A Graph Signal Processing Framework for Detecting and Locating Cyber and Physical Stresses in Smart Grids

Md Abul Hasnat, *Student Member, IEEE*, and Mahshid Rahnamay-Naeini, *Senior Member, IEEE*

***Abstract*—Monitoring the smart grid involves analyzing continuous data-stream from various measurement devices deployed throughout the system, which are topologically distributed and structurally interrelated. In this paper, a graph signal processing (GSP) framework is used to represent and analyze the interrelated smart grid measurement data for security and reliability analyses. The effects of various cyber and physical stresses in the system are evaluated in different GSP domains including vertex domain, graph-frequency domain, and the joint vertex-frequency domain. Two novel techniques based on vertex-frequency energy distribution, and the local smoothness of graph signals are proposed and their performance have been evaluated for detecting and locating various cyber and physical stresses. Based on the presented analyses, the proposed techniques show promising performance for detecting sophisticated stresses with no sharp changes at the onset, for detecting abrupt load changes, and also for locating stresses.**

***Index Terms*—Smart grid security, cyber attack, graph signal processing, local smoothness, vertex-frequency representation.**

NOMENCLATURE

Graph and Related Sets

$\mathbf{L}$	Graph Laplacian Matrix.
$\mathcal{E}$	Set of all transmission lines (edges).
$\mathcal{G}$	Graph associated with the power system (i.e., domain of the graph signal).
$\mathcal{V}_{\mathcal{A}}$	Set of all buses (vertices) under cyber attack.
$\mathcal{V}_{\mathcal{R}}$	Set of all buses (vertices) the attackers have access to record data.
$\mathcal{V}$	Set of all buses (vertices).
d_{ij}	Geographical distance between bus i and j.
e_{ij}	Link between vertex v_i and v_j.
l_{ij}	Entry of row i and column j of $\mathbf{L}$.
w_{ij}	Weight of the link e_{ij}.
λ_k	$k-$th eigenvalue of $\mathbf{L}$.

Signals and Instantaneous Quantities

$\eta(n,t)$	Difference in VFED marginalized over graph-frequency components.
$\gamma(t)$	Amount of high frequency component at time t.
$\hat{X}(\lambda_k,t)$	GFT of the graph signal $x(n,t)$ at time t.
θ_ψ	Threshold likelihood for the random variable ψ.
$\underline{\mathbf{x}}$	Graph signal $x(n)$ in vector form.
$E(n,k,t)$	VFED of the graph signal $x(n,t)$ at time t.
$H(\lambda)$	High-pass graph filter.
$l_x(n)$	$n-$ th element of the vector $\mathbf{L}\underline{\mathbf{x}}$.
$p_\psi(\zeta)$	Probability distribution of random variable ψ.
$q(t)$	Additive white Gaussian noise (AWGN) added to voltage angle time-series.
$s(n,t)$	Local smoothness at time, t.
$u_k(n)$	$k-$th eigenvector of $\mathbf{L}$, basis signal for GFT.
$x(n,t)$	Bus voltage angle time-varying graph signal.
$x(v_n), x(n)$	Graph Signal.
$c(t)$	Corrupted time-series under cyber attack (general model).

Constants

α	Ratio of the load change amount relative to the original load size.
β	Load change scaling factor, $1-\alpha$.
$\sigma^2_{n_A}$	Variance of white noise at bus n_A.
a	Accuracy of detection.
d	Amount of delay in delay attack (in samples).
LA	Location accuracy.
m	Slope of the ramp attack.
N	Cardinality of the set $\mathcal{V}$.
t_{End}	Ending time of an attack.
t_{Start}	Starting time of an attack.
x'	The magnitude of difference between the false data injected and true value in FDIA.

I. INTRODUCTION

The availability of large volume of energy data in smart grids provides extensive opportunities to support their critical functions. In recent years, various data analytics and machine learning techniques have been applied to analyze energy data in order to supplement or enhance traditional power grid monitoring and control functions. In this paper, a Graph Signal Processing (GSP) framework [1], [2] has been exploited for representation and analyses of smart grids data, particularly to support the monitoring function for their reliable and secure operation.

GSP is a fast-growing field, which extends the classical signal processing techniques and tools to irregular graph domain instead of the Euclidean domain. GSP is suitable for analyzing structured data and the dynamics of systems with interconnected components, such as those of smart grids. Particularly, it is shown that by representing the smart grid data using *graph signals*, one can exploit the rich tools that GSP framework provides to analyze the implicit structures in the

Md A. Hasnat is with the Department of Electrical Engineering, University of South Florida, Tampa, FL 33620 USA (e-mail: hasnat@usf.edu).

Mahshid R. Naeini is with the Department of Electrical Engineering, University of South Florida, Tampa, FL 33620 USA (e-mail: mahshidr@usf.edu).

Corresponding author: Md Abul Hasnat.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2022.3177154, IEEE Transactions on Smart Grid

smart grid data for security and reliability analyses. In general, for analyzing data from complex networked systems, such as smart grids, their physical topology, as well as the structured interactions (model-based or data-driven interactions [3]) among the components are of immense importance. While connectivities and interactions cannot be captured by classical signal processing approaches, GSP provides a framework to capture such information in graph signals.

The reliability and security of smart grids, as critical infrastructures, are of utmost importance. Smart grids maintain their proper functioning by continuous acquisition and processing of measurement data. Any attack on the availability and integrity of measurement data can lead to improper decisions and actions, which may result in severe consequences and instability of the system. Examples of such attacks include denial of service (DoS) attack [4], data-replay attack [5], ramp attack [6] and false data injection attack (FDIA) [4], which have been extensively studied in smart grids' literature. These attacks can be launched on the supervisory control and data acquisition (SCADA) readings as well as on the time-stamped synchrophasor measurements from the phasor measurement units (PMUs). In real-world, these attacks can be launched by unauthorized access and compromising various cyber elements of the system, ranging from sensing and monitoring devices (such as PMUs), communication channel, data processing servers, and more. In addition to cyber stresses, physical stresses can also affect the reliability and stability of the system. Examples of such stresses include line and generator failures, and abrupt load changes. In this paper, the term *stress* is used to refer to any kind of cyber or physical anomaly that can threaten the smooth operation of the system.

To ensure seamless monitoring, control, and operation of smart grids, it is essential to enhance the situational awareness toward cyber and physical stresses. To do so, in this paper, properties and characteristics of graph signals associated with the power grid measurements (e.g., bus voltage angles) are analyzed in various GSP domains including vertex domain, graph-frequency domain, and the joint vertex-frequency domain. Based on the effects of different stresses on the vertex-frequency energy distribution (VFED) [7] and the local smoothness (LS) [8] of the graph signals, two novel GSP-based stress detection techniques are proposed. These techniques also enable stress localization in the smart grid. To the best of our knowledge, this is the first work, which introduces VFED and LS-based techniques in analyzing smart grid's data for stress detection and localization. The proposed technique based on LS, is named *local smoothness second time-derivative (LSSTD)* and is particularly effective for detecting and locating the designed cyber attacks and physical stresses. For evaluation of the proposed techniques, abrupt load change (as the physical stress) and five types of cyber attacks with smooth transitions of signal values at the onset of the attack are modeled on the time-series representation of the bus voltage angle measurement values. These carefully designed attacks with smooth change of values at the onset are challenging to detect for many existing stress detection techniques. The performance of the proposed techniques are evaluated in comparison with the graph Fourier transform (GFT)-based detection technique [9], [10], as a GSP-based benchmark technique, and other non-GSP-based techniques including support vector machine (SVM), decision tree (DT), long short-term memory (LSTM) and techniques directly analyzing the time-series data, such as three sample quadratic prediction algorithm (TSQPA) [6]. The proposed GSP-based techniques show promising performance and also address some of the limitations of the GFT-based technique for detecting stresses with no sharp changes at the onset, for detecting abrupt changes in load demand, and for locating stresses. The main contribution of this paper can be summarized as follows:

- A general GSP framework for modeling power system states as graph signals is presented in order to exploit the knowledge of interaction and interconnection among the components of the system in analyzing energy data.
- A novel technique, named LSSTD, is proposed, which is based on analyzing the time-varying graph signal model of the smart grid voltage angle signals. It is shown that the LSSTD method performs well in detecting and locating challenging cyber and physical stresses with no abrupt change at the attack onset.
- A novel technique based on analyzing the vertex-graph-frequency representation of power system graph signals, namely VFED, is proposed for stress detection and localization. Although the detection accuracy of this method is not as high as the first proposed technique, it outperforms LSSTD in locating the physical stresses (i.e., the abrupt load change cases). The key merits of this method can be recognized by its new graph signal-analytical perspective and providing a new approach in locating complex physical stresses.
- A detailed analysis and discussion on the performance of the presented techniques compared to other GSP-based and non-GSP-based techniques are presented to reveal the advantages of time-varying GSP-based techniques.

II. Related Works

In this section, the related works are briefly reviewed in two categories including the developments in the area of GSP and smart grids security. Over the last decade, GSP has emerged and extended the concepts of classical signal processing to the irregular graph domain. Several works have been published on the interpretation of the frequency domain in the context of graph signals [1], [2]. The tools and theories built based on these interpretations allow studying graph signals in a new domain with a similar notion to the frequency domain for classical signals. For instance, the relationship between the graph signal frequency and the eigenvalues of the graph Laplacian as well as various concepts related to the graph signal frequency, e.g., global and local smoothness of signals, graph filtering, and modulation of graph signals have been discussed [1], [2]. Recently, GSP techniques have been used in various application domains including sensor arrays and networks [13], transportation systems [14], electrocardiogram (ECG) and electroencephalogram (EEG) signal analysis [15], [16], image, and video processing [17] and smart grids [9],

[11]. Specifically, researchers have shown that GSP can be a prospective field for detecting anomalies in different types of networks and their associated signals [18].

The application of GSP to smart grids is recent and limited so far. For instance, Kroizer *et al.* in [19] approximated the non-linear measurement functions in the power grid as the output of a graph filter and proposed a regularized least-squares estimator for signal recovery based on the inverse of the obtained graph filter. Ramakrishna and Scaglione [11] modeled the voltage phasor measurements in the power grid as the output of the low-pass graph filter in response to the low-rank excitation that comes from the generators. This developed GSP model has been used in several smart grid applications such as inferring the power grid topology as a Laplacian learning problem, detection of false data, and PMU data compression. Sampling and reconstruction of graph signals to provide observability in the smart grid under cyber attacks or under selective PMU placement have also been discussed in our earlier work [20].

Smart grid's security and reliability have been the focus of many researchers for decades. Different techniques for detecting and locating cyber and physical stresses in smart grids have been proposed in the literature based on both the traditional *supervisory control and data acquisition* (SCADA) measurements as well as the high-frequency PMU measurements. The detection methods based on state estimation of power systems are well suited for the SCADA-based static monitoring while the time-series prediction-based methods exploiting the space-time relationship among the states are more applicable to PMU-based dynamic system monitoring [21]. Examples of data-driven approaches for detecting and locating stresses in power systems include principle component analysis (PCA) and dimensionality-reduction-based methods [22], [23], spatial and temporal correlation-based methods [24], neural network-based methods [25], and linear minimum mean square error (MMSE) estimation technique [26].

Detection and determining the location of cyber attacks in the smart grid using GSP is a new domain. In our earlier work [27], [28], the effects of cyber and physical stresses on the associated power system's graph signals in the vertex and graph-frequency domains are discussed. Drayer and Routtenberg [9] proposed a GFT-based detection method for FDIA in smart grids. In the later work, it is assumed that the graph signal associated with the bus voltage angles of the power system is smooth and for this reason, the high-frequency components (corresponding to the large eigenvalues of the graph Laplacian) of the graph signals would be insignificant. The existence of the false data is proposed to be detected based on the existence of significant high-frequency components. Moreover, in [29], the authors proposed locating FDIA using graph modulation. In the work by Ramakrishna and Scaglione [11], the voltage phasor measurement model developed based on GSP is utilized to detect FDIA in smart grids. Anderson and Yu [30] proposed a physics-based graph construction technique specifically for three-phase distribution systems and used the lower dimensional representation of the GFTs associated with the voltage magnitude graph signals to identify bad data in the SCADA measurements. Shi *et. al* in [31] proposed a GSP-based technique to sort the PMUs so that the PMUs with strong correlation in measurements are kept together in the PMU data tensor, which is the input for a deep-learning model for event detection and classification.

In the current paper, novel GSP-based techniques based on VFED and LS are presented, which address some of the limitations of the existing methods in detecting and locating stresses with no abrupt changes at the onset of the attack in smart grids.

III. Review of GSP and Energy Graph Signals

A. Preliminaries and Definitions

The first important definition in GSP is the definition of the graph signal. While in classical signal processing, signals are defined by Euclidean representation of their values; in GSP, the graph signals are defined by the values residing on vertices $\mathcal{V}$ (i.e., $\mathcal{V} = \{v_1, v_2, ..., v_N\}$), which are connected over graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ with $\mathcal{E}$ representing the set of links (i.e., $\mathcal{E} = \{e_{ij} : (i, j) \in \mathcal{V} \times \mathcal{V}\}$). The graph signal can formally be represented by a vector of values denoted by $\underline{\mathbf{x}}$ with size N defined as $x : \mathcal{V} \to \mathbb{R}$. The graph signal can be denoted by $x(n)$ instead of $x(v_n)$ for simplicity.

B. Defining graph domain for power grids

In this paper, our discussion will be limited to the *bus-vertex* graph: a weighted undirected graph in which buses are considered as the vertices and the transmission lines or the branches are considered as the edges. Note that the above graph is based on the physical topology of the power system. However, the interactions among the components of the power system can be beyond the physical topology. As such, other methods of constructing a graph domain for power grids can also be used. For instance, the data-driven and electric-distance-based methods discussed in [3], can be used to infer and construct graph domains for power grids beyond their physical connectivities (when needed depending on the analyses of interest). In this paper, the geographical distance between buses i and j is denoted by d_{ij} and the weight corresponding to the edge e_{ij} in the bus-vertex graph $\mathcal{G}$ is defined as $w_{ij} = \frac{1}{d_{ij}}$, if there is an edge between node i and node j (i.e., $e_{ij} = 1$) and $w_{ij} = 0$, otherwise (if there is no edge between node i and node j, i.e., $e_{ij} = 0$). Graph Laplacian matrix $\mathbf{L}$, with l_{ij} elements, is also defined as $l_{ij} = \sum_{j=1}^{N} w_{ij}$ if $i = j$ and $l_{ij} = -w_{ij}$, otherwise. Since, the graph Laplacian, $\mathbf{L}$ is a real and symmetric matrix, it has real and non-negative eigenvalues corresponding to the orthonormal set of eigenvectors. The Laplacian matrix of the graph will be used later in defining the frequency domain representation of graph signals.

C. Representation of Power System Measurements as Graph Signals: Vertex Domain Representation

In this paper, the measurement values associated with each vertex i.e. bus voltage angles for $\mathcal{G}$ at a time instance are considered as a graph signal. Fig. 1 illustrates an example of a graph signal based on the voltage angles of all the buses for the IEEE 118 bus system [32]. It is assumed that the signal

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2022.3177154, IEEE Transactions on Smart Grid

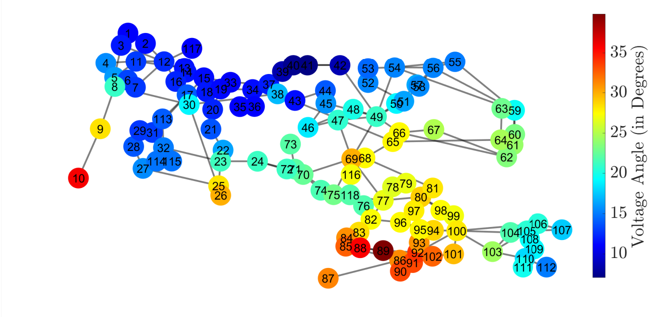


Fig. 1: Voltage angle measurements at a particular time instance as a graph signal on the IEEE 118 bus system.

values are available at all the buses of the grid (i.e., vertices of the graph). To realize this assumption, it can be further assumed that PMUs are available at every bus of the system. Alternatively, to relax this assumption based on real-world scenarios with selective PMU placement, it can be assumed that the signal values are available either directly from the measurement devices mounted on the buses (e.g., PMUs) or through state estimation using the measurements from other buses. However, the state estimation process to obtain the graph signal values and its performance are not directly a concern in this work. While state estimation is not the focus of this work, the proposed techniques can detect anomalies resulted in the state estimation process as well (for instance, due to cyber attacks). The anomalies considered in the graph signals in this work follow the models discussed in Section IV and are applied to the graph signals with complete signal values at all the buses. The graph signal values at different time instances can be modeled as time-series associated with each vertex and the resultant graph signal becomes a function of time, i.e., a time-varying graph signal that has been discussed in subsequent subsections.

D. Spectral Characteristics of Power Grid's Graph Signal - Graph-Frequency Domain

Analogous to the concept of Fourier transform and frequency domain representation of the signal in classical signal processing, the graph Fourier transform (GFT) of a graph signal $x(n)$ is defined as:

$$\hat{X}(\lambda_k) = \sum_{n=1}^{N} x(n) u_k(n), \quad (Analysis \quad equation) \qquad (1)$$

and the inverse graph Fourier transform (IGFT) is:

$$x(n) = \sum_{k=1}^{N} \hat{X}(\lambda_k) u_k(n), \quad (Synthesis \quad equation) \qquad (2)$$

Here, $u_k(n)$ is the basis graph signal for the GFT, which plays a similar role to the role of complex exponential signal in classical Fourier transform. Here, $u_k(n)$ is considered as the eigenvectors of the graph Laplacian $\mathbf{L}$, where subscript k denotes the $k-$th eigenvector and n is the index of $n-$th node in the graph $\mathcal{G}$. The corresponding eigenvalues to these eigenvectors are denoted by λ_k, which are considered as the graph-frequencies, and $0 = \lambda_1 < \lambda_2 < \lambda_3 < ... < \lambda_N$. The first eigenvalue $\lambda_1 = 0$ is analogous to the zero-frequency (DC component) in the case of temporal signals. The eigenvectors with lower/higher eigenvalues (i.e., smaller/larger k) correspond to lower/higher frequency components with less/more variation of values over vertices in a local neighborhood. In contrast to the basis functions in classical Fourier transform (i.e. complex exponential), the graph Laplacian eigenvectors are localized in the vertex domain.

E. Local Smoothness of Graph Signals

The smoothness measure of a signal quantifies how rapidly the values of the signal change. While the global smoothness [12] of a graph signal provides an overall measurement of the smoothness of a graph signal, the local smoothness associated with the graph signal, defined as $s(n) = \frac{l_{\mathbf{x}}(n)}{x(n)}$ for $x(n) \neq 0$, specifies how fast the values of the graph signal $x(n)$ change from vertex to vertex in the vicinity of the $n-$th vertex. Here $l_{\mathbf{x}}(n)$ is the $n-$th element of the vector, $\mathbf{Lx}$. The work by Daković et al. [8] shows that the concept of local smoothness in the graph signal is analogous to the concept of instantaneous frequency in classical signal processing.

F. Joint Vertex-Frequency Representations

In classical signal processing, the joint time-frequency representations of signals (e.g., spectrogram, windowed Fourier transform, wavelets, etc.) are used for the time-localization of a particular frequency component. The joint vertex-frequency representations serve a similar purpose for graph signals. In GSP, there are different approaches for localization of the frequency components in the literature. For example, Stanković *et al.* [7] propose localized vertex spectrum (LVS) of graph signal $x(n)$ as:

$$LVS_x(n, \lambda_k) = \sum_{m=1}^{N} x(m) h(n-m) u_k(m), \qquad (3)$$

where $h(n)$ is the window function. This approach has a major drawback of being dependent on the width and the characteristics of the window function. Instead, for improving the localization of the signal energy in the joint vertex-frequency domain, the VFED is introduced in [7], which does not require any window. The VFED, $E(n, k)$ is calculated from the graph signal using the equation:

$$E(n, k) = \sum_{m=1}^{N} x(n) x(m) u_k(m) u_k(n). \qquad (4)$$

G. Time-Varying Graph Signals

In our previous discussions, we have only considered the graph signal at a single time instant. However, in dynamic systems, such as power grids, the values of the signal at each node vary in time. For instance, the bus voltage measurements in power grids change in time because of changes in load demand and other changes in the power system. As a result, the graph signal $x(n)$ changes in time. Therefore, a time-varying graph signal can be thought of as a function of both vertex and time and can be denoted by $x(n, t)$. While dynamic time-varying graph signals are considered here, we assume that the underlying graph of the system (vertices and links) remains unchanged during the analyses. If the underlying graph of the system and consequently graph of the graph signal change, then the set of eigenvectors and thus the basis of GFT will change, which make the frequency analyses of graph signals before and after the graph change incomparable. For time-varying graph signal $x(n,t)$, the spectral representations, as well as the global and local smoothness of the graph signals also change with time. In this paper, the $k-$th eigenvalue, the $k-$th eigenvector, the GFT, the VFED, and the local smoothness at time t will be denoted by $\lambda_k(t), u_k(t), \hat{X}(\lambda_k,t)$, $E(n,k,t)$, and $s(n,t)$, respectively.

IV. Stress models

A. Cyber Attack Models

In this section, the approach for modeling the effects of different types of cyber attacks on the time-varying voltage angle graph-signals in smart grids are discussed. Specifically, five types of cyber attacks including DoS attack, replay attack, ramp attack, delay attack, and a special form of FDIA have been considered. For modeling cyber attacks in graph signal domain, let us consider a set of vertices, $\mathcal{V}_{\mathcal{A}} \subset \mathcal{V}$ is under attack within the time interval t_{start} to t_{end}. The corrupted signal in the generalized cyber attack model can be expressed as follows:

$$x(n_A,t) = c(t), \quad for \quad t_{start} \leq t \leq t_{end}, \quad and \quad n_A \in \mathcal{V}_{\mathcal{A}}. \tag{5}$$

The corrupted signal $c(t)$ can be defined to model and capture the effects of various types of attacks as will be discussed next. Fig. 2, illustrates different types of cyber attacks on the time-series, $x(105,t)$, which is associated with the time-varying values of the graph signal $x(n,t)$ at vertex/bus 105 in the IEEE 118 bus system.

1) Denial-of-service (DoS Attack): In a DoS attack, the attackers can prevent the communication of measurement values (at certain parts of the system) to the data collection and monitoring system, for instance through overloading network resources. In cyber security literature, DoS attacks are often modeled as the absence of measurement signal at the attack location [4]. As a result, the data collection and monitoring system receives only the measurement noise from t_{start} to t_{end} from the attacked location, which creates an abrupt change of signal value at t_{start}. To make the attack model more challenging, in this work, the DoS attack is modeled as the suspension of updating the time-series measurements at the attack location. As a result, the corrupted measurements appear to be a constant value during the attack (i.e., the value at the onset of the attack, $x(n_A,t_{start})$ plus noise). More specifically, the model for this attack considers $c(t) = x(n_A,t_{start}) + q(t)$, where $q(t)$ is the additive white Gaussian noise with zero mean and variance $\sigma^2_{n_A}$. In Fig. 2, the example DoS attack starts at time 5 and ends at time 6.

2) False Data Injection Attack (FDIA): FDIA involves sophisticated false data designing methods to deceive the traditional bad data detection techniques associated with the state estimation and monitoring mechanisms. The most common strategy of FDIA in smart grids from literature, designs the FDIA based on the power system state estimation framework with $\mathbf{z} = \mathbf{h}(\mathbf{y})$, where $\mathbf{z}$ and $\mathbf{y}$ are the measurements and the states of the power system, respectively. The non-linear function $\mathbf{h}$ relates measurements and states. The traditional bad data detector declares a set of measurements $\mathbf{z}$ as bad data if the residue of state estimation $r = ||\mathbf{z} - \mathbf{h}(\hat{\mathbf{y}})||_2$ exceeds a threshold τ, where $\hat{\mathbf{y}}$ is the estimated states. To bypass the bad data detector, the attacker injects a false measurement $\mathbf{z_{FDIA}} = \mathbf{z} + \mathbf{a}$ in such a way that the residue, $||\mathbf{z_{FDIA}} - \mathbf{h}(\hat{\mathbf{y}})||_2 \leq \tau$. In this work, the bus voltage angles are considered as the state of the power system and the measurements are taken in the form of bus voltage angles. It is also assumed that the state values of the nodes are obtained either by mounting measurement devices (e.g., PMU) on every bus or by estimating the voltage angle of buses with the available measurement devices at other buses. In this paper, a special type of FDIA is considered, which does not introduce any sharp change at the onset of the attack and is thereby challenging to be detected by many detection mechanisms. To model this type of FDIA in the general cyber attack model in equation (5), $c(t)$ can be defined as $c(t) = x(n_A,t) + (-1)^b x'$, where $b \in \{0,1\}$, $|x'|$ is considered to be a very small value that the injected false datum does not create any easily detectable abrupt change at the onset of the attack and also bypasses the bad-data detector embedded into the state estimation system. In other words, the FDIA in this paper is designed such that the absolute value of the difference of the true datum and the falsified datum change, i.e., x', to be smaller than the detector threshold τ. In Fig. 2, the example FDIA starts at time 3 and ends at time 4.

3) Ramp Attack: Ramp attack involves inserting falsified measurement gradually in the measurement time-series of the compromised buses. Since there is no abrupt change of values at the onset of the attack, the detection of ramp attack can be challenging. Ramp attack can be modeled by $c(t) = x(n_A,t_{start}) + m \times (t - t_{start}) + q(t)$, where m is the slope of the change and $q(t)$ is the additive white Gaussian noise. In Fig. 2, the example ramp attack with slope -0.8 starts at time 7 and ends at time 9.

4) Replay Attack: Replay attack involves inserting any recorded previous measurement as the current measurement in the attack duration. In this case, the attackers get access to some of the meters (PMUs), record the measurements, and afterward insert the recorded measurements as the true measurements into the same meter or other meters in the attack duration. Replay attack can be modeled by $c(t) \in \{x(n_R,t_p)\}, \quad t_p < t_{start}, \quad n_R \in \mathcal{V}_{\mathcal{R}}$, where $\mathcal{V}_{\mathcal{R}} \subset \mathcal{V}$ is the set of all buses (vertices) in which the attackers have access to record measurements before t_{start}. Depending on the selection of the compromised meter and the data to be inserted, replay attacks can be designed in various ways. In this work, $c(t)$ is considered to be $c(t) = x(n_A,-t)$. In Fig. 2, the example replay attack starts at time 15 and ends at time 17.

5) Delay Attack: In the delay attack, the attackers compromise the global positioning system (GPS) signal associated with the PMUs to falsify the measurements using the delayed version of the original measurements. The delay attack can be modeled by $c(t) = x(n_A, t - t_d)$, where t_d is the amount of delay. For small t_d's, the detection of this type of attack is very challenging. In Fig. 2, the example delay attack starts at time 19 and ends at time 21.

For a successful cyber attack from the attacker's perspec-

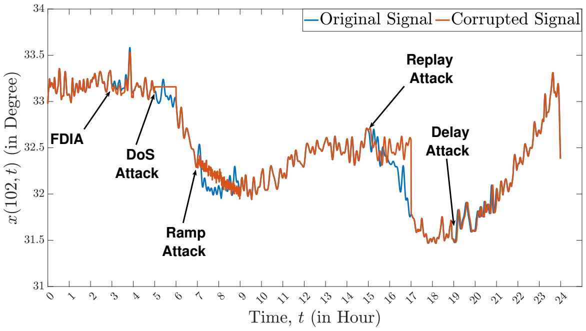


Fig. 2: cyber attacks on time-series.

tive, the attack must bypass the traditional bad data detector based on a threshold determined from historical data. The cyber attacks designed in this work involve injecting recent-past valid measurements in the current time with a smooth transition of measurement values at the attack onset. For this reason, the cyber attacks proposed in this paper can bypass the traditional bad data detectors, at least at the beginning of the attack duration. Moreover, the absence of any abrupt changes in the onset of the attack makes it difficult for the existing methods to detect them quickly in real-time.

B. Physical Stress Model

In this work, the abrupt change in the demand at a single bus is considered as a physical stress. Although the variation of load/demand with time is perpetual in electric grids, it usually occurs slowly in a smooth fashion. Sudden changes in the demand can represent abnormal conditions as can hamper the reliability of the grid. In this paper, the abrupt change in load demand is modeled using a scaling factor β. Specifically, if the original load demand of the $n-$th bus at time t is $P_n(t)$ mega-watt, then the load demand of the stressed bus at time $t+\epsilon$ is considered $\beta P_n(t)$ mega-watt, where ϵ is small. In this work, the range of the values for β is considered in such a way that the abrupt changes in the load do not cause failure of transmission lines and subsequent islanding that alter the topology of the system (i.e., changing the underlying graph $\mathcal{G}$). In other words, the techniques in this paper are for graph signals with static $\mathcal{G}$ and time and vertex varying values. Physical stresses that create changes in the topology can be addressed by dynamic graphs [33] and are out of the scope of this work and important for future studies.

V. GSP-based Detection and Localization

In this section, we first review the GFT-based technique for detecting stresses as presented in [9], [11]. Then, we present two new techniques for analyzing power grid's measurements for detecting and locating stresses based on VFED and LS of graph signals.

A. Stresses Detection using GFT

In general, the low-frequency components are prominent for the bus voltage angle graph signals because of the smooth changes of bus-to-bus values due to the power flow dynamics. The GFT coefficient magnitudes with respect to the normalized graph-frequencies (i.e., $\hat{\lambda}_k = \frac{\lambda_k - min_i\{\lambda_i\}}{max_i\{\lambda_i\} - min_i\{\lambda_i\}}$) are illustrated in Fig. 3 for a bus-voltage angle graph signal defined on the graph of the IEEE 118 bus system under normal condition, under an FDIA at bus 49, and under an abrupt change of load (physical stress) at the same bus. It can be observed that the magnitudes of the high-frequency components become larger in the case of the FDIA but remain almost unaffected in the case of physical stress. The reason is that in the case of physical stress at bus 49, the graph signal values corresponding to vertex 49 as well as its nearby vertices get affected. This means no abrupt change can be observed in the graph signal value at bus 49, instead more spread out changes occur over the graph. In contrast, in the case of FDIA, the value changes only occur at the vertex under attack, vertex 49. Such abrupt change at only a single vertex results in an increase in the magnitude of the high-graph frequency components. This property can be exploited for the detection of anomalies in the measurement data. A parameter $\gamma(t)$ is introduced to quantify the amount of high graph-frequency components corresponding to a graph signal $x(n,t)$ at the time instant t as follows:

$$\gamma(t) = \sum_k |\hat{X}(\hat{\lambda}_k, t) H(\hat{\lambda}_k)|, \tag{6}$$

where $H(\lambda)$ is a high-pass graph filter expressed by the following frequency response: $H(\lambda) = 0, \quad \text{if } \lambda \leq \lambda_c$ and $H(\lambda) = 1, \quad \text{if } \lambda > \lambda_c$, where λ_c is the cut-off graph-frequency. For detecting cyber and physical stresses, we estimate the probability distribution of γ, $p_\gamma(\zeta)$, in normal conditions from the past measurements of the system and assuming γ is a stationary random variable. For a certain time instant t, a stress is declared if the likelihood of $\gamma(t)$ corresponding to the distribution is less than a certain threshold θ_γ, (i.e., $p_\gamma(\gamma(t)) < \theta_\gamma$). The threshold θ_γ is selected empirically considering the tail probabilities of $p_\gamma(\zeta)$. Although this method detects cyber stresses reasonably well, the major drawback of this method is that it cannot provide any information about the location of the stress.

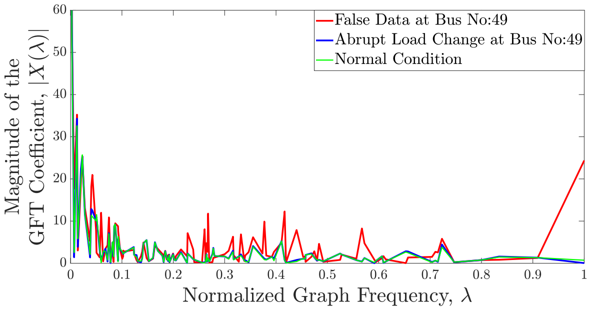


Fig. 3: GFT magnitude response for IEEE 118 bus system: emphasized high graph-frequency components can be observed in case of false data injection.

B. Detecting and locating Stresses using VFED

Containing the topological and the spectral information simultaneously, the VFED associated with the time-varying graph signal $x(n,t)$ makes itself suitable for detecting and locating anomalies in complex networks. Moreover, due to the better concentration of signal energy compared to the linear joint vertex-frequency representations [7], it serves better for locating stresses. According to equation (4), let $E(n,k,t_{start}-\epsilon)$ and $E(n,k,t_{start}+\epsilon)$ be the VFEDs corresponding to the graph signals just before the attack (under normal condition) and just after the stress, respectively. Cyber/physical stresses involve abnormal changes in the time-vertex graph signal $x(n,t)$, which also affect the graph-spectral characteristics of the graph signal at that time instant, i.e., $E(n,k,t_{start}+\epsilon)$. Hence, the VFEDs before and after the stress have certain differences that can be used in detecting and locating stresses. Here, by marginalizing the difference distribution, $\eta(n,t) = \sum_{k=1}^{N} |E(n,k,t+\epsilon) - E(n,k,t-\epsilon)|$, over the graph-frequency axis k, we use the comparatively large values of $\eta(n,t)$ as indicators for the compromised vertices. Specifically, if the likelihood of $\eta(n,t)$ value is below a certain threshold likelihood θ_{η_n} (i.e., $p_{\eta_n}(\eta(n,t)) < \theta_{\eta_n}$) at time instant t, a stress is declared at vertex n at that time instant. Fig. 4 illustrates normalized $\eta(n,t_{start})$ in the case of an FDIA at vertex 86 of IEEE 118 bus system, where a large value can be observed. Although the VFED provides a technique for locating stresses with abrupt changes in graph signal values, this method fails to detect the sophistically designed stresses with smooth transitions of graph signal values at the onset discussed in Section IV-A. It is worth mentioning that the basis signals of the graph frequency domain (i.e., eigenvectors of the Laplacian matrix) are localized around certain vertices unlike the sinusoidal bases for classical Fourier transform. For this reason, the VFED fails to contain information corresponding to the stress located at a particular vertex as distinctively as in the case of classical joint time-frequency representations (e.g., spectrogram). Moreover, this technique is computationally heavy for real-time applications.

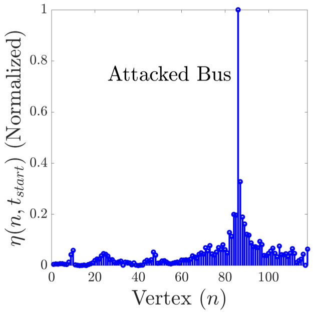
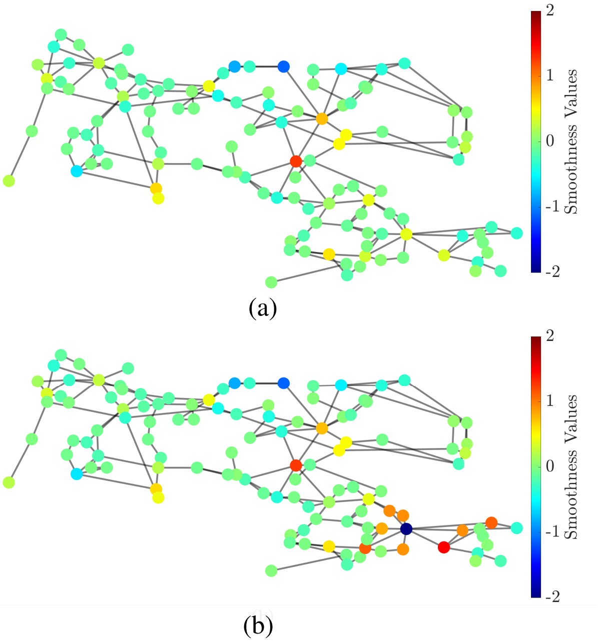


Fig. 4: Normalised $\eta(n,t_{start})$ (between 0 to 1). For $n = 86$, the largest value is obtained which indicates a stress at vertex (bus) 86.

C. Detecting and locating stresses using local smoothness

Both the GFT- and the VFED-based methods provide insights into how the graph-frequency components associated with the graph signal at one instant can be utilized to detect anomalies in the grid. The latter method is also capable of providing information about the stress location in the grid. While both of the methods work well for stress models with abrupt changes in graph signal values at the onset of the attacks, they fail to detect and locate sophistically designed stresses with no abrupt change at the onset as discussed in Section IV-A. Here, a technique for detecting and locating stresses based on the local smoothness of the graph signals is presented that addresses the limitation of the previous techniques. As described in Section III-E, the local smoothness $s(n,t)$ of the graph signal $x(n,t)$ specifies how the graph signal values at time t vary among the vertices. For example, a higher value of $s(n,t)$ specifies higher fluctuations of signal values in the vicinity of vertex n. Fig. 5 illustrates the local smoothness of the vertices of the IEEE 118 bus system corresponding to the bus-vertex graph $\mathcal{G}$ and graph signal $x(n)$ in the normal condition (Fig. 5(a)) as well as under DoS attack at bus number 100 (Fig. 5(b)). It can be observed that the local smoothness values of the vertices in the vicinity of vertex number 100 have changed significantly. This effect on the local smoothness of the vertices can be exploited to detect and locate anomalies in the grid. Specifically, by evaluating the changes in the signal values around each vertex of a graph signal, local smoothness $s(n,t)$ provides spectral and vertex-domain information simultaneously (similar to the instantaneous frequency in classical signal processing).



(b)

Fig. 5: Local smoothness of the vertices of the IEEE 118 bus system: (a) at normal condition, (b) during DoS attack at bus 100.

To this end, we propose *local smoothness second time-derivative (LSSTD)* method for detecting and locating stresses. In this method, instead of using $s(n,t)$ directly, the second time derivative of $s(n,t)$, i.e., $s''(n,t) = \frac{d^2}{dt^2}(s(n,t))$, has been considered. The rationale behind this consideration is that $s''(n,t)$ differentiate between the changes in the local smoothness values due to stresses and due to the regular load changes better by reducing non-stationarity in $s(n,t)$ (which is introduced by the non-stationarity of $x(n,t)$ due to load changes). At each time instant t, if the likelihood of $s''(n,t)$ is less than a certain threshold $\theta_{s''_n}$ (i.e., $p_{s''_n}(s''(n,t)) < \theta_{s''_n}$), a stress is declared at vertex n. If multiple vertices are obtained, all the vertices are considered as the possible candidate locations of stresses. The most possible location is identified as $\kappa \in \mathcal{V}$ for which $p_{s''_\kappa}(s''(\kappa,t)) = \min_n p_{s''_n}(s''(n,t))$. In this paper, past measurements of the system have been used to estimate the probability distribution of the second time derivative of the local smoothness of the $n-$th vertex $p_{s''_n}(\zeta)$ under normal conditions. In summary, the process consists of three critical steps: 1) calculating the second time-derivative of the local smoothness, 2) obtaining the likelihood of the second-derivative of the local smoothness values at each vertex/bus, and 3) comparing the likelihoods with the thresholds at each bus to detect and locate stresses simultaneously. In this work, Gaussian distributions are assumed for $p_{\gamma}(\zeta)$, $p_{\eta_n}(\zeta)$, and $p_{s''_n}(\zeta)$ and the estimation of the parameters of the distributions are updated regularly to be consistent with the effects of changing statistics of $x(n,t)$ (i.e., data drift [34]) that arise from changes in generations, load demands, and control parameters.

VI. Performance Evaluation

A. Simulating Stress Scenarios

For evaluating the performance of our proposed detecting and locating techniques, the IEEE 118 bus system [32] has been considered and simulated using MATPOWER 6.0 [35]. For generating time-series associated with the graph vertices, the time-varying load patterns from the New York Independent System Operator (NYISO) [36] have been added with the default MATPOWER loads as in [24]. The time-varying graph signal associated with the bus voltage angle measurements is obtained from the load flow analysis resulting. The cyber attacks are simulated according to the descriptions in Section IV-A. The noise $q(t)$ is added so that the signal-to-noise ratio is $45\ dB$ in the generated signals. For the physical stresses, i.e., abrupt changes in load demand at a bus, the original demand at that bus has been scaled up by factor β. For performance evaluation of the detecting and localization techniques with respect to cyber attacks, 10,000 random scenarios are simulated among which there are normal cases and attack cases with equal probability. For cyber stresses, the stress start time, t_{start}, and the location of the stress are selected randomly, all using the uniform distribution. The reference bus for voltage angle measurement (i.e., bus no. 69 in IEEE 118 bus system) is excluded from the consideration of being a location of a cyber stress. For FDIA, range of $x' = 0.02$ to 3 for voltage angel degrees are considered. For physical stresses (i.e., the abrupt load change), 1,000 scenarios are simulated for each value of β (specifically for $\beta = 0.5, 0.6, 0.7, 0.8$ and 0.9). Note that based on the selected range of values for β to avoid topology change, larger values indicate smaller changes in the load. For better clarity, the performance of the methods is shown as a function of parameter α defined as $1 - \beta$ to better reflect the proportional changes in the load. Among the aforementioned 1,000 simulated scenarios, there are normal cases as well as abrupt load changes with equal probability. In the normal scenarios, the loads of the buses change gradually following a pattern affected by the daily and seasonal variations and other slowly changing events that can introduce small changes in the load demand from one time sample to the next. The locations (buses) of the abrupt load change are selected from the load buses of the IEEE 118 bus system with equal probability.

B. Performance Metrics

Several metrics have been considered for the assessment of the proposed real-time detecting and locating schemes. The true positive rate (TPR) expresses the ratio of the number of true-positive (TP) and the number of total positive cases, i.e., stress scenarios, while the false positive rate (FPR) expresses the ratio of the number of the false-positive (FP) and the number of total negative cases, i.e., normal scenarios. The accuracy of detection is defined as $a = \frac{TP+TN}{TP+TN+FP+FN}$. In a real-time application, it is important to consider the time needed to detect the stress; the *detection time* is defined is as $t_{detect} - t_{start}$, where t_{detect} is the time instant at which the stress is detected. For the assessment of the performance of stress locating techniques, the location accuracy has been defined in two forms: (1) based on LA_{exact}, which specifies the efficiency based on the ability to locate the exact location (i.e., the vertex, where the stress occurred) and (2) based on the performance in locating the stress within $K-$hop distances of the actual location of the stress. In this paper, we have considered $K = 1$ and $K = 2$ and denote the corresponding performance metric by LA_{1-hop} and LA_{2-hop}, respectively.

TABLE I: Performance Evaluation of LSSTD Method.

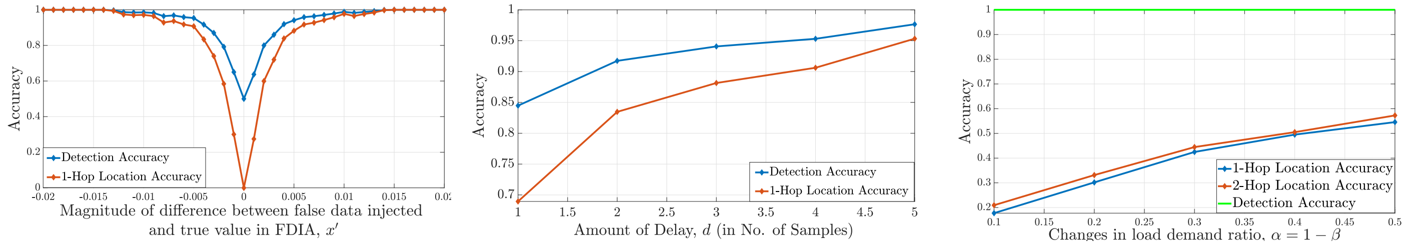
Stress Type	Accuracy, a	LA_{Exact}	LA_{1-hop}
DoS Attack	0.967	0.635	0.996
Replay Attack	0.978	0.670	1.0000
Ramp Attack	0.999	0.647	1.0000
FDIA ($x' = 0.01$) [See Fig.6(a)]	0.993	0.634	0.988
Delay Attack ($d = 2\ samples$) [See Fig.6(b)]	0.989	0.628	0.994
Load Change ($\beta = 0.6$)[See Fig.6(c)]	1.00	0.609	0.778

C. Analysis of the result

Table I summarizes the performance of detecting and localizing cyber and physical stresses by the LSSTD techniques. For all types of stresses, the false-positive rate is zero. Since the distributions ($p_{\gamma}(\zeta)$, $p_{\eta_n}(\zeta)$, and $p_{s''_n}(\zeta)$) have long tails, we have selected the detection threshold in such a way that the false-positive rate is zero without significantly affecting the false-negative rate. The detection times for most of the stresses ($> 90\%$) are instant, i.e., they are detected immediately; however, for the rest of the cases ($< 10\%$), it can take several time samples to detect the stress. Note that the results in Table I for the delay attack and the FDIA are for particular attack intensities (i.e., $x' = 0.04$ for FDIA and $d = 2\ \ samples$ for delay attack). The detailed performance for the FDIA has been illustrated in Fig. 6(a). As can be observed from the results, a large value of x' creates a large change in graph signal values of the compromised vertex and thereby becomes easy to detect. Similarly, in delay attacks, a large delay is less challenging to detect (Fig. 6(b)). The average detection accuracy for FDIA in the range $x' = -0.04$ to $x' = 0.04$ is 0.887, while the average exact location accuracy and average $1-$ hop location accuracies are, respectively, 0.485 and 0.792. For the delay attacks, the average detection accuracy, exact location accuracy, $1-$ hop location accuracy over the range $d = 1$ to $d = 5$ are, $0.978, 0.611, 0.988$, respectively. Since the physical stress, i.e., load demand change at a particular bus, is always abrupt, it can be easily detected by the proposed techniques. However, since the physical stresses affect the bus voltage angle measurements associated with a large number of buses in the grid, identifying the location of the stress is very challenging. Fig. 6(c) illustrates the location performances as a function of the changes in load demand ratio. The $1-$ hop and $2-$hop locating accuracies are 0.792 and 0.894, respectively, on average for $\beta = 0.5, 0.6, 0.7, 0.8, 0.9$.

D. Comparison with existing methods

1) Candidate techniques for comparison: In this work, the performance of the proposed techniques is compared



(a) (b) (c)

Fig. 6: Performance sensitivity to (a) magnitude of difference between false data injected and true value in FDIA x', (b) delay, d in delay attack, (c) changes in load demand ratio, α.

with other GSP- and non-GSP-based techniques. In the GSP-based category, the GFT-based detection technique [9], [11] (reviewed in Section V-A) and in the non-GSP-based category, support vector machine (SVM), decision tree (DT), long short term memory (LSTM)-based and the *three sample quadratic prediction algorithm* (TSQPA) [6] are considered. Among the non-GSP-based methods, SVM and DT are well-known machine learning methods, which do not consider the temporal correlation within the data stream. On the other hand, LSTM and TSQPA are two methods that consider the temporal correlation. LSTM is a neural network-based method that requires a large amount of data to capture the normal pattern in the time-series. The TSQPA is a signal processing-based technique that is selected in this work as it uses the time-series representation of streaming bus voltage angle data and attack models based on the time-series similar to this work. The TSQPA method predicts a measurement sample using quadratic prediction with the past three measurement samples of the same time-series. If the difference between the predicted value and the actual value exceeds a certain threshold, an attack is declared. In the LSTM-based method, the above-mentioned prediction is done by an LSTM neural network considering the multivariate setting of the time-series, and an attack is declared when the normalized prediction error exceeds a certain threshold similar to the TSQPA method.

The exact same time-series dataset and simulated cyber and physical scenarios, discussed in Section VI-A, are considered for all the techniques. Specifically, for machine learning methods (SVD, DT, and LSTM), the voltage angle time-series are directly considered as the features. The LSTM prediction model is considered with two LSTM layers with 100 neurons in each followed by an output dense layer with a single neuron. The performance of the LSTM-based stress detector improves by increasing the amount of training data; however, for ensuring the fairness of comparison among the detection methods the model is trained using the same dataset used by other methods.

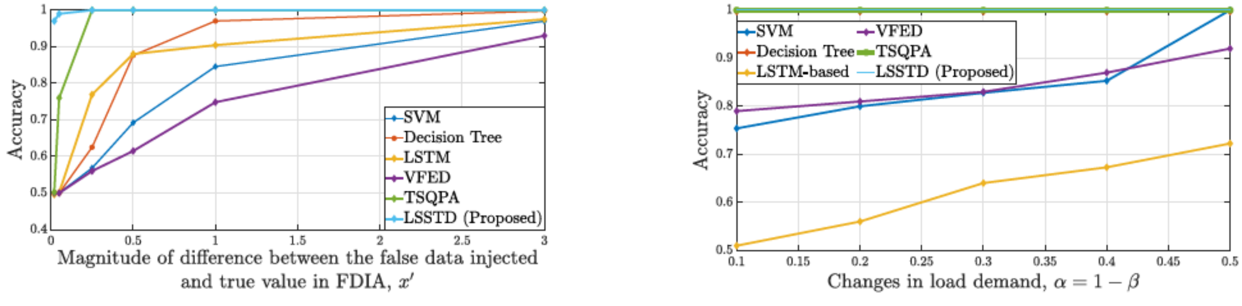
2) Comparison of detection accuracy: Our evaluations revealed that while all these methods (GFT-based, VFED-based, SVM, DT, LSTM-based, and TSQPA methods) perform well in detecting the stresses with sharp/abrupt changes at the onset, the proposed LSSTD outperforms these methods significantly in the case of more sophisticated and challenging cyber attacks with no abrupt change at the onset. The comparative performance of the proposed LSSTD method with the other GSP-based and non-GSP-based methods has been shown in Fig. 7. Next, some of the details of this comparison are presented.

In the case of FDIA, where parameter x' quantifies the change in the value of the attack at its onset, our simulations have shown that for $x' = 0.02$, the accuracy of detection for TSQPA, GFT, SVM, DT, LSTM, and the VFED method is limited to just a little over 0.5. While for $x' = 0.05$, the TSQPA method attains an accuracy of 0.76, the performance of the other methods for this setting is still limited. For a large abrupt change, i.e., $x' = 3$, the LSSTD, TSQPA, SVM, DT, LSTM, VFED methods attain accuracies of $1, 1, 0.97, 0.99, 0.97,$ and 0.93, respectively.

The performance of the GFT-based method in all these scenarios is just over 0.5. However, GFT can detect FDIA with more abrupt changes; for example, for $x' = 15$, the GFT technique achieves an accuracy of 0.94 and for $x' = 16.5$ it achieves an accuracy of 1. The reason behind the lower performance of GFT in the time-series setting is the changing statistics of the time-series data due to high non-stationarity, which poses difficulty in choosing θ_γ that leads to a high false-positive rate. In [27] and [9], it is shown that a comparable accuracy for GFT-based method is attainable in scenarios in which the statistics of the states are stationary.

The example of the physical stress case considered in this work is the abrupt load change, which in general contains sharp changes of signal values at the onset. Both the LSSTD method and the TSQPA method attain perfect accuracy in detection for $\alpha = 0.1$ to 0.5, while the accuracy of the VFED method is between 0.79 to 0.92. However, the GFT-based method is not able to detect load changes due to the absence of high-graph frequency components as illustrated in Fig. 3. In the GFT-based method, the GFT of a graph signal cannot capture the local dynamics of the grid as it is a global measurement of the contribution of the frequency components.

In the case of load change, instead of the multivariate setting of the LSTM (as for the cyber stress detection model), 118 separate LSTM models are considered. It can be observed from Fig. 7-b that although LSTM is generally an efficient method for analyzing time-series, in the specific case of this work with high dimensionality and under limited data utilization, it fails to perform up to the mark. Moreover, from Fig. 7, it can be observed that although VFED achieves lower detection accuracy than all the other methods both in the case of cyber and physical stresses, it outperforms LSTM and SVD especially in the challenging range of small load changes (i.e., $\alpha < 0.3$) as can be seen in Fig. 7-b. The VFED method is based on the joint-vertex frequency distribution of the graph



(a) (b)

Fig. 7: Comparison among the detection accuracy of different methods for various (a) FDIA attack intensity, x' (b) abrupt load changing factor $\alpha = 1 \quad \beta$.

signal, which represents the contribution of each frequency component in the vicinity of a vertex. Although VFED does not use any window explicitly, the computation of VFED by equation (4) implicitly introduces some smoothing effect and therefore, loses specificity to detect the small amount of changes in the signal. From Fig. 7, it can be observed that although TSQPA can achieve the same level of detection accuracy as the LSSTD method for abrupt load change and FDIA for the range of $x' > 0.25$ but has lower accuracy for the range of $x' < 0.25$.

3) Performance of location accuracy: Since all the aforementioned methods are not equipped with the ability to locate the stresses, the stress detection accuracy is considered as the primary criterion of comparison among the performance of the methods. However, among the GSP-based techniques, the proposed LSSTD and VFED techniques can locate the stresses along with the stress detection. Between these two techniques, LSSTD has better locating accuracy in most of the cases as the smoothing effect in calculating the VFED values reduces its vertex localization. On the other hand, the LSSTD is calculated directly in the vertex domain, which helps with the locating process. However, the locating accuracy of the VFED method for abrupt load changes is better than the LSSTD method (0.98 for $\alpha = 0.4$ and 0.70 for $\alpha = 0.1$).

4) Further discussions: In this subsection, more discussions on the observed performance of the methods in the previous subsection are presented.

One of the challenges of the LTSM-based stress detection technique, considered in this paper for comparison, is that although the LSTM-based method can capture the temporal dynamics, being a training-based pattern recognition method, it considers the very small changes that are present at the onset of the designed stresses as noise, and therefore, fails to classify them as anomalies. Moreover, in the high dimensional multivariate time-series setting (for the 118 buses in the case of IEEE 118 buses), LSTM requires a large amount of training data for good accuracy. Specifically, in the case of abrupt load change, a change of load demand in a particular bus affects the voltage angle time-series of many of its neighboring buses simultaneously. As such, for training the LSTM model to differentiate between the normal condition and the load change condition, a large amount of data is needed.

Furthermore, the SVM and DT methods are training-based data-centric methods. Although they implicitly learn the relations among data and their sources, they cannot explicitly utilize the knowledge of the grid topology, and also they are not capable of capturing the time correlation among the states. TSQPA method can tract the time evolution of data by a quadratic function; however, it cannot capture the interrelation among the time-series at different buses. GFT-based method also does not capture the temporal relations in the data and cannot capture the local dynamics of the grid as it is a global measurement of the contribution of the frequency components.

The key advantage of the proposed LSSTD method is that it combines the advantages of the existing methods by having the ability to capture both the time correlation in the state values as well as the inter-relation among the states by their structural interconnection through the graph. Specifically, the proposed LSSTD method can detect the carefully designed cyber attacks by capturing the interaction and interconnection among the graph signal values while the non-GSP methods cannot utilize the knowledge of the interaction and interconnections among the data sources explicitly. Moreover, since a small amount of data is needed to obtain and update the probability distributions ($p_\gamma(\zeta)$, $p_{\eta_n}(\zeta)$, and $p_{s''_n}(\zeta)$), it can work on real-time without any explicit training.

E. Computational Complexity

In this subsection, the computational complexity of the LSSTD and VFED is discussed. The complexity for computing $s(n,t) = \frac{l_x(n,t)}{x(n,t)}, x(n,t) \neq 0$ is dominated by the computation of $l_x(n,t)$, the $n-$th element of the vector, $\mathbf{Lx}$, which is in the order of $\mathcal{O}(N^2)$. The complexity for computing the second time-derivative of $s(n,t)$ and the comparison with the threshold $\theta_{s''_n}$ are both in the order of $\mathcal{O}(N)$. As a result, the computational complexity of LSSTD detection algorithm is $\mathcal{O}(N^2)$, where N is the number of buses in the grid. For VFED technique, equation (4) is the key computational component. Specifically, at each time instant, the value of VFED is calculated at every vertex (i.e., N buses) and every N frequency component. The calculation for each VFED value comprises of three multiplications and N summations. Therefore, the complexity of VFED is in the order of $\mathcal{O}(N^3)$. As such, although these methods have been applied to the IEEE 118 bus system, particularly VFED has limited scalability to large grid sizes. It is hoped that future research on VFED technique can lead to new developments with better computational complexity or development of complementing techniques, such as augmented graphs with reduced domain and grid partitioning, to allow VFED application to a smaller system for stress localization. In its current form, the VFED technique can be applied in parallel to LSSTD to a small system to complement the localization process after a stress is detected by the LSSTD technique.

Acknowledgement

This material is based upon work supported by the National Science Foundation under Grant No. 2118510.

VII. Conclusion and Future Works

In this work, graph signal processing is utilized to represent and analyze the power grid's measurement data for reliability and security evaluation of the system under various stresses. The physical structure of the power grid has been used to define the graph domain with the measurements associated with the grid as the graph signals. The effects of the cyber and physical stresses on the graph signals have been studied in the vertex domain, graph-frequency domain, and joint vertex-frequency domain of the signals. Based on the observations from the effects of stresses, novel techniques for detecting and locating stresses from the vertex-frequency energy distributions, and the local smoothness of graph signals have been proposed and compared with existing GSP and non-GSP methods. It is shown that the proposed techniques can detect challenging stresses with no abrupt changes at the onset. Moreover, the method based on local smoothness can perform well in locating the stresses.

The presented work in this paper can be extended in several directions. Analysis of the effects of noise on the performance of the GSP-based methods is an important and interesting topic for future studies. In this work, only the noise, implicitly present in the load profiles, is considered. Secondly, stresses that cause changes in the topology of the system (i.e., changes in the underlying/domain graph of the graph signals) are not considered in this paper and future studies can, for instance, consider GSP-based methods based on dynamic graphs to detect and locate such stresses. Future research on the proposed VFED technique can lead to new developments with better computational complexity or development of complementing techniques, such as augmented graphs with reduced domain and grid partitioning, to allow VFED application to a smaller system for stress localization. Finally, the presented technique do not distinguish among different types of stresses. A classification method utilizing the graph signal attributes and features in vertex and graph-spectral domain to classify the stresses can also be a prospective future work.

References

[1] A. Ortega, P. Frossard, J. Kovačević, J. M. F. Moura and P. Vandergheynst, "Graph Signal Processing: Overview, Challenges, and Applications," in Proceedings of the IEEE, vol. 106, no. 5, pp. 808-828, May 2018.

[2] 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," in IEEE Signal Processing Magazine, vol. 30, no. 3, pp. 83-98, May 2013.

[3] U. Nakarmi, M. Rahnamay-Naeini, M. J. Hossain, and M. A. Hasnat, "Interaction Graphs for Cascading Failure Analysis in Power Grids: A Survey," Energies, vol. 13, no. 9, pp. 2219, 2020.

[4] M. N. Kurt, Y. Yilmaz and X. Wang, "Distributed Quickest Detection of cyber-attacks in Smart Grid," in IEEE Transactions on Information Forensics and Security, vol. 13, no. 8, pp. 2015-2030, Aug. 2018.

[5] Z. Zhang, S. Gong, A. D. Dimitrovski and H. Li, "Time Synchronization Attack in Smart Grid: Impact and Analysis," in IEEE Transactions on Smart Grid, vol. 4, no. 1, pp. 87-98, March 2013.

[6] Z. Chu, A. Pinceti, R. S. Biswas, O. Kosut, A. Pal and L. Sankar, "Can Predictive Filters Detect Gradually Ramping False Data Injection Attacks Against PMUs?," IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids, 2019, pp. 1-6.

[7] L. Stanković, E. Sejdić and M. Daković, "Vertex-Frequency Energy Distributions," in IEEE Signal Processing Letters, vol. 25, no. 3, pp. 358-362, March 2018.

[8] M. Daković, L. Stanković, and E. Sejdić. "Local smoothness of graph signals," in Mathematical Problems in Engineering, 2019.

[9] E. Drayer and T. Routtenberg, "Detection of False Data Injection Attacks in Smart Grids Based on Graph Signal Processing," in IEEE Systems Journal, vol. 14, no. 2, pp. 1886-1896, June 2020.

[10] R. Ramakrishna and A. Scaglione, "Detection of False Data Injection Attack Using Graph Signal Processing for the Power Grid, " IEEE Global Conference on Signal and Information Processing, Ottawa, ON, Canada, 2019, pp. 1-5.

[11] R. Ramakrishna and A. Scaglione, "Grid-Graph Signal Processing (Grid-GSP): A Graph Signal Processing Framework for the Power Grid," in IEEE Transactions on Signal Processing, vol. 69, pp. 2725-2739, 2021.

[12] L. Stankovic, D. Mandic, M. Dakovic, M. Brajovic, B. Scalzo and A. G. Constantinides, "Graph signal processing–Part II: Processing and analyzing signals on graphs," arXiv preprint, arXiv:1909.10325, 2019.

[13] L. A. S. Moreira, A. L. L. Ramos, M. L. R. de Campos, J. A. Apolinário and F. G. Serrenho, "A Graph Signal Processing Approach to Direction of Arrival Estimation," 27th European Signal Processing Conference (EUSIPCO), 2019, pp. 1-5.

[14] M. Z. Li, K. Gopalakrishnan, K. Pantoja, and H. Balakrishnan, "Graph Signal Processing Techniques for Analyzing Aviation Disruptions. Transportation Science," vol.55, no.3, pp.553-573.

[15] M. Sun, E. Isufi, N. M. de Groot and R.C. Hendriks, "Graph-time spectral analysis for atrial fibrillation," in Biomedical Signal Processing and Control, vol. 59, pp. 101915, 2020.

[16] S. S. Saboksayr, G. Mateos and M. Cetin, "EEG-Based Emotion Classification Using Graph Signal Processing," IEEE International Conference on Acoustics, Speech and Signal Processing, 2021, pp. 1065-1069.

[17] H. E. Egilmez, A. Said, Y. Chao and A. Ortega, "Graph-based transforms for inter predicted video coding," IEEE International Conference on Image Processing (ICIP), Quebec City, QC, 2015, pp. 3992-3996.

[18] H. E. Egilmez and A. Ortega, "Spectral anomaly detection using graph-based filtering for wireless sensor networks," IEEE International Conference on Acoustics, Speech and Signal Processing, Florence, 2014, pp. 1085-1089.

[19] A. Kroizer, Y. C. Eldar and T. Routtenberg, "Modeling and Recovery of Graph Signals and Difference-Based Signals," IEEE Global Conference on Signal and Information Processing (GlobalSIP), 2019, pp. 1-5.

[20] M. A. Hasnat and M. Rahnamay-Naeini, "Sampling of Power System Graph Signals," IEEE PES Innovative Smart Grid Technologies Europe, 2021, pp. 01-06.

[21] J. Cao *et al.*, "A Novel False Data Injection Attack Detection Model of the Cyber-Physical Power System," in IEEE Access, vol. 8, pp. 95109-95125, 2020.

[22] Y. Chen, L. Xie and P. R. Kumar, "Dimensionality reduction and early event detection using online synchrophasor data," IEEE Power & Energy Society General Meeting, pp. 1-5, Vancouver, BC, 2013.

[23] K. Mahapatra and N. R. Chaudhuri, "Online Robust PCA for Malicious Attack-Resilience in Wide-Area Mode Metering Application," in IEEE Transactions on Power Systems, vol. 34, no. 4, pp. 2598-2610, July 2019.

[24] M. A. Hasnat and M. Rahnamay-Naeini, "Detecting and locating cyber and physical stresses in smart grids using the k-nearest neighbour analysis of instantaneous correlation of state," in IET Smart Grid, vol 4, no. 3, March 2021.

[25] S. Basumallik, R. Ma, and S. Eftekharnejad, "Packet-data anomaly detection in PMU-based state estimator using convolutional neural network," Electrical Power and Energy Systems vol. 107, pp. 690-702, 2019.

[26] M. J. Hossain and M. Rahnamay-Naeini, "Line Failure Detection from PMU Data after a Joint Cyber-Physical Attack" IEEE Power & Energy Society General Meeting (PESGM), pp. 1-5, Atlanta, GA, USA, 2019.

[27] M. A. Hasnat and M. Rahnamay-Naeini, "Detection and locating cyber and physical stresses in smart grids using graph signal processing," arXiv preprint, arXiv:2006.06095, 2020.

[28] M. A. Hasnat and M. Rahnamay-Naeini, "Reflection of Cyber and Physical Stresses in Smart Grids on their Graph Signals," IEEE PES Innovative Smart Grid Technologies Europe, 2021, pp. 01-05.

[29] E. Drayer and T. Routtenberg, "Cyber Attack Localization in Smart Grids by Graph Modulation (Brief Announcement)," in Cyber Security Cryptography and Machine Learning, Lecture Notes in Computer Science, vol 11527, Springer, Cham, 2019.

[30] O. Anderson and N. Yu, "Distribution System Bad Data Detection Using Graph Signal Processing," IEEE Power & Energy Society General Meeting (PESGM), 2021, pp. 01-05.

[31] J. Shi, B. Foggo and N. Yu, "Power System Event Identification Based on Deep Neural Network With Information Loading," in IEEE Transactions on Power Systems, vol. 36, no. 6, pp. 5622-5632, Nov. 2021.

[32] Electrical and Computer Engineering Department, IEEE 118-Bus,54 Unit, 24-Hour System Unit and Network Data, Illinois Institute of Tech.

[33] M. Villafane-Delgado and S. Aviyente, "Dynamic Graph Fourier Transform on temporal functional connectivity networks," IEEE International Conference on Acoustics, Speech and Signal Processing, 2017, pp. 949-953.

[34] A. Ahmed, K. S. Sajan, A. Srivastava and Y. Wu, "Anomaly Detection, Localization and Classification Using Drifting Synchrophasor Data Streams," in IEEE Transactions on Smart Grid, vol. 12, no. 4, pp. 3570-3580, July 2021.

[35] R. D. Zimmerman, C. E. Murillo-Sánchez and R. J. Thomas, "MATPOWER: Steady-State Operations, Planning, and Analysis Tools for Power Systems Research and Education," in IEEE Transactions on Power Systems, vol. 26, no. 1, pp. 12-19, Feb. 2011.

[36] The New York Independent System Operator, Inc[US], https://www.nyiso.com/.

Md Abul Hasnat received the B.Sc. degree in electrical and electronic engineering from Bangladesh University of Engineering and Technology (BUET), Dhaka, Bangladesh, in 2014 and the M.Sc. in electrical engineering from University of South Florida (USF), Tampa, FL, USA in 2020. He is currently working toward the Ph.D. degree in electrical engineering at USF. His research interests include signal processing, data analytics, machine learning, and network science in application to the security and reliability of cyber-physical systems, particularly smart grids.

Mahshid Rahnamay-Naeini received the Ph.D. degree (honors) in electrical and computer engineering with a Ph.D. minor in mathematics from the University of New Mexico, Albuquerque, NM, USA, in 2014. She is an Assistant Professor with the Electrical Engineering Department, University of South Florida (USF), Tampa, FL, USA. Before joining USF, she was an Assistant Professor with the Computer Science Department, Texas Tech University. Her research interest lies in the areas of network science, stochastic processes, system modeling, data analytics, and machine learning with applications in cyber-physical-human systems with emphasis on critical infrastructures and particularly smart grids and their reliability, security and performance evaluation and energy data analytics.