Chen, Yuzhou, and Hon Keung Tony Ng. 2024. "Statistical Models and Algorithms for Assessing Robustness and Reliability of Networks with Applications in Cybersecurity Insurance." *Variance* 17 (1).

Financial and Statistical Methods

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

Yuzhou Chen[1a], Hon Keung Tony Ng[2b]

[1] Department of Computer and Information Sciences, Temple University, [2] Department of Mathematical Sciences, Bentley University

Keywords: Bootstrap, degradation model, network motif, peer-to-peer network, Wiener Process

Variance

Vol. 17, Issue 1, 2024

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 and the Enron email network are 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.

Address for Correspondence: yuzhouc@smu.edu

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 (Department of Homeland Security 2019). In 2013, the Group of Twenty (G-20) urged to treat cyber-attacks as a threat to the global economy (Ackerman 2013). 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 (Tehan 2015). Recently, (Böhme, Laube, and Riek 2019) provided a general framework for actuaries to think about cyber risk and the approaches to cyber risk analysis. In this paper, "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 (Biener, Eling, and Wirfs 2014).

a Yuzhou Chen is an Assistant Professor Department of Computer and Information Sciences at Temple University. He was a postdoctoral scholar in Department of Electrical and Computer Engineering at Princeton University, and a research fellow at the National Renewable Energy Laboratory and INRIA. He received his Ph.D. in Statistics at Southern Methodist University in 2021, M.S. degree from University of Texas at Dallas, and B.S. degree from Zhejiang Gongshang University. His main research interests are geometric deep learning, topological data analysis, knowledge discovery in graphs and spatio-temporal data, applications to power systems, biosurveillance and blockchain data analytics.

b Hon Keung Tony Ng is a Professor with the Department of Mathematical Sciences, Bentley University. Before joining Bentley University in July 2022, he was at Southern Methodist University for 20 years. He received his Ph.D. in mathematics from McMaster University, Hamilton, ON, Canada, in 2002. His research interests include reliability, censoring methodology, ordered data analysis, non-parametric methods, and statistical inference. He has published more than 150 research papers in refereed journals. He is an elected senior member of IEEE (2008), an elected member of the International Statistical Institute (2008), and an elected fellow of the American Statistical Association (2016).

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 (Zurich Insurance Company Ltd and Atlantic Council of the United States 2014). However, research on cyber risk, especially on evaluation and comparison of the risks in the insurance domain, is fairly limited. In addition, pricing for cybersecutiry insurance is a challenging problem since sybersecutiry insurance has no standard scoring systems or actuarial tables for rate making (Xu and Hua 2017). 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, Laube, and Riek (2019) 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 (Biener, Eling, and Wirfs 2014; Böhme, Laube, and Riek 2019). 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 (Vespignani 2010; Havlin et al. 2014). However, those heuristic methods are often designed for a specific cyber network, which limited their applicability to diverse areas (Kotenko, Saenko, and Lauta 2018). 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. 2016) 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 paper, 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 (Doksum, Hóyland, and Hoyland 1992; Chen et al. 2017; Lio et al. 2019). 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.

The rest of this paper is organized as follows. In Section 2, the graph representation of the cyber network and the topological measures for evaluating the robustness/loss of availability of a network are discussed. In Section 3, the proposed Wiener process model for modeling the dynamics of a cyber network losing its functionality/connectivity upon the removal of nodes is presented. The proposed statistical testing procedures for comparing the risks of two networks are also presented in Section 3. In Section 4, illustrative examples based on real data sets of the Gnutella peer-to-peer (P2P) cyber networks and sampled subgraphs from the Enron email network are given in Section 4. A Monte Carlo simulation study is used to evaluate the performance of the proposed model and methods in Section 5. The performance and limitations of the proposed methods are discussed. Finally, in Section 6, some concluding remarks are provided.

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 $\mathcal{G} = \{\mathcal{V}, \mathcal{E}, W\}$, 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 $\mathcal{G}$, which is an $N \times N$ nonnegative symmetric matrix with entries $\{\omega_{ij}\}_{1 \le i,j \le N}$, i.e., $\omega_{ij} \neq 0$ for any $e_{ij} \in \mathcal{E}$ and $\omega_{ij} = 0$, otherwise. In the study of cyber network, we consider unweighted and undirected graph, i.e., $\omega_{ij} = 1$ and $e_{ij} = e_{ji} \in \mathcal{E}$, for all $1 \le i, j \le N$. Hence, we suppress the notation of the adjacency matrix in the graph representation and represent the graph as $\mathcal{G} = \{\mathcal{V}, \mathcal{E}\}$.

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.

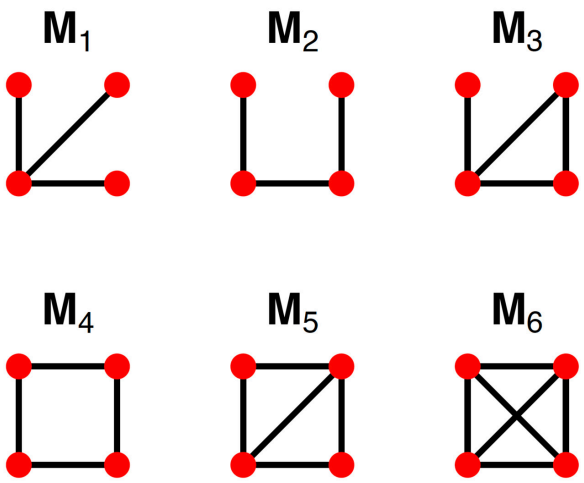

Figure 1. All connected 4-node network motifs.

High-order structures are often called the building blocks of network (Maison et al. 2002). Compared with global network topology (e.g., graph diameter and average path length) (Cohen et al. 2000; Piraveenan, Uddin, and Chung 2012; Cuadra et al. 2015), 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 (Shen-Orr et al. 2002). 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 (Newman 2010). 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 (Holland and Leinhardt 1971; Watts and Strogatz 1998). Another commonly used robustness measure is the network motifs introduced by (Milo et al. 2002) in conjunction with the assessment of the stability of biological networks and later have been studied in a variety of contexts (Alon 2007). 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 $\mathcal{G}$. Figure 1 shows all possible 4-node motifs in undirected graph. Recently, Dey, Gel, and Poor (2019) 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 (Holland and Leinhardt 1970) can be used. For large network (> 10,000 edges), algorithms to approximate the exact motif counts can be used (Kashtan et al. 2004; Böhme, Laube, and Riek 2019), 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.

3. WIENER PROCESS MODEL AND SIMILARITY TESTS FOR NETWORKS

In this paper, 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 focuses 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 (Chen et al. 2017) 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 3.1 and three statistical hypothesis testing procedures are proposed in Section 3.2.

3.1. WIENER PROCESS MODEL

Suppose that there are $\mathcal{I}$ networks and $\mathcal{J}$ different topological features (e.g., network motifs, Wasserstein distance, and weighted-pairwise distance, etc.) are used to measure the risks of those $\mathcal{I}$ networks, these topological features are observed at different time points t_k, $k = 0, 1, \ldots, \mathcal{K}$, where $\mathcal{K}+1$ is the total number of observation points. The observation point t_k 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 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 $D_{i,j}(t_k) - D_{i,j}(t_{k-1})$, $k = 1, 2, \ldots, \mathcal{K}$ are independent;

(iii) the increments $D_{i,j}(t_k) - D_{i,j}(t_{k-1})$ follows a normal distribution $\mathcal{N}(\mu^*_{i,j}, \sigma^{*2}_{i,j})$.

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

$$\mathcal{M}_W : \boldsymbol{x}_{i,k} \sim \mathcal{N}_{\mathcal{J}}(\boldsymbol{\mu}_i, \boldsymbol{\Sigma}_i), \tag{1}$$

where $\boldsymbol{\mu}_i = (\mu_{i1}, \ldots, \mu_{i\mathcal{J}})' \in \mathbb{R}^{\mathcal{J}}$ represents the slope of the linear drift and $\boldsymbol{\Sigma}_i$ represents an $\mathcal{J} \times \mathcal{J}$ symmetric variance-covariance matrix

$$\boldsymbol{\Sigma}_i = \begin{pmatrix} \sigma_{i,11} & \sigma_{i,12} & \cdots & \sigma_{i,1\mathcal{J}} \\ & \sigma_{i,22} & \cdots & \sigma_{i,2\mathcal{J}} \\ & & \ddots & \vdots \\ & & & \sigma_{i,\mathcal{J}\mathcal{J}} \end{pmatrix} \tag{2}$$

which is also known as the diffusion coefficient. The joint probability density function of the random vector $\boldsymbol{x}_{i,k}$ is

$$f(\boldsymbol{x}_{i,k}; \boldsymbol{\mu}_i, \boldsymbol{\Sigma}_i) = \frac{1}{(2\pi)^{\mathcal{J}/2}|\boldsymbol{\Sigma}_i|^{1/2}} \exp\left\{\frac{(\boldsymbol{x}_{i,k} - \boldsymbol{\mu}_i)'\boldsymbol{\Sigma}_i^{-1}(\boldsymbol{x}_{i,k} - \boldsymbol{\mu}_i)}{2}\right\}, \tag{3}$$

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

$$\ln L(\boldsymbol{\theta}|\boldsymbol{x}) = \sum_{i=1}^{\mathcal{I}} \ln L_i(\boldsymbol{\theta}_i|\boldsymbol{x}_i), \tag{4}$$

where $\boldsymbol{x} = (\boldsymbol{x}_1, \ldots, \boldsymbol{x}_{\mathcal{I}})$, $\boldsymbol{\theta} = (\boldsymbol{\theta}_1, \ldots, \boldsymbol{\theta}_{\mathcal{I}})$,

$$\ln L(\boldsymbol{\theta}_i \mid \boldsymbol{x}_i) = \sum_{k=1}^{\mathcal{K}} \left[-\frac{\mathcal{J}}{2}\ln(2\pi) - \frac{1}{2}\ln(|\Sigma_i|) - \frac{1}{2}(\boldsymbol{x}_{i,k} - \boldsymbol{\mu}_i)'\Sigma_i^{-1}(\boldsymbol{x}_{i,k} - \boldsymbol{\mu}_i)\right], \tag{5}$$

and $\boldsymbol{\theta}_i = \{(\boldsymbol{\mu}_i, \boldsymbol{\Sigma}_i) | \boldsymbol{\mu}_i \in \mathbb{R}^{\mathcal{J}}, \boldsymbol{\Sigma}_i$ is an $\mathcal{J} \times \mathcal{J}$ positive-semi-definite matrix is the parameter vector for the i-th network.

The maximum likelihood estimates (MLEs) of the model parameters can be obtained by maximizing $\ln L(\boldsymbol{\theta}_i|\boldsymbol{x}_i)$ in Eq. (5) with respect to $\boldsymbol{\mu}_i$ and $\boldsymbol{\Sigma}_i$. 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.

3.2. 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 $\mathcal{J}$ topological measures. We are interested in testing the hypotheses

$$\begin{aligned} H_0: &\ \text{Network 1 and Network 2} \\ &\ \text{have the same resilience/risk level} \\ \text{against } H_1: &\ \text{Network 1 and Network 2} \\ &\ \text{do not have the same resilience/risk level} \end{aligned} \tag{6}$$

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 $\vec{\boldsymbol{x}}_1 = \{\boldsymbol{x}_{1,1}, \boldsymbol{x}_{1,2}, \cdots, \boldsymbol{x}_{1,\mathcal{K}}\}$ and $\vec{\boldsymbol{x}}_2 = \{\boldsymbol{x}_{2,1}, \boldsymbol{x}_{2,2}, \cdots, \boldsymbol{x}_{2,\mathcal{K}}\}$ from Network 1 and Network 2, respectively, the algorithm to compute the p-value for testing the hypotheses in (6) is described here. We name this procedure as Procedure A.

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

$$d_{obs} = d_{obs}(\vec{\boldsymbol{x}}_1, \vec{\boldsymbol{x}}_2) = \left[\sum_{k=1}^{\mathcal{K}}\sum_{j=1}^{\mathcal{J}} (\boldsymbol{x}_{1,k} - \boldsymbol{x}_{2,k})^2\right]^{1/2}.$$

Step A2: Combine the two sets of observed degradation measurements and denote the combined data set as $\vec{\boldsymbol{x}}_C = (\vec{\boldsymbol{x}}_1, \vec{\boldsymbol{x}}_2)$. Based on the Wiener process model in Eq. (1), obtain the MLE of $\boldsymbol{\theta} = (\boldsymbol{\mu}, \boldsymbol{\Sigma})$ by maximizing the log-likelihood function $\ln L(\boldsymbol{\theta}, \vec{\boldsymbol{x}}_C)$ in Eq. (5) with respect to $\boldsymbol{\theta}$. The MLE of $\boldsymbol{\theta}$ based on the combined data set under H_0 in (6) is denoted by $\hat{\boldsymbol{\theta}}_C = (\hat{\boldsymbol{\mu}}_C, \hat{\boldsymbol{\Sigma}}_C)$.

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

Step A4: Compute the Euclidean distance between the two parametric bootstrap samples $\vec{\boldsymbol{x}}^{(1)}_1$ and $\vec{\boldsymbol{x}}^{(1)}_2$ as

$$d^{(1)} = d^{(1)}(\vec{\boldsymbol{x}}^{(1)}_1, \vec{\boldsymbol{x}}^{(1)}_2) = \left[\sum_{k=1}^{\mathcal{K}}\sum_{j=1}^{\mathcal{J}} (\boldsymbol{x}^{(1)}_{1,k} - \boldsymbol{x}^{(1)}_{2,k})^2\right]^{1/2}.$$

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

Step A6: The p-value of the test is computed as

$$p_A = \frac{1}{B}\sum_{b=1}^{B} 1_{\{d_{obs} > d^{(b)}\}},$$

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 (6) is rejected if $p_A < \alpha$, where α 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.

3.2.2. *TEST PROCEDURES BASED ON LIKELIHOOD RATIO TEST STATISTIC*

Under the Wiener process model described in Section 3.1, the hypotheses in (6) can be expressed as

$$\begin{aligned} H_0: &\quad \boldsymbol{\mu}_1 = \boldsymbol{\mu}_2 = \boldsymbol{\mu} \text{ and } \boldsymbol{\Sigma}_1 = \boldsymbol{\Sigma}_2 = \boldsymbol{\Sigma} \\ \text{against } H_1: &\quad \boldsymbol{\mu}_1 \neq \boldsymbol{\mu}_2 \text{ or } \boldsymbol{\Sigma}_1 \neq \boldsymbol{\Sigma}_2. \end{aligned} \tag{7}$$

Let $\hat{\boldsymbol{\theta}}_i = (\hat{\boldsymbol{\mu}}_i, \hat{\boldsymbol{\Sigma}}_i)$ be the MLE of the $\boldsymbol{\theta}_i$ that maximizes the log-likelihood function $\ln L(\boldsymbol{\theta}_i, \vec{\boldsymbol{x}}_i)$ in Eq. (5) with respect to $\boldsymbol{\theta}_i$ based on the data $\vec{\boldsymbol{x}}_i$, i.e.,

$$\hat{\boldsymbol{\theta}}_i = \arg\max_{\boldsymbol{\theta}_i} \ln L(\boldsymbol{\theta}_i, \vec{\boldsymbol{x}}_i), \tag{8}$$

for $i = 1, 2$. Similarly, based on the combined data set $\vec{\boldsymbol{x}}_C = (\vec{\boldsymbol{x}}_1, \vec{\boldsymbol{x}}_2)$, the MLE of $\boldsymbol{\theta_C} = (\boldsymbol{\mu}_C, \boldsymbol{\Sigma}_C)$ that maximizes the log-likelihood function $\ln L(\boldsymbol{\theta}_C, \vec{\boldsymbol{x}}_C)$ in Eq. (5) with respect to $\boldsymbol{\theta}_C$ under H_0 in (7) is denoted as $\hat{\boldsymbol{\theta}}_C$, i.e.,

$$\hat{\boldsymbol{\theta}}_C = \arg\max_{\boldsymbol{\theta}_C} \ln L\left(\boldsymbol{\theta}_C, \overrightarrow{\boldsymbol{x}_C}\right). \tag{9}$$

The likelihood ratio test statistic based on $\vec{\boldsymbol{x}}_1$ and $\vec{\boldsymbol{x}}_2$ is defined as

$$\Lambda\left(\overrightarrow{\boldsymbol{x}_1}, \overrightarrow{\boldsymbol{x}_2}\right) = -2 \ln \left[\frac{L\left(\hat{\boldsymbol{\theta}}_C, \overrightarrow{\boldsymbol{x}_C}\right)}{L\left(\hat{\boldsymbol{\theta}}_1, \overrightarrow{\boldsymbol{x}_1}\right) \times L\left(\hat{\boldsymbol{\theta}}_2, \overrightarrow{\boldsymbol{x}_2}\right)} \right]. \tag{10}$$

The Neyman–Pearson lemma states that the likelihood ratio test is the most powerful test at significance level α. As the sample size approaches ∞, the test statistic $\Lambda(\vec{\boldsymbol{x}}_1, \vec{\boldsymbol{x}}_2)$ is asymptotically chi-squared distribution with degrees of freedom $q = \mathcal{J} + \mathcal{J}(\mathcal{J}+1)/2$. Two statistical hypothesis test procedures, namely Procedure B1 and Procedure B2, are developed here based on the likelihood ratio test statistic in Eq. (10). The p-value of Procedure B1 is obtained based on the asymptotic distribution of the likelihood ratio test statistic $\Lambda(\vec{\boldsymbol{x}}_1, \vec{\boldsymbol{x}}_2)$, while the p-value of Procedure B2 is obtained based on resampling technique.

Based on the observed degradation measurements $\vec{\boldsymbol{x}}_1 = \{\boldsymbol{x}_{1,1}, \boldsymbol{x}_{1,2}, \cdots, \boldsymbol{x}_{1,\mathcal{K}}\}$ and $\vec{\boldsymbol{x}}_2 = \{\boldsymbol{x}_{2,1}, \boldsymbol{x}_{2,2}, \cdots, \boldsymbol{x}_{2,\mathcal{K}}\}$ 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 $\boldsymbol{\theta}_i = (\boldsymbol{\mu}_i, \boldsymbol{\Sigma}_i)$ from $\vec{\boldsymbol{x}}_i$, $i = 1, 2$ based on Eq. (8).

Step B2: Combine the two sets of observed degradation measurements $\vec{\boldsymbol{x}}_C = (\vec{\boldsymbol{x}}_1, \vec{\boldsymbol{x}}_2)$ and obtain the MLE of $\boldsymbol{\theta}_C = (\boldsymbol{\mu}_C, \boldsymbol{\Sigma}_C)$ from $\vec{\boldsymbol{x}}_C$ based on Eq. (9).

Step B3: Compute the likelihood ratio test statistic $\Lambda_{obs} = \Lambda(\vec{\boldsymbol{x}}_1, \vec{\boldsymbol{x}}_2)$ from Eq. (10).

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

$$p_{B1} = \Pr(W < \Lambda_{obs})$$

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

Step B5: Generate $\boldsymbol{x}_{1,k}^{(1)}$ and $\boldsymbol{x}_{2,k}^{(1)}$ from a $\mathcal{J}$-dimensional multivariate normal distribution $\mathcal{N}_{\mathcal{J}}(\hat{\boldsymbol{\mu}}_C, \hat{\boldsymbol{\Sigma}}_C)$, for $k = 1, 2, \ldots, \mathcal{K}$, to obtain the parametric bootstrap samples $\vec{\boldsymbol{x}}_1^{(1)} = \{\boldsymbol{x}_{1,1}^{(1)}, \boldsymbol{x}_{1,2}^{(1)}, \ldots, \boldsymbol{x}_{1,\mathcal{K}}^{(1)}\}$ and $\vec{\boldsymbol{x}}_2^{(1)} = \{\boldsymbol{x}_{2,1}^{(1)}, \boldsymbol{x}_{2,2}^{(1)}, \ldots, \boldsymbol{x}_{2,\mathcal{K}}^{(1)}\}$, respectively.

Step B6: Compute the likelihood ratio test statistic based on the two parametric bootstrap samples as $\Lambda^{(1)} = \Lambda(\vec{\boldsymbol{x}}_1^{(1)}, \vec{\boldsymbol{x}}_2^{(1)})$ from Eq. (10).

Step B7: Repeat Steps B4'–B5' B times to obtain a sequence of bootstrap likelihood ratio test statistics, $\Lambda^{(b)} = \Lambda(\vec{\boldsymbol{x}}_1^{(b)}, \vec{\boldsymbol{x}}_2^{(b)})$, for $b = 1, 2, \ldots, B$.

Step B8: For Procedure B2, the p-value is computed as

$$p_{B2} = \frac{1}{B} \sum_{b=1}^{B} 1_{\{\Lambda_{obs} < \Lambda^{(b)}\}}.$$

The null hypothesis in (7) is rejected if $p_{B1} < \alpha$ for Procedure B1, and if $p_{B2} < \alpha$ for Procedure B2, where α is a prefixed significant level.

4. PRACTICAL DATA ANALYSIS

In this section, we illustrate the proposed model and methods by analyzing two real network data sets for P2P service and email systems, which are two kinds of cyber systems that requires cybersecurity insurance. The background of the network data sets is presented in Section 4.1.1 and Section 4.2.1, and the results and discussions of the data analysis are presented in Section 4.1.2 and Section 4.2.2.

We also provide an illustration of actuarial applications of the proposed methodologies based on the P2P networks in Section 4.1.3.

4.1. PEER-TO-PEER NETWORK

4.1.1. *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 (PYMNTS 2020). 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 (Gao et al. 2005; Chandra, Srivastava, and Theng 2010; Kalinic et al. 2019; Lara-Rubio, Villarejo-Ramos, and Liébana-Cabanillas 2020) 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 (M. Ripeanu 2001). 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

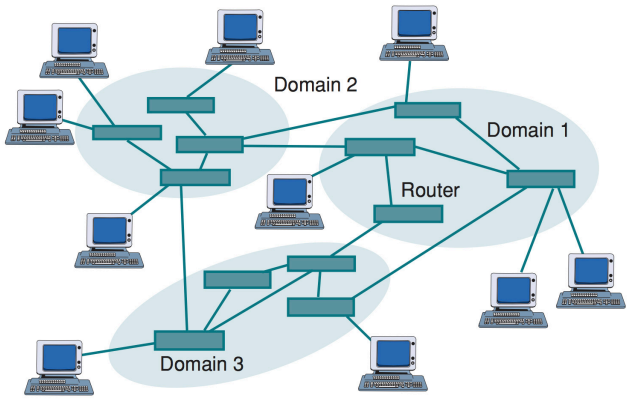

Figure 2. A synopsis of the network structure of a P2P system.

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 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) (Leskovec, Kleinberg, and Faloutsos 2007; Matei Matei Ripeanu and Foster 2002). For notation convenience, we denote the Gnutella networks collected on August 4, 6, and 9, 2002 as P2P network by $\mathbf{G}_1$, $\mathbf{G}_2$, and $\mathbf{G}_3$, respectively.

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 1.

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.

4.1.2. 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 1 in terms of the robustness and the risk of the cyber networks. The topological features for measuring the risks of the networks are the 4-node network motifs M_1, M_2, and M_3 presented in Figure 1. 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 shows the dynamics of the degradation (in percentages) of the three 4-node motifs under degree-based attacks with $\mathcal{K} = 11$ observation points (including the initial status).

Following the notation defined in Section 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 $\mathbf{G}_i$ $(i = 1, 2, 3)$, and $\boldsymbol{x}_{i,k} = (x_{i,1,k}, x_{i,2,k}, x_{i,3,k})' \in \mathbb{R}^3$ 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 $\boldsymbol{\mu}_i$ and variance-covariance $\boldsymbol{\Sigma}_i$.

For the Gnutella computer networks, the MLEs of the drift parameter $\boldsymbol{\mu}_i = (\mu_{i1}, \mu_{i2}, \mu_{i3})'$ and the diffusion coefficient $\boldsymbol{\Sigma_i} = (\sigma_{i,jj'})_{j,j'=1,2,3}$ for networks $\mathbf{G}_i$ and $\mathbf{G}_{\text{Enron},i}$, $i = 1, 2, 3$ under degree-based attack are presented in Table 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 $\{\mathbf{G}_1, \mathbf{G}_2, \mathbf{G}_3\}$ are presented in Tables 3. The number of bootstrap samples used in Procedure A and Procedure B2 is $B = 500$.

Considering statistical significance at 5% level and compensating for multiple comparisons by using the Bonferroni correction (Bonferroni 1936), the p-values presented in Table 3 that are smaller than $0.05/3 \approx 0.01667$ are highlighted in bold to indicate the cases that the null hypothesis in (6) is rejected. From Table 3, we can see that all the three proposed testing procedures (Procedures A, B1, and B2) show that networks $\mathbf{G}_1$ and $\mathbf{G}_3$ are different in the resilience/risk levels, while networks $\mathbf{G}_1$ and $\mathbf{G}_2$ have no significant difference in the resilience/risk levels at the overall 5% significance level. For the comparison between net-

Table 1. Basic network structure information of the three Gnutella computer networks.

Gnutella Computer Network	Collected on	# of nodes	# of edges
$\mathbf{G}_1$	August 4, 2002	10,876	39,994
$\mathbf{G}_2$	August 6, 2002	8,717	31,525
$\mathbf{G}_3$	August 9, 2002	8,114	26,013

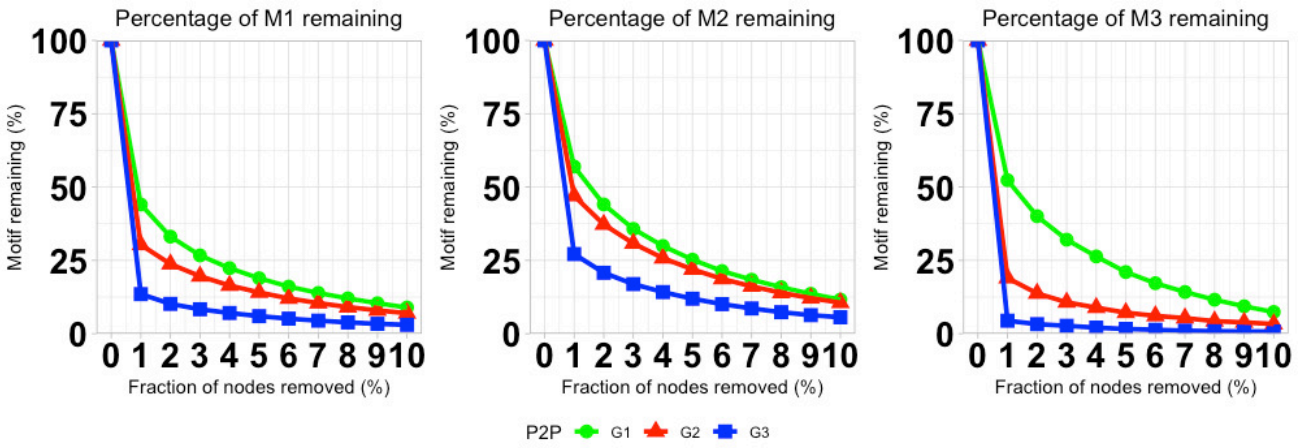

Figure 3. The dynamics of the degradation (in percentages) of the three 4-node motifs of the three networks $\mathrm{G}_1, \mathrm{G}_2$, and G_3 under degree-based attacks with $\mathcal{K} = 11$ observation points.

Table 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.

	$\hat{\mu} = (\hat{\mu}_1, \hat{\mu}_2, \hat{\mu}_3)'$			
Network	$\hat{\mu}_1$	$\hat{\mu}_2$	$\hat{\mu}_3$	$\hat{\mathbf{\Sigma}}$
$\mathbf{G}_1$	0.2415	0.2153	0.2603	$\begin{bmatrix} 0.0388 & 0.0118 & 0.0128 \\ & 0.0144 & 0.0078 \\ & & 0.0171 \end{bmatrix}$
$\mathbf{G}_2$	0.2660	0.2247	0.3408	$\begin{bmatrix} 0.0966 & 0.0278 & 0.0690 \\ & 0.0320 & 0.0397 \\ & & 0.1971 \end{bmatrix}$
$\mathbf{G}_3$	0.3497	0.2881	0.4915	$\begin{bmatrix} 0.3395 & 0.1045 & 0.2697 \\ & 0.1288 & 0.1661 \\ & & 0.8570 \end{bmatrix}$

Table 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 $\mathrm{G}_1, \mathrm{G}_2$, and G_3.

Test	d_{obs}	Λ_{obs}	Procedure A	Procedure B1	Procedure B2
$\mathbf{G}_1$ vs. $\mathbf{G}_2$	1.1122	16.1882	0.0235	**0.0127**	**0.0102**
$\mathbf{G}_1$ vs. $\mathbf{G}_3$	2.8482	44.6146	< **0.001**	< **0.001**	< **0.001**
$\mathbf{G}_2$ vs. $\mathbf{G}_3$	1.7662	12.1299	0.0682	0.0591	0.0553

works $\mathbf{G}_1$ and $\mathbf{G}_2$, 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 $\mathbf{G}_1$ and $\mathbf{G}_2$ are different in terms of the resilience/risk levels.

From the estimates of the drift parameters presented in Table 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 $\mathbf{G}_1$ drops slower than networks $\mathbf{G}_2$ and network $\mathbf{G}_3$ 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 $\mathbf{G}_1$ is the most reliable network among the three networks while networks $\mathbf{G}_2$ and $\mathbf{G}_3$ have similar risk levels. These conclusions agree with the observations obtained by looking at the graphs in Figure 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 $\mathbf{G}_1$ should be lower than the premiums for networks $\mathbf{G}_2$ and $\mathbf{G}_3$ after adjusting for the sizes of those networks and other factors. In the next subsection, we construct concrete scenarios to illustrate how the proposed methodologies can be used to qualify the financial loss due to attack.

4.1.3. *ACTUARIAL APPLICATIONS*

In order to help the readers to understand how the proposed model and methods can be used in actuarial science to determine the premium for cybersecurity insurance, we construct several synthetic scenarios to illustrate the effectiveness of our proposed procedures and the role of network motifs on the resilience aspects of financial networks. Suppose each network $\mathbf{G}_i$ $(i = 1, 2, 3)$ described in Section 4.1.1 corresponds to a company providing P2P financial services and losing a network motif in the P2P network (i.e., a higher-order subgraph in the network) due to cyber-attack translates into a monetary loss to the company. For illustrative purposes, we simplify the problem by considering that the premium of cybersecurity insurance is determined based on (i) the size of the P2P network (the larger the network, the higher the premium); (ii) the cost of losing a network motif in the P2P network (the higher the cost of losing a network motif, the higher the premium); and (iii) the resilience/risk of the P2P network (the higher the risk, the higher the premium).

For the size of the P2P network, we assume that the premium is proportional to the number of nodes in the network. We further assume that the 4-node motifs M_1, M_2, and M_3 carry the same weight, but the cost incurred by losing a motif in the P2P network, which can be viewed as a group of customers and transactions, can be different for the three companies. We denote the cost of losing a motif in the P2P network for company with network $\mathbf{G}_i$ as $\mathcal{C}_i$, $i = 1, 2, 3$.

For the case that there is no information on the resilience/risk levels of the three P2P networks, if the premium for company with network $\mathbf{G}_3$ with 8114 nodes is $\$P_3$, then the premium for company with network $\mathbf{G}_1$ with 10876 nodes can be determined as

$$\$P_1 = \$P_3 \times \left(\frac{10876}{8114}\right)\left(\frac{\mathcal{C}_1}{\mathcal{C}_3}\right),$$

and the premium for company with network $\mathbf{G}_2$ with 8717 nodes can be determined as

$$\$P_2 = \$P_3 \times \left(\frac{8717}{8114}\right)\left(\frac{\mathcal{C}_2}{\mathcal{C}_3}\right).$$

Here, the values $(10876/8114)$ and $(8717/8114)$ can be viewed as the factor adjusted for the size of the network, and the values $(\mathcal{C}_1/\mathcal{C}_3)$ and $(\mathcal{C}_2/\mathcal{C}_3)$ can be viewed as the factor adjusted for the cost of losing a network motif in the P2P network.

The methodologies proposed in this paper can provide information on the resilience/risk levels of the three P2P networks by comparing the resilience/risk of these networks statistically which will lead to a more realistic approach to determining the premium of cybersecurity insurance. Specifically, based on the proposed model and methods, the results suggest that network $\mathbf{G}_1$ is significantly more reliable than networks $\mathbf{G}_2$ and $\mathbf{G}_3$, and there is no significant difference between the risk levels of networks $\mathbf{G}_2$ and $\mathbf{G}_3$. Based on this information, we can conclude that the premium for the company with network $\mathbf{G}_1$ should be

$$\$P_1 < \$P_3 \times \left(\frac{10876}{8114}\right)\left(\frac{\mathcal{C}_1}{\mathcal{C}_3}\right).$$

To obtain a factor that adjusted for the resilience/risk of the P2P network, based on the proposed methodologies in this paper, one possible way is to utilize the estimates from Table 2 by incorporating the decay rates. For example, from Table 2, we can obtain the average decay rate (i.e., average drift parameters), $\bar{\mu} = (\hat{\mu}_1 + \hat{\mu}_2 + \hat{\mu}_3)/3$, for companies with networks $\mathbf{G}_1$ and $\mathbf{G}_3$ as $\bar{\mu}^{(1)} = 0.23903$ and $\bar{\mu}^{(3)} = 0.3764$, respectively. Then, we can consider the factor $(\bar{\mu}^{(1)}/\bar{\mu}^{(3)})$ to adjust the premium for company with network $\mathbf{G}_1$ relative to the premium for company with network $\mathbf{G}_3$. Note that other functions based on the estimates of the proposed modified Wiener process model can be used to construct a reasonable factor here.

The illustration here shows that the network motifs and our proposed statistical procedures can be applied in actuarial science with some reasonable explanations. In real practical applications of determining insurance premium, other factors that are relevant to cybersecurity insurance premium such as the country of the company providing P2P financial services registered in, losses covered/excluded by the insurance policy, security measures of the company, etc., should be considered (Romanosky et al. 2019).

4.2. ENRON EMAIL NETWORK

4.2.1. *BACKGROUND OF ENRON EMAIL NETWORK*

In the past few years, business email compromise (BEC) becomes one of the top cyber threats. According to the report from (American International Group (AIG) 2019), 23% of its 2018 cyber insurance claims in Europe, Middle East, and Africa (EMEA) region were BEC related. In this example, we consider the Enron email network data collected by the Cognitive Agent that Learns and Organizes (CALO) Project (Klimt and Yang 2004) which consists of more than half a million emails with 150 users sent over the period from May 1999 to July 2001. A node in the Enron email network represents an email address and an edge represents communication between two email addresses, i.e., there exists an edge between node i and node j if at least one email was sent in between email address i and email address j. We define the Enron email network as an undirected graph $\mathbf{G}_{\text{Enron}} = (V_{\text{Enron}}, E_{\text{Enron}})$, where V_{Enron} is a finite set of $|V_{\text{Enron}}| = 36,692$ email addresses and E_{Enron} is a set of edges (i.e., emails) with $|E_{\text{Enron}}| = 367,662$. A snapshot of the Enron email network is presented in Figure 4.

In order to illustrate our proposed methodologies for evaluating the cybersecurity risk of the Enron email network, we generate three representative subgraphs by sampling $3,000$ nodes from the original Enron email network, i.e., randomly select $3,000$ nodes from the node set V_{Enron}. The numbers of nodes and the numbers of edges of these three subgraphs are presented in Table 4. Furthermore, due to the fact that the email addresses would be different at different time points, we assume that the sampled subgraphs are independent of each other. In a practical application to cybersecurity insurance pricing, we can consider three different companies with the email networks in Table

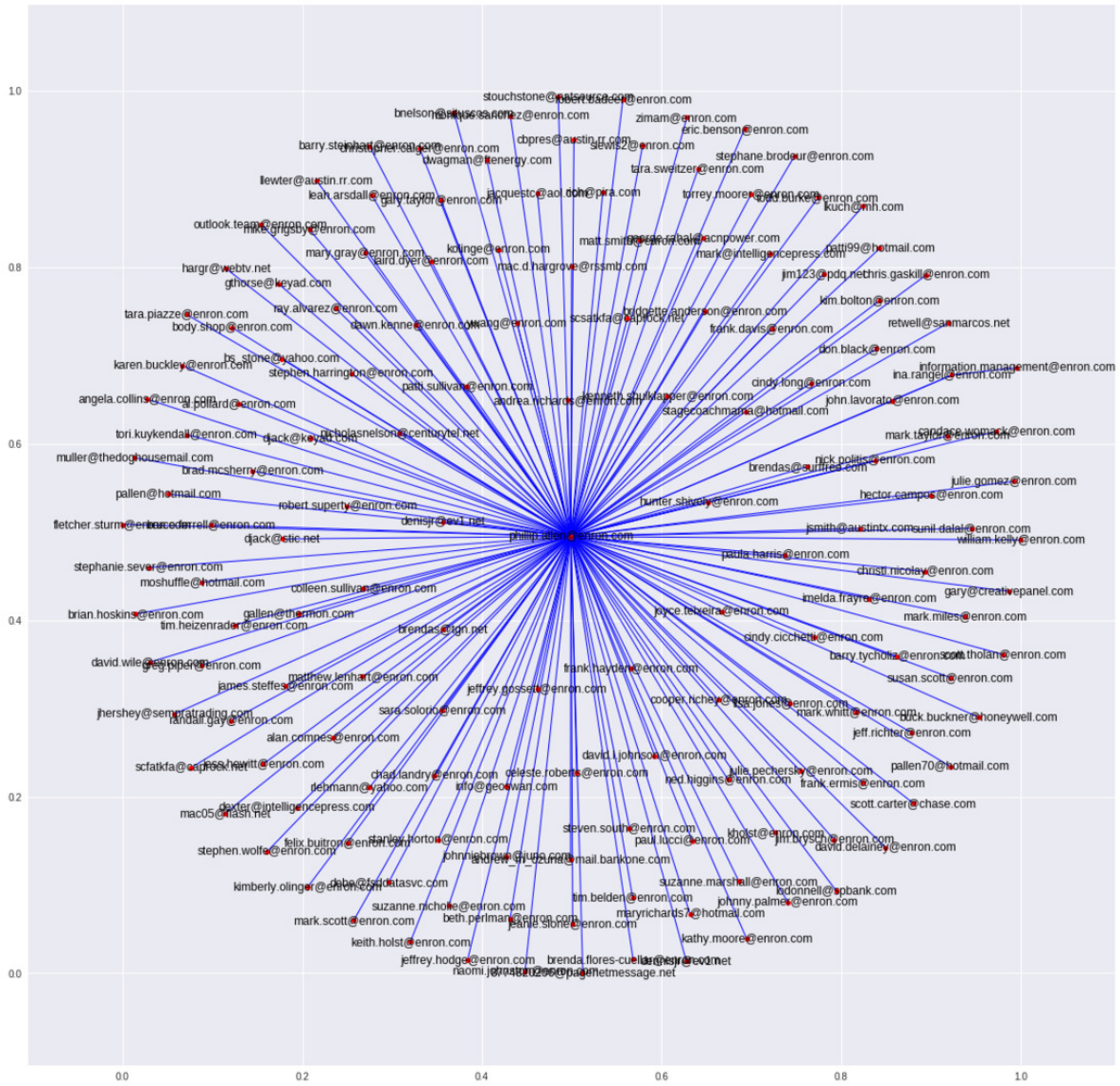

Figure 4. A snapshot of the Enron email network, where the red nodes represent email addresses and the edge is the email communication between two email addresses.

Table 4. Numbers of nodes and number of edges of three sampling subgraphs from the Enron email network.

Subgraph from Enron Email Network	# of nodes	# of edges
$\mathbf{G}_{\text{Enron},1}$	3,000	2,462
$\mathbf{G}_{\text{Enron},2}$	3,000	2,820
$\mathbf{G}_{\text{Enron},3}$	3,000	2,764

4 plan to insure their email networks and the insurance company needs to evaluate and compare the risks of these three email networks.

4.2.2. ENRON EMAIL NETWORK SECURITY LEVEL EVALUATION UNDER DEGREE-BASED ATTACK

In the evaluation and comparisons of the risks of the three email networks in Table 4, we consider the dynamics of three 4-node motif normalized concentrations (i.e., M_1, M_2, and M_3) under degree-based attack. The dynamics of the motifs M_1, M_2, and M_3 under degree-based attack for the three subgraphs $\mathbf{G}_{\text{Enron},1}$, $\mathbf{G}_{\text{Enron},2}$, and $\mathbf{G}_{\text{Enron},3}$ are presented in Figure 5.

For the three subgraphs sampled from the Enron email network, the MLEs of the drift parameter $\boldsymbol{\mu}_i = (\mu_{i1}, \mu_{i2}, \mu_{i3})'$ and the diffusion coefficient $\boldsymbol{\Sigma}_{\boldsymbol{i}} = (\sigma_{i,jj'})_{j,j'=1,2,3}$ for networks $\mathbf{G}_i$ and $\mathbf{G}_{\text{Enron},i}$, $i = 1, 2, 3$ under degree-based attack are presented in Table 5, where $j, j' = 1, 2, 3$ corresponding to the three 4-node motifs M_1, M_2, and M_3, respectively. From Table 5, the estimates of

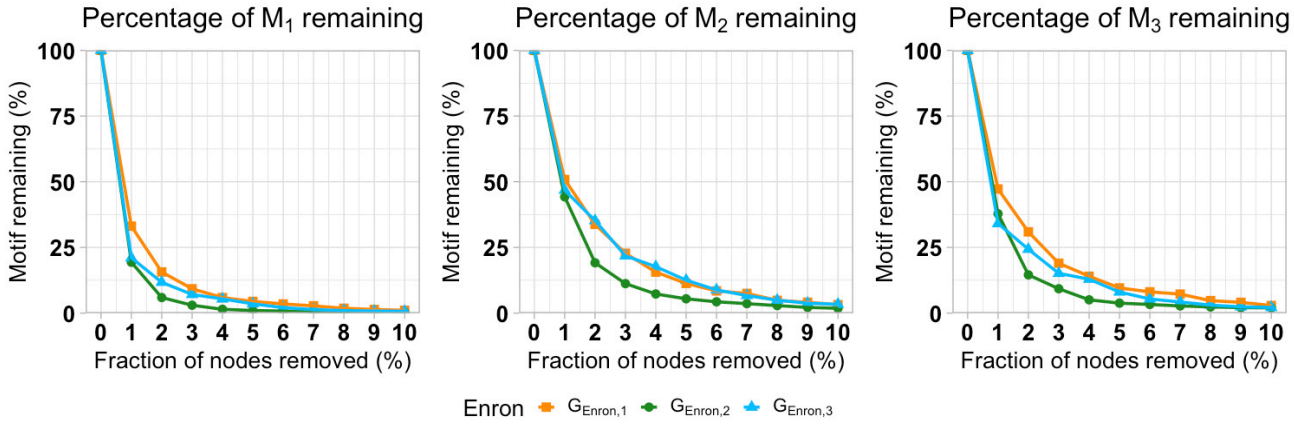

Figure 5. The dynamics of the degradation (in percentages) of the three 4-node motifs of the three networks $\mathrm{G}_{\mathrm{Enron},1}$, $\mathrm{G}_{\mathrm{Enron},2}$, and $\mathrm{G}_{\mathrm{Enron},3}$ under degree-based attacks with $\mathcal{K} = 11$ observations points.

the drift parameters, $\hat{\boldsymbol{\mu}}$, are consistent with the observations from the 4-node motif degradation curves presented in Figure 5. Specifically, except for motif M_2, the functionalities of networks $\mathbf{G}_{\mathrm{Enron},2}$ and $\mathbf{G}_{\mathrm{Enron},3}$ in terms of motifs decline more quickly than than the network $\mathbf{G}_{\mathrm{Enron},1}$ as the fraction of nodes were removed. This suggests that the vanishing rates of the motifs are reflecting the robustness (security level) of the email networks. In general, the smaller the values of $\hat{\mu}_{ij}$, the higher the security level of the email network.

For the three Enron email networks, 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 $\{\mathbf{G}_1, \mathbf{G}_2, \mathbf{G}_3\}$ are presented in Tables 6. The number of bootstrap samples used in Procedure A and Procedure B2 is $B = 500$. In the analysis of the Enron networks, similar to the analysis of the Gnutella computer networks in Section 4.1.2, we utilize the Bonferroni correction for multiple comparisons, i.e., we can reject the null hypothesis if the corresponding p-value is less than 0.01667 (highlighted in bold in Table 6). From Table 6, the results of the analysis based on the proposed methodologies suggest that networks $\mathbf{G}_{\mathrm{Enron},1}$ and $\mathbf{G}_{\mathrm{Enron},2}$ have different security levels, $\mathbf{G}_{\mathrm{Enron},2}$ and $\mathbf{G}_{\mathrm{Enron},3}$ have different security levels, and networks $\mathbf{G}_{\mathrm{Enron},1}$ and $\mathbf{G}_{\mathrm{Enron},3}$ have similar security levels. Since the smaller the values of $\hat{\mu}_{ij}$, the higher the security level of the email network, based on the estimates from Table 5, we can conclude that $\mathbf{G}_{\mathrm{Enron},1}$ and $\mathbf{G}_{\mathrm{Enron},3}$ are more robust than $G_{\mathrm{Enron},2}$ under the degree-based attacks. These conclusions agree with the observations obtained by looking at the graphs in Figure 5. Based on the results in this analysis, for insurance pricing, the premium for insuring networks $\mathbf{G}_{\mathrm{Enron},1}$ and $\mathbf{G}_{\mathrm{Enron},3}$ should be similar, while the premium for insuring network $\mathbf{G}_{\mathrm{Enron},2}$ should be higher than $\mathbf{G}_{\mathrm{Enron},1}$ and $\mathbf{G}_{\mathrm{Enron},3}$.

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 5.1; (ii) a simulation study without relying on generating data from a parametric model in Section 5.2; (iii) a sensitivity analysis to evaluate the robustness of the proposed methodologies in Section 5.3. 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.

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 Eq. (1). In this simulation, we assume that there are three different topological features for measuring the risks of two cyber-networks (i.e., $\mathcal{J} = 3$ and $\mathcal{I} = 2$) and these three topological features are observed at $\mathcal{K} = 11$ time points. We are interested in testing the hypotheses in Eq. (6). The topological features for Network 1 and Network 2 in Eq. (6) are simulated from the Wiener process model in Eq. (1) with the following parameter settings based on the networks $\mathbf{G}_1$ and $\mathbf{G}_2$ in the numerical example presented in Section 4:

- Network 1:

$$\boldsymbol{\theta}_1 = (\boldsymbol{\mu}_1, \boldsymbol{\Sigma}_1) \qquad \boldsymbol{\mu}_1 = \begin{pmatrix} 0.2660 \\ 0.2247 \\ 0.3408 \end{pmatrix} \quad \text{and}$$

$$\boldsymbol{\Sigma}_1 = \begin{pmatrix} 0.0388 & 0.0118 & 0.0128 \\ & 0.0144 & 0.0078 \\ & & 0.0171 \end{pmatrix};$$

$$\boldsymbol{\theta}_1 = (\boldsymbol{\mu}_1, \boldsymbol{\Sigma}_1) \qquad \boldsymbol{\mu}_1 = \begin{pmatrix} 0.2415 \\ 0.2153 \\ 0.2603 \end{pmatrix} \quad \text{and}$$

$$\boldsymbol{\Sigma}_1 = \begin{pmatrix} 0.0966 & 0.0278 & 0.0690 \\ & 0.0320 & 0.0397 \\ & & 0.1971 \end{pmatrix}.$$

- Network 2:

Table 5. Maximum likelihood estimates of the drift parameters and the diffusion coefficients in the Wiener process model for $\mathbf{G}_{\text{Enron, 1}}$, $\mathbf{G}_{Enron,2}$, and $\mathbf{G}_{Enron,3}$ under degree-based attack.

	$\hat{\mu} = (\hat{\mu}_1, \hat{\mu}_2, \hat{\mu}_3)'$			
Network	$\hat{\mu}_1$	$\hat{\mu}_2$	$\hat{\mu}_3$	$\hat{\mathbf{\Sigma}}$
$\mathbf{G}_{\text{Enron},1}$	0.4537	0.3446	0.3549	$\begin{bmatrix} 0.0715 & 0.0350 & 0.0411 \\ & 0.0223 & 0.0251 \\ & & 0.0326 \end{bmatrix}$
$\mathbf{G}_{\text{Enron},2}$	0.5822	0.4005	0.3921	$\begin{bmatrix} 0.2171 & 0.1065 & 0.1475 \\ & 0.0567 & 0.0753 \\ & & 0.1070 \end{bmatrix}$
$\mathbf{G}_{\text{Enron},3}$	0.4968	0.3394	0.3838	$\begin{bmatrix} 0.1461 & 0.0593 & 0.0950 \\ & 0.0281 & 0.0426 \\ & & 0.0679 \end{bmatrix}$

Table 6. 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 $\mathrm{G}_{\text{Enron},1}$, $\mathrm{G}_{\text{Enron },2}$, and $\mathrm{G}_{\text{Enron},3}$.

Test	d_{obs}	Λ_{obs}	Procedure A	Procedure B1	Procedure B2
$\mathbf{G}_{\text{Enron},1}$ vs. $\mathbf{G}_{\text{Enron},2}$	0.3904	36.9012	**0.0020**	$<$ **0.001**	$<$ **0.001**
$\mathbf{G}_{\text{Enron},1}$ vs. $\mathbf{G}_{\text{Enron},3}$	0.2135	47.1325	0.9610	0.8717	0.8150
$\mathbf{G}_{\text{Enron},2}$ vs. $\mathbf{G}_{\text{Enron},3}$	0.2969	45.8706	$<$ **0.001**	$<$ **0.001**	$<$ **0.001**

$\boldsymbol{\theta}_2 = (a \times \boldsymbol{\mu}_1, \boldsymbol{\Sigma}_1)$, where $a = \{0.05, 0.2, 0.4, 0.6, 0.8, 1.0, 1.2, 1.4, 1.6, 1.8, 2.0, 4.0\}$;
$\boldsymbol{\theta}_2 = (\boldsymbol{\mu}_1, a \times \boldsymbol{\Sigma}_1)$, where $a = \{0.8, 0.6, 0.4, 0.2, 0.05, 1.2, 1.4, 1.6, 1.8, 2.0, 4.0\}$;
$\boldsymbol{\theta}_2 = (a' + \boldsymbol{\mu}_1, \boldsymbol{\Sigma}_1)$, 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 (6) at 5% level of significance) are presented in Table 7. 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 7, 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.

5.2. NETWORK DATA GENERATED FROM NONPARAMETRIC RESAMPLING OF A REAL NETWORK DATA SET

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 4. Based on the analysis of Gnutella P2P network data set presented in Section 4, we observed that there is a significant difference between networks $\mathbf{G}_1$ and $\mathbf{G}_3$ (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 $\mathbf{G}_1$ and $\mathbf{G}_3$ using the breadth-first search (BFS) method (Cormen et al. 2009) 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

Table 7. Simulated rejection rates for network data generated from the Wiener process model

	Network 1	1(a) Procedure			1(b) Procedure		
Network 2	a/a'	A	B1	B2	A	B1	B2
2(a): $\boldsymbol{\theta}_2 = (a \times \hat{\boldsymbol{\mu}}_1, \hat{\boldsymbol{\Sigma}}_1)$	0.05	0.310	0.417	0.306	0.357	0.384	0.358
	0.20	0.160	0.183	0.155	0.168	0.170	0.165
	0.40	0.122	0.166	0.136	0.125	0.130	0.121
	0.60	0.082	0.120	0.105	0.081	0.095	0.079
	0.80	0.055	0.076	0.063	0.060	0.075	0.062
	1.00	0.046	0.072	0.055	0.047	0.046	0.051
	1.20	0.058	0.094	0.059	0.119	0.150	0.123
	1.40	0.068	0.126	0.072	0.231	0.240	0.228
	1.60	0.112	0.208	0.131	0.277	0.325	0.280
	1.80	0.148	0.270	0.150	0.308	0.375	0.316
	2.00	0.272	0.366	0.233	0.490	0.510	0.479
	4.00	0.999	0.999	0.998	1.000	1.000	1.000
2(b): $\boldsymbol{\theta}_2 = (\hat{\boldsymbol{\mu}}_1, a \times \hat{\boldsymbol{\Sigma}}_1)$	0.05	0.750	0.798	0.757	1.000	1.000	1.000
	0.20	0.699	0.734	0.710	0.827	0.858	0.833
	0.40	0.231	0.434	0.240	0.201	0.410	0.218
	0.60	0.097	0.196	0.100	0.147	0.240	0.156
	0.80	0.050	0.116	0.061	0.107	0.150	0.101
	1.00	0.046	0.072	0.055	0.047	0.046	0.051
	1.20	0.045	0.094	0.066	0.130	0.180	0.147
	1.40	0.066	0.124	0.079	0.147	0.194	0.151
	1.60	0.098	0.176	0.121	0.179	0.250	0.209
	1.80	0.155	0.268	0.180	0.269	0.366	0.299
	2.00	0.161	0.282	0.194	0.283	0.378	0.316
	4.00	0.716	0.802	0.711	0.753	0.770	0.766
2(c): $\boldsymbol{\theta}_2 = (a' + \hat{\boldsymbol{\mu}}_1, \hat{\boldsymbol{\Sigma}}_1)$	0.00	0.046	0.072	0.055	0.047	0.046	0.051
	0.05	0.080	0.142	0.110	0.115	0.135	0.113
	0.10	0.249	0.316	0.273	0.238	0.264	0.220
	0.15	0.416	0.438	0.371	0.293	0.336	0.288
	0.20	0.498	0.546	0.515	0.409	0.457	0.432

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 (6). Network 1 and Network 2 in (6) are simulated by resampling the $100\tau\%$ of nodes as follows:

- Network 1: $\mathbf{G}_1$; Network 2: $\mathbf{G}_1$;
- Network 1: $\mathbf{G}_3$; Network 2: $\mathbf{G}_3$;
- Network 1: $\mathbf{G}_1$; Network 2: $\mathbf{G}_3$.

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 8.

From the simulation results in Table 8, we observe that when Network 1 and Network 2 are resampled from $\mathbf{G}_1$ and $\mathbf{G}_3$, respectively, the three proposed test procedures reject the null hypothesis in (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 4, $\mathbf{G}_1$ and $\mathbf{G}_3$ are different in terms of their resilience/risk levels. When the two networks are resampled from the same P2P network (i.e., network $\mathbf{G}_1$ or network $\mathbf{G}_3$), 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 8. 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 $\mathbf{G}_1$ and $\mathbf{G}_3$.

			% of nodes being resampled				
Procedure	Network 1	Network 2	50%	55%	60%	65%	70%
A	$\mathbf{G}_1$	$\mathbf{G}_1$	0.202	0.164	0.075	0.043	0.001
	$\mathbf{G}_3$	$\mathbf{G}_3$	0.152	0.100	0.066	0.040	0.002
	$\mathbf{G}_1$	$\mathbf{G}_3$	0.901	0.950	0.963	0.971	0.999
B1	$\mathbf{G}_1$	$\mathbf{G}_1$	0.220	0.170	0.081	0.056	0.031
	$\mathbf{G}_3$	$\mathbf{G}_3$	0.189	0.129	0.058	0.052	0.029
	$\mathbf{G}_1$	$\mathbf{G}_3$	0.915	0.967	0.978	0.989	0.999
B2	$\mathbf{G}_1$	$\mathbf{G}_1$	0.198	0.165	0.069	0.052	0.035
	$\mathbf{G}_3$	$\mathbf{G}_3$	0.190	0.133	0.070	0.053	0.032
	$\mathbf{G}_1$	$\mathbf{G}_3$	0.910	0.961	0.969	0.983	0.999

5.3. SENSITIVITY ANALYSIS

Since the proposed methodologies rely on the Wiener process model, it is important to investigate the sensitivity of the proposed methods when the underlying data generating mechanism deviates from the proposed Wiener process model. For this reason, in this section, we consider a Monte Carlo simulation study in which the simulated datasets are generated from a gamma process model, which is a commonly used model for degradation data analysis.

Following the notation in Section 3.1, we consider $\mathcal{I} = 2$, $\mathcal{J} = 3$ and $\mathcal{K} = 10$ and generate the $\mathcal{J}$-dimensional random vector $\boldsymbol{x}_{i,k} = (x_{i,1,k}, x_{i,2,k}, \ldots, x_{i,\mathcal{J},k})' \in \mathbb{R}^{\mathcal{J}}$, where $x_{i,j,k} = \log(y_{i,j,k}/y_{i,j,k+1})$, based on a gamma process model in which $x_{i,j,k}$ follows a gamma distribution with shape parameter $\lambda_{i,j} > 0$ and scale parameter $\beta_i > 0$ (denoted as $Gamma(\lambda_{i,j}, \beta_i)$). The probability density function of $x_{i,j,k}$ is

$$g(x_{i,j,k}; \lambda_{i,j}, \beta_i) = \frac{\beta_i^{\lambda_{i,j}}}{\Gamma(\lambda_{i,j})} x_{i,j,k}^{\lambda_{i,j}-1} \exp(-\beta_i x_{i,j,k}), \quad x_{i,j,k} > 0, \tag{11}$$

where $\Gamma(z) = \int_0^\infty x^{z-1}\exp(-x)\,dx$ is the gamma function. For Network i ($i = 1$ and 2), the parameter vector for the gamma process model is $\boldsymbol{\theta}_i = (\lambda_{i,1}, \lambda_{i,2}, \lambda_{i,3}, \beta_i)$. In the simulation study, we consider the following settings for the datasets of Network 1 and Network 2 from the gamma process model:

- Networks 1 and 2 share the same shape parameters but different scale parameter:
  $\boldsymbol{\theta}_1 = (\lambda_{1,1}, \lambda_{1,2}, \lambda_{1,3}, \beta_1)$, where $\lambda_{1,1} = \lambda_{1,2} = \lambda_{1,3} = 0.5$ and $\beta_1 = 0.05$;
  $\boldsymbol{\theta}_2 = (\lambda_{2,1}, \lambda_{2,2}, \lambda_{2,3}, \beta_2)$, where $\lambda_{2,1} = \lambda_{2,2} = \lambda_{2,3} = 0.5$ and $\beta_2 = a \times \beta_1$.
- Networks 1 and 2 share the same scale parameter but different shape parameters:
  $\boldsymbol{\theta}_1 = (\lambda_{1,1}, \lambda_{1,2}, \lambda_{1,3}, \beta_1)$, where $\lambda_{1,1} = \lambda_{1,2} = \lambda_{1,3} = 0.5$ and $\beta_1 = 0.05$;
  $\boldsymbol{\theta}_2 = (\lambda_{2,1}, \lambda_{2,2}, \lambda_{2,3}, \beta_2)$, where $\lambda_{2,1} = \lambda_{2,2} = \lambda_{2,3} = a' + \lambda_{1,i}$ and $\beta_2 = 0.05$.

Based on 1000 simulations with different values of a and a', the simulated rejection rates of Procedures A, B1, and B2 under the proposed modified Wiener process model are presented in Table 9.

From Table 9, we can observe that the three proposed testing procedures, especially Procedure A, under the modified Wiener process model can effectively control the significance levels (i.e., when $a = 1.0$ and $a' = 0.0$) close to the 5% level and provide reasonable power when the two target networks are different in terms of the resilience/risk level even when the underlying data-generating mechanism is not the assumed Wiener process model. Moreover, the power values of these three testing procedures increase with the values of a and a', which indicates that these test procedures can effectively detect the dissimilarity between the two target networks.

6. CONCLUDING REMARKS

To comprehend how vulnerable is a cyber or physical network to attacks or failures and to assess the risks of a complex network, in this paper, we propose a statistical approach to assess and understand cyber risk. Specifically, we propose 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 conduct experiments on the Gnutella P2P cyber network and Enron email datasets. Network motifs, which can capture local topological information of a network, are considered as the topological measure in the example. However, other topological measures that can reflect the functionality of the complex network, including global topological measures (e.g., giant component, degree distribution, APL, D, CC, BC, etc.) and local topological features (e.g., Betti numbers, Wasserstein distances, etc.) (Salles and Marino 2011; Kim and Obah 2007; Islambekov et al. 2018) can also be used with the proposed methodologies in this paper. In the practical data analysis, we observe that the proposed methodologies can qualify and compare the risks of different complex networks. Then, we

Table 9. Simulated rejection rates for Procedures A, B1, and B2 for settings S1 and S2 with different a and a' when the data is is generated from gamma process models

Setting **S1**	$a = 1.0$	$a = 2.0$	$a = 3.0$
Procedure A	0.047	0.201	0.265
Procedure B1	0.058	0.212	0.280
Procedure B2	0.056	0.200	0.277
Setting **S2**	$a' = 0.0$	$a' = 0.1$	$a' = 0.2$
Procedure A	0.047	0.099	0.217
Procedure B1	0.058	0.107	0.239
Procedure B2	0.056	0.100	0.232

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 Weiner process model or resampling from the real Gnutella P2P cyber network data. From the simulation results, we observe 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/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 premium. The computer program to execute the proposed methodologies is written in R (R Core Team 2020) and is available from the authors upon request.

ACKNOWLEDGEMENT

This research was supported by The Society of Actuaries' Committee on Knowledge Extension Research and the Casualty Actuarial Society Individual Grant. The authors would like to thank reviewers in the oversight group of the Casualty Actuarial Society for reviewing our manuscript and for their constructive comments and suggestions. The authors are grateful for the two referees and the editor for their helpful and suggestions that improved the manuscript.

Submitted: June 15, 2021 EDT. Accepted: November 17, 2021 EDT. Published: March 11, 2024 EDT.

REFERENCES

Ackerman, G. 2013. "G-20 Urged to Treat Cyber-Attacks as Threat to Economy." *Bloomberg*, 2013. https://www.bloomberg.com/news/articles/2013-06-13/g-20-urged-to-treat-cyber-attacks-as-threat-to-economy.

Alon, Uri. 2007. "Network Motifs: Theory and Experimental Approaches." *Nature Reviews Genetics* 8 (6): 450–61. https://doi.org/10.1038/nrg2102.

American International Group (AIG). 2019. "Cyber Claims: GDPR and Business Email Compromise Drive Greater Frequencies." *Claims Intelligence Series*, 1–9.

Biener, Christian, Martin Eling, and Jan Hendrik Wirfs. 2014. "Insurability of Cyber Risk: An Empirical Analysis." *The Geneva Papers on Risk and Insurance - Issues and Practice* 40 (1): 131–58. https://doi.org/10.1057/gpp.2014.19.

Böhme, Rainer, Stefan Laube, and Markus Riek. 2019. "A Fundamental Approach to Cyber Risk Analysis." *Variance* 12 (2): 161–85.

Bonferroni, C. E. 1936. "Teoria Statistica delle Classi e Calcolo delle Probabilitá." *Pubblicazioni del R Istituto Superiore di Scienze Economiche e Commerciali di Firenze*.

Chandra, Shalini, Shirish C. Srivastava, and Yin-Leng Theng. 2010. "Evaluating the Role of Trust in Consumer Adoption of Mobile Payment Systems: An Empirical Analysis." *Communications of the Association for Information Systems* 27 (1): 29. https://doi.org/10.17705/1cais.02729.

Chen, Ding-Geng, Yuhlong Lio, Hon Keung Tony Ng, and Tzong-Ru Tsai. 2017. *Statistical Modeling for Degradation Data*. Singapore: Springer.

Cohen, Reuven, Keren Erez, Daniel Ben-Avraham, and Shlomo Havlin. 2000. "Resilience of the Internet to Random Breakdowns." *Physical Review Letters* 85 (21): 4626–28. https://doi.org/10.1103/physrevlett.85.4626.

Cormen, Thomas H, Charles E Leiserson, Ronald L Rivest, and Clifford Stein. 2009. *Introduction to Algorithms*. MIT Press.

Cuadra, Lucas, Sancho Salcedo-Sanz, Javier Del Ser, Silvia Jiménez-Fernández, and Zong Geem. 2015. "A Critical Review of Robustness in Power Grids Using Complex Networks Concepts." *Energies* 8 (9): 9211–65. https://doi.org/10.3390/en8099211.

Department of Homeland Security. 2019. "Cybersecurity Insurance." 2019. https://www.dhs.gov/cisa/cybersecurity-insurance.

Dey, Asim K., Yulia R. Gel, and H. Vincent Poor. 2019. "What Network Motifs Tell Us about Resilience and Reliability of Complex Networks." *Proceedings of the National Academy of Sciences* 116 (39): 19368–73. https://doi.org/10.1073/pnas.1819529116.

Doksum, Kjell A., Arnljot Hóyland, and Arnljot Hoyland. 1992. "Models for Variable-Stress Accelerated Life Testing Experiments Based on Wiener Processes and the Inverse Gaussian Distribution." *Technometrics* 34 (1): 74. https://doi.org/10.2307/1269554.

Ganin, Alexander A, Emanuele Massaro, Alexander Gutfraind, Nicolas Steen, Jeffrey M Keisler, Alexander Kott, Rami Mangoubi, and Igor Linkov. 2016. "Operational Resilience: Concepts, Design and Analysis." *Scientific Reports* 6 (1): 1–12.

Gao, J., K. Edunuru, J. Cai, and S.Ph.D. Shim. 2005. "P2P-Paid: A Peer-to-Peer Wireless Payment System." *Second IEEE International Workshop on Mobile Commerce and Services*, 102–11. https://doi.org/10.1109/wmcs.2005.16.

Havlin, S., D.Y. Kenett, A. Bashan, J. Gao, and H.E. Stanley. 2014. "Vulnerability of Network of Networks." *The European Physical Journal Special Topics* 223 (11): 2087–2106. https://doi.org/10.1140/epjst/e2014-02251-6.

Holland, Paul W., and Samuel Leinhardt. 1970. "A Method for Detecting Structure in Sociometric Data." *American Journal of Sociology* 76 (3): 492–513. https://doi.org/10.1086/224954.

———. 1971. "Transitivity in Structural Models of Small Groups." *Comparative Group Studies* 2 (2): 107–24. https://doi.org/10.1177/104649647100200201.

Islambekov, Umar, Asim Kumer Dey, Yulia R. Gel, and H. Vincent Poor. 2018. "Role of Local Geometry in Robustness of Power Grid Networks." *2018 IEEE Global Conference on Signal and Information Processing (GlobalSIP)*, November, 885–89. https://doi.org/10.1109/globalsip.2018.8646573.

Kalinic, Zoran, Veljko Marinkovic, Sebastián Molinillo, and Francisco Liébana-Cabanillas. 2019. "A Multi-Analytical Approach to Peer-to-Peer Mobile Payment Acceptance Prediction." *Journal of Retailing and Consumer Services* 49 (July):143–53. https://doi.org/10.1016/j.jretconser.2019.03.016.

Kashtan, N., S. Itzkovitz, R. Milo, and U. Alon. 2004. "Efficient Sampling Algorithm for Estimating Subgraph Concentrations and Detecting Network Motifs." *Bioinformatics* 20 (11): 1746–58. https://doi.org/10.1093/bioinformatics/bth163.

Kim, Charles J, and Obinna B Obah. 2007. "Vulnerability Assessment of Power Grid Using Graph Topological Indices." *International Journal of Emerging Electric Power Systems* 8 (6). https://doi.org/10.2202/1553-779x.1738.

Klimt, Bryan, and Yiming Yang. 2004. "Introducing the Enron Corpus." In *Conference on Collaboration, Electronic Messaging, Anti-Abuse and Spam (CEAS)*.

Kotenko, Igor, Igor Saenko, and Oleg Lauta. 2018. "Analytical Modeling and Assessment of Cyber Resilience on the Base of Stochastic Networks Conversion." *2018 10th International Workshop on Resilient Networks Design and Modeling (RNDM)*, August, 1–8. https://doi.org/10.1109/rndm.2018.8489830.

Lara-Rubio, J., A. F. Villarejo-Ramos, and F. Liébana-Cabanillas. 2020. "Explanatory and Predictive Model of the Adoption of P2P Payment Systems." *Behaviour & Information Technology* 40 (6): 528–41. https://doi.org/10.1080/0144929x.2019.1706637.

Leskovec, Jure, Jon Kleinberg, and Christos Faloutsos. 2007. "Graph Evolution." *ACM Transactions on Knowledge Discovery from Data* 1 (1): 2. https://doi.org/10.1145/1217299.1217301.

Lio, Yuhlong, Hon Keung Tony Ng, Tzong-Ru Tsai, and Ding-Geng Chen, eds. 2019. *Statistical Quality Technologies: Theory and Practice*. Springer International Publishing. https://doi.org/10.1007/978-3-030-20709-0.

Maison, Christèle, Delphine Bailly, Antoine H.F.M. Peters, Jean-Pierre Quivy, Danièle Roche, Angela Taddei, Monika Lachner, Thomas Jenuwein, and Geneviève Almouzni. 2002. "Higher-Order Structure in Pericentric Heterochromatin Involves a Distinct Pattern of Histone Modification and an RNA Component." *Nature Genetics* 30 (3): 329–34. https://doi.org/10.1038/ng843.

Milo, R., S. Shen-Orr, S. Itzkovitz, N. Kashtan, D. Chklovskii, and U. Alon. 2002. "Network Motifs: Simple Building Blocks of Complex Networks." *Science* 298 (5594): 824–27. https://doi.org/10.1126/science.298.5594.824.

Newman, M. E. J. 2010. *Networks: An Introduction*. Oxford, UK: Oxford University Press.

Piraveenan, M., S. Uddin, and K. S. K. Chung. 2012. "Measuring Topological Robustness of Networks under Sustained Targeted Attacks." *2012 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining*, August, 38–45. https://doi.org/10.1109/asonam.2012.17.

PYMNTS. 2020. "Fiserv on Why 2020 Is 'the Year of P2P.'" March 10, 2020. https://www.pymnts.com/news/payment-methods/2020/fiserv-p2p-real-time-payments-trust/.

R Core Team. 2020. *R: A Language and Environment for Statistical Computing*. Vienna: R Foundation for Statistical Computing.

Ripeanu, M. 2001. "Peer-to-Peer Architecture Case Study: Gnutella Network." In *Proceedings of the First International Conference on Peer-to-Peer Computing*, 99–100.

Ripeanu, Matei, and Ian Foster. 2002. "Mapping the Gnutella Network: Macroscopic Properties of Large-Scale Peer-to-Peer Systems." *Peer-to-Peer Systems*, 85–93. https://doi.org/10.1007/3-540-45748-8_8.

Romanosky, Sasha, Lillian Ablon, Andreas Kuehn, and Therese Jones. 2019. "Content Analysis of Cyber Insurance Policies: How Do Carriers Price Cyber Risk?" *Journal of Cybersecurity* 5 (1). https://doi.org/10.1093/cybsec/tyz002.

Salles, R. M., and D. A. Marino. 2011. "Strategies and Metric for Resilience in Computer Networks." *The Computer Journal* 55 (6): 728–39. https://doi.org/10.1093/comjnl/bxr110.

Shen-Orr, Shai S., Ron Milo, Shmoolik Mangan, and Uri Alon. 2002. "Network Motifs in the Transcriptional Regulation Network of Escherichia Coli." *Nature Genetics* 31 (1): 64–68. https://doi.org/10.1038/ng881.

Tehan, R. 2015. "Cybersecurity: Data, Statistics, and Glossaries." *Congressional Research Service Report*, R43310.

Vespignani, Alessandro. 2010. "The Fragility of Interdependency." *Nature* 464 (7291): 984–85. https://doi.org/10.1038/464984a.

Watts, D. J., and S. H. Strogatz. 1998. "Efficient Sampling Algorithm for Estimating Subgraph Concentrations and Detecting Network Motifs." *Nature* 393:440–42.

Xu, Maochao, and Lei Hua. 2017. “Cybersecurity Insurance: Modeling and Pricing.” *Society of Actuaries*.

Zurich Insurance Company Ltd and Atlantic Council of the United States. 2014. *Beyond Data Breaches: Global Interconnections of Cyber Risk*. Zurich, Switzerland: Risk Nexus report. Zurich Insurance Company Ltd; Washington, D.C.: Atlantic Council.