June 2023

Enhancing Smart Grid Security and Reliability through Graph Signal Processing and Energy Data Analytics

Md Abul Hasnat
University of South Florida

Enhancing Smart Grid Security and Reliability through Graph Signal Processing and Energy Data Analytics

by

Md Abul Hasnat

A dissertation submitted in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
Department of Electrical Engineering
College of Engineering
University of South Florida

Major Professor: Mia Naeini, Ph.D.
Ismail Uysal, Ph.D.
Yasin Yilmaz, Ph.D.
Sriram Chellappan, Ph.D.
Kaiqi Xiong, Ph.D.

Date of Approval:
June 21, 2023

Keywords: Cyber-physical Systems, Power Grid, Situational Awareness, Cyber Security, Data Analysis

Dedication

To my parents and family members.

Acknowledgments

This statement expresses my sincere gratitude and earnest appreciation to the individuals and organizations who had significant roles in the completion of this Ph.D. dissertation.

First, I would like to express my heartiest gratitude to my major professor, Dr. Mia Naeini. I am extremely fortunate to have such an exceptional advisor in my Ph.D. journey. For the last five years, her constant support, precious guidance, and ceaseless patience were most important for my academic growth and thereby for the completion of this dissertation. I am truly indebted to her for the expertise, encouragement, and insightful feedback she provided me during this period.

I would also like to extend my gratitude to the other members of my dissertation committee, Dr. Ismail Uysal, Dr. Yasin Yilmaz, Dr. Sriram Chellappan, and Dr. Kaiqi Xiong. Their expertise, invaluable insights, and constructive criticism have significantly contributed to the quality of this research. I am grateful for their time, effort, and commitment to excellence.

I am immensely grateful to the Electrical Engineering Department at the University of South Florida for providing me with an encouraging academic environment with excellent resources. I am particularly thankful to my TA supervisor Dr. Nasir Ghani. I am also thankful for the administrative staff who provided assistance and support at every stage of my academic journey. My sincere appreciation goes to my lab mates Upama, Jakir, Naeem, and Hamed. Their valuable discussions and suggestions had been precious in shaping my ideas and enhancing my research skills. I am grateful for their constant support and friendship.

Furthermore, I would like to acknowledge National Science Foundation (under grant No. 1761471, 2118510, and 2238658) and the Defense Threat Reduction Agency Basic Research Program (under grant No. HDTRA1- 13-1-0020) that have generously supported my re-

search. Their financial assistance has been important for conducting experiments, attending conferences and publishing journals, and pursuing various academic activities. I earnestly appreciate their investment in my research and the opportunities it has provided.

Finally, I would like to express my deep gratitude and purest love to my parents, brother, and family members for the mental support they provided me with throughout my Ph.D. journey. I would also like to thank my friends in Tampa and outside for their companionship and encouragement.

Table of Contents

List of Tables

List of Figures

Abstract

Situational awareness in a large, dynamic, and complex cyber-physical critical infrastructure, such as a smart grid, is vital for ensuring its smooth and uninterrupted operation. With the evolving realities of the modern-day smart grids, new challenges associated with the situational awareness of these systems are emerging that demand intelligent and efficient solutions. This dissertation intends to address several problems for enhancing situational awareness by studying the dynamic interaction among the components of the smart grids through energy data analytics using various data-driven, machine learning, and graph signal processing (GSP) techniques. The presented work provides valuable insight into the data-driven analysis of the dynamics of cyber-physical power systems and contributes to the research regarding the security and reliability of smart grids.

Variations in load and generations as well as the operating states and conditions of the grid equipment, and the weather and environmental factors make the smart grid's dynamics stochastic with complex interactions among their components. This dissertation attempts to understand this dynamicity and interactions using numerical and analytical approaches by exploiting the measurement data captured by numerous sensors deployed throughout the system. The analysis of the correlation among the power system states is one of the energy data analytic tools used in this dissertation to study the behavior of the power system in normal operating conditions as well as under cyber and physical stresses. However, since the smart grid is a networked system, introducing the knowledge of topology and connectivity of its components in the analyses facilitates a better understanding of the system's behavior. GSP enables an explicit inclusion of the topological and connectivity information by extending the theories of classical signal processing to the irregular graph domain. Modeling the power grid as a graph by considering the buses as the nodes and the transmission lines as the edges, the power system measurements and states can be viewed as graph signals defined in the non-Euclidean vertex space of the graph. In this dissertation, both the correlation-based and the GSP-based study of the power system have been utilized in several applications related to the security and reliability of the smart grid.

Four specific applications for enhancing situational awareness in smart grids towards security and reliability stresses are studied. The first application is the data-driven detection and location identification of cyber attacks and physical stresses in the system. Timely detection and precise localization of stresses and anomalies are crucial for the quick restoration of the grid to its normal operating condition. As soon as a stress is detected and located in the system, the next task should be its proper classification and characterization for determining the best response, the root cause, and predicting similar scenarios in the future. The third application is the recovery of smart grid's states that are missing or corrupted due to cyber-attacks and physical damages to the measurement devices to ensure the observability of the system, which is crucial for monitoring and operation purposes. The final application is analyzing the nature of propagation of a single bus perturbation through the system. Moreover, in some of the aforementioned applications, machine learning and neural network models are used along with feature extraction techniques using GSP and correlation-based methods. In the majority of the studies, the problems are approached using analytical analyses, which are then verified through experiments by simulations. The results of the experiments have been presented, interpreted, and compared with the benchmark techniques. Future work directions are also discussed for each application.

Chapter 1: Introduction

Since the guarantee of a seamless supply of electricity to the consumers is a glaring necessity in modern days, a very sophisticated, well-maintained, and effective system is essential for combining and synchronizing different parts of the energy system: generation, transmission, and distribution systems. A smart grid [1, 2], as its name suggests, refers to a union of many intelligent systems working together to ensure a continual supply of electrical energy produced from various natural resources to the customers effectively and autonomously. This dissertation focuses on several aspects related to the security and reliability of smart grids and provides mathematical, numerical, and simulation-based analyses of these aspects, and suggests solutions for the related problems by developing techniques and tools based on energy data analytics [3] and *graph signal processing* [4, 5].

A smart grid consists of a tightly coupled communication system and an electric power grid [1]. The communication system is the cyber layer, which is responsible for the flow of information throughout the system that facilitates monitoring of the system using the meter-captured measurements as well as propagating control instructions to the components. The grid is the physical layer that enables the transfer of electric power from the generators to the customers through the transmission and distribution systems. Since a smart grid is a critical infrastructure encompassing a large geographical area with complex and dynamic interactions among its components, it requires monitoring by a wide area monitoring system (WAMS) [6]. The WAMS involves the deployment of a large number of measurement devices (i.e., sensors) throughout the system and the processing of the data acquired by those devices for monitoring, operation, and maintenance of the infrastructures.

1.1 Research Problems in Situational Awareness

Smart grids are being evolved every day. In recent years, with the widespread integration of renewable distributed energy resources (DERs) [7] and electric vehicles (EVs) [8], smart grids have become more stochastic and complex than ever. Although the cyber layer facilitates the efficient monitoring and operation of these systems, it makes them vulnerable to different types of cyber attacks by adversaries [9, 10]. Moreover, various events and anomalies related to the dynamics of the power system at the physical layer are perpetual concerns in electrical energy systems. Therefore, ensuring *situational awareness* [2] becomes crucial in order to maintain the reliability and security of the grid, which is a must for providing a seamless energy supply.

Situational awareness [2] in the smart grid involves the collection of measurement data through the sensors and the measurement devices deployed throughout the grid for estimating the states of the grid, visualization, analysis, and interpretation of the data in real-time or near-real-time to detect and locate events and anomalies and predicting instabilities and stresses in the grid, and supporting the grid operators with decisions and alarms. Many problems related to situational awareness in smart grids can be addressed by tools and techniques, such as signal processing and statistical data analysis. Moreover, with the large-scale integration of high-resolution measurement devices (e.g., phasor measurement units (PMU), advanced metering infrastructure (AMI)) in the grid [6] and with the progress of computational resources, data analytic and machine learning techniques [3] are becoming more popular to solve the situation awareness-related issues. In this dissertation, several problems related to situational awareness and various techniques to address them using graph signal processing, statistical analysis, and machine learning are presented.

1.2 Situational Awareness-Related Problems

One of the key problems related to situational awareness in smart grids is the detection and location identification of the cyber and physical stresses in the grid. The cyber stresses involve adversary attacks compromising the availability, confidentiality, and integrity of the measurement data in the system, e.g., denial-of-service (DoS) attacks, false data injection attacks (FDIA), time synchronization attacks, etc [9, 10]. The physical stresses include various power dynamical events that deviate the grid from normal operating conditions [11]. While the physical and cyber stresses can lead the power grid to instability and failures, the cyber stresses can also lead the grid operators and the automated systems control mechanisms to make incorrect decisions. Timely detection of both events is important in terms of situational awareness, enabling rapid restoration of normal conditions and mitigating potential grid stress that could result in more severe damages. Despite being studied by the researchers for several years the detection and location identification problem is considered as an open and challenging problem [9]. This is mainly due to the continuous introduction of innovative and sophisticated designs for cyber attacks, aimed at evading detection mechanisms, and the evolving conditions within the modern grid, such as the integration of DERs and EVs.

As soon as a stress is detected and located in the grid, the immediate concern is to learn about the type and the characteristics of the stress [12, 13]. This is important for two reasons: identifying the root cause of the stress and eliminating it to restore normal operation and to develop strategies to prevent and treat similar stresses in the future. This problem includes the classification of the stresses between cyber and physical as well as among different types of cyber-attacks and physical stresses.

In this dissertation, the following problems regarding the classification of the stresses are considered. First, the classification between cyber and physical stresses and then classification among five different sophisticatedly designed cyber attacks on the time series measurements, as well as, the classification between two well-known physical events including line tripping and abrupt load change are considered. This dissertation also includes classification between clustered and random cyber attacks and estimating attack centers and radius in case of clustered cyber attacks.

Recovery of the missing states [14, 15] is another problem associated with situational awareness in power systems that have been considered in this dissertation. The knowledge of the grid's state is always important for grid operation, maintenance, and monitoring purposes, and they are mostly represented with the bus voltage phasors in the power grid context. Incomplete and incorrect knowledge of the states can lead to wrong operating decisions, which may cause a stressed or unstable grid. The state of the power system is either directly measured by the mounted sensors on the electrical components (e.g., buses) or estimated using state estimation methods. The states of the power system can become unobservable due to various reasons including DoS attacks, physical damage to the measuring devices, etc, and recovering the missing state is crucial for continuing the normal operation of the smart grid.

The optimum placement of measurement devices (e.g., PMUs) [16, 17] is another related problem to the state recovery problem and is also considered in this dissertation. This problem studies the placement of devices in such a way that it maximizes the observability of the states and minimizes the placement cost of the devices. However, the problem can be seen from different perspectives depending on the type of data representing the states, the application in which the state values would be used, and the operating conditions of the grid. This research addresses the issue considering the bus voltage angles as the state variable.

The last problem related to situational awareness in smart grids studied in this dissertation is the analysis of a single bus perturbation in the grid. This study focuses on how the effect of physical stress in the form of load or generation alteration in a single bus propagates throughout the electrical network. This analysis is important to understand how a physical event can affect different parts of the power system and initiate further issues (e.g., instability, islanding, cascading failure, blackouts, etc.) depending upon its nature, intensity, and location. This study can also facilitate predicting stressed grid conditions and further unwanted stresses due to perturbation in the systems. Although this research is important in terms of the diversities of events and perspective of analysis, this dissertation considers the case of abrupt changes in real-power load demand or generation as the perturbation.

1.3 An Introduction to Graph Signal Processing

Graph Signal Processing (GSP) [4, 5] is a relatively new field of signal processing that extends the theory and tools used in classical signal processing to the irregular graph domain. The vertices of a graph are considered the independent variable associated with the graph signal, and thereby graph signals are defined in the non-Euclidean graph vertex domain. A graph signal by being associated with a graph structure, inherently inherits the connectivity and topological information of the structures.

Many physical structures that consist of interconnected components can be modeled as graphs. Biological networks, transportation networks, water distribution networks, sensor networks, and wireless networks are some examples of such structures [4, 18, 19, 20, 21]. In recent years GSP is being popular for the data-driven analysis of networked structures to capture the connectivity and topological information to assist the meter-captured data for more effective analysis. Modeling network data as graph signals also facilitates applying training-based neural network models to the data.

The electrical power grid can also be modeled as a graph [22, 23] by considering the buses of the electric grid as the vertices and the transmission lines connecting the buses as the edges of the graph. The weights of the edges are determined in various ways depending on the nature of the analyses and application based on the geographical and electrical distances between the buses. The attributes associated with the buses (either measured by sensors or estimated by state estimation technique) can be considered as graph signals. The application of GSP in electrical networks enables imparting of information related to the topology, interconnection, and interaction among the grid components into many data-driven modeling and analyses of grid events and dynamics. In this dissertation, several applications of GSP techniques have been discussed related to grid security and reliability.

1.4 Overview of Energy Data Analytics

Data Analytics refers to a wide range of theories, tools, and techniques for processing, analyzing, and interpreting data collected from various sources. In the smart grid, with the extensive deployment of sensors and high-resolution measurement devices (e.g., Phasor measurement units-PMU and advanced metering infrastructures-AMI) a big amount of data associated with smart grids are available nowadays. Therefore, data-driven analyses of smart grid issues are being more popular among researchers than the previous rule-based decision-making [3].

In this dissertation, in the context of an electric energy system, the main data analytic method is the analysis of correlation among the states of the system. In most of the cases, the bus voltage angles are considered the states of the system and they are modeled as time-varying states by modeling them as multi-variate time series. The instantaneous state correlation matrix provides the correlation among the states in real-time. The conducted simulation suggests that certain stresses and events in the grid have distinguishable signatures in the correlation matrices visualized as images that can be exploited in certain applications related to smart grid security.

1.5 Key Contributions of this Dissertation

In this section, the key contribution of this dissertation has been summarized. This dissertation studies a few problems related to situational awareness in smart grids with the goal of enhancing the security and reliability of these systems using graph signal processing and energy data analytics techniques. The flowchart presented in Figure 1.1 summarizes the work presented in this dissertation. In the following subsections, the components of this flowchart have been discussed.

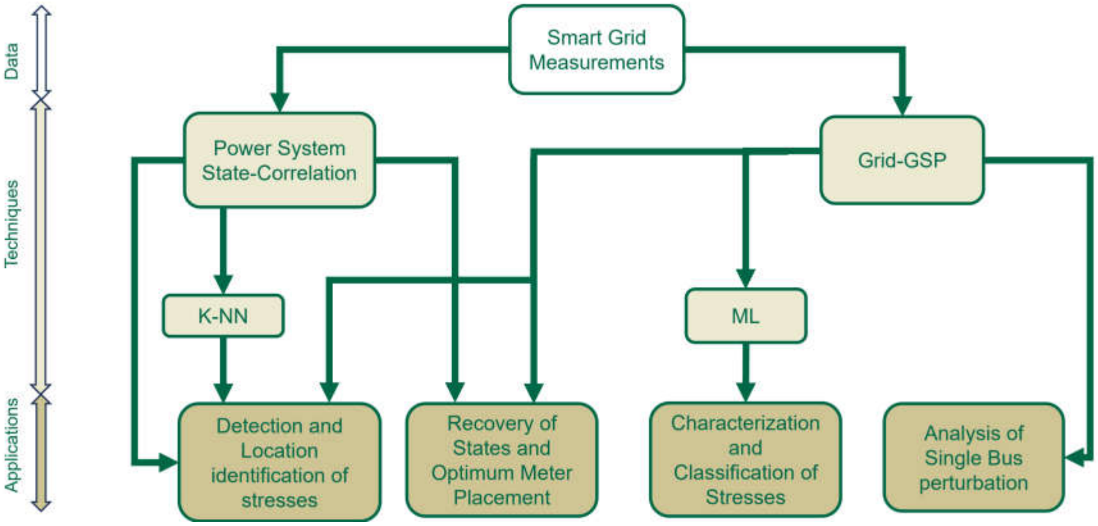

Data
Techniques
Applications
Smart Grid Measurements
Power System State-Correlation
Grid-GSP
K-NN
ML
Detection and Location identification of stresses
Recovery of States and Optimum Meter Placement
Characterization and Classification of Stresses
Analysis of Single Bus perturbation

Figure 1.1: Dissertation flow chart.

1.5.1 Data Sources

In the research work presented in this dissertation, all the data are electrical attributes of the power system (e.g. voltage magnitude and angles, current magnitude and angles, real and reactive power, etc.). All these data are generated using quasi-static simulation using power flow solutions in MATPOWER [24]. In the experiments involving time-series data, the time-varying electrical attributes are generated by superimposing the time-varying load pattern collected from NYISO [25] to the MATPOWER default load pattern. The time resolution of the time-series data varies throughout this work depending on the application and computing resources and will be mentioned in this dissertation in the context of different applications.

1.5.2 An Overview of Technical Approaches

In order to analyze the power grid data and leverage the data in applications related to the situational awareness of smart grids, data analytic and signal processing approaches including GSP are applied. In the initial stage of this research work, the correlation among the states of the grid (i.e., bus voltage magnitude and angles) is utilized for situational awareness applications. Although the state correlation-based study of power system data offers valuable insights into the interactions among grid components under normal and stressed conditions and therefore provides good performance in situational awareness applications. Consequently, we recognized that there is potential for further improvement in terms of accuracy, robustness, and applicability by explicitly imparting information about the connectivity and interaction among grid components in the analysis. By representing the electric power grid as a graph, GSP techniques have been leveraged to address the objectives related to grid situational awareness.

1.5.3 Contributions Toward Enhancing Situational Awareness in Power Grids

1.5.3.1 Detection and Location Identification of Cyber and Physical Stresses

Both the state correlation-based and GSP-based approaches have been studied for the detection of location identification of different cyber and physical stresses. The cyber attacks include DoS attacks, data replay attacks, and ramp attacks and are defined and modeled on the time-series data. The physical attacks include abrupt changes in load demand at a particular location (i.e., bus) in the grid and tripping of a transmission line.

Through the observations on the simulated stress scenarios, it has been discovered that certain cyber and physical stresses exhibit distinct signatures in the instantaneous correlation matrix associated with the time-varying states (bus voltage angle) modeled as multivariate time series. The bus voltage angle can be represented as images. Initially, simple image processing techniques have been applied for detecting and locating stresses. However, better performance has been achieved by extracting features from the instantaneous correlation images and utilizing them within a k-nearest neighbor (kNN) framework. In addition to the automated techniques for detecting and locating stresses, the real-time representation of instantaneous correlation matrix images can serve as an efficient visualization tool for grid operators.

To address the detection and localization of cyber and physical stresses using GSP, two novel techniques have been proposed based on GSP: the Vertex-Frequency Energy Distribution (VFED) method and the Local Smoothness Second Time-Derivative (LSSTD) method. The findings revealed that the LSSTD method offers the highest accuracy for detection and localization, particularly for sophisticatedly designed cyber attacks with no abrupt changes in signal values at the attack onset. This method combines the advantages of existing approaches by capturing both the time correlation in state values and the interrelation among the states through the graph's structural interconnection.

1.5.3.2 Characterization and Classification of Cyber and Physical Stresses

As soon as the stress is detected and located in the smart grid, the next task associated with the situational awareness of the smart grid is to analyze the type and the characteristics of the stress. The measurement data at the moment of detection (and immediate past data) have been proposed to utilize for the characterization and classification of stresses using GSP and machine learning techniques. The proposed classification scheme consists of a two-stage classification of stresses: the first stage classifies between cyber and physical stresses while the second stage involves classification among cyber (DoS, Replay, FDIA, Ramp, and Delay) stresses and among physical (abrupt load change and line failure) stresses. In addition, a classification model has been developed for classifying two types of cyber attacks in case of multiple attacks: clustered cyber attacks and random multiple cyber attacks, which is important to understand the attackers' intentions and strategies.

For all these classifications GSP techniques (e.g., Graph Fourier Transform, local and global smoothness of graph signals) have been applied to extract features from the bus voltage angle graph signal at the moment of detection of stresses or its temporal vicinity. Different sets of features are observed to be suitable for classification at different stages. The extracted features are used as input in different machine-learning models for classification. The presented studies show that the proposed method involving extracting GSP-based features and feeding them to machine learning-based methods, namely *Graph Signal Learning (GSL)* outperforms machine learning classification using raw voltage angle data.

Moreover, using the GSP-based feature, a neural network-based technique has been developed for detecting attack centers in case of clustered multiple cyber attacks. A simple technique for subsequent estimation of attack radius has also been proposed.

1.5.3.3 Recovery of the Unobservable States and Optimum Placement of Measurement Devices

The problem of recovering missing states in the power system has been addressed by formulating it within the framework of graph signal sampling and reconstruction. Firstly, it has been shown that in case of data unavailability due to cyber stresses, the missing data can be recovered using the graph signal reconstruction technique under band-limited graph signal assumption. Later, a reconstruction technique has been proposed that integrates the statistics of local smoothness and global smoothness of graph signals into an optimization framework for effectively recovering missing states. The significant contribution of this work is that the proposed technique is bandwidth-agnostic which makes it applicable to a wider range of scenarios, even when the graph signal is not band-limited. By considering both the global and local dynamics of the system, this method exhibits notable accuracy in estimating the missing signal values.

Since graph signal sampling can be linked to the availability of the attribute values at some of the buses and unavailability at the other buses in the power system. In the context of the optimum measurement device (Phasor Measurement Unit-PMU) placement problem, the buses where PMUs are installed can be considered as the sampling vertices, while the non-PMU buses are represented by the non-sampling vertices. To address the optimum PMU placement problem effectively, we approached it as a sampling set selection problem considering the power system scenario. The objective was to minimize the reconstruction error and maximize the observability of the system by strategically selecting the buses where PMUs should be placed.

1.5.3.4 Characterization of Single Bus Perturbation in Smart Grids

The last application associated with the situational awareness of smart grids discussed in the dissertation is the analysis of the impact of a single perturbation on power systems. A GSP framework has been developed in this regard. For this analysis, the only perturbation considered is an abrupt change in either the real-power load demand or the real-power generation of a specific bus as the single bus perturbation. The main focus of this work is to investigate how the effects of perturbation propagate through the system, depending on its location and strength. For quantifying the spreadability of a particular perturbation through the grid, a spreadability metric has been proposed, its properties have been derived by an analytical approach under DC power flow assumption, and the properties have been verified by simulation using AC power flow. Simulations also suggest that the local and global smoothness properties of the *difference bus voltage angle graph signal* before and after the perturbation are correlated statistically with the proposed measure of spreadability and are suitable for the estimation of relative spreadabilities depending on the perturbation location. Moreover, it has been shown that the global smoothness of the bus voltage angle is a quadratic function of the perturbation strength with a maximum value at the critical perturbation strength after which the global smoothness begins to decrease and further increment of perturbation strength leads to non-convergence of power flow. The critical perturbation strength varies from bus to bus and can be considered as the indicator of a stressed grid that is vulnerable to collapse.

This work presents an important study from the GSP perspective about how the effects of a single bus load or generation perturbation spread through the power grid depending upon its location and strength. This study should be important for predicting grid stress and instability due to perturbations arising from many modern-day grid scenarios, e.g., the deployment of electric vehicles and distributed energy resources in the grid. The research is also relevant for analyzing cascading failures in the power grid which may get initiated from single perturbations.

1.6 Structure of this Dissertation

For the convenience of the reader at the beginning of each chapter of this dissertation, an introduction has been added to give the reader a overview of the contents. A *Related Work* section in each chapter presents a discussion on the existing literature related to the content of the chapter. From chapters 3 to 7, each chapter is dedicated to one of the applications discussed in the previous sections. The problem of stress detection and location identification has been divided between Chapters 3 and 4. Chapter 3 discusses addressing this problem using state correlation-based techniques while Chapter 4 suggests GSP-based solutions. Since some of the applications are proposed to be solved by multiple methodologies, each of those chapters contains a general problem formulation section with multiple methodology sections.

Chapter 2 provides an introduction to GSP in the electrical grid context. The representation of the power grid as a graph and bus attributes of the grid as graph signals are demonstrated and visualized at the beginning of the chapter. The concept of the graph-frequency domain, graph signal smoothness, and their relation with the vertex-domain graph signal is presented in this chapter. The later portions of the chapter contain the representation of the power system graph signal (particularly, the bus voltage angle graph signal) in the vertex domain, graph-frequency domain, joint vertex-graph-frequency domain associated with grid normal conditions, cyber stresses, and physical stresses. The concepts of *graph signal sampling* and *graph signal learning (GSL)* are also introduced in the chapter.

Chapters 3 and 4 are dedicated to the application of detecting and locating cyber and physical stresses in the smart grid. This chapter provides models for different cyber and physical stresses in the grid and shows their effect on the bus voltage angle data. Chapter 3 illustrated the methodologies for detection and location identification using both the instantaneous correlation-based technique and the GSP-based techniques. The distinguishable effects of different stresses on the instantaneous correlation matrix image have been shown as a motivation for developing correlation-based detection and localization methods. Similar motivational illustrations on the graph signal parameters have also been presented in Chapter 4. This chapter contains a detailed description of the techniques of both types, the results of the simulation, analyses of the complexity of the methods, and a comparison with benchmark methods. All the simulations in both chapters have been performed on the IEEE 118 bus system using quasi-static simulation in MATPOWER, and load patterns collected from the NYISO data to create synthetic time series data.

Chapter 5 illustrates the problem of characterization and classification of cyber and physical stresses after detecting and locating them for the data at the moment of detection and their temporal vicinity by using GSL, a combination of GSP-based feature extraction and machine learning models. The classification model involves a two-stage classification scheme with binary classification between cyber and physical stresses at the first stage followed by classification among the cyber stresses and among the physical stresses in the next stage. An additional classification model has been proposed for classifying clustered and random multiple cyber-attack. The characterization tasks include the estimation of the attack center and attack radius. This chapter discusses the feature selections for different classification models and a feature reduction technique for the graph Fourier transform-based features.

Chapter 6 is about the state recovery problem in the smart grid and the associated optimum sensor placement problem. This chapter shows the formulation for the state recovery problem in the case of both a single-time instant and time series. This chapter established the relationship between graph signal sampling-reconstruction and state recovery problem and shows two GSP-based techniques for recovery of states i. e., recovery of bus voltage angle measurements. The first technique is directly using the graph signal reconstruction method to voltage angle data considering the buses with available measurements as the sampling vertices. A PMU placement strategy has been proposed using this technique by formulating a sampling-set selection problem. The objective is to maximize the observability with a minimum number of PMUs considering electrical grid realities. Since this technique is based on band-limited assumptions for the graph signal, a bandwidth-agnostic recovery technique has been proposed that uses the global and local smoothness of the associated graph signal. This chapter concludes with a state-correlation-based technique for recovering time-varying states for a duration of unobservability.

Chapter 7 involves the characterization of single bus perturbation in smart grids modeled as a sharp increase of real-power load demand and real-power generation at a single bus. This chapter provides a mathematical model of the perturbation under the GSP framework, defines the graph signals relevant to the analysis, and analyzes their properties under the single bus perturbation context. A GSP-based metric for quantifying the spreadability of the effect of perturbation depending on the perturbation location has been proposed and justified using analytical calculations under DC power flow and numerical approaches using more realistic AC power flow. The global and local smoothness properties of the graph signals under perturbation have been derived analytically and they are shown to be estimators of the spreadability of the perturbation.

Chapter 8 concludes the dissertation by summarizing the result and the contribution of the research and discusses a few directions in which the research can be extended corresponding to each of the applications.

Chapter 2: Fundamentals of Grid-GSP

[1]This chapter provides a brief overview of the preliminary concepts of GSP by comparing them with classical signal processing, introduces GSP in the context of the electrical power grid, and motivates using GSP-based techniques for power system security and reliability-related problems. GSP tools for the analyses of graph signals in the vertex domain, graph-frequency domain, and joint vertex-graph-frequency domain are presented with mathematical details and examples in the power system context.

2.1 GSP Literature Review

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 [4, 5]. 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 [4, 5].

Moreover, analogous to the joint time-frequency representation of temporal signals, the concept of vertex-frequency analysis of graph signals has been developed and interpreted in [32, 33]. However, unlike the Fourier basis functions, the bases for representing graph signals in the frequency domain, i.e., eigenvectors of the graph Laplacian, are localized in nature. Windowed graph Fourier transform (WGFT) [34] and graph wavelet transform (GWT) [35]

[1] Portions of this chapter were published in IEEE Transaction on Smart Grid [26], IEEE Xplore [27, 28, 29, 30], and Arxiv [31]. Copyright permissions from the publishers are included in Appendix B.

have also been introduced. Inspired by the concept of time-frequency energy distributions in classical signal processing (e.g., Rihaczek energy distribution [33]), the work by Stanković et. al. [33] introduces vertex-frequency energy distributions in the context of GSP. The vertex-frequency energy distributions can be useful for studying the frequency characteristics of the graph signal in a vertex-localized manner. A few works have also been published on time-vertex signal processing [36, 37], which treats a time series associated with each of the vertices of a graph.

Recently, GSP techniques have been used in various application domains including sensor arrays and networks [19], transportation systems [38, 39], electroencephalogram (EEG) signal analysis [40, 41], image processing [42] and imaging [43] and smart grids [44, 22]. Specifically, researchers have shown that GSP can be a prospective field for detecting anomalies in different types of networks and their associated signals [45].

In very recent times, GSP is being utilized in smart grid research, especially in the security and reliability of smart grids. For instance, Kroizer *et al.* in [46] 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 [22] 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. Saha *et. al.* [47] developed a graph signal sampling-based state estimation framework for radial distribution feeders considering a three-phase unbalanced distribution system and proposed a related optimal advanced metering infrastructure (AMI) placement algorithm. Mendes *et. al.* [48] utilized GSP for estimating load current variability in distribution feeders in the presence of distributed generation.

Another important role of GSP involves modeling the structured data as graph signals to make them suitable for applications using graph neural networks (GNN) [49, 50] such as graph convolutional networks (GCN) [51, 52]. Similar to any other fields involving network structured data, these training-based techniques are being used widely in many power system applications. State estimation [53, 54] , stress detection [55, 56, 57], power flow solution [58, 59], and cascading failure analysis [60] are some of such applications.

2.2 Review of GSP and Energy Graph Signals

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 $x : \mathcal{V} \rightarrow \mathbb{R}$. The graph signal can be denoted by $x(n)$ instead of $x(v_n)$ for simplicity. Therefore, one of the important steps in defining graph signals is to specify the underlying connectivities among the components, i.e. the graph domain.

2.2.1 Defining Graph Domain for Power Grids

In this dissertation, the 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 [61], 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 some of the applications, 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. In a few other applications, The weight matrix $\mathbf{W}$ is defined in such a way that the Laplacian matrix $\mathbf{L} = \mathbf{D} - \mathbf{W}$ of the graph represents the imaginary part of the admittance matrix of the network. Later in this dissertation, the definition of the Laplacian matrices depending on the application would be mentioned.

In some of the smart grid applications introduced in the dissertation, the power grid is needed to be 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, $\mathcal{G}(t)$.

2.2.2 Representation of Power System Measurements as Graph Signals: Vertex Domain Representation

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. Figure 2.1 illustrates an example of a graph signal based on the voltage angles of all the buses for the IEEE 118 bus system [62].

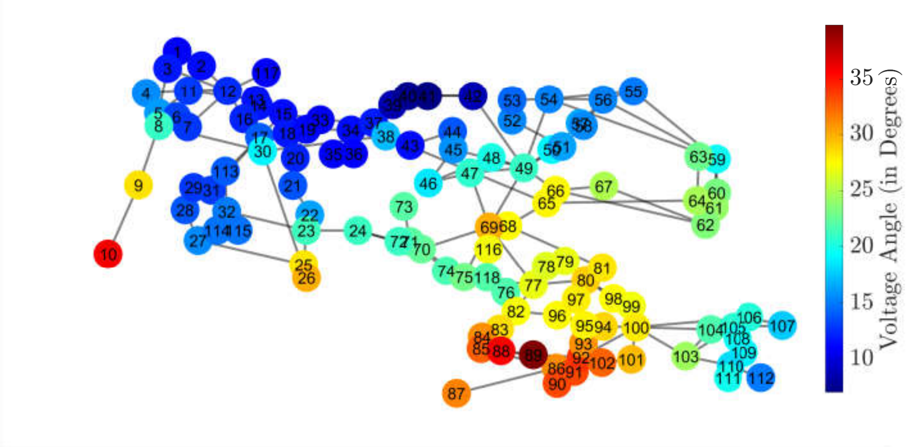


Figure 2.1: Voltage angle measurements at a particular time instance as a graph signal on the IEEE 118 bus system.

It is assumed that the signal 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 on 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. 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.

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

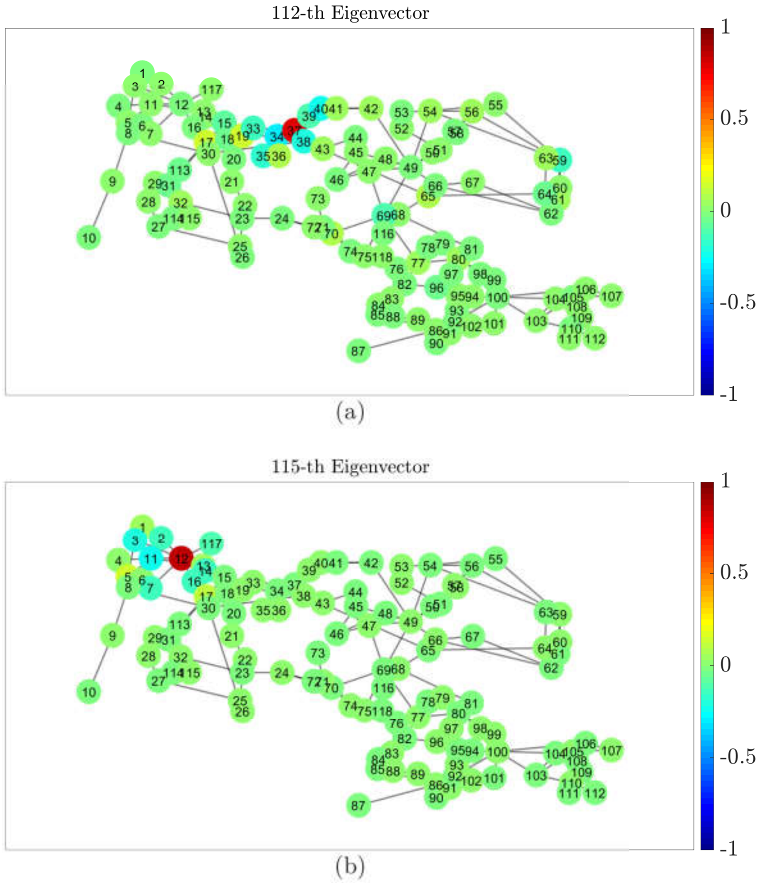
Analogous to the concept of Fourier transform and frequency domain representation of the signal in classical signal processing, the graph Fourier transform (GFT) of a graph signal $x(n)$ is defined as:

$$\hat{X}(\lambda_k) = \sum_{n=1}^{N} x(n)u_k(n), \quad \text{(Analysis equation)} \tag{2.1}$$

and the inverse graph Fourier transform (IGFT) is:

$$x(n) = \sum_{k=1}^{N} \hat{X}(\lambda_k)u_k(n), \quad \text{(Synthesis equation)} \tag{2.2}$$

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. For example, Figure 2.2 illustrates two eigenvectors of the graph structure corresponding to the IEEE 118 bus system that are localized around two different locations in the graph. The edge weights in this case are considered as the reciprocal of the geographic distance.



(a)

(b)

Figure 2.2: Two of the eigenvectors for IEEE 118 bus systems graph. The two eigenvectors are localized around two different vertices.

2.2.4 Global Smoothness of Graph Signals

The smoothness measure of a signal quantifies how rapidly the values of the signal change. In a graph signal, the smoothness characterizes the variation of the signal over graph neighborhoods, i.e., from each vertex to its neighboring vertices. The global smoothness signifies the aggregated variations in the signal while local smoothness signifies variation in the vicinity of each vertex.

The global smoothness of a graph signal $x(n)$ is defined as:

$$s_{Global} = \frac{\mathbf{x}^T \mathbf{L} \mathbf{x}}{\mathbf{x}^T \mathbf{x}}, \tag{2.3}$$

where $\mathbf{x}$ is the vector representation of the graph signal, $x(n)$. The faster the graph signal changes from vertex to vertex, the larger the value of s_{Global}.

2.2.5 Local Smoothness of Graph Signals

The smoothness measure of a signal quantifies how rapidly the values of the signal change. While the global smoothness [33] 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

$$s(n) = \frac{l_{\mathbf{x}}(n)}{x(n)}, \quad \text{for} \quad x(n) \neq 0, \tag{2.4}$$

$s(n)$ 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. [63] shows that the concept of local smoothness in the graph signal is analogous to the concept of instantaneous frequency in classical signal processing.

2.2.6 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.* [33] propose localized vertex spectrum (LVS) of graph signal $x(n)$ as:

$$LVS_x(n, \lambda_k) = \sum_{m=1}^{N} x(m)h(n-m)u_k(m), \tag{2.5}$$

where $h(n)$ is the window function. This approach has the 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 [33], which does not require any window. The VFED, $E(n, k)$ is calculated from the graph signal using the equation:

$$E(n, k) = \sum_{m=1}^{N} x(n)x(m)u_k(m)u_k(n). \tag{2.6}$$

2.2.7 Time-Varying Graph Signals

In previous discussions, the graph signals at a single time instant have been considered. 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, it is assumed 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. Here, 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.

2.2.8 Amount of High Graph-Frequency Components

In reference to [31], the amount of high graph-frequency components in the graph signal at time t, $\gamma(t)$ as:

$$\gamma(t) = \sum_{k} |X(\lambda_k, t)H(\lambda_k)|, \tag{2.7}$$

where $H(\lambda)$ is a high-pass graph filter with frequency response: $H(\lambda) = 0, \quad \text{if } \lambda \leq \lambda_c$ and $H(\lambda) = 1, \quad \text{if } \lambda > \lambda_c$ 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, the instantaneous local smoothness, $s(n, t)$ has been used to detect stresses.

2.3 Reflection of Smart Grid Stresses on Their Graph Signals

2.3.1 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:

$$x(n_A, t) = c(t), \quad \textit{for} \quad t_{start} \leq t \leq t_{end}, \quad \textit{and} \quad n_A \in \mathcal{V}_{\mathcal{A}}. \tag{2.8}$$

The corrupted signal $c(t)$ can be defined to model and capture the effects of various types of attacks as will be discussed next. Figure 2.3, illustrates different types of cyber attacks on the time-series, $x(102, t)$, which is associated with the time-varying values of the graph signal $x(n, t)$ at vertex/bus 102 in the IEEE 118 bus system.

2.3.1.1 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

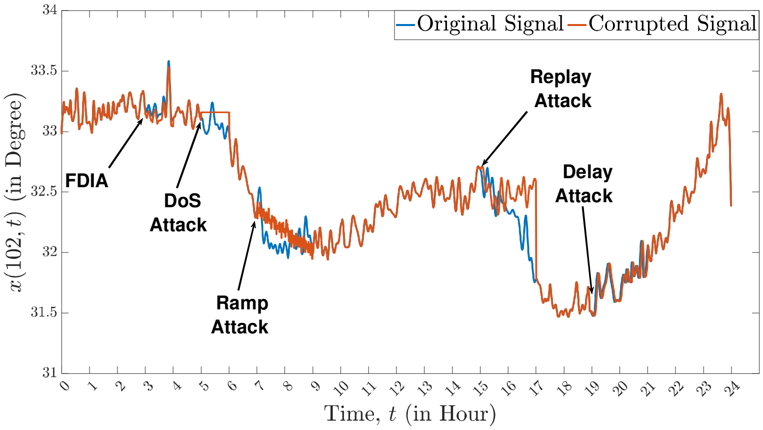


Figure 2.3: Cyber attacks on time-series.

through overloading network resources. In cyber security literature, DoS attacks are often modeled as the absence of measurement signal at the attack location [64]. 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:

$$c(t) = x(n_A, t_{start}) + q(t) \tag{2.9}$$

where $q(t)$ is the additive white Gaussian noise with zero mean and variance $\sigma^2_{n_A}$. In Figure 2.3, the example DoS attack starts at time 5 and ends at time 6.

2.3.1.2 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 work, 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 (2.8), $c(t)$ can be defined as:

$$c(t) = x(n_A, t) + (-1)^b x', \tag{2.10}$$

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 work 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 Figure 2.3, the example FDIA starts at time 3 and ends at time 4.

2.3.1.3 Ramp Attack

A ramp attack involves inserting falsified measurements 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 attacks can be challenging. Ramp attack can be modeled by:

$$c(t) = x(n_A, t_{start}) + m \times (t - t_{start}) + q(t), \tag{2.11}$$

where m is the slope of the change and $q(t)$ is the additive white Gaussian noise. In Figure 2.3, the example ramp attack with slope -0.8 starts at time 7 and ends at time 9.

2.3.1.4 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 attacks can be modeled by:

$$c(t) \in \{x(n_R, t_p)\}, \quad t_p < t_{start}, \quad n_R \in \mathcal{V}_{\mathcal{R}} \tag{2.12}$$

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 Figure 2.3, the example replay attack starts at time 15 and ends at time 17.

2.3.1.5 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:

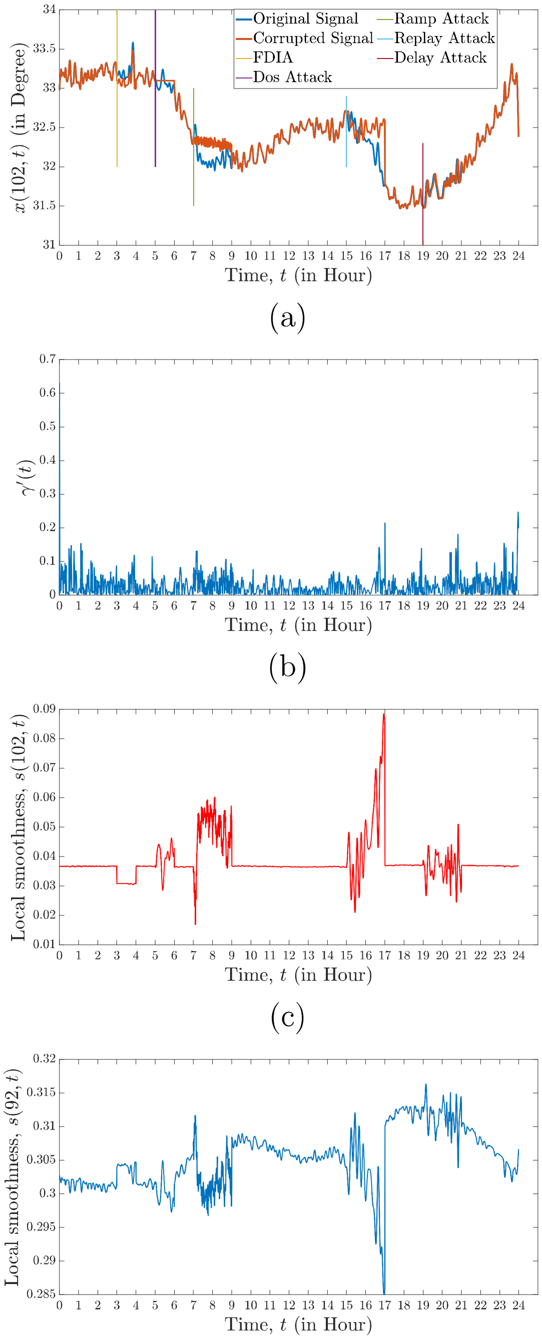
$$c(t) = x(n_A, t - t_d) \tag{2.13}$$

where t_d is the amount of delay. For small t_d's, the detection of this type of attack is very challenging. In Figure 2.3, the example delay attack starts at time 19 and ends at time 21.

For a successful cyber attack from the attacker's perspective, 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 work 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.

2.3.2 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 the local smoothness of the graph signals associated with the bus voltage angle measurements. Figure 2.4 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 Figure 2.4(a), the cyber-attacks launched at bus number 102 at different moments of the day are shown on $x(102, t)$. Figure 2.4(b), illustrates the changes in the amount of high graph-frequency components γ_t' associated with $x(n, t)$ over time. From this figure, we observe that these critically designed cyber-attacks are not well reflected on γ_t' values, although it is shown that these values can be used to detect simple cyber-attacks [44, 31]. Figure 2.4(c) shows the time-varying local smoothness corresponding to the attacked bus (vertex), $s(102, t)$. It is observed 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 $s(102, t)$. Figure 2.4(d) shows the time-varying local smoothness values at vertex 92, which corresponds to a neighboring bus of the attacked bus, 102. From



(a)

(b)

(c)

(d)

Figure 2.4: The effects of different types of cyber attacks on time-varying graph signal and its various spectral parameters. The following time series represent (a) time-varying graph signal values at vertex 102, $x(102, t)$, (b) changes in the amount of high-frequency components, $\gamma_t^{'}$, (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).

this figure, it can be noticed that although the values of $s(92, t)$ are affected by 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.

2.3.3 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 on a bus with a low degree, several GFT coefficients are affected. Figure 2.5 illustrates the scenarios for two buses having degrees 9 and 5.

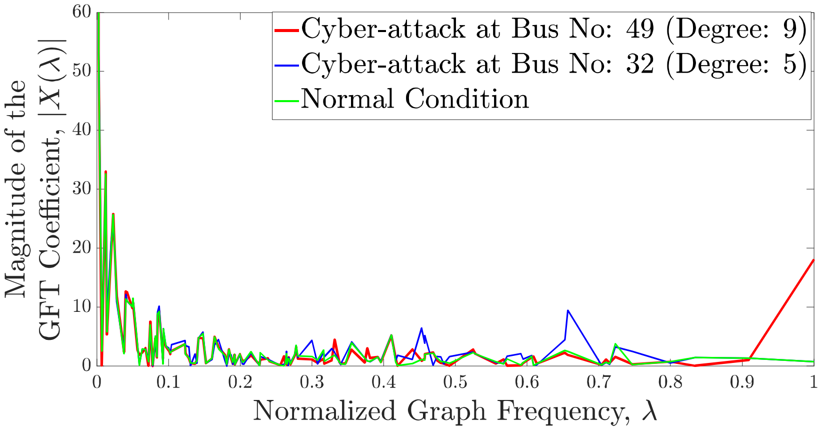


Figure 2.5: The effects of degree of the attacked bus on GFT.

2.3.4 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.

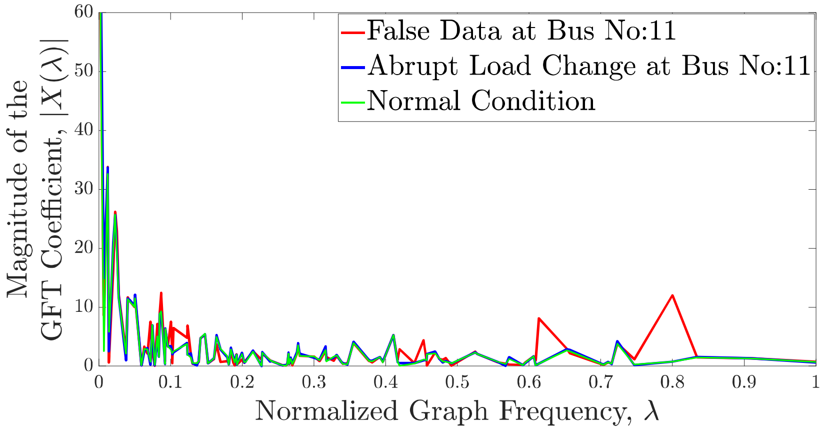


Figure 2.6: The GFT values associated with the graph signals during a normal condition, under FDIA at bus 11, and load change at bus 11.

Figure 2.6 compares the GFT of the graph signals associated 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 load at bus number 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 number 11. The bus-to-bus variations in the voltage angle measurements around bus number 11 is smooth, which corresponds to low-frequency components of GFT. In contrast, the injection of false data at bus number 11 introduces changes in the magnitude of some of the high-frequency components. False data at bus number 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 number 11 with respect to its neighboring values. This sharp variation corresponds to the high-frequency component of GFT.

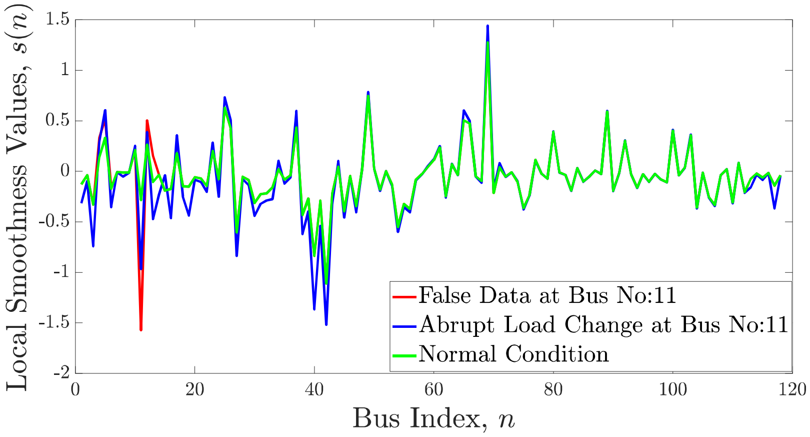


Figure 2.7: The local smoothness values of the nodes during a normal condition, cyber attack at bus 11, and load change at bus 11.

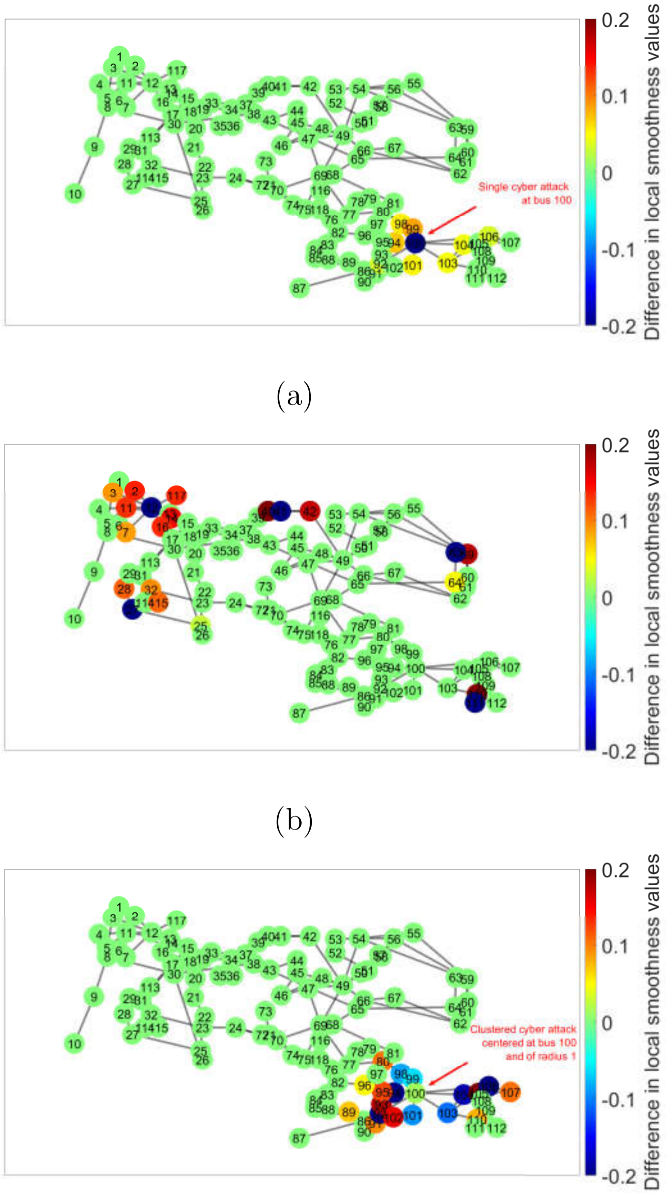
Figure 2.7 illustrates the same pair of phenomena in terms of local smoothness values. It is observed that false data injection at bus number 11 affects the local smoothness values of only a few vertices (vertices at a one-hop distance) around v_{11}, whereas the abrupt change in the load demand changes local smoothness values around a wider region, centering vertex 11.

2.4 Effects of Cyber Attacks Patterns on Local Smoothness of Graph Signals

The local smoothness [63] of the graph signal $x(n,t)$ associated with the bus voltage angles is described by:

$$s(n,t) = \frac{l_x(n,t)}{x(n,t)}, \quad x(n,t) \neq 0, \tag{2.14}$$

where $l_x(n,t)$ is the $n-$th element of the vector $L\underline{x}$ and $\underline{x}$ is the vector form of the graph signal $x(n,t)$. Here, the effects of cyber attacks on the local smoothness values are inspected analytically to evaluate the effectiveness of the detection and locating method in case of



(a)

(b)

(c)

Figure 2.8: Changes in the local smoothness values due to different types of FDIA assuming no load changes in the system. Attacks include: (a) single attack at bus 100 affects bus 100 and its 1−hop neighbors i. e., $\{100\} \cup \mathscr{N}_1(100)$, (b) multiple attacks at bus 12, 27, 41, 63, 111 affect those buses and their 1−hop neighbors i.e. $\{12, 27, 41, 63, 111\} \cup \mathscr{N}_1(12) \cup \mathscr{N}_1(27) \cup \mathscr{N}_1(41) \cup \mathscr{N}_1(63) \cup \mathscr{N}_1(111)$ (c) clustered attack centered at bus 100 and radius 1 affects $\{100\} \cup \mathscr{N}_1(100) \cup \mathscr{N}_2(100)$.

multiple, clustered, and coordinated cyber attacks. In this case, by utilizing the sparse nature of the graph Laplacian matrix, $\mathbf{L}$, $l_x(n,t)$ can be expressed alternatively as:

$$l_x(n,t) = \sum_{i \in \{n\} \cup \mathcal{N}_1(n)} l_{ni} x(i,t), \tag{2.15}$$

where $\mathcal{N}_k(n)$ is the set of all vertices in the $k-$hop neighborhood of n. Next, the effects of cyber attacks on the local smoothness $s(n)$ will be illustrated.

- Single Cyber Attack Case with Fixed Load: Let us consider a single cyber attack at bus $n_A \in \mathcal{V}_\mathcal{A}$. According to equation (2.15), this single attack will affect $l_x(n, t_d)$ for $n \in \{n_A\} \cup \mathcal{N}_1(n_A)$. According to equation (2.14), the local smoothness values for these vertices are affected because of the single cyber attack at the vertex n_A. For instance, Fig.2.8(a) illustrates the difference between the local smoothness values of each vertex before and after a single cyber attack at bus 100.

- Multiple Random Cyber Attack Case with Fixed Load: Let us consider p cyber attacks at buses $n_{A_1}, n_{A_2}, \dots n_{A_p} \in \mathcal{V}$. According to equation (2.15), this multiple attack will affect $l_x(n, t_d)$ and thereby the local smoothness $s(n, t_d)$ for:
$n \in \{n_{A_1}, n_{A_2}, \dots n_{A_p}\} \cup \mathcal{N}_1(n_{A_1}) \cup \mathcal{N}_1(n_{A_2}) \dots \mathcal{N}_1(n_{Ap})$. For instance, Figure 2.8(b) illustrates the effect of FDIA on buses 12, 27, 41, 63, and 111.

- Clustered Cyber Attack Case with Fixed Load: In a clustered cyber attack case, it is assumed that the attacker attacks a central node and its $K-$hop neighbors. The parameter K is called the *radius* of the attack. In clustered cyber attacks, the attacker can inject false data at any vertex within the radius K. For example, in a clustered cyber attack with attack center $n_C \in \mathcal{V}$ and radius 1, the attacker changes the graph signal $x(n)$ for $n \in \{n_C\} \cup \mathcal{N}_1(n_{A_C})$. According to equation (2.15), due to the changes of the signal values in the attack center n_C, the value of $l_x(n)$ would change for $n \in \{n_C\} \cup \mathcal{N}_1(n_C)$ and due to the changes of the value at each of the vertices $n'_C \in \mathcal{N}_1(n_C)$, the value of $l_x(n, t_d)$ would change for $n \in \mathscr{N}_1(n_C^{'})$, $\forall n_C' \in \mathscr{N}_1(n_C')$. Therefore, a clustered attack centered at n_C and radius 1 would affect the values of $l_x(n, t_d)$ for the vertices $n \in \{n_C\} \cup \mathscr{N}_1(n_C) \cup \mathscr{N}_2(n_C)$. According to equation (2.14), the local smoothness $s(n, t_d)$ changes for these vertices. A clustered attack centering at bus 100 and radius 1 has been considered as an example at Figure 2.8(c). In general, a clustered cyber attack, with attack center n_C and radius K, can affect the local smoothness values of the vertices: $\{n_C\} \cup \{\bigcup_{j=1}^{K+1} \mathscr{N}_j(n_C)\}$.

The above discussion provides insight for detecting, locating, and characterizing cyber attacks in power grids based on the local smoothness of the associated graph signals. However, the assumption of no-load change does not hold in real-life scenarios. Therefore, due to the perpetual changes of load demands, the graph signal, $x(n, t)$, and thereby the local smoothness $s(n, t)$ change continuously over time. It is a challenge to distinguish the changes in local smoothness due to the cyber attack from the regular changes in local smoothness due to the load changes. To overcome this problem, estimating the probability distribution of the second time-derivative of the local smoothness values for each of the buses under the load changes from the past data has been proposed [26].

2.5 Graph Signal Sampling Overview

2.5.1 The Concept of Graph Spectral Bandwidth

In this work, the spectral domain of a graph is defined by the graph Fourier transform. The graph Fourier transform (GFT) and the inverse graph Fourier transform (IGFT) of a graph signal $x(n)$ are defined by the analysis equation (equation 2.1) and the synthesis equation (equation 2.2). Analogous to the concept of bandwidth for the signals defined in the Euclidean domain, the bandwidth, λ_B of a graph signal can be defined as If $X(\lambda_k) = 0$, for $k > B$, then λ_B is called the *bandwidth* of the graph signal $x(n)$. In this case, the graph signal is said to be band-limited to the graph frequency, λ_B. The set $\{\lambda_k : \lambda_k \leq \lambda_B\}$ contains B number of significant graph-frequency components in the graph signal.

2.5.2 Sampling and Reconstruction of Band-limited Graph Signals

Sampling a graph signal can be defined as considering graph signal values corresponding to a subset $\mathcal{S}$ of the set of all vertices $\mathcal{V}$. According to the Nyquist criterion in classical signal processing while down-sampling a signal by a factor d, the signal needs to be band-limited within $\frac{\pi}{d}$ radian/sample for being able to be perfectly reconstructed from its down-sampled version [65]. If the signal is not band-limited to $\frac{\pi}{d}$ radian/sample, overlapping would occur in the spectral domain during the down-sampling process causing aliasing. To avoid aliasing signals can be made to be band-limited by discarding insignificant high-frequency contents over $\frac{\pi}{d}$ radian/sample. If the frequency component beyond $\frac{\pi}{d}$ radian/sample is not insignificant, the signal should not be down-sampled at a rate of d. Similarly, down-sampling of graph signal creates aliasing in the graph-spectral domain unless the signal is band-limited to a certain frequency. Narang and Ortega [66] showed that for $k-$*regular bipartite* graphs the phenomenon is the same as Nyquist criteria when every d vertices are sampled, However, for the arbitrary graphs, the scenario is not directly analogous to the $\frac{\pi}{d}$ limit. For the method implemented in [67], if the graph signal is band-limited to B graph-frequency components, then the number of sampling points N_s should not be less than B (i.e. $N_s \geq B$).

Let $x(n)$ be a graph signal approximately band-limited to λ_B, i.e. $X(\lambda_{k_u}) \lll X(\lambda_{k_l})$, for $k_u > B$ and $k_l \leq B$. Since the signal does not have significant frequency contents beyond λ_B, discarding those frequency components would not distort the signal notably; however, similarly to the case of sampling in classical signal processing, these insignificant frequency components cause aliasing during the sampling process, which makes reconstruction impossible. To avoid this situation and to be able to reconstruct the original signal from its samples, the high-frequency components of the original signal are discarded using an anti-aliasing graph filter. The frequency response of the proposed anti-aliasing graph filter is:

$$H(\lambda_k) = \begin{cases} 1, & \text{for } \lambda_k \leq \lambda_B \\ 0, & \text{otherwise.} \end{cases} \tag{2.16}$$

The band-limited graph signal $x_{BL}(n)$, which is obtained by filtering the original graph signal $x(n)$ can be described in the GFT domain by:

$$X_{BL}(\lambda_k) = H(\lambda_k)X(\lambda_k). \tag{2.17}$$

The set of vertices to be sampled, $\mathcal{S}$, is an indexed set with the $i-$th member of the set denoted as s_i. As such, the sampled graph signal can be expressed as:

$$x_s(n) = \begin{cases} x_{BL}(n), & \text{if } n \in \mathcal{S} \\ 0, & \text{otherwise.} \end{cases} \tag{2.18}$$

The selection of vertices to be sampled, $\mathcal{S}$, can be based on various criteria considering the topology and physics of the system. The reconstruction process estimates the original band-limited signal values from the sampled signal $x_s(n)$. The reconstructed signal can be defined as:

$$x_{re}(n) = \mathscr{R}(x_s(n)), \tag{2.19}$$

where $\mathscr{R}$ is the reconstruction operator that acts on the sampled signal. Note that the aforementioned descriptions of $x_s(n)$ and $x_{re}(n)$ provide the conceptual definition of the graph signal sampling and reconstruction process. Both of the operations have been implemented by following the approach suggested in [67] based on matrix multiplications as discussed next. The sampling process corresponds to the matrix multiplication:

$$\underline{\mathbf{s}} = \boldsymbol{\Psi}\underline{\mathbf{x}}_{BL}, \tag{2.20}$$

where $\underline{\mathbf{x}}_{BL}$, a $N \times 1$ vector, is the vector form of the graph signal $x_{BL}(n)$ and $\mathbf{\Psi}$ is a $N_s \times N$ sparse matrix. The entry at the $i-$th row and $j-$th column of $\mathbf{\Psi}$ is defined as: $\psi_{ij} = 1$ if, $j = s_i$, and $\psi_{ij} = 0$, otherwise. The $N_s \times 1$ vector $\underline{\mathbf{s}}$ contains the non-zero values of the sampled signal in the order of the indexed set, $\mathcal{S}$. The reconstruction process is implemented by:

$$\underline{\mathbf{r}} = \mathbf{U}_{\mathbf{N_s}}(\mathbf{\Psi}\mathbf{U}_{\mathbf{N_s}})^{-1}\underline{\mathbf{s}}, \tag{2.21}$$

where $\mathbf{U}_{\mathbf{N_s}}$ is a $N \times N_s$ matrix containing the first N_s eigenvectors, $\{\underline{\mathbf{u}}_k : k \leq N_s\}$ of the Laplacian matrix $\mathbf{L}$ in its N_s columns. For the application of graph signal sampling in this power grid:

$$x_{re}(n) = \begin{cases} x(n), & \text{if } n \in \mathcal{S} \\ r_n, & \text{otherwise,} \end{cases} \tag{2.22}$$

where r_n is the $n-$th element of the vector $\underline{\mathbf{r}}$. As an example, we have implemented the technique described here for power system graph signals. The voltage angle measurement of each bus for the IEEE 118 bus system [62] has been considered as the graph signal, $x(n)$. Simulations have been performed in MATPOWER 6.0 [24].

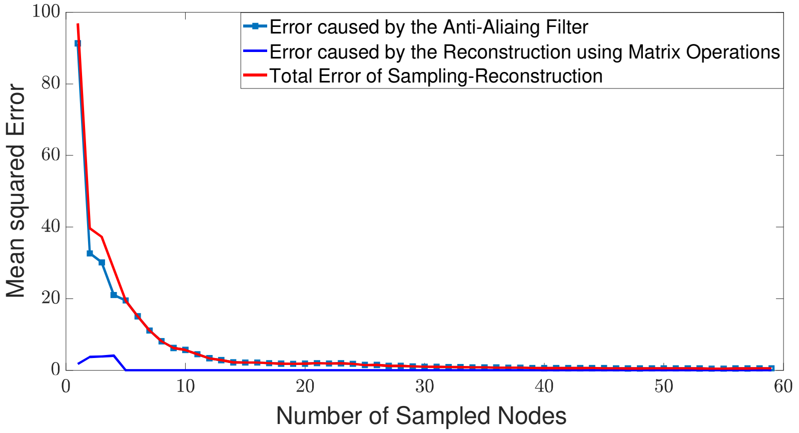


Figure 2.9: Decomposition of reconstruction error for graph-signal sampling as a function of the number of sampled nodes, N_s.

The anti-aliasing filter has been designed to obtain $x_{BL}(n)$ to be band-limited within $B = N_S$ graph-frequency components. In this sampling reconstruction process, the total error in the reconstructed signal consists of two errors: the error caused by the anti-aliasing filter for band-limiting the graph signal, and the error for reconstructing the non-sampled vertices in the matrix multiplication process. It is observed that, as N_s increases, the first type of error decreases since the anti-aliasing filter allows more high-frequency components. However, the second error depends mainly on selecting the sampling set, $\mathcal{S}$, and is relatively negligible compared to the other error. The comparison of the two types of error is shown in Figure 2.9.

2.6 Learning of Graph Signals

Under the perpetual changes in the grid scenarios including changes in load demands and generator output at different buses of the grid, the graph signal, $x(n, t)$, its graph-frequency domain representation, and the smoothness parameters calculated from $x(n, t)$ vary continuously over time. As a result, rule-based decision-making from the GSP-based signatures of various events and stresses becomes difficult, especially in the case of classification and characterization of anomalies and stresses. In spite, the GSP parameters associated with the events can be more effective for classifying than the raw data with learning-based models [30, 29]. Therefore, 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, the GSL framework has been proposed. GSL involves feature extraction using GSP techniques and feeding these features to machine learning models including neural networks. The GFT values, local and global smoothness values, and their temporal statistics can be considered GSP-based features. Chapter 5 provides a detailed analysis of classification using the learning of graph signals. Experiments show that GSL achieves better classification accuracy than learning raw data.

Chapter 3: Detection and Location Identification of Cyber and Physical Stresses in the Smart Grid: Part I: State Correlation Approach

[2]Due to the importance of system monitoring in smart grids as critical infrastructures, various types of cyber-attacks have targeted this function by compromising various components of the system and tampering with or obstructing the data from monitoring sensors. Such attacks can lead to errors in the estimated system state in the control system and potentially severe flaws in the control and operation of the system affecting its reliability and efficiency of the system. As such, identifying and locating such cyber-attack incidents is critical in enhancing the reliability and efficiency of smart grids. In addition to cyber-attacks, physical anomalies also threaten the reliability of smart grids and require real-time detection and locating by state monitoring systems.

In this work, the data streams from the PMUs, in the form of time series, will be utilized to help with the state monitoring function for detecting and locating various cyber and physical stresses in smart grids in real-time. Specifically, this work presents data-driven methods based on the correlation among the states of the components for detecting and locating stresses.

In the previous work [68], we observed that the correlations among the states of the components vary in time due to changes in the system, such as generation and load demand variations as well as cyber and physical stresses affecting the system. Particularly, we showed that different kinds of events in the power grid have certain signatures on the time series associated with the states of the system as well as on the correlation pattern among the states. We also discussed that the instantaneous correlation matrix can serve as a visualization tool

[2] Portions of this chapter were published in IEEE Xplore [68] and IET Smart Grid [69]. Copyright permissions from the publishers are included in Appendix B.

that can guide operators in detecting and locating the stresses instantaneously. By presenting the instantaneous correlation matrix corresponding to the states of the grid as an image, in [68], we proposed an image-processing-based technique for the detection and locating of anomalies in the system.

In this next work [69], we extend the work in [68] to study the effects of multiple stresses on the instantaneous correlation matrix corresponding to the states of the grid. Furthermore, we improve the technique presented in [68] for detecting and locating the stresses in the system by introducing a classification technique that alleviates the challenge of characterizing detection thresholds in the image-processing-based technique. Specifically, the proposed technique exploits the features extracted from the instantaneous correlation matrix and trains a $k-$ Nearest Neighbour ($k-$NN) classifier for the detection of the stresses. The locations of the stresses are also determined from the correlation patterns of the buses in real-time. Once the model is trained with historical data, real-time detection, and locating require a small amount of past data to calculate the instantaneous correlation matrix. The technique is capable of detecting multiple cyber attacks and single-line tripping events in the smart grid with improved and promising detection and false-positive rates.

3.1 Related Work

Over the past decades, a large body of work is focused on detecting and locating cyber and physical stresses in power systems. Many such methods are data-driven techniques that exploit PMU or other types of historical data for developing models for detecting stresses. Some of such models use dimensionality reduction techniques to represent and analyze the large volume of data using lower-dimensional models [70, 71, 72, 73]. For instance, Chen *et. al.* [70] uses historical data for real-time prediction of one-step-ahead states. In this approach, if the error of prediction exceeds a certain threshold compared to the actual measurements then an anomaly is declared. In [71], a real-time anomaly detection method is proposed in which the lower-dimensional representation of the PMU data using feature selection. Then, the isolation forest (iForest) algorithm is used for the detection of anomalies. In [72], Cai *et. al.* considered the PMU data stream as a multivariate time series. Then using principal component analysis (PCA) lower-dimensional representations of the time series are obtained and the T^2 and the Q statistics of the principal components are used as the features for detection. Finally, a $k-$nearest neighbor ($k-$NN) method has been applied in real-time to detect the stresses. Mahapatra and Chaudhuri [73] also proposed a technique for the detection of cyber-attacks in wide-area systems based on the PCA of the PMU data.

Neural network-based methods are also popular for detecting and locating stresses in smart grids. For instance, Basumallik *et. al.* [74] proposed a convolutional neural network (CNN) based detection and classification for detecting anomalies from the packet-PMU data. In this work, the PMU data from different PMUs at the phasor data concentrator (PDC) is considered as a multivariate time series. The cross-correlation matrices corresponding to different types of anomalies are taken as the features for the CNN classifier. Ganjkhani *et. al.* [75] proposed a nonlinear auto-regressive exogenous neural network (NARXNN) for the real-time detection of false data injection attacks in the smart grid. NARXNN is a robust recurrent neural network model that is specially designed for time series data. In this method, the high correlations among states are used for one-step-ahead prediction of the states using measurement values along with historical data. The false data is then detected by comparing the predicted state values and the original measurements.

In addition to the aforementioned works, some studies use data mining and Bayesian models. For instance, Pan *et. al.* [76] introduced a data mining-based intrusion detection system for the detection and classification of normal operations, cyber-attacks, and disturbances. The authors in this work used the common path mining technique on both of the synchrophasor data and the power system audit logs. Karimipour *et. al.* [77] presented an unsupervised machine-learning method for the detection of cyber-attack in smart grids in real-time. In this work, Symbolic Dynamic Filtering (SDF) is used for the extraction of the feature. The learning is based on a dynamic Bayesian network model.

Moreover, some researchers have utilized the spatial and temporal correlation among the measurements throughout the power grid to detect stresses in the system. For instance, Li *et. al.* in [78] proposed a real-time detection and locating technique for false data injection attacks in the smart grid. In this work, they used the hidden Markov model (HMM) to recover the temporal correlations in measurements that are applied to detect the anomalies. Vector auto-regression is used to capture the spatial correlation among the measurements to locate the attack. Shi [79] proposed a spatio-temporal correlation-based monitoring, and anomaly detection and locating for distribution networks.

Among the other methods for detecting anomalies, Kurt *et. al.* [80] used a cumulative sum (CUSUM) based algorithm for the real-time detection of cyber and hybrid attacks in smart grids. Furthermore, Chu *et. al.* [81] proposed a quadratic prediction-based algorithm for the detection of cyber-attacks and anomalies. In this work, a three-sample quadratic prediction algorithm (TSQPA) based filter predicts one sample from its previous three samples. The error between the predicted sample and the measured sample is used to detect the stress. This work shows that the technique performs quite accurately on the suddenly applied false data, but when a set of false measurements is inserted gradually in the system i.e. ramp-attacks the technique sometimes fails.

In this work, the time-varying states corresponding to the power grid buses are considered as the multivariate time series. The time-varying states can be obtained from the PMU data or by the sequence of measurements from the supervisory control and data acquisition (SCADA) system. In [69], a $k-$NN classification method is applied while the features for the training are determined from the instantaneous correlation matrix corresponding to the states. Instead of taking each pixel of the instantaneous correlation matrix image as features similar to [74], features are extracted to train the $k-$NN method for classification which is computationally efficient.

3.2 Effects of Cyber and Physical Stresses on Instantaneous Correlations

The electrical attributes associated with the buses and the branches in power systems can be considered as the state variables that collectively define the state of the system. The voltage phasors (voltage magnitudes and angles) of the buses in power systems are examples of key attributes that can enable the specification of the state of the system and other system attributes. Let us denote the set of all buses in the system by $\mathcal{B}$ with the cardinality of the set represented by $|\mathcal{B}| = N$. The value of a specific electrical attribute associated with bus $i \in \mathcal{B}$ at time instant t is denoted by $x_i(t)$. The $N-$ dimensional vector $\underline{\boldsymbol{x}}(t)$ represents the values of the attribute of all the buses at time t.

In this work, the voltage angles of the buses are considered as the state variables of the system. The reason behind this is that based on rigorous simulation and numerical evaluations, it is observed that the effects of changes in the system (e.g., load variations and most of the other phenomena such as cyber and physical stresses) are reflected in the bus voltage angle values. For the rest of this chapter, $\underline{\boldsymbol{x}}(t)$ represents the bus voltage angles at time t, otherwise stated.

3.2.1 Instantaneous Correlation Matrix

In power systems, the time series of bus voltage angles associated with the buses within certain vicinity (geographical or topological) have strong correlations. Figure 3.1(a) illustrates the average correlation among the bus voltage angles of the IEEE 118 [62] bus system throughout the day. Note that in this figure, the blue pair of horizontal and vertical lines correspond to the reference bus that has a voltage angle of 0 at all times. For better visualization of the average correlation matrix, the reference bus has been omitted in the analysis in the work as can be seen in Figure 3.1(b).

Based on the average correlation matrix image in Figure 3.1(b), it can be observed that the voltage angles of buses in a vicinity have strong correlations. However, due to continuous changes in the load of the buses and other dynamics of the system, the correlation among the

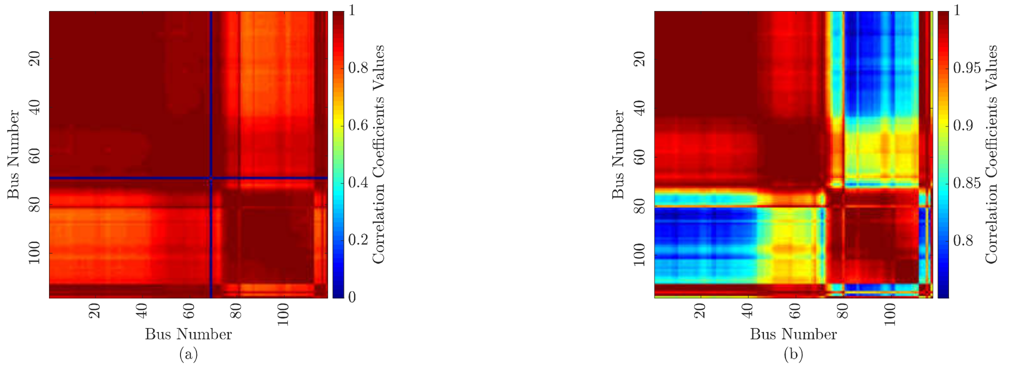


Figure 3.1: Average correlations among PMU data (specifically, voltage angles) in the IEEE 118 bus system (calculated over day-long time series). The average correlation among states are represented as images:(a) including the reference bus 69, and (b) without the reference bus and re-scales to adjust image intensity values.

bus voltage angles varies considerably from time to time. For this reason, we are interested in the instantaneous correlation among the bus voltage angles instead of the average correlation.

The instantaneous correlation matrix of the bus voltage angles at any time instant t is a $N \times N$ square matrix $\mathbf{C}(t)$ with element $c_{ij}(t)$ defined as:

$$c_{ij}(t) = \frac{\int_{t-t_c}^{t} x_i(\tau)x_j(\tau)d\tau}{\sqrt{\int_{t-t_c}^{t} x^2{}_i(\mu)d\mu}\sqrt{\int_{t-t_c}^{t} x^2{}_j(\nu)d\nu}}, \quad i,j \in \mathcal{B}, \tag{3.1}$$

where t_c is the length of the correlation window. Although the length of the correlation window affects the instantaneous correlation matrix, in this work, this effect has not been studied and instead a constant t_c is considered.

In addition to the changes in load variations in time, the instantaneous correlation matrix changes due to cyber and physical stresses. Specifically, for physical stresses, such as the tripping of a transmission line or generator, the topology and dynamics of the system change abruptly. As a result, the state variables of the grid change, and the changes will be reflected in the instantaneous correlation matrix, $\mathbf{C}(t)$. Similarly, in the case of cyber attacks, the obtained values for the state variables change, and thereby the instantaneous correlation matrix, $\mathbf{C}(t)$ undergoes abrupt change. Our studies show that although the instantaneous correlation matrix, $\mathsf{C}(t)$ changes continuously in time due to the dynamics of the system and load variations as well as stresses, the pattern of the change is quite different in normal and abnormal situations. In general, changes due to stresses are more abrupt and localized than the changes due to the normal load variations throughout the day. This difference in the changing pattern of the instantaneous correlation matrix, $\mathsf{C}(t)$ is exploited for monitoring of the system, and detecting and locating cyber and physical stresses.

In the first step, it has been proposed that the visualization of the instantaneous correlation matrix, $\mathsf{C}(t)$, as an image can enable real-time visualization of abnormal changes and detection of stresses. Specifically, any change corresponding to the cyber or physical stresses can be visually detected and located from the instantaneous correlation matrix image due to sharp lines appearing in the images (will be discussed in the following subsections). We will specifically discuss how different cyber and physical stresses can be reflected in the bus voltage angle time series and how they can be monitored visually with the help of the instantaneous correlation matrix image. Later in this work, the instantaneous correlation matrix will be analyzed using a classification method to automatically detect the abnormalities in the system.

3.2.2 Visualizing Cyber Stresses Using Instantaneous Correlation Matrix Image

Various types of cyber-attacks can threaten the security and reliability of smart grids and attackers are always on the hunt for new methods to hamper the security of the system [9, 82, 83, 84]. In this work, we have considered three types of cyber-attacks including DoS attack [85], Data-replay attack [85, 86], and Ramp attack [81]. The DoS attack and Data-replay attacks are common types of attacks in cyber-physical systems. The ramp attack is a special type of data integrity attack in which the attacker introduces false measurements into the system gradually with time to deceive the system and operators. The detection of this type of attack is difficult because of the absence of sharp discontinuities at the onset of the attack. In this subsection, we present simple mathematical formulations of different cyber-attacks and illustrate their effects on the bus voltage angle time series. We will also show the visualization of their effects in the instantaneous correlation matrix image. For the purpose of defining cyber attacks, let $\mathcal{A} \subset \mathcal{B}$ be the set of buses under cyber attack and $\mathcal{S} \subset \mathcal{B}$ be the set of buses that the attackers have access to record data. Note that in practice, various constraints, such as technical, physical and limited resources, can affect the size and distribution of the sets $\mathcal{A}$ and $\mathcal{S}$ and in general the capabilities of attackers in launching the attacks. While such constraints can affect the spread and severity of the attacks and thereby impact the performance of detection and locating mechanisms, these aspects are not the focus of this work. Here, it is assumed that the attacker has the capability to launch single or multiple attacks on any of the buses of the system.

3.2.2.1 DoS Attack

The DoS attack is modeled as the absence of measurements or unobservability of any of the state variables for a certain period of time (i.e., from the time instant t_{Start} to the time instant t_{End} the value of variables associated with attacked components are not sampled or communicated). Let, $x_i(t)$ be the actual time series of any state variable (i.e., any electrical attribute such as voltage phase angle) corresponding to the $i-$th bus, and $x_{\text{DoS}_i}(t)$ is the time series corresponding to the state under DoS attack. The DoS attack is modeled as follows:

$$x_{\text{DoS}_i}(t) = \begin{cases} n_i(t) & \text{if } t_{\text{Start}} \leq t \leq t_{\text{End}} \\ x_i(t) + n_i(t) & \text{otherwise,} \end{cases} \tag{3.2}$$

where $n_i(t)$ is the Additive White Gaussian Noise signal associated with the $i-$th bus voltage angle measurement. Figure 3.2 (a) illustrates the voltage angle time series associated the bus number 87 in the IEEE 118 system when there is a DoS attack at that bus within the time interval $t_{start=5}$ to $t_{\text{End}} = 6$. Figure 3.2 (b) and Figure 3.2 (c) are two consecutive frames of $\mathbf{C}(t)$, which show just before the onset of the attack (i.e., at $t = t_{\text{Start}} - \epsilon$, where ϵ is a small constant) and just after the onset of the attack (i.e., at $t = t_{\text{Start}} + \epsilon$), respectively. By comparing these two consecutive frames of $\mathbf{C}(t)$, one can observe that a pair of horizontal and vertical lines corresponding to the attached bus (i.e., in this case, bus 87) appear in the matrix image of $\mathbf{C}(t)$ after the attack.

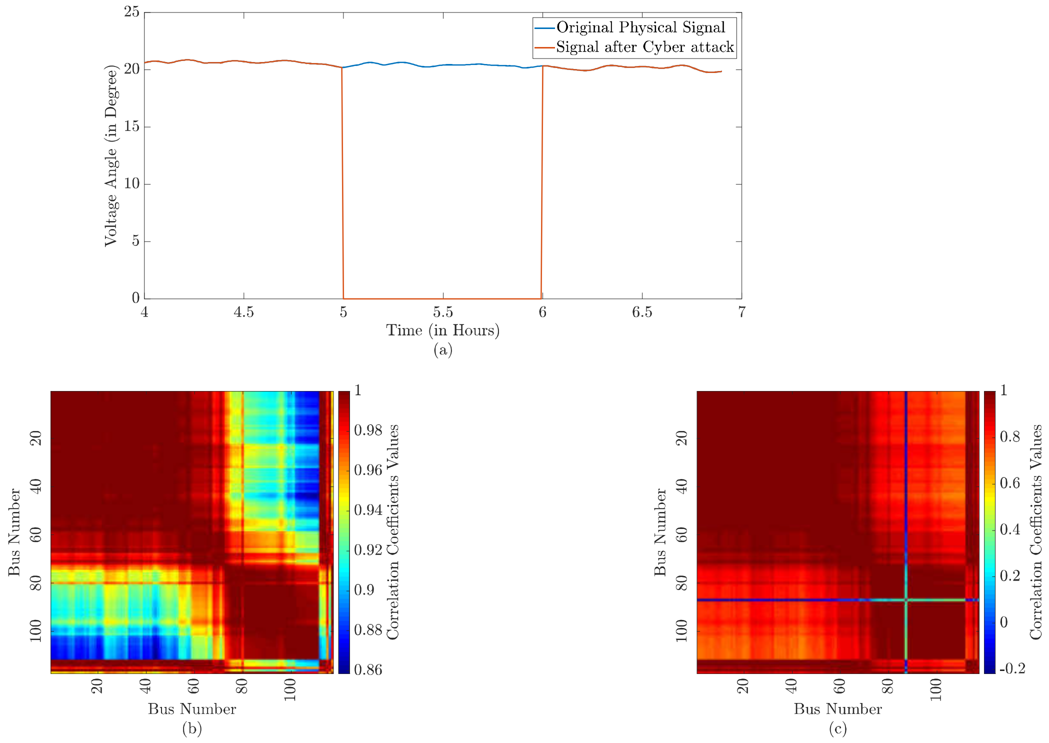


Figure 3.2: DoS attack at bus 87 in the IEEE 118 bus system. The effects of the attack are reflected on: (a) voltage angle signal at bus 87, (b) instantaneous correlation matrix at $t_{\text{Start}} - \epsilon$, and (c) instantaneous correlation matrix at $t_{\text{Start}} + \epsilon$. The blue pair of horizontal and vertical lines in the latter indicates the attack.

3.2.2.2 Data Replay Attack

The data-replay attack or replay attack is a cyber-attack in which the attacker records the data stream from some of the buses and injects them later into the data stream of the same buses or other buses that they have compromised. Mathematically the data replay can be expressed as follows:

$$x_{\text{Replay}_i}(t) = \begin{cases} x_k(t' + t - t_{\text{Start}}) + n_i(t) & \text{if } t_{\text{Start}} \leq t \leq t_{\text{End}} \\ x_i(t) + n_i(t) & \text{otherwise,} \end{cases} \tag{3.3}$$

where t_{Start} and t_{End} are the starting and ending of the replay attack, respectively, and t' is the starting of the recording time. Here, $i \in \mathcal{A}$ and $k \in \mathcal{S}$.

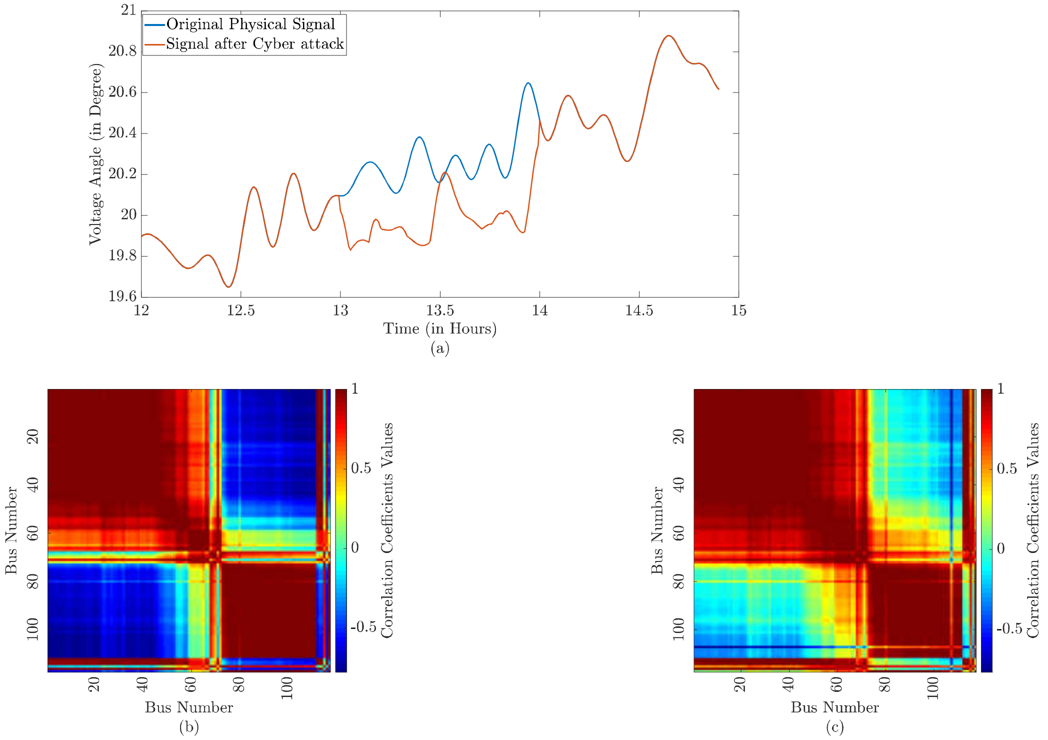


Figure 3.3: Replay attack at bus 107 in the IEEE 118 bus system. The effects of the attack are reflected on: (a) voltage angle signal at bus 87, (b) instantaneous correlation matrix at $t_{\text{Start}} - \epsilon$, and (c) instantaneous correlation matrix at $t_{\text{Start}} + \epsilon$. The blue pair of horizontal and vertical lines in the latter indicates the attack.

Figure 3.3 (a) illustrates the voltage angle time series associated with bus number 107 in the IEEE 118 system when there is a data-replay attack at that bus within the time interval $t_{start=13}$ to $t_{\text{End}} = 14$. Figure 3.3 (b) and Figure 3.3 (c) are two consecutive frames of $\mathbf{C}(t)$, which show just before the onset of the attack (i.e., at $t = t_{\text{Start}} - \epsilon$, where ϵ is a small constant) and just after the onset of the attack (i.e., at $t = t_{\text{Start}} + \epsilon$), respectively. A pair of horizontal and vertical lines corresponding to bus number 107 is visible when the attack occurred in the system. However, another pair of horizontal and vertical lines corresponding to bus number 80 is also visible in $C(t_{\text{Start}} - \epsilon)$. This is due to the dynamics of the system and load variations at bus number 80, which has resulted in a different correlation pattern with other buses. Prior knowledge of this type of behavior can be helpful in eliminating false alarms in the system. In the automated method of detection that will be discussed in the next section, these kinds of situations are handled automatically by training the model using data from normal and abnormal states of the system.

3.2.2.3 Ramp Attack

The ramp attack is a special type of FDIA in which the attacker gradually introduces bad data into the data stream. Any linear-prediction-based detector will fail to detect this type of attack due to its gradual change. In Figure 3.4 (a), we observe the ramp attack at time 3.00. Instead of a sharp change in values at the instant $t = 3.00$, falsified measurements are gradually injected into the time series associated with the bus voltage angle of bus number 28. Mathematically, this type of attack can be expressed as follows:

$$x_{\mathrm{Ramp}_i}(t) = \begin{cases} x_i(t_{\mathrm{Start}}) + n_i(t) + m \times (t - t_{\mathrm{Start}}), & \text{if } t_{\mathrm{Start}} \leq t \leq t_{\mathrm{End}} \\ x_i(t) + n_i(t), & \text{otherwise,} \end{cases} \tag{3.4}$$

where m is the slope.

Similar to the previous attacks, the ramp attack can be detected and located visually from two consecutive instantaneous correlation matrices as can be seen in Figure 3.4 (b) and Figure 3.4 (c). However, since in the ramp attack, the value of the variable (i.e., voltage angle) in the compromised bus changes gradually, the effect of the stress may be noticeable after one or two sampling instances from the attack instance (i.e., it might be reflected on $\boldsymbol{C}(t_{\mathrm{Start}} + \epsilon^{'})$ instead of $\boldsymbol{C}(t_{\mathrm{Start}} + \epsilon)$, where, $\epsilon^{'} \geq \epsilon$.

3.2.2.4 Multiple Cyber Attacks

The examples shown in Figures 2, 3, and 4 depicted the effects of single cyber attacks in the system on the instantaneous correlation matrix. We can evaluate the effects of multiple attacks similarly. In Figure 3.5 the instantaneous correlation matrix of the system is shown after multiple attacks. Figure 3.5 (a) presents the instantaneous correlation matrix of the

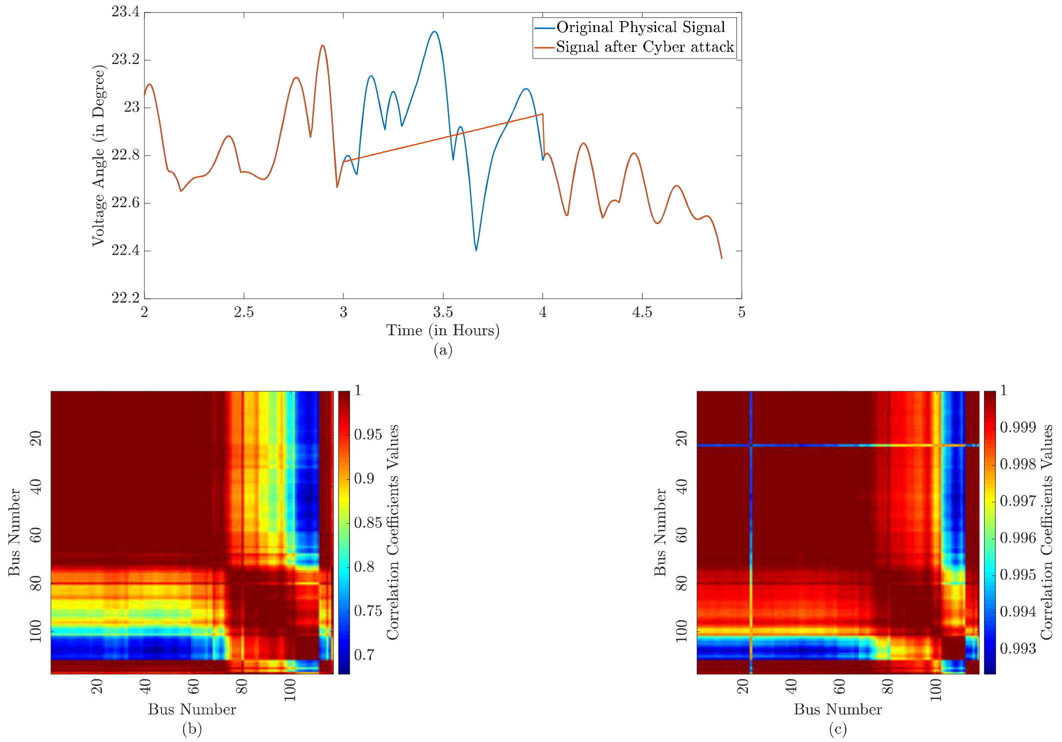
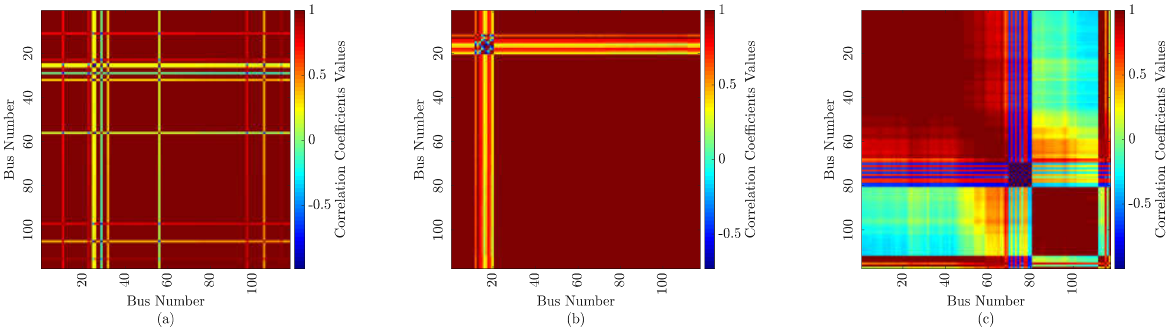


Figure 3.4: Ramp attack at bus 23 in the IEEE 118 bus system. The effects of the attack are reflected on: (a) voltage angle signal at bus 23 (b) and (c) instantaneous correlation matrices at two consecutive frames, where the blue pair of horizontal and vertical lines indicates the attack.

system after multiple cyber attacks launched on random buses throughout the grid. Figure 3.5 (b) and Figure 3.5 (c) represent multiple cyber attacks on the clustered buses (buses within certain vicinity) during normal and high fluctuation load variation periods, respectively. As can be observed from Figure 3.5 (c), when load variations in the system are high, detecting and locating attacks are more challenging.

3.2.3 Effects of Physical Stresses on Instantaneous Correlation Matrix Image

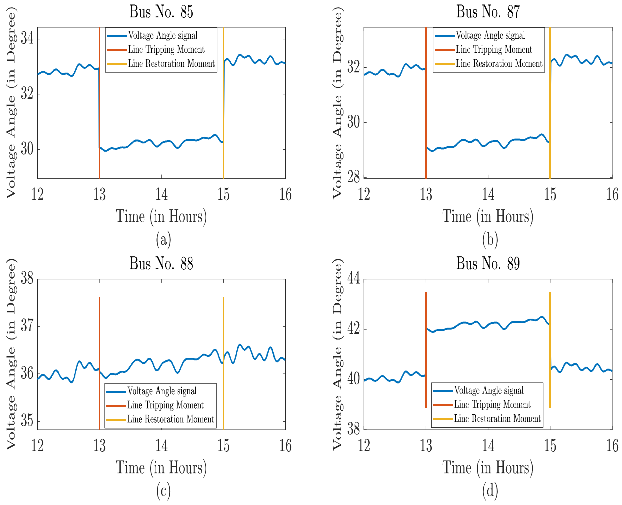
Physical stresses in power grids generally involve changes in the physical state of the components (e.g., functional state of the components, load on the components). Tripping of a transmission line or a generator or changes in the reactive power are some examples of physical stresses. In this work, the effects of tripping a single transmission line in the system on its state and the instantaneous correlation matrix will be studied.



(a) (b) (c)

Figure 3.5: Multiple cyber attacks on the IEEE 118 bus system at a single time instant. t_A is the attack instant. Instantaneous correlation matrix at $t_A + \epsilon$ for (a) random attacks, (b) clustered attacks, and (c) clustered attacks during a high load fluctuation period.

Physical stresses in power systems usually affect the state of the components that are within a certain vicinity of the location of the incidence. The effects, in general, depend on various factors such as the structure and dynamics of the system. For example, Figure 3.6 illustrates the effect of tripping the transmission line between bus number 85 and 89 of the IEEE 118 bus system on the bus voltage angle signal of the nearby buses. We observe that the tripping affects the bus voltage angle signals of bus numbers 85, 87 & 89. However, the bus voltage angle time series associated with bus number 88 seems to be unaffected although this bus is also geographically adjacent to the tripped line.



(a) (b) (c) (d)

Figure 3.6: The effects of a single line trip on the signal of a few of its adjacent buses.

Similar to the cyber-attacks, physical stresses can be visually detected from the instantaneous correlation matrix images, but since this kind of stresses affects voltage angle measurement of the nearby buses the exact location of the stress is comparatively difficult to identify. Instead of a single pair of horizontal and vertical lines in the cyber-attack cases, a region with sharp variations is observed in the instantaneous correlation matrix images. For example, from the instantaneous correlation matrix image in Figure 3.7, it can be specified that the physical stress has occurred somewhere within buses indexed 68 to 75. The stress is in fact tripping of the line connecting bus numbers 75 and 77.

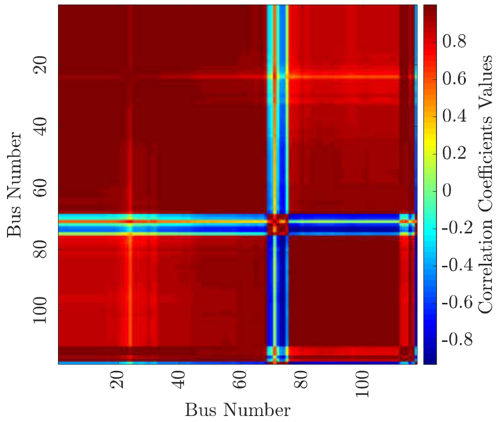


Figure 3.7: Instantaneous correlation matrix corresponding to a single line tripping.

3.3 Detection and Location Identification Using Image Processing on Instantaneous State Correlation Matrix Image

3.3.1 Detection and Location Identification Technique

In [68], a technique was proposed to provide the operator with an early alert about the cyber attacks on the smart grid and to find the attack locations based on the instantaneous state correlations. An operator can have an alarm of any cyber or physical anomaly by visualizing the instantaneous state correlation matrix image itself in real-time and the location of the attack is also identifiable from the image in real-time based on the horizontal

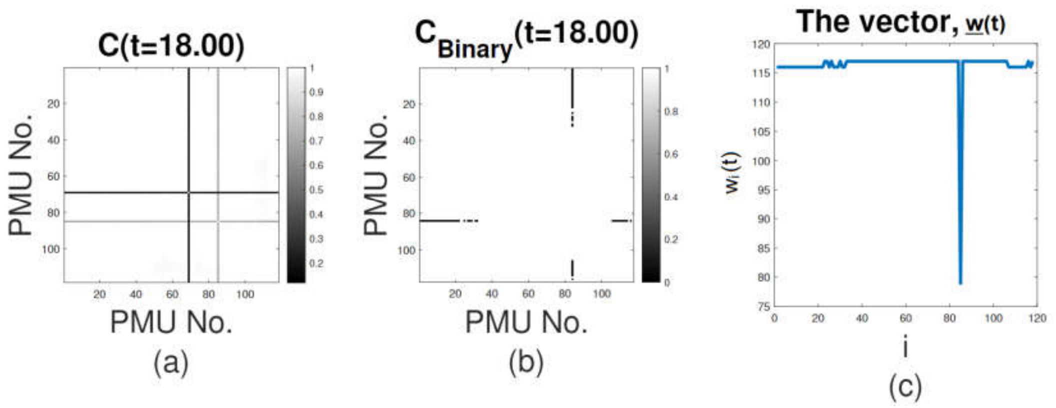


Figure 3.8: (a) Instantaneous correlation matrix at the onset of the ramp attack, (b) image after removing reference PMU and thresholding, (c) the vector, $\underline{\mathbf{w}}(t)$

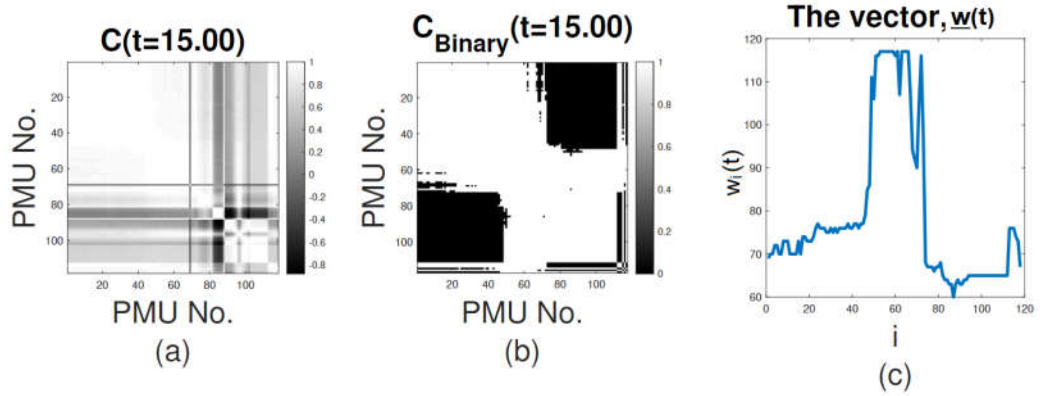


Figure 3.9: (a) Instantaneous correlation matrix at the onset of a physical event (restoration of a tripped line), (b) Image after removing reference PMU and thresholding, (c) the vector, $\underline{\mathbf{w}}(t)$.

and vertical lines that appear in the image. The automatic identification of the anomalies involves a simple image processing technique (i.e. detecting horizontal and vertical lines for cyber-attacks.)

For detecting and locating the attack in real-time, the instantaneous correlation matrix image, $\boldsymbol{C(t)}$ is processed for each time instant, t. The steps are given below:

1. Converting $\mathbf{C}(t)$ to binary form: At first, we remove the horizontal and vertical lines for the reference (slack bus) from $\mathbf{C}(t)$. Then we apply a threshold to that image to obtain a binary image, $\mathbf{C}_{Binary}(t)$. Here, we have selected the threshold as the median

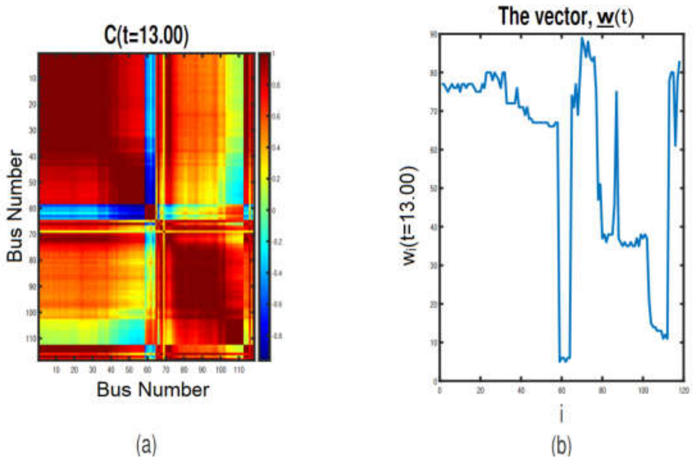


Figure 3.10: (a) Instantaneous correlation matrix at the onset of a physical event (tripping line between bus no. 55 and bus no. 59), (b) the vector, $\underline{\mathbf{w}}(t)$ at the onset of the event.

of the intensity values of the pixels of $\mathbf{C}(t)$. $\mathbf{C}(t)$ and $\mathbf{C}_{Binary}(t)$ are shown in Figure 3.8(a) and Figure 3.8(b), respectively.

2. Calculating $\underline{\mathbf{w}}(t)$: From the binary correlation image we determine the number of buses with which a particular bus has a significant amount of correlation (above threshold). Let the $i-$th element of the vector $\underline{\mathbf{w}}(t)$, denoted as $w_i(t)$ represents the number of buses with which the time series of the $i-$th bus has a significant correlation at time instant t, where $i \in \mathcal{P}$. We calculate the $\underline{\mathbf{w}}(t)$ as:

$$\underline{\mathbf{w}}(t) = C_{Binary}(t)\underline{\mathbf{u}}, \tag{3.5}$$

where $\underline{u} = [1, 1, ...1]^T$, and:

$$\underline{\mathbf{w}}_{hist} = \mathbf{C}_{hist}\underline{u}, \tag{3.6}$$

where $\mathbf{C}_{hist}$ is the historical average correlation matrix.

3. Detecting and Locating Cyber Attack: Let us denote the $n-th$ minimum element of a vector, $\underline{x}$ as $min(\underline{x}, n)$. For the detection of the cyber-attack, at first, the PMU which is compromised by the attacker is found. This PMU can be identified as the index of

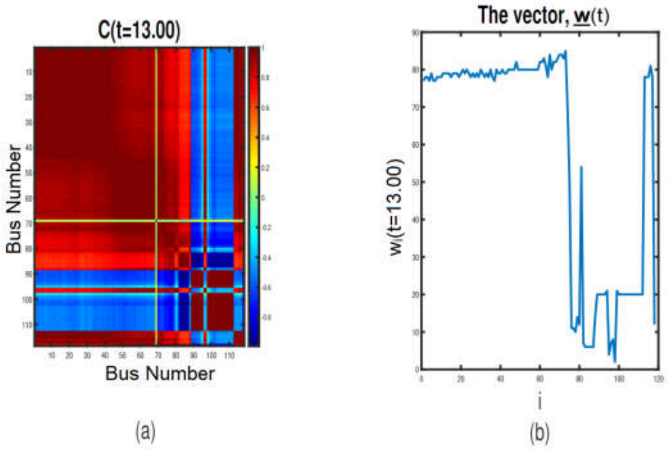


Figure 3.11: (a) Instantaneous correlation matrix at the onset of a physical event (tripping line between bus no. 92 and bus no. 102), (b) the vector, $\underline{\mathbf{w}}(t)$ at the onset of the event.

the minimum element of $\underline{\mathbf{w}}(t)$. Mathematically, the index, l of the attacked PMU is calculated from the following equation:

$$\underline{\mathbf{w}}_l(t) = min(\underline{\mathbf{w}}(t), 1). \tag{3.7}$$

Some of the PMUs have significant correlations with only a small number of PMUs, even in normal conditions. The set of all such PMUs can be defined as $\mathcal{Q} = \{q : w_{hist,q} < n_{th}\}$, where, n_{th} is selected empirically. Therefore, for avoiding false positives, it is ensured that l is not a member of this set. However, a cyber attack is declared if:

$$min(\underline{\mathbf{w}}(t), 2) - min(\underline{\mathbf{w}}(t), 1) > b, \quad l \notin \mathcal{Q}, \tag{3.8}$$

where b is a threshold selected empirically. Also, l is declared as the index of the compromised PMU.

The cyber-attacks can be distinguished from the physical events in this process as in the next example. Figure 3.9 illustrates the effect of a physical phenomenon on the correlation matrix. From Figure 3.9(c) it can be observed that, a few consecutive elements of the vector

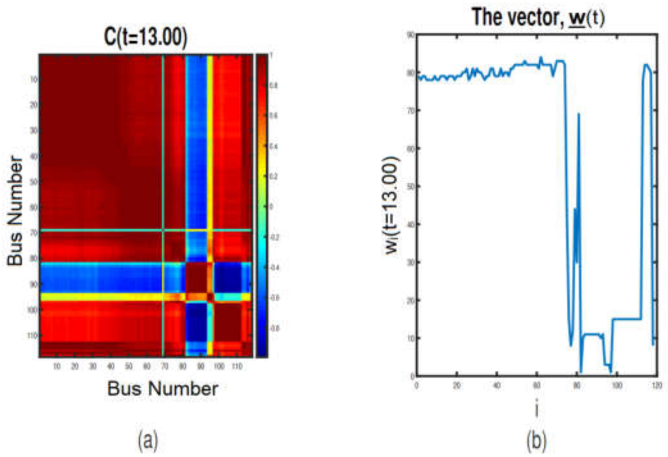


Figure 3.12: (a) Instantaneous correlation matrix at the onset of a physical event (tripping line between bus no. and bus no. 89), (b) the vector, $\underline{\mathbf{w}}(t)$ at the onset of the event.

Table 3.1: Performance Evaluation of the Image Processing on Instantaneous Correlation Matrix Technique.

Cyber Attack Type	**Detection Rate**	**Exact Locating Rate**
DoS Attack	1.0000	0.9915
Replay Attack	0.9915	0.8803
Ramp Attack	0.9402	0.8454

$\underline{\mathbf{w}}(t)$ are comparatively smaller than the others unlike cyber-attacks illustrated in Figure 3.8, where a single element of the vector $\underline{\mathbf{w}}(t)$ is very small compared to the others.

3.3.2 Simulation and Performance Analysis

Our evaluations show that the proposed method has a good performance in the detection of cyber-attacks. Table. 3.1 shows the detection and the correct locating rate for different types of cyber-attacks. The average detection and locating rates have been calculated by simulating cyber-attacks in all the buses of the IEEE 118 bus system. This method performs well for the ramp attacks as well, which are challenging to detect because of the gradual injection of the falsified data.

3.3.3 Detecting and Locating Physical Stresses

Since any physical event on a single bus affects the electrical attributes of several buses, determining the exact bus location is difficult from the correlation image. In some cases, we can exactly detect and locate physical attacks. Figure 3.10 illustrates the detection of the tripping of Branch No. 87 in the IEEE 118 bus system, which connects BUS No. 55 and BUS No. 59. From the correlation matrix in Figure 3.10(a) we can easily identify some anomaly near bus No. 58 to bus No. 64. Since we can see horizontal and vertical lines within a range instead of a single PMU (as in the case of cyber attack), it can be decided that the stress is physical. The effect is also identifiable from $\underline{\mathbf{w}}(t)$ in Figure 3.10(b) and the algorithm locates PMU No. 59 as the anomalous PMU, which was in fact connected to the tripped line.

However, in some cases, this method detects the event correctly but fails to locate it exactly. For example, we simulated a line tripping between BUS No. 92 and BUS No. 102. From Figure 3.11(a) we can easily identify that there is an event within BUS No. 82 and BUS No. 93, but the method locates the failure at BUS No. 82, which is in fact two hops away from BUS No. 92. And in some cases, the method fails to detect physical events. Figure 3.12 illustrates such cases.

In summary, the proposed method based on the state correlation matrix can detect and locate cyber attacks with good performance. However, while the method can detect physical stresses and distinguish them from cyber attacks, it may not be able to accurately locate the physical stresses in the system. In the following section, an improved method for detecting and locating stresses has been discussed which

3.4 Detection and Location Identification Using the $k-$Nearest Neighbor Analysis of Instantaneous State Correlation

In this section, the instantaneous correlation matrix, which bears information about the cyber and physical stresses, will be used to develop methods for detecting and locating the stresses in the system using the $k-$nearest neighbor analysis of the correlation matrices. In [68], a method for detecting and locating stresses from the instantaneous correlation matrix, $\mathbf{C}(t)$ has been developed for single stresses using image processing techniques. In the current work, a new method has been introduced based on classification methods to enhance the previous technique by adding robustness against load variations and being able to detect multiple cyber attacks. Specifically, the presented method in this work addresses the challenge of characterizing thresholds for the detection of stresses used in the previous method with a machine learning-based approach, which extracts features and classifies the data (as anomalous or normal) using the $k-$ nearest neighbor method. For the extraction of the features, both the correlation values at the decision instant and the difference of the correlation values with its previous instant are used. In the following subsections, the processes of detection and localization have been discussed. The steps of the presented method have been illustrated using a flow chart in Figure 3.16.

3.4.1 Aggregated Instantaneous Correlation Vectors

The proposed method in this work utilizes the information embedded in the instantaneous correlation matrix. As such the first step of the proposed process would be to calculate the instantaneous correlation among the state of the components using PMU time series. As discussed earlier, at each time instant, t we calculate $\mathbf{C}(t)$ from the values of the state variables using equation (3.1). In the results presented in this work, we have considered the correlation window of width 30 seconds. In the previous section, we observed the effects of stresses and anomalies in the system by visualizing $\mathbf{C}(t)$ as an image. For designing analytics that can detect changes in the $\mathbf{C}(t)$, we need further processing of $\mathbf{C}(t)$. To this end, we calculate the aggregated correlation for each individual component with the rest of the components of the system at time t. Specifically, we denote the vector of all aggregated correlations by $\underline{\mathbf{v}}(t)$ defined as $\underline{\mathbf{v}}(t) = \mathbf{C}(t)\underline{\mathbf{u}}$, where $\underline{\mathbf{u}} = [1, 1, ...1]^T$ (i.e., the vector $\underline{\mathbf{v}}(t)$ is the column sum of the matrix $\mathbf{C}(t)$).

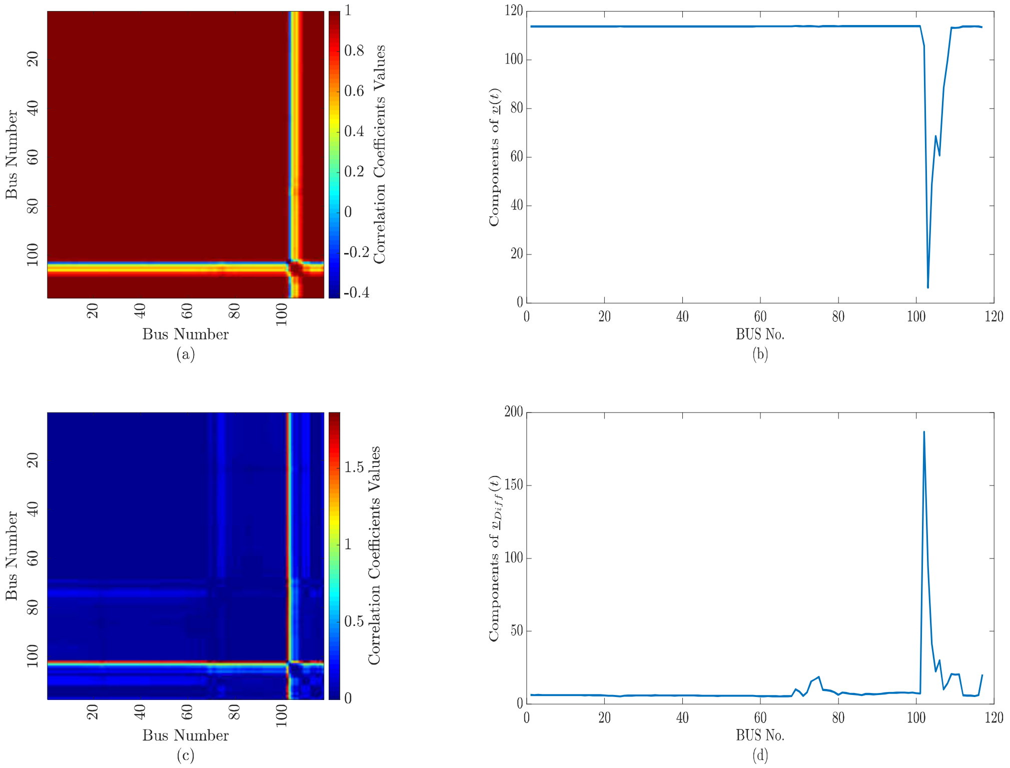
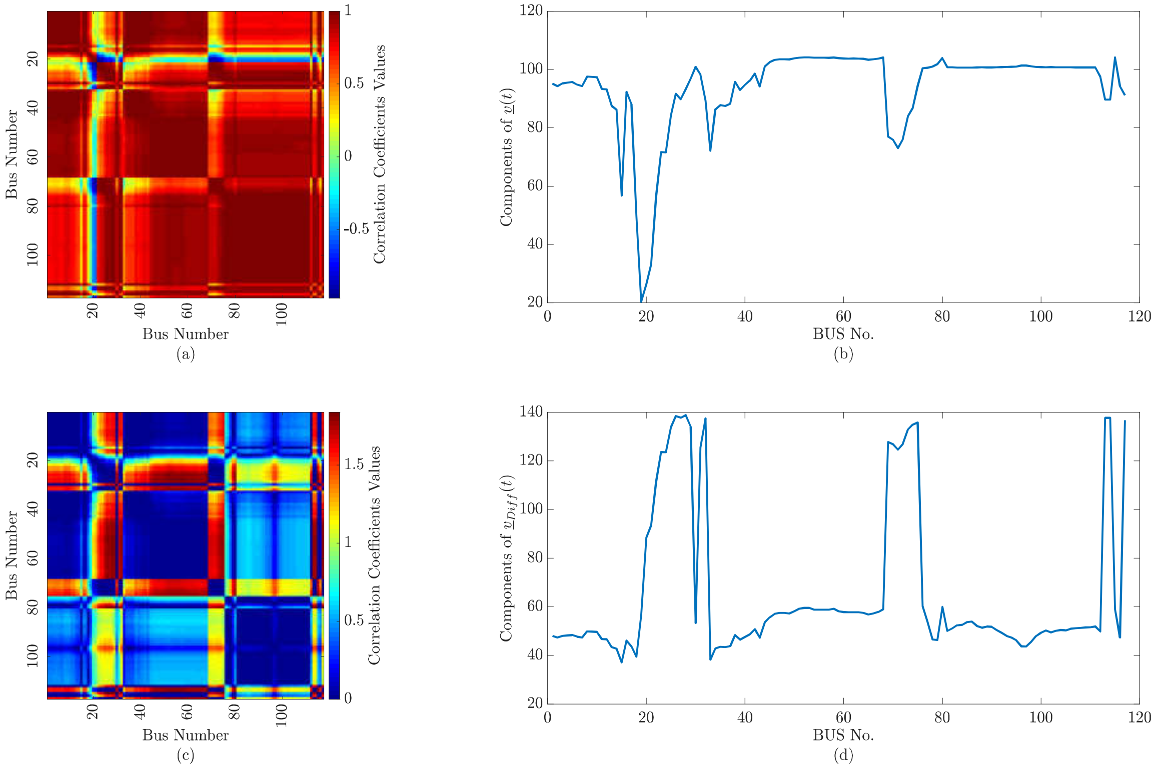


Figure 3.13: The effects of a single line failure on (a) instantaneous correlation matrix image $\mathbf{C}(t)$, (b) the aggregated correlation vector $\underline{\mathbf{v}}(t)$, (c) the correlation difference matrix image, $C_{\text{Diff}}(t)$, and (d) $\underline{\mathbf{v}}_{Diff}(t)$.

Figure 3.13 (a) and Figure 3.13 (b) illustrate $\mathbf{C}(t)$ and $\underline{\mathbf{v}}(t)$ after a single line trip. In this case, branch number 165, which is a transmission line connecting buses 103 and 104 in the IEEE 118 system, has been tripped. The state variables (i.e. the voltage angle measurements) in the nearby buses have been changed drastically and the correlation of the state variables in this area with the other state variables decreased. This effect can easily be visualized from $\mathbf{C}(t)$ in Figure 3.13(a). In addition, from Figure 3.13(b), we observe that the components of $\underline{\mathbf{v}}(t)$ in the vicinity of the tripped line are significantly lower than other components because the correlations among the other buses do not change significantly. However, depending on the load fluctuations and the location of the stresses, this effect may not be visually obvious all the time, nevertheless, $\underline{\mathbf{v}}(t)$ is a useful source of features for the automated detection and locating of the stresses.

Large load variations in the power systems can result in large variations in the instantaneous correlation matrix $\mathbf{C}(t)$. As a result, if an attack occurs during a high load variation period then sharp changes in $\underline{\mathbf{v}}(t)$ due to the stress becomes difficult to distinguish from changes due to load variations. Although in practice, the load fluctuation scenarios are likely to be less abrupt than cyber and physical stresses and show smaller variations in the correlation, to make the detection method more robust to such scenarios, we consider the difference correlation matrix to capture the temporal change of the correlation patterns in the system. The difference correlation matrix is defined as $\mathbf{C}_{Diff}(t) = \mathbf{C}(t) \sim \mathbf{C}(t - T_s)$, which is the difference matrix between the instantaneous correlation matrix images at the time, t, and its previous sampling instant, $t - T_s$. Similarly to the $\underline{\mathbf{v}}(t)$, we also define the aggregated difference correlation $\underline{\mathbf{v}}_{Diff}(t) = \mathbf{C}_{Diff}(t)\underline{\mathbf{u}}$. In this work, we consider $\mathbf{C}_{Diff}(t)$ and $\underline{\mathbf{v}}_{Diff}(t)$ along with $\mathbf{C}(t)$ and $\underline{\mathbf{v}}(t)$ for the detection of stresses.



(a)

(b)

(c)

(d)

Figure 3.14: Tripping of the transmission line 28, which connects bus number 21 and 22: (a) instantaneous correlation matrix image $\mathbf{C}(t)$, (b) the aggregated correlation vector, $\underline{\mathbf{v}}(t)$, (c) the correlation difference matrix image, $C_{\text{Diff}}(t)$, and (d) $\underline{\mathbf{v}}_{Diff}(t)$.

3.4.2 Feature Extraction and Classification for Stress Detection

In the previous subsections, it was discussed and shown that the vectors $\underline{\mathbf{v}}(t)$ and $\underline{\mathbf{v}}_{Diff}(t)$ contain signatures and patterns of the effects of stresses in the system that can be used for detection. A simple and yet not very effective approach for detecting the stresses using these vectors is to apply thresholds to identify sharp changes in the correlation of the components. However, due to the dynamics of the power system governed by the physics of electricity as well as the stochastic nature of loads and generations in the system, the state variables associated with some of the buses have high variance characteristics, which may lead to sharp changes in vectors $\underline{\mathbf{v}}(t)$ and $\underline{\mathbf{v}}_{Diff}(t)$ causing large false alarms. Moreover, in the case of multiple stresses and during load fluctuations, vectors $\underline{\mathbf{v}}(t)$ and $\underline{\mathbf{v}}_{Diff}(t)$ may contain multiple sharp changes with different amplitudes. Examples of such scenarios are depicted in Figure 3.15 and Figure 3.14. Specifically, Figure 3.15 represents a case in which there is no cyber or physical stresses. Nevertheless, some of the components of $\underline{\mathbf{v}}(t)$ and $\underline{\mathbf{v}}_{Diff}(t)$ seem to have large correlation variations compared to most of the components (they appear as peaks in $\underline{\mathbf{v}}_{Diff}(t)$ and drops in $\underline{\mathbf{v}}(t)$). Another example has been illustrated in Figure 3.14, in which there is a line failure at branch number 28 connecting bus no. 21 and 22 in the IEEE 118 system. This phenomenon is detectable visually from $\mathbf{C}(t)$ and $\underline{\mathbf{v}}(t)$ but in $\underline{\mathbf{v}}_{Diff}(t)$ we notice another anomaly-like region near bus no $70-80$. Therefore, a simple threshold-based method would fail to distinguish normal versus abnormal variations in the correlation.

For this reason, instead of taking decision directly from $\underline{\mathbf{v}}(t)$ or $\underline{\mathbf{v}}_{Diff}(t)$ and using thresholds, we propose to extract a few important features from $\underline{\mathbf{v}}(t)$ and $\underline{\mathbf{v}}_{Diff}(t)$ and apply a machine learning algorithm for classifying the normal and stressed (cyber-attack or line failure) cases. By training the model using samples of normal and abnormal conditions we will show that the false alarms due to normal conditions that cause variations in the correlation can be reduced significantly.

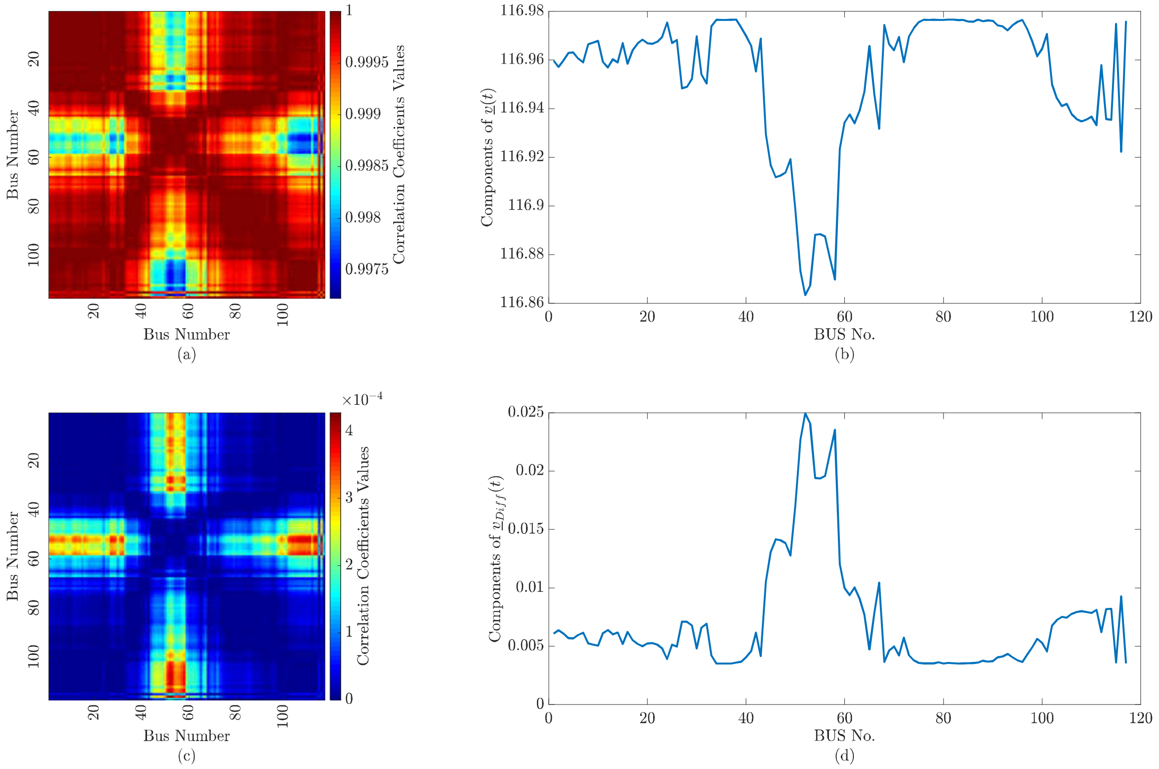


Figure 3.15: No stress scenario: (a) instantaneous correlation matrix image $\mathbf{C}(t)$, (b) the aggregated correlation vector, $\underline{\mathbf{v}}(t)$, (c) the correlation difference matrix image, $C_{\text{Diff}}(t)$, and (d) $\underline{\mathbf{v}}_{Diff}(t)$

The features to be used by the classification method in this work have been identified based on vectors $\underline{\mathbf{v}}(t)$ and $\underline{\mathbf{v}}_{Diff}(t)$ as follows. For $\underline{\mathbf{v}}_{Diff}(t)$, we consider:

- F1: Mean of the vector $\underline{\mathbf{v}}_{Diff}(t)$.
- F2: Standard deviation of vector $\underline{\mathbf{v}}_{Diff}(t)$.
- F3. Difference between the first and second maximum component of $\underline{\mathbf{v}}_{Diff}(t)$.
- F4: Difference between the first and third maximum component of $\underline{\mathbf{v}}_{Diff}(t)$.
- F5: Difference between the standard deviation of the seven largest components of $\underline{\mathbf{v}}_{Diff}(t)$ and the standard deviation of all the components of $\underline{\mathbf{v}}_{Diff}(t)$.

- F6: Difference between the mean value of the three largest components of $\underline{\mathbf{v}}_{Diff}(t)$ and the mean value of all the components of $\underline{\mathbf{v}}_{Diff}(t)$.
- F7: Cardinally of the set, $\{j : 2 \leq \frac{v_{Diff,j}(t)-\mu_{\underline{\mathbf{v}}_{Diff}(t)}}{\sigma_{\underline{\mathbf{v}}_{Diff}(t)}} \leq 6\}$, where, $v_{Diff,j}(t)$ is the $j-$th component of the vector $\underline{\boldsymbol{v}}_{Diff}$ at time t.
- F8: Cardinally of the set, $\{j : \frac{v_{Diff,j}(t)-\mu_{\underline{\mathbf{v}}_{Diff}(t)}}{\sigma_{\underline{\mathbf{v}}_{Diff}(t)}} \geq 6\}$.

To enhance the robustness of the detection method against dynamics, such as load variations, these features have been selected such that they capture multiple peaks' characteristics in $\underline{\mathbf{v}}_{Diff}(t)$. For instance, features F1 and F2 (i.e., the mean and the standard deviation of $\underline{\mathbf{v}}_{Diff}(t)$) are good overall indicators of the existence of peaks due to the stresses. Specifically, peaks due to normal load changes are not usually significant and these first two features can describe the normal variations in the correlations and $\underline{\mathbf{v}}_{Diff}(t)$. On the other hand, features F3 and F4 capture the characteristics of large peaks in $\underline{\mathbf{v}}_{Diff}(t)$ and to specify significant changes in variations. Features F5 and F6 will enable the model to recognize multiple cyber attacks. Features F7 and F8 describe the number of peaks in $\underline{\mathbf{v}}_{Diff}(t)$. The exact definition of these features and their parameters, for instance, the number of the largest values to be considered are identified based on experiment and by trial and error. We use the same set of features mentioned above from vector $|\underline{\mathbf{v}}(t)|$ as well. Note that, although none of these features is a clear indicator of the stress separately, together they can characterize abnormal variations in the signal that is required for classification between normal and abnormal cases. These 16 features are utilized for the classification as discussed next. Using the features extracted from vectors $\underline{\mathbf{v}}(t)$ and $\underline{\mathbf{v}}_{Diff}(t)$, we propose to apply $k-$nearest neighbor ($k-$NN) method for the classification of normal and stress cases.

3.4.2.1 k-NN Method for Classification

After extracting the features from the instantaneous correlation matrix by various signal processing techniques, we formulate the detection of stress at the time, t as a two-class classification problem. Let $\underline{f}(t)$ be the feature vector and $y(t)$ be the class label (i.e., $y(t) \in \{\text{Normal, Stressed}\}$) associated with the instance t. According to the $k-$NN method, the probability of stress at time t is calculated as [87]:

$$Pr\{y(t) = \text{Stressed}\} = \frac{1}{k} \sum_{i \in \mathcal{N}_k(\underline{f}(t))} \mathbb{I}(y(t) = \text{Stressed}), \tag{3.9}$$

where $\mathcal{N}_k(\underline{f}(t))$ is the set of all points in the $k-$nearest neighborhood of the point $\underline{f}(t)$, (i.e. the set of $k-$points that have minimum Euclidean distance from the point $\underline{f}(t)$ in the feature space) and $\mathbb{I}$ is the indicator function. In addition to $k-$NN, we have studied the performance of other classification methods, such as decision trees, and have observed that in this problem $k-$NN outperforms other methods in terms of accuracy and computational time. In the presented method, the $k-$NN classifier is trained with normal and anomalous data generated using the simulations of normal and stresses scenarios as discussed in the Result Section. In its training step, $k-$NN stores the coordinates of the instances and their class label using the features space. In the test step, it decides the class of the instance, i.e., normal or stressed, by computing its neighborhood. The computational efficiency of the $k-$NN classifier makes it suitable for real-time applications such as monitoring the state.

3.4.3 Locating Stresses in the System

The classification method using the introduced features will allow the detection of cyber-attacks and line failure stresses in the system. To determine the location of the stresses, we utilize the vector $\underline{\mathbf{v}}_{Diff}(t)$ directly. We choose $b = max\{\underline{\boldsymbol{v}}_{Diff_k}(t)\}$, i.e., the peak location in this vector, to specify the location of the stress. Note that index b represents the bus index under cyber attack or the bus index of the bus connected to a tripped line in case of physical failure.

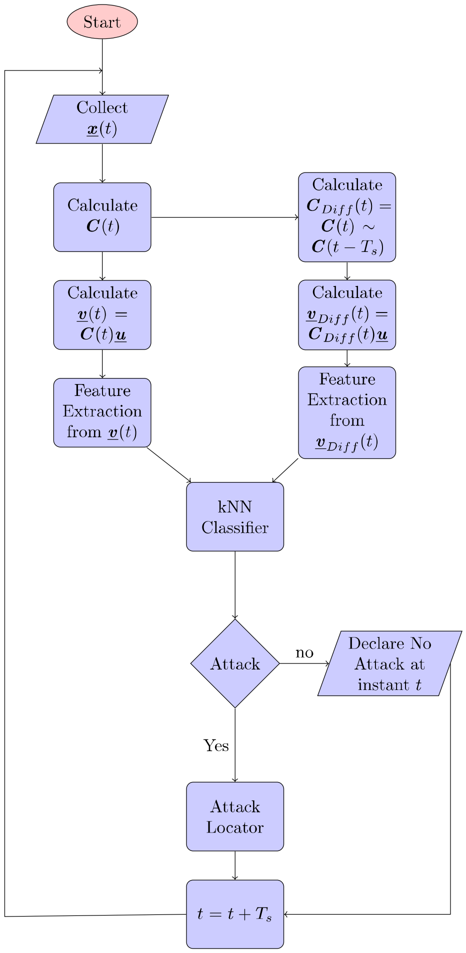

Start
Collect $\underline{\boldsymbol{x}}(t)$
Calculate $\boldsymbol{C}(t)$
Calculate $\boldsymbol{C}_{Diff}(t) = \boldsymbol{C}(t) \sim \boldsymbol{C}(t - T_s)$
Calculate $\underline{\boldsymbol{v}}(t) = \boldsymbol{C}(t)\underline{\boldsymbol{u}}$
Calculate $\underline{\boldsymbol{v}}_{Diff}(t) = \boldsymbol{C}_{Diff}(t)\underline{\boldsymbol{u}}$
Feature Extraction from $\underline{\boldsymbol{v}}(t)$
Feature Extraction from $\underline{\boldsymbol{v}}_{Diff}(t)$
kNN Classifier
Attack
no
Declare No Attack at instant t
Yes
Attack Locator
$t = t + T_s$

Figure 3.16: Flow chart of stress detection at time instant t.

3.4.4 Computational Complexity

The complexity for computing the instantaneous correlation matrix, $\boldsymbol{C}(t)$ is $O(2n_{\text{Corr}} \times \frac{N(N+1)}{2}) \approx O(N^2.n_{\text{Corr}})$, where, n_{Corr} is the number of samples within the correlation window $[t - t_c, t]$. Since n_{Corr} is kept constant the complexity of calculating $\boldsymbol{C}(t)$ is considered as $O(N^2)$ relative to the size of the system N. The complexity for computing the difference correlation matrix $\boldsymbol{C}_{\text{Diff}}(t)$, aggregated correlation matrix, $\underline{\mathbf{v}}(t)$, and aggregated differences correlation matrix, $\underline{\mathbf{v}}_{Diff}(t)$, are also $O(N^2)$ since they involve accessing all the elements of $\boldsymbol{C}(t)$. In the feature extraction level, the computations involve sorting the elements and calculating simple statistical parameters of $\underline{\mathbf{v}}(t)$, therefore the complexity is in the order of $O(Nlog(N))$ (as $\underline{\mathbf{v}}(t)$ is a vector of size N). The complexity of $k-$NN by brute force method is $O(n_{\text{Train}} \times n_{\text{Features}}) = O(n_{\text{Train}} \times 16) \approx O(n_{\text{Train}})$. However, the complexity of the $k-$NN method can be reduced up to $O(log(n_{\text{Train}}))$ [88]. In summary, the complexity of the proposed detecting and locating method is: $\max\{O(N^2), O(log(n_{\text{Train}}))\}$. For smaller grids, the computational load is dominated by the number of training samples whereas in large grids by the size of the grids. However, since in larger grids, the computational complexity is higher, the presented method would be more effective with computation by grid partitioning or optimal placement of PMUs.

3.4.5 Simulation and Results

3.4.5.1 Generating State Attribute Time Series

In this work, the power system simulations are based on MATPOWER 6.0, a package of MATLAB M-files [24]. A simulated PMU time series has been generated using the steady-state power flow calculations using MATPOWER based on time-varying loads. The process of generating data is quasi-static in the sense that the dynamic models for the generators in the power system have not been used; instead, the dynamicity is associated with the load variations. The load patterns collected from the daily load data of the New York Independent System Operator (NYISO) [25] have been used to generate time-varying loads for this quasi-static simulation. There are eleven regions in NYISO and for each of the regions, we have the time-varying day-long load data. Since in IEEE 118 bus system we have 91 load buses, we synthetically create $\binom{11}{3} = 165$ day-long load data by taking averages of the combinations of three load data similar to [89]. From these 165 load profiles, we consider the first 91 load data for the 91-load buses of the IEEE 118 bus system. The load profiles are then normalized within 0 to 1 and added to the default constant loads of the MATPOWER 118 bus case. The generations and the power factors are adjusted accordingly to ensure the convergence of the power flow solution for normal cases. The load data in the NYISO are recorded every five minutes. This time series is interpolated to increase the sampling rate to 0.33 samples/sec. However, in this process, the sampling rate can be further increased depending on the computational resources. Single-line failures are also simulated and their effects are collected in the corresponding time series. Moreover, the effects of various cyber-attacks are reflected in the time series using the models discussed in Section 3.2.2.

For the cyber-attacks, 10,000 scenarios have been simulated for the performance evaluation. Among these scenarios, some of them contain cyber-attacks of a certain kind and other scenarios do not contain any attack and are for the system under normal conditions. If the scenario contains an attack, then the type of cyber-attack (i.e. DoS attack, data-replay attack, or ramp attack) and the number of attacks are selected randomly. After that, the location of the attack is also selected randomly from all the buses with uniform probability. The time for the launching of the attack is also selected randomly among all possible time instants throughout the day with uniform probability.

For the performance evaluation in the case of a single line tripping, 1,000 scenarios were created with tripping and no-tripping cases similar to the scenarios for cyber stresses. The lines to be tripped are selected randomly from the 186 branches of the IEEE 118 bus system with uniform probabilities.

3.4.5.2 Detection and Locating Performance

Here, the voltage angles associated with buses are considered state variables. We have calculated the instantaneous correlation matrix using the equation (3.1). The correlation window, t_c is selected as 0.25 minutes.

As described previously, we use $k-$NN classification and choose $k = 5$ to detect stresses in real time. Simulation shows that the detection performance is not very sensitive to the values of k. (Figure 3.17). In fact, for physical stresses, the detection performance remains constant after $k = 20$. Randomly generated 10,000 instances in different locations and at different times throughout the day have been used in the training of the $k-$NN model by extracting features from the instances. The Performance of the model is validated by 10-fold cross-validation.

Table 3.2: Performance Evaluation of the k-NN Analysis of Instantaneous Correlation Matrix Technique.

Stress Type	**True Positive Rate**	**False Positive Rate**	**Exact Locating Rate**	**Location within 2-hop Distance**	**Location within 3-hop Distance**
Cyber-Attack (k−NN)	0.86	0.13	0.85	-	-
Cyber-Attack (DT)	0.85	0.13	0.85	-	-
Line Failure (k−NN)	0.94	0.05	0.38	0.71	0.81
Line Failure (DT)	0.93	0.04	0.38	0.71	0.81

The accuracies of the presented methods for cyber and physical stresses have been studied, separately. We apply the classification method to all 10,000 scenarios (scenarios with cyber-attack or no attack) to determine if a cyber-attack has occurred in the system or not (if the scenario does not contain any attack, a random time instant is still selected at which the proposed method runs to detect whether there is an attack). The statistics of the performance of the method (i.e., True Positive Rate (TPR), False Positive Rate (FPR), and Exact Locating Rate) are calculated and presented in Table 3.2. The work by Shi *et. al.* [79], which uses spatio-temporal correlation for detection shows a detection rate of 85% and a false-positive rate of 16.04%. Although the exact comparison of these methods is challenging due to the differences in detection parameters, test cases, measurement data, and stress models, these methods show comparable performances. Besides, the proposed method can perform well for the ramp attack, which is a challenging detection problem [81]. Moreover, many existing works, including [68], only focus on the detection rate for the performance evaluation of their proposed methods [78], while the false-positive rate is usually overlooked. One of the key advantages of the proposed method is achieving a good detection rate while keeping the false positive rate low.

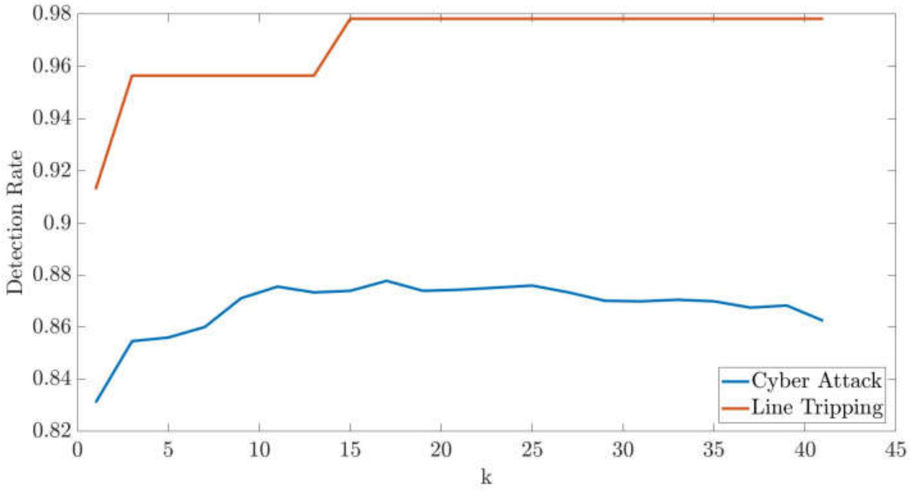


Figure 3.17: The effect k in the k-NN method on detection rate.

In the case of physical line failure, we have applied the method to the $1,000$ scenarios with one line failure and no failures. In general, identifying the exact location of the line failure is more difficult compared to cyber stresses. As such, to evaluate the performance of the locating process, in addition to the exact location, we consider a two-topology-hop vicinity of the failed line and calculate the rate of locating within this vicinity. The statistics of the performance of the method for physical failure are shown in Table 3.2 based on TPR, FPR, Exact Locating Rate, and Locating within $2-$Hop and $3-$Hop Distance Rates.

The $k-$NN method for classification is simple in implementation and robust to linearly non-separable classes. Moreover, $k-$NN facilitates easy insertion of new instances into the training set that enables updating the training instances regularly with the changing situations of the grids. This advantage makes the arrangement robust to the long-term grid dynamics. The conducted simulation shows that similar performance can be achieved by the decision tree method taking twice as much time as the $k-$NN method (Table 3.2).

Chapter 4: Detection and Location Identification of Cyber and Physical Stresses in the Smart Grid: Part II: GSP Approach

[3]The availability of large volumes 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 work, a Graph Signal Processing (GSP) framework [4, 5] has been exploited for the representation and analyses of smart grid data, particularly to support the monitoring function for their reliable and secure operation.

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 DoS attack [64], data-replay attack [86], ramp attack [81], and FDIA [64], 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 the 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,

[3] Portions of this chapter were published in IEEE Transactions on Smart Grid [26]. Copyright permissions from the publishers are included in Appendix B.

and abrupt load changes. In this work, 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 situational awareness toward cyber and physical stresses. To do so, in this work, properties and characteristics of graph signals associated with the power grid measurements (e.g., bus voltage angles) are analyzed in various GSP domains including the 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) [33] and the local smoothness (LS) [63] 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 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 changes of values at the onset are challenging to detect for many existing stress detection techniques. The performances of the proposed techniques are evaluated in comparison with the graph Fourier transform (GFT)-based detection technique [44, 22], 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) [81]. 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 work 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 to locating complex physical stresses.

- 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.

4.1 Related Works

Detection and determining the location of cyber attacks in the smart grid using GSP is a relatively new domain. In our work [31, 27], 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 [44] 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 false data is proposed to be detected based on the existence of significant high-frequency components. Moreover, in [44], the authors proposed locating FDIA using graph modulation. In the work by Ramakrishna and Scaglione [90], the voltage phasor measurement model developed based on GSP is utilized to detect FDIA in smart grids. Anderson and Yu [91] 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 [92] 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 this chapter, 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.

4.2 Stress Models

4.2.1 Cyber Attack Models

The cyber attack models used in this work are the same models described in 2.3.1.

4.2.2 Physical Stress Model

In this work, the abrupt change in the demand at a single bus is considered as 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 demand can represent abnormal conditions since they can hamper the reliability of the grid. In this work, 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

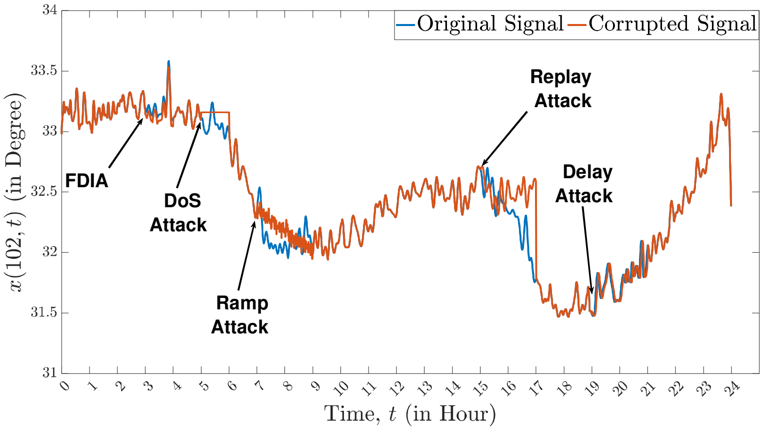


Figure 4.1: Cyber attacks on time-series according to 2.3.1.

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 the 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 work 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 [93] and are out of the scope of this work and important for future studies.

4.3 GSP-based Detection and Localization

A detailed review of GSP fundamentals in the power system context can be found in Chapter 2, Section 2.2. In the current section, the GFT-based technique for detecting stresses as presented in [44, 22] has been reviewed. Then, two new techniques have been proposed for analyzing the power grid's measurements for detecting and locating stresses based on VFED and LS of graph signals.

4.3.1 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 Figure 4.2 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:

$$\gamma(t) = \sum_k |\hat{X}(\hat{\lambda}_k, t) H(\hat{\lambda}_k)|, \tag{4.1}$$

where $H(\lambda)$ is a high-pass graph filter expressed by the following frequency response: $H(\lambda) = 0, \text{ if } \lambda \leq \lambda_c$ and $H(\lambda) = 1, \text{ if } \lambda > \lambda_c$, where λ_c is the cut-off graph-frequency. For detecting cyber and physical stresses, the probability distribution of γ, $p_\gamma(\zeta)$, has been estimated 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.

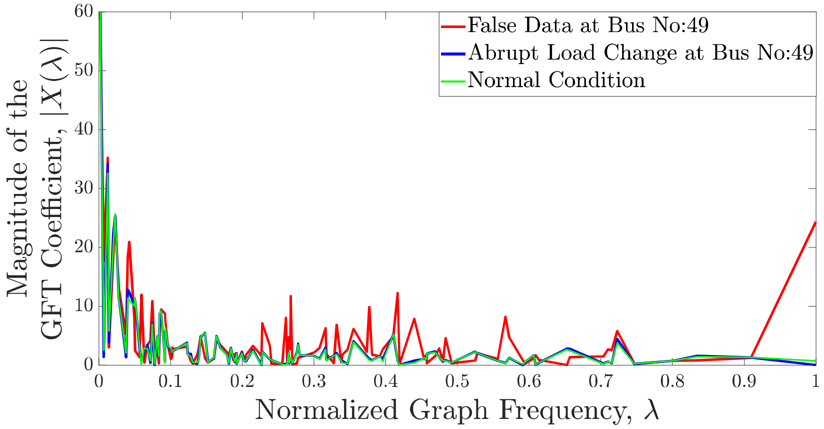


Figure 4.2: GFT magnitude response for IEEE 118 bus system: emphasized high graph-frequency components can be observed in case of false data injection.

4.3.2 Detecting and Locating Stresses Using VFED

Containing the topological and 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 [33], 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 conditions) 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. Figure 4.3 illustrates normalized $\eta(n, t_{start})$ in the case of an FDIA at vertex 86 of the 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 2.3.1. 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.

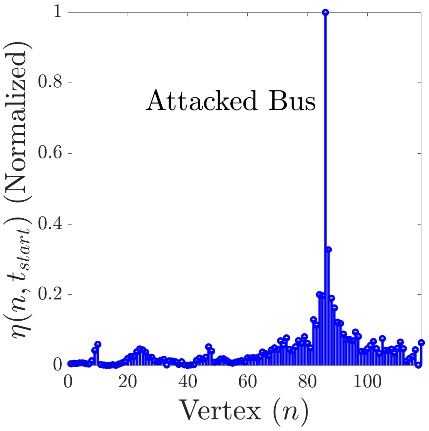
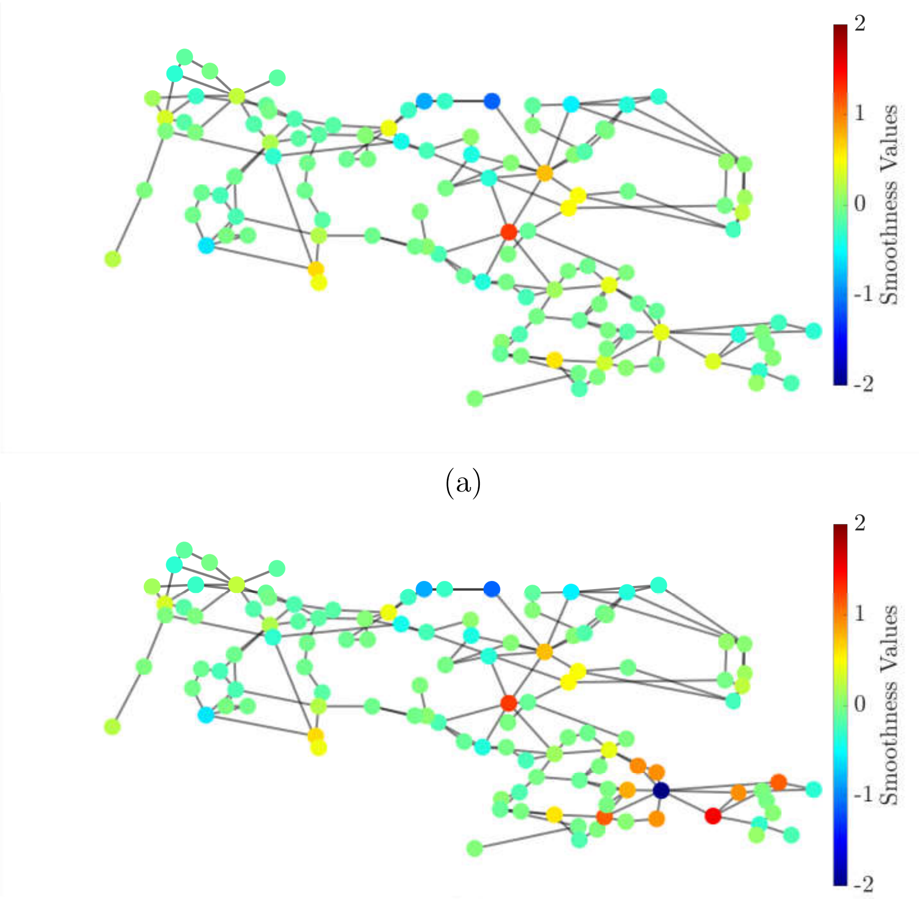


Figure 4.3: Normalised $\eta(n, t_{start})$ (between 0 to 1). For $n = 86$, the largest value is obtained which indicates stress at the vertex (bus) 86.

4.3.3 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 2.3.1. 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 2.2.5, 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. Figure 4.4 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 (Figure 4.4(a)) as well as under DoS attack at bus number 100 (Figure 4.4(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).

To this end, the *local smoothness second time-derivative (LSSTD)* method has been proposed 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 $s''(n, t)$ differentiates 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 work, 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



(a)

(b)

Figure 4.4: Local smoothness of the vertices of the IEEE 118 bus system: (a) at normal condition, (b) during DoS attack at bus 100.

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 [94]) that arise from changes in generations, load demands, and control parameters.

4.4 Performance Evaluation

4.4.1 Simulating Stress Scenarios

For evaluating the performance of our proposed detecting and locating techniques, the IEEE 118 bus system [62] has been considered and simulated using MATPOWER 6.0 [24]. For generating time series associated with the graph vertices, the time-varying load patterns from the New York Independent System Operator (NYISO) [25] have been added with the default MATPOWER loads as in [95]. 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 2.3.1. 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 number 69 in IEEE 118 bus system) is excluded from the consideration of being a location of cyber stress. For FDIA, range of $x' = 0.02$ to 3 for voltage angle 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 normal scenarios, 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

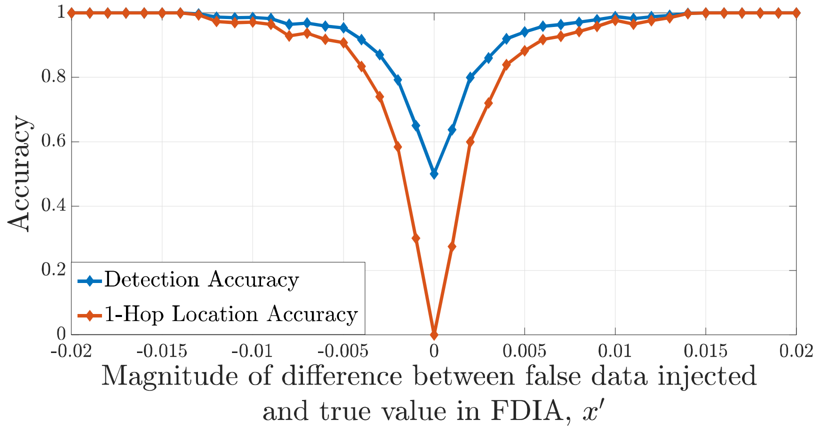


Figure 4.5: Performance sensitivity to the magnitude of difference between false data injected and true value in FDIA x'.

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.

4.4.2 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 work, we have

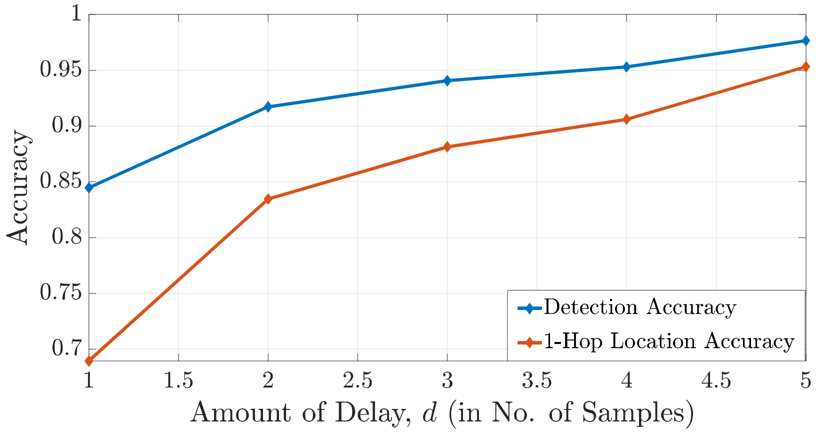


Figure 4.6: Performance sensitivity to delay, d in delay attack.

considered $K = 1$ and $K = 2$ and denote the corresponding performance metric by LA_{1-hop} and LA_{2-hop}, respectively.

4.4.3 Analyses of the Results

Table 4.1 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, the detection threshold has been chosen 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 4.1 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 Figure 4.5. 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 (Figure 4.6. 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

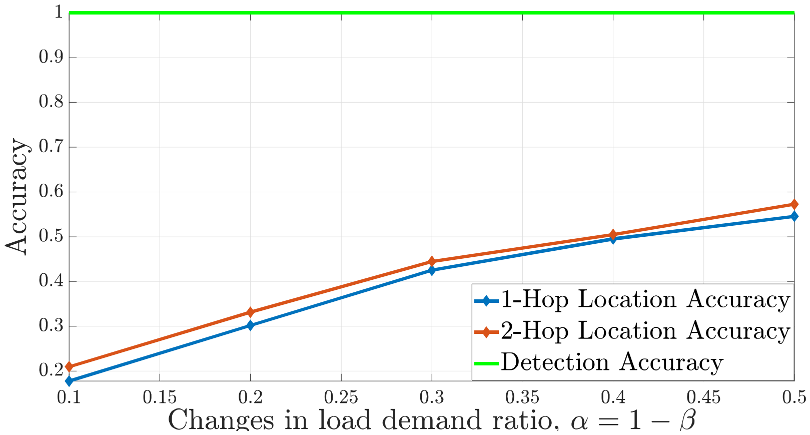


Figure 4.7: Performance sensitivity to changes in load demand ratio, α.

Table 4.1: 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.4.5]	0.993	0.634	0.988
Delay Attack ($d = 2$ samples) [See Fig.4.6]	0.989	0.628	0.994
Load Change ($\beta = 0.6$)[See Fig.4.7]	1.00	0.609	0.778

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, and 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. Figure 4.7 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 $\beta = 0.5, 0.6, 0.7, 0.8, 0.9$.

4.4.4 Comparison with Existing Methods

4.4.4.1 Candidate Techniques for Comparison

In this work, the performance of the proposed techniques is compared with other GSP- and non-GSP-based techniques. In the GSP-based category, the GFT-based detection technique [22, 44] (reviewed in Section 4.3.1) 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) [81] 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 4.2, 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,

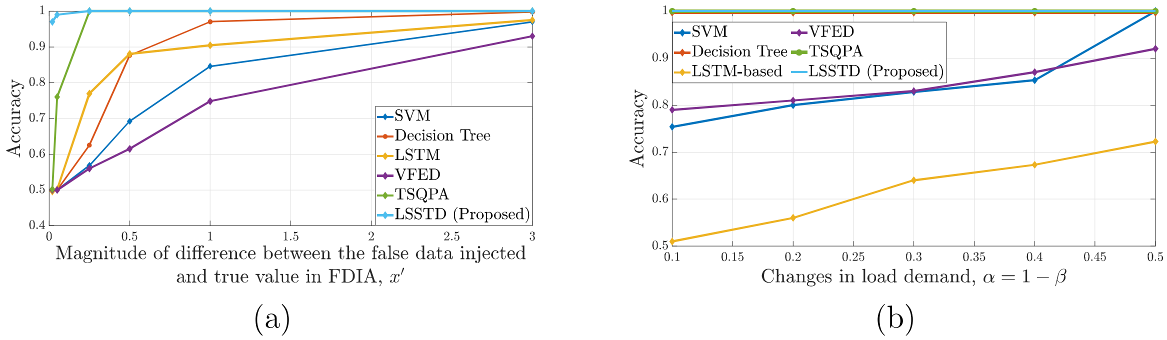


Figure 4.8: Comparison among the detection accuracy of different methods for various (a) FDIA attack intensity, x' (b) abrupt load changing factor $\alpha = 1 - \beta$.

for ensuring the fairness of comparison among the detection methods the model is trained using the same dataset used by other methods.

4.4.4.2 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 Figure 4.8. 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, 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 [31] and [44], 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 Figure 4.2. 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 Figure 4.8(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 Figure 4.8, 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 Figure 4.8(b). The VFED method is based on the joint-vertex frequency distribution of the graph 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

2.6 implicitly introduces some smoothing effect and therefore, loses specificity to detect the small amount of changes in the signal. From Figure 4.8, 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 $x' < 0.25$.

4.4.4.3 Performance of Location Accuracy

Since all the aforementioned methods are not equipped with the ability to locate the stresses, 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 $\alpha = 0.1$).

4.4.4.4 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 work 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 track the time evolution of data by a quadratic function; however, it cannot capture the interrelation among the time-series at different buses. The 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.

4.4.5 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 the LSSTD detection algorithm is $\mathcal{O}(N^2)$, where N is the number of buses in the grid. For the VFED technique, equation (2.6) 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 the VFED technique can lead to new developments with better computational complexity or the 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 stress is detected by the LSSTD technique.

Chapter 5: Classification and Characterization of Cyber and Physical Stresses in the Smart Grid Using Graph Signal Learning

[4]Once a stress is detected and located in the system, the next step would be to identify the type and characteristics of the occurred stress in order to implement effective corrective measures to mitigate the stress and also plan for preventive measures in the future. The key contributions of this chapter are summarized as:

- A two-stage classification framework for the power system stresses has been proposed based on the 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. The classification performances have been evaluated across various ML classifiers using data under different noise levels.
- Various GSP-based features of time-varying voltage angle graph signals at different classification stages are evaluated.
- A neural network-based technique for the classification of multiple random cyber attacks and clustered/coordinated cyber-attacks has been proposed using features extracted by GSP-based analysis.
- Techniques for estimating attack center and radius in case of clustered multiple cyber attacks have been proposed.

[4] Portions of this chapter were published in IEEE Xplore [29, 30]. Copyright permissions from the publishers are included in Appendix B.

- A technique for reducing the dimensionality of the GSP-based features based on down-sampling in the graph-frequency domain is proposed.

5.1 Related Works

Among the studies of stress classification in the smart grid, the classification of physical stresses (or events) using ML techniques has been extensively studied [96, 12, 97, 98, 99]. For instance, Rafferty and Liu, [98], 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 [98], the frequency, phase angle, voltage magnitude, and their time derivatives are considered as the features and their relative importance is studied. Liu *et al.* [99] present a detailed analysis of the classification of four types of power system events including frequency events, line outages, transformer outages, 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 [13], along with the physical stresses (e.g., line fault and generation loss), fake events created by false data injection are also considered for classification. Yuan *et al.* [100] also propose a GNN-based event classification technique in which the latent interaction graphs among different PMUs are learned from the PMU data.

5.2 Problem Formulations

5.2.1 Classification Problem Formulation

5.2.1.1 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 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 the 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, $x : \mathcal{V} \to \mathbb{R}$ that, in this work, represents the value of the voltage angle at bus $n \in \mathcal{V}$ at time t. A more detailed discussion about the GSP basics, especially in the power system context can be obtained in Section 2.2.

5.2.1.2 Classification Models

In this chapter, two types of stress classification models have been presented. In the first model [30], a two-stage stress classification framework has been proposed. When any stress is detected in the grid at time t_d, the first step is to determine whether it is 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. Here, 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 of the model of these stresses and their characteristics can be found in 2.3.1.

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:

$$\mathbf{y} = f(\mathbf{\Psi}(x(n,t))), \quad t_d \leq t \leq t_d + \Delta t_w, \tag{5.1}$$

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:

$$\mathbf{z_p} = g(\mathbf{\Psi_p}(x(n,t))), \quad t_d \leq t \leq t_d + \Delta t_w, \tag{5.2}$$

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. A similar formulation can be shown for stresses that are classified as cyber attacks in the first stage:

$$\mathbf{z_c} = h(\mathbf{\Psi_c}(x(n,t))), \quad t_d \leq t \leq t_d + \Delta t_w, \tag{5.3}$$

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.

The second classification model [29] is relevant after characterizing a cyber attack as a simultaneous-cyber-attacks launched at multiple locations. This model classifies clustered cyber attacks and random multiple cyber attacks. Based on the discussions in Section 2.4, it can be concluded that single random attacks, multiple random attacks, and clustered cyber attacks have distinctive signatures in the pattern of local smoothness values at the time of detecting the attack, t_d. However, under the load change at different buses, the voltage angle graph signals and thereby the local smoothness values associated with the signals vary in time. As a result, rule-based decision-making from the signatures of multiple random cyber attacks and clustered cyber attacks becomes difficult. Therefore, a neural network-based classification has been proposed between the two types of attacks.

5.2.2 Characterization of Cyber Attacks

5.2.2.1 Determining the Number of Cyber Attacks

In this approach, the probability distributions of the second time derivative of the local smoothness values associated with the voltage angle measurements of each bus $p_{s''_n}(\zeta)$ are estimated from the past data. If the likelihood of the second time-derivative of the local smoothness value at any time instant at bus/vertex n falls below the threshold $\theta_{s''_n}$ (i.e., $p_{s''_n}(s''(n,t)) < \theta_{s''_n}$), cyber stress is declared at bus n at that time. The time instant at which the attack is detected is denoted as t_d.

5.2.2.2 Determining Attack Center and Attack Radius in Clustered Cyber Attacks

After the identification of a cyber attack as a clustered one, it is crucial to determine the center of the attack and the attack radius to enhance situational awareness and mitigate the effect of the attack. In this work, the goal is to identify the center of the attack, n_C, and the attack radius, K to help with situational awareness.

Once the center of the attack, n_C, is detected, the radius, K of the attack can be estimated using the fact that a clustered attack of radius K, affects the local smoothness values of the vertices within the $K+1$ neighborhood of the attack center. The radius K can be specified as:

$$K = \max\{\mathbb{D}(n_C, n_P)\} - 1, \quad \forall n_P \in \mathcal{V} \tag{5.4}$$

such that:

$$p_{s''_{n_P}}(s''(n_P, t_d)) < \theta_{s''_{n_P}}, \tag{5.5}$$

$\mathbb{D}(n_1, n_2)$ is the hop-distance between the vertices n_1 and n_2, within the graph, $\mathcal{G}$.

5.3 Feature Extraction Using GSP

5.3.1 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 works [27, 26] and our extensive simulations on the IEEE 118 bus case [62], it is observed that in different cyber and physical stresses, different sets 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 technique for reducing the number of features of the same type has also been proposed.

5.3.1.1 Features Extracted from the Moment of Detection, t_d

- Real-number Features: 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 on 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 the 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.

- Combination of Real-valued Binary Features: This set of features is especially useful for the second type of classification between clustered and random multiple cyber attacks. A total of $N+1$ input features, $f_1, f_2, \ldots f_{N+1}$, are considered for the deep learning model. Among them, the first N features are binary, indicating whether the likelihood of the second time-derivative of the local smoothness value of a particular bus at the detection instant is less than a predefined threshold $\theta_{s''_n}$ (i.e., $f_i = 1$ if $p_{s''_n}(s''(n, t_d)) < \theta_{s''_n}$ and 0 otherwise, for $i = 1, 2, \ldots N$). The last feature, f_{N+1}, is a real-valued feature representing the global smoothness of the graph signal, $x(n, t_d)$, which is expressed as $\frac{\underline{\mathbf{x}}^T(n,t_d)\mathbf{L}\underline{\mathbf{x}}(n,t_d)}{\underline{\mathbf{x}}^T(n,t_d)\underline{\mathbf{x}}(n,t_d)}$.

5.3.1.2 *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 vector 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:

$$\psi_2(l) = \sum_{n=1}^{N} \mathcal{T}(\frac{d}{dt}x(n, t))u^*_{l_t}(n), \quad \text{for} \quad t_d \leq t \leq t_d + \Delta t_w \tag{5.6}$$

Here, $\mathcal{T}(.)$ signifies the 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 types of features are suitable for classifying cyber attacks with distinguishable temporal signatures on the time series data.

5.3.1.3 Features Extracted by Taking Temporal Statistics of the Time-Varying GFT Values

The features of the third type involve 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:

$$\psi_3(l) = \mathcal{T}(X(\lambda_{l_t}, t)), \quad \text{for} \quad t_d \leq t \leq t_d + \Delta t_w, \tag{5.7}$$

Similar, to the previous type of features, features of this type also contain both temporal and interconnection information and are therefore applicable to the classification of cyber attacks.

5.3.2 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 of 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.

5.4 Simulation Details

5.4.1 Two-stage Classification

In this work, all the simulations have been performed on the IEEE 118 bus systems, using MATPOWER [24]. The load patterns are extracted from the actual daily load profile from New York Independent Operator (NYISO) [25] and have been added to the default MATPOWER load demands to create time series data as described in [95]. 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 [26] 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.

Among different machine learning classifiers, decision trees, discriminant analysis, an ensemble method, support vector machine (SVM) with linear and radial basis function (RBF) kernels, and neural networks 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.

5.4.2 Characterization

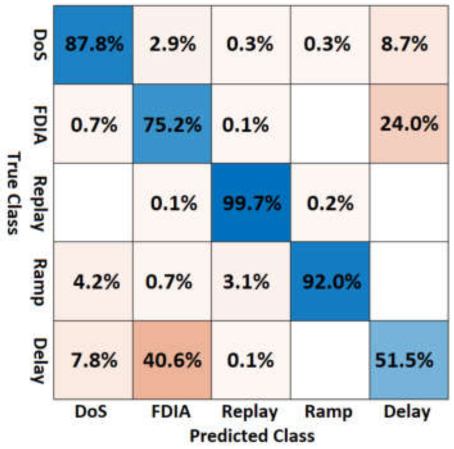
The analyses and the proposed techniques described previously have been evaluated using simulations on the IEEE 118 bus system [62]. The power flow calculations are performed in *MATPOWER 6.0* [24]. The time-varying bus voltage angle signals are simulated by introducing time-varying load demand. The patterns of the time variation of load demand throughout the day have been collected from the New York Independent System Operator (NYISO) [25] and applied as described in [26]. Different types of cyber attacks are created according to the attack model as described in [26]. A detailed description of each experiment and its performances have been presented in the following subsections.

For the classification between multiple random and clustered cyber attacks, the performance is evaluated separately for each of the five types (i.e., DoS, FDIA, data-replay, ramp, and delay attacks) of attacks as well as for different levels of attack intensities. For each case, a data set was created with 10,000 scenarios. Whether a scenario corresponds to multiple random cyber attacks or clustered cyber attacks is chosen randomly with equal probabilities. For the multiple random attacks (e.g. p number of attacks), the attack locations (p locations) are chosen from the 118 buses, with uniform probabilities for all the buses. In the case of the clustered cyber attack, the attack center (n_C) is chosen randomly from the 118 buses with equal probabilities. The deep learning model for the classification between the random and the clustered attack consists of 3 hidden dense layers with 256, 128, and 32 neurons, respectively. With the binary cross-entropy loss function, ADAM optimizer, and an initial learning rate of 0.5 which decreases at a rate of 0.5 exponent of the time step. The model has been trained and tested in *Sci-kit learn* [101] with 10-fold cross-validation.

5.5 Performance Evaluation

5.5.1 Performance of the Two-stage 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. Figure 5.2 illustrates the classification accuracy of the different machine learning classification algorithms for the first-stage binary classification between cyber and physical stresses using raw voltage angle data and using GSP-based features. Two different candidate feature



	DoS	FDIA	Replay	Ramp	Delay
DoS	87.8%	2.9%	0.3%	0.3%	8.7%
FDIA	0.7%	75.2%	0.1%		24.0%
Replay		0.1%	99.7%	0.2%	
Ramp	4.2%	0.7%	3.1%	92.0%	
Delay	7.8%	40.6%	0.1%		51.5%

Figure 5.1: Confusion matrix for cyber attack classification using GSL method. A neural network classifier has been used as the ML classifier.

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 45dB. 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 levels, while the performance of the local smoothness-based ones deteriorates significantly with increasing noise levels, 2) the dimensionality reduction method discussed in Section 5.3.2 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, $\mathcal{T}(.)$

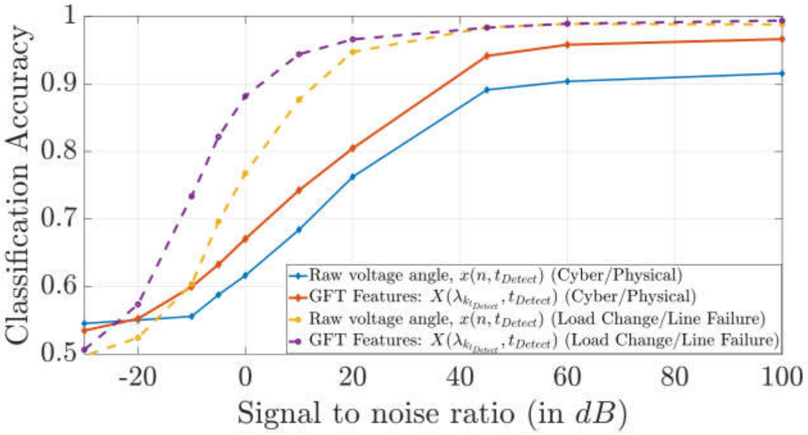


Figure 5.2: Dependency of the classification performance on the noise level of the data. The decision tree classifier has been used for all the cases.

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 $t_d \leq t \leq t_d + \Delta t_w$. Figure 5.1 presents the confusion matrix for the classification of cyber attacks. The GSL-based classification technique classifies the cyber attacks with good accuracy except for the relatively higher mis-classification rates between the FDIA and the delay attack.

5.5.1.1 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 Figure 5.2, 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 [26].

5.5.1.2 Classification Performance with a Reduced Number of Features

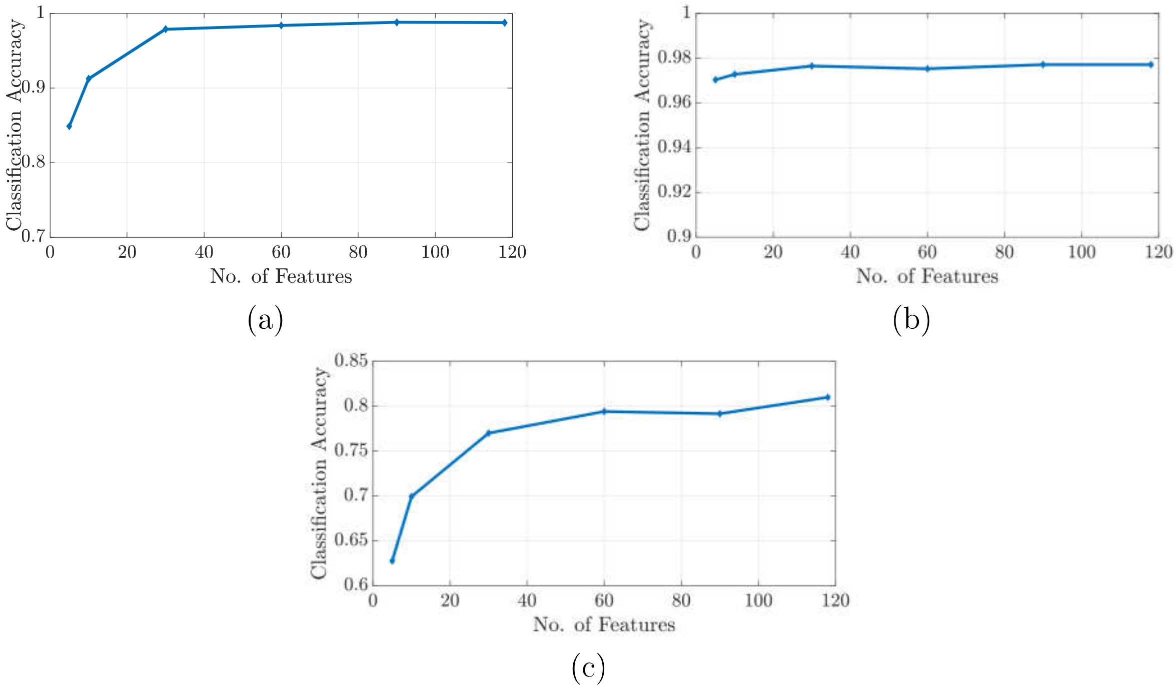


Figure 5.3: Classification performance with reduced numbers of features (by graph-frequency domain down-sampling). Results for: (a) cyber vs. physical stress classification, (b) among physical stresses classification, (c) among cyber stresses classification. The decision tree classifier has been used as the ML-based classifier for all the cases.

Figure 5.3 illustrates the classification performance with the reduced number of GFT-based features as suggested in Section 5.3.2. 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 of 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 5.5.1.

5.5.2 Classification Performance for Multiple Random Vs. Clustered Cyber Attacks

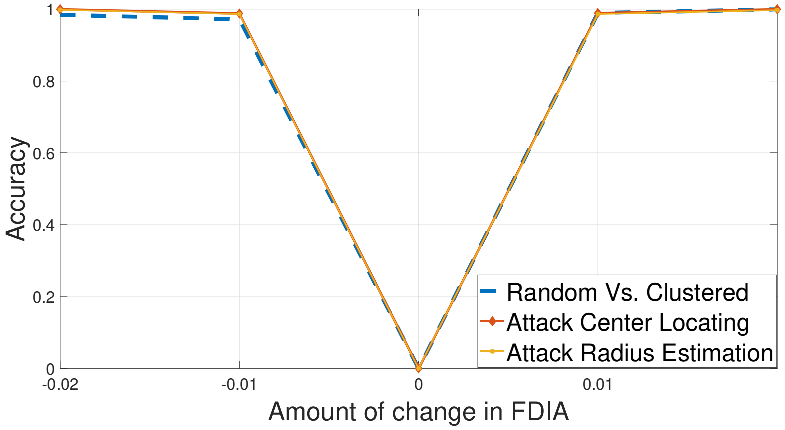


Figure 5.4: Dependence of accuracies on attack intensities for FDIA.

For the classification between multiple random and clustered cyber attacks, the performance is evaluated separately for each of the five types (i.e., DoS, FDIA, data-replay, ramp, and delay attacks) of attacks as well as for different levels of attack intensities. For each case, a data set had been created with 10,000 scenarios. Whether a scenario corresponds to multiple random cyber attacks or clustered cyber attacks is chosen randomly with equal probabilities. For the multiple random attacks (e.g. p number of attacks), the attack locations (p locations) are chosen from the 118 buses, with uniform probabilities for all the buses. In the case of the clustered cyber attack, the attack center (n_C) is chosen randomly from the 118 buses with equal probabilities.

The deep learning model for the classification between the random and the clustered attack consists of 3 hidden dense layers with 256, 128, and 32 neurons, respectively. With the binary cross-entropy loss function, ADAM optimizer, and an initial learning rate of 0.5 which decreases at a rate of 0.5 exponent of the time step. The model has been trained and tested in *Sci-kit learn* [101] with 10-fold cross-validation. The performance of the classification model

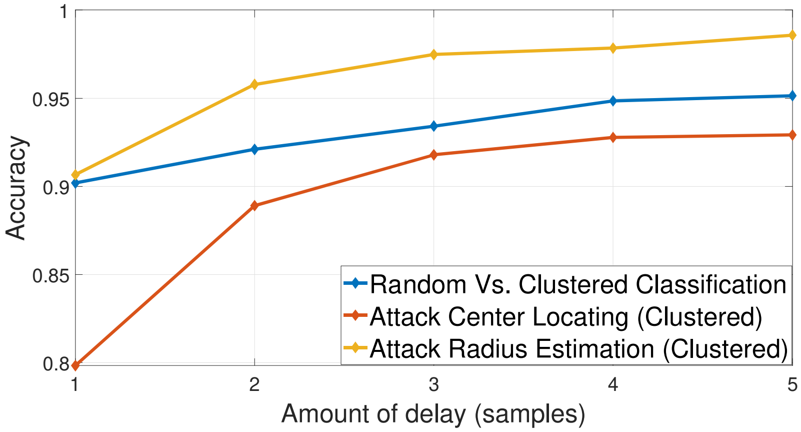


Figure 5.5: Dependence of accuracies on amount of delay in delay attack.

Table 5.1: Performance Evaluations of Random Vs. Clustered Multiple Cyber Attacks Classification, and Estimation of Attack Center and Radius.

Attack Type	Accuracy		
	Random Vs. Clustered Classification	Attack Center Locating (Clustered)	Attack Radius Estimation (Clustered)
DoS	0.851	0.886	0.978
Replay	0.922	0.883	0.955
FDIA	See Figure 5.4	See Figure 5.4	See Figure 5.4
Ramp	0.858	0.849	0.973
Delay	See Figure 5.5	See Figure 5.5	See Figure 5.5

for the sophistically designed cyber attacks described in equation (2.8) has been summarized in Table 5.1. The accuracy of the classification signifies the rate of classifying between the random attack and clustered attack correctly. Since the performance in the case of the FDIA and the delay attack is dependent on the attack intensities, their performances are illustrated separately in Figure 5.4 and Figure 5.5, respectively showing the variation with the amount of change in FDIA, x' and amount of delay (in samples) in delay attack.

5.5.3 Determining n_C and K in Clustered Cyber Attacks

For the determination of the attack center, n_C, and the attack radius K in case of clustered cyber attack, 10,000 clustered cyber attack scenarios have been considered. In each scenario, the attack center, n_C, has been chosen from the 118 buses, and the attack radius, K has been chosen from $\{1, 2, 3, 4\}$, with equal probability. Five of the nearest neighbors are considered in the $k-$NN method for the classification for determining the attack center. Performances are summarized in Table 5.1, Figure 5.4, and Figure 5.5. The accuracy of determining the attack center and the attack radius imply the rates of correctly determining the location of the central bus of the clustered attack and the radius of the attack.

Chapter 6: Recovery of Missing States and Optimum Meter Placement in Smart Grid Using Correlation of States and Graph Signal Sampling

[5]The state estimation in smart grids [103] is an essential function, which enables their secure and reliable monitoring and operation. However, this critical function is vulnerable to various forms of cyber attacks (e.g., DoS attacks and FDIA). These attacks can hamper the availability and integrity of the system state information. Once a cyber attack is detected and located in the system, the recovery of the state information at the attacked locations becomes crucial to mitigate their effects.

In this chapter, the state recovery problem has been proposed to be solved by both the GSP-based approaches and the correlation-based approaches. Under the GSP-based approach, the two techniques for state recovery have been proposed. The first approach involves modeling the state recovery problem in smart grids through a graph signal reconstruction framework [104, 105]. The graph signal sampling-reconstruction framework is effective for the recovery of unobservable signal values of the graph signals band-limited to a certain graph-frequency. The second GSP-based approach is based on the local and global smoothness of the graph signal which relaxes the band-limited assumption of the signal. This chapter also proposes a technique to estimate the time-varying unobservable states of the smart grid from the time-varying observable states by utilizing the correlations among the states.

The main contribution of this chapter is:

- The state recovery problem when the buses become unobservable due to, for instance, cyber attacks (e.g., DoS), failure of the communication link, or the physical failure of

[5] Portions of this chapter were published in IEEE Xplore [95, 28, 102]. Copyright permissions from the publishers are included in Appendix B.

the PMU has been proposed to be solved under graph signal sampling framework. The band-limitation assumption for the graph signal should be held. This problem can be fitted to a graph signal sampling-reconstruction framework by considering the buses that are not affected by the stress in the PMU network as the sampling vertices and the unobservable buses as the non-sampling vertices. Thus the measurements from the sampling set of buses can be used to recover the unobservable ones due to the stress.

- The above solution has been extended to relax the band-limited graph signal assumption. A novel reconstruction technique based on the statistics of the local smoothness of the graph signals along with the global smoothness of the graph signals is cast into an optimization framework. In contrast to many graph signal reconstruction techniques, which assume band-limited signals to be recovered, the proposed technique is applicable to general graph signals irrespective of their bandwidth.

- The optimal PMU placement problem has been discussed and formulated as a sampling set selection problem in a graph signal sampling framework. To solve the optimization, a heuristic approach based on the anti-aliasing filter error-based selection criterion is proposed and evaluated.

- Considering the continuous data stream associated with the bus voltage angles as time series, a state correlation-based technique has been proposed to recover the time-varying unobservable states using the observable states for a duration of time after the onset of unobservability. By applying this technique, the state of the power system can be estimated under various levels of unobservability with good accuracy. The estimation accuracy in terms of the mean squared error (MSE) has been used to identify the relative vulnerability of the buses (or PMUs) of the grid and the most vulnerable time for the unobservability.

6.1 Related Work

Over the last decade, with the emergence of GSP as a promising field of research, the reconstruction of graph signals is getting attention from researchers. The topic is often studied in the context of the non-uniform sampling of the graph signal, [106, 67], and the reconstruction method involves the eigenvector decomposition of the graph shift operators. In this connection, a large number of works on the graph signal reconstruction are dependent on the band-limited assumption of the graph signal. For example, Tanaka *et al.* [107] provides a detailed discussion on the theory and application of graph signal sampling from a graph-frequency domain perspective in which the reconstruction process relies on the bandwidth of the graph signals. Narang and Ortega [66] showed that the spectral domain interpretation for the sampling on *k-regular bipartite graphs* is analogous to the Nyquist criterion for down-sampling of classical discrete-time signals. Although this paper considers only a special kind of simple graph structure, the results are important for the understanding of graph signal sampling in general. Anis *et al.* [108] introduced the concept of *uniqueness set* to interpret the graph signal counterpart of the Nyquist theorem for arbitrary graphs and proposed a graph-spectral domain approach for the selection of the optimal sampling-set for graph signal sampling and reconstruction. Gadde and Ortega [109] presented a probabilistic interpretation for graph signal sampling. In [67], Chen *et al.* proposed a sampling theory for band-limited finite-length graph signals, which ensures perfect reconstruction without any probability constraints. In the subsequent works [110, 111, 112], the authors presented extensive analyses on various aspects of graph signal sampling including comparison among various selection criteria of sampling-set, different techniques of signal recovery, and theoretical aspects of the graph signal sampling-reconstruction process. Lorenzo *et al.* [106] presented sampling on a randomly generated band-limited graph signal on the IEEE 118 bus [62] topology, and on an approximately band-limited signal of a road network topology and studied the effect of different sampling-set selections. Sakiyama *et al.* [113] applied graph signal sampling for placing sensors in a network.

The concept of band-limited assumption is related to the global smoothness of the graph signal, and in the reconstruction literature minimizing the global smoothness to recover the missing signal values is widely known [114, 115, 67].

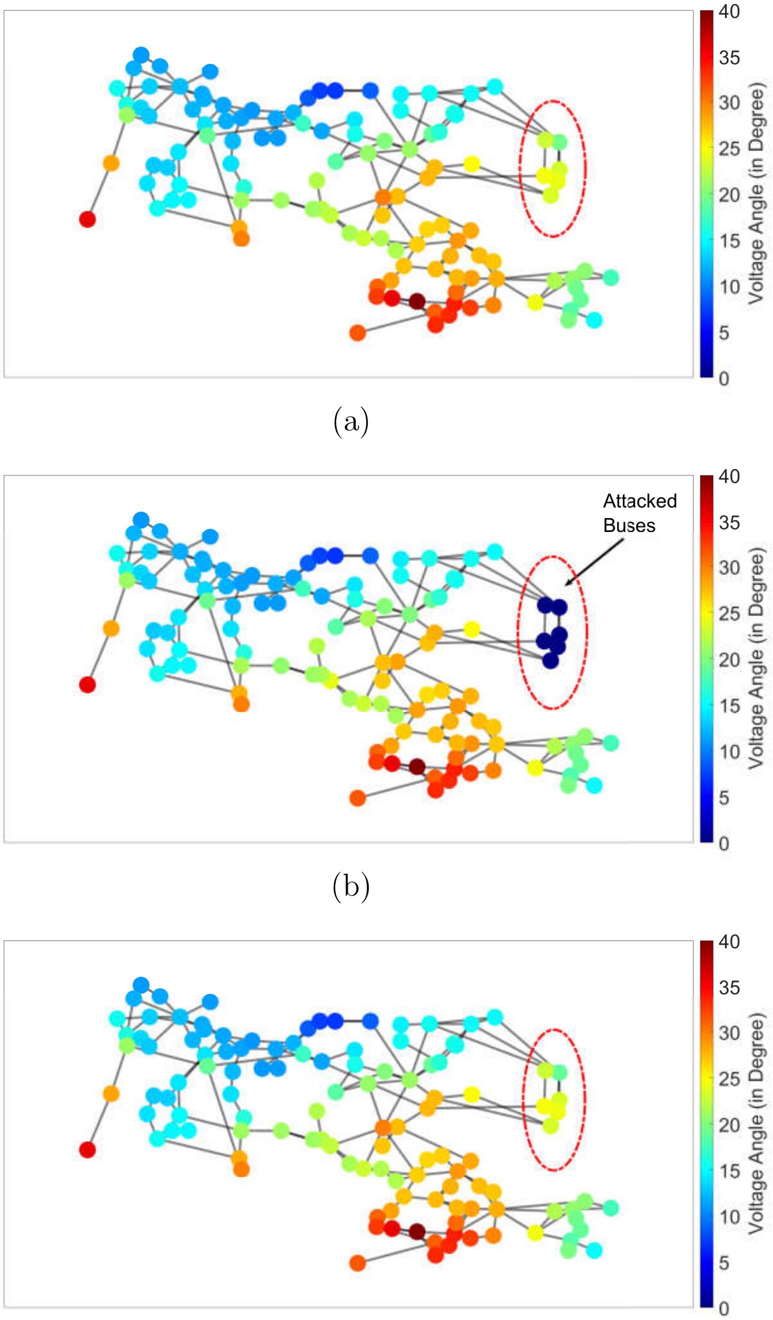
Among the other methods Isufi *et al.* [116] proposed reconstruction of the missing graph signal values using graph Wiener filter while the frequency response of the graph Wiener filter is approximated by ARMA graph filter and implemented distributively. Wang *et al.* [105] introduces the concepts of *local set* in connection with the frame theory and proposed two local set-based iterative graph signal reconstruction techniques. Mao and Gu [114] proposed a band-limited graph signal joint detection and reconstruction technique by using mixed integer linear programming. Romero *et al.* [117] proposes a kernel-based method for band-limited graph signal reconstruction.

6.2 State Recovery Using Graph Signal Sampling

Graph signal reconstruction has been an active research area in the GSP [4] domain with vast potential applications. The goal of the graph signal reconstruction is to estimate the signal values corresponding to a subset of the vertices, which are unavailable due to the down-sampling of the original signal or missing measurements (for instance, due to cyber-attacks). The sampling of graph signals can be considered as taking values corresponding to a subset of the vertices in the graph signal. For graph signals, analogous concepts and relations to classical signal processing sampling theorems can be observed.

6.2.1 Problem Formulation

Let $\mathcal{A} \subset \mathcal{V}$ be the set of all buses under cyber-attack in the grid at time t_A. Our goal is to estimate the bus voltage angle of any bus $i \in \mathcal{A}$ at any time instant, t, for $t > t_A$ using the graph signal reconstruction technique discussed in the previous section. In the graph signal sampling-reconstruction framework, it is considered that the buses under cyber-attack as non-sampling vertices and the buses, which are not under cyber-attack, as the sampling vertices, $\mathcal{S}$ i.e., $\mathcal{A} = \mathcal{V} \setminus \mathcal{S}$ and $\mathcal{V} \setminus \mathcal{A} = \mathcal{S}$.



(a)

(b)

(c)

Figure 6.1: An example of missing PMU measurements recovery by graph signal reconstruction. (a) The band-limited actual voltage angles measurements, (b) the measurements under cyber-attack at bus numbers 59 to 64 (shown in dark blue), and (c) the recovered measurements.

6.2.2 State Recovery Using Graph Signal Sampling

The unobservable states are recovered by the methods described in Chapter 2. In this case, the reconstruction method developed in [67] has been implemented. Figure 6.1 shows an example of the missing voltage angle recovery using graph signal sampling. Figure 6.2 illustrates how the location of the attack affects the recovery performance. Using this approach, it can be observed that clustered cyber attacks can cause more recovery errors than random attacks of the same size. Moreover, the vulnerable locations in the grid can be identified from the buses with higher reconstruction errors.

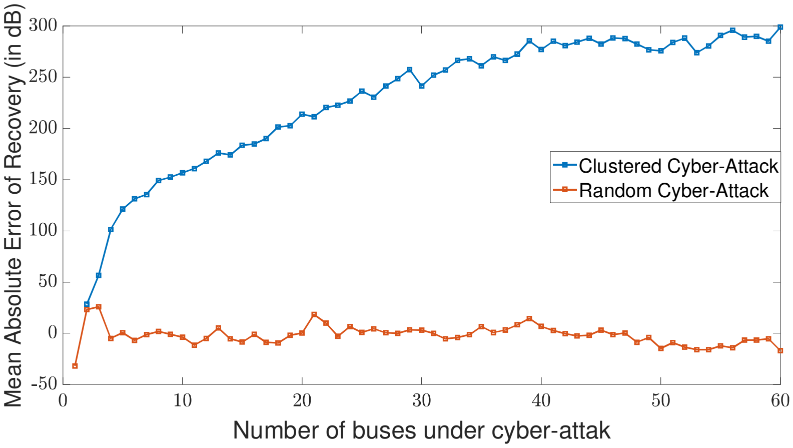


Figure 6.2: Recovery errors in cyber-attack. Clustered attacks introduce larger errors than random attacks of the same size.

6.3 State Recovery Using Global and Local Smoothness Graph Signal

In this work, a graph signal reconstruction technique based on the smoothness property of the power systems' graph signals has been proposed. The global smoothness [63] of the graph signal $x(n)$ is defined as $s_{Global} = \frac{\mathbf{x}^T\mathbf{L}\mathbf{x}}{\underline{\mathbf{x}}^T\underline{\mathbf{x}}}$ and quantifies the overall amount of fluctuations from vertices to vertices (which also relates to the bandwidth or the amount of high-frequency components in the signals). Note that smaller values of global smoothness represent smoother signals. Under the assumptions of a smooth graph signal, the reconstruction of the graph signal can be formulated with the goal of identifying values that minimize the global smoothness of the recovered graph signal. Since the power system graph signals are generally smooth [31, 22], the global smoothness can be one of the criteria for the power system's graph signal recovery. However, the global smoothness of a graph signal is a global parameter and therefore lacks local information about how signal values vary within local neighborhoods of vertices. The local smoothness of a graph signal is described for each vertex of the graph signal by $s(n) = \frac{l_x(n)}{x(n)}, \quad x(n) \neq 0$, where $l_x(n)$ is the $n-$th element of the vector, $\mathbf{L}\underline{\mathbf{x}}$ and $\mathbf{L}$ is the Laplacian matrix. The local smoothness specifies the amount of fluctuation of the signal values from one vertex to its neighboring vertices. The concept of the local smoothness of a graph signal is an analogous concept to instantaneous frequency, which quantifies the rate of change in signals at each time instant [63]. By incorporating the local smoothness of the graph signal in the recovery process, the knowledge about the local dynamics in the grid can be utilized in addition to the global dynamics to achieve better recovery performance and more robust estimation.

Our extensive simulations of power systems have shown that the local smoothness values of the power system's graph signal vary notably over vertices. By collecting and analyzing the measurement data for each vertex in the system, the probability distribution of the local smoothness values at each vertex, $p_{s_n}(\zeta)$, can be obtained. In this work, $p_{s_n}(\zeta)$ is characterized for bus voltage angle graph signals using data collected from our simulations.

6.3.1 Recovery Technique

The state information recovery technique for the power system's graph signal is formulated as an optimization framework for maximizing the likelihood of the local smoothness values at all the vertices while minimizing the global smoothness of the graph signal. This optimization problem can be cast into the following formulation:

$$\max_{x(n_{\mathcal{A}}),n_{\mathcal{A}}\in\mathcal{A}} p_{s_1,s_2,\ldots s_N}(s(n_1), s(n_2), \ldots s(n_N)) - \lambda s_{Global}, \tag{6.1}$$

where λ is the Lagrange multiplier. The joint distribution of the local smoothness for all the buses, $p_{s_1,s_2,\ldots s_N}(\zeta_1,\zeta_2,\ldots\zeta_N)$ is computationally infeasible to compute from the marginal distributions, $p_{s_n}(\zeta)$. However, maximizing the likelihood of the local smoothness values at each bus would serve a similar purpose. Therefore, an alternative objective function is proposed by maximizing the minimum likelihood value of local smoothness from all the buses along with minimizing the global smoothness.

$$\max_{x(n_{\mathcal{A}}),n_{\mathcal{A}}\in\mathcal{A}}[\min_{n} p_{s_n}(s(n))] - \lambda s_{Global}, \tag{6.2}$$

Our simulation data analyses have shown that the probability distribution of the local smoothness values at each bus does not follow any standard distribution. However, to simplify and solve this optimization problem, in this work the local smoothness values at bus n is assumed to follow a normal distribution with mean value μ_n and standard deviation σ_n. Due to this assumption, maximizing the likelihood of local smoothness values $p_{s_n}(s(n))$ at each bus in equation (6.2) takes the form of minimizing the absolute value of the normalized local smoothness, $z_n = \frac{s(n)-\mu_n}{\sigma_n}$ and the optimization problem can be expressed as:

$$\min_{x(n_{\mathcal{A}}),n_{\mathcal{A}}\in\mathcal{A}}[\max_{n}|\frac{s(n)-\mu_n}{\sigma_n}|] + \lambda s_{Global}. \tag{6.3}$$

The optimization in equation (6.3) is non-linear and proposed to be solved this optimization problem using the surrogate optimization method [118] to obtain the global minimum.

6.3.2 Simulation and Results

6.3.2.1 Experimental Setup

For validation of the proposed method and evaluating the state recovery performance, simulations have been done on the IEEE 118 bus system [62]. The power system graph signals, i.e., the bus voltage angle of each bus, have been obtained by simulating the power flow using MATPOWER [24]. A load pattern collected from the NYISO [25] is added to the default MATPOWER load to create a variation of load in the system as described in [95]. For evaluating the state recovery performance, fifty random scenarios are considered for each fixed number of unobservable buses, which can represent the buses under the cyber attack. The unobservable buses are chosen randomly with a uniform distribution from all the buses of the system except the reference bus.

6.3.2.2 Estimating the Probability Distributions of the Local Smoothness

The local smoothness values of the buses, i.e., $s(n)$ values, associated with the voltage angle graph signals are calculated for a large number of simulated graph signals for the IEEE 118 bus system. Once the local smoothness values are calculated using simulated graph signals, the probability distribution of the local smoothness values at each bus, $p_{s_n}(\zeta)$, are estimated empirically from the calculated local smoothness values. The actual distribution of the local smoothness values is intractable; however, our experiments have shown that assuming a normal distribution for local smoothness values at bus n with mean μ_n and standard deviation σ_n provides reasonable accuracy for the state recovery. Nonetheless, the parameters of the distributions need to be updated regularly to avoid the effect of data-drift [94] that can deteriorate the reconstruction performance.

6.3.2.3 Solving the Optimization Problem

In this work, the optimization problem in equation (6.3) has been solved by the surrogate optimization method [118] using MATLAB optimization toolbox [119]. The lower bounds and upper bounds of the values of $x(n_{\mathcal{A}})$ are considered as $\mu_{x_{n_{\mathcal{A}}}} - 3\sigma_{x_{n_{\mathcal{A}}}}$ and $\mu_{x_{n_{\mathcal{A}}}} + 3\sigma_{x_{n_{\mathcal{A}}}}$, respectively, where $\mu_{x_{n_{\mathcal{A}}}}$ and $\sigma_{x_{n_{\mathcal{A}}}}$ are the mean value and the standard deviation of the graph signal values at vertices $n_{\mathcal{A}}$, estimated from the past measurement data (simulated data). The value of the Lagrange polynomial, λ decides the relative importance of the global smoothness and the local dynamics to reconstruct graph signals values. For all the simulations in this work, the value of λ is considered to be 5,000. Depending on the system, the value of λ can be tuned to obtain the desired performance.

6.3.2.4 State Recovery Performance Analysis

The performance of the proposed method has been illustrated in Figure 6.3 in terms of the absolute error against the total number of unobservable buses (i.e., the number of buses under cyber attack). The mean absolute error and the maximum absolute error are the average value and the maximum value of recovery error over all the unobservable buses, respectively. The first metric is important for evaluating the general performance of the recovery method and the second one is important for evaluating the suitability of the proposed recovery method in certain power system applications demanding a standard state estimation accuracy at each bus.

As can be observed from the figure, the proposed method provides promising performance for recovering the missing states. The results also confirm that the error in recovery grows with the number of unobservable buses in the system.

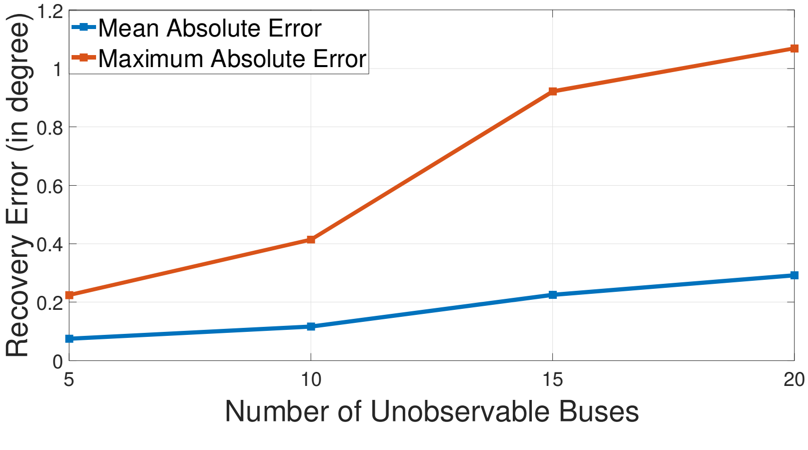
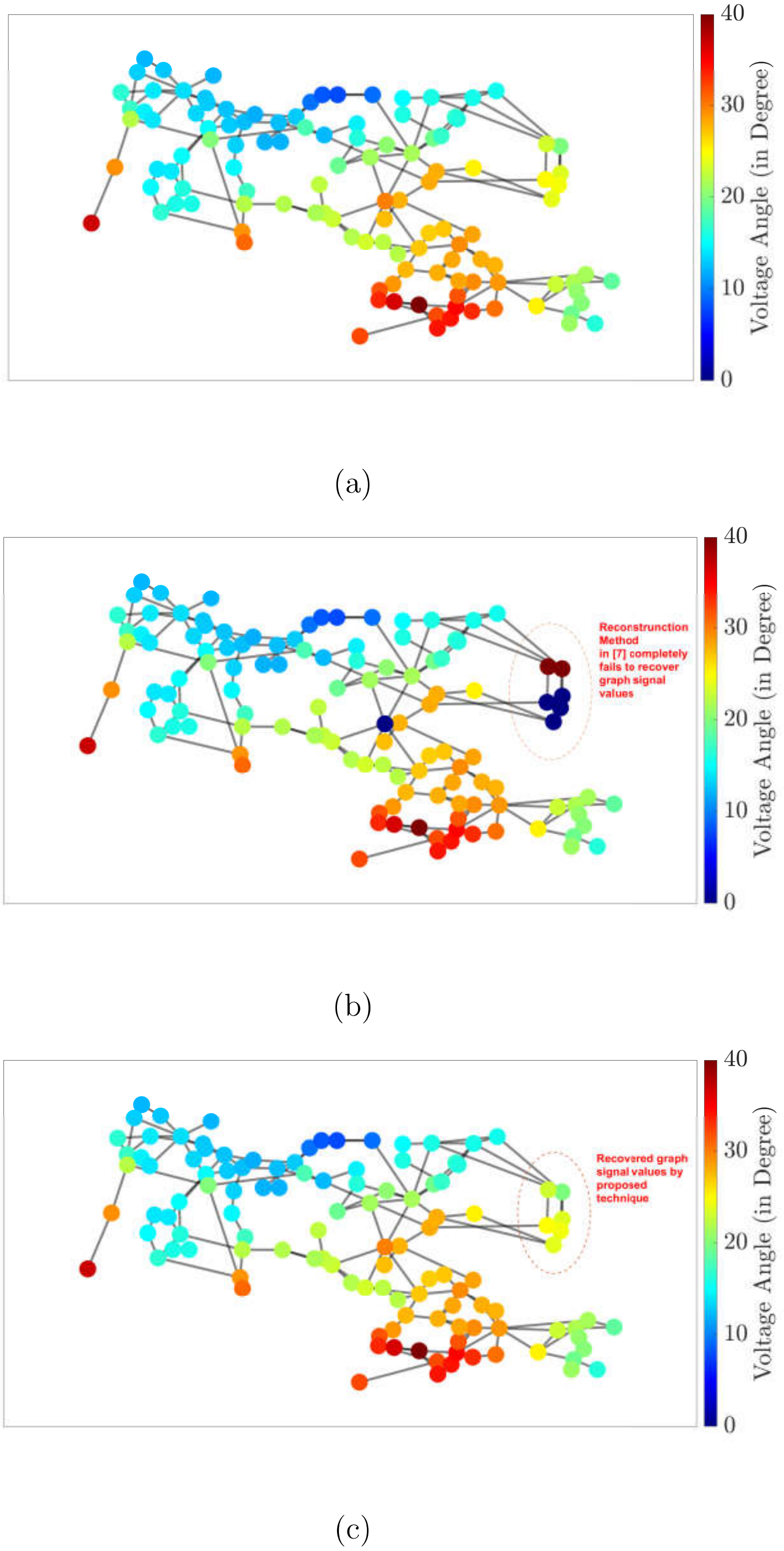


Figure 6.3: State recovery error using the proposed PMU placement method for different numbers of unobservable buses in the system.

6.3.2.5 Comparison with Other Reconstruction Methods

As discussed earlier, the reconstruction method applied in our previous work [28], which is based on matrix operation (including matrix inversion), is only applicable for graph signals that are perfectly band-limited to N_s frequency components, where N_s is the cardinality of the sampling set. For this reason, in [28], an anti-aliasing filter is applied to the originally approximately band-limited graph signals to discard the insignificant frequency components beyond N_s frequency components to make perfectly band-limited signals. The presence of components beyond N_s frequency components (even very small) leads to the computation of ill-conditioned matrices resulting in total failure to estimate the missing states. Figure 6.4(a) illustrates an example of a voltage angle graph signal, which is not band-limited (as ground truth for the experiment). In this example, the buses 59 to 64 in the IEEE 118 bus system are considered unobservable buses. In Figure 6.4(b) the missing signal values at unobservable buses are recovered using the direct matrix operation method discussed in [28], which fails to estimate the missing states in comparison to ground-truth states in Figure 6.4(a). However, the proposed method in the current work, which incorporates the global and local dynamics of the grid, is capable of estimating the missing signal values with notable accuracy as illustrated in 6.4(c). This example confirms that the applicability of the proposed method does not rely on the band-limited assumption of the graph signal to be recovered. The relaxation of the band-limited assumption makes this method applicable to many scenarios in power grids; particularly in cases where the resulted graph signals are not band-limited.

In [28], it has been shown that the major part of the error in the sampling-reconstruction process is introduced in the band-limiting process by the anti-aliasing graph filter. By avoiding the anti-aliasing filter error, the reconstruction error can be further reduced by the proposed method.



(a)

(b)

(c)

Figure 6.4: An example of missing voltage angle graph signal recovery by graph signal reconstruction. (a) The actual voltage angles measurement signal which is not band-limited, (b) recovered signal by the matrix operation-based method in [28], and (c) recovered signal using the proposed method.

6.4 Optimum Measurement Device Placement

The optimal PMU placement problem involves selecting a subset of the buses for mounting PMUs to collect component measurements. In practice, a PMU can measure the complex voltage of the bus on which it is mounted, the currents entering or leaving through all the branches connected to the bus, and the instantaneous frequency of operation. In this work, only the bus voltage angles are considered for the reconstruction of the signal and the evaluation of PMU placement strategies. The key objective is to collect the maximum amount of data reflecting the grid dynamics to provide observability of the state of the system with the minimum number of PMUs. Based on various requirements of monitoring functions in the power system, various PMU placement techniques have been proposed in the literature [79]. In this work, the PMU placement problem within the graph signal sampling-reconstruction framework has been studied to find the GSP-based optimal placement of PMUs for the reconstruction of the state of the whole system. The theoretical minimum number of required PMUs depends on the smoothness of the graph signal associated with the PMU measurement values (e.g., voltage magnitude, angle, frequency, etc.). If the graph signal at any time instant is band-limited to B graph frequency components, the theoretical minimum number of PMUs to be placed for the perfect recovery of the graph signal at each time instant is B. However, since the graph signals in power grids are not ideally band-limited, we design and use the anti-aliasing filters to analyze the reconstruction performance as a function of B. The value of B can be selected depending on the required precision of estimation and the details of the high-frequency components of the graph signal.

6.4.1 Sampling Set Selection in Power System Graph Signal Sampling

Since the optimum measurement device (e.g., PMU) placement problem is formulated as a sampling set selection problem under the graph signal sampling framework, here the sampling set selection problem is studied first. In this work, several criteria for the selection of the sampling set, $\mathcal{S}$, have been implemented and a novel sampling-set selection criterion has been proposed based on the average error introduced by the anti-aliasing filter calculated from the historical data in different buses. To present the selection criteria, let us define an operator, $\mathscr{F}$ that operates on a finite-length real-valued vector to obtain the indices of the values sorted in descending order. For example, consider a vector, $\underline{\mathbf{q}} = [77 \quad 92 \quad 28 \quad 55]^T$, then $\mathscr{F}(\underline{\mathbf{q}}) = [2 \quad 1 \quad 4 \quad 3]^T$. Next, various selection criteria would be discussed. Note that except for the random selection criterion, the rest of the sampling-set selection strategies are new techniques proposed and evaluated for the sampling of power grid graph signals in this work.

6.4.1.1 Random Selection of $\mathcal{S}$

Among the N vertices, N_s vertices are selected randomly (based on the uniform distribution over the vertices) to be sampled as discussed in [111, 120].

6.4.1.2 Degree-based Selection of $\mathcal{S}$

The vertices with higher node-degree are selected to be sampled first. Let, $\underline{\mathbf{d}}$ be the vector form of the graph signal $d(n)$, where $d(n)$ indicates the node-degree of the $n-$th vertex. Hence, if $\underline{\mathbf{d}'} = \mathscr{F}(\underline{\mathbf{d}})$ then the sampling-set can be defined as:

$$\mathcal{S} = \{v_n \in \mathcal{V} : n \in \{\text{First} \quad N_s \quad \text{elements of} \quad \underline{\mathbf{d}'}\}\}. \tag{6.4}$$

6.4.1.3 Page-rank-based Selection of $\mathcal{S}$

The vertices with higher page-rank centrality measure values are selected to be sampled first. Let $\underline{\mathbf{p}}$ be the vector form of the graph signal $p(n)$, where $p(n)$ indicates the page-rank value of the $n-$th vertex. If $\underline{\mathbf{p}'} = \mathscr{F}(\underline{\mathbf{p}})$, the sampling-set can be defined as:

$$\mathcal{S} = \{v_n \in \mathcal{V} : n \in \{\text{First} \quad N_s \quad \text{elements of} \quad \underline{\mathbf{p}'}\}\}. \tag{6.5}$$

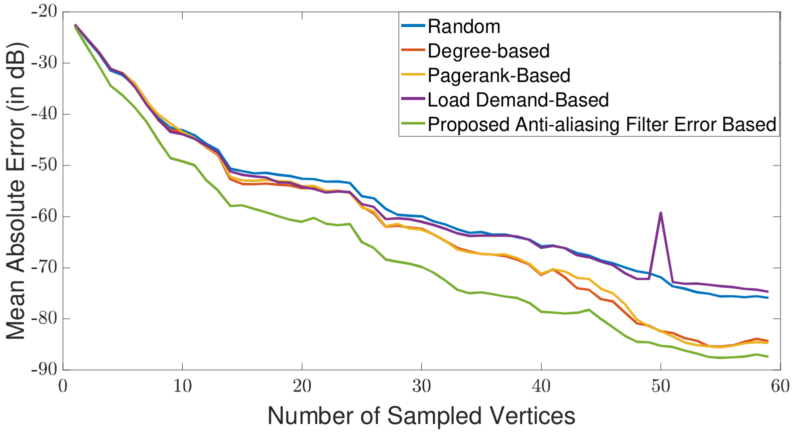


Figure 6.5: Relative performance of different selection criteria of the sampling-set, $\mathcal{S}$ in terms of the mean absolute reconstruction error (in dB).

6.4.1.4 Load Demand-based Selection of $\mathcal{S}$

Let $\underline{\ell}$ be the vector form of the graph signal $l(n)$, where $l(n)$ indicates the load demand of the $n-$th bus. If $\underline{\ell'} = \mathscr{F}(\underline{\ell})$ then the sampling-set can be defined as:

$$\mathcal{S} = \{v_n \in \mathcal{V} : n \in \{\text{First} \quad N_s \quad \text{elements of} \quad \underline{\ell'}\}\}. \tag{6.6}$$

6.4.1.5 Anti-Aliasing Filter Error-based Selection of $\mathcal{S}$

According to this criterion for selecting $\mathcal{S}$, data on the output of anti-aliasing filtering applied to instances of the system's graph signals have been collected. The vertices are then sorted based on the average amount of error introduced by the filter. From the sorted set, the vertices with the largest average errors are selected as the sampling set, $\mathcal{S}$. The rationale behind this criterion is that as the anti-aliasing filter discards the high graph-frequency components from a graph signal, the vertices with a larger amount of errors are corresponding to the regions where signal values are rapidly changing with respect to the neighboring vertices. As such, retaining the values on those vertices keeps the overall sampling-reconstruction error lower. Let $\underline{\mathbf{a}}$ be the vector form of the graph signal, where $a(n)$ indicates the average error caused by the anti-aliasing filter at the $n-$th bus. If $\underline{\mathbf{a}'} = \mathscr{F}(\underline{\mathbf{a}})$ then the sampling-set is:

$$\mathcal{S} = \{v_n \in \mathcal{V} : n \in \{\text{First } \; N_s \; \text{ elements of } \; \underline{\mathbf{a}'}\}\}. \tag{6.7}$$

Figure 6.5 illustrates the performance of the sampling-reconstruction process for these criteria in terms of the mean absolute sampling-reconstruction error expressed in (dB) for a different number of sampling vertices, N_s. It can be observed that the performance of the bus load demand-based criterion is quite similar to the uniform random selection of sampling nodes [111, 120]. However, the topology-based criteria (node degree and page-rank based) performs better than the random selection and load-demand-based criterion. The proposed criterion based on anti-aliasing filter error outperforms both the load demand-based and the topology-based criteria.

6.4.2 Optimum PMU Placement as an Optimization Problem

Let us consider $\mathcal{P} \subset \mathcal{V}$ to be the set of all the buses with PMUs mounted on them and representing the sampling set, $\mathcal{S}$. The reconstruction process is equivalent to estimating the measurements of the buses with no PMU from the measurements of the PMU buses. Mathematically, this process can be captured in the form of $x_{re}(p') = \mathscr{R}(x(p)), \quad \forall p \in \mathcal{P}, \quad \forall p' \in \mathcal{V} \setminus \mathcal{P}$, where $\mathscr{R}$ represents the estimation function described in Chapter 2 that estimates the measurements of the buses with no PMUs from the measurement of the PMU buses. In this framework, the PMU placement problem can be formulated as an optimization problem of minimizing the graph signal reconstruction error with the minimum number of PMUs as follows:

$$\min_{\mathcal{P}} \sum_{p' \in \mathcal{V} \setminus \mathcal{P}} [x_{re}(p') - x(p')]^2 + \lambda |\mathcal{P}|, \tag{6.8}$$

where λ is the Lagrange multiplier and $|\mathcal{P}|$ denotes the cardinality of the set $\mathcal{P}$. In the practical setting, in addition to minimizing the error of estimating the measurement values at the buses with no PMUs, several aspects are to be considered regarding the observability and implementation issues. These aspects can be considered as the constraints of the optimization problem in (6.8). In this work, two of these aspects are being considered as examples: 1) since placing a PMU at one bus ensures full observability of the voltage angle of its $1-$hop neighbors, if a PMU is placed at bus n, the $1-$hop neighbors of n are not considered as PMU bus, 2) a radial bus (i.e., vertex with degree 1) is not considered as a PMU bus [16]. The optimization in (6.8) can be expanded based on the reconstruction process discussed in Section 2.5.2 and shown to be an NP-hard problem [106]. Here, a heuristic is proposed for sampling-set selection based on the anti-aliasing filter error criterion described in the previous subsection 6.4.1.5. According to this technique, we consider buses one by one for placing PMUs in the sequence of the vector, $\mathbf{a}^{'}$. If a bus is a radial one or is at $1-$hop distance of an already placed PMU, the bus will be skipped and the next bus is considered for placing a PMU.

6.4.3 Results

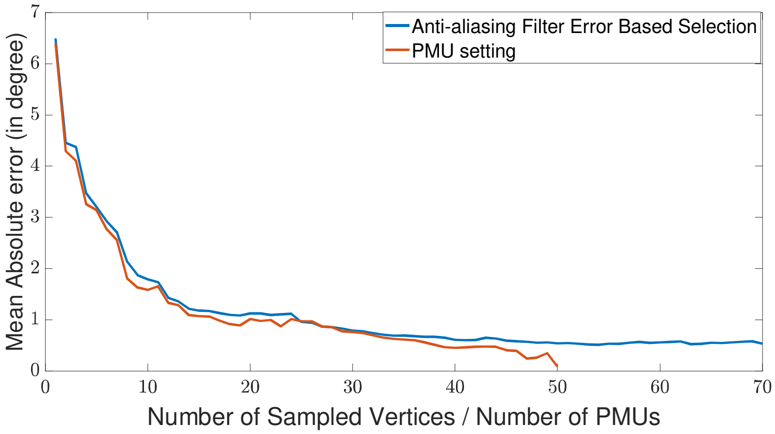


Figure 6.6: Error of reconstruction in PMU placement setting.

Figure 6.6 illustrates the mean absolute reconstruction errors as a function of the number of PMU placed in the grid for directly applying the anti-aliasing filter error-based criterion and for the modification of the anti-aliasing filter error-based criterion considering the two previously stated aspects of PMU placement. According to the modified criterion, when some of the buses are equipped with PMUs, the voltage angle of their $1-$ hop neighbors can be directly calculated using Kirchhoff's law, and the voltage angles of the rest of the buses are estimated using the graph signal reconstruction method. In Figure 6.6, the mean absolute reconstruction errors for the modified case are calculated for the unobservable buses only. From Figure 6.6 the number of PMUs can be chosen depending on the desired application and the budget. In our case, it is suggested to place 36 PMUs in IEEE 118 bus system according to the modified anti-aliasing filter error-based criterion with an average error of 0.5^0 for the non-PMU bus voltage estimation, which is acceptable for many applications (e.g. real-time performance monitoring and trending, small-signal stability monitoring, voltage stability monitoring/assessment, etc [121]).

6.5 State Recovery Using State Correlation

6.5.1 System and Attack Models

6.5.1.1 Power System Model

In this work, the power transmission system has been modeled as the sets of buses, transmission lines (branches), and their interconnections. $\mathcal{V}$ is the set of all the buses (vertices) in an N bus system as stated in the previous sections. It is assumed that there are PMUs in all the buses. Therefore, the measurements of all the bus voltage phasors are collected by the PMUs at a suitable sampling rate and sent to the control center. This assumption may not be realistic in today's smart grids as the PMUs are generally optimally placed [122] to minimize the cost and maximize the observability. Designing and developing data-driven methods similar to the one discussed here with optimally placed PMUs is prospective future work.

6.5.1.2 DoS Attack Model

It is assumed that the DoS attacks on the communication system of the power grid result in the unavailability of the data (time series of measured parameters) from a subset of the

PMUs associated with the buses, $\mathcal{B}$. $\mathcal{A} \subset \mathcal{V}$ be the set of buses, which their associated PMUs are under the DoS attack, and let us consider, $|\mathcal{A}| = M$. Let, $x_k(t)$ denote any electrical attribute (e.g., voltage or phase angles) from a PMU at time t, where, $k \in \mathcal{B}$. If a DoS attack occurs at time t_a, then, the attack is modeled by assuming the unobservability of $x_k(t)$ for $t > t_a$.

6.5.2 Method

The goal of the estimation method in this work is to estimate the state of the components, which their PMUs are under attack, from the state of the rest of the components collected by the rest of the PMUs. Specifically, it is assumed that the time series of the states of electrical attributes $x_i(t)$, where, $i \in \mathcal{V} \setminus \mathcal{A}$ is available except for buses in the attack set, $\mathcal{A}$. In the estimation method, the time series of unknown (unobservable) buses for $t > t_a$ due to DoS attack is denoted by $y_j(t)$, where, $j \in \mathcal{A}$.

The relationship between the known and unknown states is proposed to be defined as follows:

$$\dot{y}_j(t) = \sum_{i=1}^{N-M} w_{ji}\dot{x}_i(t). \tag{6.9}$$

For M DoS attacks on M buses, equation (6.9) will result in a system of equations as follows:

$$\underline{\dot{\mathbf{y}}}(t) = \mathbf{W}\underline{\dot{\mathbf{x}}}(t), \tag{6.10}$$

where $\underline{\dot{\mathbf{y}}}(t)$ and $\underline{\dot{\mathbf{x}}}(t)$ are vectors with elements representing the time derivative of the time series corresponding to unknown and known buses, respectively.

Here, the time derivative of a state variable under the DoS attack has been estimated as the weighted sum of the time derivatives of the rest of the parameters. The weights come from the correlations between any state outside the attack zone and the attacked state. The rationale behind estimating the time derivative of the state first instead of directly estimating the state is: it has been observed that although the states vary significantly in terms of the actual values, there exist very strong correlations among several states in their changing pattern with time.

The matrix **W**, contains the bus-to-bus correlation of the electrical attributes among the buses under DoS attack and the buses that are not under the attack. Any element of W is represented as:

$$w_{ji} = e^{ar_{ji}}, \tag{6.11}$$

where r_{ji} is the correlation coefficient between $y_j(t)$ and $x_i(t)$ for the last t_c moments before the DoS attack:

$$r_{ji} = \int_{t_a - t_c}^{t_a} x_i(t) y_j(t) dt. \tag{6.12}$$

Since the DoS attack is considered to be on the communication layer of the smart grid, therefore, no physical attack or topology changes is assumed. Moreover, we consider the correlation among the PMUs just before the DoS attack happens. As a result, the correlation among the PMUs before the attack and after the attack can be considered unchanged. It is true that if the DoS attack continues for a long period, the estimation accuracy decreases because the correlation among the PMUs changes within this period due to the change in loads. Besides, if any physical attack is masked by the DoS attack, our technique may not perform well because the correlation among the PMUs will be changed due to the physical attack.

The reason behind taking the exponential of correlation coefficients is to emphasize the highly correlated buses and to de-emphasize the barely correlated buses. However, the set of weights also depends on the scalar parameter, a. Here, the value of a is empirically selected and the effect of choosing different values for parameter a has been illustrated in the simulation and result section. However, the determination of the value of a from the topology of the grid and system properties directly or indirectly can be prospective future work.

For the discrete-time realization of the continuous-time time series, the derivative of a time series at t can be considered as the backward difference system: $\dot{f}(t) = f_t - f_{t-1}$, where, f_t is the sampled value of the time series f at time t, and f_{t-1} is the previous sampled value. According to this notion, the equation (6.10) can be written in the following form:

$$\underline{\mathbf{y}}_t - \underline{\mathbf{y}}_{t-1} = \mathbf{W}(\underline{\mathbf{x}}_t - \underline{\mathbf{x}}_{t-1}). \tag{6.13}$$

The sampled value of the attacked states at the moment of the attack (t_a), denoted by $\underline{\mathbf{y}}_{t_a}$ can be considered as the initial value and assumed to be known. During the attack interval, the values are updated by:

$$\underline{\mathbf{y}}_t = \underline{\mathbf{y}}_{t-1} + \mathbf{W}(\underline{\mathbf{x}}_t - \underline{\mathbf{x}}_{t-1}), \ t > t_a. \tag{6.14}$$

6.5.3 Simulations and Results

The simulations have been run on the IEEE 14 bus system [123] and IEEE 118 bus system [62]. The load patterns are collected from the New York Independent System Operator (NYISO) [25]. The NYISO consists of eleven regions. The load profiles are normalized within 0 to 1 and added with the default constant loads of the eleven load buses of the IEEE 14 bus case to generate the load profile time series. For the IEEE 118 bus case, there are not enough load data since there are 91 load buses in this system. Therefore, the available data for the different regions are combined to synthesize load profiles for those 91 load buses similar to [89]. By combining three different regions to synthesize one new load profile by taking the average, it is possible to create $\binom{11}{3} = 165$ such combinations. Out of the 165 profiles, the first 91 are considered as the load profile of the 91 load buses of the IEEE 118 bus system.

In the NYISO data, the load is measured every five minutes. However, these data are linearly interpolated to generate time series of 0.033 Hz sampling rate. MATPOWER 6.0

[24] has been used to simulate the power flow for both the IEEE 14 bus and 118 bus cases. The details of the simulation have been discussed in the following subsections:

6.5.3.1 Correlation Among PMU Time Series

As discussed in Section 6.5.2, the time-series data from the PMUs under DoS attack are estimated from the correlations among the PMU data, which arise from the physical dynamics of the power system. Figure 6.7 illustrates the correlations among the voltage angle PMU data for the IEEE 118 bus case. From the figure, it is clear that some of the PMU data have very strong correlations among them. In this figure, correlations have been shown only for the buses, which have physical connections among themselves. However, PMUs installed in the buses having no connections may still have correlations due to the physics of the electricity and power flows.

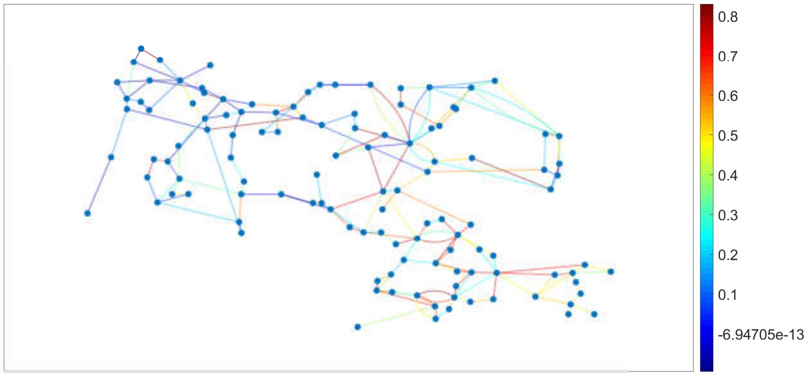
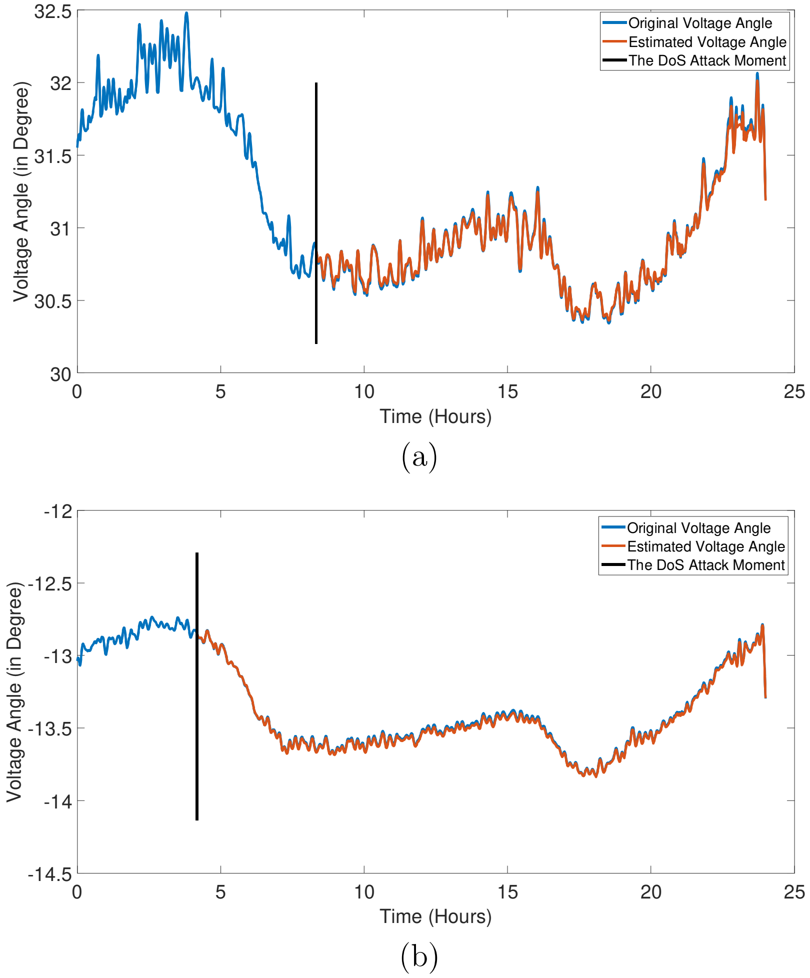


Figure 6.7: Relative correlations among the PMUs of the physically connected buses in terms of voltage angles for IEEE 118 bus case.

6.5.3.2 Estimation of PMU Time Series Under Single and Multiple DoS Attacks

Figure 6.8(a) illustrates the estimation of the voltage angle time series of bus 86 of the IEEE 118 bus system when only the PMU associated with that bus is under DoS attack. The red curve represents the estimated time series based on the method presented in Section



(a)

(b)

Figure 6.8: Estimation of bus voltage angle under single DoS attack. (a) Bus 86 for IEEE 118 bus system. (b) Bus 7 for IEEE 14 bus system.

6.5.2 and the blue line represents the ground truth, while the DoS attack occurred at t_a, it is represented by the black vertical line. The estimated time series seems to track the ground truth quite accurately. The mean squared error, in this case, is 8.8631×10^{-4} degree. The value of a is empirically selected as 300. However, the accuracy of the estimation depends on the proper choice of a, which has been discussed later in this section. Figure 6.8(b) shows similar results for bus 7 for IEEE 14 bus system. The estimation of voltage magnitude time series has been shown in Figure 6.9.

The accuracy of the estimation of PMU data deteriorates when a larger number of nearby PMUs go under a DoS attack. Figure 6.10 illustrates the estimation of voltage angle at

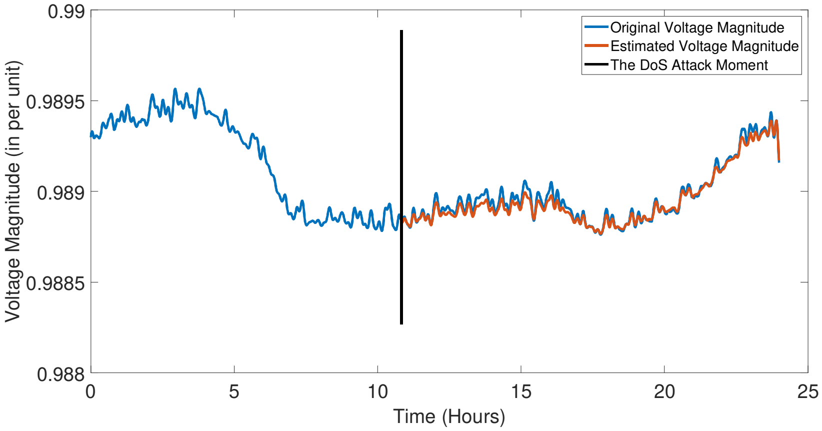


Figure 6.9: Estimation of bus voltage magnitude under DoS attack at bus no. 86 for IEEE 118 bus system.

the PMU associated with bus number 86, respectively, for the failure of 2, 8, 16, and 32 PMUs including the PMU associated with bus 86. It is clear that although the accuracy of the estimation decreases with the increase in the number of DoS attacks, this method can estimate the PMU data even for a large number of DoS attacks. Figure 6.11 illustrates the relation between the Mean squared error and the number of PMUs under the DoS attack for three types of distribution of attacks: uniform, clustered, and inhibition.

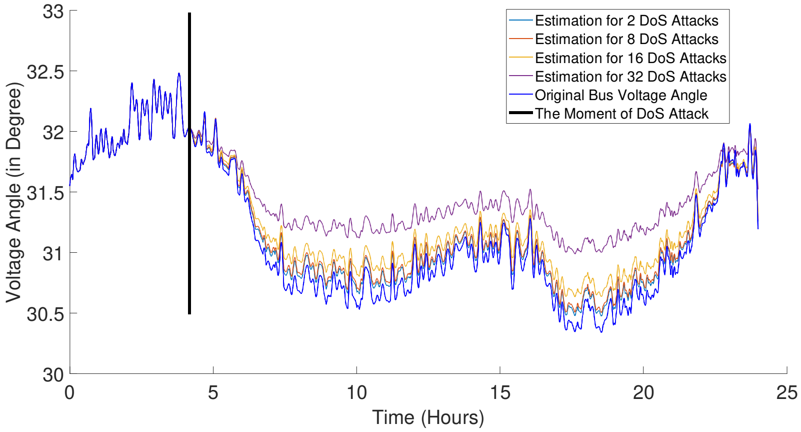


Figure 6.10: Estimation of bus voltage angle under DoS attack at bus no. 86 for IEEE 118 bus system for multiple attacks.

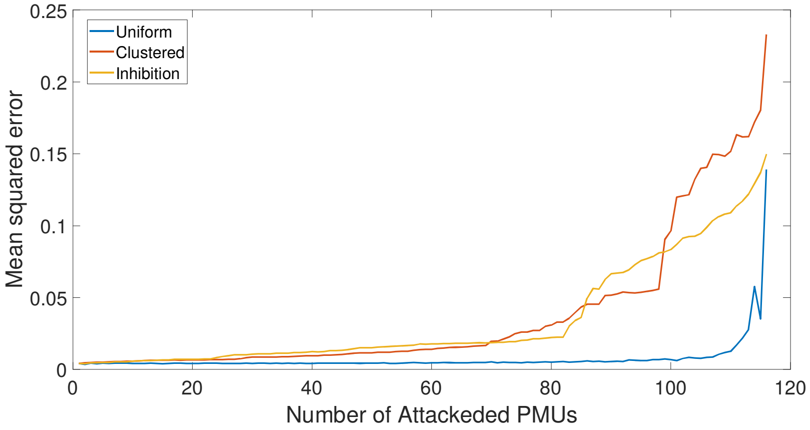


Figure 6.11: Mean squared error vs. number of DoS attacks (average over all possibilities).

6.5.3.3 *Most Vulnerable Combination of Attacks*

The most vulnerable PMU for the initial DoS attack from the attackers' point of view can be identified on the basis of the largest mean squared error (MSE) of estimation of the voltage angle under the single DoS attack. The relative vulnerability of the PMUs of the IEEE 118 bus system has been represented in Figure 6.12 by the node colors. For example, from the attackers' perspective, it is possible to create more unobservability in the power system by launching a DoS attack on a red node (e.g. node 82) in Figure 6.12.

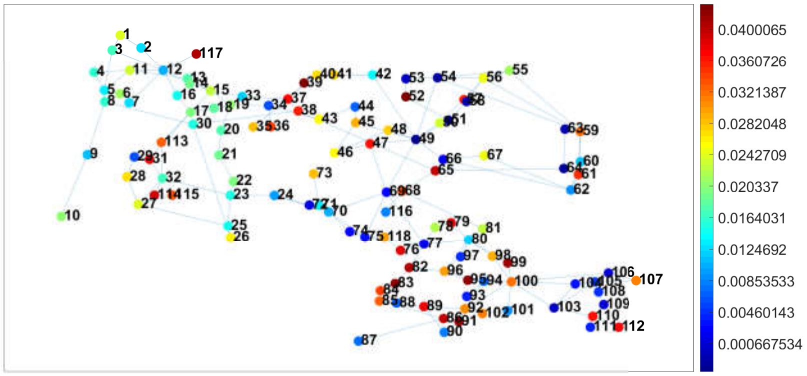


Figure 6.12: Relative vulnerability of the PMU locations for initial DoS attack on the basis of MSE for IEEE 118 bus system.

6.5.3.4 Parameter a Values

The choice of the parameter a has a significant impact on the accuracy of the estimator. Figure 6.13 illustrates the effect of parameter a on the estimation. Here, the value of the parameter a is kept fixed for all buses. From Figure 6.13 it can be inferred that a value between 200 and 500 can be a good choice. When the bus voltage to be estimated has strong correlations with only a few numbers of bus voltages, then larger values of a, work better (the weights for the barely-correlated buses would be negligible compared to the weights for the strongly correlated buses). However, a small value of parameter a would work better, when that bus has significant correlations with many buses.

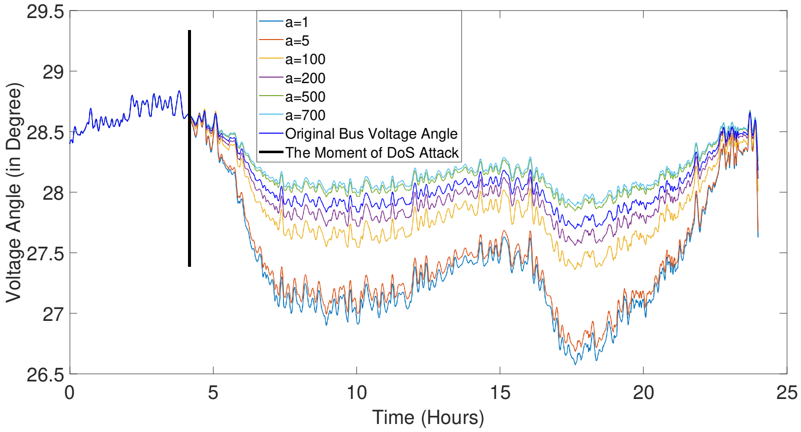


Figure 6.13: The effect of the parameter a on the estimation of bus voltage angles in IEEE 118 bus system.

6.5.3.5 Most Vulnerable Time for the DoS Attack

The moment when the DoS attack initiates also impacts the estimation accuracy. This is because the correlations among the bus parameters vary in time. This variation comes from the variation in the load profile at the load buses throughout the day. Figure 6.14 represents the MSE in the cases of DoS attacks at different times of the day. The two profiles are from two different days, however, show the same pattern. It can be inferred from the two figures that in terms of the MSE, the most vulnerable time for the initiation of the attack is during the end of office hours when the load fluctuation is very high. From the attackers' perspective, the highest amount of unobservability can be created by initiating DoS attacks during this period.

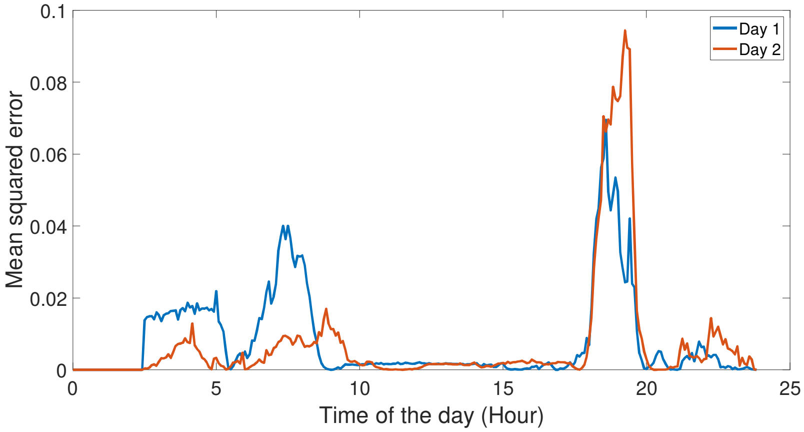


Figure 6.14: The effect of the attack time on the estimation of bus voltage angles in IEEE 118 bus system.

Chapter 7: GSP-based Grid Perturbation Analysis

[6]GSP has emerged as a prominent field that focuses on the analysis of structured data over the graph domain. Recently, GSP has found applications in the analysis of power system data by representing the power system as a graph and its measurements over the graph as graph signals [22, 26].

By extending the theories and tools of classical signal processing to the irregular graph domain, GSP facilitates imparting explicit information about the topology, connectivity, and interactions among the components of the grid in the analysis of data. Detection, localization, and classification of anomalies, attacks, and stresses in the electric grid [22, 26, 125], state estimation and recovery [47, 102, 126], estimation of load current variability in the presence of distributed generators [48], and load disaggregation [127] are examples of applications of GSP in addressing problems in power systems.

Analyzing power grid data through the lens of GSP has revealed that signatures and patterns of stresses in the system are embedded in various properties and features related to the system's graph signals [26, 27]. In this work, the focus is on understanding the features and patterns in power systems graph signals due to abrupt changes in the load demand or generated power in a single bus. Although fluctuation of load demand within an acceptable range is normal and perpetual in the power system, understanding the patterns of load change is important for situational awareness, particularly in the context of smart grids with intermittent and low-inertia loads [128]. A typical scenario is the charging of electrical vehicles (EVs) as a load added to the grid (G2V technology) [129]. Since the load demand associated with the charging of the EVs is more probable to be clustered

[6] Portions of this chapter were published in arxiv [124]. Copyright permissions from the publishers are included in Appendix B.

geographically [130], a monotonous increase of load demand at a particular bus can be a common situation. Another origin of the monotonous increase in load demand can be the load-altering cyber attacks purposefully launched by adversaries [131, 132]. The abrupt changes in the generation of real power are not common in traditional power systems but are possible in modern power grids when a large number of renewable energy resources are connected to the grid by converters [128]. In this work, a general approach has been considered, from the GSP perspective, to analyze the effect of changes in the load demand or generated real power at a particular bus, modeled as *single bus perturbation*, without explicitly modeling the cause of perturbation.

The first presented study is focused on understanding how a single bus perturbation spreads through the power grid depending on the strength and the location of the perturbation. The analysis of the spreadability of a bus perturbation is important from several perspectives in the context of grid stability and reliability analysis. A more spreadable perturbation can affect a large number of components (e.g., buses, transmission lines), even at distant locations from the perturbation point, and introduces stresses in the grid that may even lead to cascading failures or blackouts. Here, a GSP-based measure is defined to quantify the spreadability of the perturbation depending on its strength and location. This spreadability measure is also useful for planning the placement of low-inertia loads and generators in the grid.

In addition to understanding the spreadability, it is important to understand how the perturbation affects other graph signal features to gain an improved situational awareness under stress. For instance, power system graph signals, especially the bus voltage angle graph signal, are generally smooth during normal grid operation [22, 26, 27]; however, the local and global smoothness properties of the graph signals vary under stress. This study focuses on understanding how the global and local smoothness values associated with the power system graph signals are affected as a function of the perturbation strength and location. The relation between the proposed spreadability measure and local and global smoothness features of graph signals has also been explored and it has been shown that certain smoothness parameters associated with the difference graph signals (before and after perturbation) can be estimators of spreadability of the perturbations.

The effects of single bus perturbation on the power system graph signals have been derived analytically using the DC power flow model and simulated using AC power flow model to verify the properties in more realistic scenarios. The presented analytical approach shows that the proposed measure of spreadability does not depend on the perturbation strength, but rather depends on the location of the perturbation. Our experiment based on the AC power flow model closely supports this property. Moreover, the presented analytical analysis shows that the global smoothness of the bus voltage angle graph signal is a quadratic function of the increasing load demand (or generated real power) at a particular bus. Based on this analysis, there is a critical value of input power at each bus beyond which the global smoothness begins to decrease and further increase in the input power leads to divergence of the power flow equations. Failing of power flow convergence, although arises from various issues, is an indicator of a stressed system. The presented analytical study shows that the critical load (or generation) at each bus for which the global smoothness is maximized depends on the topology.

The main contributions of this article have been summarized below:

- A quantitative measure of the spreadability of a perturbation has been proposed and the properties of this measure have been analyzed theoretically under the DC power flow model and verified using the AC power flow model. The proposed measure has been compared with an existing network-science-based spreadability metric.

- The global smoothness of the voltage angle graph signal has been shown to follow a quadratic function of the perturbation strength with a maximum, defined as the critical perturbation. It is shown that this critical point suggests approaching the power flow model divergence, which although can arise from various issues, is an indicator of an unstable grid.

- This work studied the global and local smoothness properties of the difference graph signal of the bus voltage angles before and after the perturbation. The studies show that under DC plow flow assumptions these smoothness parameters are independent of the perturbation strength and can be suitable for comparing perturbations at different locations of the grid. The results of the simulation with AC power flow support this property approximately and it has been shown that these smoothness parameters can be estimators of the spreadability of perturbations depending on their locations.

7.1 Related Work

The effects of perturbations in the electrical grid has been studied from various perspectives in the literature. The stability of the grid after the perturbation, the dependency on the perturbation location, the propagation of the effect of perturbation through the system, and the identification of vulnerable locations in the grid are some of the topics of interest in this domain. A number of works analyze the effects of perturbation from the complex network perspective using the concept of *Basin stability* [133, 134] using the frequency measurements in the grid. For example, Wolff *et. al.* [133] analyzed the effect of perturbation of a single node (bus) in the electric grid based on the Basin stability of the grid, which is evaluated in terms of the return time of the grid to the steady-state after the perturbation. This work defines perturbation as the direct change of voltage phase angle and angular frequency at the perturbation bus. Menck and Kurths [134] identify the weaker buses due to small perturbations in the grid based on Basin stability.

The propagation of spatio-temporal signals through the system (as a complex network) has been studied by several authors. Hens *et. al.* [135] provide a generalized theoretical analysis of how spatio-temporal signals propagate in time through complex networks depending on the topology and dynamic mechanisms of interactions among the vertices. A few works studied the spreading of disturbance in the electric power grid. For example, Molner *et. al.* [136] proposed a heuristic technique to relate the spread of oscillations due to the variable renewable resources to the network structure. Nnoli and Kettemann [137] analyzed the propagation of disturbance in the electric grid depending on the topology of the grid, its inertia, and heterogeneity. In [138], the authors considered a network science based approach to quantify the spreadability of a single perturbation in the grid depending on the perturbation location.

As discussed earlier, the impact analysis of grid perturbations can be useful in several scenarios in the modern power grids including the integration of distributed energy resources (DERs) and electric vehicle charging stations. Although in most cases, the problems do not directly correspond to the single vertex perturbation, the single perturbation analysis can be useful for the simplification of such problems. In the current literature, the issues related to the integration of EVs and DERs have been studied using various methods. Vasilij *et. al.* [139] developed a model for the worst-case analysis of the impact of placing EV charging stations in the grid, which involves observing the impact of the placement of charging stations on voltage profile and line loading.

The current work presents a generalized approach to analyze the impact of a single perturbation in the grid. Moreover, unlike the Basin stability-based analyses, this work does not consider the frequency data and only considers the impact of the perturbation on the bus voltage angle data. The current work adds a GSP-perspective into the analysis to directly impart the topology and interconnection into the analysis.

7.2 Mathematical Representation of Perturbation and Associated Electrical Attributes

7.2.1 Power System Graph Signals

An electric power grid with N buses and M transmission lines has been modeled as a weighted undirected graph, $\mathcal{G} = (\mathcal{V}, \mathcal{E}, \mathcal{W})$. The buses of the grid are considered as the vertices of the $\mathcal{V} = \{v_1, v_2, ..., v_N\}$, whereas the transmission lines are considered as the edges, $\mathcal{E} = \{e_{ij} : (i, j) \in \mathcal{V} \times \mathcal{V}\}$, and therefore, $|\mathcal{V}| = N$ and $|\mathcal{E}| = M$, where $|.|$ denotes the cardinality of the set. The element w_{ij} of the weight matrix, $\mathcal{W}$ is the weight corresponding to the edge, e_{ij}. The vertices corresponding to the buses with generators (i.e. energy sources) and loads are denoted by $\mathcal{S} \subset \mathcal{V}$ and $\mathcal{L} \subset \mathcal{V}$. The Laplacian matrix $\mathbf{L}$ associated with the graph $\mathcal{G}$ with elements l_{ij} is defined as: $l_{ij} = \sum_{j=1}^{N} w_{ij}$, if $i = j$ and $l_{ij} = -w_{ij}$, otherwise. In the GSP literature, the weights are defined in various ways, for instance, based on the geographical and physical relational aspects, depending on the applications. In this work, the weights w_{ij} are defined such that the Laplacian matrix, $\mathbf{L}$ represents the imaginary part of the admittance matrix of the grid which is related to the transmission line parameters of the grid.

The graph signal $x(v_n)$, written as $x(n)$ for simplicity, can be considered as a mapping of the vertices of the graph to real-number space, $x : \mathcal{V} \to \mathbb{R}$ and can represent various electrical attributes associated with the buses of the grid. The signal values of $x(n)$ arranged in a vector form would be denoted by $\underline{\mathbf{x}}$. In this article, the graph signal $x(n)$ at a particular time instant t is denoted as $x(n, t)$.

Let us consider $\theta(n)$, the bus voltage angle graph signal that represents the angles of the voltage phasors at each bus. While any or combination of electrical attributes at each bus can be considered, here the focus will be on the voltage angle graph signal $\theta(n)$ to evaluate the state of the power system without the direct information on the transient aspects through the fluctuations in voltage magnitudes and frequency. Moreover, bus voltage angle measurements are directly related to the load demands, which are important in this study. The generated real power and the real power demand at each bus are denoted by the *generated power graph signal*, $p_g(n)$ and *load demand graph signal*, $p_d(n)$, respectively. Note that $p_g(n) = 0$ for $n \in \mathcal{V} \setminus \mathcal{S}$ and $p_d(n) = 0$ for $n \in \mathcal{V} \setminus \mathcal{L}$. The *input power graph signal* is denoted by $p(n)$, where $p(n) = p_g(n) - p_d(n)$.

7.2.2 DC Power Flow Model

The DC power flow model [24] describes a linear relationship between the input power and the bus voltage angle, described by the equation $\underline{\mathbf{p}} = \mathbf{B}\underline{\theta}$, where $\mathbf{B}$ is the susceptance matrix (imaginary part of the admittance matrix) of the grid with element b_{ij} at the $i-$th row and $j-$th column. Knowing the topology, the bus voltages can be computed from the active power input based on $\underline{\theta} = \mathbf{B^{-1}}\underline{\mathbf{p}}$ and can be represented in a graph signal form as:

$$\theta(n) = \sum_{j=1}^{N} \beta_{nj} p(j), \tag{7.1}$$

where β_{ij} is the element of $\mathbf{B^{-1}}$ at the $i-$th row and the $j-$th column. In this work, the linearity of the DC power flow model facilitates analytical investigation of the properties of the graph signals. However, since the DC power flow model is an approximation of the power flow in power systems, in certain cases, the results from this model may deviate from the real scenarios. Nevertheless, through the graph signal analysis, we will show that the DC power flow assumption can still provide key information that can reveal the state of the system. Whenever necessary, in this work, the AC power flow model is utilized for numerical verification of the state of the system through MATPOWER [24].

7.2.3 Smoothness of Graph Signals

The global smoothness of a graph signal is a measurement of the overall amount of vertex-to-vertex fluctuations in the graph signal [63]. The global smoothness value associated with graph signal, $x(n)$ is defined as [63]:

$$g_x = \frac{\underline{\mathbf{x}}^T \mathbf{L} \underline{\mathbf{x}}}{\underline{\mathbf{x}}^T \underline{\mathbf{x}}} = \frac{\sum_{i=1}^{N} \sum_{j=1}^{N} L_{ij} x(i) x(j)}{\sum_{k=1}^{N} x^2(k)}, \tag{7.2}$$

where $\underline{\mathbf{x}}$ is the signal values of $x(n)$ arranged in a vector form. A small value of g_x indicates a smooth graph signal, whereas increasing values of g_x indicate the increasing vertex-to-vertex fluctuations of signal values [63]. The bus voltage angle graph signal $\theta(n)$ in normal conditions is generally smooth with a small value of g_θ.

The local smoothness [63] of a graph signal $x(n)$ is defined by the following equation and represents how rapidly the value of a graph signal changes from each vertex n to its neighboring vertices:

$$l_x(n) = \frac{\sum_{k=1}^{N} L_{nk} x(k)}{x(n)}, \quad x(n) \neq 0, \tag{7.3}$$

Our previous analyses of the local smoothness for the bus voltage angle graph signals in power systems in [26, 102] have revealed that the voltage angle graph signals is smoother at certain locations in the grid depending on the topology and interconnections among the components of the system.

The global and local smoothness of graph signals are important features in the vertex domain that can allow analyzing some of the behavior and properties of the signals and the system they represent. Deviation from nominal ranges of these parameters can be an indication of an anomaly [26]. In the power system context, the anomalies may indicate a *stressed* system due to cyber attacks or physical events, such as line outages, generator trips, and abrupt load changes. In our previous works, local and global smoothness of bus voltage angle graph signals (i.e., g_θ and $l_\theta(n)$) have been utilized for the detection [26], location identification [26], characterization (determining whether clustered or random stress, determination of cyber-attack centers and radii) [29], and classification [30] of these stresses in the power system. The current work provides a focused study on the changing pattern of global and local smoothness values of different graph signals under single bus perturbation due to, for instance, abrupt changes in load demand or generation. Through this study, the spread of the effects of perturbation in the system will also be investigated through graph signal properties. Understanding the properties of stresses and their spread can support power system monitoring and planning, for instance, for predicting the grid instability due to load and generator changes, the effects of renewable energy resources on the system state, and for analyzing the effect of loads connected through grid-following and grid-forming inverters.

7.2.4 Single Bus Perturbation

A single bus perturbation $\mathscr{U}$ at the vertex (i.e., bus), $v_u \in \mathcal{S} \cup \mathcal{L}$ is defined by an abrupt change of value in the bus input at time t_u and can be defined in the power graph signal form as:

$$p(u, t_u) = p(u, t_u - \epsilon) + \Delta p_u(u), \tag{7.4}$$

where ϵ is a very small amount of time. The perturbation graph signal $\Delta p_u(n)$ can be modeled as a Kronecker Delta [140] graph signal:

$$\Delta p_u(n) = \gamma \delta_u(n), \tag{7.5}$$

where $\delta_u(n)$ is the Kronecker delta graph signal defined as: $\delta_u(u) = 1$ and $\delta_u(n) = 0$, for $n \neq u$ and γ is a scalar called *perturbation strength* associated with the perturbation, $\mathscr{U}$. Therefore, $\Delta p_u(u) = \gamma$. A positive value of γ at the generator-only bus (i.e., $v_u \in \mathcal{S} \setminus \mathcal{L}$) indicates an increase in generated real power while a positive value of γ at load-only bus (i.e., $v_u \in \mathcal{L} \setminus \mathcal{S}$) indicates an increase in the real power load demand. The value of γ in buses with both generators and loads (i.e., $v_u \in \mathcal{S} \cap \mathcal{L}$) can be described by the increase and decrease of both generations and loads. However, in this work, only one change at a time (i.e., either an increase or decrease in generated power or load demand) is considered. It is also assumed that the inertia of the grid is negligible in response to the perturbation, $\mathscr{U}$. This assumption is reasonable for the modern and future grids, where renewable energy resources are connected to the grid with inverters and loads are connected with converters.

In this work, the effects of the perturbation $\mathscr{U}$ on the voltage angle graph signal, $\theta(n)$ are evaluated. Let the *difference voltage angle graph signal* due to the perturbation $\mathscr{U}$ at bus u at time t_u be defined as:

$$\Delta\theta_u(n) = |\theta(n, t_u) - \theta(n, t_u - \epsilon)|, \tag{7.6}$$

where ϵ is a small value. The signal values of the graph signal $\Delta\theta_u(n)$ have a direct relation with the perturbation strength, γ. Therefore, for a better understanding of the dependency on the perturbation location a normalized version of $\Delta\theta_u(n)$ has been considered. The *normalized difference voltage angle graph signal* is defined as:

$$\psi_u(n) = \frac{\Delta\theta_u(n)}{|\gamma|}, \tag{7.7}$$

where $\psi_u(n)$ is expressed in $degree/mega - watt$.

Property 1. *Considering the DC Power flow model, the $\psi_u(n)$ depends only on the topology.*

Proof: Substituting the definition of $\theta(n)$ from equation (7.1) into equation (7.6):

$$\begin{aligned}
\Delta\theta_u(n) &= \left|\sum_{j=1}^{N} \beta_{nj} p\left(j, t_u\right) - \sum_{j=1}^{N} \beta_{nj} p\left(i, t_u - \epsilon\right)\right| \\
&= \left|\sum_{j=1}^{N} \beta_{jj}\left[p\left(j, t_u\right) - p\left(j, t_u - \epsilon\right)\right]\right| \\
&= \left|\sum_{j=1}^{N} \beta_{nj} \Delta p_u(n)\right| \\
&= \left|\sum_{j=1}^{N} \beta_{nj} \gamma \delta_u(j)\right| \\
&= \left|\gamma\beta_{nu}\right|, \quad \text{(using the property of Kronecker Delta).}
\end{aligned} \tag{7.8}$$

Next, substituting $\Delta\theta_u(n)$ into equation(7.7) leads to:

$$\psi_u(n) = \frac{|\gamma\beta_{nu}|}{|\gamma|} = |\beta_{nu}|. \tag{7.9}$$

This property shows that $\psi_u(n)$ does not depend on γ, under the DC power flow assumption. The normalized difference in voltage angle before and after the perturbation depends only on the location of the perturbation. In other words, the location of the perturbation affects

$\psi_u(n)$ according to the topology of the grid, which captures the interconnections among the buses and the electrical distances between the components. Since the power system dynamics deviate from the DC power flow model, this property may not hold accurately in real power grids, nevertheless, it indicates that the effect of perturbation in the grid predominantly depends on its location rather than its strength. This property is important as it can be used for instance, for identifying the vulnerable buses with respect to perturbation issues, which is important for stability, maintenance, and resilience planning.

The perturbation $\mathscr{U}$ affects the bus attributes of the perturbed bus, $v_u \in \mathcal{S} \cup \mathcal{L}$ as well as the other buses ($v \in \mathcal{V}, v \neq v_u$) in the system. The effects of the perturbation spread throughout the grid (similar to a stone causing ripples in the water). However, the effects are more complex in the power systems because of their irregular topology (i.e., non-Euclidean vertex domain) and complex interconnections based on the physics of electricity. While it is expected that the attributes of the nearby (geographical and topological) buses of the perturbed bus v_u get affected more than the far-away buses, deviation from this expectation is very common. In other words, the relationship between the geographical/topological distance and the perturbation effects is irregular. In the next section, the spreadability of the perturbation $\mathscr{U}$ is studied in terms of the location of the perturbation and the perturbation strength.

7.3 Effects of Single Bus Perturbation

7.3.1 Spreadability of Single Bus Perturbation

For analyzing the spreadability of perturbation $\mathscr{U}$ in the grid in terms of the bus attributes, we propose to evaluate the changes introduced in the bus voltage angle graph signal at the buses at different hop-distances from the perturbed bus, v_u. The mean of the signal values of $\psi(n)$ at all the vertices at $K - hop$ distance from the perturbed bus v_u specifies how the buses at $K - hop$ distance are affected on average by the perturbation. This can be expressed as:

$$\bar{\psi}_u^{(K)} = \frac{1}{|\mathcal{N}_u^{(K)}|} \sum_{n \in \mathcal{N}_u^{(K)}} \psi_u(n), \tag{7.10}$$

where $\mathcal{N}_u^{(K)} \subset \mathcal{V}$ is the set of the $K-$ hop neighbors of v_u. According to Property 1, $\psi_u(n)$ does not depend on the perturbation strength, $\bar{\psi}_u^{(K)}$ also does not depend on the perturbation strength under DC power flow assumptions.

Corollary 1.1. *Under the DC Power flow assumption, the $\bar{\psi}_u^{(K)}$ depends only on the topology.*

Proof: Substituting $\psi_u(n)$ from equation (7.9) into equation (7.10) results :

$$\bar{\psi}_u^{(K)} = \frac{1}{|\mathcal{N}_u^{(K)}|} \sum_{n \in \mathcal{N}_u^{(K)}} |\beta_{nu}|. \tag{7.11}$$

Therefore, under DC power flow model $\bar{\psi}_u^{(K)}$ does not depend upon the perturbation strength, γ, rather depends upon the perturbation location, v_u. As such, $\bar{\psi}_u^{(K)}$ can be calculated from the susceptance matrix, $\mathbf{B}^{-1}$. □

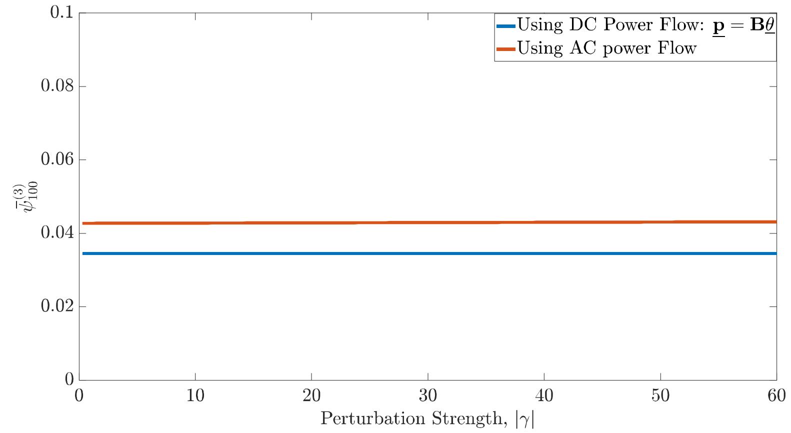


Figure 7.1: Average of the values of normalized difference voltage angle graph signal at 3-hop distance from the perturbation bus $v_u = 100$ for IEEE 118 bus system.

Figure 7.1 shows $\bar{\psi}_{100}^{(3)}$, the average of the values of normalized difference voltage angle graph signal calculated from the equation $\underline{\theta} = \mathbf{B}^{-1}\underline{\mathbf{p}}$ (DC power flow model) at $K = 3-$ hop distance from the perturbed bus number 100 of the IEEE 118 bus system. It can be observed that $\bar{\psi}_{100}^{(3)}$ is independent of the perturbation strength, γ. The results obtained from the AC power flow model in MATPOWER show a similar property, i.e., very weak dependence of $\bar{\psi}_{100}^{(3)}$ on γ. For the AC model results the value shows a slight variation (around 0.008 $degree/MW$) from the value obtained using DC power flow model.

The values of $\bar{\psi}_u^{(K)}$ show a decreasing trend as a function of K as illustrated in Figure 7.2 when calculated using the AC power flow model in MATPOWER. This behavior is expected as the effects of perturbation should spread and diminish from the source of the perturbation (i.e., v_u). Our experiments show that this decreasing trend is non-uniform over the grid and varies significantly depending on the location of the perturbation. Generally, a larger value of $\bar{\psi}_u^{(K)}$ at a far-away bus (i.e., a higher value of K) from the perturbation source indicates larger spreadability of the perturbation. Therefore, a flatter $\bar{\psi}_u^{(K)}$vs. K curve indicates greater spreadability of the perturbation. As such, to quantify the spreadability we propose to consider the slope of the best-fitted line (Figure 7.2, red straight line) to the $\bar{\psi}_u^{(K)}$vs. K curve as the *spreadability measure*, s. To this end, the spreadability measure due to the perturbation, $\mathscr{U}$ at bus v_u can be expressed as:

$$s(u) = \frac{1}{\mathscr{S}[\bar{\psi}_u^{(1)}, \bar{\psi}_u^{(2)}, \dots \bar{\psi}_u^{(D)}]}, \tag{7.12}$$

where $\mathscr{S}[\bar{\psi}_u^{(1)}, \bar{\psi}_u^{(2)}, \dots \bar{\psi}_u^{(D)}]$ denotes the negative slope of best-fitted lines to the points: $[\bar{\psi}_u^{(1)}, \bar{\psi}_u^{(2)}, \dots \bar{\psi}_u^{(D)}]$.

Corollary 1.2. *Considering the DC Power flow model, $s(u)$ depends only on the location of perturbation, $\mathscr{U}$.*

Proof: Since $\bar{\psi}_u^{(K)}$ is independent of γ as proved in equation (7.11), from equation (7.12), it can be shown that $s(u)$ is independent of γ and only a function of the perturbation location v_u under DC power flow assumptions. □

Figure 7.3(a) shows the spreadability measurement, $s(u)$ due to perturbation in different perturbation locations, $v_u \in \mathcal{L} \cup \mathcal{S}$ for a fixed perturbation strength. Although according

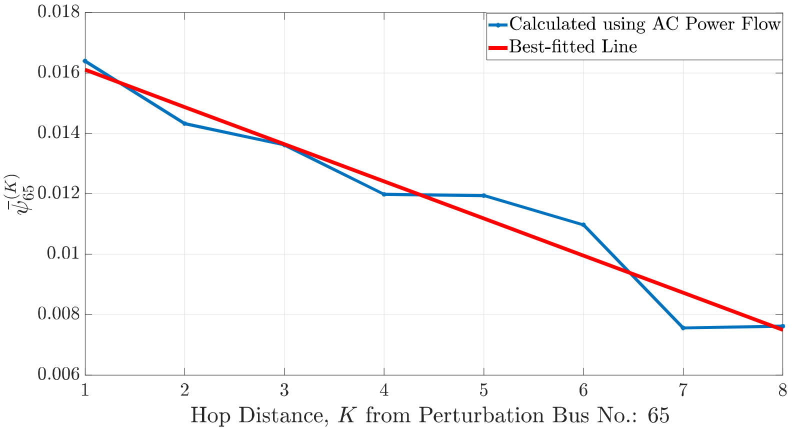


Figure 7.2: Average of the values of normalized difference voltage angle graph signal at different hop distances from the perturbation bus $v_u = 65$ for IEEE 118 bus system.

to the DC power flow model, our proposed measurement of spreadability $s(u)$ is strictly independent of the strength of perturbation, our simulation with the more realistic AC power flow model exhibits very small dependency on the perturbation strength and depends mostly on the perturbation location aligning with the theoretical analysis. Figure 7.3(a) illustrates how the effect of load perturbation in different load buses spreads through the grid as reflected in the bus voltage angle difference graph signals. This result can become useful in several real-life applications related to the maintenance, planning, and reliability of the smart grid. Firstly, it indicates the vulnerable buses for perturbation which the perturbation can cause a more spreadable event in the grid and cause greater damage. For example, from Figure 7.3(a) it is observable that the impact of a load perturbation at bus number 116 of the IEEE 118 bus system is spreadable through the grid than a load perturbation at any other bus in the grid. This observation can be useful for the planning of placement of renewable generations and low-inertia loads in the grid. Certain locations in the grid can be avoided from the consideration of renewable integration or EV connection depending on the analysis of the spreadability.

For comparing the results for the spreadability measure, $s(u)$ we have calculated the *spreadability* introduced in [138] in our case of load perturbation which is developed using a network-science-based approach and considering the difference voltage angle graph signal

$\Delta\underline{\theta}_u$ as the *mean displacement vector* as defined in [138]. According to the definition of spreadability in [138], the *spreadability,* $s'(u)$ can be defined as:

$$s'(u) = C'(u) \sum_{i=1}^{N} \frac{\Delta\theta_u(i)}{\sum_{j=1}^{N} \Delta\theta_u(j)} \mathscr{D}(v_u, v_i), \tag{7.13}$$

where, $\mathscr{D}(v_u, v_i)$ is the shortest path length between the perturbation bus v_u and all the buses $v_i \in \mathcal{V}$ calculated from the graph $\mathcal{G}'(\mathcal{V}, \mathcal{E})$ which can be obtained by ignoring the weights of the graph $\mathcal{G}$ but containing same sets of vertices and edges, and $C'(u)$ is the *modified normalized closeness centrality* as proposed in [138]:

$$C'(n) = \frac{N}{\sum_{\forall v_i \in \mathcal{V}} \mathscr{D}(v_n, v_i)}. \tag{7.14}$$

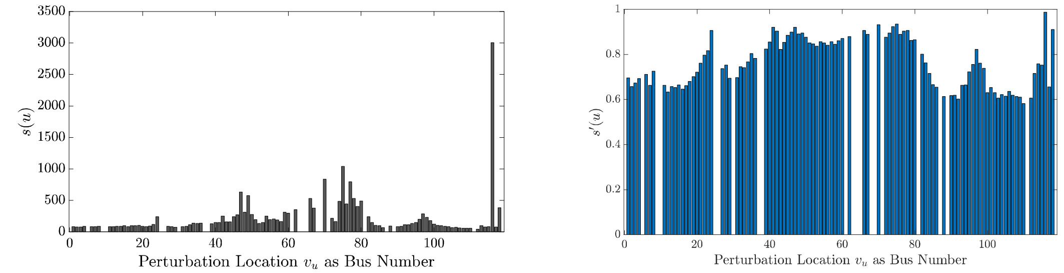
Corollary 1.3. *Considering the DC Power flow model, $s'(u)$ is independent of the perturbation strength γ.*

Proof: By plugging the expression of $\Delta\theta_u(n)$ from the equation (7.8) to the equation (7.14) we obtain:

$$s'(u) = C'(u) \sum_{i=1}^{N} \frac{|\beta_{iu}|}{\sum_{j=1}^{N} |\beta_{ju}|} \mathscr{D}(v_u, v_i), \tag{7.15}$$

The terms $C'(u)$ and $\mathscr{D}(v_u, v_i)$ is calculated from the unweighted graph $\mathcal{G}'$ for a certain perturbation location v_u and therefore, depends only upon the interconnections among the buses of the grid while the β_{ij} terms are related to the electrical parameters of the transmission line. Therefore, for a particular electrical grid, $s'(u)$ depends on the location of the perturbation and is independent of the perturbation strength. □

Our proposed GSP-based spreadability measurement $s(n)$ and the network-science-based spreadability $s'(u)$ shows similarity up to a certain level for a perturbation of 50 MW real power load perturbation at every bus as illustrated in Figure 7.3(a) and Figure 7.3(b). The similarity is quantified by a *Spearman's correlation coefficient* [141] of 0.8562 with no tied rank and a $p - value$ of 0.



(a) (b)

Figure 7.3: Spreadability indices for a load perturbation of 50 MW in different buses of IEEE 118 bus system. The Spreadability indices are calculated as in (a) equation (7.12) which is our proposed measure of spreadability, (b) equation (7.15) which is proposed in Buttner *et. al.* [138]. The MATPOWER default loads and generations are considered as the pre-perturbation real power, $p(n, t_u - \epsilon)$. The similarity between (a) and (b) from visual inspection might be challenging, however, their similarity can be justified by the Spearman rank correlation coefficient of 0.8562.

The spreadability metric $s(n)$ provides a relative measure of how the effect of a single perturbation can spread through the electric grid depending on the location of the perturbation. This metric is important in analyzing the effects of perturbation in the grid, which can also be helpful in determining the optimum location for placing renewable sources and batteries [142]. In addition to evaluating the spreadability due to perturbations, it is important to evaluate other graph signal properties, which may be affected by the perturbations and may encode important information about the behavior of the system under perturbation. The global smoothness of graph signals describes the variation of values over buses in an aggregate form. Next, the effects of perturbation on the global smoothness of the bus voltage angle graph signals are discussed. In this analysis, load changes are considered as the main kind of perturbation.

Property 2. *Under the DC Power flow assumption, the global smoothness of the voltage angle graph signal is a quadratic function of the increased load.*

Proof: Let us start by writing the definition of the global smoothness for the voltage angle graph signal $\underline{\theta}$ and use the DC power flow model to expand the definition of $\underline{\theta}$ as follows:

$$\begin{aligned} g_\theta &= \frac{\underline{\theta}^T \mathbf{L} \underline{\theta}}{\underline{\theta}^T \underline{\theta}} \\ &= \frac{\left(\mathbf{B}^{-1}\underline{\mathbf{p}}\right)^T \mathbf{L} \left(\mathbf{B}^{-1}\underline{\mathbf{p}}\right)}{\left(\mathbf{B}^{-1}\underline{\mathbf{p}}\right)^T \left(\mathbf{B}^{-1}\underline{\mathbf{p}}\right)} \\ &= \frac{\underline{\mathbf{p}}^T \left(\mathbf{B}^{-1}\right)^T \mathbf{L}\mathbf{B}^{-1}\underline{\mathbf{p}}}{\underline{\mathbf{p}}^T \left(\mathbf{B}^{-1}\right)^T \mathbf{B}^{-1}\underline{\mathbf{p}}} \\ &= \frac{\underline{\mathbf{p}}^T \mathbf{Q} \underline{\mathbf{p}}}{\underline{\mathbf{p}}^T \mathbf{R} \underline{\mathbf{p}}} \end{aligned} \tag{7.16}$$

Here, $\mathbf{Q} = \left(\mathbf{B}^{-1}\right)^T \mathbf{L}\mathbf{B}^{-1}$ and $\mathbf{R} = \left(\mathbf{B}^{-1}\right)^T \mathbf{B}^{-1}$, both contain topological information and are independent of $\underline{\mathbf{p}}$. Since the other elements of the vector $\underline{\mathbf{p}}$, except the $u-$th element, are the same before and after the perturbation, $\mathscr{U}$ (as described in Section 7.2), g_θ is a *quadratic function* of the real power $p(u, t_u)$ at the perturbed bus $v_u \in \mathcal{V}$. Specifically, from equation (7.4) and equation (7.5), the global smoothness can be written as:

$$\begin{aligned} & g_\theta \propto p^2\left(u, t_u\right) \\ & \Rightarrow g_\theta \propto \left[p^2\left(u, t_u - \epsilon\right) + \gamma^2 + 2\gamma p\left(u, t_u - \epsilon\right)\right] \\ & \Rightarrow g_\theta \propto \gamma^2 + 2\gamma p\left(u, t_u - \epsilon\right) \end{aligned} \tag{7.17}$$

Therefore, g_θ is a quadratic function of γ. Figure 7.4 shows g_θ as a function of perturbation strength γ for load perturbation at bus number 16 of the 118 IEEE bus systems. The values of g_θ are calculated using equation (7.2) with the values of $\theta(n)$ obtained from the AC power flow model in MATPOWER. Although Property 2 is derived under the DC power flow assumption, Figure 7.4 shows that it also holds for the AC power flow (although with some numerical deviation). The quadratic form of g_θ as the function of perturbation strength can have important implications. For instance, our experiments have shown that an increasing trend in g_θ may indicate a stressed system. Specifically, the power grid bus voltage

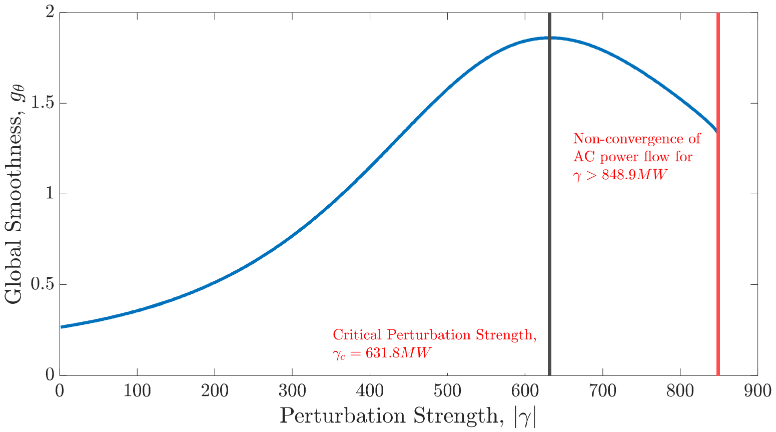


Figure 7.4: Global smoothness of the bus voltage angle graph signal as a function of perturbation strength in case of real-power load perturbation at bus 102 of IEEE 118 bus system calculated using AC power flow in MATPOWER. At the critical perturbation, γ_c the global smoothness is maximum and begins to drop beyond it. Any increase of perturbation strength beyond γ_{nc} the power flow becomes non-convergent.

angle graph signal is generally smooth over the vertices under normal operating conditions [26, 22]. Therefore the value of g_θ generally stays small, while the actual value depends on several factors, such as the system topology, load demand, and generation amount in the system. From Figure 7.4 it can be observed that when the load is increasing continually at a particular bus, initially g_θ increases with the increasing load, which indicates increasing fluctuations of signal values from vertex-to-vertex until the perturbation strength reaches a critical point γ_c (associated with a critical load demand of $p_{d_c}(u)$) for the perturbed bus, v_u. Increasing the load beyond this critical point results in decreasing values of g_θ, which in general can indicate smoother signal and normal grid conditions. However, in this particular case, the decrease in the global smoothness after reaching its maximum suggests a stressed system, and the issue of non-convergence of the AC power flow calculations rise in this phase. Moreover, the increase of, $p_d(u)$, i.e., γ, at the perturbed bus increases the power flow through a number of transmission lines. Increasing the size of perturbation can lead to overloading of transmission lines and outages and in severe cases cascading failures.

Application 2.1. *Determining the critical value of perturbation strength, γ for smooth grid operation.*

The critical value of the perturbation strength, γ, which also corresponds to the critical load size at bus v_u can be identified based on the maximum values of g_θ as follows:

$$\frac{\partial g_\theta}{\partial p(u)}\Big|_{p_d(u)=p_{d_c}(u)} = \frac{\partial g_\theta}{\partial p(u)}\Big|_{\gamma=\gamma_c} = 0 \tag{7.18}$$

By substituting equation (7.16) into equation (7.18) and applying the rules of matrix differentiation:

$$\underline{\mathbf{p}}^T\mathbf{Q}\underline{\mathbf{p}}\frac{\partial g_\theta}{\partial p(u)}(\underline{\mathbf{p}}^T\mathbf{R}\underline{\mathbf{p}}) = \underline{\mathbf{p}}^T\mathbf{R}\underline{\mathbf{p}}\frac{\partial g_\theta}{\partial p(u)}(\underline{\mathbf{p}}^T\mathbf{Q}\underline{\mathbf{p}}) \tag{7.19}$$

By solving the equation for $p(u)$ which is the same as the $u-$th element of $\underline{\mathbf{p}}$ the value of real power for which g_θ is maximum can be obtained, and therefore the critical perturbation strength γ_c can be obtained by equation (7.5).

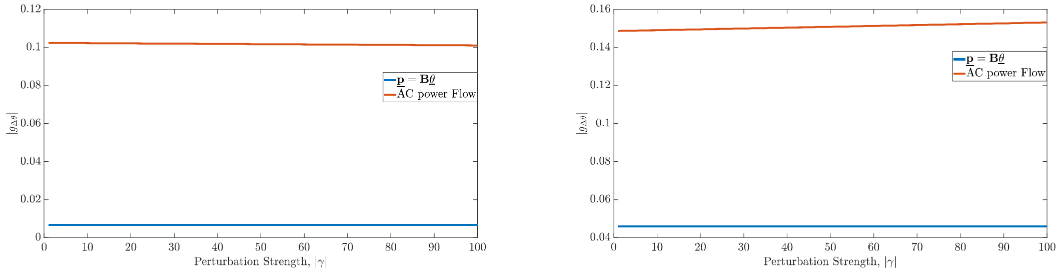
Figure 7.4 shows g_θ for monotonous load increase at bus 17 of the IEEE 118 bus system (which is purely a load bus). The result presented in this figure suggests that the perturbation strength of $\gamma_c = 631.8MW$ results in the maximum g_θ value and corresponds to our defined critical load. This critical load advises on a stressed system for which the power flow non-convergence based on the numerical results occurred at the perturbation strength of $\gamma_{nc} = 848.9$ corresponding to a load size of 853.9 MW.

Property 3. *Under the DC Power flow assumption the global smoothness of the difference voltage angle graph signal, $\Delta\theta$ is independent of the perturbation strength.*

Proof: Following the definition of global smoothness in equation (7.2), the global smoothness of the difference bus voltage angle graph signal $\Delta\theta_u(n)$ before and after the perturbation $\mathscr{U}$ can be written as:

$$g_{\Delta\theta} = \frac{\sum_{i=1}^N \sum_{j=1}^N L_{ij}\Delta\theta_u(i)\Delta\theta_u(j)}{\sum_{k=1}^N \Delta\theta_u^2(k)} \tag{7.20}$$

By substituting the $\Delta\theta_u(n)$ from the result expressed in equation (7.8) we obtain:



(a) (b)

Figure 7.5: The absolute value of global smoothness of the difference bus voltage angle graph signal before and after the perturbation as a function of perturbation strength γ. Both analytical (under DC power flow assumption) and simulation (using AC power flow) results are shown for (a) load perturbation in bus number 8 and (b) generation perturbation in bus number 10 of IEEE 118 bus system. The results show that $|g_{\Delta\theta}|$ is purely independent for the DC power assumption based power flow calculation using $\underline{\mathbf{p}} = \mathbf{B}\underline{\theta}$ and shows a very slight dependency on γ for more realistic AC power flow based simulation in both perturbation cases.

$$\begin{aligned} g_{\Delta\theta} &= \frac{\sum_{i=1}^{N}\sum_{j=1}^{N} L_{ij}\,|\gamma\beta_{iu}|\,|\gamma\beta_{ju}|}{\sum_{k=1}^{N}|\gamma\beta_{ku}|\,|\gamma\beta_{ku}|} \\ &= \frac{\sum_{i=1}^{N}\sum_{j=1}^{N} L_{ij}\,|\beta_{iu}\beta_{ju}|}{\sum_{k=1}^{N}|\beta_{ku}|^{2}}. \end{aligned} \tag{7.21}$$

Since there is no γ present on the right-hand side of the equation, $g_{\Delta\theta}$ does not depend on the perturbation strength but rather depends on the topology of the network. □

This GSP-based property associated with both real power load perturbation (Figure 7.5(a)) and real power generation perturbation (Figure 7.5(b)) has been justified by simulation on IEEE 118 bus system. From Figure 7.5 it can be observed that in perturbations in both cases, power flow calculation using $\underline{\mathbf{p}} = \mathbf{B}\underline{\theta}$ under DC power flow yields purely horizontal $|g_{\Delta\theta}|$ vs. γ curve which indicates strict independence of perturbation strength. The more realistic AC power flow also justifies this property, however, shows a slight dependency on perturbation strength.

This property enables $g_{\Delta\theta}$ to be a GSP-based indicator for comparing perturbation in different locations in the grid. Figure 7.6 shows the values for $g_{\Delta\theta}$ for a perturbation of $\gamma = 50MW$ in each of the load buses of the IEEE 118 bus system. It is clear that load

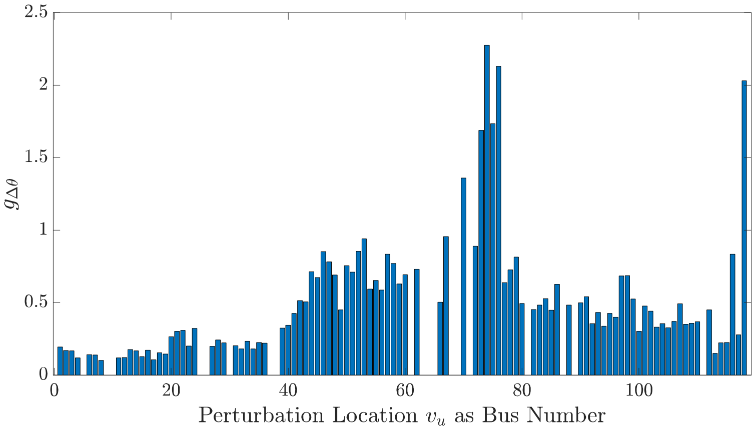


Figure 7.6: Global smoothness of the difference bus voltage angle graph signal before and after the perturbation for the same amount of load perturbation $\gamma = 50MW$ in each of the load buses of IEEE 118 bus system.

perturbations of the same strength on different buses have different degrees of effects in the grid which is reflected in the graph signal $\Delta\theta(n)$ and its smoothness. Since the graph signal $\Delta\theta(n)$ by being a difference graph signal before and after the perturbation, inherently contains time evolution information to a certain degree and can be indicators of spreading patterns of the effect of perturbations. This can also be understood from the visual resemblance of the bar diagram of $g_{\Delta\theta}$ in Figure 7.6 with the bar diagram of our proposed spreadability measure, $s(u)$ in Figure 7.3. The similarity between $g_{\Delta\theta}$ and $s(u)$ can be also justified by the *cosine similarity* of 0.8281 and *Spearman rank correlation co-efficient* of 0.61 for $\gamma = 50MW$ perturbations in all the load buses of IEEE 118 bus system. Therefore, the GSP-based parameter $g_{\Delta\theta}$ can be an indicator of locational dependency of perturbations in the grid, especially to estimate the spreadability of the perturbation effects. Similar results can be observed in the local smoothness of the graph signal $\Delta\theta_u(n)$.

Property 4. *Under the DC Power flow assumption the local smoothness of the difference voltage angle graph signal at any vertex, $\Delta\theta$ is independent of the perturbation strength.*

Proof: From equation (7.3), the local smoothness at bus n of the difference bus voltage angle graph signal $\Delta\theta_u(n)$ before and after the perturbation $\mathscr{U}$:

$$l_{\Delta\theta}(n) = \frac{\sum_{k=1}^{N} L_{nk}\Delta\theta_u(k)}{\Delta\theta_u(n)}, \Delta\theta_u(n) \neq 0 \tag{7.22}$$

By substituting the $\Delta\theta_u(n)$ from equation (7.8) we obtain:

$$l_{\Delta\theta}(n) = \frac{\sum_{k=1}^{N} L_{nk}|\gamma\beta_{ku}|}{|\gamma\beta_{nu}|} = \frac{\sum_{k=1}^{N} L_{nk}|\beta_{ku}|}{|\beta_{nu}|}, \quad \Delta\theta(n) \neq 0 \tag{7.23}$$

Equation (7.23) provides the local smoothness values of $\Delta\theta_u(n)$ at any vertex, v_n of the graph. The local smoothness values at the perturbation bus can be obtained by putting $n = u$ in equation (7.23):

$$l_{\Delta\theta}(u) = \frac{\sum_{k=1}^{N} L_{uk}\beta_{ku}}{\beta_{uu}}, \beta_{uu} \neq 0 \tag{7.24}$$

which is independent of the perturbation strength. □

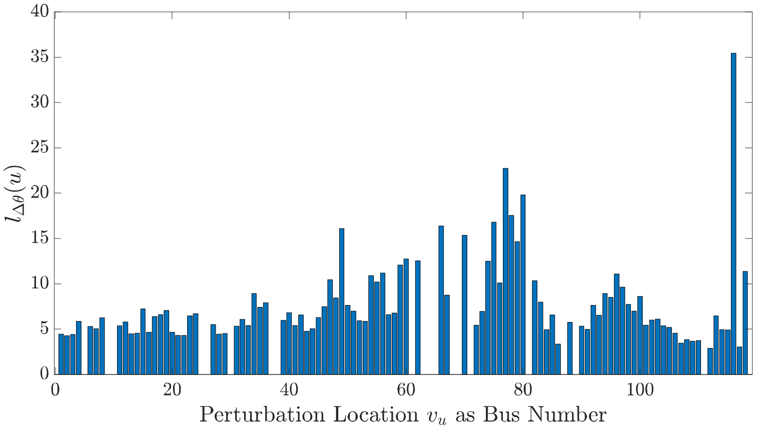


Figure 7.7: Local smoothness values at the perturbation vertex of the difference bus voltage angle graph signal before and after the perturbation for the same amount of load perturbation $\gamma = 50MW$ in each of the load buses of IEEE 118 bus system.

The independence of the perturbation strength makes $l_{\Delta\theta}(u)$ suitable for analysis of locational dependence of perturbations in the grid similar to $g_{\Delta\theta}$. Similar to $g_{\Delta\theta}$, the local smoothness value of the difference bus voltage angle graph signal before and after the perturbation evaluated at the perturbation point can be served as an estimator of the spreadability of the perturbation effect. Figure 7.7 shows the values of local smoothness at the perturbation vertices due to the same amount of load perturbation $\gamma = 50MW$ at each load bus of the IEEE 118 bus system. The bar diagram of $I_{\Delta\theta}(u)$ seems similar to the bar diagram of our proposed spreadability measure, $s(u)$ for the IEEE 118 bus system. The cosine similarity and the Spearman rank correlation coefficient between $s(u)$ and $I_{\Delta\theta}(u)$ for 50 MW perturbations are, respectively, 0.8925 and 0.66, which justifies $I_{\Delta\theta}(u)$ as a GSP-based estimator of perturbation spreads.

Chapter 8: Conclusion and Future Work

This dissertation discusses the importance of situational awareness in the context of modern smart grids. By utilizing graph signal processing and energy data analytic techniques, several specific problems related to the security and reliability of the smart grid are studied. The main goal was to capture the dynamic interactions among the components of the grid from the available data using analytical tools and apply the knowledge to improve the security and reliability of smart grids. The experimental results show that the proposed techniques provide very effective solutions to the security and reliability-related problems in power systems in specific situations with the available data. Moreover, the proposed techniques are analytically evaluated and verified using simulation-based analysis. There are several directions in which the research in this dissertation can be extended to further improve situational awareness in ever-evolving smart grids. This chapter concludes the dissertation with concluding remarks on all the considered applications and discusses future work scopes in each direction.

8.1 Concluding Remarks

In this dissertation, the problem of detecting different cyber attacks and physical anomalies and stresses has been studied by using both the state-correlation approach and the GSP-based analysis. For both approaches, the power system states (i.e., bus voltage angles) are considered as multivariate time series. In the state-correlation-based approach, it has been shown that the instantaneous correlation matrix, which captures the correlation among the state of the components, bears important information about the dynamics and stresses in the system. Visualizing the instantaneous correlation matrix image can provide a simple yet effective tool for detecting and locating stresses in the real-time monitoring of the power grid. Further, a $k-$NN classification method has been developed using features extracted from the instantaneous correlation matrix to detect various types of cyber-attacks as well as single-line failures in the system. The presented method shows promising performance and sheds light on the importance of the correlation information among the state of components in the system. In the GSP-based approach, energy graph signals are 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 graph 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 techniques can perform well in locating the stresses.

Once a stress or anomaly is detected and located in the smart grid, its characterization, and classification are crucial for the prompt mitigation of the damage, as well as for perceiving the intention and strategy of the attacker. It has been shown that along with the detection and locating of the cyber stresses in the grid, the GSP-based features extracted from the graph signals associated with the electrical attributes of the buses at the moment of detection or its temporal vicinity are effective for their characterization and classification. A two-stage classification framework for classifying cyber and physical stresses in the smart grid has been proposed based on the learning of the power system's graph signal features. This approach involves combining GSP-based 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 the temporal information in the signals into the 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 GFT-based features has also been proposed based on down-sampling the graph frequency domain for efficient implementation of the classification techniques. Moreover, it has been shown that the GSP-based features, especially the local smoothness-based features are effective in classifying clustered and random multiple cyber attacks and estimating the center and radius of the clustered attacks.

For recovering bus voltage angle graph signal values at the unobservable buses at a single time instant using the signal values at the observable buses, the graph signal sampling-reconstruction framework has been utilized under the band-limited graph signal assumptions. This technique successfully recovers missing signal values with good accuracy. For relaxing the band-limitation assumption, our further work proposes a novel technique for reconstructing graph signals for the power system's state recovery problem. The proposed technique specifically utilizes the local dynamics of the system through the local smoothness of the system's graph signals. The statistics of the local smoothness measures along with the assumption of globally smooth graph signals are used to formulate an optimization problem for the state recovery problem. The key advantage of the proposed technique is that it relaxes the band-limited signal assumption for reconstructing graph signals. Simulation results for the IEEE 118 bus system show promising accuracy and performance in recovering the unobservable states. For recovering states for a duration of time, a state-correlation-based approach has been proposed in which the time-varying states inside the unobservable zone from the dynamic states of components outside the attack zone by using the correlations among the states. The accuracy of the estimation is compared using the mean squared error (MSE) between the estimated time series and the ground truth for the DoS duration. The MSEs for the different numbers of unobservable states have been compared. The relative vulnerability of the locations of the PMUs and the relative vulnerability of the time of the day from the attackers' perspective have been analyzed based on the calculated MSEs.

The optimum sensor (e.g., PMU) placement strategy in the grid has also been studied under the graph signal sampling-reconstruction framework by considering it as a sampling set selection problem. Several criteria based on the topology and power-dynamical properties of the electric grid for selecting the sampling set have been studied to evaluate their effects on the graph signal reconstruction performance. Specifically, a criterion based on the anti-aliasing filter error has been proposed that minimizes the reconstruction error of sampling. The anti-aliasing filter error-based criterion modified according to the power grid reality has been proposed for PMU placement to minimize the measurement reconstruction error.

The work on single-bus perturbation presents a GSP-based analysis of the effect of the real-power perturbation associated with a single bus on the electric grid in terms of how the effects of the perturbation spread throughout the grid and how the associated graph signals behave depending on the location and strength of the perturbation. This work is based on a few assumptions (e.g., DC power flow) and considers a perturbation model, which is simple and generic. Nevertheless, this work provides interesting and important insights into the effects of perturbation in the grid and opens the door to viewing many modern-day electric grid problems as perturbation analysis using GSP.

8.2 Future Work

In this section, the future research scopes in the studied applications have been discussed. The scopes include implementing the proposed techniques on more challenging stress scenarios and more detailed system and data models, considering larger electric grids, and solving problems related to computational resources. In the case of large data availability, many problems with the GSP measurement model can also be explored with the training-based graph neural networks (GNN).

8.2.1 Detection and Location Identification of Cyber and Physical Stresses

There are a few directions in which the detection and location identification research can be extended considering both the state correlation-based and the GSP-based approaches. Noise effect analysis on the performance of the GSP-based methods can be an interesting topic for future studies. In the current works, only the noise, implicitly present in the load profiles, is considered. Secondly, stresses causing topology changes are not considered in this GSP-based work 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 computationally efficient implementation techniques or the development of complementing techniques, such as augmented graphs with reduced domain and grid partitioning, to allow VFED application to a smaller model for stress localization.

8.2.2 Characterization and Classification of Cyber and Physical Stresses

New and diverse physical stresses and cyber attacks can be considered for classification and characterization. The characterization of physical stresses with the determination of stress center and root cause analysis can be future work direction. For sophisticated cyber attacks, a deeper characterization can be considered by estimating the parameters of the attack models.

8.2.3 Recovery of the Unobservable States and Optimum Placement of Measurement Devices

Extending this study for recovering the states of the grid under topology change and cyber-physical attack under optimum PMU placement can be considered as prospective future work. Moreover, the PMU placement strategy can be studied from other observability perspectives (e.g., fault detection) considering different electrical attributes (e.g., current and frequency).

8.2.4 Characterization of Single Bus Perturbation in Smart Grids

This work can be extended in several directions to make the approach suitable for analyzing various complex dynamics in power systems. Perturbation analysis using graph signals beyond bus voltage angle (e.g., instantaneous frequency, rate of change of frequency, injected real or reactive power, etc.) would be a prospective extension of the current work for better capturing of the grid dynamics. Considering grid inertia in GSP-based analysis is another research direction that can be explored. The critical load value and the divergence points analyzed in this work can be related to the instability, islanding, and collapse of the grid, and associated GSP parameters (e.g., smoothness) can be predictors of grid conditions. Future research may include exploring these relationships.

References

[1] Xi Fang, Satyajayant Misra, Guoliang Xue, and Dejun Yang. Smart grid — the new and improved power grid: A survey. *IEEE Communications Surveys Tutorials*, 14(4):944–980, 2012.

[2] Muhammad Nouman Nafees, Neetesh Saxena, Alvaro Cardenas, Santiago Grijalva, and Pete Burnap. Smart grid cyber-physical situational awareness of complex operational technology attacks: A review. *ACM Comput. Surv.*, 55(10), Feb 2023.

[3] *Advanced Data Analytics for Power Systems.* Cambridge University Press, 2021.

[4] Antonio Ortega, Pascal Frossard, Jelena Kovačević, José M. F. Moura, and Pierre Vandergheynst. Graph signal processing: Overview, challenges, and applications. *Proceedings of the IEEE*, 106(5):808–828, 2018.

[5] David I Shuman, Sunil K. Narang, Pascal Frossard, Antonio Ortega, and Pierre Vandergheynst. The emerging field of signal processing on graphs: Extending high-dimensional data analysis to networks and other irregular domains. *IEEE Signal Processing Magazine*, 30(3):83–98, 2013.

[6] Antonello Monti, Carlo Muscas, and Ferdinanda Ponci. *Phasor measurement units and wide area monitoring systems.* Academic Press, 2016.

[7] Jiaqi Shi, Liya Ma, Chenchen Li, Nian Liu, and Jianhua Zhang. A comprehensive review of standards for distributed energy resource grid-integration and microgrid. *Renewable and Sustainable Energy Reviews*, 170:112957, 2022.

[8] Xiaohui Li, Zhenpo Wang, Lei Zhang, Fengchun Sun, Dingsong Cui, Christopher Hecht, Jan Figgener, and Dirk Uwe Sauer. Electric vehicle behavior modeling and applications in vehicle-grid integration: An overview. *Energy*, 268:126647, 2023.

[9] Chih-Che Sun, Adam Hahn, and Chen-Ching Liu. Cyber security of a power grid: State-of-the-art. *International Journal of Electrical Power & Energy Systems*, 99:45–56, 2018.

[10] Md Musabbir Hossain and Chen Peng. Cyber–physical security for on-going smart grid initiatives: a survey. *IET Cyber-Physical Systems: Theory & Applications*, 5(3):233–244, 2020.

[11] Reza Arghandeh, Alexandra von Meier, Laura Mehrmanesh, and Lamine Mili. On the definition of cyber-physical resilience in power systems. *Renewable and Sustainable Energy Reviews*, 58:1060–1069, 2016.

[12] Jose Cordova, Reza Arghandeh, Yuxun Zhou, Sergiusz Wesolowski, Wei Wu, and Stifter Matthias. Shape-based data analysis for event classification in power systems. In *IEEE Manchester PowerTech*, pages 1–6, 2017.

[13] Rui Ma, Sagnik Basumallik, and Sara Eftekharnejad. A pmu-based data-driven approach for classifying power system events considering cyberattacks. *IEEE Systems Journal*, 14(3):3558–3569, 2020.

[14] Pengzhi Gao, Meng Wang, Scott G. Ghiocel, Joe H. Chow, Bruce Fardanesh, and George Stefopoulos. Missing data recovery by exploiting low-dimensionality in power system synchrophasor measurements. *IEEE Transactions on Power Systems*, 31(2):1006–1013, 2016.

[15] Denis Osipov and Joe H. Chow. Pmu missing data recovery using tensor decomposition. *IEEE Transactions on Power Systems*, 35(6):4554–4563, 2020.

[16] Nadia H.A. Rahman and Ahmed F. Zobaa. Optimal pmu placement using topology transformation method in power systems. *Journal of Advanced Research*, 7(5):625–634, 2016.

[17] Prachi Mafidar Joshi and H.K. Verma. Synchrophasor measurement applications and optimal pmu placement: A review. *Electric Power Systems Research*, 199:107428, 2021.

[18] Kevin Schultz, Marisel Villafañe-Delgado, Elizabeth P. Reilly, Grace M. Hwang, and Anshu Saksena. Graph signal processing for infrastructure resilience: Suitability and future directions. In *2020 Resilience Week (RWS)*, pages 64–70, 2020.

[19] Ireneusz Jabłoński. Graph signal processing in applications to sensor networks, smart grids, and smart cities. *IEEE Sensors Journal*, 17(23):7659–7666, 2017.

[20] Leah Goldsberry, Weiyu Huang, Nicholas F. Wymbs, Scott T. Grafton, Danielle S. Bassett, and Alejandro Ribeiro. Brain signal analytics from graph signal processing perspective. In *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pages 851–855, 2017.

[21] Sarah Itani and Dorina Thanou. A graph signal processing framework for the classification of temporal brain data. In *28th European Signal Processing Conference (EUSIPCO)*, pages 1180–1184, 2021.

[22] Raksha Ramakrishna and Anna Scaglione. Grid-graph signal processing (grid-gsp): A graph signal processing framework for the power grid. *IEEE Transactions on Signal Processing*, 69:2725–2739, 2021.

[23] Sivan Grotas, Yair Yakoby, Idan Gera, and Tirza Routtenberg. Power systems topology and state estimation by graph blind source separation. *IEEE Transactions on Signal Processing*, 67(8):2036–2051, 2019.

[24] Ray Daniel Zimmerman, Carlos Edmundo Murillo-Sánchez, and Robert John Thomas. Matpower: Steady-state operations, planning, and analysis tools for power systems research and education. *IEEE Transactions on Power Systems*, 26(1):12–19, 2011.

[25] Load data, new york independent system operator. https://www.nyiso.com/load-data, Accessed: June 21, 2023.

[26] Md Abul Hasnat and Mahshid Rahnamay-Naeini. A graph signal processing framework for detecting and locating cyber and physical stresses in smart grids. *IEEE Transactions on Smart Grid*, 13(5):3688–3699, 2022.

[27] Md Abul Hasnat and Mahshid Rahnamay–Naeini. Reflection of cyber and physical stresses in smart grids on their graph signals. In *IEEE PES Innovative Smart Grid Technologies Europe (ISGT Europe)*, pages 01–05, 2021.

[28] Md Abul Hasnat and Mahshid Rahnamay-Naeini. Sampling of power system graph signals. In *IEEE PES Innovative Smart Grid Technologies Europe (ISGT Europe)*, pages 01–06, 2021.

[29] Md Abul Hasnat and Mahshid Rahnamay-Naeini. Characterization and classification of cyber attacks in smart grids using local smoothness of graph signals. In *North American Power Symposium (NAPS)*, pages 01–06, 2021.

[30] Md Abul Hasnat and Mia Naeini. Learning power system's graph signals for cyber and physical stress classification. In *North American Power Symposium (NAPS)*, pages 1–6, 2022.

[31] Md Abul Hasnat and Mahshid Rahnamay-Naeini. Detection and locating cyber and physical stresses in smart grids using graph signal processing. *arXiv:2006.06095v1.*

[32] Vertex-frequency analysis on graphs. *Applied and Computational Harmonic Analysis*, 40(2):260–291, 2016.

[33] LJ. Stanković, D. Mandic, M. Daković, M. Brajović, B. Scalzo-Dees, S. Li, and A.G. Constantinides. *Data Analytics on Graphs.* NOW publishers, February 2021.

[34] Le Trung Thanh, Nguyen Linh-Trung, Nguyen Viet Dung, and Karim Abed-Meraim. A new windowed graph fourier transform. In *4th NAFOSTED Conference on Information and Computer Science*, pages 150–155, 2017.

[35] David K. Hammond, Pierre Vandergheynst, and Rémi Gribonval. Wavelets on graphs via spectral graph theory. *Applied and Computational Harmonic Analysis*, 30(2):129–150, 2011.

[36] Francesco Grassi, Andreas Loukas, Nathanaël Perraudin, and Benjamin Ricaud. A time-vertex signal processing framework: Scalable processing and meaningful representations for time-series on graphs. *IEEE Transactions on Signal Processing*, 66(3):817–829, 2018.

[37] Elvin Isufi, Andreas Loukas, Nathanaël Perraudin, and Geert Leus. Forecasting time series with varma recursions on graphs. *IEEE Transactions on Signal Processing*, 67(18):4870–4885, 2019.

[38] Karthik Gopalakrishnan, Max Z. Li, and Hamsa Balakrishnan. Identification of outliers in graph signals. In *IEEE 58th Conference on Decision and Control (CDC)*, pages 4769–4776, 2019.

[39] Arman Hasanzadeh, Xi Liu, Nick Duffield, Krishna R Narayanan, and Byron Chigoy. A graph signal processing approach for real-time traffic prediction in transportation networks. *arXiv preprint arXiv:1711.06954*, 2017.

[40] Seyed Saman Saboksayr, Gonzalo Mateos, and Mujdat Cetin. Eeg-based emotion classification using graph signal processing. In *ICASSP 2021 - 2021 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pages 1065–1069, 2021.

[41] Priyanka Mathur and Vijay Kumar Chakka. Graph signal processing based cross-subject mental task classification using multi-channel eeg signals. *IEEE Sensors Journal*, 22(8):7971–7978, 2022.

[42] Vijay Kumar Sharma, Devesh Kumar Srivastava, and Pratistha Mathur. Efficient image steganography using graph signal processing. *IET Image Processing*, 12(6):1065–1071, 2018.

[43] Weiyu Huang, Thomas A. W. Bolton, John D. Medaglia, Danielle S. Bassett, Alejandro Ribeiro, and Dimitri Van De Ville. A graph signal processing perspective on functional brain imaging. *Proceedings of the IEEE*, 106(5):868–885, 2018.

[44] Elisabeth Drayer and Tirza Routtenberg. Detection of false data injection attacks in smart grids based on graph signal processing. *IEEE Systems Journal*, 14(2):1886–1896, 2020.

[45] Hilmi E. Egilmez and Antonio Ortega. Spectral anomaly detection using graph-based filtering for wireless sensor networks. In *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pages 1085–1089, 2014.

[46] Ariel Kroizer, Yonina C. Eldar, and Tirza Routtenberg. Modeling and recovery of graph signals and difference-based signals. In *IEEE Global Conference on Signal and Information Processing (GlobalSIP)*, pages 1–5, 2019.

[47] Shammya Shananda Saha, Anna Scaglione, Raksha Ramakrishna, and Nathan G. Johnson. Distribution systems ac state estimation via sparse ami data using graph signal processing. *IEEE Transactions on Smart Grid*, 13(5):3636–3649, 2022.

[48] Oureste Elias Batista Mariana Altoé Mendes, Marcia Helena Moreira Paiva. Signal processing on graphs for estimating load current variability in feeders with high integration of distributed generation. *Sustainable Energy, Grids and Networks*, 34:101032, 2023.

[49] Zonghan Wu, Shirui Pan, Fengwen Chen, Guodong Long, Chengqi Zhang, and Philip S. Yu. A comprehensive survey on graph neural networks. *IEEE Transactions on Neural Networks and Learning Systems*, 32(1):4–24, 2021.

[50] Alaa Bessadok, Mohamed Ali Mahjoub, and Islem Rekik. Graph neural networks in network neuroscience. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 45(5):5833–5848, 2023.

[51] Felix Wu, Amauri Souza, Tianyi Zhang, Christopher Fifty, Tao Yu, and Kilian Weinberger. Simplifying graph convolutional networks. In Kamalika Chaudhuri and Ruslan Salakhutdinov, editors, *Proceedings of the 36th International Conference on Machine Learning*, volume 97 of *Proceedings of Machine Learning Research*, pages 6861–6871. PMLR, 09–15 Jun 2019.

[52] Chuanpan Zheng, Xiaoliang Fan, Shirui Pan, Haibing Jin, Zhaopeng Peng, Zonghan Wu, Cheng Wang, and Philip S. Yu. Spatio-temporal joint graph convolutional networks for traffic forecasting. *IEEE Transactions on Knowledge and Data Engineering*, pages 1–14, 2023.

[53] Md Jakir Hossain and Mahshid Rahnamay–Naeini. State estimation in smart grids using temporal graph convolution networks. In *2021 North American Power Symposium (NAPS)*, pages 01–05, 2021.

[54] Huayi Wu, Zhao Xu, and Minghao Wang. Unrolled spatiotemporal graph convolutional network for distribution system state estimation and forecasting. *IEEE Transactions on Sustainable Energy*, 14(1):297–308, 2023.

[55] Wenlong Liao, Dechang Yang, Yusen Wang, and Xiang Ren. Fault diagnosis of power transformers using graph convolutional network. *CSEE Journal of Power and Energy Systems*, 7(2):241–249, 2021.

[56] Osman Boyaci, M. Rasoul Narimani, Katherine Davis, and Erchin Serpedin. Cyberattack detection in large-scale smart grids using chebyshev graph convolutional networks. In *9th International Conference on Electrical and Electronics Engineering (ICEEE)*, pages 217–221, 2022.

[57] Seyed Hamed Haghshenas, Md Abul Hasnat, and Mia Naeini. A temporal graph neural network for cyber attack detection and localization in smart grids. In *EEE Power Energy Society Innovative Smart Grid Technologies Conference (ISGT)*, pages 1–5, 2023.

[58] Damian Owerko, Fernando Gama, and Alejandro Ribeiro. Optimal power flow using graph neural networks. In *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pages 5930–5934, 2020.

[59] Maosheng Gao, Juan Yu, Zhifang Yang, and Junbo Zhao. A physics-guided graph convolution neural network for optimal power flow. *IEEE Transactions on Power Systems*, pages 1–11, 2023.

[60] Yuxiao Liu, Ning Zhang, Dan Wu, Audun Botterud, Rui Yao, and Chongqing Kang. Searching for critical power system cascading failures with graph convolutional network. *IEEE Transactions on Control of Network Systems*, 8(3):1304–1313, 2021.

[61] Upama Nakarmi, Mahshid Rahnamay Naeini, Md Jakir Hossain, and Md Abul Hasnat. Interaction graphs for cascading failure analysis in power grids: A survey. *Energies*, 13(9), 2020.

[62] IEEE 118 Bus System, Illinois Center for a Smarter Electric Grid (ICSEG). https://icseg.iti.illinois.edu/ieee-118-bus-system/, Accessed June 23, 2023.

[63] Miloš Daković, Ljubiša Stanković, and Ervin Sejdić. Local smoothness of graph signals. *Mathematical Problems in Engineering*, 2019, 2019.

[64] Mehmet Necip Kurt, Yasin Yılmaz, and Xiaodong Wang. Distributed quickest detection of cyber-attacks in smart grid. *IEEE Transactions on Information Forensics and Security*, 13(8):2015–2030, 2018.

[65] Alan V Oppenheim. *Discrete-time signal processing*. Pearson Education India, 1999.

[66] Sunil K Narang and Antonio Ortega. Downsampling graphs using spectral theory. In *2011 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pages 4208–4211, 2011.

[67] Siheng Chen, Aliaksei Sandryhaila, and Jelena Kovačević. Sampling theory for graph signals. In *2015 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pages 3392–3396, 2015.

[68] Md Abul Hasnat and Mahshid Rahnamay-Naeini. A data driven detection and locating of cyber and physical stresses in smart grid based on state correlations. In *2019 9th International Conference on Power and Energy Systems (ICPES)*, pages 1–6, 2019.

[69] Md Abul Hasnat and Mahshid Rahnamay-Naeini. Detecting and locating cyber and physical stresses in smart grids using the k-nearest neighbour analysis of instantaneous correlation of states. *IET Smart Grid*, 4(3):307–320.

[70] Yang Chen, Le Xie, and P. R. Kumar. Dimensionality reduction and early event detection using online synchrophasor data. In *2013 IEEE Power Energy Society General Meeting*, pages 1–5, 2013.

[71] Tong Wu, Ying-Jun Angela Zhang, and Xiaoying Tang. Isolation forest based method for low-quality synchrophasor measurements and early events detection. In *2018 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*, pages 1–7, 2018.

[72] Lianfang Cai, Nina F. Thornhill, Stefanie Kuenzel, and Bikash C. Pal. Wide-area monitoring of power systems using principal component analysis and k-nearest neighbor analysis. *IEEE Transactions on Power Systems*, 33(5):4913–4923, 2018.

[73] Kaveri Mahapatra and Nilanjan Ray Chaudhuri. Online robust pca for malicious attack-resilience in wide-area mode metering application. *IEEE Transactions on Power Systems*, 34(4):2598–2610, 2019.

[74] Sara Eftekharnejad Sagnik Basumallik, Rui Ma. Packet-data anomaly detection in pmu-based state estimator using convolutional neural network. *International Journal of Electrical Power Energy Systems*, 107:690–702, 2019.

[75] Mehdi Ganjkhani, Seyedeh Narjes Fallah, Sobhan Badakhshan, Shahaboddin Shamshirband, and Kwok-wing Chau. A novel detection algorithm to identify false data injection attacks on power system state estimation. *Energies*, 12(11), 2019.

[76] Shengyi Pan, Thomas Morris, and Uttam Adhikari. Developing a hybrid intrusion detection system using data mining for power systems. *IEEE Transactions on Smart Grid*, 6(6):3104–3113, 2015.

[77] Hadis Karimipour, Ali Dehghantanha, Reza M. Parizi, Kim-Kwang Raymond Choo, and Henry Leung. A deep and scalable unsupervised machine learning system for cyber-attack detection in large-scale smart grids. *IEEE Access*, 7:80778–80788, 2019.

[78] Boda Li, Ying Chen, Shaowei Huang, Shengwei Mei, Zhisheng Wang, and Junjun Li. Real-time detecting false data injection attacks based on spatial and temporal correlations. In *2019 IEEE Power Energy Society General Meeting (PESGM)*, pages 1–5, 2019.

[79] Xin Shi, Robert Qiu, Zenan Ling, Fan Yang, Haosen Yang, and Xing He. Spatio-temporal correlation analysis of online monitoring data for anomaly detection and location in distribution networks. *IEEE Transactions on Smart Grid*, 11(2):995–1006, 2020.

[80] Mehmet Necip Kurt, Yasin Yılmaz, and Xiaodong Wang. Real-time detection of hybrid and stealthy cyber-attacks in smart grid. *IEEE Transactions on Information Forensics and Security*, 14(2):498–513, 2019.

[81] Zhigang Chu, Andrea Pinceti, Reetam Sen Biswas, Oliver Kosut, Anamitra Pal, and Lalitha Sankar. Can predictive filters detect gradually ramping false data injection attacks against pmus? In *IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*, pages 1–6, 2019.

[82] Fabio Pasqualetti, Florian Dörfler, and Francesco Bullo. Cyber-physical attacks in power networks: Models, fundamental limitations and monitor design. In *2011 50th IEEE Conference on Decision and Control and European Control Conference*, pages 2195–2201, 2011.

[83] Christopher Beasley, Xingsi Zhong, Juan Deng, Richard Brooks, and Ganesh Kumar Venayagamoorthy. A survey of electric power synchrophasor network cyber security. In *IEEE PES Innovative Smart Grid Technologies, Europe*, pages 1–5, 2014.

[84] Yilin Mo, Tiffany Hyun-Jin Kim, Kenneth Brancik, Dona Dickinson, Heejo Lee, Adrian Perrig, and Bruno Sinopoli. Cyber–physical security of a smart grid infrastructure. *Proceedings of the IEEE*, 100(1):195–209, 2012.

[85] Derui Ding, Qing-Long Han, Yang Xiang, Xiaohua Ge, and Xian-Ming Zhang. A survey on security control and attack detection for industrial cyber-physical systems. *Neurocomputing*, 275:1674–1683, 2018.

[86] Zhenghao Zhang, Shuping Gong, Aleksandar D. Dimitrovski, and Husheng Li. Time synchronization attack in smart grid: Impact and analysis. *IEEE Transactions on Smart Grid*, 4(1):87–98, 2013.

[87] Kevin P Murphy. *Machine learning: a probabilistic perspective*. MIT press, 2012.

[88] Donghui Yan, Yingjie Wang, Jin Wang, Honggang Wang, and Zhenpeng Li. K-nearest neighbor search by random projection forests. In *2018 IEEE International Conference on Big Data (Big Data)*, pages 4775–4781, 2018.

[89] Chaojun Gu and Panida Jirutitijaroen. Dynamic state estimation under communication failure using kriging based bus load forecasting. *IEEE Transactions on Power Systems*, 30(6):2831–2840, 2015.

[90] Raksha Ramakrishna and Anna Scaglione. Detection of false data injection attack using graph signal processing for the power grid. In *2019 IEEE Global Conference on Signal and Information Processing (GlobalSIP)*, pages 1–5, 2019.

[91] Osten Anderson and Nanpeng Yu. Distribution system bad data detection using graph signal processing. In *2021 IEEE Power Energy Society General Meeting (PESGM)*, pages 01–05, 2021.

[92] Jie Shi, Brandon Foggo, and Nanpeng Yu. Power system event identification based on deep neural network with information loading. *IEEE Transactions on Power Systems*, 36(6):5622–5632, 2021.

[93] Marisel Villafañe-Delgado and Selin Aviyente. Dynamic graph fourier transform on temporal functional connectivity networks. In *2017 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pages 949–953, 2017.

[94] A. Ahmed, K. S. Sajan, A. Srivastava, and Y. Wu. Anomaly detection, localization and classification using drifting synchrophasor data streams. *IEEE Transactions on Smart Grid*, 12(4):3570–3580, 2021.

[95] Md Abul Hasnat and Mahshid Rahnamay-Naeini. A data-driven dynamic state estimation for smart grids under dos attack using state correlations. In *2019 North American Power Symposium (NAPS)*, pages 1–6, 2019.

[96] Yang Chen, Le Xie, and P. R. Kumar. Power system event classification via dimensionality reduction of synchrophasor data. In *2014 IEEE 8th Sensor Array and Multichannel Signal Processing Workshop (SAM)*, pages 57–60, 2014.

[97] G. A. Susto, A. Cenedese, and M. Terzi. Time-series classification methods: Review and applications to power systems data. page 179–220, 2018.

[98] Mark Rafferty and Xueqin Amy Liu. Automatic power system event classification using quadratic discriminant analysis on pmu data. In *2020 IEEE Power Energy Society General Meeting (PESGM)*, pages 1–6, 2020.

[99] 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*, volume 2110.10128, 2021.

[100] Yuxuan Yuan, Zhaoyu Wang, and Yanchao Wang. Learning latent interactions for event classification via graph neural networks and pmu data. *IEEE Transactions on Power Systems*, 38(1):617–629, 2023.

[101] Scikit-learn. https://scikit-learn.org/stable/, Accessed: June 24, 2023.

[102] Md Abul Hasnat and Mahshid Rahnamay-Naeini. Power system state recovery using local and global smoothness of its graph signals. In *2022 IEEE Power Energy Society General Meeting (PESGM)*, pages 01–05, 2022.

[103] Ali Abur and Antonio Gomez Exposito. *Power system state estimation: theory and implementation*. CRC press, 2004.

[104] Fen Wang, Gene Cheung, and Yongchao Wang. Low-complexity graph sampling with noise and signal reconstruction via neumann series. *IEEE Transactions on Signal Processing*, 67(21):5511–5526, 2019.

[105] Xiaohan Wang, Pengfei Liu, and Yuantao Gu. Local-set-based graph signal reconstruction. *IEEE Transactions on Signal Processing*, 63(9):2432–2444, 2015.

[106] PaoloDi Lorenzo, Sergio Barbarossa, and Paolo Banelli. Sampling and recovery of graph signals. In *Cooperative and Graph Signal Processing*, pages 261–282. Elsevier, 2018.

[107] Yuichi Tanaka, Yonina C. Eldar, Antonio Ortega, and Gene Cheung. Sampling signals on graphs: From theory to applications. *IEEE Signal Processing Magazine*, 37(6):14–30, 2020.

[108] Aamir Anis, Akshay Gadde, and Antonio Ortega. Efficient sampling set selection for bandlimited graph signals using graph spectral proxies. *IEEE Transactions on Signal Processing*, 64(14):3775–3789, 2016.

[109] Akshay Gadde and Antonio Ortega. A probabilistic interpretation of sampling theory of graph signals. In *2015 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pages 3257–3261, 2015.

[110] Siheng Chen, Aliaksei Sandryhaila, José M. F. Moura, and Jelena Kovačević. Signal recovery on graphs: Variation minimization. *IEEE Transactions on Signal Processing*, 63(17):4609–4624, 2015.

[111] Siheng Chen, Rohan Varma, Aarti Singh, and Jelena Kovacević. Signal recovery on graphs: Random versus experimentally designed sampling. In *2015 International Conference on Sampling Theory and Applications (SampTA)*, pages 337–341, 2015.

[112] Siheng Chen, Rohan Varma, Aarti Singh, and Jelena Kovačević. Signal recovery on graphs: Fundamental limits of sampling strategies. *IEEE Transactions on Signal and Information Processing over Networks*, 2(4):539–554, 2016.

[113] Akie Sakiyama, Yuichi Tanaka, Toshihisa Tanaka, and Antonio Ortega. Efficient sensor position selection using graph signal sampling theory. In *2016 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pages 6225–6229, 2016.

[114] Xianghui Mao, Kai Qiu, Tiejian Li, and Yuantao Gu. Spatio-temporal signal recovery based on low rank and differential smoothness. *IEEE Transactions on Signal Processing*, 66(23):6281–6296, 2018.

[115] Peter Berger, Gabor Hannak, and Gerald Matz. Graph signal recovery via primal-dual algorithms for total variation minimization. *IEEE Journal of Selected Topics in Signal Processing*, 11(6):842–855, 2017.

[116] Elvin Isufi, Paolo Di Lorenzo, Paolo Banelli, and Geert Leus. Distributed wiener-based reconstruction of graph signals. In *2018 IEEE Statistical Signal Processing Workshop (SSP)*, pages 21–25, 2018.

[117] Daniel Romero, Meng Ma, and Georgios B. Giannakis. Kernel-based reconstruction of graph signals. *IEEE Transactions on Signal Processing*, 65(3):764–778, 2017.

[118] Zhong-Hua Han, Ke-Shi Zhang, et al. Surrogate-based optimization. *Real-world applications of genetic algorithms*, 343, 2012.

[119] Mathworks optimization toolbox. https://www.mathworks.com/products/optimization.html, Accessed: June 24, 2023.

[120] Menghao Wu, Qiang Zhang, Yanbin Gao, and Ningbo Li. Graph signal sampling with deep q-learning. In *2020 International Conference on Computer Information and Big Data Applications (CIBDA)*, pages 450–453, 2020.

[121] P NASPI. Pmu data quality: A framework for the attributes of pmu data quality and quality impacts to synchrophasor applications. 2017.

[122] William Yuill, A. Edwards, S. Chowdhury, and S. P. Chowdhury. Optimal pmu placement: A comprehensive literature review. In *2011 IEEE Power and Energy Society General Meeting*, pages 1–8, 2011.

[123] IEEE 14 Bus System. http://labs.ece.uw.edu/pstca/pf14/pg_tca14bus.htm, Accessed June 25, 2023.

[124] Md Abul Hasnat and Mia Naeini. Characterizing the effects of single bus perturbation on power systems graph signals. *arXiv:2306.03254v1.*

[125] Abdulrahman Takiddin, Rachad Atat, Muhammad Ismail, Katherine Davis, and Erchin Serpedin. A graph neural network multi-task learning-based approach for detection and localization of cyberattacks in smart grids. In *ICASSP 2023 - 2023 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pages 1–5, 2023.

[126] Lital Dabush, Ariel Kroizer, and Tirza Routtenberg. State estimation in partially observable power systems via graph signal processing tools. *Sensors*, 23(3):1387, 2023.

[127] Kanghang He, Lina Stankovic, Jing Liao, and Vladimir Stankovic. Non-intrusive load disaggregation using graph signal processing. *IEEE Transactions on Smart Grid*, 9(3):1739–1747, 2018.

[128] Kamala Sarojini Ratnam, K Palanisamy, and Guangya Yang. Future low-inertia power systems: Requirements, issues, and solutions-a review. *Renewable and Sustainable Energy Reviews*, 124:109773, 2020.

[129] Prateek Jain and Trapti Jain. Impacts of g2v and v2g power on electricity demand profile. In *2014 IEEE International Electric Vehicle Conference (IEVC)*, pages 1–8, 2014.

[130] Jonathan Mullan, David Harries, Thomas Bräunl, and Stephen Whitely. Modelling the impacts of electric vehicle recharging on the western australian electricity supply system. *Energy policy*, 39(7):4349–4359, 2011.

[131] Jason Stamp, Annie McIntyre, and Bryan Ricardson. Reliability impacts from cyber attack on electric power systems. In *2009 IEEE/PES Power Systems Conference and Exposition*, pages 1–8, 2009.

[132] Amir-Hamed Mohsenian-Rad and Alberto Leon-Garcia. Distributed internet-based load altering attacks against smart power grids. *IEEE Transactions on Smart Grid*, 2(4):667–674, 2011.

[133] Matthias F Wolff, Pedro G Lind, and Philipp Maass. Power grid stability under perturbation of single nodes: Effects of heterogeneity and internal nodes. *Chaos: An Interdisciplinary Journal of Nonlinear Science*, 28(10):103120, 2018.

[134] Peter J. Menck and Juergen Kurths. Topological identification of weak points in power grids. In *NDES 2012; Nonlinear Dynamics of Electronic Systems*, pages 1–4, 2012.

[135] Chittaranjan Hens, Uzi Harush, Simi Haber, Reuven Cohen, and Baruch Barzel. Spatiotemporal signal propagation in complex networks. *Nature Physics*, 15(4):403–412, 2019.

[136] Samantha Molnar, Elizabeth Bradley, and Kenny Gruchalla. Oscillatory spreading and inertia in power grids. *Chaos: An Interdisciplinary Journal of Nonlinear Science*, 31(12):123103, 2021.

[137] Kosisochukwu P Nnoli and Stefan Kettemann. Spreading of disturbances in realistic models of transmission grids in dependence on topology, inertia and heterogeneity. *Scientific Reports*, 11(1):1–17, 2021.

[138] Anna Büttner, Jürgen Kurths, and Frank Hellmann. Ambient forcing: Sampling local perturbations in constrained phase spaces. *New Journal of Physics*, 24(5):053019, 2022.

[139] Josip Vasilj, Damir Jakus, Mateo Marusic, and Mate Relja. Robust model for ev driven grid impact estimation. In *2022 International Conference on Smart Systems and Technologies (SST)*, pages 231–235. IEEE, 2022.

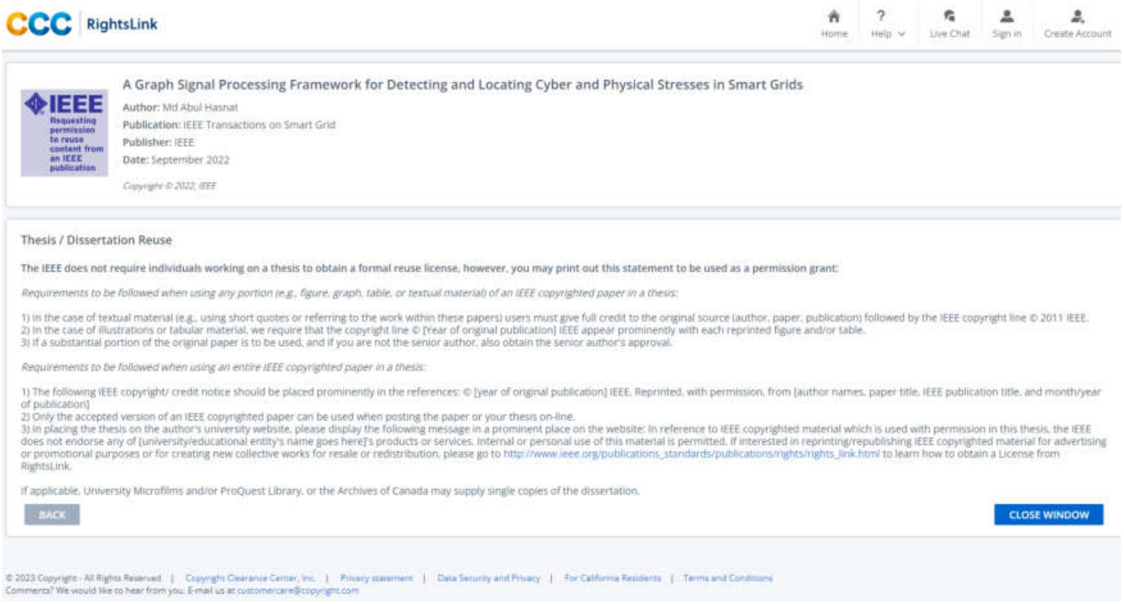
[140] Pijush K Kundu, Ira M Cohen, and David R Dowling. *Fluid mechanics*. Academic press, 2015.

[141] Peipei Xia, Li Zhang, and Fanzhang Li. Learning similarity with cosine similarity ensemble. *Information sciences*, 307:39–52, 2015.

[142] Kumari Sandhya and Kalyan Chatterjee. Two-stage ann based intelligent technique for optimal positioning and sizing of ders in distribution system. *Engineering Applications of Artificial Intelligence*, 121:105932, 2023.

Appendix A: Copyright Permissions

The permission below is for the reproduction of material in Chapter 2 and 4.


CCC RightsLink
Home
Help
Live Chat
Sign in
Create Account
IEEE
Requesting permission to reuse content from an IEEE publication

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

Author: Md Abul Hasnat
Publication: IEEE Transactions on Smart Grid
Publisher: IEEE
Date: September 2022

Copyright © 2022, IEEE

Thesis / Dissertation Reuse

The IEEE does not require individuals working on a thesis to obtain a formal reuse license, however, you may print out this statement to be used as a permission grant:

Requirements to be followed when using any portion (e.g., figure, graph, table, or textual material) of an IEEE copyrighted paper in a thesis:

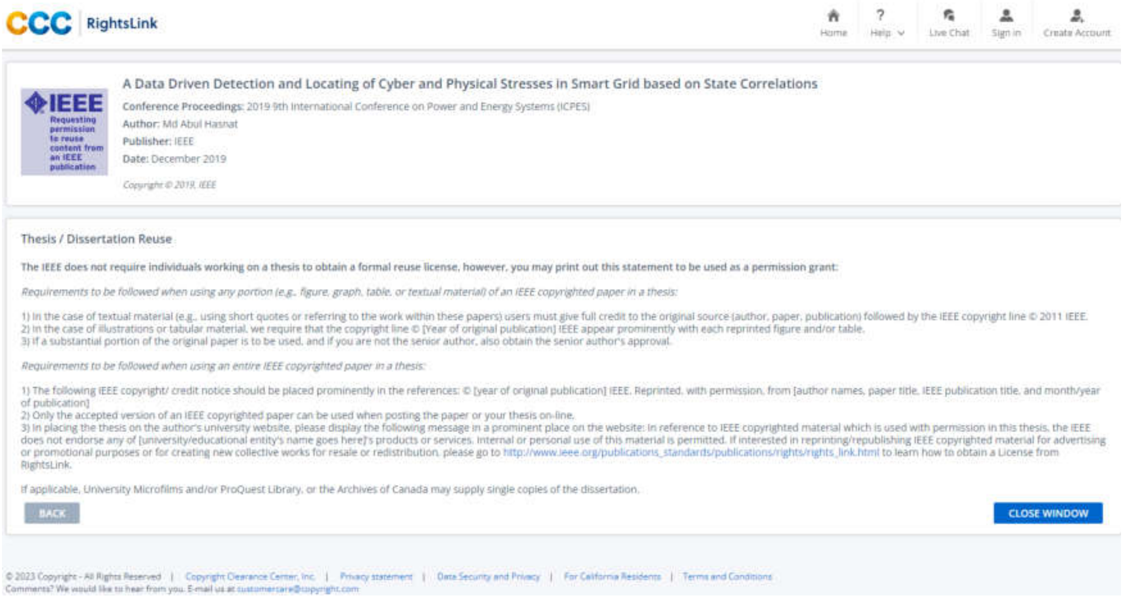
1) In the case of textual material (e.g., using short quotes or referring to the work within these papers) users must give full credit to the original source (author, paper, publication) followed by the IEEE copyright line © 2011 IEEE.
2) In the case of illustrations or tabular material, we require that the copyright line © [Year of original publication] IEEE appear prominently with each reprinted figure and/or table.
3) If a substantial portion of the original paper is to be used, and if you are not the senior author, also obtain the senior author's approval.

Requirements to be followed when using an entire IEEE copyrighted paper in a thesis:

1) The following IEEE copyright/ credit notice should be placed prominently in the references: © [year of original publication] IEEE. Reprinted, with permission, from [author names, paper title, IEEE publication title, and month/year of publication]
2) Only the accepted version of an IEEE copyrighted paper can be used when posting the paper or your thesis on-line.
3) In placing the thesis on the author's university website, please display the following message in a prominent place on the website: In reference to IEEE copyrighted material which is used with permission in this thesis, the IEEE does not endorse any of [university/educational entity's name goes here]'s products or services. Internal or personal use of this material is permitted. If interested in reprinting/republishing IEEE copyrighted material for advertising or promotional purposes or for creating new collective works for resale or redistribution, please go to http://www.ieee.org/publications_standards/publications/rights/rights_link.html to learn how to obtain a License from RightsLink.

If applicable, University Microfilms and/or ProQuest Library, or the Archives of Canada may supply single copies of the dissertation.

The permission below is for the reproduction of material in Chapter 3.



CCC RightsLink
Home
Help
Live Chat
Sign in
Create Account
IEEE
Requesting permission to reuse content from an IEEE publication

A Data Driven Detection and Locating of Cyber and Physical Stresses in Smart Grid based on State Correlations

Conference Proceedings: 2019 9th International Conference on Power and Energy Systems (ICPES)
Author: Md Abul Hasnat
Publisher: IEEE
Date: December 2019

Copyright © 2019, IEEE

Thesis / Dissertation Reuse

The IEEE does not require individuals working on a thesis to obtain a formal reuse license, however, you may print out this statement to be used as a permission grant:

Requirements to be followed when using any portion (e.g., figure, graph, table, or textual material) of an IEEE copyrighted paper in a thesis:

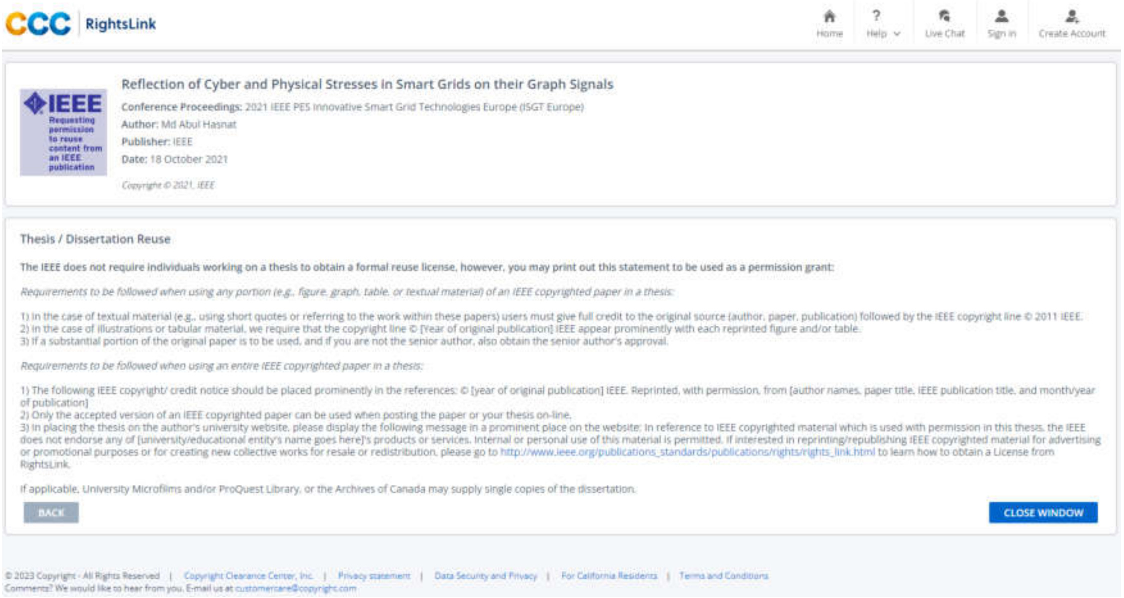
1) In the case of textual material (e.g., using short quotes or referring to the work within these papers) users must give full credit to the original source (author, paper, publication) followed by the IEEE copyright line © 2011 IEEE.
2) In the case of illustrations or tabular material, we require that the copyright line © [Year of original publication] IEEE appear prominently with each reprinted figure and/or table.
3) If a substantial portion of the original paper is to be used, and if you are not the senior author, also obtain the senior author's approval.

Requirements to be followed when using an entire IEEE copyrighted paper in a thesis:

1) The following IEEE copyright/ credit notice should be placed prominently in the references: © [year of original publication] IEEE. Reprinted, with permission, from [author names, paper title, IEEE publication title, and month/year of publication]
2) Only the accepted version of an IEEE copyrighted paper can be used when posting the paper or your thesis on-line.
3) In placing the thesis on the author's university website, please display the following message in a prominent place on the website: In reference to IEEE copyrighted material which is used with permission in this thesis, the IEEE does not endorse any of [university/educational entity's name goes here]'s products or services. Internal or personal use of this material is permitted. If interested in reprinting/republishing IEEE copyrighted material for advertising or promotional purposes or for creating new collective works for resale or redistribution, please go to http://www.ieee.org/publications_standards/publications/rights/rights_link.html to learn how to obtain a License from RightsLink.

If applicable, University Microfilms and/or ProQuest Library, or the Archives of Canada may supply single copies of the dissertation.

The permission below is for the reproduction of material in Chapter 2.


CCC RightsLink
Home
Help
Live Chat
Sign in
Create Account
IEEE
Requesting permission to reuse content from an IEEE publication

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

Conference Proceedings: 2021 IEEE PES Innovative Smart Grid Technologies Europe (ISGT Europe)
Author: Md Abul Hasnat
Publisher: IEEE
Date: 18 October 2021

Copyright © 2021, IEEE

Thesis / Dissertation Reuse

The IEEE does not require individuals working on a thesis to obtain a formal reuse license, however, you may print out this statement to be used as a permission grant:

Requirements to be followed when using any portion (e.g., figure, graph, table, or textual material) of an IEEE copyrighted paper in a thesis:

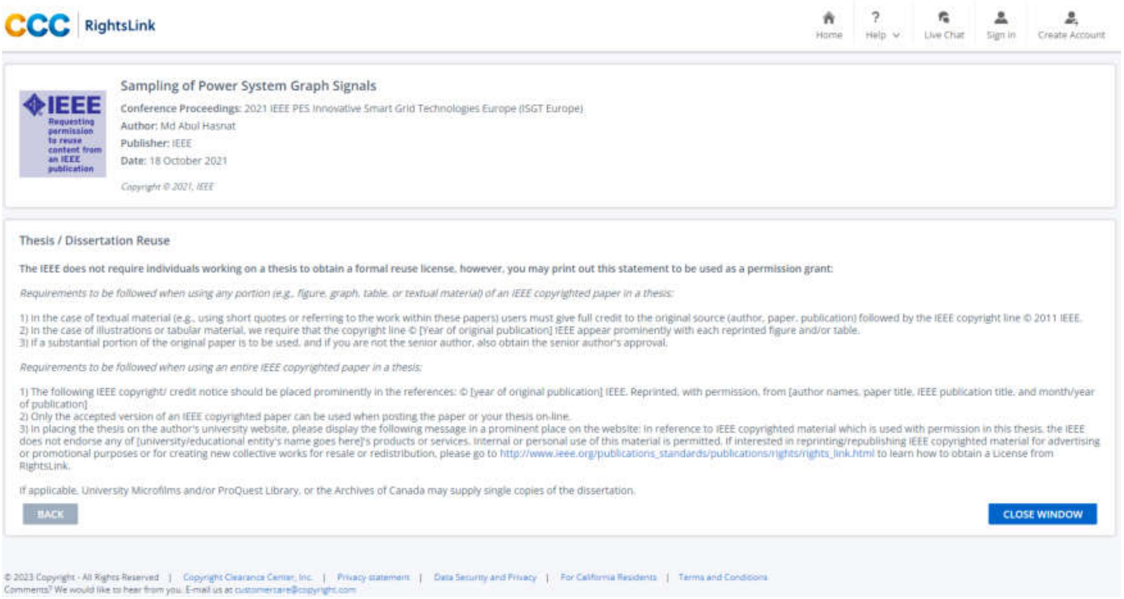
1) In the case of textual material (e.g., using short quotes or referring to the work within these papers) users must give full credit to the original source (author, paper, publication) followed by the IEEE copyright line © 2011 IEEE.
2) In the case of illustrations or tabular material, we require that the copyright line © [Year of original publication] IEEE appear prominently with each reprinted figure and/or table.
3) If a substantial portion of the original paper is to be used, and if you are not the senior author, also obtain the senior author's approval.

Requirements to be followed when using an entire IEEE copyrighted paper in a thesis:

1) The following IEEE copyright/ credit notice should be placed prominently in the references: © [year of original publication] IEEE. Reprinted, with permission, from [author names, paper title, IEEE publication title, and month/year of publication]
2) Only the accepted version of an IEEE copyrighted paper can be used when posting the paper or your thesis on-line.
3) In placing the thesis on the author's university website, please display the following message in a prominent place on the website: In reference to IEEE copyrighted material which is used with permission in this thesis, the IEEE does not endorse any of [university/educational entity's name goes here]'s products or services. Internal or personal use of this material is permitted. If interested in reprinting/republishing IEEE copyrighted material for advertising or promotional purposes or for creating new collective works for resale or redistribution, please go to http://www.ieee.org/publications_standards/publications/rights/rights_link.html to learn how to obtain a License from RightsLink.

If applicable, University Microfilms and/or ProQuest Library, or the Archives of Canada may supply single copies of the dissertation.

The permission below is for the reproduction of material in Chapter 2 and 6.


CCC RightsLink
Home
Help
Live Chat
Sign in
Create Account
IEEE
Requesting permission to reuse content from an IEEE publication

Sampling of Power System Graph Signals

Conference Proceedings: 2021 IEEE PES Innovative Smart Grid Technologies Europe (ISGT Europe)
Author: Md Abul Hasnat
Publisher: IEEE
Date: 18 October 2021

Copyright © 2021, IEEE

Thesis / Dissertation Reuse

The IEEE does not require individuals working on a thesis to obtain a formal reuse license, however, you may print out this statement to be used as a permission grant:

Requirements to be followed when using any portion (e.g., figure, graph, table, or textual material) of an IEEE copyrighted paper in a thesis:

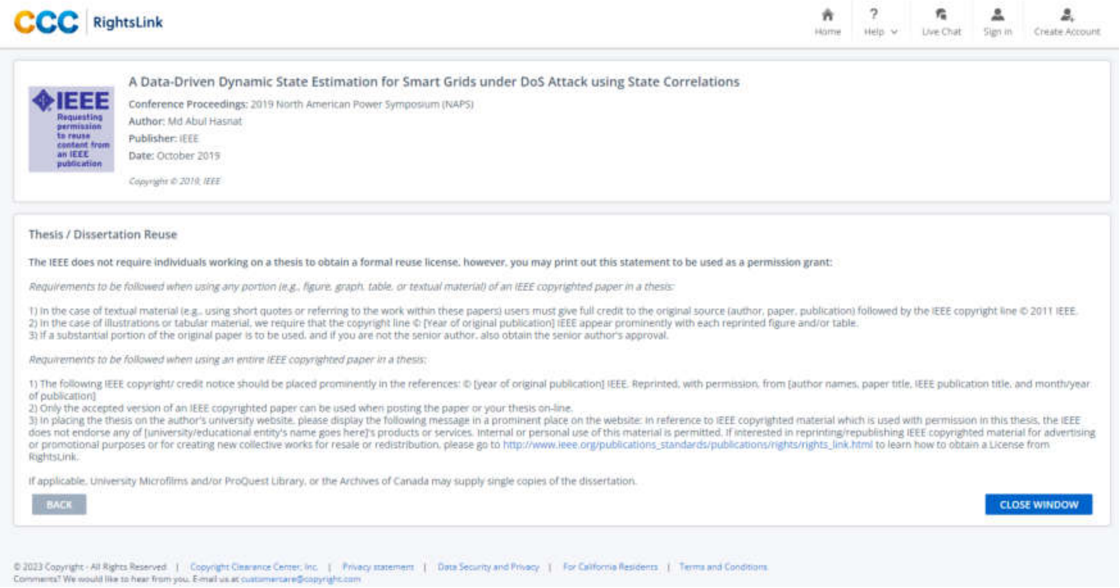
1) In the case of textual material (e.g., using short quotes or referring to the work within these papers) users must give full credit to the original source (author, paper, publication) followed by the IEEE copyright line © 2011 IEEE.
2) In the case of illustrations or tabular material, we require that the copyright line © [Year of original publication] IEEE appear prominently with each reprinted figure and/or table.
3) If a substantial portion of the original paper is to be used, and if you are not the senior author, also obtain the senior author's approval.

Requirements to be followed when using an entire IEEE copyrighted paper in a thesis:

1) The following IEEE copyright/ credit notice should be placed prominently in the references: © [year of original publication] IEEE. Reprinted, with permission, from [author names, paper title, IEEE publication title, and month/year of publication]
2) Only the accepted version of an IEEE copyrighted paper can be used when posting the paper or your thesis on-line.
3) In placing the thesis on the author's university website, please display the following message in a prominent place on the website: In reference to IEEE copyrighted material which is used with permission in this thesis, the IEEE does not endorse any of [university/educational entity's name goes here]'s products or services. Internal or personal use of this material is permitted. If interested in reprinting/republishing IEEE copyrighted material for advertising or promotional purposes or for creating new collective works for resale or redistribution, please go to http://www.ieee.org/publications_standards/publications/rights/rights_link.html to learn how to obtain a License from RightsLink.

If applicable, University Microfilms and/or ProQuest Library, or the Archives of Canada may supply single copies of the dissertation.

The permission below is for the reproduction of material in Chapter 6.



CCC RightsLink
Home
Help
Live Chat
Sign in
Create Account
IEEE
Requesting permission to reuse content from an IEEE publication

A Data-Driven Dynamic State Estimation for Smart Grids under DoS Attack using State Correlations

Conference Proceedings: 2019 North American Power Symposium (NAPS)
Author: Md Abul Hasnat
Publisher: IEEE
Date: October 2019

Copyright © 2019, IEEE

Thesis / Dissertation Reuse

The IEEE does not require individuals working on a thesis to obtain a formal reuse license, however, you may print out this statement to be used as a permission grant:

Requirements to be followed when using any portion (e.g., figure, graph, table, or textual material) of an IEEE copyrighted paper in a thesis:

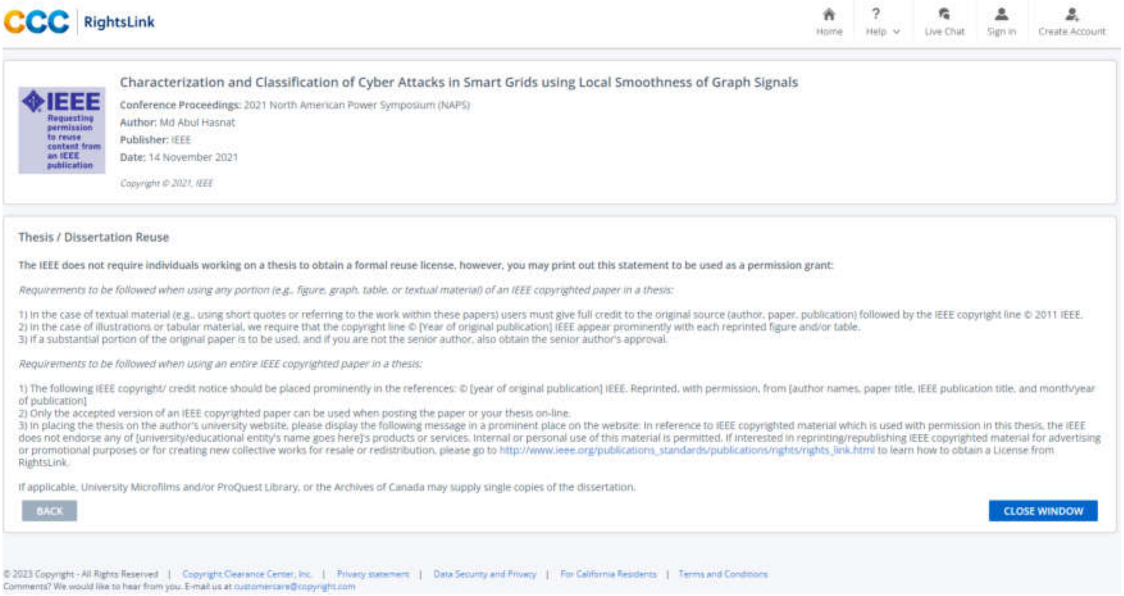
1) In the case of textual material (e.g., using short quotes or referring to the work within these papers) users must give full credit to the original source (author, paper, publication) followed by the IEEE copyright line © 2011 IEEE.
2) In the case of illustrations or tabular material, we require that the copyright line © [Year of original publication] IEEE appear prominently with each reprinted figure and/or table.
3) If a substantial portion of the original paper is to be used, and if you are not the senior author, also obtain the senior author's approval.

Requirements to be followed when using an entire IEEE copyrighted paper in a thesis:

1) The following IEEE copyright/ credit notice should be placed prominently in the references: © [year of original publication] IEEE. Reprinted, with permission, from [author names, paper title, IEEE publication title, and month/year of publication]
2) Only the accepted version of an IEEE copyrighted paper can be used when posting the paper or your thesis on-line.
3) In placing the thesis on the author's university website, please display the following message in a prominent place on the website: In reference to IEEE copyrighted material which is used with permission in this thesis, the IEEE does not endorse any of [university/educational entity's name goes here]'s products or services. Internal or personal use of this material is permitted. If interested in reprinting/republishing IEEE copyrighted material for advertising or promotional purposes or for creating new collective works for resale or redistribution, please go to http://www.ieee.org/publications_standards/publications/rights/rights_link.html to learn how to obtain a License from RightsLink.

If applicable, University Microfilms and/or ProQuest Library, or the Archives of Canada may supply single copies of the dissertation.

The permission below is for the reproduction of material in Chapter 5.


CCC RightsLink
Home
Help
Live Chat
Sign in
Create Account
IEEE
Requesting permission to reuse content from an IEEE publication

Characterization and Classification of Cyber Attacks in Smart Grids using Local Smoothness of Graph Signals

Conference Proceedings: 2021 North American Power Symposium (NAPS)
Author: Md Abul Hasnat
Publisher: IEEE
Date: 14 November 2021

Copyright © 2021, IEEE

Thesis / Dissertation Reuse

The IEEE does not require individuals working on a thesis to obtain a formal reuse license, however, you may print out this statement to be used as a permission grant:

Requirements to be followed when using any portion (e.g., figure, graph, table, or textual material) of an IEEE copyrighted paper in a thesis:

1) In the case of textual material (e.g., using short quotes or referring to the work within these papers) users must give full credit to the original source (author, paper, publication) followed by the IEEE copyright line © 2011 IEEE.
2) In the case of illustrations or tabular material, we require that the copyright line © [Year of original publication] IEEE appear prominently with each reprinted figure and/or table.
3) If a substantial portion of the original paper is to be used, and if you are not the senior author, also obtain the senior author's approval.

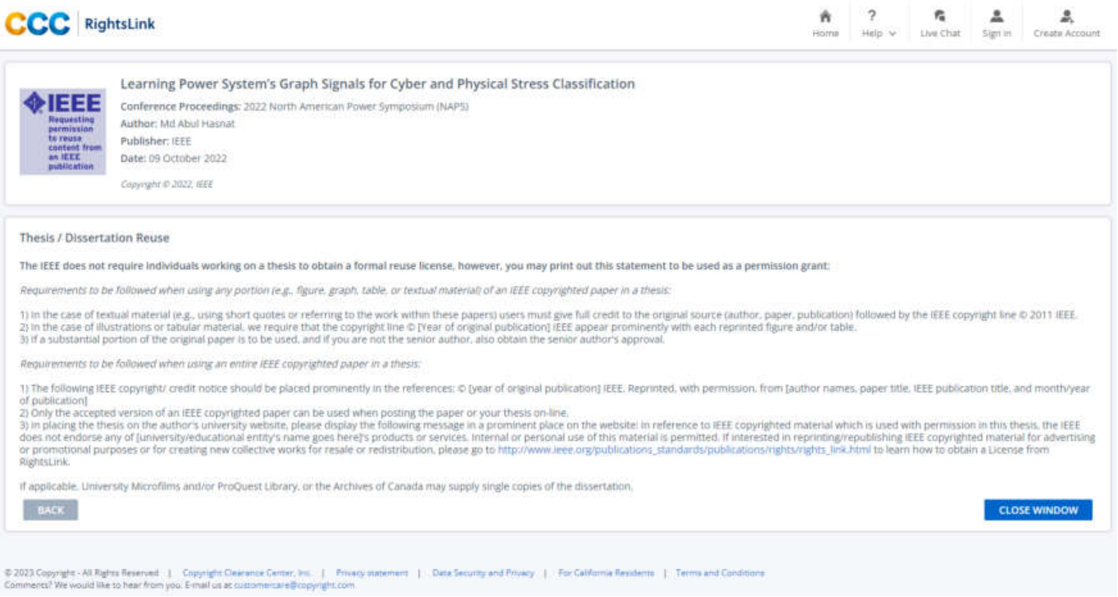
Requirements to be followed when using an entire IEEE copyrighted paper in a thesis:

1) The following IEEE copyright/ credit notice should be placed prominently in the references: © [year of original publication] IEEE. Reprinted, with permission, from [author names, paper title, IEEE publication title, and month/year of publication]
2) Only the accepted version of an IEEE copyrighted paper can be used when posting the paper or your thesis on-line.
3) In placing the thesis on the author's university website, please display the following message in a prominent place on the website: In reference to IEEE copyrighted material which is used with permission in this thesis, the IEEE does not endorse any of [university/educational entity's name goes here]'s products or services. Internal or personal use of this material is permitted. If interested in reprinting/republishing IEEE copyrighted material for advertising or promotional purposes or for creating new collective works for resale or redistribution, please go to http://www.ieee.org/publications_standards/publications/rights/rights_link.html to learn how to obtain a License from RightsLink.

If applicable, University Microfilms and/or ProQuest Library, or the Archives of Canada may supply single copies of the dissertation.

© 2023 Copyright - All Rights Reserved | Copyright Clearance Center, Inc. | Privacy statement | Data Security and Privacy | For California Residents | Terms and Conditions
Comments? We would like to hear from you. E-mail us at customercare@copyright.com

The permission below is for the reproduction of material in Chapter 5.


CCC RightsLink
Home
Help
Live Chat
Sign in
Create Account
IEEE
Requesting permission to reuse content from an IEEE publication

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

Conference Proceedings: 2022 North American Power Symposium (NAPS)
Author: Md Abul Hasnat
Publisher: IEEE
Date: 09 October 2022

Thesis / Dissertation Reuse

The IEEE does not require individuals working on a thesis to obtain a formal reuse license, however, you may print out this statement to be used as a permission grant:

Requirements to be followed when using any portion (e.g., figure, graph, table, or textual material) of an IEEE copyrighted paper in a thesis:

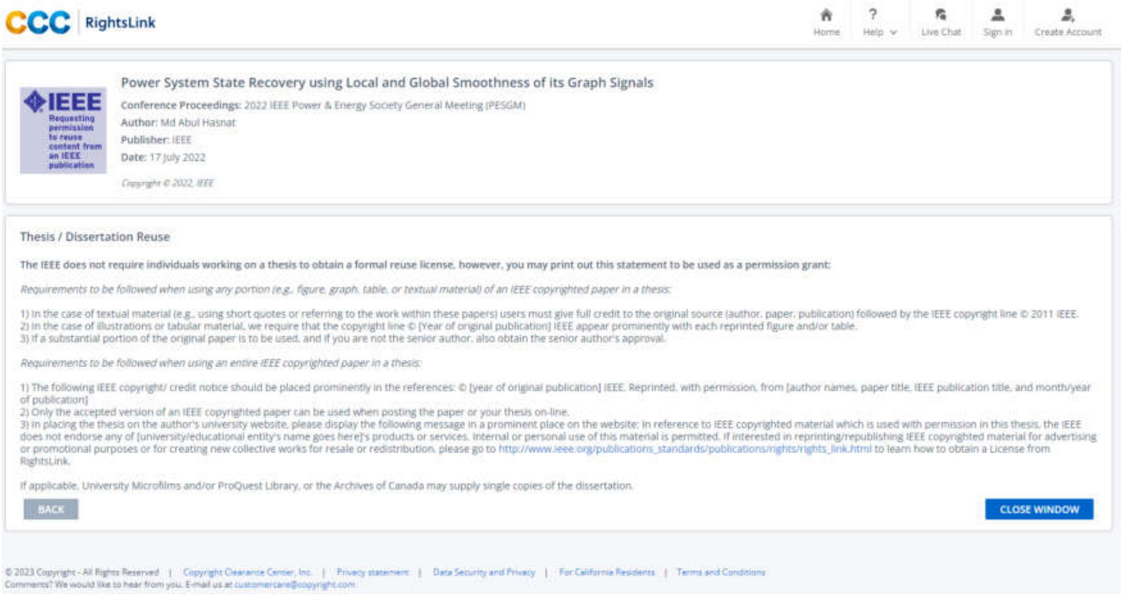
1) In the case of textual material (e.g., using short quotes or referring to the work within these papers) users must give full credit to the original source (author, paper, publication) followed by the IEEE copyright line © 2011 IEEE.
2) In the case of illustrations or tabular material, we require that the copyright line © [Year of original publication] IEEE appear prominently with each reprinted figure and/or table.
3) If a substantial portion of the original paper is to be used, and if you are not the senior author, also obtain the senior author's approval.

Requirements to be followed when using an entire IEEE copyrighted paper in a thesis:

1) The following IEEE copyright/ credit notice should be placed prominently in the references: © [year of original publication] IEEE. Reprinted, with permission, from [author names, paper title, IEEE publication title, and month/year of publication]
2) Only the accepted version of an IEEE copyrighted paper can be used when posting the paper or your thesis on-line.
3) In placing the thesis on the author's university website, please display the following message in a prominent place on the website: In reference to IEEE copyrighted material which is used with permission in this thesis, the IEEE does not endorse any of [university/educational entity's name goes here]'s products or services. Internal or personal use of this material is permitted. If interested in reprinting/republishing IEEE copyrighted material for advertising or promotional purposes or for creating new collective works for resale or redistribution, please go to http://www.ieee.org/publications_standards/publications/rights/rights_link.html to learn how to obtain a License from RightsLink.

If applicable, University Microfilms and/or ProQuest Library, or the Archives of Canada may supply single copies of the dissertation.

The permission below is for the reproduction of material in Chapter 6.



Power System State Recovery using Local and Global Smoothness of its Graph Signals

Conference Proceedings: 2022 IEEE Power & Energy Society General Meeting (PESGM)
Author: Md Abul Hasnat
Publisher: IEEE
Date: 17 July 2022

Copyright © 2022, IEEE

Thesis / Dissertation Reuse

The IEEE does not require individuals working on a thesis to obtain a formal reuse license, however, you may print out this statement to be used as a permission grant:

Requirements to be followed when using any portion (e.g., figure, graph, table, or textual material) of an IEEE copyrighted paper in a thesis:

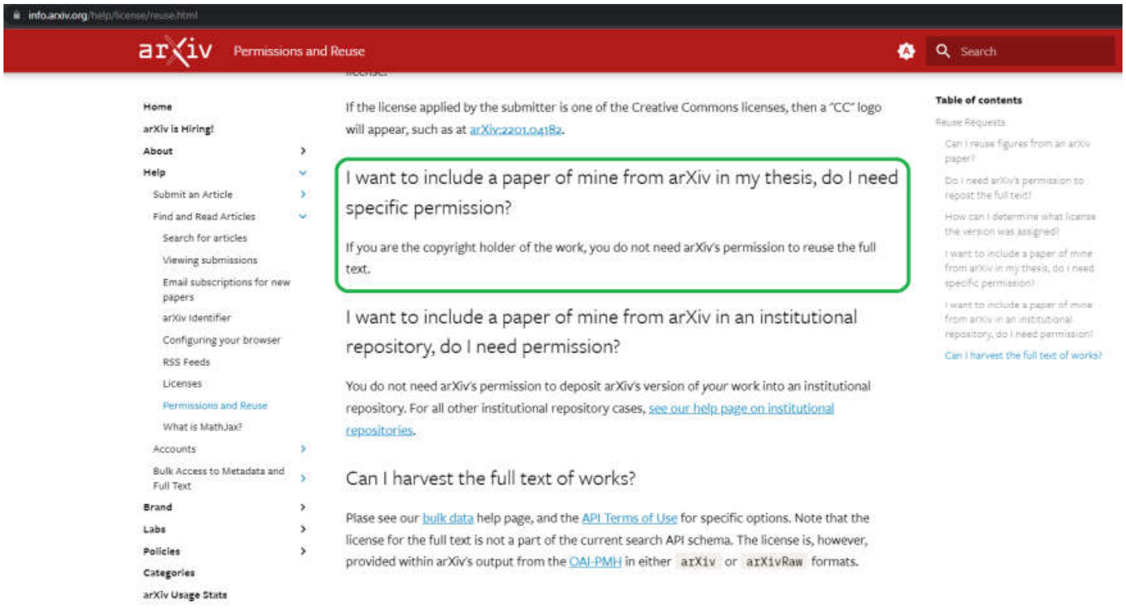
1) In the case of textual material (e.g., using short quotes or referring to the work within these papers) users must give full credit to the original source (author, paper, publication) followed by the IEEE copyright line © 2011 IEEE.
2) In the case of illustrations or tabular material, we require that the copyright line © [Year of original publication] IEEE appear prominently with each reprinted figure and/or table.
3) If a substantial portion of the original paper is to be used, and if you are not the senior author, also obtain the senior author's approval.

Requirements to be followed when using an entire IEEE copyrighted paper in a thesis:

1) The following IEEE copyright/ credit notice should be placed prominently in the references: © [year of original publication] IEEE. Reprinted, with permission, from [author names, paper title, IEEE publication title, and month/year of publication]
2) Only the accepted version of an IEEE copyrighted paper can be used when posting the paper or your thesis on-line.
3) In placing the thesis on the author's university website, please display the following message in a prominent place on the website: In reference to IEEE copyrighted material which is used with permission in this thesis, the IEEE does not endorse any of [university/educational entity's name goes here]'s products or services. Internal or personal use of this material is permitted. If interested in reprinting/republishing IEEE copyrighted material for advertising or promotional purposes or for creating new collective works for resale or redistribution, please go to http://www.ieee.org/publications_standards/publications/rights/rights_link.html to learn how to obtain a License from RightsLink.

If applicable, University Microfilms and/or ProQuest Library, or the Archives of Canada may supply single copies of the dissertation.

The permission below is for the reproduction of material in Chapters 2 and 7.


info.arxiv.org/help/license/reuse.html
arXiv
Permissions and Reuse
Search
Home
arXiv is Hiring!
About
Help
Submit an Article
Find and Read Articles
Search for articles
Viewing submissions
Email subscriptions for new papers
arXiv Identifier
Configuring your browser
RSS Feeds
Licenses
Permissions and Reuse
What is MathJax?
Accounts
Bulk Access to Metadata and Full Text
Brand
Labs
Policies
Categories
arXiv Usage Stats
Table of contents
Reuse Requests
Can I reuse figures from an arXiv paper?
Do I need arXiv's permission to repost the full text?
How can I determine what license the version was assigned?
I want to include a paper of mine from arXiv in my thesis, do I need specific permission?
I want to include a paper of mine from arXiv in an institutional repository, do I need permission?
Can I harvest the full text of works?

license.

If the license applied by the submitter is one of the Creative Commons licenses, then a "CC" logo will appear, such as at arXiv:2201.04182.

I want to include a paper of mine from arXiv in my thesis, do I need specific permission?

If you are the copyright holder of the work, you do not need arXiv's permission to reuse the full text.

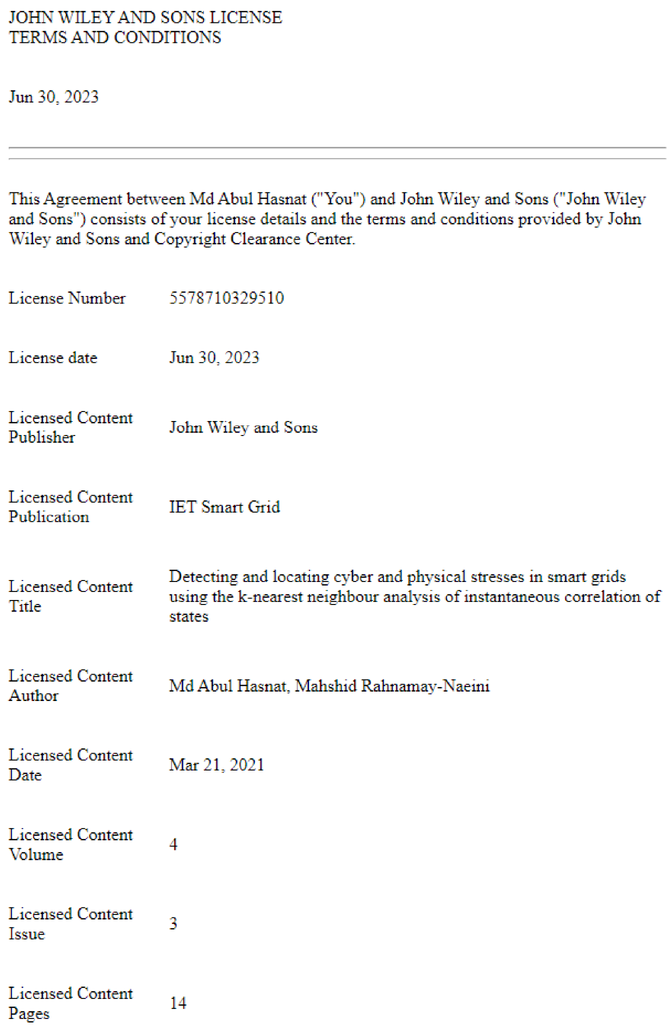
I want to include a paper of mine from arXiv in an institutional repository, do I need permission?

You do not need arXiv's permission to deposit arXiv's version of *your* work into an institutional repository. For all other institutional repository cases, see our help page on institutional repositories.

Can I harvest the full text of works?

Plase see our bulk data help page, and the API Terms of Use for specific options. Note that the license for the full text is not a part of the current search API schema. The license is, however, provided within arXiv's output from the OAI-PMH in either `arXiv` or `arXivRaw` formats.

The permission below is for the reproduction of material in Chapter 3.

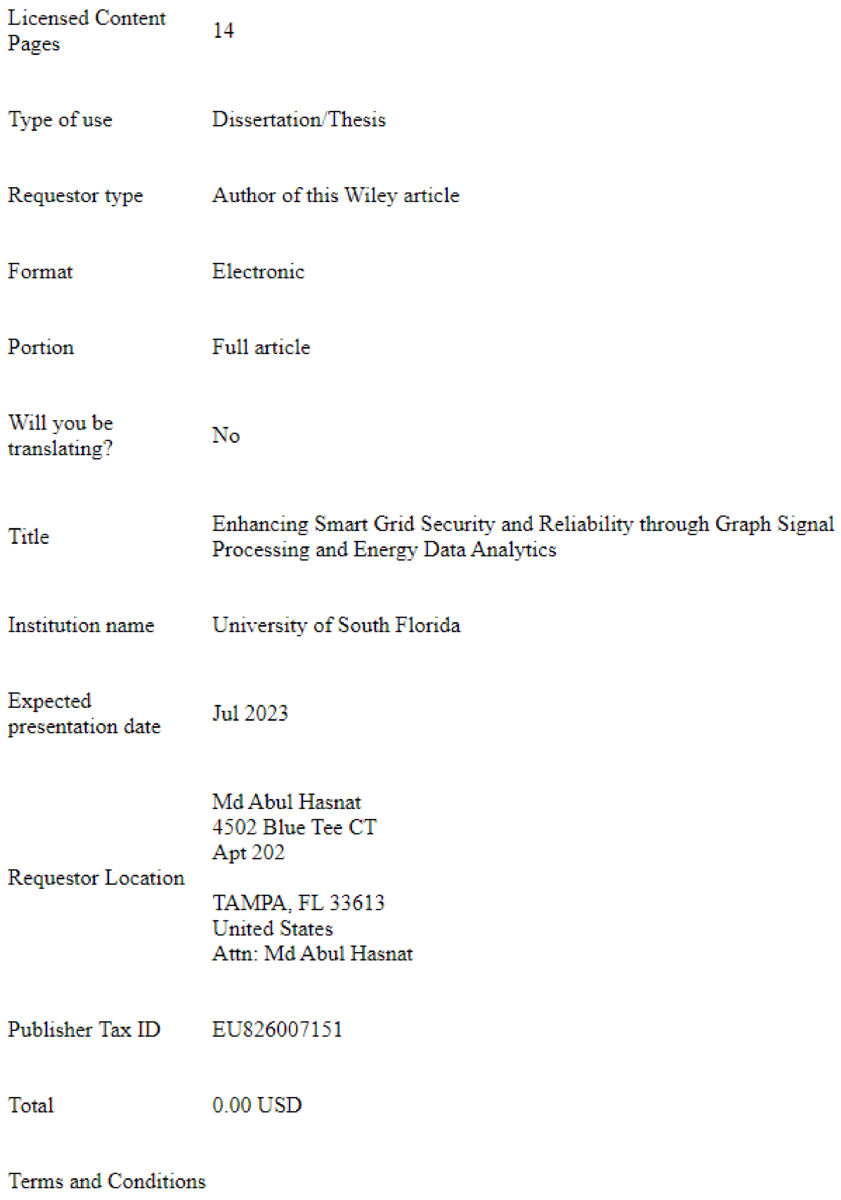


JOHN WILEY AND SONS LICENSE
TERMS AND CONDITIONS

Jun 30, 2023

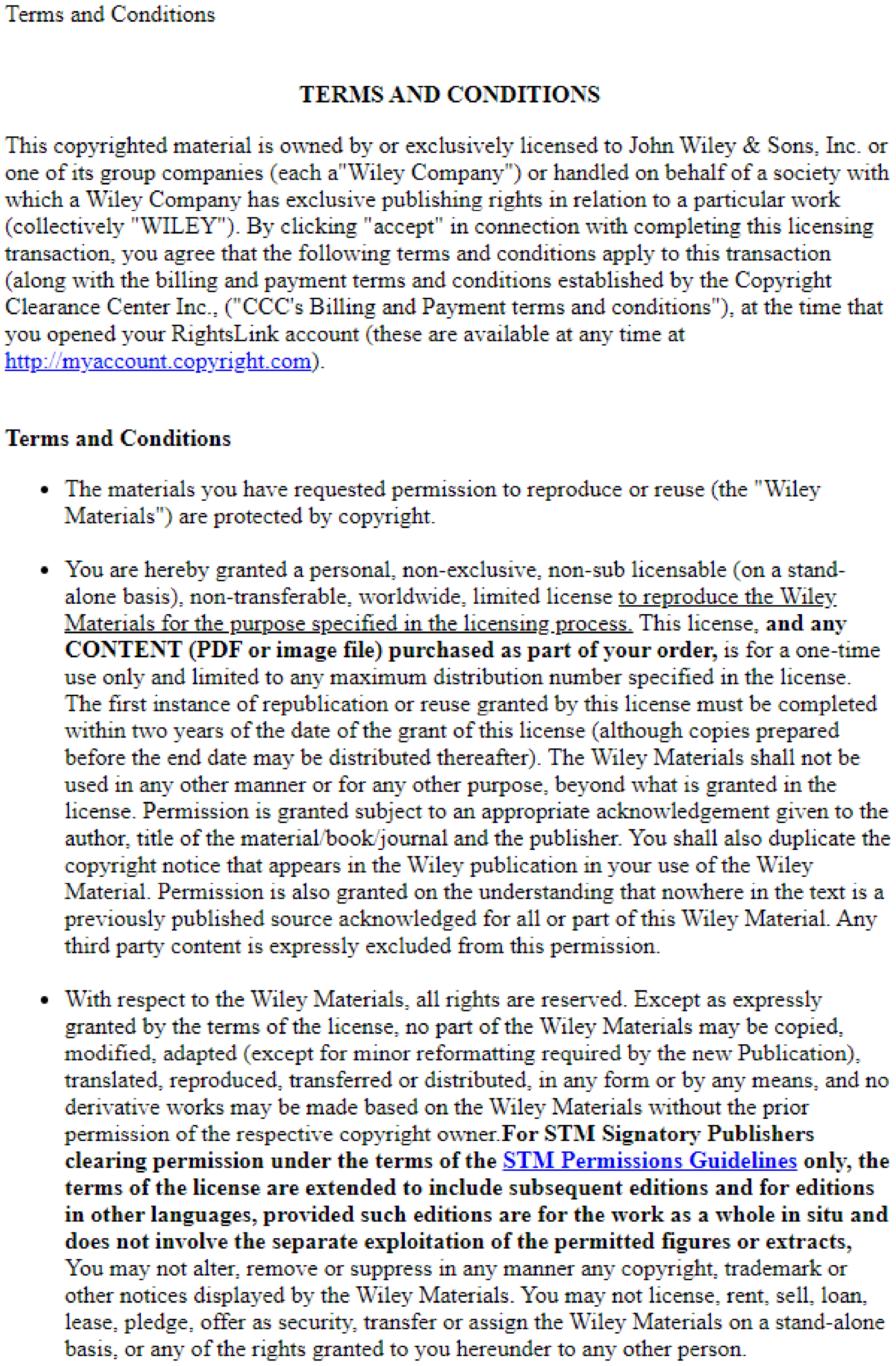
This Agreement between Md Abul Hasnat ("You") and John Wiley and Sons ("John Wiley and Sons") consists of your license details and the terms and conditions provided by John Wiley and Sons and Copyright Clearance Center.

License Number	5578710329510
License date	Jun 30, 2023
Licensed Content Publisher	John Wiley and Sons
Licensed Content Publication	IET Smart Grid
Licensed Content Title	Detecting and locating cyber and physical stresses in smart grids using the k-nearest neighbour analysis of instantaneous correlation of states
Licensed Content Author	Md Abul Hasnat, Mahshid Rahnamay-Naeini
Licensed Content Date	Mar 21, 2021
Licensed Content Volume	4
Licensed Content Issue	3
Licensed Content Pages	14



Licensed Content Pages	14
Type of use	Dissertation/Thesis
Requestor type	Author of this Wiley article
Format	Electronic
Portion	Full article
Will you be translating?	No
Title	Enhancing Smart Grid Security and Reliability through Graph Signal Processing and Energy Data Analytics
Institution name	University of South Florida
Expected presentation date	Jul 2023
Requestor Location	Md Abul Hasnat 4502 Blue Tee CT Apt 202 TAMPA, FL 33613 United States Attn: Md Abul Hasnat
Publisher Tax ID	EU826007151
Total	0.00 USD

Terms and Conditions



Terms and Conditions

TERMS AND CONDITIONS

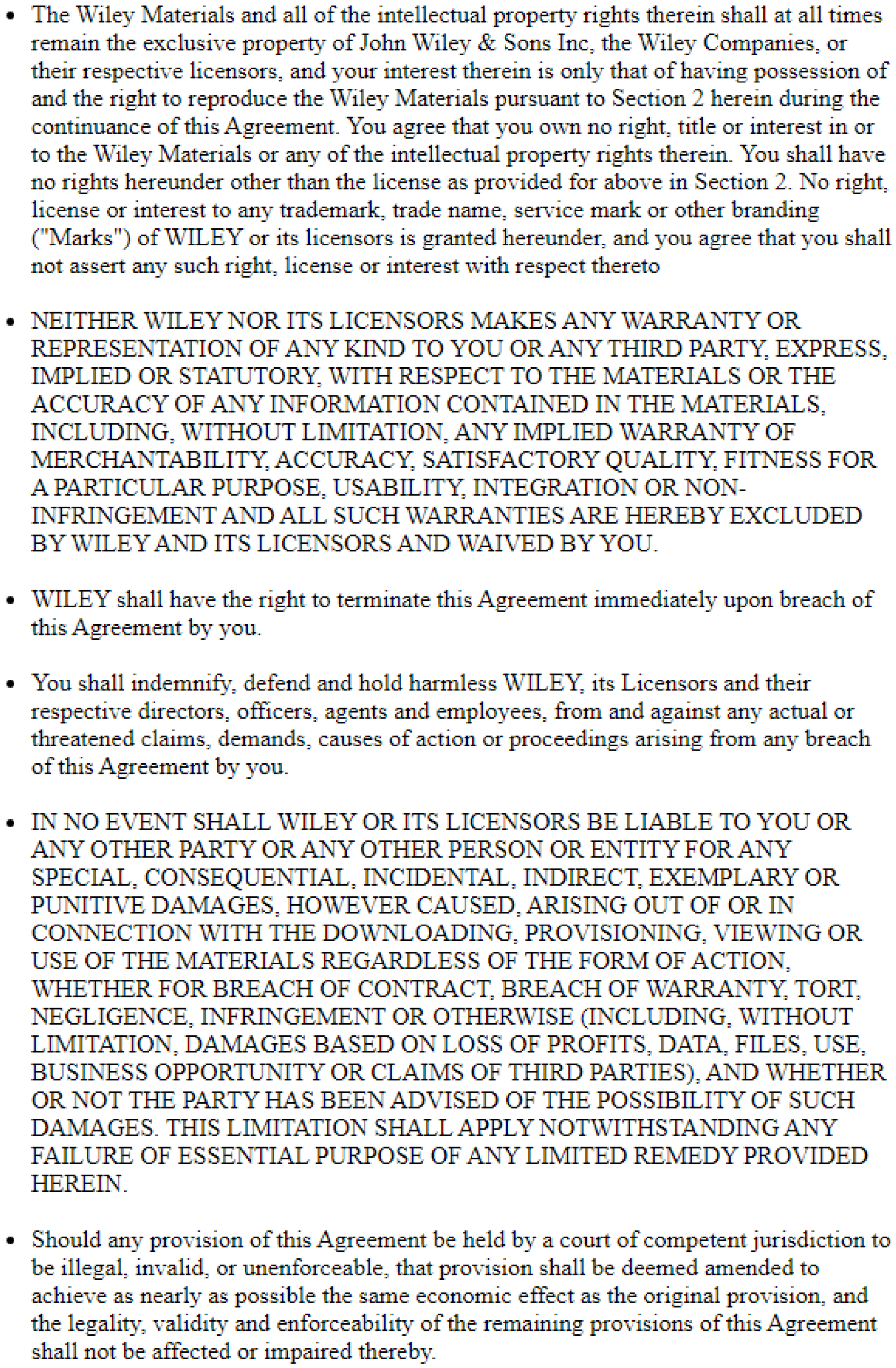
This copyrighted material is owned by or exclusively licensed to John Wiley & Sons, Inc. or one of its group companies (each a"Wiley Company") or handled on behalf of a society with which a Wiley Company has exclusive publishing rights in relation to a particular work (collectively "WILEY"). By clicking "accept" in connection with completing this licensing transaction, you agree that the following terms and conditions apply to this transaction (along with the billing and payment terms and conditions established by the Copyright Clearance Center Inc., ("CCC's Billing and Payment terms and conditions"), at the time that you opened your RightsLink account (these are available at any time at http://myaccount.copyright.com).

Terms and Conditions

- The materials you have requested permission to reproduce or reuse (the "Wiley Materials") are protected by copyright.

- You are hereby granted a personal, non-exclusive, non-sub licensable (on a stand-alone basis), non-transferable, worldwide, limited license to reproduce the Wiley Materials for the purpose specified in the licensing process. This license, **and any CONTENT (PDF or image file) purchased as part of your order,** is for a one-time use only and limited to any maximum distribution number specified in the license. The first instance of republication or reuse granted by this license must be completed within two years of the date of the grant of this license (although copies prepared before the end date may be distributed thereafter). The Wiley Materials shall not be used in any other manner or for any other purpose, beyond what is granted in the license. Permission is granted subject to an appropriate acknowledgement given to the author, title of the material/book/journal and the publisher. You shall also duplicate the copyright notice that appears in the Wiley publication in your use of the Wiley Material. Permission is also granted on the understanding that nowhere in the text is a previously published source acknowledged for all or part of this Wiley Material. Any third party content is expressly excluded from this permission.

- With respect to the Wiley Materials, all rights are reserved. Except as expressly granted by the terms of the license, no part of the Wiley Materials may be copied, modified, adapted (except for minor reformatting required by the new Publication), translated, reproduced, transferred or distributed, in any form or by any means, and no derivative works may be made based on the Wiley Materials without the prior permission of the respective copyright owner.**For STM Signatory Publishers clearing permission under the terms of the STM Permissions Guidelines only, the terms of the license are extended to include subsequent editions and for editions in other languages, provided such editions are for the work as a whole in situ and does not involve the separate exploitation of the permitted figures or extracts,** You may not alter, remove or suppress in any manner any copyright, trademark or other notices displayed by the Wiley Materials. You may not license, rent, sell, loan, lease, pledge, offer as security, transfer or assign the Wiley Materials on a stand-alone basis, or any of the rights granted to you hereunder to any other person.



- The Wiley Materials and all of the intellectual property rights therein shall at all times remain the exclusive property of John Wiley & Sons Inc, the Wiley Companies, or their respective licensors, and your interest therein is only that of having possession of and the right to reproduce the Wiley Materials pursuant to Section 2 herein during the continuance of this Agreement. You agree that you own no right, title or interest in or to the Wiley Materials or any of the intellectual property rights therein. You shall have no rights hereunder other than the license as provided for above in Section 2. No right, license or interest to any trademark, trade name, service mark or other branding ("Marks") of WILEY or its licensors is granted hereunder, and you agree that you shall not assert any such right, license or interest with respect thereto

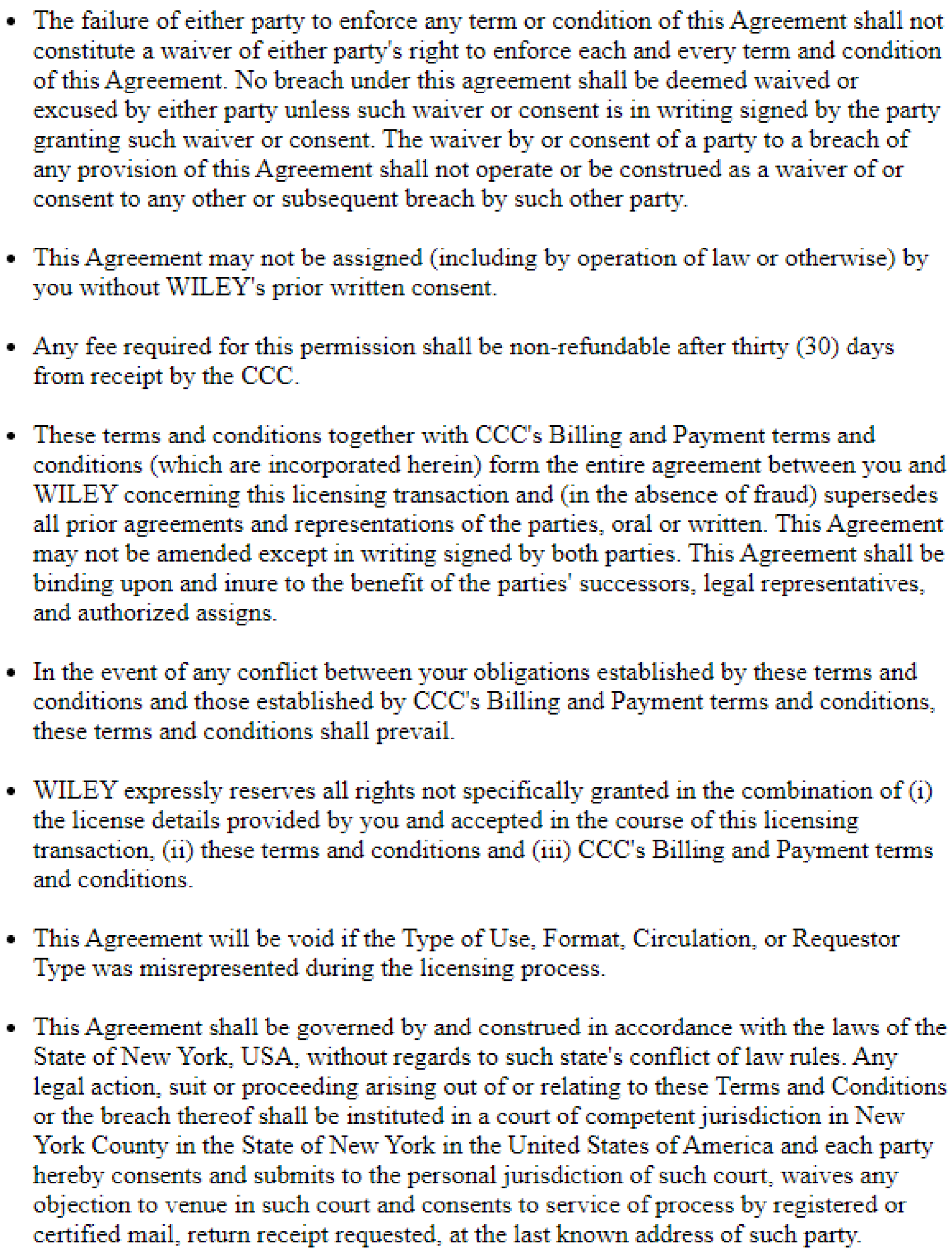
- NEITHER WILEY NOR ITS LICENSORS MAKES ANY WARRANTY OR REPRESENTATION OF ANY KIND TO YOU OR ANY THIRD PARTY, EXPRESS, IMPLIED OR STATUTORY, WITH RESPECT TO THE MATERIALS OR THE ACCURACY OF ANY INFORMATION CONTAINED IN THE MATERIALS, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY OF MERCHANTABILITY, ACCURACY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, USABILITY, INTEGRATION OR NON-INFRINGEMENT AND ALL SUCH WARRANTIES ARE HEREBY EXCLUDED BY WILEY AND ITS LICENSORS AND WAIVED BY YOU.

- WILEY shall have the right to terminate this Agreement immediately upon breach of this Agreement by you.

- You shall indemnify, defend and hold harmless WILEY, its Licensors and their respective directors, officers, agents and employees, from and against any actual or threatened claims, demands, causes of action or proceedings arising from any breach of this Agreement by you.

- IN NO EVENT SHALL WILEY OR ITS LICENSORS BE LIABLE TO YOU OR ANY OTHER PARTY OR ANY OTHER PERSON OR ENTITY FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, INDIRECT, EXEMPLARY OR PUNITIVE DAMAGES, HOWEVER CAUSED, ARISING OUT OF OR IN CONNECTION WITH THE DOWNLOADING, PROVISIONING, VIEWING OR USE OF THE MATERIALS REGARDLESS OF THE FORM OF ACTION, WHETHER FOR BREACH OF CONTRACT, BREACH OF WARRANTY, TORT, NEGLIGENCE, INFRINGEMENT OR OTHERWISE (INCLUDING, WITHOUT LIMITATION, DAMAGES BASED ON LOSS OF PROFITS, DATA, FILES, USE, BUSINESS OPPORTUNITY OR CLAIMS OF THIRD PARTIES), AND WHETHER OR NOT THE PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THIS LIMITATION SHALL APPLY NOTWITHSTANDING ANY FAILURE OF ESSENTIAL PURPOSE OF ANY LIMITED REMEDY PROVIDED HEREIN.

- Should any provision of this Agreement be held by a court of competent jurisdiction to be illegal, invalid, or unenforceable, that provision shall be deemed amended to achieve as nearly as possible the same economic effect as the original provision, and the legality, validity and enforceability of the remaining provisions of this Agreement shall not be affected or impaired thereby.



- The failure of either party to enforce any term or condition of this Agreement shall not constitute a waiver of either party's right to enforce each and every term and condition of this Agreement. No breach under this agreement shall be deemed waived or excused by either party unless such waiver or consent is in writing signed by the party granting such waiver or consent. The waiver by or consent of a party to a breach of any provision of this Agreement shall not operate or be construed as a waiver of or consent to any other or subsequent breach by such other party.

- This Agreement may not be assigned (including by operation of law or otherwise) by you without WILEY's prior written consent.

- Any fee required for this permission shall be non-refundable after thirty (30) days from receipt by the CCC.

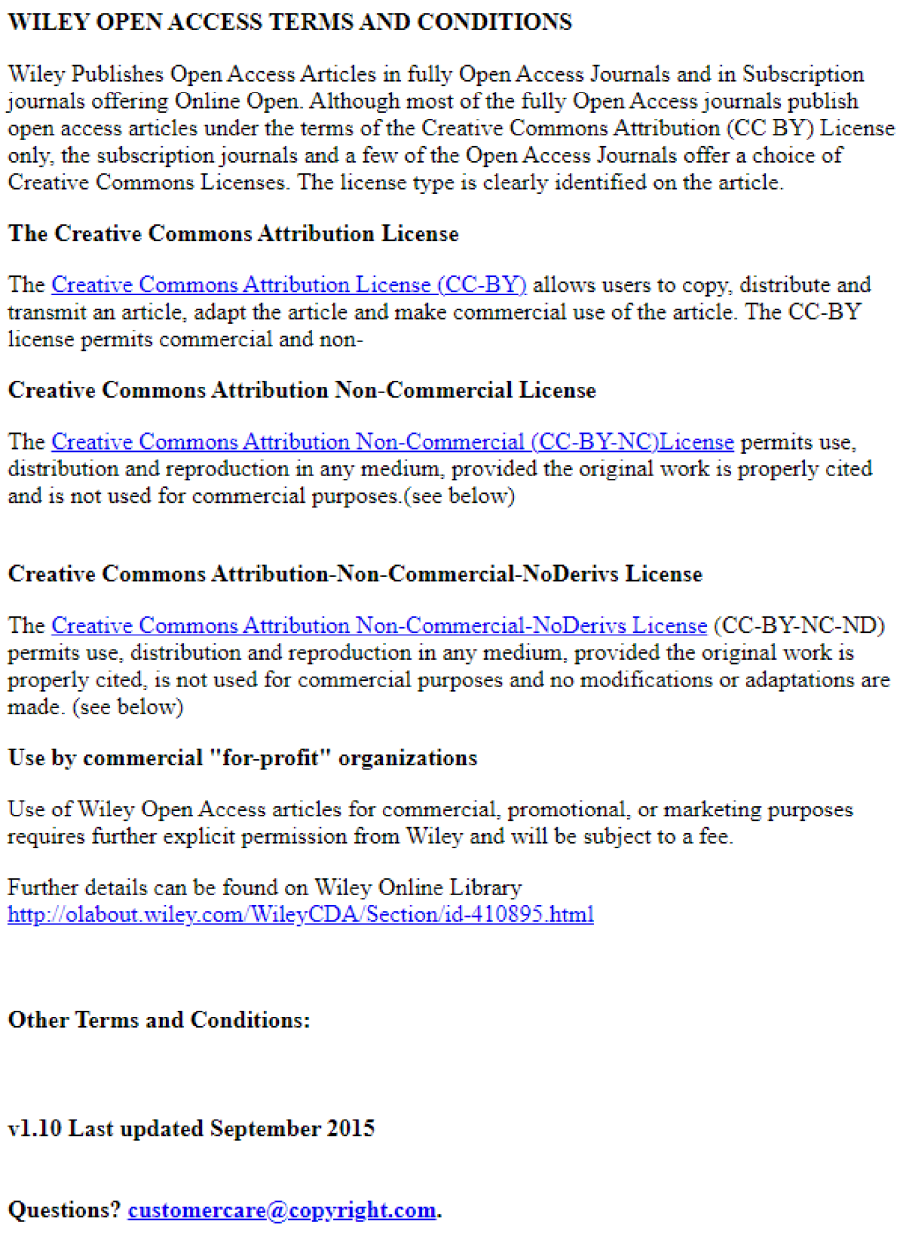
- These terms and conditions together with CCC's Billing and Payment terms and conditions (which are incorporated herein) form the entire agreement between you and WILEY concerning this licensing transaction and (in the absence of fraud) supersedes all prior agreements and representations of the parties, oral or written. This Agreement may not be amended except in writing signed by both parties. This Agreement shall be binding upon and inure to the benefit of the parties' successors, legal representatives, and authorized assigns.

- In the event of any conflict between your obligations established by these terms and conditions and those established by CCC's Billing and Payment terms and conditions, these terms and conditions shall prevail.

- WILEY expressly reserves all rights not specifically granted in the combination of (i) the license details provided by you and accepted in the course of this licensing transaction, (ii) these terms and conditions and (iii) CCC's Billing and Payment terms and conditions.

- This Agreement will be void if the Type of Use, Format, Circulation, or Requestor Type was misrepresented during the licensing process.

- This Agreement shall be governed by and construed in accordance with the laws of the State of New York, USA, without regards to such state's conflict of law rules. Any legal action, suit or proceeding arising out of or relating to these Terms and Conditions or the breach thereof shall be instituted in a court of competent jurisdiction in New York County in the State of New York in the United States of America and each party hereby consents and submits to the personal jurisdiction of such court, waives any objection to venue in such court and consents to service of process by registered or certified mail, return receipt requested, at the last known address of such party.



WILEY OPEN ACCESS TERMS AND CONDITIONS

Wiley Publishes Open Access Articles in fully Open Access Journals and in Subscription journals offering Online Open. Although most of the fully Open Access journals publish open access articles under the terms of the Creative Commons Attribution (CC BY) License only, the subscription journals and a few of the Open Access Journals offer a choice of Creative Commons Licenses. The license type is clearly identified on the article.

The Creative Commons Attribution License

The Creative Commons Attribution License (CC-BY) allows users to copy, distribute and transmit an article, adapt the article and make commercial use of the article. The CC-BY license permits commercial and non-

Creative Commons Attribution Non-Commercial License

The Creative Commons Attribution Non-Commercial (CC-BY-NC)License permits use, distribution and reproduction in any medium, provided the original work is properly cited and is not used for commercial purposes.(see below)

Creative Commons Attribution-Non-Commercial-NoDerivs License

The Creative Commons Attribution Non-Commercial-NoDerivs License (CC-BY-NC-ND) permits use, distribution and reproduction in any medium, provided the original work is properly cited, is not used for commercial purposes and no modifications or adaptations are made. (see below)

Use by commercial "for-profit" organizations

Use of Wiley Open Access articles for commercial, promotional, or marketing purposes requires further explicit permission from Wiley and will be subject to a fee.

Further details can be found on Wiley Online Library
http://olabout.wiley.com/WileyCDA/Section/id-410895.html

Other Terms and Conditions:

v1.10 Last updated September 2015

Questions? customercare@copyright.com.