Modified Degradation Process Models and Statistical Methods for Assessing Robustness and Reliability of Complex Networks

Yuzhou Chen
yuzhouc@smu.edu

Follow this and additional works at: https://scholar.smu.edu/hum_sci_statisticalscience_etds

Recommended Citation

This Dissertation is brought to you for free and open access by the Statistical Science at SMU Scholar. It has been accepted for inclusion in Statistical Science Theses and Dissertations by an authorized administrator of SMU Scholar. For more information, please visit http://digitalrepository.smu.edu.
MODIFIED DEGRADATION PROCESS MODELS AND STATISTICAL METHODS
FOR ASSESSING ROBUSTNESS AND RELIABILITY OF COMPLEX NETWORKS

Approved by:

Dr. Hon Keung Tony Ng
Professor in Department of Statistical Science, Southern Methodist University

Dr. Jing Cao
Professor in Department of Statistical Science, Southern Methodist University

Dr. Chul Moon
Assistant Professor in Department of Statistical Science, Southern Methodist University

Dr. Yulia R. Gel
Professor in Department of Mathematical Sciences, University of Texas at Dallas
MODIFIED DEGRADATION PROCESS MODELS AND STATISTICAL METHODS
FOR ASSESSING ROBUSTNESS AND RELIABILITY OF COMPLEX NETWORKS

A Dissertation Presented to the Graduate Faculty of the
Dedman College
Southern Methodist University
in
Partial Fulfillment of the Requirements
for the degree of
Doctor of Philosophy
with a
Major in Statistical Science
by
Yuzhou Chen

B.S., Mathematics, Zhejiang Gongshang University
M.S., Statistics, University of Texas at Dallas

August 4, 2021
ACKNOWLEDGMENTS

First, I would like to thank my advisor, Professor Hon Keung Tony Ng for his support, guidance, and encouragement during my Ph.D. study. In my Ph.D. study, Professor Hon Keung Tony Ng gave me extremely visionary advice and most sincere and constructive feedback. Professor Hon Keung Tony Ng’s research foresight and technical depth to the students is a valuable treasure for me.

I am grateful to have the rest of my doctoral committee: Professor Jing Cao, Professor Chul Moon, and Professor Yulia R. Gel. I would like to thank them for their valuable suggestions and insightful discussions to greatly enhance the quality of this thesis. More importantly, through communication with my doctoral committee, I got to learn how extraordinary researchers think and solve problems.

I gave my sincere thanks to Professor Yulia R. Gel. She is my first mentor in network analysis, and topological and geometric methods in statistics. Professor Yulia R. Gel offered me invaluable advice and most generous support in my research journey.

I would also like to take this moment to express my deep appreciation to other Professors and collaborators for their excellent guidance and help during my Ph.D. study.

Finally, I would like to thank my parents and my wife for their unconditional support and encouragement.
Modified Degradation Process Models and Statistical Methods
for Assessing Robustness and Reliability of Complex Networks

Advisor: Dr. Hon Keung Tony Ng
Doctor of Philosophy degree conferred August 4, 2021
Dissertation completed July 23, 2021

Many modern systems and collections of components/devices can be represented as complex networks. These networks, such as the cyberspace, internet, power grids, and water supply chains, are expected to exhibit high-reliability levels since failures of these systems can lead to catastrophic cascading events. As a result, enhancing our understanding of the mechanisms behind the functionality and reliability of such networks is the key to ensure the security, sustainability, and resilience of most modern critical infrastructures. While there exists a broad variety of statistical methods for assessing the reliability of networks, most existing techniques utilize only a single network topological metric. There is an urgent need to develop advanced methodologies that can systematically assess the risk, robustness, reliability, or vulnerability of a network and compare the risks of different networks.

In this thesis, we develop a novel stochastic modeling approach based on multiple interdependent topological measures of complex networks. The key engine behind our approach is to evaluate the dynamics of multiple network motifs as descriptors of the underlying network topology and its response to adverse events. Under a framework of the gamma degradation model, we develop a formal statistical framework for the analysis of reliability and robustness of a single complex network as well as for assessing differences in reliability properties exhibited by two different networks. We validate the proposed methodology with extensive Monte Carlo simulation studies and illustrate the utility of the proposed approach by performing a vulnerability analysis of European power grid networks under various targeted attacks.
Furthermore, we also consider cyber systems and computer infrastructures for commerce and communications such as cyberspace, the Internet, electronic payment systems. Cybersecurity insurance is one of the possible ways to manage risk exposure for these complex cyber networks. Therefore, comprehending how vulnerable is a cyber or physical network to attacks or failures and assessing the risks of a complex network is of great interest. To understand the risks of complex networks, we propose a modified Wiener process model for the degeneration of the network functionality upon the removal of nodes due to attacks or malfunctions. We also propose three statistical testing procedures based on the Wiener process model to compare the risk and resilience of two different networks, which can be used to comparing risks in the cybersecurity insurance domain. The proposed methodologies can be applied to any topological measures of network robustness or risk. A practical data analysis for a peer-to-peer file-sharing network is presented to illustrate the proposed model and methods. Monte Carlo simulations are used to evaluate the performance of the proposed methodologies and practical recommendations are provided.
# TABLE OF CONTENTS

LIST OF FIGURES.................................................................................................................. x

LIST OF TABLES ...................................................................................................................... xi

CHAPTER

1. INTRODUCTION .............................................................................................................. 1
   1.1. Background ............................................................................................................... 1
   1.2. Graph representation of networks ............................................................................ 1
   1.3. Motif-based analysis of complex networks .............................................................. 3
   1.4. Stochastic Process Models ....................................................................................... 6
   1.5. Synopsis of the Thesis ............................................................................................. 8

2. Understanding Power Grid Network Vulnerability through the Stochastic Lens of Network Motif Evolution ...................................................... 12
   2.1. Introduction: Motivation and Overview .................................................................. 13
   2.2. Background on Network Motifs .............................................................................. 14
   2.3. Stochastic Process Model and Statistical Hypothesis Tests .................................. 15
      2.3.1. Modified Gamma Degradation Model .............................................................. 15
      2.3.1.1. Likelihood Ratio Test on Network Motifs ................................................. 18
      2.3.2. Testing on Network Motif Importance .......................................................... 20
         2.3.2.1. Hypothesis Testing for a Subset of Network Motifs ......................... 20
         2.3.2.2. Determine which Network Motifs Contribute to the Difference ........ 21
   2.4. Analysis of Power Grid Network Data ................................................................. 23
      2.4.1. Data Description .............................................................................................. 23
      2.4.2. Comparing Network Vulnerability ................................................................. 24
      2.4.3. Determine which Motifs Contribute to the Difference ................................... 27
A. APPENDIX of CHAPTER 2 .......................................................... 66

A.1. Existence and Uniqueness of the Maximum Likelihood Estimators ....... 66

A.2. Comparison to the Conventional Vulnerability Metrics for Power Grid Networks .......................................................... 69

A.2.1. Graph-theoretic metrics .................................................... 69

A.2.2. Higher-order structures and electricity-based metrics ................. 70

A.3. Functionality of Power Grid Network under Attacks ....................... 71

A.3.1. Relations between Network Motifs and Functionality of Power System 73

A.3.2. The Impact of Removing Transmission Lines ......................... 74

A.4. Sensitive Analysis ............................................................... 76

A.5. Computation and Memory Usage ......................................... 78

A.6. Power Systems from TAMU Repository .................................. 79

BIBLIOGRAPHY ........................................................................... 79
# LIST OF FIGURES

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1</td>
<td>Higher-order structures are captured by network motifs. All connected 3-node and 4-node undirected motifs (left) and all connected 3-node directed motifs (right).</td>
<td>5</td>
</tr>
<tr>
<td>2.1</td>
<td>Toy examples for Case 1 (left), Case 2 (center), and Case 3 (right), where x-axis is the observation point and y-axis is the number of the $j$-th $\ell$-node motif for network $i$ at the observation point.</td>
<td>18</td>
</tr>
<tr>
<td>2.2</td>
<td>Degradation of motifs of six power grids under degree-based attack.</td>
<td>25</td>
</tr>
<tr>
<td>2.3</td>
<td>Heatmap with pairwise $p$-value between six European power grids.</td>
<td>26</td>
</tr>
<tr>
<td>2.4</td>
<td>Degradation of motifs of six power grids under betweenness-based attacks.</td>
<td>31</td>
</tr>
<tr>
<td>2.5</td>
<td>Degradation of motifs of six power grids under eigenvector-based attacks.</td>
<td>32</td>
</tr>
<tr>
<td>2.6</td>
<td>Simulated rejection rates for $\mathcal{K} = 10$ (red) and 30 (blue) with $a = {0.1, \cdots, 2.0}$.</td>
<td>35</td>
</tr>
<tr>
<td>2.7</td>
<td>Simulated and observed motifs curves of the six power grids under degree-based attacks.</td>
<td>36</td>
</tr>
<tr>
<td>2.8</td>
<td>Simulated and observed motifs curves of the six power grids under betweenness-based attacks.</td>
<td>37</td>
</tr>
<tr>
<td>2.9</td>
<td>Simulated and observed motifs curves of the six power grids under eigenvector-based attacks.</td>
<td>37</td>
</tr>
<tr>
<td>3.1</td>
<td>All connected 4-node network motifs.</td>
<td>44</td>
</tr>
<tr>
<td>3.2</td>
<td>A synopsis of the network structure of a P2P system [105].</td>
<td>53</td>
</tr>
<tr>
<td>3.3</td>
<td>The dynamics of the degradation (in percentages) of the three 4-node motifs of the three networks $G_1$, $G_2$, and $G_3$ under degree-based attacks with $\mathcal{K} = 11$ observation points.</td>
<td>56</td>
</tr>
<tr>
<td>Table</td>
<td>Page</td>
<td></td>
</tr>
<tr>
<td>-------</td>
<td>------</td>
<td></td>
</tr>
<tr>
<td>2.1</td>
<td>Basic network structure information of six European power grids.</td>
<td>24</td>
</tr>
<tr>
<td>2.2</td>
<td>Estimates of the gamma degradation model parameters for six power grids dataset under degree-based attack.</td>
<td>27</td>
</tr>
<tr>
<td>2.3</td>
<td>Estimates of the gamma degradation model parameters for Italy and Spain power grids under degree-based attack with assuming $\beta_{Italy} = \beta_{Spain} = \beta$.</td>
<td>27</td>
</tr>
<tr>
<td>2.4</td>
<td>Parameter estimates of the gamma degradation model for the six power grids under betweenness-based attacks.</td>
<td>32</td>
</tr>
<tr>
<td>2.5</td>
<td>Parameter estimates of the gamma degradation model for the six power grids under eigenvector-based attacks.</td>
<td>33</td>
</tr>
<tr>
<td>2.6</td>
<td>Simulated rejection rate for different values of $a = {0.1, \cdots, 2.0}$ with $K = {10, 30}$.</td>
<td>36</td>
</tr>
<tr>
<td>2.7</td>
<td>Simulated rejection rates between two sub-graphs under BFS sampling with fraction $f$ from the power grid networks of Germany, France and Spain.</td>
<td>39</td>
</tr>
<tr>
<td>3.1</td>
<td>Basic network structure information of the three Gnutella computer networks.</td>
<td>53</td>
</tr>
<tr>
<td>3.2</td>
<td>Maximum likelihood estimates of the drift parameters and the diffusion coefficient in the Wiener process model for $G_1$, $G_2$, and $G_3$ under degree-based attack.</td>
<td>56</td>
</tr>
<tr>
<td>3.3</td>
<td>The observed values of the test statistics and the corresponding p-values based on Procedures A, B1 and B2 for the pairwise comparisons of the three networks $G_1$, $G_2$, and $G_3$.</td>
<td>56</td>
</tr>
<tr>
<td>3.4</td>
<td>Simulated rejection rates for network data generated from the Wiener process model.</td>
<td>60</td>
</tr>
<tr>
<td>3.5</td>
<td>Simulated rejection rates between two subgraphs under BFS sampling with $100%$ nodes, where $\tau \in {0.50, 0.55, \cdots, 0.70}$ from the P2P networks $G_1$ and $G_3$.</td>
<td>62</td>
</tr>
</tbody>
</table>
A.1 Network-based vulnerability metrics for the European power grid networks.

A.2 Dynamics of motifs remaining, mean LOLP (LOLP), and mean EUE (EUE) for ACTIVSg500 and ACTIVSg2000 power systems under degree-based attacks, respectively; the average degradation rate \( \bar{A} \) for ACTIVSg500 and ACTIVSg2000 power systems based on (1) 4-node motifs, (2) \( \text{LOLP} \) and \( \text{EUE} \). ................................................................. 72

A.3 Dynamics of motifs remaining, the fraction of load served, and the fraction of generators operating for the IEEE 118-Bus system under attacks (fraction of nodes removed). ............................................................... 73

A.4 Correlation coefficients between the remaining 4-node motifs and three electrical properties (i.e., power flow, fraction of load served, and fraction of generators operating) by randomly removing nodes. .................... 74

A.5 Number of lines in service and number of lines which power flow direction is impacted by random attacks. ................................................................. 75

A.6 Dynamics of 4-node motifs remaining \( (M_1, M_2, M_3, \text{ and } M_4) \), the fraction of load served, and the fraction of generators operating for the IEEE 118-Bus system under random attacks (fraction of lines removed)............. 75

A.7 Correlation coefficients between the remaining 4-node motifs and two electrical properties (i.e., fraction of load served and fraction of generators operating) by randomly removing links/edges. ............................ 76

A.8 Simulated rejection rates for settings \( S_1, S_2, \text{ and } S_3 \). ................................. 78

A.9 Average running time and memory used for seven tasks/procedures in this paper. 79

A.10 Basic components information of three synthetic power systems. ............... 79
This dissertation is dedicated to my family.
CHAPTER 1
INTRODUCTION

1.1. Background

Reliability and robustness analysis for complex systems is one of the important topics in system design and analysis, which has a wide range of applications in power systems, peer-to-peer (P2P) networks, blockchain, and financial systems, etc. In recent years, complex systems such as power systems and financial systems have posed more potential threats of cyber-attacks. Therefore, to better assess the behavior of complex systems under attacks and control and minimize the cost of failure, reliability and robustness analysis can be used to detect the proper resilience metrics and robustness structures. The evaluation of reliability and resilience is one of the key aspects of the design and planning of complex systems. In this dissertation, we illustrate the utility of the robustness metrics and apply different stochastic models for accessing the reliability of complex networks.

In this chapter, we first introduce the graph representation of networks and the concept of motif-based analysis of complex networks. Then, we review some stochastic process models that will be applied in the methodologies proposed in this thesis.

1.2. Graph representation of networks

A graph structure can be represented as $\mathcal{G} = \{\mathcal{V}, \mathcal{E}, W\}$, where $\mathcal{V}$ is a node set with cardinality (the number of elements in a set) $|\mathcal{V}|$ of $N$, $\mathcal{E} \subseteq \mathcal{V} \times \mathcal{V}$ is an edge set, and $W$ is
the adjacency matrix of $G$, which is an $N \times N$ nonnegative symmetric matrix with entries $\{\omega_{ij}\}_{1 \leq i,j \leq N}$, i.e., $\omega_{ij} \neq 0$ for any $e_{ij} \in \mathcal{E}$ and $\omega_{ij} = 0$, otherwise. In our study, we consider unweighted and undirected graph, i.e., $\omega_{ij} = 1$ and $e_{ij} = e_{ji} \in \mathcal{E}$, for all $1 \leq i, j \leq N$. Hence, we suppress the notation of the adjacency matrix in the graph representation and represent the graph as $G = \{V, E\}$, where $V = \{v_1, v_2, \ldots, v_n\}$ (where $n$ is the number of nodes in graph $G$) is the node set and $E \subseteq \{ (v_i, v_j) | v_i, v_j \in V \}$ is the edge set. In the unweighted graph, edge weights are binary, i.e., $e_{i,j} = 1$ if there is an edge between nodes $i$ and $j$ and 0 otherwise. In contrast, in weighted graph, the edge weights are real numbers which represent the similarity or relatedness between two nodes.

Graphs are the most widely used representation to study the information management and hidden patterns among the elements in the complex system [10]. In recent decades, the analysis of complex systems with graph theory has been studied and applied to solve many real-world problems. For example, for the protein-protein interactions (PPI) in a cell that describe the physical contacts of high specificity established between molecules, although there are a bunch of methods have been proposed to detect PPI [50, 63, 108], these methods may not be able to capture the information about fraction of existing interactions. To capture the interactions between two proteins, Brohée and van Helden [17] and Sprinzak et al. [103] considered the interaction between proteins as interaction graph where the nodes represent proteins and edges represent the interaction between two proteins. Equipped with graph theory, the descriptive statistics, e.g., the distribution of node degree, graph diameter can help better understand the relationship between the organization and functionality of PPI.

Given the rising complexity of modern economies and societies, power systems are the backbone of modern life. In order to study the design and performance of power systems, engineers are required to understand the components in a power system and assess the reliability of the power system. Reliability evaluation is very critical for the planning and operation of power systems, where it can ensure robust performance and maximize the
plant availability under normal and faulty operational scenarios. Analysis of power networks in electrical engineering [11, 13, 72] provides many effective metrics (e.g., resourcefulness, adaptability, and rapid recovery) and methods to evaluate and compare the resilience between different power systems. However, these metrics and methods may not efficiently capture the geometric and topological information from power systems. To enhance the learning of feature representations and the ability to model complex hidden information, graph theory has been applied to the robustness studies of power systems [37]. For power systems, Watts [118] treated the Western States Power Grid of the US as an unweighted network, where the nodes in the graph represent generators, transformers, and substations. In addition to power systems, there are numerous applications of graphs for network analysis in different disciplines, for example, Anand et al. [7] examined the role of macroeconomic fluctuations of a financial system via using a network structure where the nodes are international/domestic banks. Dunne et al. [35] converted food-web data to the network structure and study its topological properties via clustering coefficients and degree distributions.

1.3. Motif-based analysis of complex networks

The evaluation of complex network resilience is challenging due to the complex intra-dependencies and inter-dependencies structures generated from different types of nodes and edges. Traditional graph metrics such as betweenness centrality (BC), graph diameter (D), average path length (APL), clustering coefficient (CC), critical threshold $f_c$ based on the giant component assessment [4, 31, 130], and estimated scale parameter $\gamma$ from the approximating exponential cumulative degree distribution [92] can be used to describe the network topology and quantify network robustness. For example, BC is the fraction of shortest paths that pass through each node where the range of BC score is between 0 and 1; CC ($C_u$) is the number of connected pairs between the 1-hop neighborhood of the target node $u$; $D$ ($d_{u,v}$) is the average length (i.e., number of edges) of the shortest path between nodes $u$ and $v$. The directions of these vulnerability metrics change in response to the increase of
resilience/robustness of a network can be described as follows:

\[
\text{APL} \downarrow \text{D} \downarrow \text{CC} \uparrow \text{BC} \downarrow f_c \uparrow \gamma \downarrow.
\]

In other words, lower APL, lower D, higher CC, lower BC, higher \( f_c \), and lower \( \gamma \) are typically considered to be associated with small world-ness and higher resilience.

However, traditional resilience metrics have three main drawbacks: (i) these global-level metrics tend to focus on global topological information and thus, they may fail to capture the hidden mechanisms such as local information from communities and local substructures; for instance, the BC score always uses for flow network which can capture the traffic capacities between nodes, however, it has been shown that the BC score may not be appropriate when there exists loop structures (i.e., higher-order structures) in flow network [41]; (ii) the evaluation results from these traditionally resilience metrics may not be consistent, i.e., one network can have both low APL (the lower APL, the higher topological resiliency of the network is) and low CC (the higher CC, the higher topological resiliency of the network is). Furthermore, we found that, under different attack strategies, the evaluation results from these traditional resilience metrics can be different; (iii) the focus of these traditional graph metrics is mostly on critical components/nodes (i.e., without all connected components/nodes are considered).

Due to these drawbacks, to better assess the network resilience, we consider the local topological information from the topological perspective by encoding richer topological information via higher-order connections. In recent years, the analysis of the higher-order structure of complex networks has been proposed to learn the functionality and representation of graph structure data and attract a growing interest [30, 94, 126]. One of the most representative higher-order structure features is network motifs, which are recurrent multi-node topological patterns that tend to appear more often than it would be expected in a randomized network. Network motifs are first introduced by Alon [6] in the transcrip-
tional regulation network of bacteria and widely used in cellular networks of transcription-regulation and protein-protein interaction. Different from regular resilience metrics, network motifs can capture the prominent connectivity patterns which are essential to understanding the node and structural information in the network. It is worth noting that different types of network motifs have different functionalities and focuses, for example, feed-forward loop (FFL) [28, 70] constitutes a gene circuit that can be used to model the correlation between multiple circuit architectures and network motifs connected by the minimum spanning tree format can degrade the dynamic stability of power systems.

Figure 1.1: Higher-order structures are captured by network motifs. All connected 3-node and 4-node undirected motifs (left) and all connected 3-node directed motifs (right).

Formally, let $G = (V, E)$ and $G' = (V', E')$ be two undirected graphs. Graph $G'$ is a sub-graph of graph $G$ if $V' \subseteq V$ and $E' \subseteq E$. If $G' \subseteq G$ contains all edges between $u$ and $v$ ($u, v \in V'$), then $G'$ is called an induced sub-graph of $G$. Broadly speaking, network motifs are induced $\ell$-node subgraphs of $G$, $\ell > 2$. While in the earlier studies, only subgraphs $G'$ that occur more or less frequently than expected, have been called network motifs. Nowadays, the term network motif is referred generally to all induced subgraphs $G'$. Figure 1.1 presents some commonly used higher-order structures including the undirected 4-node motifs as well as the directed and undirected 3-node motifs. Following [30, 97], we primarily focus on 4-node motifs as descriptors of complex network response to disruptive events.

There exist many algorithms to count the exact number of network motifs via enumerating and sampling subgraphs, for example, RANDESU [120], MFinder [75], MAVISTO [96],
and G TrieScanner [89]. Based on the ESU-tree structure, the RANDESU motif finder algorithm is less dependent on the size of the graph and thus is significantly faster than other existing approaches. In our experiments, we utilize the FANMOD tool [121] for motif computations, which implements the RANDESU algorithm. It worth mentioning that the detected network motifs can be fed into the statistical and machine learning models for different tasks.

1.4. Stochastic Process Models

In engineering and sciences, degradation process is defined as a gradually and irreversible accumulation loss of system functionality during system life cycle or significant attacks [73, 100]. In order to characterize the evolutionary dynamics of degradation signals and measure the performance of system under attacks, there are many degradation data analysis methodologies and degradation models have been developed, which utilize the measurements of degradation signals to estimate the failure time and quantify the robustness level of the system. Some commonly used models are stochastic process models [61, 112] and Markov chain models [27, 43]. For stochastic process models, gamma process model, Wiener process model, and inverse-Gaussian process model are widely used to model the degradation processes of systems.

The Wiener process model is one of the greatest assets of the Markov processes due to the attractive theoretical properties of normal distribution [106, 125, 127, 129]. Usually, the degradation process of the target complex system can be characterized by a normal distribution when the degradation process is non-monotonic over time. For the cumulative degradation value of the system \( i \) at time point \( t_k \), denoted as \( D_{i,k} \), we consider \( D_{i,k} \) follows a Wiener process with drift rate \( \mu_i > 0 \) and diffusion coefficient \( \sigma_i > 0 \). Then, \( D_{i,k} \) has the following properties:
1. $D_{i,0} = 0$, i.e., the degradation value is 0 at the initial time point;

2. For any time sequence, i.e., $0 < t_1 < t_2 < \cdots t_k < \cdots < t_n$ (where $k \in [1, n]$ and $n$ represents the total number of time points), the increments $D_{i,k} - D_{i,k-1}$ are independent with each other;

3. The increment between any two time points $D_{i,k} - D_{i,q}$ (where $k \neq q$) follows the normal distribution with mean $\mu_i$ and variance $\sigma_i^2$.

Given the increment $y_{i,k} = D_{i,k} - D_{i,k-1}$ and the parameter set $\Theta_i = (\mu_i, \sigma_i)$, the probability density function (PDF) of $y_{i,k}$ is given by

$$f_W(y_{i,k}) = \frac{1}{\sqrt{2\pi\sigma_i^2}} \exp \left[ -\frac{(y_{i,k} - \mu_i)^2}{2\sigma_i^2} \right], -\infty < y_{i,k} < \infty. \quad (1.1)$$

Although the Wiener process model can provide efficiency and remarkable performance for different datasets, it may not be precise enough to model monotonic degradation processes due to the degradation signals of the Wiener process model can increase and decrease over time. Fortunately, the gamma process model has been proven to be an appropriate model for the degradation signals that are monotonically accumulated over time (e.g., the light intensity of light-emitting diodes (LEDs) and corrosion of materials [9, 78, 101, 113]). Similar to the Wiener process, the gamma process model also belongs to the class of Markov processes, i.e., a stochastic process with independent and non-negative increments. In the gamma process model, we assume that the cumulative degradation $Y_i$ of system $i$ at time point $t_k$ follows a gamma distribution with shape parameter $\lambda_i > 0$, scale parameter $\beta_i > 0$ where are constants. The PDF of $y_{i,k}$ can be formulated as

$$f_G(y_{i,k}) = \frac{y_{i,k}^{\lambda_i - 1}}{\Gamma(\lambda_i)\beta_i^{\lambda_i}} \exp \left( -\frac{y_{i,k}}{\beta_i} \right), \quad y_{i,k} > 0, \quad (1.2)$$

where $\Gamma(z) = \int_0^\infty x^{z-1} \exp(-x) dz$. Note that $y_{i,k}$ can be viewed as an increment in the degradation processes.
However, there are some datasets which both the Wiener process and gamma process cannot provide a well fit, e.g., GaAs Lasers data [114]. When both Wiener and gamma processes cannot provide unreliable results, one can consider the inverse-Gaussian (IG) process proposed by Wasan [116], which was widely used for monotonic degradation path. The IG process has been studied and extended to handle covariates and random effects [114]. The IG process model is a natural alternative solution for degradation process modeling. To utilize the IG process, we assume that the degradation process follows an IG process, i.e., each increment $y_{i,k}$ of system $i$ at time point $t_k$ is statistical independent and has an IG distribution, denoted as $\text{IG}(\delta_i, \eta_i)$, where $\delta_i > 0$ is the mean which represents the degradation rate and $\eta_i > 0$ is the shape parameter which does not have direct physical meaning. Then, the PDF of $y_{i,k}$ is given by

$$f_{IG}(y_{i,k}) = \frac{\eta_i}{2\pi y_{i,k}^3} \exp\left(-\frac{\eta_i(y_{i,k} - \delta_i)^2}{2\delta_i^2 y_{i,k}}\right), y_{i,k} > 0. \quad (1.3)$$

1.5. Synopsis of the Thesis

After years of research and practice, achievements have been made in utilizing network motifs for the evaluation of network robustness, node classification, and network trend forecasting. For instance, Dey et al. [30] evaluated power system reliability using network motif concentrations calculated under a node-centrality-based attack. Yin et al. [126] developed a spectral graph clustering method based on eigenvalues and eigenvectors of network motif-based matrix. Wang et al. [111] presented a principal component analysis (PCA) that characterizes node importance in biological networks using network motifs. Tsourakakis et al. [107] developed a scalable graph clustering approach based on graph motifs. Hochreiter and Schmidhuber [46] and Chen and Ng [21] considered deep learning methods such as the Long Short-Term Memory (LSTM) neural networks for model the token price time series data based on network motifs. Lee et al. [58] utilized weighted multi-hop motif adjacency
matrices to capture higher-order neighborhoods for node classification in graph convolution networks. In this thesis, we further consider using network motifs to assess the robustness and reliability of complex networks.

Due to the random behaviour in reliability engineering, such as the stochastic nature of the failure, stochastic models have played an important role in reliability engineering. Stochastic model-based reliability, resilience, and similarity analysis have been developed in the literature. For example, Ng et al. [78] proposed a stochastic gamma process model for quantifying the similarity of two dissolution profiles. Wang et al. [115] utilized the generalized Wiener process for residual life estimation about crack size of product. Lawless and Crowder [57] constructed a tractable gamma-process model for Hudak Crack-growth Data [49] by incorporating random effects and covariates. Wang et al. [114] applied the IG process model for degradation GaAs lasers datasets and developed maximum likelihood inference. There is an increasing research interest in integrating Bayesian framework with Wiener process models [62, 119] for degradation signals of multiple-phase characteristics. In this thesis, we attempt to address two important questions: (i) how network motifs can be used to assess resilience of complex systems; and (ii) how to leverage network motifs and stochastic process models to facilitate effective applications to resilience analysis on complex systems under various types of intentional attacks. Here, to model the data for assessing the reliability of complex networks with specific data structures, we modify some existing degradation process models for this purpose. To the best of our knowledge, our proposed models are the first attempt in the direction of using stochastic process models equipped with local topological information for complex network resilience evaluation. In a broad sense, assessing robustness and reliability of complex systems is crucial, for power companies to improve power system security margins, for cyber insurance providers to deliver the risk for insured individuals/companies, for governments to take the most optimal policy action while minimizing the negative impact from attacks or failures.
This thesis is organized as follows. In Chapter 2, we focus on developing a novel stochastic modeling approach based on multiple independent local topological measures of complex network. First, we propose a modified gamma degradation model that takes network motifs as input. Then, we construct the likelihood function through the joint distribution of network motifs and propose a new statistical procedure for testing potential differences in network motifs exhibited by two networks. In our experiments, we illustrate the utility of the proposed motif-based methodology in application to vulnerability analysis of the European power grid networks and synthetic power systems under a broad range of hazardous scenarios. To assess the performance of the proposed approach under model uncertainties, we also perform extensive Monte Carlo simulation studies.

In Chapter 3, we propose a modified Wiener process model for the evaluation of network functionality under cyber attacks. First, we show the graph representation of the cyber network and utilize topological measures for evaluating the robustness/loss of availability of a network. Then, the proposed Wiener process model is used to model the dynamics of a cyber network losing its functionality/connectivity upon the removal of nodes. Different statistical testing procedures for comparing the risks of two networks are also presented. We conduct experiments on real data sets of the Gnutella peer-to-peer (P2P) cyber networks. Furthermore, we evaluate the performance of the proposed model and methods using a Monte Carlo simulation study.

In Chapter 4, we conclude that our proposed modified stochastic process models equipped with network motifs are able to accurately classify resilience of complex networks under attacks. Extensive Monte Carlo simulation studies based on a parametric model and non-parametric resampling verify the effectiveness of our proposed methodologies. In general, our work enables accurate robustness and reliability evaluation of complex networks, which provides important insights into the organization and planning of various complex systems.

Besides evaluating the robustness of complex systems, the qualitative and quantitative results based on our proposed models would be crucial for data-driven understanding of com-
plex system operation, that can help domain experts for effective real-time decision-making. For future research, we plan to integrate other state-of-the-arts higher-order connectivity patterns into time- and state-dependent Markov degradation models for learning the dynamic behavior of specific components under attacks and for discovering correlations between different higher-order connectivity patterns from complex systems.
CHAPTER 2

Understanding Power Grid Network Vulnerability through the Stochastic Lens of Network Motif Evolution

Many cyber-physical systems can be represented as complex networks. These networks such as the internet, power grids, and supply chains, are expected to exhibit high reliability levels since their failures can lead to catastrophic cascading events. As a result, enhancing our understanding of mechanisms behind functionality of such networks is the key toward ensuring security, sustainability, and resilience of most modern critical infrastructures. While there exists a broad variety of methods for assessing reliability of networks, most existing techniques utilize only a single network topological metric. In this chapter we develop a new stochastic model approach based on multiple interdependent topological measures of complex networks. The key engine behind our approach is to evaluate dynamics of multiple network motifs as descriptors of the underlying network topology and its response to adverse events. Under a framework of the gamma degradation family of models, we develop a formal statistical inference for analysis of reliability and robustness levels of a single complex network as well as for assessing differences in reliability properties exhibited by two different networks. Our studies on EU and US power grid networks indicate that the new approach delivers competitive performance, while requiring substantially less information about the underlying systems.
2.1. Introduction: Motivation and Overview

Reliability analysis of complex networks and, particularly, power grids nowadays constitutes one of the most actively developing interdisciplinary research directions, largely due to its key role in facilitating functionality, sustainability and resilience of modern critical infrastructures under random failures and targeted attacks [see, for example, 1, 34, 36, and references therein].

A conventional approach to address power grid network reliability is to assess dynamics of the graph structure described by various network topological characteristics such as, for instance, betweenness, clustering coefficient, and average path length, under adverse events [25, 33, 44, 81]. However, some recent studies, e.g., [30, 74, 93, 97] show that network robustness is also intrinsically connected to higher order network substructures, or network motifs. Network motifs, or recurrently re-appearing subgraphs, have been first analyzed in conjunction with biological systems [99] and later network motifs has been found to show high utility in understanding functionality of many complex phenomena, from gene-to-gene interaction to brain connectome to finance [see, e.g., 8, 52, 110, and references therein]. For instance, using the framework of ordinary differential equations, Schultz et al. [97] showed that abundance of tree-like structured motifs in the underlying power grid network leads to higher system instability and changing at least one tree-like motif to a cycle motif may result in improving the system response to perturbations. In turn, Dey et al. [30] showed how a nonparametric concept of data depth can be used to assess network resilience based on evolution of multiple motifs under attacks.

However, neither of these network motif studies offer a formal statistical inferential procedure to understand which motif or a subset thereof is important and how to test for differences in reliability levels of networks in terms of their motifs. In this chapter we aim to address this knowledge gap and develop statistical inference for accessing network reliability based on network motifs. Since network motifs reflect system connectivity while the system response
to disruptive events intrinsically depends on the network connectivity, modeling evolution of network motifs under random failures or intentional attacks can provide an insight on the power grid response and overall system reliability under hazards. Our key approach is based on viewing the gradually decreasing number of multiple network motifs under hazardous scenarios as a degradation process [14] and then developing a gamma degradation model to capture properties of the resulting network evolution [22, 64, 78]. In turn, assessing multiple degradation measures allows for better characterization of the system functionality under attacks and random failures.

There are numerous engineering studies on evaluating and predicting system reliability using degradation models [e.g., 42, 65, 80]. One of the commonly used degradation models is the gamma degradation model which describes the degradation process by a gamma process with stationary increments (decrements). However, neither a gamma process nor a degradation framework, in general, have ever been used before to address the important questions on network reliability described via network motifs and other network topological descriptors. In contrast to currently available techniques, the proposed methodology allows us to utilize the entire range of structure-dependent network motifs to conduct statistical inference on the network robustness and reliability, to access differences between the target network and any other networks, and to provide a vulnerability ranking of networks under various targeted attacks. In addition, we propose a novel network motifs importance ranking statistical test – partial motifs test – which provide a measure of importance of each network motif in identifying the difference in vulnerability between networks.

2.2. Background on Network Motifs

The concept of network motifs is first introduced by Shen-Orr et al. [99] in which network motifs are discovered in the gene regulation network of the bacteria in which the experiments showed that each of the motifs carries out a unique information processing function in the
biological network. Later network motifs have been proven to play a fundamental role in understanding hidden mechanisms behind functionality of many complex systems, from brain connectome to protein-protein interactions to power grids [see, for example, 30, 82, 126, and references therein]. More details of network motifs can be found in Chapter 1.

2.3. Stochastic Process Model and Statistical Hypothesis Tests

2.3.1. Modified Gamma Degradation Model

A degradation process in natural science and engineering is the process that a system or decreases in performance, reliability or life span of assets gradually and irreversibly over time. For example, lithium-ion batteries degrade gradually after they put into use and the capacity ratio at the charging cycles of lithium-ion batteries are recorded over time as the degradation measurements for system health management purposes. Degradation modeling attempts to characterize progression of the system degradation measurements. Different degradation models have been proposed and studied in the literature and gamma degradation model is one of the commonly used stochastic processes used to model a variety of monotonic degradation phenomena in engineering and science [see, for example, 19, 39, 76, 128, and references therein].

In this subsection, we consider network motif counts as the degradation measurement and introduce a modified gamma degradation model for these degradation measurements. Since network motifs are subgraphs that highly depend on the network structure and the numbers of \( \ell \)-node motifs remain in the network structure under attacks can be viewed as a monotone decreasing degradation process, therefore, a gamma degradation model is adopted here for modeling and statistical analysis. Since the counts of \( \ell \)-node motifs are dependent, it is reasonable to model these counts using a shared parameter. Suppose that \( I \) networks are under intentional attacks, the remaining numbers of the \( \ell \)-node motifs are observed at an
observation point \( t_k, k = 1, \ldots, K \), where \( K \) is the total number of observation points. For instance, the observation point \( t_k \) can be considered as a specific fraction of random/selective nodes (e.g., nodes with the highest degrees and nodes with the largest betweenness) being removed from the network. Let \( x_{i,j,k} \) be the number of the \( j \)-th \( \ell \)-node motif for the network \( i \) at observation point \( t_k \), \( j = 1, \ldots, J \) and \( k = 1, \ldots, K \). For the 4-node motifs, \( J = 6 \) and the six 4-node motifs are presented in Figure 1.1 (see Chapter 1). Under the logarithmic transformation, we define \( y_{i,j,k} = \log(x_{i,j,k}/x_{i,j,k+1}) \) and assumed that \( y_{i,j,k} \) are independent and identical gamma random variables with shape parameter \( \lambda_{i,j} > 0 \), and scale parameter \( \beta_i > 0 \), denoted as \( y_{i,j,k} \overset{iid}{\sim} Ga(\lambda_{i,j} \Delta t_i, \beta_i) \). Here, we assume that each \( \ell \)-node motif has its own shape parameter and different \( \ell \)-node motifs share the same scale parameter in a gamma process model. When the attack sequence is taken at points with equally spaced, without loss of generality, we can consider \( y_{i,j,k} \overset{iid}{\sim} Ga(\lambda_{i,j}, \beta_i) \). With probability density function (PDF)

\[
f(y_{i,j,k}) = \frac{y_{i,j,k}^{\lambda_{i,j} - 1}}{\Gamma(\lambda_{i,j})\beta_i^{\lambda_{i,j}}} \exp\left(-\frac{y_{i,j,k}}{\beta_i}\right), \quad y_{i,j,k} > 0,
\]

(2.1)

where \( \Gamma(z) = \int_0^\infty x^{z-1} \exp(-x)dx \).

The parameter \( \beta_i \) in the gamma degradation model in Equation (2.1) is intended to capture the dependence among the counts of different motifs within the same network. Based on the observed values (i.e., the motif counts) \( x_{i,j,k} \) and the proposed gamma degradation model, the likelihood function can be expressed as

\[
L(\theta) = \prod_{i=1}^{I} L_i(\theta_i),
\]

(2.2)

where

\[
L_i(\theta_i) = \prod_{j=1}^{J} \prod_{k=1}^{K} \frac{y_{i,j,k}^{\lambda_{i,j} - 1}}{\Gamma(\lambda_{i,j})\beta_i^{\lambda_{i,j}}} \exp\left(-\frac{y_{i,j,k}}{\beta_i}\right),
\]

(2.3)

\( \theta = (\theta_1, \ldots, \theta_I), \theta_i = (\lambda_{i,1}, \ldots, \lambda_{i,J}, \beta_i)^T \) are the parameters vectors. Based on the functions presented in Equations (2.2) and (2.3), the log-likelihood function for the \( i \)-th network can
be expressed as

\[
l_i(\theta_i) = \sum_{j=1}^{J} \left\{ -K \ln(\Gamma(\lambda_{i,j})) - KL_i \ln(\beta_i) + (\lambda_{i,j} - 1) \sum_{k=1}^{K} \ln(y_{i,j,k}) - \frac{\sum_{k=1}^{K} y_{i,j,k}}{\beta_i} \right\}
\]

\[
= -K \sum_{j=1}^{J} \ln(\Gamma(\lambda_{i,j})) - KL_i \ln(\beta_i) \sum_{j=1}^{J} \lambda_{i,j} + \sum_{j=1}^{J} (\lambda_{i,j} - 1) \sum_{k=1}^{K} \ln(y_{i,j,k}) - \frac{\sum_{j=1}^{J} \sum_{k=1}^{K} y_{i,j,k}}{\beta_i}.
\]

(2.4)

Theorems 2.3.1 and 2.3.2 hold for the log-likelihood function of the \(i\)-th network and ensure that the proposed gamma degradation model is identifiable.

**Theorem 2.3.1** Constancy on the boundary: \(\lim_{\lambda_{i,j} \to \infty} \sup_{\max(y_{i,j,k}) \leq \beta_i} l_i(\theta_i) \to -\infty.\)

**Theorem 2.3.2** Negative-definiteness of Hessian matrix \(H(\theta_i) \in \mathbb{R}^{(J+1) \times (J+1)}.\)

Proofs are provided in Appendix A.1.

Since there are situations that the counts of motifs at different time points are equal or the counts of motifs can be zero, to incorporate these cases in the likelihood function, we propose the following methods based on the stationary and independent increments property of the gamma process. In Figure 2.1, we provide some toy examples to describe the three specific cases:

- **Case 1:** \(x_{i,j,1} > x_{i,j,2} > \cdots > x_{i,j,k-1} = x_{i,j,k} > x_{i,j,k+1} > x_{i,j,k+2} > \cdots > x_{i,j,K} \neq 0\)

  In this case, we have \(y_{i,j,k-1} = \log(x_{i,j,k-1}/x_{i,j,k}) = 0\) for \(x_{i,j,k-1} = x_{i,j,k}.\) Since \(x_{i,j,\cdot}\) is independent with each other, we can get \(\log(x_{i,j,k-1}/x_{i,j,k}) \sim Ga(2\lambda_{i,j}, \beta_i)\) by adding \(\log(x_{i,j,k-1}/x_{i,j,k}) \sim Ga(\lambda_{i,j}, \beta_i)\) and \(\log(x_{i,j,k}/x_{i,j,k+1}) \sim Ga(\lambda_{i,j}, \beta_i)\) together.
• Case 2: \(x_{i,j,1} > x_{i,j,2} > \cdots > x_{i,j,k-1} > x_{i,j,k} = x_{i,j,k+1} = x_{i,j,k+2} = \cdots = x_{i,j,K} \neq 0\)

Similar to case 1, we can get 
\[
\log \left( \frac{x_{i,j,k-1}}{x_{i,j,K}} \right) \sim \text{Ga}((K + 1 - k) \lambda_{i,j}, \beta_i).
\]

• Case 3: \(x_{i,j,1} > x_{i,j,2} > \cdots > x_{i,j,k-1} > x_{i,j,k} = \cdots = x_{i,j,k+w-1} > x_{i,j,k+w} = \cdots = x_{i,j,K} = 0\)

When \(2 \leq w < K - k\), we can obtain 
\[
\log \left( \frac{x_{i,j,k-1}}{x_{i,j,k+w-1}} \right) \sim \text{Ga}(w \lambda_{i,j}, \beta_i)
\] and omit the number of the \(j\)-th \(\ell\)-node motif for the network \(i\) which is equal to zero.

The maximum likelihood estimates (MLEs) of the unknown model parameters can be obtained by maximizing \(L(\theta)\) with respect to \(\theta\). Here, we use the function \texttt{constrOptim} in R [86] to maximize the likelihood function in order to obtain the corresponding MLEs subject to the constraints \(\lambda_{i,j} > 0, \beta_i > 0, i = 1, \ldots, I, j = 1, \ldots, J\). In Appendix A.5, we provide the computation time and memory usage for the computation procedures presented in this chapter.

### 2.3.1.1. Likelihood Ratio Test on Network Motifs

Consider that the purpose of the study is to identify whether two networks are in the same resilience level/group, we propose a likelihood ratio test with the gamma degradation model to assess the statistical significance. We define the notation \(\mathcal{R}(\cdot)\) as the measure of
robustness of a network, which can be evaluated in different ways depending on the context and model under considerations. For instance, based on the gamma degradation model in Section 2.3.1, $R(\cdot)$ can be evaluated based on the parameters in the gamma degradation model. To evaluate and compare the robustness of two different networks, we consider the likelihood ratio test for testing the hypotheses:

$$H_0 : R(\text{Network}_i) = R(\text{Network}_{i'})$$

versus $H_1 : R(\text{Network}_i) \neq R(\text{Network}_{i'})$. (2.5)

Based on the gamma degradation model discussed in Section 2.3.1, the hypotheses in Equation (2.5) could be expressed as

$$H_0 : \beta_i = \beta_{i'}, \lambda_{i,j} = \lambda_{i',j} = \lambda_j$$

versus $H_1 : \beta_i \neq \beta_{i'}$ or $\lambda_{i,j} \neq \lambda_{i',j}$ for at least one pair of $i$ and $i'$. (2.6)

From the Neyman-Pearson lemma, the likelihood ratio test statistic is defined as

$$\Lambda = \frac{\max\{L(\hat{\theta}_0|H_0)\}}{\max\{L(\hat{\theta}_1|H_1)\}}.$$ (2.7)

where $\hat{\theta}_0$ is the MLE of $\theta$ under $H_0$ and $\hat{\theta}_1$ is the MLE of $\theta$ under $H_1$. In particular, $\hat{\theta}_0 = (\hat{\lambda}_1, \ldots, \hat{\lambda}_J, \hat{\beta})^T$ is the value of $(\lambda_1, \ldots, \lambda_J, \beta)^T$ that maximizes $L(\theta)$. In turn, $\hat{\theta}_1 = (\hat{\lambda}_{1,1}, \ldots, \hat{\lambda}_{1,J}, \hat{\beta}_1, \ldots, \hat{\lambda}_{I,1}, \ldots, \hat{\lambda}_{I,J}, \hat{\beta}_I)^T$ is the value that maximize the likelihood function in Equation (2.2).

Wilks’ theorem suggests that the asymptotic distribution of the log-likelihood ratio statistic follows a chi-square distribution with degrees of freedom $q = (I - 1)(J + 1)$, i.e., $-2\log(\Lambda) \overset{D}{\to} \chi^2(q)$. Hence, we reject the null hypothesis $H_0$ in Equation (2.6) at $\alpha$ level if
\(-2 \log(\Lambda) > \chi^2_\alpha(q)\), and the \(p\)-value of the likelihood ratio test can be obtained as

\[
\Pr(\chi^2(q) < -2 \log(\Lambda)),
\]

where \(\chi^2(q)\) is a random variable that follows a chi-square distribution with degrees of freedom \(q\). Note that the \(p\)-value obtained from the likelihood ratio test can be used to determine if two networks have the same level of resilience, robustness and reliability in terms of the measure \(R(\cdot)\). In particular, a smaller \(p\)-value (i.e., \(p\)-value closer to 0) indicates that two networks have different levels of robustness and a larger \(p\)-value (i.e., \(p\)-value closer to 1) indicates that two networks have similar levels of robustness. Therefore, the \(p\)-value in Equation (2.8) can be used as a similarity measure between two networks in terms of robustness.

2.3.2. Testing on Network Motif Importance

In addition to applying the likelihood ratio test based on all the \(\ell\)-node motifs to compare two networks in terms of robustness, we consider performing the analysis based on a subset of motifs as well as determining which motif contribute to the difference if the null hypothesis in Equation (2.6) is rejected.

2.3.2.1. Hypothesis Testing for a Subset of Network Motifs

In motif-based network analysis, researchers found that some of the \(\ell\)-node (\(\ell = 3, 4\)) motifs may reveal the dynamic properties of network and clearly capture the network architectural principles [see 30, 83, 107]. For example, in biological networks such as gene regulatory networks and protein-protein interaction networks, researchers found that the feed-forward loop (FFL) motif (3-node motif: an input node, an output node, and an internal node) has higher frequency in gene networks [6, 70] and the FFL motif has three important roles: (i)
pulse generation; (ii) performing SUM (addition) function; (iii) generating non-monotonic
input functions for genes. In the context of power grid network, the detour motifs suggested
by [97] have been shown that it is important for enhancing the overall dynamical stability
of power grid networks. The sketch of a detour motif contains at least three nodes in which
the degree of the detour node is two and the degrees of the other nodes are greater than
or equal to two. In a simulation study of artificially power grids and a case study of the
northern European power grid [74], the tree-like dead ends (i.e., minimum spanning trees
where $|E| = |V| - 1$) have shown to be weakening the stability of power grids. Hence, the
hypotheses in Equation (2.5) can be tested based on a subset of specific motifs. Using some
specific motifs that are known to be relate to the robustness of power grid network may
improve the detection accuracy and reduce the computational efforts.

In turn, in many applications it is possible that some motifs could not be observed in the
network, especially for smaller networks. For instance, the number of the $j$-th $\ell$-node motif
in the network $i$ at any observation point, denoted as $x_{i,j,\ell}$, can always equal to zero, i.e.,
there is no observed motif $M_j$ in the network $i$. In this situation, the hypotheses in Equation
(2.5) can be tested based on a subset of motifs that are non-zero for the two networks under
consideration.

2.3.2.2. Determine which Network Motifs Contribute to the Difference

In comparing the network robustness between two networks based on the gamma degra-
dation model and likelihood ratio test described in Section 2.3.1, if the null hypothesis in
Equation (2.6) is rejected, it will be interesting to determine which motif(s) is (are) con-
tributed to the difference. This problem is similar to the paired comparisons after the
rejection of an overall $F$-test in regression analysis or analysis of variance (ANOVA). In
particular, in multiple regression with two or more explanatory variables, we are interested
in testing whether a certain subset of the regression coefficients are significant after the null
hypothesis of an overall $F$-test is rejected. A partial $F$ test that involves the comparison of the sum of squared errors (SSE) of the reduced model (i.e., excluding the parameters hypothesized to be significant) to the SSE of the full model (including all the parameters) is used for this purpose. Here, we propose a test for comparing network robustness based on motifs using the concept of partial $F$ test. Hence, we name this proposed test as partial-motifs test.

Suppose that the null hypothesis on Network$_i$ and Network$_i'$ in Equation (2.6) is rejected, we propose a partial-motifs test procedure by focusing on a single shape parameter $\lambda_j$ and assuming $\lambda_{i,j}$ equals to $\lambda_{i',j}$ for $j \neq \tilde{j}$.

The proposed partial-motifs test is summarized in Algorithm 1. By implementing the partial-motifs tests for different values $\tilde{j} = 1, 2, \ldots, J$, the corresponding $p$-values can be used as difference factor and similarity factor for network motifs categorization/contribution, which are used in describing influential power of motifs in comparing the robustness of power grid networks.

Note that the proposed partial-motifs test considers testing different alternative hypotheses $H_{1(j)}$ (i.e., assuming only $\lambda_{i,j}$ equals to $\lambda_{i',j}$ for $j \neq \tilde{j}$ in the alternative hypothesis $H_1$, see Line 5 in Algorithm 1) with the same null hypothesis $H_0$. We can also consider another way to implement the partial-motifs test by testing different null hypotheses $H_{0(j)}$ (i.e., assuming only $\lambda_{i,j}$ equals to $\lambda_{i',j}$ for $j \neq \tilde{j}$ in the null hypothesis $H_0$) with the same null hypothesis $H_1$. This partial-motifs test, namely the inverse-partial-motifs test, can be used to verify the results of the partial-motifs test. These procedures will be illustrated in the numerical example in Section 2.4.
Algorithm 1 Partial Motifs Test

**Input:** Degradation $J$-node motifs data $(X, X')$ for Network $i$ and Network $i'$

**Output:** $p$-values from leave-one-parameter-out hypotheses $H_0$: $\beta_i = \beta_i' = \beta, \lambda_{i,j} = \lambda_{i',j} = \lambda_j$, where $j = 1, \ldots, J$

for $j \in \{1, \ldots, J\}$ do

$H_{1(j)}: \beta_i \neq \beta_i', \lambda_{i,j} = \lambda_{i',j}, \lambda_{i,j} \neq \lambda_{i',j}$, where $j \neq \tilde{j}$

Feed $(X, X')$ into log-likelihood function Obtain MLEs

\[
\begin{align*}
\hat{\theta}_0 &= (\hat{\lambda}_1, \ldots, \hat{\lambda}_J, \hat{\beta}), \quad \text{under } H_0 \\
\hat{\theta}_{1(j)} &= (\hat{\lambda}_{\tilde{j}}, \hat{\lambda}_{i,j}, \hat{\lambda}_{i',j}, \hat{\beta}_i, \hat{\beta}_i'), \quad \text{under } H_{1(j)}
\end{align*}
\]

Calculate LRT $j = -2\log \left[ \frac{L(\hat{\theta}_0)}{L(\hat{\theta}_{1(j)})} \right]$, $\hat{\theta}_{1(j)}$ is the MLE under $H_{1(j)}$

Calculate the $p$-value $j = \Pr(\text{LRT}_j > \chi^2(J))$ based on the partial motifs test hypothesis

end

Compare the absolute differences among $J$ scenarios between $p$-value $= [p$-value$_1, \ldots, p$-value$_J]$ from partial motifs test and the $p$-value$^*$ from the overall test

2.4. Analysis of Power Grid Network Data

2.4.1. Data Description

To illustrate utility of the new methodology, we study the data from the Union for the Coordination of Transport of Electricity (UCTE) that includes power grid networks of 15 European countries (https://www.ucte.org/). For illustrative purposes, we consider six European countries: France, Germany, Italy, Poland, Romania and Spain. The nodes in each network represent the various substations, and the edges represent the high voltage transmission lines that connect different substations. To measure the remaining functionality of power grid network, we focus on four types of 4-node motifs, $M_1$, $M_2$, $M_3$ and $M_4$, in Figure 1.1 because of motifs $M_5$ or $M_6$ are not available in some of the power grid networks. The basic network structure information of six European power grid networks are presented in Table 2.1.
We measure system response to disruptive events using the degradation rates of motifs under attacks (i.e., removal of nodes in the network) using the parameters in the gamma degradation model in Section 2.3.1. We focus on the degree-centrality-based attacks in Sections 2.4.2 and 2.4.3 and consider other sequences of node removal (attacks) such as the betweenness-centrality-based and eigenvector-centrality-based attacks. For degree-centrality-based attacks, the larger the degree of a node (i.e., more neighbors a node has), the earlier the node is removed from the network.

Figure 2.2 illustrates the remaining (%) 4-node motifs ($M_1$, $M_2$, $M_3$, and $M_4$) of the six European power grids graphically under degree-centrality-based attacks. Note that the degradation rates of different 4-node motifs are different when the same fraction of nodes have been removed. For example, we find that the motif $M_3$ in Poland (black curve) degrades faster than other countries, however, the motif $M_4$ in Poland degrades slower than the other countries. It is clear that one may not conclude which power grid is more robust or fragile with the behavior of a single 4-node motif as a fraction of nodes have been removed.

2.4.2. Comparing Network Vulnerability

In this subsection, we apply the proposed gamma degradation model to fit the data presented in Table 2.1 and the estimates of the model parameters are presented in Table 2.2.
In order to assess the similarity of the two power grids in terms of robustness, we compute the $p$-value of the test for hypotheses in Equation (2.6) for each pair of power grids based on the likelihood ratio test. For comparative purposes, we present the $p$-values through the clustered heatmap in Figure 2.3 where the $p$-values are indicated by the heatmap color (yellow: high, dark blue: low). Based on the heatmap in Figure 2.3, we can observe, for example, in contrast to other power grids, the robustness of the Italy power grid is similar to that of the Germany power grid; moreover, France power grid confers similar robustness to Spain power grid. To evaluate the rankings of the six power grids in terms of robustness, we can obtain two possible robustness rankings based on the heatmap:

[Italy, Germany] > [Romania, Poland] > [France, Spain]

or

[France, Spain] > [Romania, Poland] > [Italy, Germany]
To evaluate which ranking is more probable, we consider two extensions of the proposed gamma degradation model. First, we calculate the average degradation rate for the $i$-th power grid as

$$
\bar{A}_i = \frac{\lambda_{i,1} \times \beta_i + \cdots + \lambda_{i,J} \times \beta_i}{J},
$$

where $\bar{A}_i$ is the average of the expected values of gamma random variables. The smaller the $\bar{A}_i$, the more robust the $i$-th network. Based on the values of $\bar{A}$ in Table 2.2, we can observe the average degradation rates of the motifs of Italy and Germany are much smaller than those of Romania, Poland, France and Spain, and the average of degradation rates of Romania and Poland are smaller than those of France and Spain. Second, we can compare the robustness between Spain and Italy based on assuming equal scale parameters for Italy and Spain (i.e., through combining the Italy and Spanish power grids) and then compare

Figure 2.3: Heatmap with pairwise $p$-value between six European power grids.
the shape parameters between Italy and Spain power grids (see Table 2.3). From Table 2.3, we observe that all of the shape parameters in the Spain power grid is larger than those in the Italy power grid. Hence, we conclude that the vulnerability ranking of these six power grids is

\[ \text{[Italy, Germany]} > \text{[Romania, Poland]} > \text{[France, Spain]} \].

<table>
<thead>
<tr>
<th>Country</th>
<th>( \lambda_1 )</th>
<th>( \lambda_2 )</th>
<th>( \lambda_3 )</th>
<th>( \lambda_4 )</th>
<th>( \beta )</th>
<th>( \hat{A} )</th>
</tr>
</thead>
<tbody>
<tr>
<td>France</td>
<td>4.055</td>
<td>3.399</td>
<td>5.295</td>
<td>2.576</td>
<td>0.060</td>
<td>0.230</td>
</tr>
<tr>
<td>Germany</td>
<td>3.082</td>
<td>2.445</td>
<td>2.383</td>
<td>2.161</td>
<td>0.069</td>
<td>0.174</td>
</tr>
<tr>
<td>Italy</td>
<td>2.368</td>
<td>2.270</td>
<td>2.437</td>
<td>3.080</td>
<td>0.063</td>
<td>0.159</td>
</tr>
<tr>
<td>Poland</td>
<td>1.917</td>
<td>1.633</td>
<td>2.245</td>
<td>0.721</td>
<td>0.125</td>
<td>0.203</td>
</tr>
<tr>
<td>Romania</td>
<td>1.627</td>
<td>1.477</td>
<td>0.967</td>
<td>1.033</td>
<td>0.162</td>
<td>0.207</td>
</tr>
<tr>
<td>Spain</td>
<td>4.544</td>
<td>3.390</td>
<td>4.483</td>
<td>3.252</td>
<td>0.072</td>
<td>0.282</td>
</tr>
</tbody>
</table>

Table 2.2: Estimates of the gamma degradation model parameters for six power grids dataset under degree-based attack.

<table>
<thead>
<tr>
<th>Country</th>
<th>( \lambda_1 )</th>
<th>( \lambda_2 )</th>
<th>( \lambda_3 )</th>
<th>( \lambda_4 )</th>
<th>( \beta )</th>
</tr>
</thead>
<tbody>
<tr>
<td>Italy</td>
<td>2.285</td>
<td>2.191</td>
<td>2.349</td>
<td>2.964</td>
<td>0.066</td>
</tr>
<tr>
<td>Spain</td>
<td>4.939</td>
<td>3.673</td>
<td>4.876</td>
<td>3.534</td>
<td>0.066</td>
</tr>
</tbody>
</table>

Table 2.3: Estimates of the gamma degradation model parameters for Italy and Spain power grids under degree-based attack with assuming \( \beta_{\text{Italy}} = \beta_{\text{Spain}} = \beta \).

2.4.3. Determine which Motifs Contribute to the Difference

In this subsection, we use the power grids of Germany and Spain to illustrate the partial-motifs tests proposed in Section 2.3.1.1. Based on the gamma degradation model and the likelihood ratio test, testing the hypotheses in Equation (2.6) for the power grids of Germany
and Spain, the $p$-value is 0.0074 and the null hypothesis $H_0 - \mathcal{R}(\text{Network}_1) = \mathcal{R}(\text{Network}_2)$, where $1 = \text{Germany}$ and $2 = \text{Spain}$, is rejected at 1% level of significance. Therefore, we conclude that the network robustness of the power grids of Germany and Spain are different with 1% level of significance.

After rejecting the null hypothesis that the two power grids are the same in terms of robustness, we would be interested in identify the similarity factor (motif/shape parameter) and difference factor (motif/shape parameter) and identify which motif decreases/increases the network robustness using the proposed partial-motifs test. For the partial-motif tests, we fix the null hypothesis and consider four different alternative hypotheses for the power grids of Germany and Spain:

[I] Test for the parameter of motif $M_1$ under $H_{1(1)}$: $H_0 : \beta_1 = \beta_2 = \beta, \lambda_{1,1} = \lambda_{2,1} = \lambda_1, \lambda_{1,2} = \lambda_{2,2} = \lambda_2, \lambda_{1,3} = \lambda_{2,3} = \lambda_3, \lambda_{1,4} = \lambda_{2,4} = \lambda_4$ versus $H_{1(1)} : \beta_i \neq \beta_j, \lambda_{1,1} = \lambda_{2,1} = \lambda_1, \lambda_{1,2} \neq \lambda_{2,2}, \lambda_{1,3} \neq \lambda_{2,3}, \lambda_{1,4} \neq \lambda_{2,4}$.

[II] Test for the parameter of motif $M_2$ under $H_{1(2)}$: $H_0 : \beta_1 = \beta_2 = \beta, \lambda_{1,1} = \lambda_{2,1} = \lambda_1, \lambda_{1,2} = \lambda_{2,2} = \lambda_2, \lambda_{1,3} = \lambda_{2,3} = \lambda_3, \lambda_{1,4} = \lambda_{2,4} = \lambda_4$ versus $H_{1(2)} : \beta_i \neq \beta_j, \lambda_{1,2} = \lambda_2, \lambda_{1,1} \neq \lambda_{2,1}, \lambda_{1,3} \neq \lambda_{2,3}, \lambda_{1,4} \neq \lambda_{2,4}$.

[III] Test for the parameter of motif $M_3$ under $H_{1(3)}$: $H_0 : \beta_1 = \beta_2 = \beta, \lambda_{1,1} = \lambda_{2,1} = \lambda_1, \lambda_{1,2} = \lambda_{2,2} = \lambda_2, \lambda_{1,3} = \lambda_{2,3} = \lambda_3, \lambda_{1,4} = \lambda_{2,4} = \lambda_4$ versus $H_{1(3)} : \beta_i \neq \beta_j, \lambda_{1,3} = \lambda_{2,3} = \lambda_3, \lambda_{1,1} \neq \lambda_{2,1}, \lambda_{1,2} \neq \lambda_{2,2}, \lambda_{1,4} \neq \lambda_{2,4}$.

[IV] Test for the parameter of motif $M_4$ under $H_{1(4)}$: $H_0 : \beta_1 = \beta_2 = \beta, \lambda_{1,1} = \lambda_{2,1} = \lambda_1, \lambda_{1,2} = \lambda_{2,2} = \lambda_2, \lambda_{1,3} = \lambda_{2,3} = \lambda_3, \lambda_{1,4} = \lambda_{2,4} = \lambda_4$ versus $H_{1(4)} : \beta_i \neq \beta_j, \lambda_{1,4} = \lambda_{2,4} = \lambda_4, \lambda_{1,1} \neq \lambda_{2,1}, \lambda_{1,2} \neq \lambda_{2,2}, \lambda_{1,3} \neq \lambda_{2,3}$.

In the above four hypotheses, we assume that $\lambda_{i,j}$ is equivalent to $\lambda_{i',j}$ in both the null and alternative hypothesis, $j = 1, 2, 3, 4$. The $p$-values obtained from the above four hypotheses are: $p$-value$_I = 0.0054$, $p$-value$_{II} = 0.0046$, $p$-value$_{III} = 0.0113$, and $p$-value$_{IV} = 0.0053$. Comparing these $p$-values, motif $M_3$ exhibits somewhat more obvious difference because
there is an increase of the absolute difference between \( p \)-values from the partial-motifs test in hypotheses [III] above and the overall test in Equation (2.6).

To verify the conclusion here, we perform an inverse-partial-motifs test for \( \lambda_1, \lambda_2, \lambda_3, \) and \( \lambda_4. \) We fix the alternative hypothesis as the overall test and consider different null hypotheses. The corresponding four different null hypotheses are:

[V] Test for the parameter of \( M_1 \) under \( H_{0(1)}: H_{0(1)} : \beta_1 \neq \beta_2, \lambda_{1,1} = \lambda_{2,1} = \lambda_1, \lambda_{1,2} \neq \lambda_{2,2}, \lambda_{1,3} = \lambda_{2,3}, \lambda_{1,4} \neq \lambda_{2,4} \) versus \( H_1 : \beta_i \neq \beta_{i'}, \lambda_{1,1} \neq \lambda_{2,1}, \lambda_{1,2} \neq \lambda_{2,2}, \lambda_{1,3} \neq \lambda_{2,3}, \lambda_{1,4} \neq \lambda_{2,4}. \)

[VI] Test for the parameter of \( M_2 \) under \( H_{0(2)}: H_{0(2)} : \beta_1 \neq \beta_2, \lambda_{1,2} = \lambda_{2,2} = \lambda_2, \lambda_{1,1} \neq \lambda_{2,1}, \lambda_{1,3} \neq \lambda_{2,3}, \lambda_{1,4} \neq \lambda_{2,4} \) versus \( H_1 : \beta_i \neq \beta_{i'}, \lambda_{1,1} \neq \lambda_{2,1}, \lambda_{1,2} \neq \lambda_{2,2}, \lambda_{1,3} \neq \lambda_{2,3}, \lambda_{1,4} \neq \lambda_{2,4}. \)

[VII] Test for the parameter of \( M_3 \) under \( H_{0(3)}: H_{0(3)} : \beta_1 \neq \beta_2, \lambda_{1,3} = \lambda_{2,3} = \lambda_3, \lambda_{1,1} \neq \lambda_{2,1}, \lambda_{1,2} \neq \lambda_{2,2}, \lambda_{1,4} \neq \lambda_{2,4} \) versus \( H_1 : \beta_i \neq \beta_{i'}, \lambda_{1,1} \neq \lambda_{2,1}, \lambda_{1,2} \neq \lambda_{2,2}, \lambda_{1,3} \neq \lambda_{2,3}, \lambda_{1,4} \neq \lambda_{2,4}. \)

[VIII] Test for the parameter of \( M_4 \) under \( H_{0(4)}: H_{0(4)} : \beta_1 \neq \beta_2, \lambda_{1,4} = \lambda_{2,4} = \lambda_4, \lambda_{1,1} \neq \lambda_{2,1}, \lambda_{1,2} \neq \lambda_{2,2}, \lambda_{1,3} \neq \lambda_{2,3}, \lambda_{1,4} \neq \lambda_{2,4} \) versus \( H_1 : \beta_i \neq \beta_{i'}, \lambda_{1,1} \neq \lambda_{2,1}, \lambda_{1,2} \neq \lambda_{2,2}, \lambda_{1,3} \neq \lambda_{2,3}, \lambda_{1,4} \neq \lambda_{2,4}. \)

The \( p \)-values obtained from hypotheses [V]–[VIII] are: \( p\)-value\(_V\) = 0.2906, \( p\)-value\(_VI\) = 0.3814, \( p\)-value\(_VII\) = 0.0938, and \( p\)-value\(_VIII\) = 0.2913. We can observe that the \( p \)-values corresponding to motif \( M_3 \) is smaller than the others and the results achieve consistently performance compared with the findings from the partial-motifs test. The partial-motifs tests identify the 4-node motif \( M_3 \) as the most informative measure for identifying the difference between two power networks. This finding agrees with the results discussed in [97] in which the motif \( M_3 \) (i.e., detour motif) has drastically impact on the power grid stability.
2.4.4. Comparison of Network Vulnerability under Different Attacks

As mentioned in Section 2.4.1, the nodes of a graph can be removed in different order based on different types of attacks. Instead of comparing the robustness of two power grid networks, the proposed model and testing procedure can be applied to compare the robustness of a power grid network under different target attacks. In this subsection, we consider the comparisons of degree-centrality-based attacks, betweenness-centrality-based attacks, and eigenvector-centrality-based attacks (i.e., the nodes are selected in the decreasing order of their degree, betweenness, and eigenvector centrality).

Figure 2.4 shows the degradation of 4-node motifs under the betweenness-centrality-based attacks, i.e., the nodes in the network are removed sequentially from the highest to the lowest betweenness centrality scores. We find that the motif degradation curves of the power grid are substantially different from the corresponding curves under the degree-centrality-based attacks (see Figure 2.2). The parameter estimates of the gamma degradation model and the average degradation rates of the six European power grids based on betweenness-centrality-based attacks are presented in Table 2.4. Based on the average of degradation rates, $\bar{A}$, in Table 2.4, we obtain the ranking of the six European power grids in terms of robustness as

$$[\text{Italy, Germany}] > [\text{Romania, France}] > [\text{Spain, Poland}].$$

In contrast to the degree-centrality-based attacks, when the betweenness-centrality-based attacks is considered, the most robust and the most fragile power grids are Germany and Spain, respectively.

For eigenvector-centrality-based attacks, Figure 2.5 shows the motif degradation curves of each power grid based on sequentially removing nodes following eigenvector centrality scores. The degradation rates based on eigenvector-centrality-based attacks are noticeably slower than the corresponding remaining motif change under degree-centrality-based and
betweenness-centrality-based attacks. The parameter estimates of gamma degradation model and the average degradation rates of the six European power grids based on eigenvector-centrality-based attacks are presented in Table 2.5. Under eigenvector-centrality-based attacks, the most robust power grid is still Germany, however, the most fragile power grid is Poland. The implication of these results is that, under different attack strategies, the robustness of network can be different.
Betweenness-based attacks

<table>
<thead>
<tr>
<th></th>
<th>$\lambda_1$</th>
<th>$\lambda_2$</th>
<th>$\lambda_3$</th>
<th>$\lambda_4$</th>
<th>$\beta$</th>
<th>$\bar{A}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>France</td>
<td>3.429</td>
<td>2.971</td>
<td>3.445</td>
<td>2.186</td>
<td>0.054</td>
<td>0.163</td>
</tr>
<tr>
<td>Germany</td>
<td>0.931</td>
<td>0.897</td>
<td>0.510</td>
<td>0.621</td>
<td>0.092</td>
<td>0.068</td>
</tr>
<tr>
<td>Italy</td>
<td>2.921</td>
<td>2.771</td>
<td>2.367</td>
<td>3.323</td>
<td>0.034</td>
<td>0.098</td>
</tr>
<tr>
<td>Poland</td>
<td>1.697</td>
<td>1.444</td>
<td>2.315</td>
<td>0.678</td>
<td>0.121</td>
<td>0.186</td>
</tr>
<tr>
<td>Romania</td>
<td>1.091</td>
<td>1.317</td>
<td>0.098</td>
<td>1.169</td>
<td>0.137</td>
<td>0.126</td>
</tr>
<tr>
<td>Spain</td>
<td>2.878</td>
<td>2.793</td>
<td>2.563</td>
<td>2.953</td>
<td>0.071</td>
<td>0.199</td>
</tr>
</tbody>
</table>

Table 2.4: Parameter estimates of the gamma degradation model for the six power grids under betweenness-based attacks.

Figure 2.5: Degradation of motifs of six power grids under eigenvector-based attacks.
Table 2.5: Parameter estimates of the gamma degradation model for the six power grids under eigenvector-based attacks.

<table>
<thead>
<tr>
<th>Country</th>
<th>$\lambda_1$</th>
<th>$\lambda_2$</th>
<th>$\lambda_3$</th>
<th>$\lambda_4$</th>
<th>$\beta$</th>
<th>$\bar{A}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>France</td>
<td>1.001</td>
<td>0.961</td>
<td>0.841</td>
<td>0.649</td>
<td>0.096</td>
<td>0.083</td>
</tr>
<tr>
<td>Germany</td>
<td>0.649</td>
<td>0.614</td>
<td>0.478</td>
<td>0.401</td>
<td>0.055</td>
<td>0.029</td>
</tr>
<tr>
<td>Italy</td>
<td>0.919</td>
<td>0.898</td>
<td>0.783</td>
<td>0.713</td>
<td>0.058</td>
<td>0.048</td>
</tr>
<tr>
<td>Poland</td>
<td>0.402</td>
<td>0.453</td>
<td>0.209</td>
<td>0.486</td>
<td>0.222</td>
<td>0.086</td>
</tr>
<tr>
<td>Romania</td>
<td>1.067</td>
<td>0.907</td>
<td>0.238</td>
<td>0.557</td>
<td>0.081</td>
<td>0.056</td>
</tr>
<tr>
<td>Spain</td>
<td>0.460</td>
<td>0.543</td>
<td>0.413</td>
<td>0.490</td>
<td>0.127</td>
<td>0.061</td>
</tr>
</tbody>
</table>

Comparisons with more conventional global network-based vulnerability metrics are in Appendix A.2.1. We also compare the use of motifs with some state-of-the-art power flow reliability measures for network vulnerability based on synthetic ACTIVSg500 and ACTIVSg2000 power systems in Appendix A.2.2 (the data are publicly available from https://electricgrids.engr.tamu.edu/). We emphasize that quantification of system resilience based on optimal power flow information should be viewed as a valuable, complementary rather than competing direction, especially in view of the fact that such resilience measures based on power flow tend to be very-resource intensive and often limited by available data. In Appendix A.3, we further justify the use of network motifs in network reliability analysis by studying how network motifs affect the functionality of a power system under removal of nodes or edges using the IEEE 118-Bus system.

2.5. Monte Carlo Simulation Studies

In this section, we verify the usefulness and study the properties of the proposed gamma degradation model and hypothesis testing procedures using Monte Carlo simulation studies.
2.5.1. Based on a Parametric Statistical Model

To evaluate the performances of the proposed model and test procedures, a Monte Carlo simulation study with two networks (i.e., $I = 2$), four observed 4-node motifs (i.e., $J = 4$) and different numbers of observation points $K = \{10, 30\}$. We consider the gamma degradation model with original parameter vectors $\theta_1 = \{\lambda_{1,1}, \lambda_{1,2}, \lambda_{1,3}, \lambda_{1,4}, \beta_1\} = \{3.0, 2.0, 3.0, 2.0, 0.1\}$ and alternative parameter vectors $\theta_2 = \{a\lambda_{1,1}, a\lambda_{1,2}, a\lambda_{1,3}, a\lambda_{1,4}, \beta_1\} = \{3a, 2a, 3a, 2a, 0.1\}$, where $a = \{0.1, \ldots, 2.0\}$. The following steps are used to simulate the rejection rate of the proposed likelihood ratio test procedure in Section 2.3.1.1:

Step 1: Generate $y_{i,j,k}$ based on the gamma distribution with shape $\lambda = \lambda_{i,j} = a\lambda_{i,j}$, and scale $\beta = \beta_i$, $i = 1, 2$, $j = 1, 2, 3, 4$, $k = 1, 2, \ldots, K$.

Step 2: Set the each motif’s degradation at time $t_1$ equals to 100%, (i.e., $x_{i,j,1} = 1$). Compute $x_{i,j,k+1} = x_{i,j,k}/\exp(y_{i,j,k})$, $i = 1, 2$, $j = 1, 2, 3, 4$, $k = 1, 2, \ldots, K$.

Step 3: Perform the likelihood ratio test presented in Section 2.3.1 based on the simulated data and obtain the $p$-value.

Step 4: Repeat Step 1 to Step 3 $N$ times. The simulated rejection rate is $\# \{p$-value $< 0.05\}/N$.

The simulated rejection rates based on $N = 10,000$ simulations are presented in Figure 2.6 and Table 2.6. We find that the simulated rejection rates increase when $a$ increases from 1.0 to 2.0 and when $a$ decreases from 1.0 to 0.1. Under the null hypothesis (i.e., $a = 1.0$), the simulated rejection rates are higher than the nominal level 0.05, especially when $K = 10$. However, when the number of observation points increases from $K = 10$ to 30, the simulated rejection rate gets closer to 0.05.

To validate the appropriateness of using the proposed gamma process model for the remaining motifs data, we simulate 1,000 remaining motifs curves based on the fitted gamma process models with the parameters in Tables 2.2, 2.4 and 2.5, along with the observed
Figure 2.6: Simulated rejection rates for $K = 10$(red) and 30(blue) with $a = \{0.1, \cdots, 2.0\}$.

remaining motifs curves. Plots of the simulated (blue) and observed (orange) remaining motifs curves are presented in Figures 2.7, 2.8, 2.9. As Figures 2.7, 2.8, 2.9 demonstrate, the observed remaining motifs curves for motifs $M_1,M_2,M_3,M_4$ of the six power grids fall within those simulated motifs curves, based on the proposed gamma process model (except the curve for motif $M_3$ of Poland power grid), which indicates that the proposed model provides reasonable fits of the data. Note that some of the simulated motifs curves do not contain the observed motif curve (e.g., motif $M_4$ in Poland and Romania). This phenomenon can be explained by the lower orders of these power grid networks (i.e, both Poland and Romania have lowest numbers of nodes) and, as a result, lower representation of motif $M_4$ in these networks.
Table 2.6: Simulated rejection rate for different values of $a = \{0.1, \cdots, 2.0\}$ with $K = \{10, 30\}$.

<table>
<thead>
<tr>
<th>$a$</th>
<th>$K = 10$</th>
<th>$K = 30$</th>
<th>$a$</th>
<th>$K = 10$</th>
<th>$K = 30$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>1.000</td>
<td>1.000</td>
<td>1.1</td>
<td>0.111</td>
<td>0.114</td>
</tr>
<tr>
<td>0.2</td>
<td>1.000</td>
<td>1.000</td>
<td>1.2</td>
<td>0.212</td>
<td>0.337</td>
</tr>
<tr>
<td>0.3</td>
<td>1.000</td>
<td>1.000</td>
<td>1.3</td>
<td>0.380</td>
<td>0.648</td>
</tr>
<tr>
<td>0.4</td>
<td>0.998</td>
<td>1.000</td>
<td>1.4</td>
<td>0.589</td>
<td>0.890</td>
</tr>
<tr>
<td>0.5</td>
<td>0.973</td>
<td>1.000</td>
<td>1.5</td>
<td>0.781</td>
<td>0.982</td>
</tr>
<tr>
<td>0.6</td>
<td>0.822</td>
<td>0.988</td>
<td>1.6</td>
<td>0.908</td>
<td>0.998</td>
</tr>
<tr>
<td>0.7</td>
<td>0.521</td>
<td>0.831</td>
<td>1.7</td>
<td>0.965</td>
<td>1.000</td>
</tr>
<tr>
<td>0.8</td>
<td>0.250</td>
<td>0.421</td>
<td>1.8</td>
<td>0.991</td>
<td>1.000</td>
</tr>
<tr>
<td>0.9</td>
<td>0.113</td>
<td>0.132</td>
<td>1.9</td>
<td>0.999</td>
<td>1.000</td>
</tr>
<tr>
<td>1.0</td>
<td>0.076</td>
<td>0.058</td>
<td>2.0</td>
<td>1.000</td>
<td>1.000</td>
</tr>
</tbody>
</table>

Figure 2.7: Simulated and observed motifs curves of the six power grids under degree-based attacks.
Figure 2.8: Simulated and observed motifs curves of the six power grids under betweenness-based attacks.

Figure 2.9: Simulated and observed motifs curves of the six power grids under eigenvector-based attacks.
2.5.2. Nonparametric Resampling of a Network

In order to evaluate the performance of the proposed model and test procedures when the data are not generated from a parametric model, we conducted a simulation study based on resampling of a power grid network. Specifically, we sample two sub-networks (sub-graphs) from a power grid network in the UCTE power grid network data in Section 2.4 and apply the proposed model and testing procedure for data analysis.

Here, we use the network sampling method called breadth-first sampling (BFS). Breadth-first search is a classic graph traversal algorithm that starts from the chosen-seed and progressively explores all neighbors. Consequently, BFS obtains first the nodes closest to the seed. Compared with random walk (RW), graph traversals (e.g., breadth-first search and depth-first search) never revisits the same node. At the end of the process, if the graph is connected, then all nodes will be visited. However, when using graph traversals for sampling, we terminate after having collected a fraction $\delta < 1$ of graph nodes.

In this simulation study, we consider the power grid networks of Germany, France and Spain for the resampling process. We set the fraction of sample graph nodes $\delta$ from 70.0% to 90.0%. The following steps are used to simulate the rejection rate of the proposed test procedure based on network resampling:

Step 1: The 1st sample sub-network, denoted as $G'_1$ is obtained from network $G_1$ by BFS with fraction 100$\delta$%.

Step 2: The 2nd sample sub-network $G''_2$ is obtained from $G_2$ by BFS with fraction 100$\delta$%.

Step 3: Perform the likelihood ratio test presented in Section 2.3.1 based on the simulated data and obtain the $p$-value.

Step 4: Repeat Step 1 to Step 3 $N$ times. The simulated rejection rate is $\# \{p$-value $< 0.05\}/N$. 
The simulation rejection rates between two sub-graphs under BFS sampling with different fractions $\delta$ for testing the hypotheses is $H_0 : \mathcal{R}(G_i') = \mathcal{R}(G_i'')$ versus $H_1 : \mathcal{R}(G_i') \neq \mathcal{R}(G_i'')$, where sub-graphs $G_i'$ and $G_i''$ sampled from the graph ($G_G$: Germany; $G_F$: France; $G_S$: Spain) based on 10000 simulations are presented in Table 2.7. In Table 2.7, the upper part of table shows the simulated rejection rates between two sub-graphs resampled from the same power grid with different fractions. We find that the corresponding rejection rates in the three scenarios (i.e., $G_G'$ versus $G_G''$, $G_F'$ versus $G_F''$, and $G_S'$ versus $G_S''$) become closer to 0.05 as the fraction $\delta$ increases. Most of these rejection rates are below the nominal level 0.05, which indicate that the proposed model and testing procedure work as expected. The lower part of Table 2.7 presents the simulated rejection rates between two sub-graphs resampled from two different power grid networks which are difference in terms of robustness based on the results in Section 2.4. In contrast, the lower part of table has substantially higher rejection rates compared to the upper part of Table 2.7. The results from these analyses demonstrate that the proposed model and testing procedures provide reasonable power in detecting the difference between two networks in terms of robustness.

To detect the sensitive of the proposed gamma degradation model, we use the simulated datasets generated from Wiener process model (please see Appendix A.4 for details).
CHAPTER 3
Statistical Models and Algorithms for Assessing Robustness and Reliability of Networks with Applications in Cybersecurity Insurance

Modern cyber systems and computer infrastructure for commerce and communications such as cyberspace, the Internet, electronic payment systems, and file-sharing systems can be represented as complex networks. Cybersecurity insurance is one of the possible ways to manage risk exposure for these complex cyber networks. For the pricing of cybersecurity insurance, comprehending the loss of availability of a cyber or physical network subject to attacks or failures and assessing the risks of a complex network is of great interest. To understand the risk of complex networks, we propose a modified Wiener process model for the degeneration of the network functionality upon the removal of nodes due to attacks or malfunctions. We also propose three statistical testing procedures based on the Wiener process model to compare the risk and resilience of two different networks, which can be used to comparing risks in the cybersecurity insurance domain. The proposed methodologies can be applied to any topological measures of network robustness or risk. Practical data analysis for the peer-to-peer file-sharing networks is presented to illustrate the proposed model and methods. Monte Carlo simulations are used to evaluate the performance of the proposed methodologies and practical recommendations are provided.

3.1. Introduction

Many complex networks, such as cyberspace, the Internet, power grids, are critical infrastructures for commerce and communications that require extremely high reliability and
safety standard. Significant attacks or failures on those complex networks could cause serious damage to society. Insurance is one of the possible ways to manage risk exposure for these complex networks. For example, cybersecurity insurance is designed to mitigate losses from a variety of cyber incidents, including data breaches, business interruption, and network damage [29]. In 2013, the Group of Twenty (G-20) urged to treat cyber-attacks as a threat to the global economy [3]. For the data and statistics from government, industry, and information technology related to the current state of cybersecurity threats in the United States and internationally, one can refer to [104]. Recently, Böhme et al. [15] provided a general framework for actuaries to think about cyber risk and the approaches to cyber risk analysis. In this chapter, “cyberspace” refers to the interactive domain composed of all digital networks used to store, modify, and communicate information, and the term “cyber risk” refers to a multitude of different sources of risk affecting the information and technology assets of a company [12]. Since the internet is one of the most complex systems humanity has ever devised, cyber risk management becomes a prominent issue for society, especially for insurance companies [132]. However, research on cyber risk, especially on evaluation and comparison of the risks in the insurance domain, is fairly limited. In addition, pricing for cybersecurity insurance is a challenging problem since cybersecurity insurance has no standard scoring systems or actuarial tables for rate making [122]. Moreover, there is a lack of open-source data for organizations’ internal networks for security breaches and losses due to the disinclination of organizations to disclose details of security breaches. As Böhme et al. [15] pointed out, understanding cyber risk is a hard problem, therefore, comprehending how vulnerable is a cyber or physical network to attacks or failures and assessing the risks of a complex network is of great interest. There is an urgent need to develop advanced methodologies that can systematically assess the risk, robustness, reliability, or loss of availability of a network and comparing the risk and robustness of different networks.

Cyber risk is a fundamental measurement providing a quantitative measure of the security level, the capability of capturing attacks, and the lost of availability that results in loss of integrity and availability [12, 15]. To evaluate the loss of availability of cyber networks,
various heuristic methods were proposed to measure the resilience of cyber networks under malicious cyber attacks [5, 45]. However, those heuristic methods are often designed for a specific cyber network, which limited their applicability to diverse areas [55]. In general, metric-based approaches use specific measures of individual properties of cyber system components to access resilience. For example, when evaluating the resilience of a computer system, Ganin et al. [38] considered the percentage of computers that are functioning and the ratio of a system’s actual flow to its maximum capacity for measuring resilience. This metric-based approach may not be appropriate for systems that the connections between the nodes (computers) have an important effect on the resilience of the system. Therefore, some high-order structures and topological measures of a network should be considered.

In managing cyber risk in the insurance domain, different tools and methods have been proposed for evaluating the network robustness in the past decades, however, algorithms/techniques based on statistical models and stochastic processes have not been broadly developed. In this chapter, we aim to develop dependable and flexible statistical models and hypothesis testing procedures to assess the risk and robustness of a complex network which can provide useful information for cyber insurance providers. Specifically, we propose a modified Wiener process model with several statistical hypothesis testing procedures for this purpose. The Wiener process model is one of the widely used stochastic models for non-monotonic degradation processes which can provide a good description of the system’s behavior in the cascading failure process [20, 32, 66]. Compared with observing dynamics of the topological measures under attacks, the proposed modified Wiener process model can model the evolution of the degradation data in each network topological measure and also provide great flexibility in degradation modeling, e.g., non-linear degradation mechanisms. The proposed methodologies will expand the actuarial knowledge on the evaluation and comparison of risks for different physical and/or cyber networks and cybersecurity insurance pricing models.
3.2. Graph Representation of Cyber Network

Inherently, a cyber network, such as the P2P cyber network, can be viewed as a graph structure consisting of nodes and edges. For example, in a P2P cyber network, the hosts are considered as nodes in a graph, and the host’s neighbor set is described by the set of edges in a graph. A graph structure can be represented as $\mathcal{G} = \{V, E, W\}$, where $V$ is a node set with cardinality (the number of elements in a set) $|V|$ of $N$, $E \subseteq V \times V$ is an edge set, and $W$ is the adjacency matrix of $\mathcal{G}$, which is an $N \times N$ nonnegative symmetric matrix with entries $\{\omega_{ij}\}_{1 \leq i,j \leq N}$, i.e., $\omega_{ij} \neq 0$ for any $e_{ij} \in E$ and $\omega_{ij} = 0$, otherwise. In the study of cyber network, we consider unweighted and undirected graph, i.e., $\omega_{ij} = 1$ and $e_{ij} = e_{ji} \in E$, for all $1 \leq i, j \leq N$. Hence, we suppress the notation of the adjacency matrix in the graph representation and represent the graph as $\mathcal{G} = \{V, E\}$.

To evaluate the robustness/loss of availability of a network, the decrease of network performance due to a selected removal of nodes or edges is considered. For example, in cyberspace, computers and hand-held devices are connected to servers over active Internet signals or local area network (LAN) lines. In this case, those computers, hand-held devices, and servers are the nodes and the LAN lines and Internet signals are edges of the network graph of interest. The failure of a server or broken LAN lines (due to physical or cyber attacks, or human errors) will reduce the functionality of the cyber network.

High-order structures are often called the building blocks of network [68]. Compared with global network topology (e.g., graph diameter and average path length) [23, 26, 84], through studying the high-order structures, we can capture more local information of network structure. For instance, feedforward loops have proven fundamental to understanding the mechanism of transcriptional regulation networks [99]. Here, the robustness of a cyber network can be defined as the ability of a network to maintain its functionality/connectivity when it is subject to failure or attack. There is a variety of graph measures that provide robustness measures on a network [77]. For example, vertex connectivity is defined as the
minimum number of vertices that need to be removed to disconnect the graph and the average cluster coefficient that represents the probability that neighbors of a node are also connected [48, 117]. Another commonly used robustness measure is the network motifs introduced by Milo et al. [75] in conjunction with the assessment of the stability of biological networks and later have been studied in a variety of contexts [6]. Network motifs are subgraphs (smaller patterns) that the numbers of appearances are statistically significantly greater than a predefined threshold in a randomized network. A motif here is broadly defined as a recurrent multi-node subgraph pattern. Formally, a motif is an induced subgraph of $G$.

Figure 3.1 shows all possible 4-size motifs in undirected graph. Recently, Dey et al. [30] focused on incorporating network motifs to evaluate and estimate the power system reliability with the help of statistical models.

To obtain the exact motif counts of different motif types in a specific $k$-size motif in a network, the RANDESU motif finder algorithm can be used [47]. For large network ($> 10,000$ edges), algorithms to approximate the exact motif counts can be used [15, 54], which introduces another layer of randomness in the data whereas suitable statistical models and techniques are required. To assess the robustness of a complex network like the cyber network, we focus on remaining motif distributions under various attacks like the physical or cyber-attack and cascading failure of attacks.
In this chapter, we assume that either the exact or approximate measures of network robustness can be obtained and focus on the development of novel statistical algorithms to assess the robustness and the risk, as well as to compare the risks of different networks. Although the methods described here focus on network motifs, the proposed methodologies can be applied to any topological measures of network robustness/risk such as the Wasserstein distance and the weighted-pairwise distance. The process of reducing the functionality of the physical or cyber networks under removal of nodes and/or edges can be viewed as a degradation process [20] and hence, novel statistical models and algorithms for degradation data analysis can be applied to evaluate and compare the risks of different complex networks.

In this section, we investigate how local topological features (e.g., local network structures) evolve under the removal of nodes and/or edges. Our main postulate here is that a complex system can be considered more resilient if it tends to preserve its original properties longer under the removal of nodes and/or edges, and our primary focus is to quantify the risks of different networks through statistical modeling and analyses of the geometric properties of different network systems. A stochastic model, the Wiener process model, along with several statistical hypothesis testing procedures to compare the risks of different networks are developed. The mathematical notation and the Wiener process model are introduced in Section 3.3.1 and three statistical hypothesis testing procedures are proposed in Section 3.3.2.

3.3.1. Wiener process model

Suppose that there are $I$ networks and $J$ different topological features (e.g., network motifs, Wasserstein distance, and weighted-pairwise distance, etc.) are used to measure the risks of those $I$ networks, these topological features are observed at different time points $t_k$, $k = 0, 1, \ldots, K$, where $K+1$ is the total number of observation points. The observation point
can be considered as a specific fraction of random/selective nodes (e.g., nodes with the highest degrees or nodes with the largest betweenness) being removed from the network. We denote the observed value of the \( j \)-th topological feature for network \( i \) at the \( k \)-th time point as \( y_{i,j,k} \). For example, consider the 4-node motif \( M_1 \) in Figure 3.1 as the \( j \)-th topological feature, then \( y_{i,j,0} \) is the number of the 4-node motif \( M_1 \) in network \( i \) when all the nodes and edges in the network are fully functioning (i.e., at time \( t_0 \)), \( y_{i,j,1} \) is the number of the 4-node motif \( M_1 \) in network \( i \) when 10% of the nodes and edges in the network are removed (say, at time \( t_1 \)), \( y_{i,j,2} \) is the number of the 4-node motif \( M_1 \) in network \( i \) when 20% of the nodes and edges in the network are removed (say, at time \( t_2 \)), and so on.

Since the dynamics of the local topological measures upon removal of the nodes/edges may not necessarily be a monotonic deterioration process and due to the stochastic nature of this process, we thus propose using the Wiener process model to characterize the degradation paths of those topological measures of a complex network. We consider modeling the degeneration process of the functionality of the \( i \)-th network based on the \( j \)-th topological measure by using a Wiener process with drift parameter \( \mu_{i,j}^* \) and diffusion coefficient \( \sigma_{i,j}^* \).

Specifically, we consider \( D_{i,j}(t_k) = 1 - y_{i,j,k}/y_{i,j,0} \) as a stochastic process \( \{D_{i,j}(t_k), t_k \geq 0\} \), which is characterized by the following properties:

(i) \( D_{i,j}(t_0) = 1 - y_{i,j,0}/y_{i,j,0} = 0; \)

(ii) \( \{D_{i,j}(t_k), t_k \geq 0\} \) has stable independent increments, i.e., the increments \( x_{i,j,k} \) defined by \( \{D_{i,j}(t_k) - D_{i,j}(t_{k-1})\}, k = 1, 2, \ldots, K \) are independent;

(iii) the increments \( x_{i,j,k} \) follows a normal distribution \( \mathcal{N} (\mu_{i,j}^*, \sigma_{i,j}^2) \).

Since different topological measures may share similar characteristics, therefore, we modify the Wiener process model by introducing a correlation structure among the \( J \) topological measures. Based on the modified Wiener process model, in our study, we define a \( J \)-dimensional vector of random variables \( \mathbf{x}_{i,k} = (x_{i,1,k}, x_{i,2,k}, \ldots, x_{i,J,k})' \in \mathbb{R}^J \), where \( x_{i,j,k} = (y_{i,j,k} - y_{i,j,k+1})/y_{i,j,0}, i = 1, 2, \ldots, I; j = 1, 2, \ldots, J; k = 0, 1, 2, \ldots, K \), and assume that the
degradation process follows a Wiener process with drift $\mu_i$ and variance-covariance $\Sigma_i$. In other words, the $J$-dimensional vector of random variables $x_{i,k} = (x_{i,1,k}, x_{i,2,k}, \ldots, x_{i,J,k})' \in \mathbb{R}^J$ follows a $J$-dimensional multivariate normal distribution denoted as

$$\mathcal{M}_W : x_{i,k} \sim \mathcal{N}_J(\mu_i \Delta t_i, \Sigma_i \Delta t_i),$$  \hspace{1cm} (3.1)

where $\Delta t_i$ represents the difference between two time points, $\mu_i = (\mu_{i1}, \ldots, \mu_{iJ})' \in \mathbb{R}^J$ represents the slope of the linear drift and $\Sigma_i$ represents an $J \times J$ symmetric variance-covariance matrix

$$\Sigma_i = \begin{pmatrix}
\sigma_{i,11} & \sigma_{i,12} & \cdots & \sigma_{i,1J} \\
\sigma_{i,21} & \sigma_{i,22} & \cdots & \sigma_{i,2J} \\
\vdots & \vdots & \ddots & \vdots \\
\sigma_{i,J1} & \sigma_{i,J2} & \cdots & \sigma_{i,JJ}
\end{pmatrix},$$  \hspace{1cm} (3.2)

which is also known as the diffusion coefficient. It is worth to mention that, in our study, we assume the attack sequence taken at successive equally spaced points in time, i.e., $\Delta t_i = t_i - t_{i-1} = \Delta t$; without loss of generality, we can consider $x_{i,k} \sim \mathcal{N}_J(\mu_i, \Sigma_i)$. The joint probability density function of the random vector $x_{i,k}$ is

$$f(x_{i,k}; \mu_i, \Sigma_i) = \frac{1}{(2\pi)^{J/2}|\Sigma_i|^{1/2}} \exp \left\{ -\frac{1}{2} (x_{i,k} - \mu_i)' \Sigma_i^{-1} (x_{i,k} - \mu_i) \right\},$$  \hspace{1cm} (3.3)

for $x_{i,k} \in \mathbb{R}^J$. Under this setting, the log-likelihood function can be expressed

$$\ln L(\theta|x_i) = \sum_{i=1}^{I} \ln L_i(\theta_i|x_i),$$  \hspace{1cm} (3.4)

where $x = (x_1, \ldots, x_I)$, $\theta = (\theta_1, \ldots, \theta_I)$,

$$\ln L(\theta_i|x_i) = \sum_{k=1}^{J} \left[ -\frac{J}{2} \ln (2\pi) - \frac{1}{2} \ln (|\Sigma_i|) - \frac{1}{2} (x_{i,k} - \mu_i)' \Sigma_i^{-1} (x_{i,k} - \mu_i) \right],$$  \hspace{1cm} (3.5)
and $\theta_i = \{ (\mu_i, \Sigma_i) | \mu_i \in \mathbb{R}^J, \Sigma_i \text{ is an } J \times J \text{ positive-semidefinite matrix} \}$ is the parameter vector for the $i$-th network. The maximum likelihood estimates (MLEs) of the model parameters can be obtained by maximizing $\ln L(\theta_i|x_i)$ in Equation (3.5) with respect to $\mu_i$ and $\Sigma_i$. Iterative numerical algorithms for solving a non-linear system of equations with constraints, such as the limited-memory Broyden-Fletcher-Goldfarb-Shanno algorithm for box constraints (L-BFGS-B algorithm), can be utilized here to obtain the MLEs.

### 3.3.2. Similarity tests for two complex networks

In this subsection, we consider three different statistical procedures for testing the similarity of two complex networks (say, Network 1 and Network 2) in terms of their resilience/risk level based on the $J$ topological measures. We are interested in testing the hypotheses

$$H_0 : \text{Network 1 and Network 2 have the same resilience/risk level}$$

against $H_1 : \text{Network 1 and Network 2 do not have the same resilience/risk level}$ \hspace{0.5cm} (3.6)

#### 3.3.2.1. A test procedure based on resampling

The first proposed testing procedure is based on the Euclidean distance of degradation curves with resampling approach. Based on the observed degradation measurements $\vec{x}_1 = \{ x_{1,1}, x_{1,2}, \cdots, x_{1,K} \}$ and $\vec{x}_2 = \{ x_{2,1}, x_{2,2}, \cdots, x_{2,K} \}$ from Network 1 and Network 2, respectively, the algorithm to compute the $p$-value for testing the hypotheses in Equation (3.6) is described here. We name this procedure as Procedure A.

**Step A1:** Compute the Euclidean distance between $\vec{x}_1 = \{ x_{1,1}, x_{1,2}, \cdots, x_{1,K} \}$ and $\vec{x}_2 = \{ x_{2,1}, x_{2,2}, \cdots, x_{2,K} \}$ for the two networks:

$$d_{\text{obs}} = d_{\text{obs}}(\vec{x}_1, \vec{x}_2) = \left[ \sum_{k=1}^{K} \sum_{j=1}^{J} (x_{1,k} - x_{2,k})^2 \right]^{1/2}.$$
Step A2: Combine the two sets of observed degradation measurements and denote the combined data set as \( \mathbf{x}_C = (\mathbf{x}_1, \mathbf{x}_2) \). Based on the Wiener process model in Equation (3.1) obtain the MLE of \( \theta = (\mathbf{\mu}, \Sigma) \) by maximizing the log-likelihood function \( \ln L(\theta, \mathbf{x}_C) \) in Equation (3.5) with respect to \( \theta \). The MLE of \( \theta \) based on the combined data set under \( H_0 \) in Equation (3.6) is denoted by \( \hat{\theta}_C = (\hat{\mathbf{\mu}}_C, \hat{\Sigma}_C) \).

Step A3: Generate \( x_{1,k}^{(1)} \) and \( x_{2,k}^{(1)} \) from a \( J \)-dimensional multivariate normal distribution \( \mathcal{N}_J(\hat{\mathbf{\mu}}_C, \hat{\Sigma}_C) \), for \( k = 1, 2, \ldots, K \), to obtain the bootstrap samples \( \mathbf{x}_1^{(1)} = \{x_{1,1}^{(1)}, x_{1,2}^{(1)}, \ldots, x_{1,K}^{(1)}\} \) and \( \mathbf{x}_2^{(1)} = \{x_{2,1}^{(1)}, x_{2,2}^{(1)}, \ldots, x_{2,K}^{(1)}\} \), respectively.

Step A4: Compute the Euclidean distance between the two bootstrap samples \( \mathbf{x}_1^{(1)} \) and \( \mathbf{x}_2^{(1)} \) as
\[
d^{(1)} = d^{(1)}(\mathbf{x}_1^{(1)}, \mathbf{x}_2^{(1)}) = \left[ \sum_{k=1}^{K} \sum_{j=1}^{J} (x_{1,k}^{(1)} - x_{2,k}^{(1)})^2 \right]^{1/2}.
\]

Step A5: Repeat Steps A3–A4 \( B \) times to obtain a sequence of bootstrap Euclidean distances, \( d^{(b)} = d^{(b)}(\mathbf{x}_1^{(b)}, \mathbf{x}_2^{(b)}) \), for \( b = 1, 2, \ldots, B \).

Step A6: The \( p \)-value of the test is computed as
\[
p_A = \frac{1}{B} \sum_{b=1}^{B} 1\{d_{\text{obs}} > d^{(b)}\},
\]
where \( 1\{A\} \) is an indicator function defined as \( 1\{A\} = 1 \) if event \( A \) is true and \( 1\{A\} = 0 \) otherwise.

The null hypothesis in Equation (3.6) is rejected if \( p_A < \alpha \), where \( \alpha \) is a prefixed significant level. Note that Procedure A only uses the Wiener process model in the resampling process in Steps A3 and A4. In this procedure, we use the Euclidean distance as a measure of the distance between two vectors, however, other types of distance metrics such as the Manhattan distance can be used in place of the Euclidean distance.
3.3.2.2. Test procedures based on likelihood ratio test statistic

Under the Wiener process model described in Section 3.3.1, the hypotheses in Equation (3.6) can be expressed as

\[ H_0 : \mu_1 = \mu_2 = \mu \text{ and } \Sigma_1 = \Sigma_2 = \Sigma \]

against \( H_1 : \mu_1 \neq \mu_2 \text{ or } \Sigma_1 \neq \Sigma_2 \). \hspace{1cm} (3.7)

Let \( \hat{\theta}_i = (\hat{\mu}_i, \hat{\Sigma}_i) \) be the MLE of the \( \theta_i \) that maximizes the log-likelihood function \( \ln L(\theta_i, \bar{x}_i) \) in Equation (3.5) with respect to \( \theta_i \) based on the data \( \bar{x}_i \), i.e.,

\[ \hat{\theta}_i = \arg \max_{\theta_i} \ln L(\theta_i, \bar{x}_i), \hspace{1cm} (3.8) \]

for \( i = 1, 2 \). Similarly, based on the combined data set \( \bar{x}_C = (\bar{x}_1, \bar{x}_2) \), the MLE of \( \theta_C = (\mu_C, \Sigma_C) \) that maximizes the log-likelihood function \( \ln L(\theta_C, \bar{x}_C) \) in Equation (3.5) with respect to \( \theta_C \) under \( H_0 \) in Equation (3.7) is denoted as \( \hat{\theta}_C \), i.e.,

\[ \hat{\theta}_C = \arg \max_{\theta_C} \ln L(\theta_C, \bar{x}_C). \hspace{1cm} (3.9) \]

The likelihood ratio test statistic based on \( \bar{x}_1 \) and \( \bar{x}_2 \) is defined as

\[ \Lambda(\bar{x}_1, \bar{x}_2) = -2 \ln \left[ \frac{L(\hat{\theta}_C, \bar{x}_C)}{L(\hat{\theta}_1, \bar{x}_1) \times L(\hat{\theta}_2, \bar{x}_2)} \right]. \hspace{1cm} (3.10) \]

The Neyman–Pearson lemma states that the likelihood ratio test is the most powerful test at significance level \( \alpha \). As the sample size approaches \( \infty \), the test statistic \( \Lambda(\bar{x}_1, \bar{x}_2) \) is asymptotically chi-squared distribution with degrees of freedom \( q = J + J(J + 1)/2 \). Two statistical hypothesis test procedures, namely Procedure B1 and Procedure B2, are developed here based on the likelihood ratio test statistic in Equation (3.10). The \( p \)-value of Procedure B1 is obtained based on the asymptotic distribution of the likelihood ratio test statistic.
\( \Lambda(\vec{x}_1, \vec{x}_2) \), while the \( p \)-value of Procedure B2 is obtained based on resampling technique.

Based on the observed degradation measurements \( \vec{x}_1 = \{x_{1,1}, x_{1,2}, \ldots, x_{1,K}\} \) and \( \vec{x}_2 = \{x_{2,1}, x_{2,2}, \ldots, x_{2,K}\} \) from Network 1 and Network 2, respectively, the algorithm to computer the \( p \)-value for Procedures B1 and B2 can be described as follows:

Step B1: Obtain the MLE of \( \theta_i = (\mu_i, \Sigma_i) \) from \( \vec{x}_i, i = 1, 2 \) based on Equation (3.8).

Step B2: Combine the two sets of observed degradation measurements \( \vec{x}_C = (\vec{x}_1, \vec{x}_2) \) and obtain the MLE of \( \theta_C = (\mu_C, \Sigma_C) \) from \( \vec{x}_C \) based on Equation (3.9).

Step B3: Compute the likelihood ratio test statistic \( \Lambda_{obs} = \Lambda(\vec{x}_1, \vec{x}_2) \) from Equation (3.10).

Step B4: For Procedure B1, the \( p \)-value is computed as

\[
\begin{align*}
p_{B1} &= \Pr(W < \Lambda_{obs}),
\end{align*}
\]

where \( W \) is random variable that follows a chi-square distribution with degrees of freedom \( q = J + J(J + 1)/2 \).

Step B4': Generate \( x_{1,k}^{(1)} \) and \( x_{2,k}^{(1)} \) from a \( J \)-dimensional multivariate normal distribution

\( \mathcal{N}_J(\hat{\mu}_C, \hat{\Sigma}_C) \), for \( k = 1, 2, \ldots, K \), to obtain the bootstrap samples

\( \vec{x}_1^{(1)} = \{x_{1,1}^{(1)}, x_{1,2}^{(1)}, \ldots, x_{1,K}^{(1)}\} \) and \( \vec{x}_2^{(1)} = \{x_{2,1}^{(1)}, x_{2,2}^{(1)}, \ldots, x_{2,K}^{(1)}\} \), respectively.

Step B5': Compute the likelihood ratio test statistic based on the two bootstrap samples as

\( \Lambda^{(1)} = \Lambda(\vec{x}_1^{(1)}, \vec{x}_2^{(1)}) \) from Equation (3.10).

Step B6': Repeat Steps B4'–B5' \( B \) times to obtain a sequence of bootstrap likelihood ratio test statistics, \( \Lambda^{(b)} = \Lambda(\vec{x}_1^{(b)}, \vec{x}_2^{(b)}) \), for \( b = 1, 2, \ldots, B \).

Step B7': For Procedure B2, the \( p \)-value is computed as

\[
\begin{align*}
p_{B2} &= \frac{1}{B} \sum_{b=1}^{B} 1\{\Lambda_{obs} < \Lambda^{(b)}\}.
\end{align*}
\]

51
The null hypothesis in Equation (3.7) is rejected if $p_{B1} < \alpha$ for Procedure B1, and if $p_{B2} < \alpha$ for Procedure B2, where $\alpha$ is a prefixed significant level.

3.4. Practical Data Analysis

In this section, we illustrate the proposed model and methods by analyzing the real network datasets for P2P service, which is a kind of cyber system that requires cybersecurity insurance. The background of the network datasets is presented in Section 3.4.1, and the results and discussions of the data analysis are presented in Section 3.4.2.

3.4.1. Background of the peer-to-peer network datasets

In recent years, digital currency electronic payment has become more popular, and hence, many countries and companies are committed to strengthening security in digital payments to gain customer’s confidence. The number of people sending money using P2P payments was up 116% and the transactions increased by 207% in 2019 compared with the previous year [85]. P2P networks are also used for sharing electronic files and digital media. Cybersecurity insurance is an indispensable part of the digital currency electronic payment and file-sharing system, especially for the P2P payments/services [18, 40, 53, 56] and the blockchain ecosystem which has a large number of clients and servers. Evaluating the reliability of the P2P systems is an important issue for P2P service providers since scammers can destruct the P2P platform.

Gnutella is an open, decentralized, distributed, P2P search protocol that mainly used to find files [90]. A P2P system can be considered as a cyber network in which individual computers connect directly with each other and share information and resources without using dedicated servers. The nodes in Gnutella perform tasks normally associated with both servers and clients. The nodes provide the client-side interfaces that users can issue
queries and accept queries from other users. A synopsis of the network structure of a P2P system is illustrated in Figure 3.2. For illustrative purposes, in this example, we consider three snapshots of the Gnutella network collected on August 4, 6, and 9, 2002 from the Stanford Network Analysis Project (SNAP) [59, 91]. For notation convenience, we denote the Gnutella networks collected on August 4, 6, and 9, 2002 as P2P network by $G_1$, $G_2$, and $G_3$, respectively.

![Figure 3.2: A synopsis of the network structure of a P2P system [105].](image)

Here, nodes represent hosts in the Gnutella network topology and edges represent connections between the Gnutella hosts. The basic network structure information of the three Gnutella computer networks are presented in Table 3.1.

<table>
<thead>
<tr>
<th>Gnutella Computer Network</th>
<th>Collected on</th>
<th># of nodes</th>
<th># of edges</th>
</tr>
</thead>
<tbody>
<tr>
<td>$G_1$</td>
<td>August 4, 2002</td>
<td>10,876</td>
<td>39,994</td>
</tr>
<tr>
<td>$G_2$</td>
<td>August 6, 2002</td>
<td>8,717</td>
<td>31,525</td>
</tr>
<tr>
<td>$G_3$</td>
<td>August 9, 2002</td>
<td>8,114</td>
<td>26,013</td>
</tr>
</tbody>
</table>

Table 3.1: Basic network structure information of the three Gnutella computer networks.

In this example, since P2P networks do not have fixed client and servers and the roles of peer nodes would be always changed across different days, the nodes (computers) in the P2P
system are not likely to be the same on the three different dates. Therefore, it is reasonable to assume that the P2P network snapshots on August 4, 6, and 9, 2002 are independent and they are three cyber networks with different structures. We are interested in evaluating and comparing the risks of these three networks with different structures for the purpose of determining appropriate cyber insurance policies. For instance, if we find that the three cyber networks are different in terms of risk and reliability, the cyber insurance premium for the network with the highest risk should be higher than the others.

3.4.2. Peer-to-peer network similarity analysis under degree-based attack

In this subsection, we apply the proposed Wiener process model and hypothesis testing procedures to assess and compare the cyber networks presented in Tables 3.1 in terms of the robustness and the risk of the cyber networks. Here, the 4-node network motifs $M_1$, $M_2$, and $M_3$ presented in Figure 3.1 are the topological features that can be observed in target network for measuring the risks of the networks. We remove the nodes in the cyber network based on the degree sequence of the graph (i.e., degree-based attacks), where the degree of a node in a graph is the number of edges that are connected to the node. In other words, the node with the largest degree will get removed first, and the counts of 4-node motifs are obtained when 1%, 2%, ..., 10% of the nodes are removed. Figure 3.3 shows the dynamics of the degradation (in percentages) of the three 4-node motifs under degree-based attacks with $K = 11$ observation points (including the initial status).

Following the notation defined in Section 3.3, $y_{i,j,k}$ corresponds to the counts of the 4-node motif $M_j$ $(j = 1, 2, 3)$ when $k\%$ $(k = 0, 1, 2, \ldots, 10)$ of the nodes are removed based on degree-based attack in cyber network $G_i$ $(i = 1, 2, 3)$, and $x_{i,k} = (x_{i,1,k}, x_{i,2,k}, x_{i,3,k})^T \in \mathbb{R}^3$ is a three-dimensional vector of random variables, where $x_{i,j,k} = (y_{i,j,k} - y_{i,j,k+1})/y_{i,j,0}$, $i = 1, 2, 3$; $j = 1, 2, 3$; $k = 0, 1, 2, \ldots, 10$ is assume to follow a trivariate normal distribution with mean vector $\mu_i$ and variance-covariance $\Sigma_i$. 
For the Gnutella computer networks, the MLEs of the drift parameter $\mu_i = (\mu_{i1}, \mu_{i2}, \mu_{i3})'$ and the diffusion coefficient $\Sigma_i = (\sigma_{i,j,j'})_{j,j'=1,2,3}$ for network $G_i$, $i = 1, 2, 3$ under degree-based attack are presented in Table 3.2, where $j, j' = 1, 2, 3$ corresponding to the three 4-node motifs $M_1$, $M_2$, and $M_3$, respectively. The observed values of the test statistics and the corresponding $p$-values based on Procedures A, B1 and B2 for the pairwise comparisons of the networks $\{G_1, G_2, G_3\}$ are presented in Tables 3.3. The number of bootstrap samples used in Procedure A and Procedure B2 is $B = 500$.

3.4.3. Experiments on peer-to-peer networks

Considering statistical significance at 5% level and compensating for multiple comparisons by using the Bonferroni correction [16], the $p$-values presented in Table 3.3 that are smaller than $0.05/3 \approx 0.01667$ are highlighted in bold to indicate the cases that the null hypothesis in Equation (3.6) is rejected. From Table 3.3, we can see that all the three proposed testing procedures (Procedures A, B1, and B2) show that networks $G_1$ and $G_3$ are different in the resilience/risk levels, while networks $G_1$ and $G_2$ have no significant difference in the resilience/risk levels at the overall 5% significance level. For the comparison between networks $G_1$ and $G_2$, although the $p$-value obtained from Procedure A is greater than the adjusted nominal significance level 0.01667, the small $p$-values from the three test procedures suggests that networks $G_1$ and $G_2$ are different in terms of the resilience/risk levels.
Figure 3.3: The dynamics of the degradation (in percentages) of the three 4-node motifs of the three networks $G_1$, $G_2$, and $G_3$ under degree-based attacks with $K = 11$ observation points.

<table>
<thead>
<tr>
<th>$\hat{\mu} = (\hat{\mu}_1, \hat{\mu}_2, \hat{\mu}_3)'$</th>
<th>$\hat{\mu}_1$</th>
<th>$\hat{\mu}_2$</th>
<th>$\hat{\mu}_3$</th>
<th>$\Sigma$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$G_1$</td>
<td>0.2415</td>
<td>0.2153</td>
<td>0.2603</td>
<td>$\begin{pmatrix} 0.0388 &amp; 0.0118 &amp; 0.1283 \ 0.0144 &amp; 0.0078 &amp; 0.0171 \ 0.0966 &amp; 0.0278 &amp; 0.0695 \end{pmatrix}$</td>
</tr>
<tr>
<td>$G_2$</td>
<td>0.2660</td>
<td>0.2247</td>
<td>0.3408</td>
<td>$\begin{pmatrix} 0.0966 &amp; 0.0278 &amp; 0.0695 \ 0.0320 &amp; 0.0397 &amp; 0.1971 \ 0.3395 &amp; 0.1045 &amp; 0.2695 \end{pmatrix}$</td>
</tr>
<tr>
<td>$G_3$</td>
<td>0.3497</td>
<td>0.2881</td>
<td>0.4915</td>
<td>$\begin{pmatrix} 0.1288 &amp; 0.1661 &amp; 0.8579 \end{pmatrix}$</td>
</tr>
</tbody>
</table>

Table 3.2: Maximum likelihood estimates of the drift parameters and the diffusion coefficient in the Wiener process model for $G_1$, $G_2$, and $G_3$ under degree-based attack.

<table>
<thead>
<tr>
<th>Test</th>
<th>$d_{\text{obs}}$</th>
<th>$\Lambda_{\text{obs}}$</th>
<th>Procedure A</th>
<th>Procedure B1</th>
<th>Procedure B2</th>
</tr>
</thead>
<tbody>
<tr>
<td>$G_1$ vs. $G_2$</td>
<td>1.1122</td>
<td>16.1882</td>
<td>0.0235</td>
<td>0.0127</td>
<td>0.0102</td>
</tr>
<tr>
<td>$G_1$ vs. $G_3$</td>
<td>2.8482</td>
<td>44.6146</td>
<td>$&lt; 0.001$</td>
<td>$&lt; 0.001$</td>
<td>$&lt; 0.001$</td>
</tr>
<tr>
<td>$G_2$ vs. $G_3$</td>
<td>1.7662</td>
<td>12.1299</td>
<td>0.0682</td>
<td>0.0591</td>
<td>0.0553</td>
</tr>
</tbody>
</table>

Table 3.3: The observed values of the test statistics and the corresponding p-values based on Procedures A, B1 and B2 for the pairwise comparisons of the three networks $G_1$, $G_2$, and $G_3$.

From the estimates of the drift parameters presented in Table 3.2, we observe that $\hat{\mu}_{3j} > \hat{\mu}_{2j} > \hat{\mu}_{1j}$ for $j = 1, 2, 3$, which indicates that the functionality of network $G_1$ drops slower than networks $G_2$ and network $G_3$ subject to the degree-based attacks. In other words, the
smaller the values of $\hat{\mu}_{ij}$, the more robust (smaller the risk of) the P2P network. Thus, the results of the analysis based on the proposed methodologies suggest that network $G_1$ is the most reliable network among the three networks while networks $G_2$ and $G_3$ have similar risk levels. These conclusions agree with the observations obtained by looking at the graphs in Figure 3.3.

In this example, we can see that the proposed methodologies can qualify and compare the risks of different complex networks by using the $p$-values of the hypothesis testing procedures as $p$-value is in $(0, 1)$, and the model parameter estimates. This information can be used in determining the premium of cybersecurity insurance. For example, based on the results in this example, the cybersecurity insurance premium for network $G_1$ should be lower than the premiums for networks $G_2$ and $G_3$.

3.5. Monte Carlo Simulation Studies

In this section, Monte Carlo simulation studies are used to verify the usefulness of the proposed Wiener process model and testing procedures for the similarity of two complex networks in terms of the resilience/risk level. We conduct (i) a simulation study based on a parametric statistical model in Section 3.5.1 and (ii) a simulation study without relying on generating data from a parametric model in Section 3.5.2. In these simulation studies, we compare the performance of the three proposed testing procedures, Procedure A, Procedure B1, and Procedure B2, for assessing the similarity of different complex networks based on the simulated type-I error rates and the simulated power values.

3.5.1. Network data generated from a parametric statistical model

In order to evaluate and validate the effectiveness of the proposed methodologies, we consider a simulation study in which the network data are generated based on the Wiener
process model in Equation (3.1). In this simulation, we assume that there are three different
topological features for measuring the risks of two cyber-networks (i.e., \( J = 3 \) and \( I = 2 \))
and these three topological features are observed at \( K = 11 \) time points. We are interested
in testing the hypotheses in Equation (3.6). The topological features for Network 1 and
Network 2 in Equation (3.6) are simulated from the Wiener process model in Equation (3.1)
with the following parameter settings based on the networks \( G_1 \) and \( G_2 \) in the numerical
example presented in Section 3.4:

- Network 1:

  1(a) \( \theta_1 = (\mu_1, \Sigma_1) \mu_1 = \begin{pmatrix} 0.2660 \\ 0.2247 \\ 0.3408 \end{pmatrix} \) and \( \Sigma_1 = \begin{pmatrix} 0.0388 & 0.0118 & 0.0128 \\ 0.0144 & 0.0078 & 0.0017 \end{pmatrix} \);

  1(b) \( \theta_1 = (\mu_1, \Sigma_1) \mu_1 = \begin{pmatrix} 0.2415 \\ 0.2153 \\ 0.2603 \end{pmatrix} \) and \( \Sigma_1 = \begin{pmatrix} 0.0966 & 0.0278 & 0.0690 \\ 0.0320 & 0.0397 & 0.1971 \end{pmatrix} \).

- Network 2:

  2(a) \( \theta_2 = (a \times \mu_1, \Sigma_1) \), where \( a = \{0.05, 0.2, 0.4, 0.6, 0.8, 1.0, 1.2, 1.4, 1.6, 1.8, 2.0, 4.0\} \);

  2(b) \( \theta_2 = (\mu_1, a \times \Sigma_1) \), where \( a = \{0.8, 0.6, 0.4, 0.2, 0.05, 1.2, 1.4, 1.6, 1.8, 2.0, 4.0\} \);

  2(c) \( \theta_2 = (a' + \mu_1, \Sigma_1) \), where \( a' = \{0.00, 0.05, 0.10, 0.15, 0.20\} \).

For each combination of the settings for Network 1 and Network 2, we simulated 1,000
sets of experiments and applied the three proposed testing procedures. The number of
bootstrap samples used in Procedure A and Procedure B2 is \( B = 500 \). Considering using
5% significance level, the simulated proportions of the \( p \)-values less than 0.05 (i.e., rejecting
the null hypothesis in Equation (3.6) at 5% level of significance) are presented in Table
3.4. Note that when \( a = 1.0 \) and \( a' = 0.0 \), the proportions of the \( p \)-values less than 0.05
are corresponding to the simulated type-I error rates and when $a \neq 1.0$ or $a' \neq 0.0$, the proportions of the $p$-values less than 0.05 are corresponding to the simulated power values.

From the simulation results in Tables 3.4, we observe that the simulated type-I error rates (i.e., the simulation rejection rates when $a = 1.0$ or $a' = 0.0$) for Procedure A are always controlled under the nominal 5% level for all the settings considered here, while the simulated type-I error rates for Procedures B1 and B2 can be higher than the nominal 5% level. Especially for setting 1(a), Procedure B1 has the simulated type-I error rate of 0.072. For the power of the three proposed procedures, we observe that the power values increases when the simulated settings are further away from the null hypothesis that Network 1 and Network 2 have the same resilience/risk level, i.e., when $a$ increases from 1.0 to 4.0 or $a$ decreases from 1.0 to 0.05, or $a'$ increases from 0.0 to 0.20. These simulation results indicate that the proposed testing procedures can effectively detect the difference in resilience/risk levels between two complex networks. Although Procedure B1 gives larger power values compare to Procedures A and B2 in most cases, it may be due to the inflated type-I error rate. In comparing the power values of Procedures A and B2, the power values of these two procedures are similar, therefore, when taking the ability in controlling type-I error rate, we would recommend using Procedure A based on the simulation results.
<table>
<thead>
<tr>
<th>Network 2</th>
<th>( \theta_2 = (a \times \hat{\mu}_1, \hat{\Sigma}_1) )</th>
<th>( a/a' )</th>
<th>Procedure 1(a)</th>
<th>Procedure 1(b)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>A</td>
<td>B1</td>
<td>B2</td>
</tr>
<tr>
<td>2(a)</td>
<td>0.05</td>
<td>0.310</td>
<td>0.417</td>
<td>0.306</td>
</tr>
<tr>
<td></td>
<td>0.20</td>
<td>0.160</td>
<td>0.183</td>
<td>0.155</td>
</tr>
<tr>
<td></td>
<td>0.40</td>
<td>0.122</td>
<td>0.166</td>
<td>0.136</td>
</tr>
<tr>
<td></td>
<td>0.60</td>
<td>0.082</td>
<td>0.120</td>
<td>0.105</td>
</tr>
<tr>
<td></td>
<td>0.80</td>
<td>0.055</td>
<td>0.076</td>
<td>0.063</td>
</tr>
<tr>
<td></td>
<td>1.00</td>
<td>0.046</td>
<td>0.072</td>
<td>0.055</td>
</tr>
<tr>
<td></td>
<td>1.20</td>
<td>0.058</td>
<td>0.094</td>
<td>0.059</td>
</tr>
<tr>
<td></td>
<td>1.40</td>
<td>0.068</td>
<td>0.126</td>
<td>0.072</td>
</tr>
<tr>
<td></td>
<td>1.60</td>
<td>0.112</td>
<td>0.208</td>
<td>0.131</td>
</tr>
<tr>
<td></td>
<td>1.80</td>
<td>0.148</td>
<td>0.270</td>
<td>0.150</td>
</tr>
<tr>
<td></td>
<td>2.00</td>
<td>0.272</td>
<td>0.366</td>
<td>0.233</td>
</tr>
<tr>
<td></td>
<td>4.00</td>
<td>0.999</td>
<td>0.999</td>
<td>0.998</td>
</tr>
<tr>
<td></td>
<td>2(b): ( \theta_2 = (\hat{\mu}_1,a \times \hat{\Sigma}_1) )</td>
<td>( a/a' )</td>
<td>Procedure 1(a)</td>
<td>Procedure 1(b)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>A</td>
<td>B1</td>
<td>B2</td>
</tr>
<tr>
<td></td>
<td>0.05</td>
<td>0.750</td>
<td>0.798</td>
<td>0.757</td>
</tr>
<tr>
<td></td>
<td>0.20</td>
<td>0.699</td>
<td>0.734</td>
<td>0.710</td>
</tr>
<tr>
<td></td>
<td>0.40</td>
<td>0.231</td>
<td>0.434</td>
<td>0.240</td>
</tr>
<tr>
<td></td>
<td>0.60</td>
<td>0.097</td>
<td>0.196</td>
<td>0.100</td>
</tr>
<tr>
<td></td>
<td>0.80</td>
<td>0.050</td>
<td>0.116</td>
<td>0.061</td>
</tr>
<tr>
<td></td>
<td>1.00</td>
<td>0.046</td>
<td>0.072</td>
<td>0.055</td>
</tr>
<tr>
<td></td>
<td>1.20</td>
<td>0.045</td>
<td>0.094</td>
<td>0.066</td>
</tr>
<tr>
<td></td>
<td>1.40</td>
<td>0.066</td>
<td>0.124</td>
<td>0.079</td>
</tr>
<tr>
<td></td>
<td>1.60</td>
<td>0.098</td>
<td>0.176</td>
<td>0.121</td>
</tr>
<tr>
<td></td>
<td>1.80</td>
<td>0.155</td>
<td>0.268</td>
<td>0.180</td>
</tr>
<tr>
<td></td>
<td>2.00</td>
<td>0.161</td>
<td>0.282</td>
<td>0.194</td>
</tr>
<tr>
<td></td>
<td>4.00</td>
<td>0.716</td>
<td>0.802</td>
<td>0.711</td>
</tr>
<tr>
<td></td>
<td>2(c): ( \theta_2 = (a' + \hat{\mu}_1, \hat{\Sigma}_1) )</td>
<td>( a/a' )</td>
<td>Procedure 1(a)</td>
<td>Procedure 1(b)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>A</td>
<td>B1</td>
<td>B2</td>
</tr>
<tr>
<td></td>
<td>0.00</td>
<td>0.046</td>
<td>0.072</td>
<td>0.055</td>
</tr>
<tr>
<td></td>
<td>0.05</td>
<td>0.080</td>
<td>0.142</td>
<td>0.110</td>
</tr>
<tr>
<td></td>
<td>0.10</td>
<td>0.249</td>
<td>0.316</td>
<td>0.273</td>
</tr>
<tr>
<td></td>
<td>0.15</td>
<td>0.416</td>
<td>0.438</td>
<td>0.371</td>
</tr>
<tr>
<td></td>
<td>0.20</td>
<td>0.498</td>
<td>0.546</td>
<td>0.515</td>
</tr>
</tbody>
</table>

Table 3.4: Simulated rejection rates for network data generated from the Wiener process model.
3.5.2. Network data generated from nonparametric resampling of a real network dataset

To evaluate the performance of the proposed model and test procedures when the network data are not simulated from a parametric model, we conduct a simulation study based on resampling the real Gnutella P2P network data set presented in Section 3.4. Based on the analysis of Gnutella P2P network data set presented in Section 3.4, we observed that there is a significant difference between networks $G_1$ and $G_3$ (i.e., the Gnutella P2P network snapshots on August 4 and 9, 2002, respectively). Therefore, we consider obtaining the simulated networks by resampling from networks $G_1$ and $G_3$ using the breadth-first search (BFS) method [24] as the network sampling approach. The BFS method is known as an important traversing algorithm with many graph-processing applications and has low computational complexity. After deciding the starting target node arbitrarily, the BFS algorithm traverses the graph layerwise in a tree by exploring all of the neighbor nodes at the same layer before moving on to the nodes at a deeper layer until the required number of nodes is reached. In our study, we terminate the graph traversal procedure when we achieved $100\tau\%$ nodes, where $\tau \in \{0.50, 0.55, \ldots, 0.70\}$. Once again, we are interested in testing the hypotheses in Equation (3.6). Network 1 and Network 2 in Equation (3.6) are simulated by resampling the $100\tau\%$ of nodes as follows:

- Network 1: $G_1$; Network 2: $G_1$
- Network 1: $G_3$; Network 2: $G_3$
- Network 1: $G_1$; Network 2: $G_3$

The simulated rejection rates between two subgraphs under BFS sampling with $100\tau\%$ nodes, where $\tau \in \{0.50, 0.55, \ldots, 0.70\}$, are presented in Table 3.5.
From the simulation results in Table 3.5, we observe that when Network 1 and Network 2 are resampled from $G_1$ and $G_3$, respectively, the three proposed test procedures reject the null hypothesis in Equation (3.6) more than 90% of times for all the percentages of nodes being resampled considered here. Moreover, the simulated rejection rates increase when the percentage of nodes being resampled increases from 50% to 70%. As we observed in the results presented in Section 3.4, $G_1$ and $G_3$ are different in terms of their resilience/risk levels. When the two networks are resampled from the same P2P network (i.e., network $G_1$ or network $G_3$), we observed that the simulated rejection rates decrease when the percentage of nodes being resampled increases from 50% to 70%. This agrees with our intuition since the higher the percentage of the nodes being sampled from the same network, the similarity of the two sampled subgraphs is increasing. These simulation results indicate that the proposed testing procedures can effectively detect the difference in resilience/risk levels between two complex networks even when the two networks are not generated from the proposed Wiener process model.

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Network 1</th>
<th>Network 2</th>
<th>50%</th>
<th>55%</th>
<th>60%</th>
<th>65%</th>
<th>70%</th>
</tr>
</thead>
<tbody>
<tr>
<td>A $G_1$</td>
<td>$G_1$</td>
<td>0.202</td>
<td>0.164</td>
<td>0.075</td>
<td>0.043</td>
<td>0.001</td>
<td></td>
</tr>
<tr>
<td>$G_3$</td>
<td>$G_3$</td>
<td>0.152</td>
<td>0.100</td>
<td>0.066</td>
<td>0.040</td>
<td>0.002</td>
<td></td>
</tr>
<tr>
<td>$G_1$</td>
<td>$G_3$</td>
<td>0.901</td>
<td>0.950</td>
<td>0.963</td>
<td>0.971</td>
<td>0.999</td>
<td></td>
</tr>
<tr>
<td>B1 $G_1$</td>
<td>$G_1$</td>
<td>0.220</td>
<td>0.170</td>
<td>0.081</td>
<td>0.056</td>
<td>0.031</td>
<td></td>
</tr>
<tr>
<td>$G_3$</td>
<td>$G_3$</td>
<td>0.189</td>
<td>0.129</td>
<td>0.058</td>
<td>0.052</td>
<td>0.029</td>
<td></td>
</tr>
<tr>
<td>$G_1$</td>
<td>$G_3$</td>
<td>0.915</td>
<td>0.967</td>
<td>0.978</td>
<td>0.989</td>
<td>0.999</td>
<td></td>
</tr>
<tr>
<td>B2 $G_1$</td>
<td>$G_1$</td>
<td>0.198</td>
<td>0.165</td>
<td>0.069</td>
<td>0.052</td>
<td>0.035</td>
<td></td>
</tr>
<tr>
<td>$G_3$</td>
<td>$G_3$</td>
<td>0.190</td>
<td>0.133</td>
<td>0.070</td>
<td>0.053</td>
<td>0.032</td>
<td></td>
</tr>
<tr>
<td>$G_1$</td>
<td>$G_3$</td>
<td>0.910</td>
<td>0.961</td>
<td>0.969</td>
<td>0.983</td>
<td>0.999</td>
<td></td>
</tr>
</tbody>
</table>

Table 3.5: Simulated rejection rates between two subgraphs under BFS sampling with $100\tau\%$ nodes, where $\tau \in \{0.50, 0.55, \ldots, 0.70\}$ from the P2P networks $G_1$ and $G_3$. 


In this dissertation, we develop the statistical models and methods for assessing the resilience of complex systems and networks via network theory and Markov models. On one hand, to describe the higher-order connectivity patterns, we consider network motifs that unveil hidden mechanisms behind the complex systems. On the other hand, using network motifs, we show that the proposed modified gamma process model and modified Wiener process model can effectively distinguish the resilience levels of complex systems under various types of intentional attacks. Different from the recently proposed stochastic models in [88, 109], which focus on the global degradation signals, our proposed models are able to capture the dynamic local information of complex systems and networks. Extensive experiments on synthetic and real datasets show that our motif-based stochastic models can evaluate the dynamics of network motifs and classify the fragility of complex networks under different types of attacks. For future work, integrating higher-order topological signatures into the proposed modified stochastic models and expanding the study to the design of a knowledge-based system for strategic planning are possible directions.

4.1. Understanding Power Grid Network Vulnerability through the Stochastic Lens of Network Motif Evolution

In Chapter 2, we have developed a gamma degradation modeling approach to assess the reliability and robustness of modern complex networks, with a primary focus on power grid networks. In contrast to other currently available approaches, one of the key advantages of
the proposed methodology is that this approach accounts for *multiple* network topological metrics. We have primarily focused on network motifs as the descriptors of network topology under hazardous scenarios. We have illustrated utility of the new tools in application to the vulnerability analysis of European power grid networks. In addition, to illustrate the performance and utility of the proposed methodology under uncertainties, we performed extensive Monte Carlo simulation studies based on parametric models and resampling of power grid networks. Although our primary application is on power grids, the proposed framework can be applied in a conjunction with analysis of functionality, organization, and vulnerability of many other complex networks and systems (e.g., blockchain transaction graphs, transportation, and telecommunication systems). Furthermore, while we have considered network motifs as the primary descriptors of the underlying network topology and associated system reliability, our approach can be advanced to incorporate other indicators of network vulnerability based on global network topology such as average path length, giant component, and clustering coefficient [1, 25, 81], and local topological descriptors such as Betti numbers and persistent diagrams [79].

For future research, we can consider advancing the proposed motif-based reliability framework to model the resilience of multi-layer networks such as critical infrastructures, blockchain Ethereum token networks, and cryptocurrency-fiat currency interactions.

4.2. Statistical Models and Algorithms for Assessing Robustness and Reliability of Networks with Applications in Cybersecurity Insurance

In Chapter 3, to comprehend the vulnerability of a cyber or physical network subject to attacks or failures and to assess the risks of a complex network, we proposed a statistical approach to assess and understand cyber risk. Specifically, we proposed a Wiener process model to model the dynamics of the topological measures of the network under attacks or failures.
To illustrate the utility of the proposed model and testing procedures, we conducted experiments based on the Gnutella P2P cyber network. Network motifs, which can capture local topological information of a network, are considered as the topological measure in the example. The proposed methodologies can be applied to different topological measures that can reflect the functionality of the complex network. In the practical data analysis, we observe that the proposed methodologies can qualify and compare the risks of different complex networks. We further studied the validity of the proposed methodologies by using two Monte Carlo simulation studies in which the network data are generated from the proposed Wiener process model and resampling from the real Gnutella P2P cyber network data, respectively. From the simulation results, we observed that the proposed testing procedures can effectively detect the difference in resilience/risk levels between two complex networks.

To the best of our knowledge, this is the first study that evaluating the resilience or robustness of cyber networks by using a stochastic model with statistical hypothesis testing procedures. The results obtained from the proposed statistical methodologies can provide some important insights to manage and compare the risks of cyber networks and help cybersecurity insurance providers to determine insurance policy and insurance premiums. The computer program to execute the proposed methodologies is conducted by R [87].

For future research, we plan to utilize other global network topologies, such as betweenness centrality (BC), graph diameter (D), and average path length (APL), to qualify cyber network resiliency and apply the proposed method to internal networks. In addition, the studies presented in this thesis focus on the connectivity of a network, we can further consider using node’s information (e.g., server or customer in P2P system) in quantifying the risk of a network.
A.1. Existence and Uniqueness of the Maximum Likelihood Estimators

According to [69], to show the existence and uniqueness of MLEs of the proposed gamma degradation model, we need to prove that the log-likelihood function \( l(\theta) \) is constant on the boundary of the parameter space and the Hessian matrix, i.e., \( H(\theta) = \partial^2 l(\theta) / \partial \theta_i \partial \theta_j \) is negative-definite everywhere. Based on the functions presented in Eqs. (2.2) and (2.3) in the main body, the log-likelihood function for the \( i \)-th network can be expressed as

\[
l_i(\theta_i) = \sum_{j=1}^{J} \left\{ -K \ln (\Gamma(\lambda_{i,j})) - K \lambda_{i,j} \ln (\beta_i) + (\lambda_{i,j} - 1) \sum_{k=1}^{K} \ln (y_{i,j,k}) - \frac{\sum_{k=1}^{K} y_{i,j,k}}{\beta_i} \right\}
\]

\[
= -K \sum_{j=1}^{J} \ln (\Gamma(\lambda_{i,j})) - K \ln (\beta_i) \sum_{j=1}^{J} \lambda_{i,j} + \sum_{j=1}^{J} (\lambda_{i,j} - 1) \sum_{k=1}^{K} \ln (y_{i,j,k}) - \frac{\sum_{j=1}^{J} \sum_{k=1}^{K} y_{i,j,k}}{\beta_i}.
\]

Differentiating \( l_i(\theta_i) \) with respect to \( \lambda_{i,j} \) and \( \beta_i \), we obtain the first derivatives

\[
\frac{\partial l_i(\theta_i)}{\partial \lambda_{i,j}} = -K \psi(\lambda_{i,j}) - K \ln (\beta_i) + \sum_{k=1}^{K} \ln (y_{i,j,k}), \tag{A.1}
\]

\[
\frac{\partial l_i(\theta_i)}{\partial \beta_i} = -K \sum_{j=1}^{J} \lambda_{i,j} \beta_i + \sum_{j=1}^{J} \sum_{k=1}^{K} y_{i,j,k} \beta_i^2 \tag{A.2}
\]
where $\psi(x) = \Gamma'(x)/\Gamma(x)$ is the digamma function. Then, we can obtain the second derivatives

$$\frac{\partial^2 l_i(\theta_i)}{\partial \lambda_{i,j}^2} = -K\psi_1(\lambda_{i,j}), \quad (A.3)$$

$$\frac{\partial^2 l_i(\theta_i)}{\partial \lambda_{i,j} \partial \lambda_{i,j'}} = 0, \quad (A.4)$$

$$\frac{\partial^2 l_i(\theta_i)}{\beta_i^2} = \frac{K\sum_{j=1}^J \lambda_{i,j}}{\beta_i^3} - 2 \sum_{j=1}^J \sum_{k=1}^K y_{i,j,k}, \quad (A.5)$$

$$\frac{\partial^2 l_i(\theta_i)}{\partial \beta_i \partial \lambda_{i,j}} = -\frac{K}{\beta_i}, \quad (A.6)$$

where $\psi_1(x) = \frac{d\psi(x)}{dx} \in \mathbb{R}^+$ is the trigamma function.

In our study, $\theta_i$ represents the parameter vector of $i$-th power grid network, where $\theta_i = (\lambda_{i,1}, \ldots, \lambda_{i,J}, \beta_i)^\top$. Here, we show that (i) the log-likelihood function is a constant on the boundary and (ii) the Hessian matrix $\left\{ \frac{\partial^2 l_i(\theta_i)}{\partial \theta_a \partial \theta_b} \right\}$ is negative definite at every point $\theta_i$, where $\theta_a, \theta_b \in \{\lambda_{i,1}, \ldots, \lambda_{i,J}, \beta_i\}$.

(i) **Constancy on the Boundary:** $\lim_{\lambda_{i,j} \rightarrow \infty} \sup_{\beta_i \leq \beta_i} l_i(\theta_i) \rightarrow -\infty$.

**Proof:** Since $y_{i,j,k} = \ln(\frac{x_{i,j,k}}{x_{i,j,k+1}}) \in (0, 1)$; $\Gamma(\lambda_{i,j}) \geq 1$; $\lambda_{i,j} > 0$ and $\beta_i > 0$, from Equation (A.1), we can get the first term $-K \sum_{j=1}^J \ln(\Gamma(\lambda_{i,j})) < 0$ and the fourth term $-\sum_{j=1}^J \sum_{k=1}^K \frac{y_{i,j,k}}{\beta_i} < 0$.

For the second and third terms, we have

$$-K \ln(\beta_i) \sum_{j=1}^J \lambda_{i,j} + \sum_{j=1}^J (\lambda_{i,j} - 1) \sum_{k=1}^K \ln(y_{i,j,k})$$

$$= -K \ln(\beta_i) \sum_{j=1}^J \lambda_{i,j} + \sum_{j=1}^J \lambda_{i,j} \sum_{k=1}^K \ln(y_{i,j,k}) - \sum_{j=1}^J \sum_{k=1}^K \ln(y_{i,j,k})$$

$$= \sum_{j=1}^J \lambda_{i,j} \sum_{k=1}^K \ln\left(\frac{y_{i,j,k}}{\beta_i}\right) - \sum_{j=1}^J \sum_{k=1}^K \ln(y_{i,j,k}). \quad (A.7)$$
Therefore, if $\max(y_{i,j,k}) \leq \beta_i$, then Eq. (A.7) < 0, and \(\lim_{\lambda_{i,j} \to \infty} \sup_{\max(y_{i,j,k}) \leq \beta_i} l_i(\theta_i) \to -\infty\). Similarly, we can show that \(\lim_{\beta_i \to \infty} \sup_{\lambda_{i,j} > 0} l_1(\theta_i) \to -\infty\).

Note that since the likelihood function of the modified gamma degradation model includes logarithm (i.e., \(y_{i,j,k} = \log(x_{i,j,k}/x_{i,j,k+1})\) and \(x_{i,j,k} \geq x_{i,j,k+1}\), thus \(y_{i,j,k} \in (0, 1)\).

(ii) Negative-Definiteness of Hessian Matrix: The Hessian matrix \(H(\theta_i) \in \mathbb{R}^{(J+1) \times (J+1)}\) of the parameter vector (i.e., \(\theta_i\)) of \(i\)-th power grid network is given by

\[
H(\theta_i) = \begin{pmatrix}
-K\psi_1(\lambda,1) & 0 & \cdots & -\frac{K}{\beta_i} \\
0 & -K\psi_1(\lambda,2) & \cdots & -\frac{K}{\beta_i} \\
\vdots & \vdots & \ddots & \vdots \\
-\frac{K}{\beta_i} & -\frac{K}{\beta_i} & \cdots & -\frac{K \sum_{j=1}^J \lambda_{i,j}}{\beta_i^2} - 2 \frac{\sum_{j=1}^J \sum_{k=1}^K y_{i,j,k}}{\beta_i^3}
\end{pmatrix}
\]  (A.8)

From Eqs. (A.3), (A.4), (A.5), and (A.6), we can find that the \(m\)-th order leading principal minor\(^1\) of the matrix has sign \((-1)^m\), i.e., the determinant of the upper left 1-by-1 corner of \(H(\theta_i)\) is negative \((-K\psi_1(\lambda,1))\), the determinant of the upper left 2-by-2 corner of \(H(\theta_i)\) is positive \((K^2\psi_1(\lambda,1)\psi(\lambda,2))\), the determinant of the upper left 3-by-3 corner of \(H(\theta_i)\) is negative \((-K^3\psi_1(\lambda,1)\psi(\lambda,2)\psi(\lambda,3))\), etc. The corresponding Hessian matrix is negative-definite everywhere.

For the parameter vector \(\theta = (\theta_1, \ldots, \theta_I)\), the Hessian matrix, \(H(\theta) = (H(\theta_1), H(\theta_2), \ldots, H(\theta_I))\), which can be thought of as an array of \(I\) Hessian matrices. Since each Hessian matrix \(H(\theta_i)\) is negative-definite, thus the array of Hessian matrices is negative-definite.

\(^1\)The leading principal submatrix of order \(m\) of an \(n \times n\) matrix is obtained by deleting the last \(n - m\) rows and column of the matrix; the determinant of a leading principal submatrix is called the leading principal minor of the matrix.
Hence, the existence and uniqueness of the MLE of parameters $\lambda_{1,j}$ (where $j = 1, \cdots, J$) and $\beta_1$ of network 1 for log-likelihood function is guaranteed.

A.2. Comparison to the Conventional Vulnerability Metrics for Power Grid Networks

There generally exist two main directions in the analysis of power grid vulnerability, namely, graph-theoretic tools based on the underlying topology of the power grid network and hybrid tools which incorporate important power flow information into resilience and reliability quantification [2, 26, 51, 95]. As noted by Abedi et al. [2], Cuadra et al. [26], and Sharifi and Yamagata [98], neither of these two approaches can be considered as a preferred technique but rather these two methods should be viewed as complementary directions.

A.2.1. Graph-theoretic metrics

To better place the proposed new technique within the context of the existing vulnerability measures, we compare the utility of these graph-theoretic vulnerability metrics (see Section 1.3) in comparison to the proposed new gamma degradation model.

First, according to the values of APL, D, and BC for all power grids, we find (1) Romania can be classified as the most robust power grid (i.e., Romania has the lowest APL, D, and BC, respectively); (2) both France and Germany have higher APL, higher D, and higher BC, which suggests that they shall be classified as fragile. Second, based on CC, we find (1) Spain is the most resilient power grid which achieves the highest CC and Romania with the lowest CC shall be classified as the most fragile one; (2) CC of France, Germany, Italy, and Poland are equal/close, which suggests that these four power grids have similar levels of resilience. Third, based on $f_c$, Spain with the highest $f_c$ can be viewed as the most resilient one and France can be also classified as the next most resilient power grid. Fourth, we evaluate robustness of the power grid using the vulnerability metric $\gamma$ of [92], who suggest that a power grid is robust if $\gamma < 1.5$ and fragile otherwise. As Table A.1 shows, [Italy
> Germany > Romania > Poland > France > Spain]. However, the fragility parameter \( \gamma \) cannot assist in further discrimination among power grid vulnerability levels. In total, these contradictory findings suggest that the existing graph-theoretic vulnerability metrics based on lower order network connectivity might be insufficient to classify power grid resiliency. To enhance our understanding of the key mechanisms behind fragility of the power grids, a deeper insight into higher-order structures (e.g., network motifs) or electricity-based metrics (e.g., power flow) is needed.

<table>
<thead>
<tr>
<th>Country</th>
<th>APL</th>
<th>D</th>
<th>CC</th>
<th>BC</th>
<th>( f_c )</th>
<th>( \gamma )</th>
</tr>
</thead>
<tbody>
<tr>
<td>France</td>
<td>9.59</td>
<td>26</td>
<td>0.08</td>
<td>2750.01</td>
<td>0.66</td>
<td>2.16</td>
</tr>
<tr>
<td>Germany</td>
<td>11.75</td>
<td>30</td>
<td>0.07</td>
<td>2235.80</td>
<td>0.58</td>
<td>1.32</td>
</tr>
<tr>
<td>Italy</td>
<td>9.74</td>
<td>28</td>
<td>0.08</td>
<td>981.85</td>
<td>0.61</td>
<td>1.21</td>
</tr>
<tr>
<td>Poland</td>
<td>6.94</td>
<td>16</td>
<td>0.07</td>
<td>478.38</td>
<td>0.60</td>
<td>1.64</td>
</tr>
<tr>
<td>Romania</td>
<td>5.52</td>
<td>11</td>
<td>0.05</td>
<td>237.37</td>
<td>0.59</td>
<td>1.42</td>
</tr>
<tr>
<td>Spain</td>
<td>8.26</td>
<td>18</td>
<td>0.09</td>
<td>1670.02</td>
<td>0.70</td>
<td>2.22</td>
</tr>
</tbody>
</table>

Table A.1: Network-based vulnerability metrics for the European power grid networks.

A.2.2. Higher-order structures and electricity-based metrics

We thus compare the robustness of power systems with respect to either network motifs or power flow information [60, 102, 131]. Since the European power grid networks used above only contain the graph structural information, to compare with the state-of-the-art (SOTA) power system reliability metrics, we now consider ACTIVSg500 and ACTIVSg2000 power systems [123, 124] and examine loss-of-load probability (LOLP) and expected unserved energy (EUE) [67, 71] based on an optimal power flow (OPF) model [60]. The basic components of are ACTIVSg500 and ACTIVSg2000 power systems listed in Table A.10, Appendix A.6. Note that LOLP indicates the probability of the occurrence of a loss-of-load event during a given period, and EUE is used to measure the unserved energy in absolute megawatt hours or in fractions of total load. By solving the OPF model [60], we calculate mean LOLP and
mean EUE for both the ACTIVSg500 and ACTIVSg2000 power systems under degree-based attacks. Table A.2 displays the dynamics of 4-node motifs, mean LOLP, and mean EUE under degree-based target attacks for ACTIVSg500 and ACTIVSg2000 power systems respectively, where the fraction of nodes removed $\in \{10\%, 20\%, \ldots, 100\%\}$. We also provide the average degradation rates ($\bar{A}$) of our proposed degradation model for ACTIVSg500 and ACTIVSg2000 power systems for (1) observed four types of 4-node motifs ($M_1$, $M_2$, $M_3$, and $M_4$) and (2) mean LOLP and mean EUE. As demonstrated by the $\bar{A}$ row in Table A.2 (see highlighted parts), we find that the ACTIVSg500 power system is more robust than the ACTIVSg2000 power system, since the average degradation rates of ACTIVSg500 are always smaller than the average degradation rates of ACTIVSg2000 in terms of both network motifs and SOTA reliability metrics. This means that robustness analysis based on network motifs can yield a similar conclusion as reliability metrics. There are advantages of our proposed gamma degradation model: (1) our model has lower complexity (whose complexity depends on the structure of the graph) when the size of power grid is larger and (2) motif information can be used as alternative local metrics of fragility under various attacks as well as early warning indicators of system degradation and failure.

We find that both approaches (i.e., based on either network motifs or power flow information) lead to the same conclusion. However, the new motif-based gamma degradation model uses noticeably less information than the competing measure based on power flow properties. As a result, the new motif-based gamma degradation model can be used for such important problems as forecasting power system response to contingencies under limited data and uncertain scenarios. That is, motif characteristics can be further used as local measures of reliability for power systems under attacks.

A.3. Functionality of Power Grid Network under Attacks

In this section, we evaluate how network motifs affect the functionality of power system under random attacks and how transmission lines removal impact the functionality of power system.
<table>
<thead>
<tr>
<th>Fraction node</th>
<th>ACTIVSg500</th>
<th></th>
<th></th>
<th></th>
<th>ACTIVSg2000</th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>$M_1$</td>
<td>$M_2$</td>
<td>$M_3$</td>
<td>$M_4$</td>
<td>$M_1$</td>
<td>$M_2$</td>
<td>$M_3$</td>
<td>$M_4$</td>
</tr>
<tr>
<td>0.1</td>
<td>114</td>
<td>512</td>
<td>0</td>
<td>5</td>
<td>0.387</td>
<td>0.070</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0.2</td>
<td>44</td>
<td>253</td>
<td>0</td>
<td>3</td>
<td>0.402</td>
<td>0.090</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0.3</td>
<td>14</td>
<td>103</td>
<td>0</td>
<td>1</td>
<td>0.474</td>
<td>0.121</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0.4</td>
<td>19</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.549</td>
<td>0.132</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0.5</td>
<td>14</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.764</td>
<td>0.147</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0.6</td>
<td>9</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.869</td>
<td>0.182</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0.7</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.915</td>
<td>0.258</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0.8</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.978</td>
<td>0.323</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0.9</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.996</td>
<td>0.467</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1.000</td>
<td>0.558</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table A.2: Dynamics of motifs remaining, mean LOLP ($\text{LOLP}$), and mean EUE ($\text{EUE}$) for ACTIVSg500 and ACTIVSg2000 power systems under degree-based attacks, respectively; the average degradation rate $\bar{A}$ for ACTIVSg500 and ACTIVSg2000 power systems based on (1) 4-node motifs, (2) $\text{LOLP}$ and $\text{EUE}$. 


A.3.1. Relations between Network Motifs and Functionality of Power System

To illustrate how the power flow, load served, and generators operating are related to the number of remaining 4-node motifs under random attacks, here we analyze the data based on the IEEE 118-Bus system with 118 nodes and 177 edges (for more detail, see Table A.10, Appendix A.6). Table A.3 shows how losing network motifs (i.e., observed 4 types of 4-node motifs) would affect functional integrity of the IEEE 118-Bus system including power flow, the fraction of load served, and the fraction of generators operating, under the adverse scenario of random node removal. (Here fractions of nodes removed are $\in \{10\%, 20\%, \ldots, 100\%\}$). Table A.4 reports the correlation coefficients between four different types of 4-node motifs and these three electrical properties (i.e., power flows, fraction of load served, and fraction of generators operating). We observe that there exists a strong correlation between 4-node motifs and three electrical properties. Furthermore, power flow and fraction of generators operating exhibit a somewhat stronger correlation with 4-node motifs than the fraction of load served does.

<table>
<thead>
<tr>
<th>Fraction node</th>
<th>$M_1$</th>
<th>$M_2$</th>
<th>$M_3$</th>
<th>$M_4$</th>
<th>Power flows</th>
<th>Fraction load served</th>
<th>Fraction generators operating</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>269</td>
<td>660</td>
<td>114</td>
<td>16</td>
<td>87.43</td>
<td>0.88</td>
<td>0.85</td>
</tr>
<tr>
<td>0.2</td>
<td>201</td>
<td>462</td>
<td>82</td>
<td>10</td>
<td>73.50</td>
<td>0.79</td>
<td>0.74</td>
</tr>
<tr>
<td>0.3</td>
<td>112</td>
<td>291</td>
<td>45</td>
<td>9</td>
<td>53.57</td>
<td>0.68</td>
<td>0.60</td>
</tr>
<tr>
<td>0.4</td>
<td>30</td>
<td>93</td>
<td>12</td>
<td>3</td>
<td>34.76</td>
<td>0.53</td>
<td>0.42</td>
</tr>
<tr>
<td>0.5</td>
<td>14</td>
<td>48</td>
<td>3</td>
<td>1</td>
<td>29.06</td>
<td>0.44</td>
<td>0.31</td>
</tr>
<tr>
<td>0.6</td>
<td>4</td>
<td>23</td>
<td>3</td>
<td>0</td>
<td>19.95</td>
<td>0.34</td>
<td>0.18</td>
</tr>
<tr>
<td>0.7</td>
<td>1</td>
<td>5</td>
<td>1</td>
<td>0</td>
<td>6.15</td>
<td>0.25</td>
<td>0.08</td>
</tr>
<tr>
<td>0.8</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>2.59</td>
<td>0.22</td>
<td>0.04</td>
</tr>
<tr>
<td>0.9</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.00</td>
<td>0.19</td>
<td>0.00</td>
</tr>
<tr>
<td>1.0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
</tbody>
</table>

Table A.3: Dynamics of motifs remaining, the fraction of load served, and the fraction of generators operating for the IEEE 118-Bus system under attacks (fraction of nodes removed).
Table A.4: Correlation coefficients between the remaining 4-node motifs and three electrical properties (i.e., power flow, fraction of load served, and fraction of generators operating) by randomly removing nodes.

<table>
<thead>
<tr>
<th>Motif</th>
<th>Power flow</th>
<th>Fraction load served</th>
<th>Fraction generators operating</th>
</tr>
</thead>
<tbody>
<tr>
<td>$M_1$</td>
<td>0.948</td>
<td>0.885</td>
<td>0.925</td>
</tr>
<tr>
<td>$M_2$</td>
<td>0.956</td>
<td>0.897</td>
<td>0.935</td>
</tr>
<tr>
<td>$M_3$</td>
<td>0.942</td>
<td>0.877</td>
<td>0.917</td>
</tr>
<tr>
<td>$M_4$</td>
<td>0.953</td>
<td>0.904</td>
<td>0.943</td>
</tr>
</tbody>
</table>

To show the dynamics of transmission lines when removing a fraction of selective nodes, we also analyze the statuses of transmission lines of the IEEE 118-Bus system when a fraction of random nodes are removed randomly. Table A.5 displays the number of available transmission lines in service and the number of lines that change in the direction of power flow under random attacks.

Table A.5 indicates that as can be expected, the number of lines in service decreases as the fraction of nodes removed increases. However, the number of power flow direction reversals is not monotone, implying that the reversal of power flow directions tend to be less relevant to the number of removed lines and more relevant to the locations of the removed lines.

A.3.2. The Impact of Removing Transmission Lines

Since the European power grid networks contain only graph structural information without AC flow, we study the impact of removing transmission lines under random attacks on the IEEE 118-Bus system. Table A.6 shows how losing network motifs affects the fraction of load served and the fraction of generators operating for the IEEE 118-Bus system, under the adverse scenario of random line removal. (Here fractions of removed lines are $\in \{10\%, 20\%, \ldots, 100\%\}$). As Table A.7 demonstrates, both fraction of load served and fraction of generators operating exhibit strong correlation with 4-node motifs.
<table>
<thead>
<tr>
<th>Fraction</th>
<th>Number lines in service</th>
<th>Number power direction change</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>161</td>
<td>9</td>
</tr>
<tr>
<td>0.2</td>
<td>131</td>
<td>17</td>
</tr>
<tr>
<td>0.3</td>
<td>105</td>
<td>14</td>
</tr>
<tr>
<td>0.4</td>
<td>70</td>
<td>13</td>
</tr>
<tr>
<td>0.5</td>
<td>50</td>
<td>8</td>
</tr>
<tr>
<td>0.6</td>
<td>36</td>
<td>4</td>
</tr>
<tr>
<td>0.7</td>
<td>20</td>
<td>3</td>
</tr>
<tr>
<td>0.8</td>
<td>10</td>
<td>0</td>
</tr>
<tr>
<td>0.9</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>1.0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Table A.5: Number of lines in service and number of lines which power flow direction is impacted by random attacks.

<table>
<thead>
<tr>
<th>Fraction</th>
<th>$M_1$</th>
<th>$M_2$</th>
<th>$M_3$</th>
<th>$M_4$</th>
<th>Fraction load served</th>
<th>Fraction generators operating</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>364</td>
<td>840</td>
<td>127</td>
<td>19</td>
<td>0.96</td>
<td>0.96</td>
</tr>
<tr>
<td>0.2</td>
<td>260</td>
<td>631</td>
<td>108</td>
<td>15</td>
<td>0.87</td>
<td>0.87</td>
</tr>
<tr>
<td>0.3</td>
<td>202</td>
<td>493</td>
<td>88</td>
<td>10</td>
<td>0.81</td>
<td>0.81</td>
</tr>
<tr>
<td>0.4</td>
<td>138</td>
<td>342</td>
<td>52</td>
<td>9</td>
<td>0.72</td>
<td>0.72</td>
</tr>
<tr>
<td>0.5</td>
<td>71</td>
<td>201</td>
<td>30</td>
<td>6</td>
<td>0.64</td>
<td>0.64</td>
</tr>
<tr>
<td>0.6</td>
<td>56</td>
<td>149</td>
<td>20</td>
<td>5</td>
<td>0.60</td>
<td>0.59</td>
</tr>
<tr>
<td>0.7</td>
<td>30</td>
<td>91</td>
<td>12</td>
<td>3</td>
<td>0.52</td>
<td>0.52</td>
</tr>
<tr>
<td>0.8</td>
<td>11</td>
<td>44</td>
<td>3</td>
<td>1</td>
<td>0.41</td>
<td>0.41</td>
</tr>
<tr>
<td>0.9</td>
<td>1</td>
<td>10</td>
<td>1</td>
<td>0</td>
<td>0.29</td>
<td>0.29</td>
</tr>
<tr>
<td>1.0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.00</td>
<td>0.00</td>
</tr>
</tbody>
</table>

Table A.6: Dynamics of 4-node motifs remaining ($M_1$, $M_2$, $M_3$, and $M_4$), the fraction of load served, and the fraction of generators operating for the IEEE 118-Bus system under random attacks (fraction of lines removed).
<table>
<thead>
<tr>
<th></th>
<th>Fraction of load served</th>
<th>Fraction of generators operating</th>
</tr>
</thead>
<tbody>
<tr>
<td>$M_1$</td>
<td>0.861</td>
<td>0.863</td>
</tr>
<tr>
<td>$M_2$</td>
<td>0.879</td>
<td>0.881</td>
</tr>
<tr>
<td>$M_3$</td>
<td>0.877</td>
<td>0.879</td>
</tr>
<tr>
<td>$M_4$</td>
<td>0.904</td>
<td>0.906</td>
</tr>
</tbody>
</table>

Table A.7: Correlation coefficients between the remaining 4-node motifs and two electrical properties (i.e., fraction of load served and fraction of generators operating) by randomly removing links/edges.

### A.4. Sensitive Analysis

Since the proposed methodologies rely on the parametric gamma degradation model, it is important to investigate the sensitivity of the proposed methods to the mis-specification of the underlying data generating mechanism. For this purpose, we consider a Monte Carlo simulation study in which the data are generated from a Wiener process model, which is a commonly used degradation model for non-monotonic degradation data, and apply the proposed gamma process model for data analysis. This provides important information to practitioners to ensure the proposed methodologies are not sensitive to the data generating mechanism and they will not result in unacceptable changes in the conclusions.

Suppose $J$ represents the total number of 4-node motifs and $K$ represents the total number of observation points, to generate data from a Wiener process model in our setting, we define the $J$-dimensional random vector $\mathbf{x}_{i,k} = (x_{i,1,k}, x_{i,2,k}, \ldots, x_{i,J,k})' \in \mathbb{R}^J$, where $x_{i,j,k} = y_{i,j,k} - y_{i,j,k+1}$, $y_{i,j,k}$ is the 4-node motifs of $j$-th type for network $i$ at observation point $t_k$ ($k = 0, \ldots, K$), follows a multivariate normal distribution denoted as

$$
\mathcal{M}_W : \mathbf{x}_{i,k} \sim \mathcal{N}_J(\mu_i, \Sigma_i), \quad (A.9)
$$
where \( \mu_i = (\mu_1, \ldots, \mu_J)^T \in \mathbb{R}^J \) and \( \Sigma_i \) is a \( J \times J \) variance-covariance matrix given by

\[
\Sigma_i = \begin{pmatrix}
\sigma_{i,1}^2 & \rho_{1,2} \sigma_{i,1} \sigma_{i,2} & \cdots & \rho_{1,J} \sigma_{i,1} \sigma_{i,J} \\
\rho_{2,1} \sigma_{i,2} \sigma_{i,1} & \sigma_{i,2}^2 & \cdots & \rho_{2,J} \sigma_{i,2} \sigma_{i,J} \\
\vdots & \vdots & \ddots & \vdots \\
\rho_{J,1} \sigma_{i,J} \sigma_{i,1} & \rho_{J,2} \sigma_{i,J} \sigma_{i,2} & \cdots & \sigma_{i,J}^2
\end{pmatrix}.
\] (A.10)

Here, \( \mu_i \) is the slope of the linear drift and \( \Sigma_i \) is the diffusion coefficient of the Wiener process. In the simulation study, to evaluate the performance of the proposed method for comparing two networks, we generate data for network 1 from a Wiener process model \( M_1^W \) with parameter vector \( \theta_1 = (\mu_1, \Sigma_1) \) and data for network 2 from a Wiener process model \( M_2^W \) with parameter vector \( \theta_2 = (\mu_2, \Sigma_2) \). The following three settings are considered:

**S1.** \( M_1^W \) and \( M_2^W \) have same diffusion coefficient but different drifts; motifs are independent:

\[
\theta_1 = (\mu_1, \Sigma_1), \text{ where } \mu_1 = (1, 1, 1, 1)^T \text{ and } \Sigma_1 = \begin{bmatrix} 0.01 & 0 & 0 & 0 \\
0.01 & 0.01 & 0 & 0 \\
0 & 0.01 & 0.01 & 0 \\
0 & 0 & 0.01 & 0.01 \end{bmatrix};
\]

\[
\theta_2 = (\mu_2, \Sigma_1), \text{ where } \mu_2 = \mu_1 + a_1 \text{ with } a_1 = \{0.01, 0.02, \cdots, 0.05\};
\]

**S2.** \( M_1^W \) and \( M_2^W \) have the same drift but different diffusion coefficients; motifs are independent:

\[
\theta_1 = (\mu_1, \Sigma_1), \text{ where } \mu_1 = (1, 1, 1, 1)^T \text{ and } \Sigma_1 = \begin{bmatrix} 0.01 & 0 & 0 & 0 \\
0.01 & 0.01 & 0 & 0 \\
0 & 0.01 & 0.01 & 0 \\
0 & 0 & 0.01 & 0.01 \end{bmatrix};
\]

\[
\theta_2 = (\mu_1, \Sigma_2), \text{ where } \Sigma_2 = a_2 \times \Sigma_1 \text{ and } a_2 = \{1.2, 1.4, \cdots, 2.0\};
\]

**S3.** \( M_1^W \) and \( M_2^W \) have the same drift but different diffusion coefficients; motifs are dependent:

\[
\theta_1 = (\mu_1, \Sigma_1), \text{ where } \mu_1 = (1, 1, 1, 1)^T \text{ and } \Sigma_1 = \begin{bmatrix} 0.01 & 0.001 & 0.001 & 0.001 \\
0.001 & 0.01 & 0.01 & 0.001 \\
0.001 & 0.001 & 0.001 & 0.001 \\
0.001 & 0.001 & 0.001 & 0.001 \end{bmatrix};
\]

\[
\theta_2 = (\mu_1, \Sigma_2'), \text{ where } \Sigma_2' = a_2' \times \Sigma_1 \text{ and } a_2' = \{1.2, 1.4, \cdots, 2.0\}.
\]
Table A.8 presents the simulated rejection rates based on 10000 simulations. Based on the simulation results, we observe that when the motifs are independent, even when the data is generated from a non-gamma model, the proposed gamma process model and the testing procedure can control the significance level close to the 5% level and provide reasonable power when the two networks are different. When the motifs are dependent, the simulated significance level is higher than the nominal 5% level, which indicates that caution needs to be taken when the underlying model is suspected to be non-gamma and the motifs are dependent.

<table>
<thead>
<tr>
<th>Setting</th>
<th>μ_2</th>
<th>μ_1</th>
<th>μ_1 + 0.01</th>
<th>μ_1 + 0.02</th>
<th>μ_1 + 0.03</th>
<th>μ_1 + 0.04</th>
<th>μ_1 + 0.05</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rejection rate</td>
<td>0.056</td>
<td>0.094</td>
<td>0.136</td>
<td>0.155</td>
<td>0.304</td>
<td>0.414</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Setting</th>
<th>Σ_2</th>
<th>Σ_1</th>
<th>Σ_1 × 1.2</th>
<th>Σ_1 × 1.4</th>
<th>Σ_1 × 1.6</th>
<th>Σ_1 × 1.8</th>
<th>Σ_1 × 2.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rejection rate</td>
<td>0.056</td>
<td>0.084</td>
<td>0.150</td>
<td>0.186</td>
<td>0.272</td>
<td>0.402</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Setting</th>
<th>Σ_2</th>
<th>Σ_1</th>
<th>Σ_1 × 1.2</th>
<th>Σ_1 × 1.4</th>
<th>Σ_1 × 1.6</th>
<th>Σ_1 × 1.8</th>
<th>Σ_1 × 2.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rejection rate</td>
<td>0.080</td>
<td>0.085</td>
<td>0.134</td>
<td>0.194</td>
<td>0.298</td>
<td>0.372</td>
<td></td>
</tr>
</tbody>
</table>

Table A.8: Simulated rejection rates for settings S1, S2 and S3.

A.5. Computation and Memory Usage

We run our computer programs on Amazon EC2 Bare Metal Instance “m5d.metal” with 96 CPUs and 384 GiB memory. In Table A.9, we present the average running time (in seconds) and memory used for

(1) motifs calculation;

(2) targeted attacks;
(3) MLEs calculation of the gamma degradation model;

(4) likelihood ratio test;

(5) partial motifs test;

(6) parametric statistical model (average running time for fitting one dataset);

(7) nonparametric statistical model (average running time for fitting one dataset).

<table>
<thead>
<tr>
<th>Task</th>
<th>Avg. CPU time</th>
<th>Avg. Memory used</th>
</tr>
</thead>
<tbody>
<tr>
<td>Motifs calculation</td>
<td>$6.3 \times 10^{-4}$ s</td>
<td>736 B</td>
</tr>
<tr>
<td>Targeted attacks</td>
<td>$2.4 \times 10^{-4}$ s</td>
<td>824 B</td>
</tr>
<tr>
<td>MLEs of model paras. (Equation (3))</td>
<td>$1.8 \times 10^{-1}$ s</td>
<td>26.8 kB</td>
</tr>
<tr>
<td>Likelihood ratio test (Equation (4))</td>
<td>$2.1 \times 10^{-1}$ s</td>
<td>725 B</td>
</tr>
<tr>
<td>Partial Motifs Test</td>
<td>1.5 s</td>
<td>102 kB</td>
</tr>
<tr>
<td>Parametric statistical model (one time)</td>
<td>$2.0 \times 10^{-1}$ s</td>
<td>328 kB</td>
</tr>
<tr>
<td>Nonparametric statistical model (one time)</td>
<td>$1.5 \times 10^{-1}$ s</td>
<td>498 kB</td>
</tr>
</tbody>
</table>

Table A.9: Average running time and memory used for seven tasks/procedures in this paper.

A.6. Power Systems from TAMU Repository

<table>
<thead>
<tr>
<th>Power system</th>
<th>Buses</th>
<th>Generators</th>
<th>Loads</th>
<th>Lines</th>
<th>Transformers</th>
</tr>
</thead>
<tbody>
<tr>
<td>IEEE 118</td>
<td>118</td>
<td>19</td>
<td>91</td>
<td>177</td>
<td>9</td>
</tr>
<tr>
<td>ACTIVSg500</td>
<td>500</td>
<td>90</td>
<td>409</td>
<td>597</td>
<td>1</td>
</tr>
<tr>
<td>ACTIVSg2000</td>
<td>2,000</td>
<td>544</td>
<td>1,347</td>
<td>2,345</td>
<td>861</td>
</tr>
</tbody>
</table>

Table A.10: Basic components information of three synthetic power systems.
BIBLIOGRAPHY


