Reflection of Cyber and Physical Stresses in Smart Grids on their Graph Signals

Md Abul Hasnat
Electrical Engineering Department
University of South Florida
Tampa, Florida, USA
hasnat@usf.edu

Mahshid Rahnamay-Naeini
Electrical Engineering Department
University of South Florida
Tampa, Florida, USA
mahshidr@usf.edu

2021 IEEE PES Innovative Smart Grid Technologies Europe (ISGT Europe) | 978-1-6654-4875-8/21/$31.00 ©2021 IEEE | DOI: 10.1109/ISGTEUROPE52324.2021.9639997

***Abstract*—Graph signal processing has been shown to provide a unique platform and new perspective for representing and analyzing power system measurements. In this paper, the effects of various cyber and physical stresses, as well as their differences on the graph signals of the system and their spectral domain are presented and discussed. Specifically, graph Fourier transform (GFT) and the local smoothness corresponding to the graph signals are presented as tools for the characterization of the effects of stresses. Particularly, various cyber-attacks including denial-of-service, replay attack, ramp attack, and delay attack are considered on the time-series associated with the voltage angle measurements. An analysis of the relation of the degrees of the nodes under cyber-attack with the GFT of the associated graph signal has also been presented. Finally, a comparative analysis of the effects of cyber and physical stresses on the graph spectrum in the context of detecting and locating stresses in the smart grid are presented.**

***Index Terms*—Graph Signal Processing, cyber-physical stress, smart grid, graph-frequency, local smoothness.**

I. Introduction

The issues of security and reliability of smart grids are becoming more challenging day by day because of the insertion of various modern equipment with more complex and stochastic nature into the system. With the modernization of electric grids, a large number of sensing and metering devices are being deployed throughout geographically widespread regions that increases the risk of cyber-attacks in the smart grid. The denial-of-service (DoS) attack [1], [2], timing-related attacks (e.g. GPS spoofing, data-replay attack, delay attack) [1]–[3], and false data injection attack (FDIA) [4], [5] are some of the common cyber-attacks on smart grids. Moreover, different types of physical stresses (e.g. abrupt changes of loads, tripping of branches, and failure of generators, etc.) are always prevalent in the grid. Proper maintenance and operation of the smart grid require detecting, locating, and identifying various types of stresses in the grid quickly and accurately.

Due to the advancement of the sensing and metering infrastructure in power systems in recent years by the deployment of high-resolution measurement devices (e.g. Phasor measurement units - PMUs), a massive amount of data are being produced in smart grids. For this reason, data-driven methods for security and reliability assessment of the smart grid are getting attention from researchers. Smart grids are networks of electric equipment, in which their elements may interact in complex ways. Therefore, data generated at different locations of the grid have interdependency among themselves. Classical data representations in Euclidean data domains (e.g. multivariate time-series model for the PMUs) are not well suited to capture these internal relations and dynamic interactions among the components of the system. Graph signal processing (GSP) enables handling data from such complex networks by considering the underlying topology of the system in representing and analyzing data. For instance, by considering the buses and transmission lines of an electrical grid as the vertices and the edges of a graph, respectively, one can view the bus measurements of the grid as graph signals residing on the vertices of the graph. In this way, the topological and relational information about the data sources can be imparted into the signal model to inspect deeper into the dynamics of the network for security and resilience issues.

In classical signal processing, observing the signal in the time-domain and its spectral components in the frequency-domain offer a better understanding of the physical process associated with the signal. Similarly, in GSP, analyses of the signal in the vertex domain along with the graph-frequency domain enable extracting more information from the graph signal and better understand the system. The signatures of various events in a graph signal are often easily detectable in the graph-frequency domain. For example, in our previous work [6], we showed that stresses in power systems can be detectable from the graph-frequency representation of the power system graph signal. In this work, we use graph Fourier transform (GFT) and local smoothness values as the frequency domain tools for analyzing the effect of different cyber and physical stresses in the smart grid. The GFT is the graph signal counterpart of the Fourier transform in traditional signal processing. Although the local smoothness of a graph signal is defined in its vertex domain, it provides the degree of relative fluctuations of signal values at each vertex and thereby presents the amount of high-frequency components in the vicinity of each vertex.

In this work, the voltage angle measurements associated with the buses of the grid are considered as the graph signals.

978-1-6654-4875-8/21/$31.00 ©2021 IEEE

Specifically, in this work, cyber-attacks on the smart grid have been considered as corruptions of the time-varying graph signals. The denial-of-service (DoS) attack, data-replay attack, ramp attack, false data injection attack, and delay attack are considered among the cyber-attacks. In the current paper, we have studied the characteristics of GFT and local smoothness of graph signals (described in [6]) associated with the cyber-attacks modeled in this paper as well as on physical stresses. This study shows that cyber and physical stresses have different effects on graph signals of the power system, their local smoothness as well as on the GFT of the signals and thereby need different techniques for characterization and localization by the grid operators. Our analyses have revealed that although GFT is applicable for detecting anomalies with sharp changes of values, it is not suitable for detecting attacks with a smooth transition of signal values on the stress onset. Moreover, the effects of physical stresses are not obvious from the GFT of the associated signal. However, the local smoothness of the graph signal is suitable for detecting both types of anomalies, although determining the exact location in case of physical stresses is challenging.

II. Related Works

In recent years, the field of GSP has become very popular among the signal processing researchers working in various domains, especially in applications with topological data (e.g. sensor networks [7], brain signal analytics [8], [9], image processing [10], [11]). The application of GSP in power systems is relatively new. The application mainly involves modeling power system measurements in the GSP environment and detecting anomalies from power system measurements. For instance, Ramakrishna and Scaglione [12] proposed a graph signal based model for the power system in which the measurements are considered to be the output of a graph filter while the low-rank excitations from the generators act as an input graph signal. A similar model is also proposed by Kroizer *et al.* [13] to consider the non-linear measurements as the output of a graph filter. In addition, the authors in [13] showed that an inverse system of the filter can be used to recover the input signal under smoothness constraints by regularized least-squares estimation. Schultz *et al.* [14] proposed resilience analysis of smart grid using GSP.

Ramakrishna and Scaglione [15] proposed a detection of false data injection attack (FDIA) in power system by using their measurement model developed in [12]. Drayer and Routtenberg [16] proposed a detecting technique for FDIA based on graph Fourier transform. In this paper, it has been showed that the graph signal associated with the bus measurements is smooth, and thereby does not contain significant high-frequency components. The authors suggested that the presence of a significantly large GFT component corresponding to a higher graph frequency indicates the insertion of falsified measurements. A location technique for FDIA is also proposed by the same author using modulation of the graph signal [17]. In our previous work [6], we have proposed three different graph spectral domain techniques for detecting stresses in the smart grid: GFT-based technique, local smoothness-based technique, and vertex-frequency energy distribution-based technique. The latter two techniques are capable of locating the anomalies.

In this paper, the work in [6] is extended for detecting and localization of cyber and physical stresses in the smart grid to evaluate the effectiveness of the GSP-based techniques for special types of stresses on the time-varying measurement signals. A comparative study on the effects of cyber and physical stresses on graph signals has also been presented.

III. Graph Signal Processing- Preliminaries

In this section, we have presented a brief review of the fundamental concepts of GSP in the context of power grid's measurements. A detailed discussion can be found in our previous work [6].

A. Graph and Graph signals in power system

A graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ consists of two sets, $\mathcal{V}$ and $\mathcal{E}$, where, $\mathcal{V} = \{v_1, v_2, ..., v_N\}$ represents the set of all vertices (nodes) and $\mathcal{E} = \{e_{ij} : (i,j) \in \mathcal{V} \times \mathcal{V}\}$ represents the set of all edges (links between two nodes) of the graph $\mathcal{G}$. Let us define the weights associated with the graph $\mathcal{G}$ as w_{ij} for $e_{ij} \in \mathcal{E}$, and zero, otherwise. In this work, we will use the bus-vertex graph [6] for power systems in which the buses and the transmission lines of an electric grid are considered as the vertices and the edges of the graph, $\mathcal{G}$, respectively. The *order*, $N = |\mathcal{V}|$ and the *size*, $M = |\mathcal{E}|$ of the graph $\mathcal{G}$ represents the number of the buses and the number of the transmission lines in the grid, where $|.|$ denotes the cardinality of a set. The weights are defined as $w_{ij} = 1/d_{ij}$ for $e_{ij} \in \mathcal{E}$, where d_{ij} is the normalized geographical distance between the $i-$th and $j-$th buses i.e. normalized length of the transmission line represented by the edge e_{ij}. However, other structure of graphs and its weights are also used in power system [18] depending on the application and characteristics of the analysis.

Signals in classical signal processing are defined over the Euclidean domain. The graph signals, on the other hand, reside on the vertices of a graph, $\mathcal{G} = (\mathcal{V}, \mathcal{E})$, a non-Euclidean irregular domain. A real-valued graph signal $x(v_n)$ can be defined as the mapping of the vertices of the graph into an $N-$dimensional vector of real numbers, i.e., $x : \mathcal{V} \rightarrow \mathbb{R}$. However, for simplicity, we will use $x(n)$ instead of $x(v_n)$ to denote the graph signal value at the $n-$th vertex. In this work, we consider the bus voltage angle at a single time instant (in degree) as the graph signal. Therefore, $x(n)$ signifies the voltage angle at the $n-$th bus. The Laplacian matrix of the graph, $\mathcal{G}$ is denoted by $\mathbf{L}$. The element, l_{ij} of the $\mathbf{L}$ is defined as: $l_{ij} = \sum_{j=1}^{N} w_{ij}$ if $i = j$ and $l_{ij} = -w_{ij}$, otherwise.

B. The graph Fourier transform (GFT)

The GFT and the inverse graph Fourier transform (IGFT) of a graph signal $x(n)$ are defined, respectively as:

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

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

where $u_k(n)$ is a graph signal, which is the basis signal of GFT analogous to complex exponential being the basis signal for traditional Fourier transform. The graph signal $u_k(n)$ is defined as the $k-$th eigenvector of Laplacian matrix of the graph $\mathbf{L}$. The eigenvalues, λ_k of $\mathbf{L}$ are considered as the graph frequencies. Since in this application $\mathbf{L}$ is real and symmetric, all the eigenvalues are real and the eigenvectors form an orthogonal set.

C. Local Smoothness of graph signals

The local smoothness of a graph signal $x(n)$ (similar to the concept of instantaneous frequency in temporal signal processing [19]) at vertex n is:

$$s(n) = \frac{l_{\mathbf{x}}(n)}{x(n)}, \quad x(n) \neq 0, \qquad (3)$$

where $l_{\mathbf{x}}(n)$ is the $n-$th element of $\mathbf{Lx}$. The local smoothness corresponding to a vertex, n of a graph signal specifies the amount of fluctuations near the $n-$th vertex, i.e., how abruptly the signal values changes from the vertex, n to the neighboring vertices.

D. Time-varying graph signal

The time-varying graph signal $x(n,t)$ represents the voltage angle graph signal $x(v_n)$ at time t. In this paper, we have simulated the time-varying graph signals for IEEE 118 [20] bus system by adding a time-varying load pattern collected from New York independent system operator (NYISO) [21] to the static loads of MATPOWER [22]. The corresponding GFT and local smoothness are denoted as $X(\lambda_k, t)$ and $s(n,t)$.

E. Detecting grid stresses

In reference to our previous work [6], we will discuss detecting cyber and physical stresses using GFT and local smoothness of the graph signal. For detection, we define the amount of high graph-frequency components in the graph signal at time t, $\gamma(t)$ as:

$$\gamma(t) = \sum_{k} |X(\lambda_k, t) H(\lambda_k)|, \qquad (4)$$

where $H(\lambda)$ is a high-pass graph filter with frequency response: $H(\lambda) = 0$, if $\lambda \leq \lambda_c$ and $H(\lambda) = 1$, if $\lambda > \lambda_c$ and λ_c is the cut-off frequency. Since during normal operation, the graph signal is smooth and thereby contains only low graph-frequency components, a high value of $\gamma(t)$ indicates an anomaly in the grid. However, all kinds of anomalies are not reflected in the value of $\gamma(t)$ and this quantity is dependent on the selection of λ_c. For detecting stresses by using the local smoothness, we use the instantaneous local smoothness, $s(n,t)$ to detect stresses.

IV. Effects of Cyber Attacks on Graph Spectra

A. Cyber Attack Models

In this work, a generalized approach for modeling various cyber attacks based on various corruptions in the time series of system measurements has been considered. We have specifically considered DoS attack, replay attack, ramp attack, delay attack, and one type of false data injection attack in smart grids. The models presented in this work improve the attack models in [6] as they are designed to be more challenging to detect. Let $\mathcal{V}_{\mathcal{A}}$ be the set of all buses (i.e. vertices) under cyber-attack in between the time interval $[t_{start}, t_{end}]$ and $\mathcal{V}_{\mathcal{R}}$ be the set of all buses (vertices) in which the attackers have

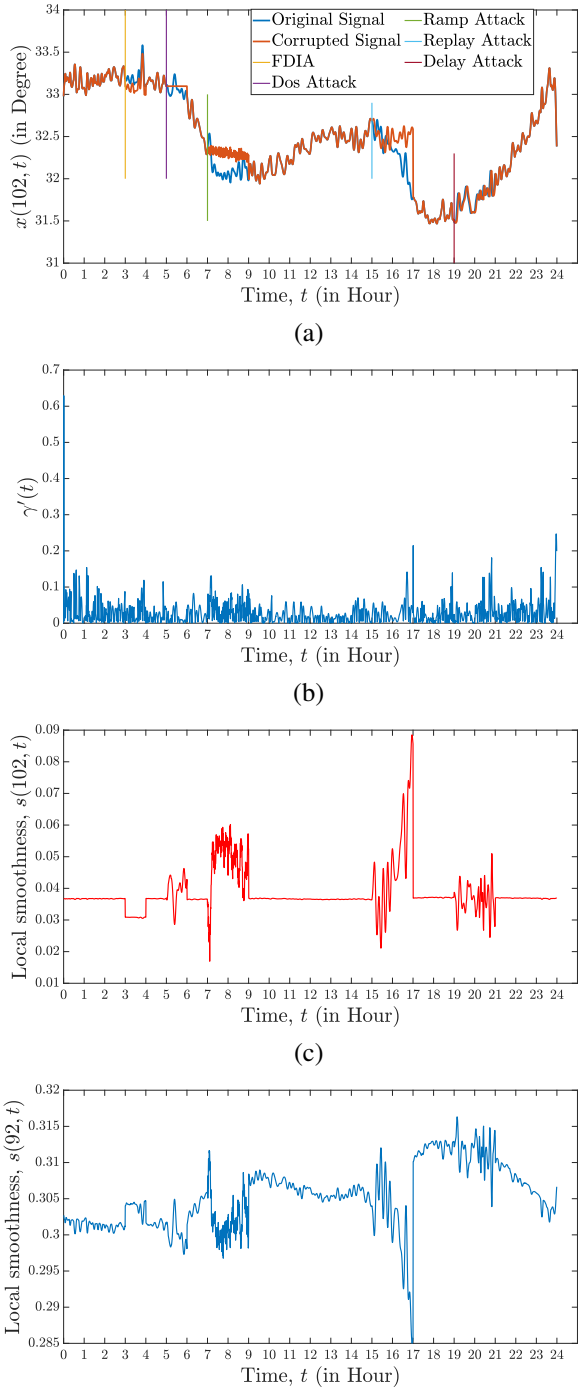

Fig. 1. The effects of various cyber-attacks on (a) time-varying graph signal values at vertex 102, $x(102,t)$, (b) changes in the amount of high-frequency components, γ_t', (c) local smoothness values of vertex 102, $s(102,t)$, and (d) local smoothness values of vertex 92, $s(92,t)$ (neighboring vertex of 102).

access to record data. The values of $x(n,t)$ during the attack at any vertex under cyber attack can be described as:

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

Next, models for different cyber-attacks are presented by defining $c(t)$.

1) Denial-of-service (DoS Attack): The denial-of-service (DoS) attack involves the unavailability of the data during the duration of the attack. In this case, we have modeled the DoS attack as the suspension of updating the measurement values at the attack onset, t_{start} corresponding to the attacked bus, n_A. During the attack duration, the bus measurement (i.e., graph signal value at vertex n_A) is considered to be constant at the value that was measured just before the attack was launched. In other words, $c(t) = x(n_A, t_{start})$.

2) False Data Injection Attack (FDIA): The FDIA can be modeled from various perspectives and by using different techniques in the cyber security literature. In this work we have used a simple but challenging-to-detect model for FDIA, which involves changing the original measurements by a small amount mathematically expressed as $c(t) = x(n_A,t) + (-1)^d x'$, where $d \in \{0,1\}$ and x' is a small value such that the change at the onset of the attack cannot be considered as abrupt (cause a small deviation from current value).

3) Replay Attack: In the replay attack, the attackers record previous measurements from any of the measurement devices that they have access to and record data and insert the data into the attacked meter during the attack duration, i.e., $c(t) \in \{x(n_R,t_p)\}, \quad t_p < t_{start}, \quad n_R \in \mathcal{V}_\mathcal{R}$. In this work, we have considered a special type of replay-attack, where $c(t) = x(n_A, t_{start} - t)$.

4) Delay Attack: The delay attack is modeled as inserting the delayed version of the original measurement time-series to corrupt the signal. This type of attack can be launched by compromising the global positioning system (GPS) signal associated with the PMUs. This can be expressed as $c(t) = x(n_A, t - t_d)$, where t_d is the amount of delay. For small delays, this type of cyber-attack is very challenging from the detection perspective.

5) Ramp Attack: In ramp attack, the attackers insert falsified measurements gradually in the buses under attack. This type of attack is challenging from the detection perspective because of not having abrupt changes at the onset of the attack. This attack can be specified as $c(t) = x(n_A, t_{start}) + m \times (t - t_{start}) + q(n_A,t)$, where m is the slope of change and $q(n_A,t)$ is the additive white Gaussian noise associated with the measurement devices at the bus n_A.

B. Reflection of cyber-attacks on Graph Spectra

In this subsection, analyses of the impacts of types and the location of cyber stresses in the smart grid on the graph-spectral domain are presented through GFT and local smoothness of the graph signals associated with the bus voltage angle measurements. Fig. 1 illustrates how the aforementioned cyber-attacks affect the time-varying graph signal of the system as well as the frequency domain representations associated with it. In Fig. 1(a), the cyber-attacks launched at the bus no. 102 at different moments of the day are shown on $x(102,t)$. Fig. 1(b), illustrates the changes in the amount of high graph-frequency components $\gamma_t^{'}$ associated with $x(n,t)$ over time. From this figure, we observe that these critically designed cyber-attacks are not well reflected on $\gamma_t^{'}$ values, although it is shown that these values can be used to detect simple cyber-attacks [6], [16]. Fig. 1(c) shows the time-varying local smoothness corresponding to the attack bus (vertex), $s(102,t)$. We observe that all the attacks are well reflected on $s(102,t)$. In particular, the delay attack at hour 19, which is even difficult to perceive from $x(102,t)$ itself, has a noticeable signature on $s(102,t)$. Fig. 1(d) shows the time-varying local smoothness values at vertex 92, which corresponds to a neighboring bus of the attacked bus, 102. From this figure, it can be noticed that although the values of $s(92,t)$ are affected by the cyber-attacks, they are not as prominent as in $s(102,t)$. The vertex in which the change of local smoothness value is the most can be considered as the location of the cyber-attack.

C. Effects of Node-degree of Stressed Buses on Graph Spectra

The degrees of the buses (i.e. nodes), which are under cyber-attack or physical stress, affect the graph spectra of the associated graph signal. The reason behind this is the localization of the eigenvectors of the graph Laplacian, $\mathbf{L}$. It is observed that the eigenvectors corresponding to the high graph-frequency components are more localized in nature and each of the high-frequency eigenvectors is localized in the vicinity of a particular vertex with a high degree. Whenever a cyber-attack occurs in a bus with a high degree, the GFT coefficient corresponding to the particular eigenvector localized in that vertex (i.e. bus) is mostly affected. In contrast, when a cyber-attack occurs at a bus with a low degree, several GFT coefficients are affected. Fig. 2 illustrates the scenarios for two buses having degrees 9 and 5.

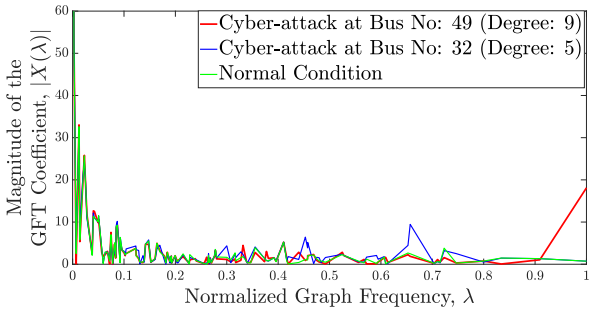

Fig. 2. The effects of degree of the attacked bus on GFT.

V. Comparative Analyses of Effects of Cyber and Physical Stresses

In this subsection, we have compared the effects of cyber and physical stresses on the graph-spectral domain of the corresponding graph signals. The motivation behind this comparison is that cyber-attacks and physical stresses affect the bus voltage angle graph signal differently that consequently has a distinguishable effect on the spectral domain representations of the graph signals. Since from the perspective of the monitoring and operation of the smart grid, characterization of stress is

crucial along with its detection and localization, analysis of their distinct signatures on the graph signal and its spectral representation is important.

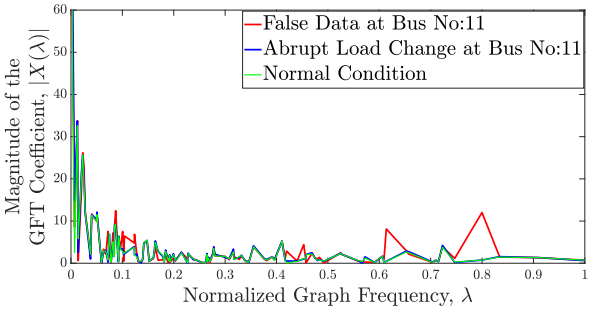

Fig. 3. The GFT values associated with the graph signals during normal condition, under FDIA at bus 11, and load change at bus 11.

Fig. 3 compares the GFT of the graph signals associates with a cyber-attack, and a physical stress occurring on the same bus. From the GFT representation of the graph signals, it can be observed that an abrupt change of a load at bus no. 11 affects the low-frequency components of the GFT. The abrupt load change being a physical event changes the power flow around a region centering bus no. 11. The bus-to-bus variations in the voltage angle measurements around bus no. 11 is smooth, which corresponds to low-frequency components of GFT. In contrast, the injection of false data at bus no. 11 introduces changes in the magnitude of some of the high-frequency components. A false data at bus no. 11 causes a change in the voltage angle value of bus no 11 only. For this reason, there introduces a sharp variation in the values of voltage angles (i.e. graph signal values) of bus no. 11 with respect to its neighboring values. This sharp variation corresponds to the high-frequency component of GFT.

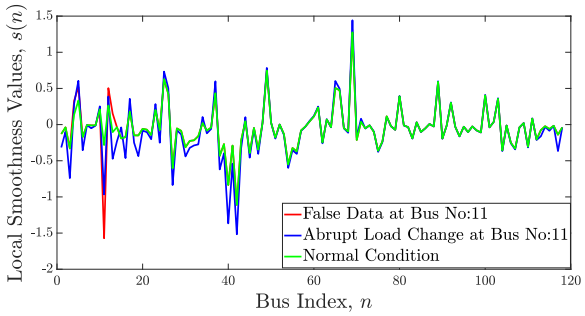

Fig. 4. The local smoothness values of the nodes during normal condition, cyber attack at bus 11, and load change at bus 11.

Fig. 4 illustrates the same pair of phenomena in terms of local smoothness values. We observe that false data injection at the bus no. 11 affects the local smoothness values of only a few vertices (vertices at a one-hop distance) around v_{11}, whereas the abrupt change in the load demand changes local smoothness values around a wider region centering vertex 11.

VI. Conclusion

In this paper, various cyber-attacks on the voltage angle time-series of the power grid are considered, and a technique for detecting and locating these cyber-attacks using the changes in local smoothness values of the associated graph signal have been proposed. The proposed technique is effective for detecting cyber-attacks that are challenging (e.g. ramp attack and delay attack) to detect by traditional techniques. This paper also presents a comparison between the effects of cyber and physical stresses (abrupt load change) on the graph spectral domain of the associated voltage angle graph signal.

Acknowledgement

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

References

[1] C. Sun, A. Hahn and C. Liu, "Cyber security of a power grid: State-of-the-art," Electrical Power and Energy Systems, 99, pp. 45-56, 2018.
[2] M. M. Hossain and C. Peng, "Cyber–physical security for on-going smart grid initiatives: a survey," in IET Cyber-Physical Systems: Theory Applications, vol. 5, issue 3, pp. 233-254, July 2020.
[3] E. Shereen and G. Dán, "Model-Based and Data-Driven Detectors for Time Synchronization Attacks Against PMUs," in IEEE Journal on Selected Areas in Commun., vol. 38, no. 1, pp. 169-179, Jan. 2020.
[4] A. S. Musleh, G. Chen and Z. Y. Dong, "A Survey on the Detection Algorithms for False Data Injection Attacks in Smart Grids," in IEEE Transactions on Smart Grid, vol. 11, no. 3, pp. 2218-2234, May 2020.
[5] G. Liang, J. Zhao, F. Luo, S. R. Weller and Z. Y. Dong, "A Review of False Data Injection Attacks Against Modern Power Systems," in IEEE Transactions on Smart Grid, vol. 8, no. 4, pp. 1630-1638, July 2017.
[6] M. A. Hasnat and M. Rahnamay-Naeini, "Detection and locating cyber and physical stresses in smart grids using graph signal processing," arXivpreprint arXiv:2006.06095, 2020.
[7] I. Jabłoński, "Graph Signal Processing in Applications to Sensor Networks, Smart Grids, and Smart Cities," in IEEE Sensors Journal, vol. 17, no. 23, pp. 7659-7666, 1 Dec.1, 2017.
[8] L. Goldsberry *et al.*, "Brain signal analytics from graph signal processing perspective," IEEE ICASSP, New Orleans, LA, 2017, pp. 851-855.
[9] S. Itani and D. Thanou, "A graph signal processing framework for the classification of temporal brain data," in Proc. European Signal Process. Conf., 2020, pp. 1180–1184.
[10] G. Cheung, E. Magli, Y. Tanaka and M. K. Ng, "Graph Spectral Image Processing," in Proc. of the IEEE, vol. 106, no. 5, pp. 907-930, 2018.
[11] V. K. Sharma, D. K. Srivastava and P. Mathur, "Efficient image steganography using graph signal processing," in IET Image Processing, vol. 12, no. 6, pp. 1065-1071, 2018.
[12] R. Ramakrishna and A. Scaglione, "On Modeling Voltage Phasor Measurements as Graph Signals," IEEE Data Science Workshop (DSW), Minneapolis, MN, USA, 2019, pp. 275-279.
[13] A. Kroizer, Y. C. Eldar and T. Routtenberg, "Modeling and Recovery of Graph Signals and Difference-Based Signals," IEEE GlobalSIP, Ottawa, ON, Canada, 2019, pp. 1-5.
[14] K. Schultz, M. Villafañe-Delgado, E. P. Reilly, G. M. Hwang and A. Saksena, "Graph Signal Processing for Infrastructure Resilience: Suitability and Future Directions," Resilience Week (RWS), Salt Lake City, ID, USA, 2020, pp. 64-70.
[15] R. Ramakrishna and A. Scaglione, "Detection of False Data Injection Attack Using Graph Signal Processing for the Power Grid," IEEE GlobalSIP, Ottawa, ON, Canada, 2019, pp. 1-5.
[16] E. Drayer and T. Routtenberg, "Detection of False Data Injection Attacks in Power Systems with Graph Fourier Transform," IEEE GlobalSIP, Anaheim, CA, USA, 2018, pp. 890-894.
[17] E. Drayer and T. Routtenberg, "Cyber Attack Localization in Smart Grids by Graph Modulation (Brief Announcement)," in CSCML, 2019.
[18] 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, issue 9, pp. 2219, 2020.
[19] M. Daković, L. Stanković, and E. Sejdić. "Local smoothness of graph signals," Mathematical Problems in Engineering, 2019.
[20] IEEE 118-Bus System, https://icseg.iti.illinois.edu/ieee-118-bus-system/.
[21] The New York Independent System Operator, Inc[US], https://www.nyiso.com/.
[22] R. D. Zimmerman Murillo-Sanchez and R. J. Thomas, "MATPOWER: Steady-State Operations, Planning and Analysis Tools for Power Systems Research and Education," in IEEE Trans. on Power Sys., vol. 26, no. 1, pp. 12–19, Feb. 2011.