Distributed-Graph-Based Statistical Approach for Intrusion Detection in Cyber-Physical Systems

Hamidreza Sadreazami, *Member, IEEE*, Arash Mohammadi, *Member, IEEE*, Amir Asif, *Senior Member, IEEE*, and Konstantinos N. Plataniotis, *Fellow, IEEE*

***Abstract*—Cyber-physical systems have recently emerged in several practical engineering applications where security and privacy are of paramount importance. This motivated the paper and a recent surge of interest in development of innovative and novel anomaly and intrusion detection technologies. This paper proposes a novel distributed blind intrusion detection framework by modeling sensor measurements as the target graph-signal and utilizing the statistical properties of the graph-signal for intrusion detection. To fully take into account the underlying network structure, the graph similarity matrix is constructed using both the data measured by the sensors and sensors' proximity resulting in a data-adaptive and structure-aware monitoring solution. In the proposed supervised detection framework, the magnitude of the captured data is modeled by Gaussian Markov random field and the corresponding precision matrix is estimated by learning a graph Laplacian matrix from sensor measurements adaptively. The proposed intrusion detection methodology is designed based on a modified Bayesian likelihood ratio test and the closed-form expressions are derived for the test statistic. Finally, temporal analysis of the network behavior is established by computing the Bhattacharyya distance between the measurement distributions at the consecutive time instants. Experiments are conducted to evaluate the performance of the proposed method and to compare it with that of the state-of-the-art methods. The results show that the proposed intrusion detection framework provides a detection performance superior to those provided by the other existing schemes.**

***Index Terms*—Cyber-physical systems (CPSs), distributed sensor network, distributed signal processing, intrusion detection, statistical distance measures.**

I. Introduction

CYBER-PHYSICAL Systems (CPSs) [1]–[5] are integrations of control, communication and computation technologies which are employed to monitor and manage physical infrastructures. Recent advancements in communication and sensor technologies have paved the way for deployment of a large number of sensor nodes in CPSs, resulting in an exceptional growth in practical implementations and opportunistic applications of such systems. The rapid growth of CPSs and the fact that their applications are typically safety critical, have increased a recent surge of interest in security issues of CPSs [2]–[10]. Potential cyber and physical attacks by adversaries may lead to a variety of severe consequences in the societies including, but not limited to, customer information leakage, extensive damages to the economy, destruction of infrastructures, and endangering human lives. This makes identification and prevention of new cyber attacks of significant practical importance.

In particular, the focus of this paper is on sensor network intrusions which are irregular and distinctive changes in the data captured by the sensor nodes. Authentic activities such as transient changes in the temperature vapor detection by the smoke detector in the air flow, and illegitimate activities such as, injecting viruses and worms into the power grid are two examples of such intrusions. Nowadays, a sensor network incorporated in CPSs play an important role in managing and advancements of critical social and economic infrastructures. It is known that network intrusion detection constitutes an indispensable part of the network security and will become more vital in the future [11]–[14]. Today's network intrusion detection schemes have evolved to highly sophisticated levels, involving advanced signal processing techniques including but not limited to principal component analysis, time series analysis, and wavelets among other methodologies. The signature and non-signature based detectors are the most commonly used detectors for network anomaly detection. In the signature-based detection, anomaly can be detected by a correlation detector through matching the known signatures to the empirical data [15], while in the non-signature based methods signal analysis approaches are taken into consideration without requiring any prior knowledge about the anomalies such as the principal component analysis (PCA) based approaches [16]–[18].

Recently, there has been a surge of interest in devising new signal processing methodologies to cope with challenges of the "Big-Data Era". It is observed that classical signal processing solutions are typically incapable of properly handling big-data problems. Recent advances in graph signal processing (GSP) provides an opportunity to revisit traditional signal processing

Manuscript received January 5, 2017; revised April 13, 2017 and July 17, 2017; accepted August 24, 2017. Date of publication September 7, 2017; date of current version February 19, 2018. This work was supported in part by the Natural Sciences and Engineering Research Council (NSERC) of Canada under Create Grant 466280-2015. The guest editor coordinating the review of this manuscript and approving it for publication was Dr. Yan Sun. *(Corresponding author: Hamidreza Sadreazami.)*

H. Sadreazami and A. Asif are with the Department of Electrical and Computer Engineering, Concordia University, Montreal, QC H3G 1M8, Canada (e-mail: h_sadrea@encs.concordia.ca; amir.asif@encs.concordia.ca).

A. Mohammadi is with the Concordia Institute for Information Systems Engineering, Concordia University, Montreal, QC H3G 1M8, Canada (e-mail: arashmoh@encs.concordia.ca).

K. N. Plataniotis is with the Department of Electrical and Computer Engineering, University of Toronto, Toronto, ON M5S 3G4, Canada (e-mail: kostas@ece.utoronto.ca).

Digital Object Identifier 10.1109/TSIPN.2017.2749976

solutions and extend their applicability to emerging problems with large data sets. The GSP has provided a new framework for representing model relations among data samples [19], [20]. In data-oriented applications, the similarities between data samples measured by the sensors can be represented by a weighted graph.

In this paper, inspired by the recent advances in graph signal processing, a blind intrusion detection framework is proposed using statistical properties of the target graph signal. To this end, the network is supposed to be composed of a number of distributed sensors having spatial dependencies with irregular data measurements as signals on nodes of a weighted graph. It is assumed that the sensor placement is fixed with varying measurements over time. The graph affinity matrix is constructed where edges reflect both the similarities between signals and closeness of the sensors. In a supervised scenario, the magnitude of the measured data is assumed to be random variables distributed with a Gaussian Markov random field (GMRF) distribution having finite mean and precision matrices. A new statistical-based intrusion detection method is proposed by employing a Bayesian log-likelihood ratio test. The precision matrix of the model is estimated by learning a graph Laplacian matrix from the empirical data and used in the following computations of the intrusion detection. The resulting design provides a superior performance to other intrusion detection methods.

To summarize, the main contributions of our work can be summarized as follows:

1) The graph affinity matrix used in the proposed scheme is constructed based on both the sensors measured data and the proximity of the sensors. In this way, the proposed method differs from other existing methods by not only being data-adaptive but also fully taking into account the underlying network structure.
2) The proposed scheme develops a blind statistical-based intrusion detection method. The GMRF is used as an underlying probabilistic model for the graph signals in the context of detecting any deviation from the normal behavior of the network. In other words, the graph signals are treated as random variables with dependencies across sensor measurements and sensor physical placements. This assumption on the distribution of the graph signals has been thoroughly investigated in [42]. The detection scheme is then realized by using a hypothesis test based on the log-likelihood ratio criterion. Closed-form expression for the test statistic is derived.
3) The proposed scheme establishes a temporal analysis of the network behavior by computing the *Bhattacharyya* distance between the measurement distributions at consecutive time instants.

The remainder of the paper is organized as follows: Section II provides a brief review on the related works. Section III presents the graph construction, a model based on the GMRF and a parameter estimation method for the precision matrix. In Section IV, the proposed graph-based intrusion detection method is presented. Section V includes the experimental results and finally Section VI concludes the paper.

II. Related Works

In this section, we provide a brief overview of the recent state-of-the-art research works in the field of intrusion detection. We would like to point out that various types of anomalies have been introduced/considered in the literature in wide range of applications where usually each individual study only focuses on a subset of these cases. Consequently, direct comparison between different methods is not straightforward and is beyond the scope of this paper. In general, anomaly detection methodologies can be classified into a number of main categories which will be reviewed below.

In signal analysis approaches, PCA, a commonly used method for dimension reduction, can be employed as an effective technique to detect network anomalies by projecting the empirical data onto the principal axis and decomposing the subspace into normal and abnormal subspaces by setting a certain threshold [15]. The data projection on each axis is sequentially compared with a predefined threshold in order to identify the two subspaces. In addition, the PCA-based techniques have been used for detecting anomalies caused by the feature distribution diffusion [21]. In such cases, the PCA has been applied to a feature entropy matrix which is a metric for capturing the dispersal of the feature distributions [22]–[24]. In [16], a PCA-based intrusion detection scheme has been proposed to discern normal and abnormal data. However, since the corresponding principal components provide no locality information, the PCA-based techniques are not optimal for the intrusion detection in distributed applications in CPSs consisting of several dispersed sensors scattered across the network.

A second category of anomaly detection methodologies is model-based mechanisms where the network anomaly is identified using change detection algorithms [25], [26]. This is realized by assuming a model, e.g., sliding window averaging and exponential smoothing, for normal behavior of the sensors according to the record of measured data. In this case, anomaly is identified when a substantial deviation from the model happens in the current empirical data. However, the change detection techniques are not scalable to large-scale sensor measurements collected across the network for anomaly detection in CPSs [27]. Third category classified here is the wavelet-based approaches. In the algorithms belonging to this category the network anomaly detection is performed by analyzing the time-frequency characterization of the signal [28]. The wavelet analysis decomposes the measured data into a number of frequency bands including the low and high frequencies. Anomaly may be detected when the local variance of the frequency bands exceeds a certain threshold, indicating an unpredictable change in the network behavior.

In contrary to the above categories, anomalies can be automatically detected by unsupervised learning approaches based on clustering which can be performed in a top-down or bottom-up manner [21]. The latter merges smaller clusters into larger ones while the former divides the subspace hierarchically. It should be noted that irrespective of the method employed, a twofold criteria needs to be satisfied; minimizing the intra-cluster variations and maximizing the inter-cluster variations.

Other methodologies were developed based on the knowledge that anomaly may impose dispersal or concentration of feature distributions. In this regard, multi-way subspace methods have been used to enable anomaly detection across multiple features simultaneously by utilizing the sample entropy [15]. Anomalies can be detected by comparing the sample entropy with a threshold, determined by a predefined false alarm rate. In [31], entropy and conditional entropy have been used to provide data partitioning for intrusion detection. In [22], histograms of features have been obtained to detect the anomaly by using different clustered features. In [23], an anomaly detection scheme has been proposed by comparing the data measured by the sensors with an assumed distribution using the maximum entropy criterion. In [30], a clustering-based method has been proposed for anomaly detection in wireless sensor networks. Data point belonging to dense clusters have been considered to be in the normal profile, while data samples in other clusters including those with either small or sparse clusters have been regarded as anomalies. However, these methods are highly dependent to the distribution of the data. In other words, the performance of such methods is only acceptable when the data samples with normal profile are densely clustered.

It is known that GSP framework has recently provided a paradigm to unify the similarity metrics and design adaptive filtering algorithms by flexibly defining the measure of similarity, especially for high-dimensional data [20]. In addition, a probabilistic framework for signals defined on graphs has been always of interest. For instance, graphical models such as hidden Markov models have been used in signal processing and bioinformatics. Despite recent developments of GSP solutions, their applications to anomaly and intrusion detection are still in their infancy limited to few research works. For instance, in [31], an intrusion detection technique has been proposed by using a time-series graph for which principal eigenvectors of the affinity matrix are extracted and employed to detect intrusions. In [32], a method for detecting graph anomalies has been proposed based on the eigenvectors of the graph similarity matrix. In [33], using the graph regularity, a detection method has been developed for graph anomalies. In [34], the graph wavelet has been used for network analysis. A web graph similarity has been proposed for anomaly detection in [35]. In [36], an event detection method has been proposed in wireless sensor networks in which a graphical model has been used to capture the spatial dependency of the neighboring sensors and enhance the detection accuracy. However, the detection scheme is not blind and needs the knowledge of the true event indicator value. In addition, there is no temporal analysis on the sensor measurements and choice of parameters are adhoc. For instance, the nearest neighbor sensors are limited to maximum four sensors and the number of event-regions and their corresponding sizes depends on how well the training data represents the true field. In [37], a spectral interpretation of the graph filtering and PCA has been proposed for intrusion detection. In [37], a new subspace for given data samples has been derived to distinguish the data with normal and abnormal profiles by using projection. However, the performance of this method highly depends on the choice of the subspace employed.

While a variety of approaches exist for detecting intrusion in CPSs, they are mostly incapable of distinguishing between the spatial and temporal anomalies. In addition, they fall short in providing a unified method to take into consideration both the sensor proximity information and its measured data. In view of this and in order to achieve higher intrusion detection rate, in this work, a new supervised graph-based statistical approach for intrusion detection in cyber physical systems is proposed. The graph similarity matrix is constructed using a Gaussian kernel by taking into account both the sensors geodesic distances and their measured data. A new blind intrusion detection framework is designed based on the GMRF model for the graph signals using the log-likelihood ratio criterion. Closed-form expression for the test statistic is derived and temporal analysis of the network behavior is established.

III. Proposed Graph-Based Modeling Framework

Throughout the paper, the following notations are used: Capital non-bold letter X denotes a scalar variable, lowercase bold letter $\boldsymbol{x}$ represents a vector, and capital bold letter $\boldsymbol{X}$ denotes a matrix. A script letter (e.g., $\mathcal{A}$) denotes a set. In this paper, we consider a diagnostic solution where N sensors are employed and scattered throughout the system to monitor the operating condition of the underlying CPS. A distributed processing architecture is considered including a fusion center (FC) where for real-time anomaly/intrusion detection, each sensor node communicates its local observations to the FC which then implements the diagnostic solution on the collected set of measurements. In addition, the sensors are assumed to be static (as is the case in several applications of CPSs) and the location of sensor l, for $(1 \leq l \leq N)$, denoted by $[X_l, Y_l]$ is known in advance. For real-time monitoring of the CPSs, sensor measurements are collected periodically over time and are typically related to the system state of the CPS defined as the state-vector $\boldsymbol{x}$, which characterizes the current operating condition of the CPS. The measurement corresponding to sensor l, for $(1 \leq l \leq N)$, is defined as follows

$$S_l(k) = \boldsymbol{h}_l(\boldsymbol{x}(k)) + \nu_l(k), \tag{1}$$

where k denotes time index, and $\nu_l(k)$ represents the uncertainties in the sensor model. A general observation model $\boldsymbol{h}_l(\cdot)$ is considered relating the measurements of sensor l to the system state. Based on the measurements of the N randomly distributed sensors (nodes), we construct instantaneous graph signals at each time. In other words, each sensor measures data $S_l(k)$ at time instant $k = 1, \ldots, K$, resulting in the following instantaneous graph signal

$$(k) = [S_1(k), \ldots, S_N(k)], \tag{2}$$

which is a vector of size N of graph signals in one observation. In the following sections we formulate the proposed monitoring model as the basis for the proposed graph-based intrusion detection. In what follows, first we construct the graph representing the N constituent sensors utilized for monitoring the CPS, and investigate its properties. Then we formulate the graph model followed by its parameter estimation methodology

before describing the proposed graph-based intrusion detection framework in the next section.

A. Graph Construction

Emerging field of graph signal processing offers a framework for incorporating classical signal processing approaches into large data sets by representing the signals on graphs [19]. To exploit the similarity in the sensor measurements, the N considered sensors are treated as the vertices of a weighted graph $G = (\mathcal{V}, \mathcal{E}, \boldsymbol{W})$ consisting of a finite set $\mathcal{V}$ of vertices and a finite set $\mathcal{E}$ of edges with the corresponding weights $w_{\mathrm{pq}} \in \boldsymbol{W}$. The weight w_{pq}, for $(1 \leq p, q \leq N)$, is a measure of similarity between vertices (sensors) p and q. A sensor q is considered to be similar to sensor p, if it is within the first κ-closest sensors to p, i.e., κ-nearest neighbors set of sensors. The similarity weight w_{pq} is defined by the standard Gaussian kernel as follows

$$w_{\mathrm{pq}} = \exp\left(-\left(\frac{D_{\mathrm{pq}}^2}{2\sigma_{\mathrm{pq}}^2} + \frac{D_g^2}{2\sigma_g^2}\right)\right), \tag{3}$$

where

$$D_{\mathrm{pq}} = \sqrt{(X_p - X_q)^2 + (Y_p - Y_q)^2}, \tag{4}$$

is the geometrical distance, $D_g^2 = (S_p - S_q)^2$ is the signal value distance, σ_{pq} and σ_g control the level of similarity achieved by (3), S_p and S_q are the graph-signals on nodes p and q. Having the graph similarity matrix $\boldsymbol{W}$, the corresponding real-valued and symmetric graph Laplacian matrix is defined as [19]

$$\boldsymbol{L} = \boldsymbol{D} - \boldsymbol{W}, \tag{5}$$

where

$$\boldsymbol{D} = \mathrm{diag}\left\{\sum_q w_{1q}, \ldots, \sum_q w_{\mathrm{Nq}}\right\}. \tag{6}$$

The graph Laplacian matrix plays an important role in describing the underlying structure of the graph signal. In graph spectral domain, the graph properties are studied in terms of eigenvalues and eigenvectors associated with the graph Laplacian matrix (collective set of measurements at each time instant at the FC). The set of eigenvectors of $\boldsymbol{L}$ is considered as basis functions of the underlying signal defined on the graph, and its eigenvalues are known as the corresponding graph frequencies. The eigendecomposition of the Laplacian is given by [38], [39],

$$\boldsymbol{L} = \sum_i \lambda_i \boldsymbol{u}_i \boldsymbol{u}_i^T, \tag{7}$$

where superscript T denotes transpose operator, $\lambda = \{\lambda_i\}_{i=1,\ldots,N}$ is the set of eigenvalues and $\mathcal{U} = \{\boldsymbol{u}_i\}_{i=1,\ldots,N}$ is the set of orthogonal eigenvectors associated with the Laplacian matrix. Set $\mathcal{U}$ constitutes the basis functions for the underlying signal defined on the graph, and λ is known as the corresponding graph frequencies. The graph signal $\boldsymbol{s}(k)$ is decomposed into the graph Fourier domain components denoted by $\tilde{\boldsymbol{s}}(k)$ at each time instant using the eigenvectors $\boldsymbol{u}_i(k)$, for $(1 \leq i \leq N)$, of the corresponding Laplacian matrix at that time $\boldsymbol{L}(k)$ as given by [52], [53]

$$\tilde{\boldsymbol{s}}(k) = \boldsymbol{U}(k)^T \boldsymbol{s}(k), \tag{8}$$

where $\boldsymbol{U}(k)$ is a matrix composed of the eigenvectors of $\boldsymbol{L}(k)$. A graph signal $\boldsymbol{s}(k)$ is regarded as smooth with respect to the graph G if most of its energy is concentrated in the low frequencies, i.e., most $\tilde{\boldsymbol{s}}(k)$ coefficients are zero for large values of λ's. In other words, a smooth signal $\boldsymbol{s}(k)$ gives rise to a smaller value of graph smoothness regularizer $\boldsymbol{s}^T(k)\boldsymbol{L}(k)\boldsymbol{s}(k)$, as given by [51]

$$\boldsymbol{s}^T(k)\boldsymbol{L}(k)\boldsymbol{s}(k) = \sum_{i=1}^{N} \lambda_i \left(\boldsymbol{u}_i(k)^T \boldsymbol{s}(k)\right)^2, \tag{9}$$

The smoothness regularizer $\boldsymbol{s}^T(k)\boldsymbol{L}(k)\boldsymbol{s}(k)$ will be further used for sparse graph learning discussed later in Section III-C.

B. Graph Model

In this paper, our main goal is to develop a blind intrusion detection framework. In a blind detection scheme, the receiver has no access to the graph construction information, and thus, the graph Laplacian matrix (or correspondingly, the graph similarity matrix containing the weights) for the graph modeling is not known. In view of this, we consider a prior distribution for the graph-signal. More specifically, the observation $\boldsymbol{s}(k)$ is assumed to be instances of a GMRF having the probability density function as follows [40]

$$f(\boldsymbol{s}(k)) = (2\pi)^{\frac{-N}{2}} |\boldsymbol{Q}(k)|^{\frac{1}{2}} \times \exp\left(\frac{-1}{2}(\boldsymbol{s}(k) - \boldsymbol{m}(k))^T \boldsymbol{Q}(k)(\boldsymbol{s}(k) - \boldsymbol{m}(k))\right) \tag{10}$$

where $\boldsymbol{m}(k)$ is the mean vector and $\boldsymbol{Q}(k)$ is a symmetric precision matrix. The precision matrix $\boldsymbol{Q}(k)$ is assumed to be related to the graph similarity matrix, given in (3), by the following expression [42]

$$Q_{\acute{p}\acute{q}} = \begin{cases} \sum_{\acute{q}} w_{\acute{p}\acute{q}} & \acute{p} = \acute{q} \\ -w_{\acute{p}\acute{q}} & \acute{p} \neq \acute{q} \end{cases} \tag{11}$$

In view of this, there exist a consistent relationship between the precision matrix $\boldsymbol{Q}(k)$ and the graph Laplacian matrix $\boldsymbol{L}(k)$. In the graph-based model, a node is connected to its κ-closest neighbors; thus, the resulting precision matrix is sparse [41].

C. Parameter Estimation

In this section, we describe the learning approach that is used in this paper for estimating the parameters of the GMRF distribution. One naive approach to this end is to simply use the sample mean and covariance of the observation vector computed based on the previous measurements stacked over time. The sample $(N \times N)$ covariance matrix $\boldsymbol{C} = \{C_{\mathrm{ij}}\}$ is obtained as

$$C_{\mathrm{ij}} = \frac{1}{N-1} \sum_{o=1}^{N} \left(S_{\mathrm{oi}} - \bar{S}_i\right)^T \left(S_{\mathrm{oj}} - \bar{S}_j\right), \tag{12}$$

where sensor observations at each time instant $k = 1, \ldots, K$ are used, S_{oi} denotes the o-th sensor measurement of sensor i, and

$\bar{S}_o$ denotes the mean of sensors' measurements at each time instant o. Accordingly, the precision matrix $\boldsymbol{Q}$ in a GMRF model can be computed using a covariance matrix $\boldsymbol{C}$ for N samples as $\boldsymbol{Q} = \boldsymbol{C}^{-1}$. However, the estimated $\boldsymbol{C}$ may not be robust resulting in a precision matrix $\boldsymbol{Q}$ that deviates significantly from the true precision matrix [42]. In order to robustly estimate $\boldsymbol{Q}$, there exist several approaches based on learning a sparse precision matrix [43]–[48]. In this paper, we follow the approach presented in [46], in which a sparse graph learning approach has been employed. More specifically, the GMRF model with precision matrix $\boldsymbol{Q}$ has a corresponding graphical representation given in (11) in such a way that the weight w_{pq} connects nodes p and q in the graph with the edge value $-L_{\mathrm{pq}}$. When there is no edge connecting nodes p and q, $L_{\mathrm{pq}} = 0$. The graph Laplacian of the corresponding graph is in fact the precision matrix $\boldsymbol{Q}$. In view of this and in order to estimate $\boldsymbol{Q}$, the signal $\boldsymbol{s}(k)$ is projected into the graph Fourier basis and the following optimization problem is solved [46]

$$\underbrace{\min}_{\boldsymbol{L}(k),\hat{\boldsymbol{s}}(k)} \; ||\boldsymbol{s}(k) - \hat{\boldsymbol{s}}(k)||_F^2 + \zeta \mathrm{tr}(\hat{\boldsymbol{s}}(k)^T \boldsymbol{L}(k)\hat{\boldsymbol{s}}(k)) + \gamma ||\boldsymbol{L}(k)||_F^2, \tag{13}$$

where ζ and γ are the regularization parameters, $||\cdot||_F$ denotes the Frobenious norm. In addition $L_{\mathrm{ij}} = L_{\mathrm{ji}} \leq 0$, for $i \neq j$ and $\mathrm{tr}(\boldsymbol{L}) = M$, where $\mathrm{tr}(\cdot)$ denotes the trace operator and $\mathbf{L} \in \Re^{M \times M}$. The first term on the right hand side (RHS) of (13) is the fidelity term insuring the closeness of the estimate to the original signal, while the second term is the smoothness term defined as follows

$$\begin{aligned} \hat{\boldsymbol{s}}(k)^T \boldsymbol{L}(k)\hat{\boldsymbol{s}}(k) &= \sum_{p=1}^{N} w_{\mathrm{pp}} \hat{\boldsymbol{s}}_p^2 \\ &\quad + \sum_{p=1}^{N} \sum_{q:q\neq p}^{N} w_{\mathrm{pq}} \big(\hat{\boldsymbol{s}}_p - \hat{\boldsymbol{s}}_q\big)^2, \end{aligned} \tag{14}$$

and used as a measure of graph signal smoothness. The last term on the RHS of (13) is a measure of cardinality and promotes sparsity. Equation (13) can be solved for the matrix $\boldsymbol{L}(k)$ to be a valid graph Laplacian matrix by utilizing an alternating optimization approach [45]. It is to be noted that there exist other approaches to estimate the graph Laplacian $\boldsymbol{L}(k)$ given observations $\boldsymbol{s}(k)$ as the graph signals. For instance, in [43], the inverse covariance matrix has been estimated using the graphical lasso as an extension of the l_1-regularization in the sparse coding. In [44], a graph template with edges in the two different directions has been developed and used for estimation of two weight parameters for edges of the two different directions based on the computed structure tensor.

IV. Graph-Based Intrusion Detection

In this section, we introduce the proposed intrusion detection framework which is designed based on the proposed graph-based modeling discussed in Section III. In order to detect any deviation from the normal behavior of the network, in this work, we propose a detection method based on the graph signal statistics. To this end, the Bayesian log-likelihood ratio test is employed to detect any possible intrusion in each time instant. This method can be reduced to a binary hypothesis test consisting of testing an alternative hypothesis H_1 against a null hypothesis H_0 and can be mathematically formulated based on the statistical properties of the graph signals. The hypotheses H_1 and H_0 represent as to whether the signal suffers from a significant change by the anomaly $\boldsymbol{a}$ or not, respectively, and can be stated as

$$\begin{aligned} H_1 &: \; \boldsymbol{y}(k) = \boldsymbol{s}(k) + \xi \boldsymbol{a}(k) \\ H_0 &: \; \boldsymbol{y}(k) = \boldsymbol{s}(k) \end{aligned} \tag{15}$$

As discussed in Section III, the data is assumed to follow a statistical distribution, namely, the GMRF model. The decision rule is defined using the likelihood ratio $\Lambda(\boldsymbol{y}(k))$ as follows

$$\begin{aligned} \Lambda(\boldsymbol{y}(k)) &= \frac{Pr(\boldsymbol{y}(k)|H_1)}{Pr(\boldsymbol{y}(k)|H_0)} \\ &= \frac{Pr(\boldsymbol{y}(k) - \xi\boldsymbol{a}(k); \boldsymbol{Q}(k), \boldsymbol{m}(k))}{Pr(\boldsymbol{y}(k); \boldsymbol{Q}(k), \boldsymbol{m}(k))} \underset{H_0}{\overset{H_1}{\gtrless}} \eta, \end{aligned} \tag{16}$$

where η is the threshold. The PDFs $Pr(\boldsymbol{y}(k)|H_1)$ and $Pr(\boldsymbol{y}(k)|H_0)$ follow the GMRF distribution. After taking the logarithm from (16), the log-likelihood ratio is given by

$$\begin{aligned} l(\boldsymbol{y}(k)) &= \ln\left(\frac{Pr(\boldsymbol{y}(k)|H_1)}{Pr(\boldsymbol{y}(k)|H_0)}\right) \\ &= \ln\left(\frac{Pr(\boldsymbol{y}(k) - \xi\boldsymbol{a}(k); \boldsymbol{Q}(k), \boldsymbol{m}(k))}{Pr(\boldsymbol{y}(k); \boldsymbol{Q}(k), \boldsymbol{m}(k))}\right) \underset{H_0}{\overset{H_1}{\gtrless}} \tau, \end{aligned} \tag{17}$$

where $l(\boldsymbol{y}(k)) \triangleq \ln[\Lambda(\boldsymbol{y}(k))]$ is the log-likelihood ratio and $\tau = \ln(\eta)$. The detection statistic is then obtained by inserting (10) into (17) as

$$\begin{aligned} l(\boldsymbol{y}(k)) &= -\frac{1}{2}(\boldsymbol{y}(k) - \xi\boldsymbol{a}(k))^T \boldsymbol{Q}(k)(\boldsymbol{y}(k) - \xi\boldsymbol{a}(k)) \\ &\quad + \frac{1}{2}\boldsymbol{y}(k)^T \boldsymbol{Q}(k)\boldsymbol{y}(k). \end{aligned} \tag{18}$$

The detector is supposed to choose between H_1 and H_0 based on the received observations. The detection is performed by comparing $l(\boldsymbol{y}(k))$ with τ, determined by maximizing the probability of detection P_{Det} for a predefined probability of false alarm P_{Fa} [54]. It is noted that P_{Det} is the probability that the detector decides the preposition H_1 to be true when an intrusion occurs and that P_{Fa} is the probability that it decides H_1 to be true when, in fact, there is no intrusion. By considering all terms of the summation to be independent, the log-likelihood ratio is clearly a superposition of N random variables with finite mean and variance. Thus, according to the central limit theorem for large value of N [55], the log-likelihood ratio follows an approximately Gaussian distribution under each hypothesis. The mean and variance of each of the Gaussian distributions can be estimated from the empirical data and are given by (μ_0, σ_0^2)

and (μ_1, σ_1^2) for H_0 and H_1, respectively. Once the mean and variance of the log-likelihood ratio under both hypotheses are known, for a particular value of τ, the probabilities of false alarm and detection can be estimated as follows [55]

$$P_{\text{Fa}} = Q\left(\frac{\tau - \mu_0}{\sigma_0}\right)$$
$$P_{\text{Det}} = Q\left(\frac{\tau - \mu_1}{\sigma_1}\right), \tag{19}$$

where $Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^\infty e^{-z^2/2} dz$. The decision threshold is obtained using the Neyman-Pearson criterion and can be expressed as

$$\tau = \sigma_0 Q^{-1}(P_{\text{Fa}}) + \mu_0. \tag{20}$$

The performance of the proposed statistical detector can be analyzed experimentally by relating the probability of detection and the probability of false alarm as given by the following expression

$$P_{\text{Det}} = Q\left(\frac{\sigma_0}{\sigma_1} Q^{-1}(P_{\text{Fa}}) - \frac{\mu_1 - \mu_0}{\sigma_1}\right). \tag{21}$$

Resulting curves are called the receiver operating characteristics (ROC). In order to evaluate the performance of the proposed intrusion detection method, we resort to a Monte Carlo simulations to numerically find the log-likelihood ratio $l(\boldsymbol{y}(k))$ by generating random anomalies. To this end, 1000 randomly generated anomaly sequences are employed. For each run, $l(\boldsymbol{y}(k))$ is estimated using (18) for both the hypotheses. The experimental mean and variance of $l(\boldsymbol{y}(k))$ are then estimated. Thus, when the means and variances of the log-likelihood ratio under both hypotheses for a particular value of τ are known, the probabilities of false alarm and detection can be estimated using (19). It should be noted that to increase the reliability of detection, P_{Det} needs to be kept at a high level for a predefined rate of false alarm.

It should be noted that there exist two kinds of anomaly detection algorithms; (i) supervised anomaly detection, where some prior statistical information on normal and anomalous signals are known, and (ii) unsupervised anomaly detection, where no knowledge about the normal and anomalous signals is required. Since our proposed approach belongs to the category of supervised methods, a discrete probability distribution is assumed for variable $\boldsymbol{a}$ with equiprobable values in $\{-1, +1\}$. The corresponding distribution is given by

$$Pr(A = a) = f(a) = \begin{cases} 0.5 & \text{if } a = +1 \\ 0.5 & \text{if } a = -1 \end{cases} \tag{22}$$

It is to be noted that different types of anomalies can be analyzed using (18), irrespective of making any probabilistic assumption on the behavior of the anomalies. If we do not assume any probabilistic behavior for the anomalies, i.e., manually annotating the anomalous points, our proposed detector can be experimentally evaluated based on the Monte Carlo simulations by finding the log-likelihood ratio $l(\mathbf{y}(k))$, for randomly generated anomaly sequences. In our proposed approach, we assume a probability distribution for the anomalies to analytically derive the mean and variance of the log-likelihood ratio under the hypotheses H_0 and H_1. For this purpose, let $l(\boldsymbol{y}(k)) = -\frac{1}{2} g_1(\boldsymbol{y}(k)) + \frac{1}{2} g_2(\boldsymbol{y}(k))$, where

$$\begin{aligned} g_1(\boldsymbol{y}(k)) &= (\boldsymbol{y}(k) - \xi \boldsymbol{a}(k))^T \boldsymbol{Q}(k)(\boldsymbol{y}(k) - \xi \boldsymbol{a}(k)) \\ g_2(\boldsymbol{y}(k)) &= \boldsymbol{y}(k)^T \boldsymbol{Q}(k) \boldsymbol{y}(k). \end{aligned} \tag{23}$$

The mean and variance of the log-likelihood ratio under H_0 can be obtained as [54]

$$\mu_0 = \mu(l(\boldsymbol{y}(k))); H_0) = (\mu_{g_1} + \mu_{g_2}), \tag{24}$$

and

$$\begin{aligned} \sigma_0^2 &= \sigma^2(l(\boldsymbol{y}(k))); H_0) \\ &= (\sigma_{g_1}^2 + \sigma_{g_2}^2 - 2\mu_{g_1 g_2} + 2\mu_{g_1}\mu_{g_2}). \end{aligned} \tag{25}$$

From (22), $\boldsymbol{a}(k)$ takes values of $+1$ and -1 with equal probability. Hence, μ_{g_1} and μ_{g_2} can be obtained as

$$\begin{aligned} \mu_{g_1} = \frac{1}{2}&((\boldsymbol{y}(k) - \xi)^T \boldsymbol{Q}(k)(\boldsymbol{y}(k) - \xi) \\ &+ (\boldsymbol{y}(k) + \xi)^T \boldsymbol{Q}(k)(\boldsymbol{y}(k) + \xi)), \end{aligned} \tag{26}$$

and

$$\mu_{g_2} = \boldsymbol{y}(k)^T \boldsymbol{Q}(k) \boldsymbol{y}(k). \tag{27}$$

And hence μ_0 can be calculated using (24). In order to find the variance of the log-likelihood ratio, given by (25), the various terms are found and given below

$$\begin{aligned} \sigma_{g_1}^2 &= E[g_1^2] - \mu_{g_1}^2 \\ &= \Bigg(\frac{1}{2}(\boldsymbol{y}(k) - \xi)^T \boldsymbol{Q}(k)(\boldsymbol{y}(k) - \xi) \\ &\quad - \frac{1}{2}(\boldsymbol{y}(k) + \xi)^T \boldsymbol{Q}(k)(\boldsymbol{y}(k) + \xi)\Bigg)^2, \end{aligned} \tag{28}$$

$$\sigma_{g_2}^2 = E[g_2^2] - \mu_{g_2}^2 = 0, \tag{29}$$

$$\begin{aligned} \mu_{g_1 g_2} = &\frac{1}{2}\left((\boldsymbol{y}(k) - \xi)^T \boldsymbol{Q}(k)(\boldsymbol{y}(k) - \xi)\right)\left(\boldsymbol{y}(k)^T \boldsymbol{Q}(k) \boldsymbol{y}(k)\right) \\ &+ \frac{1}{2}\left((\boldsymbol{y}(k) + \xi)^T \boldsymbol{Q}(k)(\boldsymbol{y}(k) + \xi)\right)\left(\boldsymbol{y}(k)^T \boldsymbol{Q}(k) \boldsymbol{y}(k)\right), \end{aligned} \tag{30}$$

and

$$\begin{aligned} \mu_{g_1}\mu_{g_2} = &\frac{1}{2}\left(\boldsymbol{y}(k)^T \boldsymbol{Q}(k) \boldsymbol{y}(k)\right) \\ &\times \left((\boldsymbol{y}(k) - \xi)^T \boldsymbol{Q}(k)(\boldsymbol{y}(k) - \xi) + (\boldsymbol{y}(k) + \xi)^T \boldsymbol{Q}(k)(\boldsymbol{y}(k) + \xi)\right). \end{aligned} \tag{31}$$

Thus, the theoretical mean and variance of the log likelihood ratio under H_0 can be shown to be

$$\mu_0 = -\frac{1}{4}(\boldsymbol{y}(k)-\xi)^T\boldsymbol{Q}(k)(\boldsymbol{y}(k)-\xi) - \frac{1}{4}(\boldsymbol{y}(k)+\xi)^T\boldsymbol{Q}(k)(\boldsymbol{y}(k)+\xi) + \frac{1}{2}(\boldsymbol{y}(k)^T\boldsymbol{Q}(k)\boldsymbol{y}(k)), \tag{32}$$

and

$$\sigma_0^2 = \frac{1}{16}((\boldsymbol{y}(k)-\xi)^T\boldsymbol{Q}(k)(\boldsymbol{y}(k)-\xi) + (\boldsymbol{y}(k)+\xi)^T\boldsymbol{Q}(k)(\boldsymbol{y}(k)+\xi))^2. \tag{33}$$

In a similar manner, the mean and variance of the log-likelihood ratio under H_1 are obtained. It can be also shown that $\mu_1 = -\mu_0$ and $\sigma_1^2 = \sigma_0^2$. It is observed from (32) and (33) that the test statistic is dependent on the power of the intrusion. Thus, the theoretical ROC curves can be obtained using (21) for different values of ξ.

To detect the anomalies over time, we propose the use of *Bhattacharyya* distance [49] between the measurement distributions at consecutive time instants. The *Bhattacharyy*a distance (BD) measures the similarity of two discrete or continuous probability distribution and is closely related to the *Bhattacharyya* coefficient (BC), also known as Hellinger affinity [50], which measures the amount of overlap between two statistical samples. Specifically, the BD for Gaussian distributions is typically used for evaluating class separability in classification problems and feature extraction in pattern recognition. In general, feature extraction can be considered as the process of transforming high dimensional data into a low dimensional feature space based on an optimization criterion. In other words, reducing dimensionality without a serious loss of class separability is the key to feature extraction. Dimensionality reduction and identification of relevant features are, therefore, important for the classification accuracy. In discriminant analysis, the Bayes error is the best criterion to evaluate feature sets, and posterior functions are the ideal features. Unfortunately, the Bayes error is too complex to be used as an analytical tool for extracting features. The BC/BD is directly related to the classification error and provides an upper bound on the Bayes error, therefore, it has been widely used in pattern recognition as an effective measure of the separability of two distributions.

The BC between two probability distributions, $f_1(\boldsymbol{s})$ and $f_2(\boldsymbol{s})$, is denoted by $\rho_{\mathrm{B}}(f_1, f_2)$ and is defined as follows

$$\rho_{\mathrm{B}}(f_1, f_2) = \int \sqrt{f_1(\boldsymbol{s})f_2(\boldsymbol{s})}d\boldsymbol{s} = \int f_2(\boldsymbol{s})\sqrt{\frac{f_1(\boldsymbol{s})}{f_2(\boldsymbol{s})}}d\boldsymbol{s}. \tag{34}$$

Another closely related measure is referred to as the *Bhattacharyy*a distance (BD), denoted by $d_{\mathrm{B}}(f_1(\boldsymbol{s}), f_2(\boldsymbol{s}))$, which is defined based on the BC as follows

$$d_{\mathrm{B}}(f_1(\boldsymbol{s}), f_2(\boldsymbol{s})) = -\ln \rho_{\mathrm{B}}(f_1(\boldsymbol{s}), f_2(\boldsymbol{s})). \tag{35}$$

Below, we consider the distance measure obtained as follows

$$d_{\mathrm{B}}\left(f_k, f_{k+1}\right) = -\ln\left(\int \sqrt{f_k(\boldsymbol{s})f_{k+1}(\boldsymbol{s})}\right)d\boldsymbol{s}, \tag{36}$$

The Bhattacharyya distance is computed for two consecutive time instants by inserting (10) into (36), as given by

$$d_{\mathrm{B}}\left(f_k, f_{k+1}\right) = \frac{1}{8}\left(\boldsymbol{m}_k - \boldsymbol{m}_{k+1}\right)^T \times \frac{\boldsymbol{Q}_k + \boldsymbol{Q}_{k+1}}{2}\left(\boldsymbol{m}_k - \boldsymbol{m}_{k+1}\right) + \frac{1}{2}\ln\frac{\frac{\boldsymbol{Q}_k+\boldsymbol{Q}_{k+1}}{2}}{\sqrt{|\boldsymbol{Q}_k||\boldsymbol{Q}_{k+1}|}}, \tag{37}$$

where $\boldsymbol{m}_k$ and $\boldsymbol{m}_{k+1}$ are the mean vectors and, $\boldsymbol{Q}_k$ and $\boldsymbol{Q}_{k+1}$ are the precision matrices of the f_k and f_{k+1}, respectively. In addition and in view of the fact that the *Bhattacharyya* distance in (37) measures the distance between two exponential probability distributions with estimated precision matrices $\boldsymbol{L}_k$ and $\boldsymbol{L}_{k+1}$, we can directly compute the distance between the two estimated Laplacian matrices. To this end, the Frobenious norm of the difference matrix is obtained as follows

$$\mathrm{Dist}\left(\boldsymbol{L}_k, \boldsymbol{L}_{k+1}\right) = \left\|\boldsymbol{L}_k - \boldsymbol{L}_{k+1}\right\|_F. \tag{38}$$

The Dist in (38) is computationally less expensive without compromising the detection performance. The performance of both the distances will be investigated in Section V.

V. Experimental Results

Experiments are conducted to investigate the performance of the proposed graph-based intrusion detection method and to compare its performance with those of the other existing works. In the experiments, time-series temperature data are generated in the intervals of 1 hour for 30 days. We consider 64 randomly distributed sensors collecting univariate data corresponding to the room temperature at 64 locations for 720 time instants. Fig. 1 illustrates the configuration of the sensor placement and some of the sensor measurements normalized by the maximum reading. Fig. 2 shows a sample sensor measurement values over time when the sensor measures the temperature during 30 days. At each time instant, the graph similarity matrix is constructed for the entire network and the corresponding graph Laplacian matrix is obtained. The graph Laplacian is then utilized in the detection scheme in the context of the GMRF precision matrix as discussed in Section III-B. It should be noted that since we estimate the graph Laplacian matrix $\boldsymbol{L}$ at each time instant independently, no stationarity assumption is needed in our proposed approach.

In order to obtain the experimental ROC curves, as stated previously, Monte Carlo simulations are carried out in which 1000 pseudo-random sequences are generated for intrusion and at every run for a given ξ. Then, experimental values of the mean and variance of the test statistic conditioned on each hypothesis are computed and the resulting ROC curve, obtained. Fig. 3 depicts the theoretical as well as the experimental ROC curves in the range $0 \leq P_{\mathrm{Fa}} \leq 10^{-2}$ obtained using the proposed intrusion detection method. It is seen from this figure that the experimental ROC curves are very close to the theoretical ones, thus establishing the validity of the expression derived in (32)

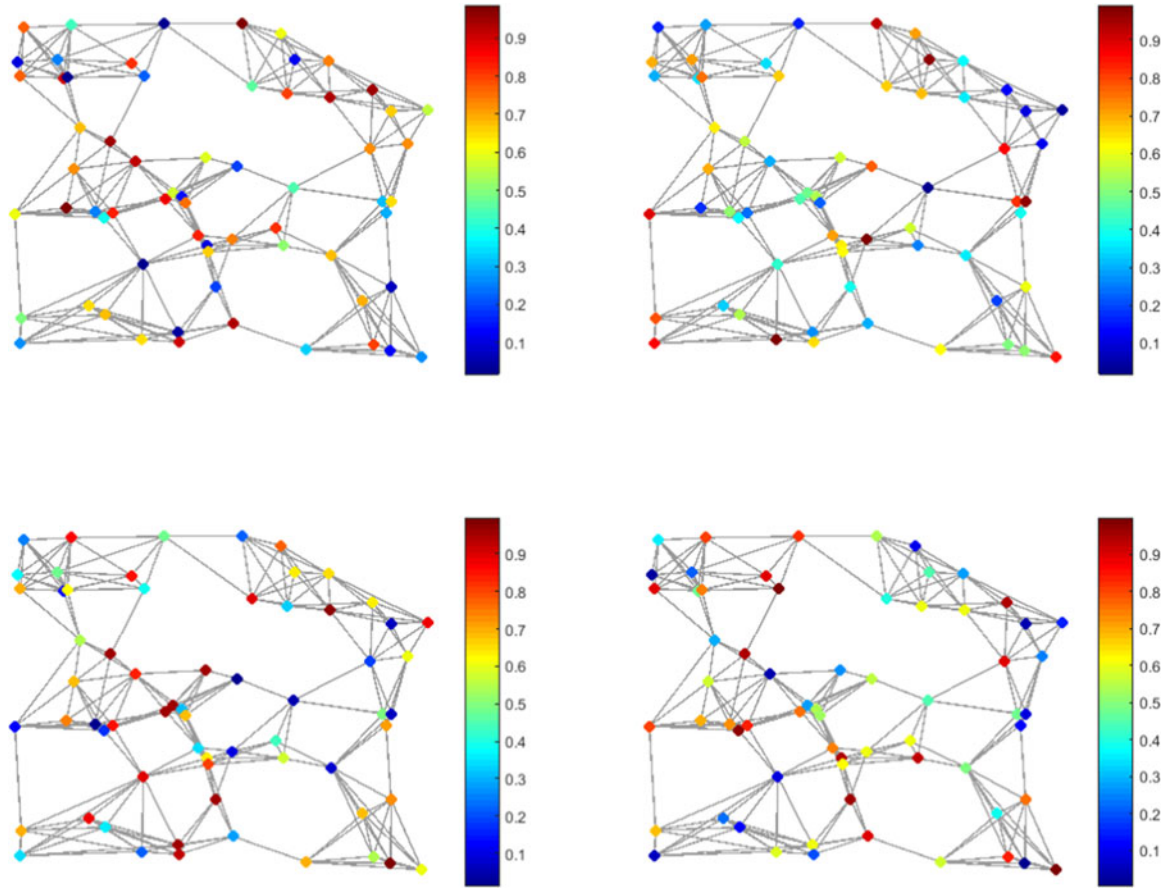

Fig. 1. Configuration of the sensors placement and their consecutive four normalized measurements.

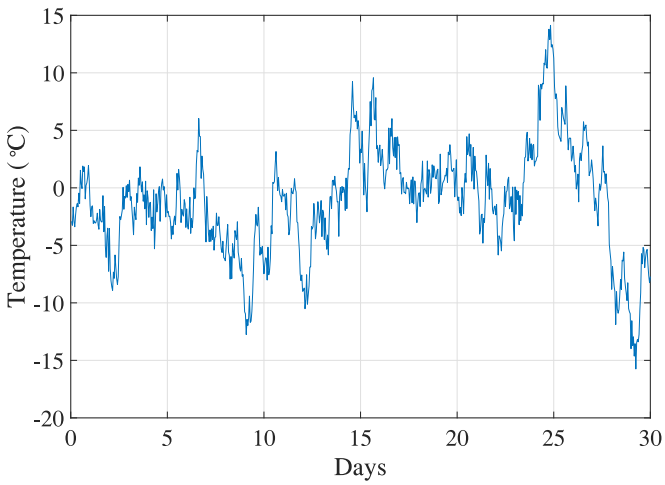

Fig. 2. Sample temperature sensor measurement in 30 days.

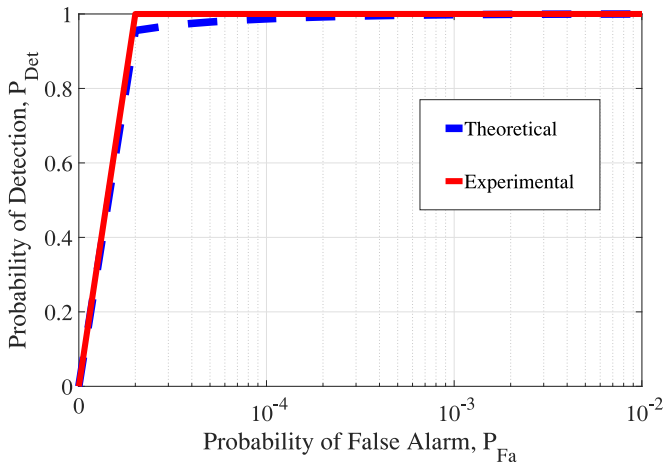

Fig. 3. Theoretical (dashed) and experimental (solid) ROC curves for the proposed intrusion detection method.

and (33). In view of this result, henceforth we use the theoretical means and variances.

In order to compare the performance of the proposed detector with that of the PCA-based [16], Clustering-based [30], GBF [37], local-GLRT [36], in terms of the ROC curves. For this purpose, we first obtain the ROC curves of the various methods for a predefined P_{Fa}. Fig. 4 shows the ROC curves for the various intrusion detection methods. It is seen from this figure that the proposed intrusion detection method has a superior performance to other methods, in terms of providing the highest probability of detection for a given probability of false alarm. Similar results have been obtained for various values of ξ. It should be noted that in the PCA-based method, we consider a robust Mahalanobis distance by replacing the sample covariance with the minimum covariance determinant. In addition, in the

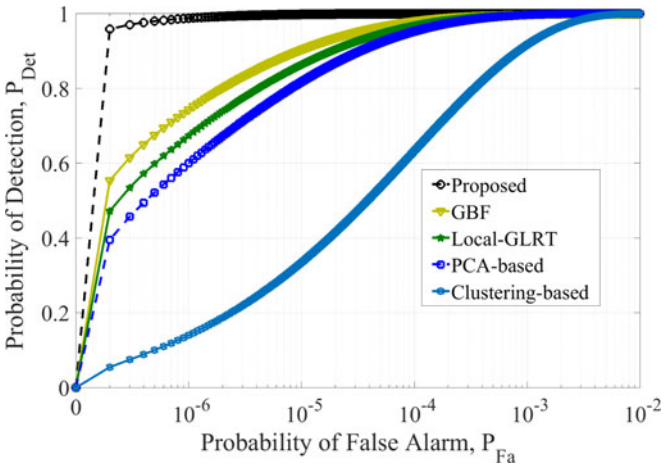

Fig. 4. ROC curves for various intrusion detection schemes when $\xi = 0.5$.

TABLE I
AREA UNDER ROC CURVES FOR VARIOUS INTRUSION DETECTION METHODS AND DIFFERENT VALUES OF ξ

ξ	Proposed	GBF	PCA-based	local-GLRT	Clustering
0.1	0.9315	0.7832	0.7337	0.7789	0.2573
0.3	0.9645	0.8434	0.7819	0.8260	0.3106
0.5	0.9823	0.8771	0.8382	0.8612	0.3837
0.7	0.9975	0.9124	0.8733	0.9009	0.4583

TABLE II
AVERAGED CPU TIMES (IN SECOND) REQUIRED BY VARIOUS DETECTORS

	Proposed	GBF	PCA-based	local-GLRT	Clustering
CPU time	5.27	4.62	2.39	6.36	2.88

GBF method θ_s is set to 0.9 and in the Clustering-based approach the number of clusters is set to 15. Next, the area under ROC curve is computed for various schemes. Table I gives the area under ROC curve for various methods for different values of ξ, for P_{Fa} in $\left[0, 10^{-4}\right]$. It is seen from this table that the proposed method yields the best performance in that it provides the largest value of area under ROC curve irrespective of the intrusion strength. In order to further investigate the performance of the proposed intrusion detection scheme, the temporal behavior of the network with anomalies imposed at different time instants are analyzed.

To compare the computational complexity of the proposed method to that of the other methods, we compute the required CPU time averaged over 50 runs, when the experiments are implemented in MATLAB on an Intel Core i5 2.8 GHz personal computer with 4 GB RAM. Table II gives the averaged CPU times required by the various intrusion detection methods. It is seen from this table that running time of our algorithm is in par with GBF, another graph-based approach, while its detection rate is significantly higher than this method.

To detect the anomalies over time, we incorporate the proposed *Bhattacharyya* distance mechanism as derived in Section IV. Fig. 5 shows the *Bhattacharyya* distance values between the two consecutive time instants. It is seen from this figure that the arrival of an unexpected observation over time is clearly visible at the time instants $k = \{20, ..., 30\}$ and $k = \{70, ..., 80\}$. Fig. 6 shows the distance between the two consecutive Laplacian matrices for $k = \{0, ..., 120\}$. It can be seen from this figure that the proposed method is very well capable of detecting the existence of any deviation from the normal behavior profile. It should be noted that the intrusions are generated at the same time instants as mentioned above.

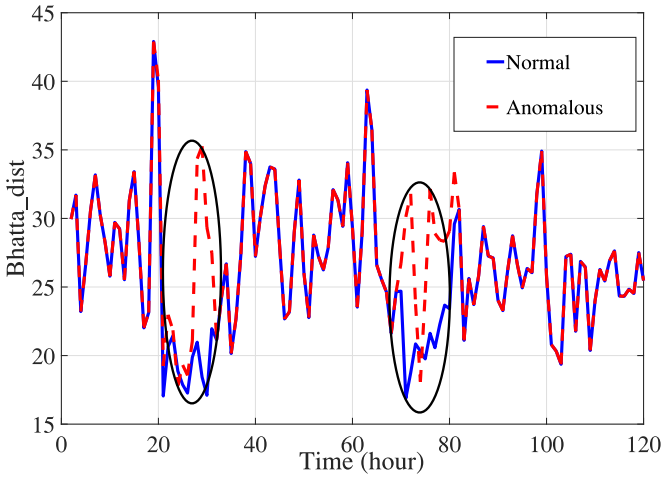

Fig. 5. *Bhattacharyya* distance values between $f_k(\boldsymbol{s})$ and $f_{k+1}(\boldsymbol{s})$.

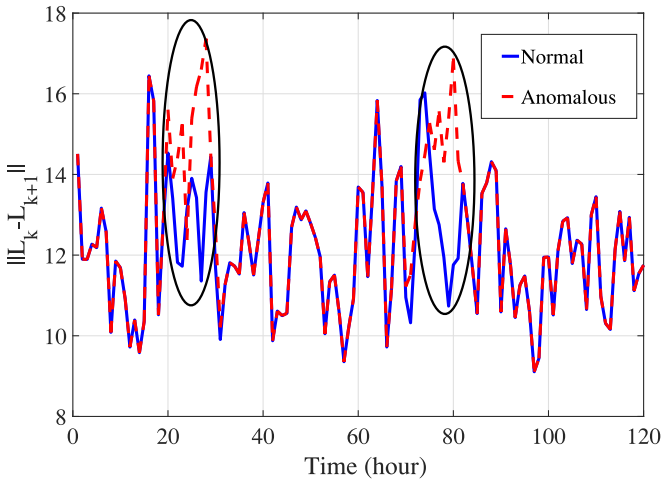

Fig. 6. Approximating the *Bhattacharyya* distance using the estimated Laplacian matrices for two consecutive time instants.

VI. CONCLUSION

In this paper, a new statistical-based intrusion detection scheme for distributed sensor networks has been proposed. The proposed method has been realized by constructing a graph signal from both the sensor measurements and placements, resulting in the corresponding similarity and Laplacian matrices. The proposed intrusion detector has been designed utilizing the Gaussian Markov random field distribution based on the

hypothesis testing and employing the log-likelihood ratio criterion. Closed-form expression for the test statistic has been derived and validated experimentally. The performance of the proposed intrusion detection scheme has been evaluated in detail by conducting several experiments. It has been shown that the proposed intrusion detection scheme provides a performance significantly superior to that of the other schemes as evidenced by the higher detection rate values. The temporal behavior of the proposed intrusion detection scheme has been evaluated by computing both the *Bhattacharyya* distance and its approximated version using the graph Laplacian matrices of the consecutive time instants. It has been shown that the proposed scheme is very well capable of detecting sensor measurement anomalies over time.

REFERENCES

[1] S. Deshmukh, B. Natarajan, and A. Pahwa, "State estimation over a lossy network in spatially distributed cyber-physical systems," *IEEE Trans. Signal Process.*, vol. 62, no. 15, pp. 3911–3923, Aug. 2014.

[2] A. Hahn and M. Govindarasu, "Cyber attack exposure evaluation framework for the smart grid," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 835–843, Dec. 2011.

[3] F. Pasqualetti, F. Dorfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," *IEEE Trans. Autom. Control*, vol. 58, no. 11, pp. 2715–2729, Nov. 2013.

[4] L. Xie, Y. Mo, and B. Sinopoli, "Integrity data attacks in power market operations," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 659–666, Dec. 2011.

[5] D. G. Eliades and M. M. Polycarpou, "A fault diagnosis and security framework for water systems," *IEEE Trans. Control Syst. Technol.*, vol. 18, no. 6, pp. 1254–1265, Nov. 2010.

[6] J. Kim, L. Tong, and R. J. Thomas, "Subspace methods for data attack on state estimation: A data driven approach," *IEEE Trans. Signal Process.*, vol. 63, no. 5, pp. 1102–1114, Mar. 2015.

[7] J. Zhang, R. S. Blum, X. Lu, and D. Conus, "Asymptotically optimum distributed estimation in the presence of attacks," *IEEE Trans. Signal Process.*, vol. 63, no. 5, pp. 1086–1101, Mar. 2015.

[8] Y. Mo and B. Sinopoli, "Secure estimation in the presence of integrity attacks," *IEEE Trans. Signal Process.*, vol. 60, no. 4, pp. 1145–1151, Apr. 2015.

[9] H. Fawzi, P. Tabuada, and S. Diggavi, "Secure estimation and control for cyber-physical systems under adversarial attacks," *IEEE Trans. Autom. Control*, vol. 59, no. 6, pp. 1454–1467, Jun. 2014.

[10] A. Vempaty, O. Ozdemir, K. Agrawal, H. Chen, and P. K. Varshney, "Localization in wireless sensor networks: Byzantines and mitigation techniques," *IEEE Trans. Signal Process.*, vol. 61, no. 6, pp. 1495–1508, Mar. 2013.

[11] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection: A survey," *ACM Comput. Survey*, vol. 41, no. 3, pp. 15:1–15:58, 2009.

[12] M. Xie, S. Han, B. Tian, and S. Parvin, "Anomaly detection in wireless sensor networks: A survey," *J. Netw. Comput. Appl.*, vol. 34, no. 4, pp. 1302–1325, 2011.

[13] H. Dong, Z. Wang, S. X. Ding, and H. Gao, "A survey on distributed filtering and fault detection for sensor networks," *Math. Problems Eng.*, vol. 2014, no. 858–624, 2014.

[14] C. OReilly, A. Gluhak, M. A. Imran, and S. Rajasegarar, "Anomaly detection in wireless sensor networks in non-stationary environment," *IEEE Commun. Surveys Tut.*, vol. 16, no. 3, pp. 1413–1432, Oct.–Dec. 2014.

[15] H. Huang, H. Al-Azzawi, and H. Brani, "Network traffic anomaly detection," arxiv:1402.0856v1, 2014.

[16] R. Kwitt and U. Hofmann, "Unsupervised anomaly detection in network traffic by means of robust PCA," in *Proc. Int. Multi-Conf. Comput. Global Inf. Technol.*, 2007, pp. 37–40.

[17] B. Zhang, J. Yang, J. Wu, D. Qin, and L. Gao, "PCA-subspace method—Is it good enough for network-wide anomaly detection", in *Proc. IEEE Network Operations Manage. Symp.*, 2012, pp. 359–367.

[18] M. A. Livani and M. Abadi, "Distributed PCA-based anomaly detection in wireless sensor networks," in *Proc. 5th Int. Conf. Internet Technol. Secured Trans.*, 2010, pp. 1–8.

[19] D. I. Shuman, S. K. Narang, P. Frossard, A. Ortega, and P. Vandergheynst, "The emerging field of signal processing on graphs: Extending high-dimensional data analysis to networks and other irregular domains," *IEEE Signal Process. Mag.*, vol. 30, no. 3, pp. 83–98, May 2013.

[20] A. Sandryhaila and J. M. F. Moura, "Discrete signal processing on graphs," *IEEE Trans. Signal Process.*, vol. 61, no. 7, pp. 1644–1656, Apr. 2013.

[21] A. Lakhina, M. Crovella, and C. Diot, "Mining anomalies using traffic feature distributions," in *Proc. ACM SIGCOMM*, 2005, pp. 217–228.

[22] A. Kind, M. P. Stoecklin, and X. Dimitropoulos, "Histogram-based traffic anomaly detection," *IEEE Trans. Netw. Service Manage.*, vol. 6, no. 2, pp. 110–121, Jun. 2009.

[23] G. Nychis, V. Sekar, D. G. Andersen, H. Kim, and H. Zhang, "An empirical evaluation of entropy-based traffic anomaly detection," in *Proc. 8th ACM SIGCOMM Conf. Internet Meas.*, 2008, pp. 151–156.

[24] H. Ringberg, A. Soule, J. Rexford, and C. Diot, "Sensitivity of PCA for traffic anomaly detection," in *Proc. SIGMETRICS*, 2007.

[25] G. E. P. Box, *Time Series Analysis: Forecasting and Control*. London, U.K.: Pearson Education, 1994.

[26] P. Brockwell and R. Davis, *Introduction to Time Series and Forecasting*. Berlin, Germany: Springer, 1996.

[27] S. Muthukrishnan, "Data streams: Algorithms and applications," Man uscript based on invited talk from 14th SODA, 2003. [Online]. Available: http://www.cs.rutgers.edu/muthu/stream-1-1.ps

[28] P. Barford, J. Kline, D. Plonka, and A. Ron, "A signal analysis of network traffic anomalies," in *Proc. Internet Meas. Workshop*, 2002, pp. 71–82.

[29] W. Lee and D Xiang, "Information-theoretic measures for anomaly detection," in *Proc. IEEE Symp. Security Privacy*, 2001, pp. 130–143.

[30] S. Rajasegarar, C. Leckie, and M. Palaniswami, "Hyperspherical cluster based distributed anomaly detection in wireless sensor networks," *J. Parallel Distrib. Comput.*, vol. 74, pp. 1833–1847, 2014.

[31] T. Ide and H. Kashima, "Eigenspace-based anomaly detection in computer systems," in *Proc Knowledge Discovery Data Mining*, 2004, pp. 440–449.

[32] B. A. Miller, N. T. Bliss, and P. J. Wolfe, "Subgraph detection using eigenvector l_1 norms," in *Proc. Neural Inf. Process. Syst.*, 2010, pp. 1633–1641.

[33] C. C. Noble and D. J. Cook, "Graph-based anomaly detection," in *Proc. 9th ACM SIGKDD*, 2003, pp. 631–636.

[34] M. Crovella and E. Kolaczyk, " Graph wavelets for spatial traffic analysis," in *Proc. INFOCOM*, 2003, vol. 3, pp. 1848–1857.

[35] P. Papadimitriou, A. Dasdan, and H. Garcia-Molina, "Web graph similarity for anomaly detection," *J. Internet Services Appl.*, vol. 1, no. 1, pp. 19–30, 2010.

[36] J. Fang and H. Li, "Distributed event-region detection in wireless sensor networks," *EURASIP J. Adv. Signal Process.*, vol. 2008, 2008, Art. no. 287870.

[37] H. E. Egilmez and A. Ortega, "Spectral anomaly detection using graph-based filtering for wireless sensor networks," in *Proc. IEEE Int. Conf. Acoustic, Speech, Signal Process.*, 2014, pp. 1085–1089.

[38] H. Sadreazami, A. Asif, and A. Mohammadi, "Data-adaptive color image denoising and enhancement using graph-based filtering," in *Proc. IEEE Int. Symp. Circuits Syst.*, 2017, pp. 2751–2754.

[39] H. Sadreazami, A. Asif, and A. Mohammadi, "Iterative graph-based filtering for image abstraction and stylization," *IEEE Trans. Circuits Syst. II, Express Briefs*, to be published.

[40] H. Rue and L. Held, *Gaussian Markov Random Fields: Theory and Applications*. London, U.K.: Chapman and Hall/CRC, 2005.

[41] C. Zhang and D. Florencio, "Analyzing the optimality of predictive transform coding using graph-based models," *IEEE Signal Process. Lett.*, vol. 20, no. 1, pp. 106–109, Jan. 2013.

[42] C. Zhang, D. Florencio and P. A. Chou, "Graph signal processing—A probabilistic framework," Microsoft Research, Redmond, WA, USA, Tech. Rep., MSR-TR-2015-31, 2015.

[43] J. Friedman, T. Hastie, and R. Tibshirani, "Sparse inverse covariance estimation with the graphical lasso," *Biostatistics*, vol. 9, no. 3, pp. 432–441, 2008.

[44] I. Rotondo, G. Cheung, A. Ortega, and H. Egilmez, "Designing sparse graphs via structure tensor for block transform coding of images," in *Proc. Asia Pacific Signal Inf. Process. Assoc. ACS*, 2015, pp. 571–574.

[45] X. Dong, D. Thanou, P. Frossard, and P. Vandergheynst, "Laplacian matrix learning for smooth graph signal representation," in *Proc. IEEE Int. Conf. Acoustics, Speech, Signal Process.*, 2015, pp. 3736–3740.

[46] X. Dong, D. Thanou, P. Frossard, and P. Vandergheynst, "Learning Laplacian matrix in smooth graph signal representations," *IEEE Trans. Signal Process.*, vol. 64, no. 23, pp. 6160–6173, Dec. 2016.

[47] H. E. Egilmez, E. Pavez, and A. Ortega, "Graph learning from data under structural and Laplacian constraints," *IEEE J. Selected Topics Signal Process.*, vol. 11, no. 6, pp. 825–841, 2017.
[48] H. E. Egilmez, E. Pavez, and A. Ortega, "Graph learning with Laplacian constraints: modeling attractive Gaussian Markov random fields," in *Proc. 50th Asilomar Conf. Signals, Syst. Comput.*, 2016, pp. 1470–1474.
[49] A. Mohammadi and K. N. Plataniotis, "Improper complex-valued *Bhattacharyya* distance," *IEEE Trans. Neural Netw. Learning Syst.*, vol. 27, no. 5, pp. 1049–1064, May 2016.
[50] T. Kailath, "The divergence and *Bhattacharyya* distance measures in signal selection," *IEEE Trans. Commun. Technol.*, vol. CT-15, no. 1, pp. 52–60, Feb. 1967.
[51] F. K. Chung, *Spectral Graph Theory* (CBMS Regional Conference Series in Mathematics, vol. 92). Providence, RI, USA: AMS Bookstore, 1997.
[52] H. Sadreazami, A. Asif and A. Mohammadi, "Image stylization using iterative graph filtering," in *Proc. IEEE Canadian Conf. Elect. Comput. Eng.*, 2017, pp. 1–4.
[53] H. Sadreazami, A. Asif and A. Mohammadi, "A late adaptive graph-based edge-aware filtering with iterative weight updating process," in *Proc. IEEE Mid-West Symp. Circuits Syst.*, 2017, pp. 1581–1584.
[54] S. M. Kay, *Fundamentals of Statistical Signal Processing: Detection Theory*. Upper Saddle River, NJ, USA: Prentice-Hall, 1998.
[55] A. Papoulis, *Probability, Random Variables, and Stochastic Processes*. New York, NY, USA: McGraw-Hill, 1991.

Authors' photograph and biography not available at the time of publication.