Learning Power System's Graph Signals for Cyber and Physical Stress Classification

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

Mia Naeini
Department of Electrical Engineering
University of South Florida
Tampa, USA
mnaeini@usf.edu

2022 North American Power Symposium (NAPS) | 978-1-6654-9921-7/22/$31.00 ©2022 IEEE | DOI: 10.1109/NAPS56150.2022.10012213

***Abstract*—Situational awareness towards various types of cyber and physical stresses in power systems is critical for the reliable operation of these critical infrastructures. Identifying the type of stress that has occurred in the system is particularly crucial for deciding the corrective measures for mitigating the stress and also for future preventive planning. In this paper, a two-stage stress classification framework based on the learning of the power system's graph signals has been proposed. Specifically, graph signal processing (GSP) has been utilized to extract features from the power system's graph signals for building the models. Using GSP allows for capturing information about the interconnections and interactions among the components of the grid along with its spatio-temporal dynamics. It has been shown that this machine learning-based classification with GSP-based features is effective for classifying between cyber and physical stresses as well as further classifying among different types of cyber and physical stresses. Abrupt changes in the load demand and tripping of a transmission line are considered as examples of physical stresses, while five types of cyber attacks with no abrupt onset on the PMU time-series are considered as cyber stresses. Various GSP-based features are evaluated and a dimensionality reduction technique based on down-sampling in the graph-frequency domain is proposed. The classification performances have been evaluated across various classifiers using data under different noise levels.**

***Index Terms*—Graph signal learning, graph signal processing, classification, phasor measurement unit, cyber attack, smart grid.**

I. Introduction

Extensive integration of cyber elements into modern smart grids has provided immense opportunities for improving their reliability and performance; however, these systems can still experience various kinds of stresses in their cyber and physical layers. Situational awareness through detecting and locating such stresses using the available measurement data in the system is crucial for reliable and secure operation of the system; and as such it has earned great attention from the researchers and practitioners in this domain [1]–[3]. Once a stress is detected and located in the system, the next step would be to identify the type of the occurred stress in order to implement effective, corrective measures to mitigate the stress and also plan for preventive measures in future.

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

In this work, the focus is on the latter step through the classification of stresses after they have been detected. Specifically, a two-stage classification framework for cyber and physical stresses in smart grids has been proposed, which consists of a binary classifier to first classify between the cyber and physical stresses and a classifier to further classify among different types of cyber and physical stresses depending on the predicted binary class in the first stage. The proposed framework is based on learning power system's measurement data in the form of graph signals. Specifically, graph signal processing (GSP) has been utilized to extract features from power system's graph signals for building the models. Using GSP allows for capturing information about the interconnections and interactions among the components of the grid in the form of a graph along with its spatio-temporal dynamics. Various attributes related to the power system graph signals and their graph-spectral representations, such as, the Graph Fourier Transform (GFT) and the global and local smoothness of graph signals, have been shown to capture and encode the signatures of cyber and physical stresses in the grid [1], [3]. In our earlier work in [3], GSP-based techniques were developed for detecting and locating the stresses in smart grids. Here, the GSP tools are adopted to extract features in both vertex and frequency domains of the system's graph signals to train models that can further classify the stresses after they have been detected.

Abrupt load changes in the buses and tripping of transmission lines are examples of common physical stresses that are considered in this work and their signatures are reflected in the graph signals of the system. The proposed models and analysis can be applied to other types of physical stresses, such as oscillatory events, and reactive power events depending on the availability of measurement data. In addition, various types of cyber attacks can disrupt the normal operation of the power system by targeting the confidentiality, availability, and integrity of the data [4].

In this paper, five types of cyber attacks including Denial of Service (DoS) attack, False Data Injection Attack (FDIA), and synchronization-based attacks including replay attack, ramp attack, and delay attack, are considered and modeled on the PMU time-series. Specifically, the bus voltage angle measurement time-series of each bus are considered; describing the state of the grid components. Following our previous work

[3], the cyber attacks are defined in such a way that they do not introduce any sharp changes in the values of the time-series at their onset. As such, they are not easily detectable by the existing residual-based or abrupt change detection techniques. However, our experiments have revealed that information about dynamic interactions among the components of the grid (e.g., the spatio-temporal correlations among the states) embeds important information about these sophisticated attacks [3], [5].

The key contributions of this work are summarized next:

- A two-stage classification framework for power system stresses has been proposed based on learning power system's graph signals. The proposed framework involves incorporating GSP-based features into machine learning (ML) methods for leveraging the potential of GSP in capturing the topological as well as interaction and interdependency dynamics among the components of the grid for improved classification accuracy.
- Various GSP-based features of time-varying voltage angle graph signals at different stages of the classification are evaluated.
- A technique for reducing the dimensionality of the GSP-based features based on down-sampling in the graph-frequency domain is proposed.
- The classification performances have been evaluated across various ML classifiers using data under different noise levels.

II. Related Work

Over the past few decades, the reliability and security of smart grids under various cyber and physical stresses have been being studied [3], [4], [6]. With the availability of data due to the extensive deployment of smart measuring devices (e.g., PMUs) in the power systems, data-driven analyses for the detection, characterization, and classification of stresses are gaining more attention. Among the studies of stress classification in the smart grid, the classification of physical stresses (or events) using ML techniques has been extensively studied [7]–[11]. For instance, Rafferty and Liu, [10], considered three types of physical stresses: generation dip, loss of load, and line tripping for classification at the PMU level using the quadratic discriminant analysis (QDA) method that also facilitates the identification of unknown events for further human interaction. In [10], the frequency, phase angle, voltage magnitude, and their time derivatives are considered as the features and their relative importance is studied. Liu *et al.* [11] present a detailed analysis of the classification of four types of power system events including frequency events, line outage, transformer outage, and oscillation events by applying various benchmark classification techniques. The proposed three-step technique involves pre-processing of real-world imperfect PMU data, extraction of fine-grained event waveform data after the detection of the event, and extraction of useful features for classification from the waveform of multiple attributes. The analysis has revealed that each event has signatures on the waveform of different particular attributes (e.g., voltage magnitude) and the signal similarity among different PMUs, under different events, is different. In [12], along with the physical stresses (e.g., line fault and generation loss), fake events created by false data injection are also considered for classification.

Detection, locating, and characterization of cyber and physical stresses in the smart grids by modeling the grid data as graph signals has become a topic of interest among researchers in recent years. In [1], [13] the authors provided GSP-based frameworks for FDIA detection in the power grid in which the significant presence of high-graph frequency components has been used as the indicator of falsified measurements. Shereen *et al.* [2] proposed leveraging GFT along with machine learning algorithms to detect and locate time-synchronization attacks in the smart grid. In one of our previous works [3], we introduced two GSP-based techniques, namely, *local smoothness second time-derivative (LSSTD)* and *vertex-frequency energy distribution (VFED)* for detecting and locating physical stresses as well as sophisticatedly designed cyber attacks with no sharp change of values at the attack onset. In another work [14], we discussed the characterization of the cyber attacks through a GSP framework which involved classifying between the clustered cyber attacks and multiple random cyber attacks, attack center, and attack radius estimation in the case of clustered cyber attacks. In addition, techniques based on graph neural networks (GNN) to capture the structured interactions and dependencies in data have also been applied to this problem. For instance, Boyaci *et al.* [15] proposed a GNN model for detecting and locating FDIA in the grid. In [16], the authors propose the *infinite impulse response graph neural network (IIR-GNN)* model for locating cyber attacks in the smart grid. Yuan *et al.* [17] also propose a GNN-based event classification technique in which the latent interaction graphs among different PMUs are learned from the PMU data. In the current work, we propose to combine a GSP-based analysis and feature extraction method with ML models for the classification of different cyber and physical stresses in two stages.

III. Classification Problem Formulation

A. A Short Review of GSP Concepts

The power grid has been modeled by a dynamic weighted graph, $\mathcal{G}(t) = (\mathcal{V}, \mathcal{E}(t), \mathcal{W}(t))$, representing the *known topology* of the grid at time t. The set of vertices, $\mathcal{V}$, represents the buses of the grid and is considered to remain unchanged over time. The set of edges $\mathcal{E}(t) = \{e_{ij}(t) : (i,j) \in \mathcal{V} \times \mathcal{V}\}$ represents the transmission lines that are active at time t and thus may change over time in the event of a line outage, an intentional line tripping, and restoration of a transmission line. The set of edge weights, $\mathcal{W}(t)$ includes w_{ij} elements, which represents the i-th row and j-th column of the weight matrix at time t denoted by $\mathbf{W}_t$. The weight matrix $\mathbf{W}_t$ is defined in such a way that the Laplacian matrix $\mathbf{L}_t = \mathbf{D}_t - \mathbf{W}_t$ of the graph represents the imaginary part of the admittance matrix associated with the known topology of the grid at time, t, where $\mathbf{D}_t$ is the degree matrix of the graph, $\mathcal{G}(t)$.

The time-varying graph signal, $x(n,t)$ defined over the graph, $\mathcal{G}(t)$, is a mapping of the graph vertices to real numbers, $x : \mathcal{V} \rightarrow \mathbb{R}$ that, in this work, represents the value of the voltage angle at bus $n \in \mathcal{V}$ at time t.

The graph spectral domain of the graph signal is characterized by the GFT. Let λ_{k_t} and $u_{k_t}(n)$ be the $k-$th eigenvalue and $k-$th eigenvector of $\mathbf{L}_t$ representing the graph-frequencies and the basis graph signals for GFT, respectively. The GFT of the graph signal, $x(n,t)$ at time, t is described as:

$$X(\lambda_{k_t}, t) = \sum_{n=1}^{N} x(n,t) u^*_{k_t}(n). \tag{1}$$

The local smoothness of the graph signal $x(n,t)$ at time t is expressed as:

$$s(n,t) = \frac{\mathbf{L}_t \underline{\mathbf{x}}_t}{x(n,t)}, \tag{2}$$

when $x(n,t) \neq 0$ and $\underline{\mathbf{x}}_t$ is the vector form of the graph signal $x(n,t)$ at time t. These are the GSP concepts used in this paper. A more detailed discussion about the GSP basics, especially in the power system context can be obtained in our previous work [3].

B. Classification Model

In this paper, a two-stage stress classification framework has been proposed. When a stress is detected in the grid at time t_d, the first step is to determine whether it is a cyber or physical stress. This binary classification task is performed in the first stage of the proposed two-stage classification scheme. The second stage involves classification among different physical stresses and different types of cyber attacks. In this paper, abrupt load changes and transmission line outages as physical stresses and five types of cyber attacks (DoS, FDIA, replay, ramp, and delay attacks) are considered. These stresses are modeled on the voltage angle time-series. A detailed description on the model of these stresses and their characteristics can be found in [3].

For the classification tasks at both stages, first, a set of features will be engineered from the associated graph signals, $x(n,t)$, starting from when the attack was detected, t_d, for a duration of Δt_w. The extracted features can then be fed to any ML-based classifier. The features being extracted from the time-varying graph signals contain temporal as well as topological information to incorporate into the classification framework. The binary classification (i.e., physical stress vs. cyber attack) at the first stage can be formulated as:

$$\mathbf{y} = f(\mathbf{\Psi}(x(n,t))), \quad t_d \leq t \leq t_d + \Delta t_w, \tag{3}$$

where $\mathbf{y} \in \{$Physical stress, Cyber attack$\}$ and $\mathbf{\Psi}(x(n,t))$ is the graph signal feature matrix obtained from the time-varying graph signal $x(n,t)$ for the time interval Δt_w, starting from the moment of the detection. For the stresses that are detected as physical ones, the next stage classification involves classifying them between abrupt load changes and transmission line outages, which can be expressed as:

$$\mathbf{z_p} = g(\mathbf{\Psi_p}(x(n,t))), \quad t_d \leq t \leq t_d + \Delta t_w, \tag{4}$$

where $\mathbf{z_p} \in \{$Abrupt load changes, Line failure$\}$ and $\mathbf{\Psi_p}(x(n,t))$ is the graph signal feature matrix obtained from the time-varying graph signal $x(n,t)$ for the time interval Δt_w, starting from the moment of the detection. Similar formulation can be shown for stresses that are classified as cyber attack in the first stage:

$$\mathbf{z_c} = h(\mathbf{\Psi_c}(x(n,t))), \quad t_d \leq t \leq t_d + \Delta t_w, \tag{5}$$

where $\mathbf{z_c} \in \{$DoS, FDIA, Replay attack, Ramp attack, Delay attack$\}$ and $\mathbf{\Psi_c}(x(n,t))$ is the graph signal feature matrix obtained from the time-varying graph signal $x(n,t)$ for the time interval Δt_w, starting from the moment of the detection of the cyber attack.

IV. GSP-based Feature Extraction

A. Different Types of GSP-based Features

For the classification using the proposed method, GSP-based features are extracted from the time-varying graph signals from the moment of detecting the stress, t_d to the end of the stress data window, $t_d + \Delta t_w$. In our previous works [3], [14] and our extensive simulations on the IEEE 118 bus case [18], we have observed that in different cyber and physical stresses different set of features are more suitable in classifications. In this section, different types of GSP-based features will be presented along with a discussion on their suitability in different cyber and physical stress scenarios. A general technique for reducing the number of features of the same type has also been proposed.

1) Features extracted from the moment of detection, t_d: A number of features denoted by feature vector $\underline{\psi}_1$ are proposed to be extracted from the graph signal just at the moment of detecting the stress, i.e., $x(n,t_d)$. An example of such features is the GFT values of the graph signal at the moment of detection. In this case, the $l-$th element of the $\underline{\psi}_1$ can be expressed as: $\psi_1(l) = X(\lambda_{l_{t_d}}, t_d)$, where X is derived from equation (1). The local smoothness values of the graph signal at the moment of the detection is another set of features of this type; for which, the $l-$th element of the $\underline{\psi}_1$ can be expressed as $\psi_1(l) = s(l,t_d)$, where s can be derived from equation (2). The two aforementioned sets of features capture information of structure, interdependency, and interactions among the components of the grid; however, being calculated on a single snapshot of the time-varying graph signal (at $t = t_d$), they do not contain the temporal evolution information of the signal values. Our simulations have shown that features of this type are effective for classification between cyber and physical stresses as well as for the classification between abrupt load changes and transmission line failures but fail to classify among cyber attacks, since the cyber attacks are distinguished mostly by their temporal signatures.

2) Features extracted using GFT of temporal statistics: The next type of features considered in this work are calculated by applying GSP techniques (e.g., GFT and local smoothness) over the temporal statistics of $x(n,t)$ during the time window after the detection of stress. Let $\mathcal{T}(.)$ be the operator for determining any temporal statistics (e.g., mean,

standard deviation, and range) of any time-varying graph signal within a window of time. We denote this type of feature vectors by $\underline{\psi}_2$. One example of such features can be derived by taking the GFT of the graph signal, which is obtained by computing the temporal standard deviation of the time derivative of the original graph signal values at each bus within the stress time window. This feature can be represented by $\psi_2(l) = \sum_{n=1}^{N} \mathcal{T}(\frac{d}{dt}x(n,t))u_{l_t}^*(n)$, for $t_d \leq t \leq t_d + \Delta t_w$. Here, $\mathcal{T}(.)$ signifies temporal standard deviation of the signal values at each bus. By containing the temporal information along with the information and interdependency among the components, these type of features are suitable for classifying among cyber attacks with distinguishable temporal signature on the time series data.

3) Features extracted taking temporal statistics of the time-varying GFT values: The features of the third type involves taking temporal statistics of the GFT values calculated at every time instant within Δt_w. For these features, the $l-$th element of the feature vector $\underline{\psi}_3$ can be expressed as $\psi_3(l) = \mathcal{T}(X(\lambda_{l_t}, t))$, for $t_d \leq t \leq t_d + \Delta t_w$. Similar, to the previous type of features, features of this type also contain both temporal and interconnection information and therefore applicable to the classification among cyber attacks.

B. Dimensionality Reduction of the GFT-based Features

All the feature vectors discussed in the previous section, are of dimensionality equal to the number of buses in the grid, i.e., N. Moreover, the classification among different types of cyber attacks requires the combination of different types of features, which makes the dimensionality of the classification problem large. The high dimensionality of the feature space raises the computational cost of implementing the proposed GSP-based learning classification technique. However, if the feature set is GFT-based, the dimensionality can be reduced by taking a smaller subset of the GFT samples, i.e., down-sampling in the graph-frequency domain. In this work, instead of taking all the GFT samples, K equally spaced GFT values are considered, where $K < N$. The equally spaced samples ensure the presence of GFT samples in all ranges of graph-frequencies and serve as a good representative of the whole spectral information. This concept is similar to the concept of down-sampling the discrete Fourier transform in classical signal processing; however, the analogy is not strictly perfect due to the localized basis functions of GFT representation.

V. Performance Evaluation

A. Simulation Details

In this work, all the simulations have been performed on the IEEE 118 bus systems, using MATPOWER [19]. The load patterns are extracted from the actual daily load profile from New York Independent Operator (NYISO) [20] and have been added to the default MATPOWER load demands to create time series data as described in [5]. In total 10,000 different types of physical stresses and cyber attacks are generated using MATPOWER at different times and different locations of the grid, which are randomly selected with uniform probability distributions. For the generation of cyber attacks, the time-series-based models in [3] have been used in which there is no sharp change in the signal values at the attack onset. For the classification among these cyber attacks presented in this work, we consider, $\Delta t_w = 10$ samples; however, this parameter can be tuned depending on the grid and the application. For all the classifications, the models are trained with 80% of the data and tested on the rest of the data.

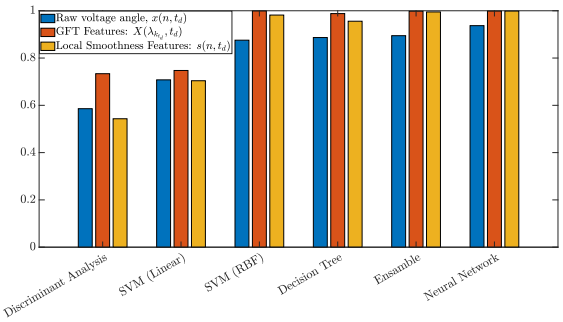


Fig. 1: Classification accuracy for different ML methods for the first-stage binary classification between physical and cyber stresses. $45dB$ noise level is considered in all the cases.

Among different machine learning classifiers, decision tree, discriminant analysis, ensemble method, support vector machine (SVM) with linear and radial basis function (RBF) kernels, and neural network have been used. The neural network classifier consists of two hidden layers with 25 and 10 neurons, respectively, with ReLu activation functions in each layer. All the classifiers have been implemented using MATLAB classifier functions.

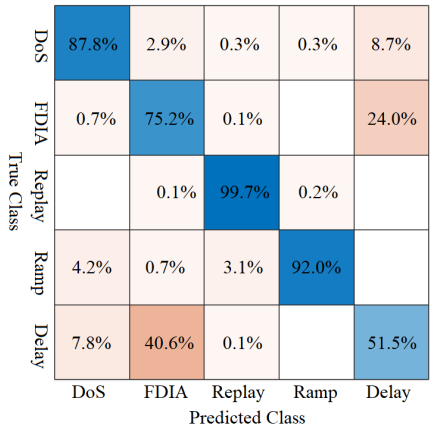


Fig. 2: Confusion matrix for cyber attack classification using GSL method. Neural network classifier has been used as the ML classifier.

B. Performance of the Classification

The simulation results show that, in both stages of the classifications, the GSL technique outperforms direct machine learning-based classification applied to the raw voltage angle data. Fig. 1 illustrates the classification accuracy of the different machine learning classification algorithms for the

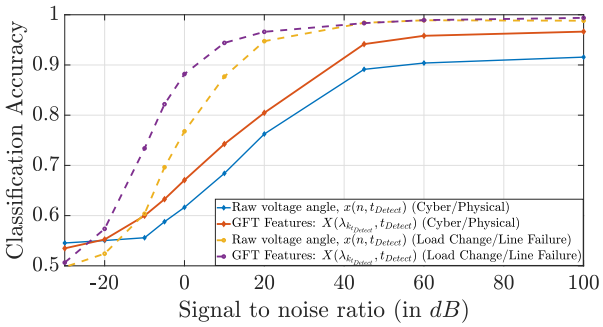


Fig. 3: Dependency of the classification performance on the noise level of the data. Decision Tree classifier has been used for all the cases.

first-stage binary classification between cyber and physical stresses using raw voltage angle data and using GSP-based features. Two different candidate feature vectors of the first type (i.e., feature extracted at t_d): GFT and local smoothness features are considered. From the figure, it is observed that both the GFT and local smoothness-based features outperform the direct classification on raw voltage angle data for all the machine learning methods for the signal-to-noise ratio of $45 \;\; dB$. Similar results have been obtained for the abrupt load change vs. line failure classification at the same noise level. However, among the GSP-based features, the GFT-based ones are preferable over the local smoothness-based features, mostly because of two reasons: 1) the GFT-based provide consistent performance at different noise level, while the performance of the local smoothness-based ones deteriorates significantly with increasing noise levels, 2) the dimensionality reduction method discussed in Section IV(B) is only applicable to the GFT-based features.

For the classification among the cyber attacks on noiseless data, the GSL technique with the GFT-based sets of features successfully classifies the five types of cyber attacks. The accuracies of classification using the decision tree and neural network classifiers are, respectively, 0.814 and 0.813. However, for this classification, multiple sets of features of different types are required. By observing the performance of different combinations of the set of features the following set of features are considered to be appropriate for the classification among the cyber attacks: Firstly, the GFT of the temporal standard deviation of the time-derivative signal, $\sum_{n=1}^{N} \mathcal{T}(\frac{d}{dt}x(n,t))u^*_{k_t}(n)$, for $t_d \leq t \leq t_d + \Delta t_w$. Here, $\mathcal{T}(.)$ signifies the temporal standard deviation of the signal values at each bus. Secondly, the GFT of the temporal standard deviation of the original signal, $\sum_{n=1}^{N} \mathcal{T}(x(n,t))u^*_{k_t}(n)$, for $t_d \leq t \leq t_d + \Delta t_w$. Thirdly, the GFT of the graph signal, $x(n,t_d) - x(n,t_d + t_w)$ calculated as: $\sum_{n=1}^{N}[x(n,t_d) - x(n,t_d + t_w)]u^*_{k_t}(n)$, for $t_d \leq t \leq t_d + \Delta t_w$. Finally, the temporal mean of $X(\lambda_{k_t}, t)$ for $t_d \leq t \leq t_d + \Delta t_w$. Fig. 2 presents the confusion matrix for the classification among cyber attacks. The GSL-based classification technique classifies the cyber attacks with good accuracy except for the relatively higher misclassification rates between the FDIA and the delay attack.

C. Noise Sensitivity of Classification Performance

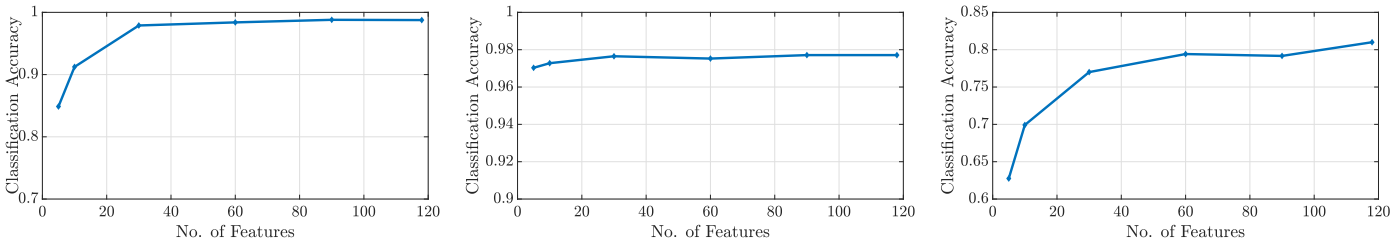
The classification accuracy for the first-stage classification between the cyber and physical stresses and the second-stage classification between the abrupt changes of loads and the line failure (in the case of the prediction as physical stress at the first stage) have been analyzed as a function of the signal-to-noise ratio (SNR) of the additive noise present in the voltage angle data. As illustrated in Fig. 3, for both classifications, the GSL classification technique with GFT features outperforms direct machine learning-based classification at all levels of noise intensity. However, the classification among the cyber attacks works only on noise-free data and achieves very limited accuracy for noise levels below $100 \; dB$ SNR. This is due to the fact that these sophisticatedly designed cyber attacks introduce very small changes in signal values which are comparable to noise as discussed in [3].

D. Classification Performance with Reduced Number of Features

Fig. 4 illustrates the classification performance with the reduced number of GFT-based features as suggested in Section IV(B). From the figure, it is observed that for all the classification tasks in both stages, it is possible to reduce the number of features using the graph-frequency domain down-sampling keeping the classification performances at reasonable levels. As an example, for the first-stage binary classification between cyber and physical stresses, a classification accuracy of 0.95 is achievable with only 20 GFT features instead of all the 118 GSP features for the IEEE 118 bus system. It is worth mentioning that for the classification among cyber attacks, it is required to apply the graph-frequency domain down-sampling separately on the four types of GFT-based features mentioned in Section V(B).

VI. Conclusion

In this work, a two-stage classification framework for classifying cyber and physical stresses in the smart grid has been proposed based on learning power system's graph signals features. This approach involves combining GSP-based analysis and feature extraction and machine learning-based classification methods. The first stage classifies between cyber and physical stresses, while the second stage involves classification among different physical stresses or among cyber attacks depending on the predicted class at the first stage. Various GSP-based features are designed to capture both the topological and connectivity information of the system as well as temporal information in the signals into machine learning methods. The experimental results show that the proposed GSP-based learning technique outperforms the machine learning-based classification techniques that are directly applied to the measurement data, for different levels of signal noise. A technique for reducing the number of GSP-based features has also been proposed based on down-sampling the graph frequency domain for efficient implementation of the classification techniques.



(a) (b) (c)

Fig. 4: Classification performance with reduced numbers of features (by graph-frequency domain down-sampling) for (a) cyber vs. physical stress classification, (b) among physical stresses classification, (c) among cyber stresses classification. Decision tree has been used as the ML-based classifier for all the cases.

REFERENCES

[1] 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.

[2] E. Shereen, R. Ramakrishna and G. Dán, "Detection and Localization of PMU Time Synchronization Attacks via Graph Signal Processing," in IEEE Transactions on Smart Grid, vol. 13, no. 4, pp. 3241-3254, July 2022.

[3] M. A. Hasnat and M. Rahnamay-Naeini, "A Graph Signal Processing Framework for Detecting and Locating Cyber and Physical Stresses in Smart Grids," in IEEE Transactions on Smart Grid, vol. 13, no. 5, pp. 3688-3699, Sept. 2022.

[4] M. Z. Gunduz and R. Das, "Analysis of cyber-attacks on smart grid applications," International Conference on Artificial Intelligence and Data Processing (IDAP), 2018, pp. 1-5.

[5] M. A. Hasnat and M. Rahnamay-Naeini, "A Data-Driven Dynamic State Estimation for Smart Grids under DoS Attack using State Correlations," North American Power Symposium (NAPS), 2019, pp. 1-6.

[6] X. Cai, Q. Wang, Y. Tang and L. Zhu, "Review of Cyber-attacks and Defense Research on Cyber Physical Power System," IEEE Sustainable Power and Energy Conference (iSPEC), 2019, pp. 487-492.

[7] Y. Chen, L. Xie and P. R. Kumar, "Power system event classification via dimensionality reduction of synchrophasor data," IEEE 8th Sensor Array and Multichannel Signal Processing Workshop (SAM), 2014, pp. 57-60.

[8] J. Cordova, R. Arghandeh, Y. Zhou, S. Wesolowski, W. Wu and S. Matthias, "Shape-based data analysis for event classification in power systems," IEEE Manchester PowerTech, 2017, pp. 1-6.

[9] G. A. Susto, A. Cenedese and M. Terzi, "Time-series classification methods: Review and applications to power systems data," in Big data application in power systems, pp. 179–220, Elsevier, 2018.

[10] M. Rafferty and X. A. Liu, "Automatic Power System Event Classification Using Quadratic Discriminant Analysis on PMU Data," IEEE Power & Energy Society General Meeting (PESGM), 2020, pp. 1-6.

[11] Yunchuan Liu, Lei Yang, Amir Ghasemkhani, Hanif Livani, Virgilio A. Centeno, Pin-Yu Chen and Junshan Zhang, "Robust Event Classification Using Imperfect Real-world PMU Data," in arXiv preprint, arXiv:2110.10128, 2021.

[12] R. Ma, S. Basumallik and S. Eftekharnejad, "A PMU-Based Data-Driven Approach for Classifying Power System Events Considering Cyberattacks," in IEEE Systems Journal, vol. 14, no. 3, pp. 3558-3569, Sept. 2020.

[13] 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.

[14] M. A. Hasnat and M. Rahnamay-Naeini, "Characterization and Classification of Cyber Attacks in Smart Grids using Local Smoothness of Graph Signals," North American Power Symposium (NAPS), 2021, pp. 01-06.

[15] O. Boyaci et al., "Graph Neural Networks Based Detection of Stealth False Data Injection Attacks in Smart Grids," in IEEE Systems Journal, vol. 16, no. 2, pp. 2946-2957, June 2022.

[16] O. Boyaci et al., "Infinite Impulse Response Graph Neural Networks for Cyberattack Localization in Smart Grids," in arXiv preprint arXiv:2206.12527, 2022.

[17] Y. Yuan, Z. Wang and Y. Wang, "Learning Latent Interactions for Event Identification via Graph Neural Networks and PMU Data," in IEEE Transactions on Power Systems, 2022.

[18] IEEE 118-Bus System, Illinois Center for a Smarter Electric Grid (ICSEG), https://icseg.iti.illinois.edu/ieee-118-bus-system/, accessed July 15, 2022.

[19] 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.

[20] Load Data, New York Independent System Operator, https://www.nyiso.com/load-data, accessed July 15, 2022.