem 2: For chosen $\alpha < 1/e$ and $h > 0$, the average false alarm period of the proposed anomaly detection algorithm, $\mathbb{E}_\infty[\Gamma]$, asymptotically (as $N_2 \to \infty$) achieves the following lower bound:

$$\mathbb{E}_\infty[\Gamma] \geq e^{(1-\theta)h}, \tag{17}$$

where $0 < \theta < 1$ is given by

$$\theta = \frac{W(\alpha \log(\alpha))}{\log(\alpha)}, \tag{18}$$

where $W(c)$ is the Lambert-W function[2] that provides solutions z to the equation

$$z\, e^z = c.$$

Proof. See Appendix B. □

Based on Theorem 2, α and h can be chosen to asymptotically satisfy the minimum acceptable level of the average false alarm period. Specifically, if the desired (asymptotic) minimum average false alarm period is $L > 0$, then

$$\mathbb{E}_\infty[\Gamma] \geq e^{(1-\theta)h} \geq L,$$

which is equivalent to

$$h \geq \frac{\log(L)}{1 - W(\alpha \log(\alpha))/\log(\alpha)},$$

that presents a lower bound on the test threshold h for a chosen level of α. As an example, for $L = 10^6$, Fig. 2 illustrates the lower bound on h for $\alpha < 1/e$.

Note that lower α and/or higher h lead to larger false alarm periods and also larger detection delays. This is because lower α results in lower $\hat{s}_t$ and hence lower g_t, that increases the stopping time Γ (see (15) and (16)). Similarly, higher h results in larger stopping time (see (16)). Hence, α and h are essentially tradeoff parameters that can be used to strike a desired balance between the false alarm rate and the detection delays of the proposed algorithm. However, since the post-change (anomalous) case is totally unknown and no anomalous data is available, it seems difficult to provide theoretical results regarding the average detection delay of the proposed algorithm. Nonetheless, we know that as the discrepancy, e.g., the KL divergence, between the

[2] There is a built-in MATLAB function **lambertw**.

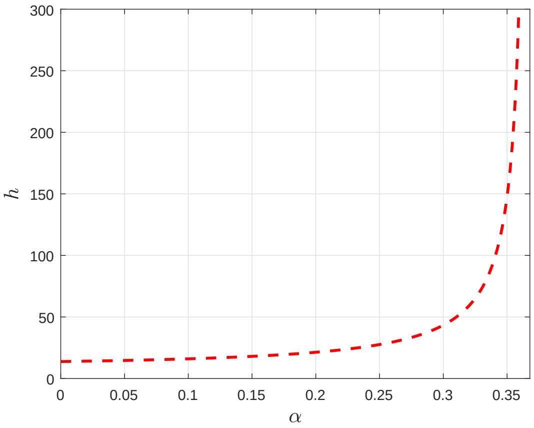

Fig. 2: The lower bound (dashed curve) on the decision threshold h of the proposed algorithm for $\alpha < 1/e$ such that $\mathbb{E}_\infty[\Gamma] \geq 10^6$ as $N_2 \to \infty$.

nominal and anomalous pdfs increases, it is likely to observe more significant outliers after anomaly happens, that increases $\hat{s}_t$ (see (14) and (15)) for $t \geq \tau$, which in turn decreases the detection delays (see (16)).

V. Simulations

In this section, we evaluate the performance of the proposed real-time anomaly detection schemes using both synthetic and real application data. In particular, we evaluate the GEM-based scheme in detection of cyber-attacks targeting the smart grid. Moreover, we evaluate both the GEM-based and the PCA-based schemes in detection of changes in human physical activity and botnet attacks in an IoT network. Throughout the section, we choose $\alpha = 0.1$ and obtain the tradeoff curves between the average detection delay and the average false alarm period by varying the test threshold h. In computing the detection delays, we assume that anomalies happen at $\tau = 1$, that corresponds to the worst-case detection delay for the proposed algorithm since the decision statistic g_t is equal to zero just before the anomalies happen (recall that $g_0 = 0$). In the following, we firstly briefly explain the benchmark algorithms and then present the application setups along with the corresponding performance curves.

A. Benchmark Algorithms

1) Nonparametric CUSUM Test: In cases where the univariate test statistic is expected to take higher values in the post-change case compared to the pre-change case, a nonparametric CUSUM test can be used for change detection, where the difference between the test statistic and its mean value in the pre-change case is accumulated over time and a change is declared if the accumulated statistic exceeds a predetermined threshold. For instance, the chi-squared statistic [32] and the magnitude of the innovation sequence in the Kalman filter [36] are expected to increase in case of an anomaly and several variants of the nonparametric CUSUM detector have been proposed in the context of anomaly/attack detection in the smart grid [32], [36].

In our case, both summary statistics, i.e., d_t and $\|\mathbf{r}_t\|_2$, are expected to increase in case of an anomaly compared to their nominal mean values. Hence, after obtaining a set of nominal summary statistics, we can compute the empirical mean of them and then apply the nonparametric CUSUM test for real-time anomaly detection. Let us specifically consider d_t and let

$$\bar{d} \triangleq \frac{1}{N_2} \sum_{\mathbf{x}_j \in \mathcal{S}_2} d_j$$

denote the empirical nominal mean of d_t. Then, the nonparametric CUSUM test is given by

$$\begin{aligned} \bar{\Gamma} &= \inf\{t : \bar{g}_t \geq \bar{h}\}, \\ \bar{g}_t &= \max\{0, \bar{g}_{t-1} + d_t - \bar{d}\}, \end{aligned}$$

where $\bar{g}_0 = 0$ and $\bar{\Gamma}$, $\bar{g}_t$, and $\bar{h}$ denote the stopping time, the decision statistic at time t, and the test threshold, respectively.

The nonparametric CUSUM test requires storing only the nominal mean of the summary statistics. Hence, in terms of storage cost, it is advantageous compared to our proposed CUSUM-like detection schemes, that make use of the entire set of nominal summary statistics computed in an offline phase. On the other hand, using only the nominal mean statistic reduces the performance of the nonparametric CUSUM test compared to our proposed detectors, as illustrated in the following subsections. In each simulation setup presented below, we firstly compute the empirical mean of the nominal summary statistics (either for d_t or $\|\mathbf{r}_t\|_2$) and then obtain the performance curves for the nonparametric CUSUM test by varying its decision threshold $\bar{h}$.

2) Information Theoretic Multivariate Change Detection (ITMCD) Algorithm: The ITMCD algorithm presented in [23] is a sequential nonparametric change detection algorithm for multivariate data streams. In particular, it is a two sample test based on the KL divergence between the multivariate distributions corresponding to two consecutive (over time) sliding windows of observations. The KL divergence is estimated in a nonparametric way based on the distances of observations to their NNs both within a window and between the windows.

Let $\mathcal{X}_{t,w_1}$ and $\mathcal{X}_{t,w_2}$ denote the most recent consecutive sliding windows of observations at time t with sizes w_1 and w_2, respectively. That is, at time t, we have $\mathcal{X}_{t,w_1} = \{\mathbf{x}_{t-w_1+1}, \dots, \mathbf{x}_t\}$ and $\mathcal{X}_{t,w_2} = \{\mathbf{x}_{t-w_1-w_2+1}, \dots, \mathbf{x}_{t-w_1}\}$. Moreover, let $e_{m,n}(i)$ denote the Euclidean distance between $\mathbf{x}_i \in \mathcal{X}_{t,w_m}$ and its kth NN among the set $\mathcal{X}_{t,w_n}$, where $m, n \in \{1, 2\}$. The KL divergence between the multivariate distributions corresponding to $\mathcal{X}_{t,w_m}$ and $\mathcal{X}_{t,w_n}$ is estimated as follows [23], [37]:

$$\mathrm{KL}_{t,m,n} \triangleq \log\left(\frac{w_n}{w_m - 1}\right) + \frac{p}{w_m} \sum_{\mathbf{x}_i \in \mathcal{X}_{t,w_m}} \log\left(\frac{e_{m,n}(i)}{e_{m,m}(i)}\right),$$

where $\mathbf{x}_t \in \mathbb{R}^p$. The ITMCD algorithm is then given by

$$\tilde{\Gamma} = \inf\{t : \mathrm{KL}_{t,1,2} + \mathrm{KL}_{t,2,1} \geq \tilde{h}\},$$

where $\tilde{\Gamma}$ and $\tilde{h}$ denote the stopping time and the test threshold, respectively.

The ITMCD algorithm is based on the fact that the discrepancy between the multivariate distributions increases in case of a change/anomaly. Particularly, after an anomaly, since the window $\mathcal{X}_{t,w_1}$ includes recently acquired anomalous observations before $\mathcal{X}_{t,w_2}$, the distribution of the observations in $\mathcal{X}_{t,w_1}$ changes while the observations in $\mathcal{X}_{t,w_2}$ still have the nominal distribution for some time period. Then, the KL divergence between the two windows of observations increases compared to the case where the both windows have the same nominal distribution. Note that the ITMCD algorithm requires, after obtaining each new observation, repeating the search for the kth NN for each data point within both its own window and the other window. This is computationally intensive for an online algorithm. Further, the window-based approach reduces the time resolution and induces an inherent detection latency. Throughout the section, for the ITMCD algorithm, we choose $k = 4$ and the window sizes as $w_1 = 20$ and $w_2 = 100$. Moreover. we obtain the corresponding performance curves by varying the test threshold $\tilde{h}$.

B. Real-Time Cyber-Attack Detection in Smart Grid

We consider the IEEE-57 bus power system that consists of 57 buses and 80 smart meters. Let $\boldsymbol{\phi}_t \in \mathbb{R}^{57}$ denote the voltage angles (phases) of the buses and $\mathbf{x}_t \in \mathbb{R}^{80}$ denote the measurement vector collected through the smart meters at time t. Suppose that the smart grid is operating according to the following commonly employed linearized DC model [38]:

$$\mathbf{x}_t = \mathbf{H}\,\boldsymbol{\phi}_t + \boldsymbol{\omega}_t, \tag{19}$$

where $\mathbf{H} \in \mathbb{R}^{80 \times 57}$ is the measurement matrix determined based on the power network topology and $\boldsymbol{\omega}_t \in \mathbb{R}^{80}$ is the measurement noise vector. Moreover, let

$$\boldsymbol{\omega}_t \sim \mathcal{N}(\mathbf{0}_{80}, \sigma^2 \mathbf{I}_{80}), \tag{20}$$

where $\mathbf{0}_{80} \in \mathbb{R}^{80}$ consists of all zeros and σ^2 denotes the noise variance for each measurement. We simulate the DC optimal power flow for case-57 using MATPOWER [39] and obtain the nominal voltage angles $\boldsymbol{\phi}_t$. Since we consider a steady-state, i.e., static, power system model, we expect that the voltage angles stay nearly the same in the absence of anomalies.

Notice that (19) defines the normal system operation. However, in case of an anomaly, e.g., a cyber-attack, the measurement model in (19) no longer holds. For instance, in case of a false data injection (FDI) attack launched at time τ, the measurement vector takes the following form:

$$\mathbf{x}_t = \mathbf{H}\,\boldsymbol{\phi}_t + \mathbf{a}_t + \boldsymbol{\omega}_t, \; t \geq \tau, \tag{21}$$

where $\mathbf{a}_t \triangleq [a_{t,1}, a_{t,2}, \dots, a_{t,80}]^{\mathrm{T}}$ is the injected malicious data at time t. Furthermore, in case of a jamming attack with additive noise, the measurement vector can be written as

$$\mathbf{x}_t = \mathbf{H}\,\boldsymbol{\phi}_t + \boldsymbol{\omega}_t + \mathbf{j}_t, \; t \geq \tau, \tag{22}$$

where $\mathbf{j}_t$ is the jamming noise that corrupts the meter measurements at time t. We aim to detect both FDI and jamming attacks targeting the smart grid.

Based on (19) and (20), we have

$$\mathbf{x}_t \sim \mathcal{N}(\mathbf{H}\,\boldsymbol{\phi}_t, \sigma^2 \mathbf{I}_{80}), \tag{23}$$

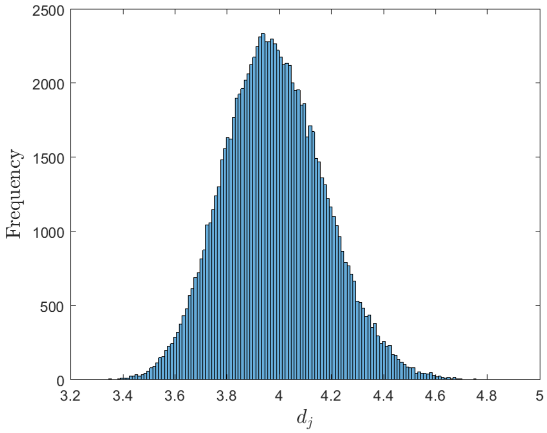

Fig. 3: GEM-based nominal summary statistics for the IEEE-57 bus power system.

i.e., the nominal data covariance matrix is diagonal and every dimension has equal variance. If we collect a set of nominal data points and perform the PCA, we can observe that every dimension is equally important so that the observed high-dimensional nominal data do not exhibit a low intrinsic dimensionality. Nevertheless, we can still use our proposed GEM-based detector (see Algorithm 1).

In this setup, we generate synthetic data based on the system and attack models presented above. Specifically, during the normal system operation given by (23), we assume $\sigma^2 = 10^{-2}$ and acquire $N = 10^5$ nominal data points, and then uniformly partition them into two parts $\mathcal{S}_1$ and $\mathcal{S}_2$ with sizes $N_1 = 2 \times 10^3$ and $N_2 = 9.8 \times 10^4$, respectively. We choose $k = 4$ and for each data point $\mathbf{x}_j \in \mathcal{S}_2$, we compute d_j, the sum of distances of $\mathbf{x}_j$ to its first k NNs among $\mathcal{S}_1$ (see (5)). Then, we obtain the histogram of $\{d_j : \mathbf{x}_j \in \mathcal{S}_2\}$, as given in Fig. 3.

In case of an FDI attack (see (21)), we assume that $a_{t,i} \sim \mathcal{U}[-0.14, 0.14], \forall i \in \{1, 2, \ldots, 80\}, \forall t \geq \tau$ where $\mathcal{U}[\rho_1, \rho_2]$ denotes a uniform random variable that takes values in the range of $[\rho_1, \rho_2]$. We present the corresponding performance curve in Fig. 4. Note that the detection delays critically depend on the attack magnitudes. Specifically, if higher attack magnitudes are used, then detection delays become smaller. Further, to illustrate how the proposed algorithm works, we present a sample path of decision statistics over time in Fig. 5. Here, the FDI attack is launched at $\tau = 200$, and we observe that after the attack is launched, the decision statistic increases and exceeds the test threshold h, illustrated with a red dashed line. Finally, in case of a jamming attack (see (22)), we assume that $\mathbf{j}_t \sim \mathcal{N}(\mathbf{0}_{80}, \frac{\sigma^2}{2}\mathbf{I}_{80}), \forall t \geq \tau$ and present the corresponding performance curve in Fig. 6. In detection of both FDI and jamming attacks, we observe via Fig. 4 and Fig. 6 that the proposed algorithm outperforms the benchmark algorithms.

C. Real-Time Detection of Changes in Human Physical Activity

The Human Activities and Postural Transitions (HAPT) dataset [40] obtained from the UCI Machine Learning Repository [41] contain data for six physical activities: sitting, standing, laying, walking, walking upstairs, and walking downstairs. The first three, i.e., sitting, standing, and laying, are static and the remaining three are dynamic activities. We divide the given dataset into two parts based on the given activity labels such that the first part of the dataset contains data for static activities and the second part contains data for dynamic activities. Our goal is to timely and reliably detect changes from a static to a

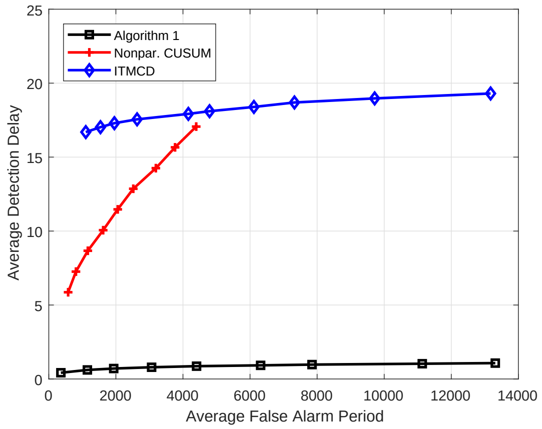

Fig. 4: Average detection delay vs. average false alarm period in detection of an FDI attack against the smart grid.

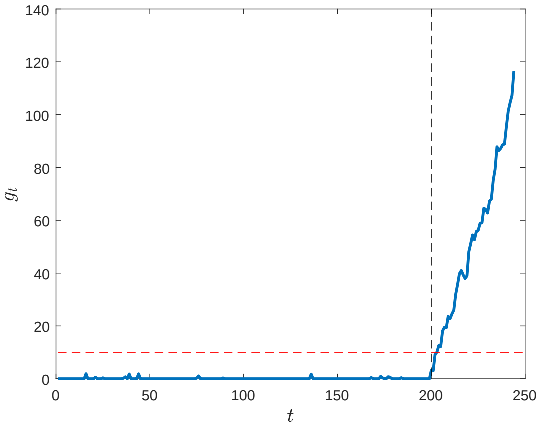

Fig. 5: Sample path of the decision statistic where the FDI attack is launched at $\tau = 200$.

dynamic activity where each data point is 561-dimensional. We hence consider the static activities as the pre-change (nominal) state and the dynamic activities as the post-change (anomalous) state. Although there are finite number of data points in the given dataset, we assume that at each time we sequentially observe a new data point. Particularly, up to the change-point τ, at each time, we observe a data point chosen uniformly among the set of data points corresponding to static activities and after the change-point, at each time, we observe a data point chosen uniformly from the set of dynamic activities.

We firstly uniformly select 2500 data points from the set of data points corresponding to static activities and using the PCA method (see Algorithm 2), we obtain the eigenvalues of the corresponding sample data covariance matrix, as shown in descending order in Fig. 7. We observe through Fig. 7 that the nominal data exhibit a low intrinsic dimensionality. We then choose the minimum desired γ as 0.99. Accordingly, we choose $r = 115$ and retain approximately $\gamma = 0.9903$ fraction of the data variance in the 115-dimensional principal subspace. Then, for the entire set of static activities ($\mathcal{S}_2 = \mathcal{X}$), we compute the PCA-based nominal summary statistics that form the histogram shown in Fig. 8. Fig. 9 illustrates the superior performance of the proposed PCA-based nonparametric detection scheme over the benchmark algorithms in detection of a change from a static to a dynamic activity.

In cases where the observed data stream exhibits a low intrinsic dimensionality, another approach is applying the proposed

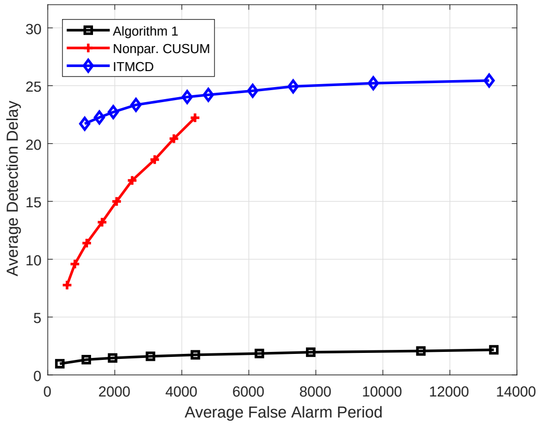

Fig. 6: Average detection delay vs. average false alarm period in detection of a jamming attack against the smart grid.

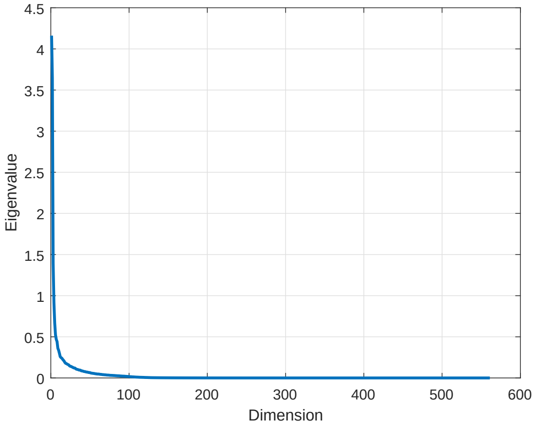

Fig. 7: Eigenvalues of the sample data covariance matrix for a representative set of static activities in the HAPT dataset.

GEM-based detection scheme (Algorithm 1) after dimensionality reduction. That is, after obtaining the matrix $\mathbf{V}$ as described in Algorithm 2, each data point in the nominal training set, $\mathbf{x}_i \in \mathcal{X}$, and also each sequentially available data point, $\mathbf{x}_t$, can be projected onto a r-dimensional space as $\mathbf{V}^{\mathrm{T}}\mathbf{x}_i$ and $\mathbf{V}^{\mathrm{T}}\mathbf{x}_t$, respectively. Algorithm 1 can then be employed over the low-dimensional space, which is computationally more efficient compared to employing Algorithm 1 over the original data space. Fig. 9 illustrates the performance of the proposed GEM-based detection scheme over the projected data, where we obtain the projection matrix $\mathbf{V}$ as described above and uniformly choose $\mathcal{S}_1$ and $\mathcal{S}_2$ (in Algorithm 1) with sizes $N_1 = 1000$ and $N_2 = 4738$, respectively. We use an asterisk for Algorithm 1 to emphasize that it is employed based on the projected low-dimensional data. We observe that Algorithm 1 outperforms the benchmark tests and shows a comparable performance to Algorithm 2.

D. Real-Time Detection of IoT Botnet Attacks

Data for network-based detection of IoT botnet attacks (N-BaIoT) [42] obtained from the UCI Machine Learning Repository [41] contain network traffic statistics for an IoT network under both normal and attack conditions, where the IoT network consists of nine devices, namely a thermostat, a baby monitor, a webcam, two doorbells, and four security cameras and the IoT

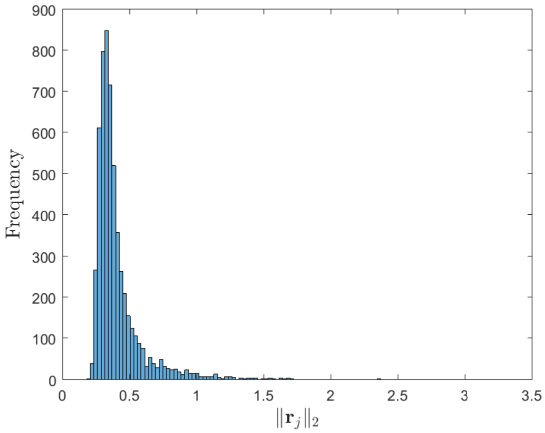

Fig. 8: PCA-based nominal summary statistics for static activities in the HAPT dataset.

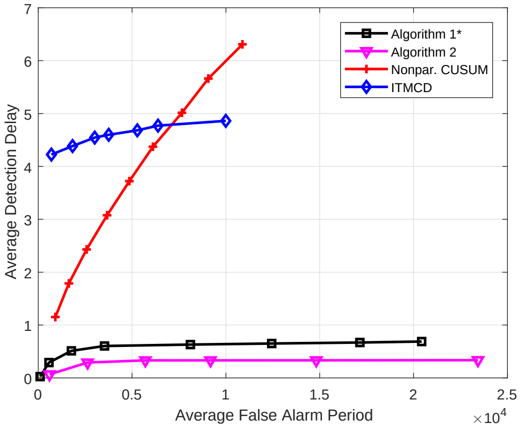

Fig. 9: Average detection delay vs. average false alarm period for detecting changes in human physical activities.

devices are connected via Wi-Fi to several access points. In case of botnet attacks, attackers search for vulnerable devices in the network and inject malwares to the vulnerable devices. Then, they take control of the compromised devices and use them as a part of a bot network (botnet) to perform large-scale attacks such as distributed denial of service (DDoS) attacks over the entire network [42]–[44]. In the N-BaIoT dataset, statistical features such as time intervals between packet arrivals, packet sizes and counts are extracted from the real network traffic for each IoT device such that each data point is 115-dimensional. For each device, the data are obtained under both normal operating conditions and several different attacks performed by BASHLITE and Mirai botnets.

Timely and accurate detection of IoT botnet attacks has a critical importance to prevent further malware propagation over the network, e.g., by disconnecting the compromised devices immediately after the detection. As an illustrative attack case, we consider that the thermostat is compromised by the BASHLITE botnet and the compromised device is used to send spam data to the other devices in the network [42]. Firstly, based on the PCA method summarized in Algorithm 2, 6500 data points chosen uniformly among the nominal dataset are used to compute the sample data covariance matrix, where the corresponding eigenvalues are presented in Fig. 10. We observe that the nominal data can be represented in a lower-dimensional linear subspace and choosing $r = 5$, we retain nearly all the data variance in the 5-dimensional principal subspace, i.e., $\gamma \approx 1$. Then,

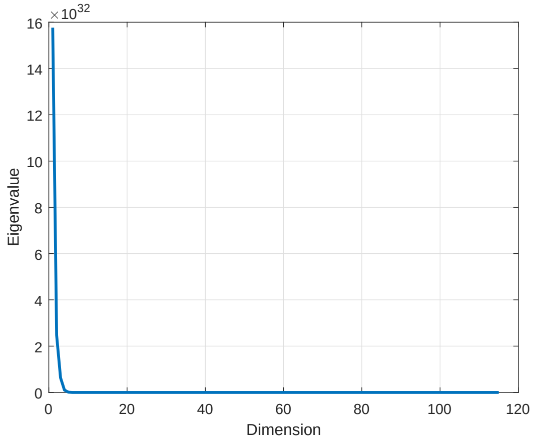

Fig. 10: Eigenvalues of the sample data covariance matrix for a representative set of nominal data points (thermostat) in the N-BaIoT dataset.

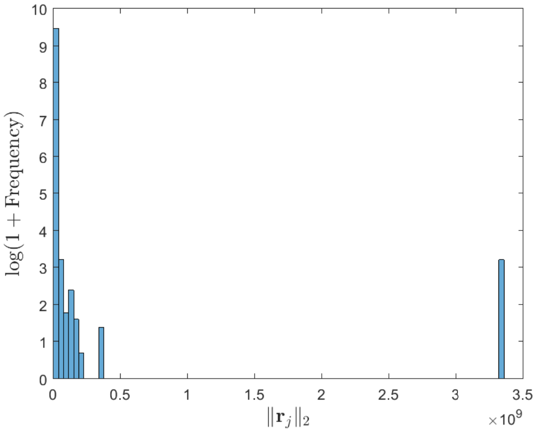

Fig. 11: PCA-based nominal summary statistics for the nominal data (thermostat) in the N-BaIoT dataset.

using the entire nominal dataset, we compute the magnitudes of the residual terms, constituting the nominal summary statistics, a histogram of which is presented in Fig. 11 where the frequencies are shown in the log-scale to have a better illustration.

We assume that before the attack launch time τ, at each time, we observe a nominal data point chosen uniformly among the set of nominal data points and after the attack, at each time, we observe a data point chosen uniformly from the "junk" dataset given for the thermostat [42]. The corresponding performance curve is given in Fig. 12. Similarly to the previous application case, we employ Algorithm 1 using the projected r-dimensional data where we uniformly choose S_1 and S_2 in Algorithm 1 with sizes $N_1 = 1215$ and $N_2 = 11896$, respectively. In this setup, we observe that the nonparametric CUSUM test performs considerably worse compared to the other detectors. This is due to some significant outliers in the nominal dataset. Particularly, we observe through Fig. 11 that the baseline summary statistics mostly lie on an interval of smaller values, i.e., the majority of the nominal data points fit well to the principal subspace. On the other hand, we also observe that for some nominal data points, the summary statistics take significantly high values, that dramatically increase the empirical mean of the nominal summary statistics. This, in turn, leads to higher detection delays for the nonparametric CUSUM test. Moreover, the significant outliers among the nominal data points (with very large $\|\mathbf{r}_t\|_2$) also increase the false alarm rate of the nonparametric CUSUM test.

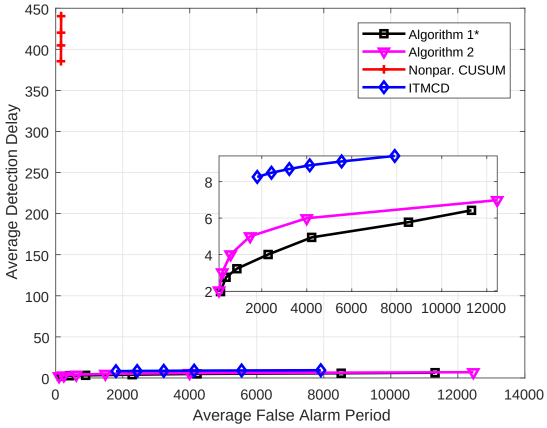

Fig. 12: Average detection delay vs. average false alarm period in detection of a spam attack launched by a BASHLITE botnet.

VI. Conclusions

In this paper, we have proposed nonparametric data-driven real-time anomaly detection schemes. The proposed schemes are reliable, effective, scalable, and hence ideally suited for high-dimensional settings. Moreover, the proposed schemes are widely applicable in a variety of settings as we do not make unrealistic data model assumptions. We have considered both the special case where the observed data stream has a low intrinsic dimensionality and the general case. In both cases, we have proposed to extract and process univariate summary statistics from the observed high-dimensional data streams, where the summary statistics are useful to distinguish anomalous data from nominal data. We have proposed a low-complexity CUSUM-like anomaly detection algorithm based on the extracted summary statistics. We have provided a sufficient condition to asymptotically ensure that the decision statistic of the proposed algorithm does not grow unbounded in the absence of anomalies. We have also provided a controllable asymptotic lower bound on the average false alarm period of the proposed algorithm. Simulations with synthetic and real application data demonstrate the effectiveness of the proposed schemes in timely and accurate detection of anomalies in a variety of high-dimensional settings.

In this study, we have studied stationary (i.i.d.) high-dimensional data streams. However, in practice, the observed data stream might be non-stationary (non-i.i.d.) over time. In such cases, a common approach is assuming a slowly time-varying submanifold underlying the observed data stream [9], [10], [45]. We can extend our results to this case where we can employ a subspace tracking algorithm [46] to dynamically estimate the underlying submanifold and using a (sequentially acquired) nominal dataset, for each nominal data point, we can compute the distance between the data point and its representation in the estimated submanifold, that form a set of nominal summary statistics. Then, in the online anomaly detection phase, the proposed CUSUM-like algorithm can be employed based on the extracted summary statistics to evaluate whether the sequentially available data stream rapidly deviates from the nominal dynamic submanifold. Notice that for this approach to be effective, we still need that the nominal summary statistics (the distance terms) have a stationary distribution over time.

Appendix

A. Proof of Theorem 1

Proof. Firstly, we derive the asymptotic distribution of $\hat{s}_t$ (see (15)) in the absence of anomalies, i.e., for $t < \tau$. By the Glivenko-Cantelli theorem, the edf of the nominal summary statistics, i.e., $\hat{F}^d_{0,N_2}$ given in (13), converges to the cdf F^d_0 as $N_2 \to \infty$ [31]. Hence, $\hat{p}_t$ in (14) converges to p_t in (12) and equivalently $\hat{s}_t$ converges to s_t in (3). The proposed CUSUM-like detector in (16) thus converges to the algorithm in (4). It is well known that the cdf of any continuous random variable is uniformly distributed $\mathcal{U}[0,1]$ [47]. Then, we have

$$p_t = 1 - F^d_0(d_t) \sim \mathcal{U}[0,1].$$

The cdf of $s_t, t < \tau$, denoted with $F^{s_t}_0$, is then given by

$$\begin{aligned} F^{s_t}_0(y) &= \mathbb{P}(s_t \leq y) = \mathbb{P}\left(\log\left(\frac{\alpha}{p_t}\right) \leq y\right) \\ &= \mathbb{P}\left(p_t \geq \frac{\alpha}{e^y}\right) \\ &= \begin{cases} 1 - \frac{\alpha}{e^y}, & \text{if } y > \log(\alpha) \\ 0, & \text{otherwise.} \end{cases} \end{aligned}$$

Moreover, the pdf of $s_t, t < \tau$, denoted with $f^{s_t}_0$, is given as follows:

$$\begin{aligned} f^{s_t}_0(y) &= \frac{\partial F^{s_t}_0(y)}{\partial y} \\ &= \begin{cases} \alpha\, e^{-y}, & \text{if } y > \log(\alpha) \\ 0, & \text{otherwise.} \end{cases} \end{aligned} \tag{24}$$

Then, based on (24), we have $\mathbb{E}[s_t] = 1 + \log(\alpha)$ and $\mathbb{E}[s_t^2] = 1 + (1 + \log(\alpha))^2$.

From (4), we have $g_t = \max\{0, g_{t-1} + s_t\}$, that implies $g_t^2 \leq (g_{t-1} + s_t)^2$. We can then write

$$\begin{aligned} \mathbb{E}[g_t^2 \mid g_{t-1}] &\leq \mathbb{E}[(g_{t-1} + s_t)^2 \mid g_{t-1}] \\ &= g_{t-1}^2 + 2g_{t-1}\mathbb{E}[s_t] + \mathbb{E}[s_t^2] \\ &= g_{t-1}^2 + 2g_{t-1}(1 + \log(\alpha)) + 1 + (1 + \log(\alpha))^2. \end{aligned} \tag{25}$$

Next, we solve the following inequality:

$$g_{t-1}^2 + 2g_{t-1}(1 + \log(\alpha)) + 1 + (1 + \log(\alpha))^2 \leq g_{t-1}^2, \tag{26}$$

which is equivalent to

$$-2g_{t-1}(1 + \log(\alpha)) \geq 1 + (1 + \log(\alpha))^2. \tag{27}$$

Recalling that $g_{t-1} \geq 0$ and since the RHS of (27) is positive, the solution to (27) is given as follows:

$$\alpha < 1/e \text{ and } g_{t-1} \geq \frac{1 + (1 + \log(\alpha))^2}{-2(1 + \log(\alpha))}. \tag{28}$$

Firstly, let $\alpha < 1/e$ and $g_{t-1} \geq f(\alpha)$, where

$$f(\alpha) \triangleq \frac{1 + (1 + \log(\alpha))^2}{-2(1 + \log(\alpha))} > 0.$$

Then, based on (25), (26), and (28), we have

$$\mathbb{E}[g_t^2 \,|\, g_{t-1}] \leq g_{t-1}^2. \tag{29}$$

Moreover, since $g_{t-1} \geq f(\alpha) > 0$, we have

$$g_{t-1} = \max\{0, g_{t-2} + s_{t-1}\} = g_{t-2} + s_{t-1}. \tag{30}$$

Here, we can either have $g_{t-2} < f(\alpha)$ or $g_{t-2} \geq f(\alpha)$. In the case where $g_{t-2} < f(\alpha) < \infty$, since $\mathbb{P}(s_{t-1} < \infty) = 1$ (cf. (24)), we have $\mathbb{P}(g_{t-1} < \infty) = 1$ (cf. (30)). Then, from (29),

$$\mathbb{P}(\mathbb{E}[g_t^2 \,|\, g_{t-1}] < \infty) = 1. \tag{31}$$

Note that

$$\mathbb{E}\left[\mathbb{E}[g_t^2 \,|\, g_{t-1}] \,|\, g_0 = 0\right] = \mathbb{E}[g_t^2 \,|\, g_0 = 0], \tag{32}$$

where in the LHS of (32), the inner expectation is with respect to (wrt) $g_t \,|\, g_{t-1}$ and the outer expectation is wrt $g_{t-1} \,|\, g_0 = 0$. Moreover, in the RHS of (32), the expectation is wrt $g_t \,|\, g_0 = 0$. Then, based on (31) and (32), and since the expectation of a finite variable is also finite, we have

$$\mathbb{P}(\mathbb{E}[g_t^2 \,|\, g_0 = 0] < \infty) = 1. \tag{33}$$

Further, in the case where $g_{t-2} \geq f(\alpha)$, similar to (29), we have

$$\mathbb{E}[g_{t-1}^2 \,|\, g_{t-2}] \leq g_{t-2}^2. \tag{34}$$

Using nested expectations, (29), and (34), we can write

$$\begin{aligned}\mathbb{E}[g_t^2 \,|\, g_{t-2}] &= \mathbb{E}\left[\mathbb{E}[g_t^2 \,|\, g_{t-1}] \,|\, g_{t-2}\right] \\ &\leq \mathbb{E}[g_{t-1}^2 \,|\, g_{t-2}] \leq g_{t-2}^2.\end{aligned}$$

Here, since $g_{t-2} \geq f(\alpha) > 0$, we have

$$g_{t-2} = \max\{0, g_{t-3} + s_{t-2}\} = g_{t-3} + s_{t-2}.$$

Again, there are two possibilities: we either have $g_{t-3} < f(\alpha)$ or $g_{t-3} \geq f(\alpha)$ and as such the procedure repeats itself backward in time. The conclusion is that if there exists $\omega \leq t$ such that $g_{t-\omega} < f(\alpha)$, then we have $\mathbb{P}(\mathbb{E}[g_t^2 \,|\, g_0 = 0] < \infty) = 1$. Since $g_0 = 0 < f(\alpha)$, there indeed exists at least one ω, which is $\omega = t$, such that $g_{t-\omega} < f(\alpha)$. Then, in case where $\alpha < 1/e$ and $g_{t-1} \geq f(\alpha)$, we have $\mathbb{P}(\mathbb{E}[g_t^2 \,|\, g_0 = 0] < \infty) = 1$.

Next, let $\alpha < 1/e$ and $g_{t-1} < f(\alpha)$. Since $g_t = \max\{0, g_{t-1} + s_t\}$, we either have $g_t = 0$ or $g_t = g_{t-1} + s_t$. If $g_t = 0$, we clearly have $\mathbb{E}[g_t^2 \,|\, g_0 = 0] = 0 < \infty$. On the other hand, if $g_t = g_{t-1} + s_t$, we have

$$\begin{aligned}
\mathbb{E}[g_t^2 \,|\, g_{t-1}] &= g_{t-1}^2 + 2g_{t-1}\mathbb{E}[s_t] + \mathbb{E}[s_t^2] \\
&= g_{t-1}^2 + 2g_{t-1}(1 + \log(\alpha)) + 1 + (1 + \log(\alpha))^2 \\
&< g_{t-1}^2 + 1 + (1 + \log(\alpha))^2 && (35) \\
&< f(\alpha)^2 + 1 + (1 + \log(\alpha))^2 < \infty, && (36)
\end{aligned}$$

where (35) follows since $g_{t-1}(1 + \log(\alpha)) < 0$ and (36) follows since $g_{t-1} < f(\alpha)$. Then, using nested expectations and the fact that the expectation of a finite variable is finite, we obtain the following inequality:

$$\mathbb{E}\left[\mathbb{E}[g_t^2 \,|\, g_{t-1}] \,|\, g_0 = 0\right] = \mathbb{E}[g_t^2 \,|\, g_0 = 0] < \infty,$$

that also implies

$$\mathbb{P}(\mathbb{E}\left[g_t^2 \,|\, g_0 = 0\right] < \infty) = 1.$$

In conclusion, if $\alpha < 1/e$, we have showed above that for both of the complementary conditions, namely $g_{t-1} \geq f(\alpha)$ and $g_{t-1} < f(\alpha)$, we have

$$\mathbb{P}(\mathbb{E}\left[g_t^2 \,|\, g_0 = 0\right] < \infty) = 1. \tag{37}$$

This implies that $\alpha < 1/e$ is a sufficient condition to obtain (37) asymptotically as $N_2 \to \infty$.

□

B. Proof of Theorem 2

Proof. As discussed in Appendix A, as $N_2 \to \infty$, $\hat{s}_t$ converges to s_t and hence the proposed CUSUM-like detector in (16) converges to the algorithm in (4). Note that if $\alpha < 1/e$, then $\mathbb{E}[s_t] = 1 + \log(\alpha) < 0$. In [5, Sec. 5.2.2.4], for CUSUM-like algorithms such as (4), a lower bound on the average false alarm period is then given as follows:

$$\mathbb{E}_\infty[\Gamma] \geq e^{-w_0 h},$$

where $w_0 < 0$ is the solution to

$$\mathbb{E}[e^{-w_0 s_t}] = 1. \tag{38}$$

Defining $\theta \triangleq w_0 + 1$, we can rewrite (38) based on the pdf of s_t (see (24)) as follows:

$$\begin{aligned} \mathbb{E}[e^{-w_0 s_t}] &= \int_{\log(\alpha)}^{\infty} e^{(1-\theta)y} \alpha e^{-y} dy \\ &= \alpha \int_{\log(\alpha)}^{\infty} e^{-\theta y} dy \\ &= \alpha \, \frac{e^{-\theta \log(\alpha)}}{\theta} = 1, \end{aligned} \tag{39}$$

provided that $\theta > 0$. The conditions $w_0 = \theta - 1 < 0$ and $\theta > 0$ together lead to $0 < \theta < 1$. Moreover, we can rewrite (39) as follows:

$$\theta \, e^{\theta \log(\alpha)} = \alpha,$$

and multiplying both sides by $\log(\alpha)$, we have

$$\theta \log(\alpha) \, e^{\theta \log(\alpha)} = \alpha \log(\alpha). \tag{40}$$

Now, define $z \triangleq \theta \log(\alpha)$ and $c \triangleq \alpha \log(\alpha)$ so that (40) can be rewritten as

$$z \, e^{z} = c,$$

where $z = W(c) = W(\alpha \log(\alpha))$. Then, we have

$$\theta = \frac{W(\alpha \log(\alpha))}{\log(\alpha)}.$$

Next, we show that there exists a unique solution to (39) by contradiction. Assume that there exists two solutions θ_1 and θ_2 to (39) where $\theta_1 \neq \theta_2$. Further, without loss of generality, assume $\theta_2 < \theta_1$. Then, we have $0 < \theta_2 < \theta_1 < 1$. From (39), we have

$$\alpha \, \frac{e^{-\theta_1 \log(\alpha)}}{\theta_1} = 1,$$

which implies that

$$\frac{\log(\theta_1)}{1 - \theta_1} = \log(\alpha), \tag{41}$$

and similarly,

$$\frac{\log(\theta_2)}{1 - \theta_2} = \log(\alpha). \tag{42}$$

Then, based on (41) and (42), we have

$$\frac{\log(\theta_1)}{1 - \theta_1} = \frac{\log(\theta_2)}{1 - \theta_2}. \tag{43}$$

Furthermore, for $0 < \theta < 1$, we have

$$\begin{aligned}\frac{\partial \frac{\log(\theta)}{1-\theta}}{\partial \theta} &= \frac{1/\theta - 1 + \log(\theta)}{(1-\theta)^2} \\ &= \frac{\mu - 1 - \log(\mu)}{(1-1/\mu)^2} > 0, \end{aligned} \tag{44}$$

where $\mu \triangleq 1/\theta > 1$. The inequality in (44) follows due to the fact that $\log(\mu) < \mu - 1$ for $\mu > 1$. Then, since the first order derivative of the function

$$\frac{\log(\theta)}{1-\theta}$$

is positive, it is monotonically increasing in the range of $0 < \theta < 1$. Since $0 < \theta_2 < \theta_1 < 1$, we then have

$$\frac{\log(\theta_2)}{1-\theta_2} < \frac{\log(\theta_1)}{1-\theta_1}, \tag{45}$$

which contradicts with (43). Hence, there exists a unique solution to (39).

□

References

[1] V. Chandola, A. Banerjee, and V. Kumar, “Anomaly detection: A survey,” *ACM computing surveys (CSUR)*, vol. 41, no. 3, p. 15, 2009.

[2] M. A. Pimentel, D. A. Clifton, L. Clifton, and L. Tarassenko, “A review of novelty detection,” *Signal Processing*, vol. 99, pp. 215–249, 2014.

[3] J. Kittler, W. Christmas, T. de Campos, D. Windridge, F. Yan, J. Illingworth, and M. Osman, “Domain anomaly detection in machine perception: A system architecture and taxonomy,” *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 36, no. 5, pp. 845–859, May 2014.

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

[5] M. Basseville and I. V. Nikiforov, *Detection of Abrupt Changes: Theory and Application*. Upper Saddle River, NJ, USA: Prentice-Hall, Inc., 1993.

[6] A. O. Hero, III, “Geometric entropy minimization (gem) for anomaly detection and localization,” in *Proceedings of the 19th International Conference on Neural Information Processing Systems*, ser. NIPS’06. Cambridge, MA, USA: MIT Press, 2006, pp. 585–592.

[7] K. Srichanran and A. O. Hero, “Efficient anomaly detection using bipartite k-nn graphs,” in *Advances in Neural Information Processing Systems*, 2011, pp. 478–486.

[8] S. V. Georgakopoulos, S. K. Tasoulis, and V. P. Plagianakos, “Efficient change detection for high dimensional data streams,” in *2015 IEEE International Conference on Big Data (Big Data)*, Oct 2015, pp. 2219–2222.

[9] X. J. Hunt and R. Willett, “Online data thinning via multi-subspace tracking,” *IEEE Transactions on Pattern Analysis and Machine Intelligence*, pp. 1–1, 2018.

[10] Y. Xie, J. Huang, and R. Willett, “Change-point detection for high-dimensional time series with missing data,” *IEEE Journal of Selected Topics in Signal Processing*, vol. 7, no. 1, pp. 12–27, 2013.

[11] R. Laxhammar and G. Falkman, “Online learning and sequential anomaly detection in trajectories,” *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 36, no. 6, pp. 1158–1173, June 2014.

[12] R. Dunia and S. J. Qin, “Multi-dimensional fault diagnosis using a subspace approach,” in *American Control Conference*, 1997.

[13] A. Lakhina, M. Crovella, and C. Diot, “Diagnosing network-wide traffic anomalies,” in *ACM SIGCOMM Computer Communication Review*, vol. 34, no. 4. ACM, 2004, pp. 219–230.

[14] A. L. Toledo and X. Wang, “Robust detection of selfish misbehavior in wireless networks,” *IEEE Journal on Selected Areas in Communications*, vol. 25, no. 6, pp. 1124–1134, August 2007.

[15] M. N. Kurt, Y. Yilmaz, and X. Wang, “Real-time detection of hybrid and stealthy cyber-attacks in smart grid,” *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 2, pp. 498–513, Feb 2019.

[16] B. Schölkopf, J. C. Platt, J. Shawe-Taylor, A. J. Smola, and R. C. Williamson, “Estimating the support of a high-dimensional distribution,” *Neural computation*, vol. 13, no. 7, pp. 1443–1471, 2001.

[17] G. Ratsch, S. Mika, B. Scholkopf, and K. . Muller, “Constructing boosting algorithms from svms: an application to one-class classification,” *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 24, no. 9, pp. 1184–1199, Sept 2002.

[18] M. Wu and J. Ye, “A small sphere and large margin approach for novelty detection using training data with outliers,” *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 31, no. 11, pp. 2088–2092, Nov 2009.

[19] V. Jumutc and J. A. K. Suykens, “Multi-class supervised novelty detection,” *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 36, no. 12, pp. 2510–2523, Dec 2014.

[20] M. Zhao and V. Saligrama, “Anomaly detection with score functions based on nearest neighbor graphs,” in *Advances in neural information processing systems*, 2009, pp. 2250–2258.

[21] H. Chen, “Sequential change-point detection based on nearest neighbors,” *arXiv preprint arXiv:1604.03611*, 2016.

[22] A. Gretton, K. M. Borgwardt, M. Rasch, B. Schölkopf, and A. J. Smola, “A kernel method for the two-sample-problem,” in *Advances in neural information processing systems*, 2007, pp. 513–520.

[23] L. Faivishevsky, “Information theoretic multivariate change detection for multisensory information processing in internet of things,” in *2016 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, March 2016, pp. 6250–6254.

[24] T. Dasu, S. Krishnan, S. Venkatasubramanian, and K. Yi, “An information-theoretic approach to detecting changes in multi-dimensional data streams,” in *In Proc. Symp. on the Interface of Statistics, Computing Science, and Applications*. Citeseer, 2006.

[25] Y. Yilmaz, “Online nonparametric anomaly detection based on geometric entropy minimization,” in *2017 IEEE International Symposium on Information Theory (ISIT)*, June 2017, pp. 3010–3014.

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

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

[28] M. N. Kurt, Y. Yilmaz, and X. Wang, “Distributed quickest detection of cyber-attacks in smart grid,” *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 8, pp. 2015–2030, Aug 2018.

[29] A. Ghoting, S. Parthasarathy, and M. E. Otey, “Fast mining of distance-based outliers in high-dimensional datasets,” *Data Mining and Knowledge Discovery*, vol. 16, no. 3, pp. 349–364, 2008.

[30] C. M. Bishop, *Pattern Recognition and Machine Learning (Information Science and Statistics)*. Secaucus, NJ, USA: Springer-Verlag New York, Inc., 2006.

[31] A. W. Van der Vaart, *Asymptotic statistics*. Cambridge University Press, 1998, vol. 3.

[32] C. Murguia and J. Ruths, “Cusum and chi-squared attack detection of compromised sensors,” in *2016 IEEE Conference on Control Applications (CCA)*, Sept 2016, pp. 474–480.

[33] R. A. Khan, “Wald’s approximations to the average run length in cusum procedures,” *Journal of Statistical Planning and Inference*, vol. 2, no. 1, pp. 63–77, 1978.

[34] C. W. Champ and S. E. Rigdon, “A a comparison of the markov chain and the integral equation approaches for evaluating the run length distribution of quality control charts,” *Communications in Statistics-Simulation and Computation*, vol. 20, no. 1, pp. 191–204, 1991.

[35] M. R. Reynolds, “Approximations to the average run length in cumulative sum control charts,” *Technometrics*, vol. 17, no. 1, pp. 65–71, 1975.

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

[37] Q. Wang, S. R. Kulkarni, and S. Verdu, “A nearest-neighbor approach to estimating divergence between continuous random vectors,” in *2006 IEEE International Symposium on Information Theory*, July 2006, pp. 242–246.

[38] A. Abur and A. Gomez-Exposito, *Power System State Estimation: Theory and Implementation*. New York, NY: Marcel Dekker, 2004.

[39] R. Zimmerman, C. Murillo-Sanchez, and R. Thomas, “Matpower: Steady-state operations, planning, and analysis tools for power systems research and education,” *IEEE Transactions on Power Systems*, vol. 26, no. 1, pp. 12–19, Feb 2011.

[40] J.-L. Reyes-Ortiz, L. Oneto, A. Samà, X. Parra, and D. Anguita, “Transition-aware human activity recognition using smartphones,” *Neurocomputing*, vol. 171, pp. 754–767, 2016.

[41] D. Dheeru and E. Karra Taniskidou, “UCI machine learning repository,” 2017. [Online]. Available: http://archive.ics.uci.edu/ml

[42] Y. Meidan, M. Bohadana, Y. Mathov, Y. Mirsky, D. Breitenbacher, A. Shabtai, and Y. Elovici, “N-baiot: Network-based detection of iot botnet attacks using deep autoencoders,” *arXiv preprint arXiv:1805.03409*, 2018.

[43] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, “Ddos in the iot: Mirai and other botnets,” *Computer*, vol. 50, no. 7, pp. 80–84, 2017.

[44] E. Bertino and N. Islam, “Botnets and internet of things security,” *Computer*, vol. 50, no. 2, pp. 76–79, 2017.

[45] R. Zimmermann, B. Peherstorfer, and K. Willcox, “Geometric subspace updates with applications to online adaptive nonlinear model reduction,” *SIAM Journal on Matrix Analysis and Applications*, vol. 39, no. 1, pp. 234–261, 2018.

[46] D. J. Pierre, *Subspace Tracking for Signal Processing*. Wiley-Blackwell, 2010, ch. 4, pp. 211–270.

[47] A. Papoulis and S. U. Pillai, *Probability, random variables, and stochastic processes*. Tata McGraw-Hill Education, 2002.