A Spectral Measure for Network Robustness: Assessment, Design, and Evolution

Shengmin Jin
Data Lab, EECS Department
Syracuse University
shengmin@data.syr.edu

Rui Ma
EECS Department
Syracuse University
rma102@syr.edu

Jiayu Li
Data Lab, EECS Department
Syracuse University
jli221@data.syr.edu

Sara Eftekharnejad
EECS Department
Syracuse University
seftekha@syr.edu

Reza Zafarani
Data Lab, EECS Department
Syracuse University
reza@data.syr.edu

2022 IEEE International Conference on Knowledge Graph (ICKG) | 978-1-6654-5101-7/22/$31.00 ©2022 IEEE | DOI: 10.1109/ICKG55886.2022.00020

***Abstract*—A robust system should perform well under random failures or targeted attacks, and networks have been widely used to model the underlying structure of complex systems such as communication, infrastructure, and transportation networks. Hence, network robustness becomes critical to understanding system robustness. In this paper, we propose a spectral measure for network robustness: the second spectral moment m_2 of the network. Our results show that a smaller second spectral moment m_2 indicates a more robust network. We demonstrate both theoretically and with extensive empirical studies that the second spectral moment can help (1) capture various traditional measures of network robustness; (2) assess the robustness of networks; (3) design networks with controlled robustness; and (4) study how complex networked systems (e.g., power systems) behave under cascading failures.**

***Index Terms*—Network Robustness, Graph Spectrum**

I. Introduction

The study of network robustness in complex systems plays an important role in various fields such as biology, economics, and engineering. Network robustness is often defined as *a network's ability to continue functioning when part of the network is either naturally damaged or targeted for attack* [1]–[3]. In the study of network robustness, there are two fundamental research goals: (1) the assessment of the robustness of a network, i.e., how to quantify the network robustness? (2) the utility of network robustness, i.e., how to use the robustness of a network? In this paper, we aim to have a systematic study on network robustness, by answering the following three questions: [**Q1**] how to assess the robustness of networks?; [**Q2**] how to design networks with controlled robustness?; [**Q3**] how to study the behavior of a complex system by observing the evolution of its network robustness?

To answer the questions, we should seek an appropriate measure. We consider using a powerful tool in graph analysis: spectral graph theory, as spectral graph theory connects the structure of a network to the eigenvalues and eigenvectors of its associated matrices, e.g., the adjacency matrix or the Laplacian. Previously, the extreme eigenvalues and associated eigenvectors have been connected to the study of network robustness. A well-known example is that the second-smallest eigenvalue of a graph Laplacian is related to algebraic graph connectivity, and the associated eigenvector is used for spectral clustering [4]. Recently, instead of the extreme eigenvalues, the overall distribution of eigenvalues, also known as the *spectral density* of the graph has received more attention. Dong and his colleagues utilize methods from condensed matter physics to study spectral densities in networks, and they show that the spectral density is a practical tool to analyze large real-world networks [5], as different types of networks have different patterns in their spectral density [5]. In this paper, we aim to measure the network robustness through the spectral density.

The Present Work: Spectral Moments for Network Robustness Assessment. We propose utilizing spectral moments, especially the second spectral moment m_2 of the random walk transition matrix of a network as a robustness measure, justified by various reasons: (a) **Capture network robustness**. We prove that spectral moments are tightly connected to existing network robustness measures including average distance, diameter, spectral radius, and the existence of a giant component; (b) **Interpretablity**. Spectral moments have been used to capture the shape of a spectral density, and they have been proved to capture various network structures and properties [6]. Specifically, m_2 has a clear meaning, which is the expected return probability of a 2-step random walk. Intuitively, in a graph with a small expected return probability for a random walk (a walk which travels far away from its starting node) is more likely an indication of a well-connected graph. This observation motivates the use of m_2 as a measure of network robustness. (c) **Easy and fast to compute.** For large networks, m_2 can be approximated accurately in seconds.

Overall, our contributions are mainly the following:

I. A Spectral Measure for Network Robustness. We propose using the second spectral moment m_2 of a network as a network robustness measure. We show that m_2 can capture network robustness on both synthetic and real-world networks. Specifically, when m_2 is smaller, the network is more robust.

978-1-6654-5101-7/22/$31.00 ©2022 IEEE
DOI 10.1109/ICKG55886.2022.00020

The spectral moments can be used to assess the degree of robustness of a network, or to compare the robustness of two networks varying in size.

II. Connection to Existing Network Robustness Measures. We prove that the second spectral moment m_2 is closely related to four well-known robustness measures (average distance, diameter, spectral radius, and the existence of a giant component) for random graphs with given expected (or exact) degrees sequences.

III. Designing Networks with Controllable Robustness. We show that we can control the network robustness by manipulating its m_2 value, to design a network that is more robust under failures. We conduct experiments on real-world networks, and evaluate the method.

IV. Evolution of Network Robustness under Cascading Failures. We demonstrate that with m_2 as the robustness measure, one can study how a complex networked system behaves under cascading failures by looking at how network robustness evolves. By studying cascading failures in a power grid network, we show that after an initial failure making the grid vulnerable, the grid stabilizes after the cascading failures.

The rest of the paper is organized as follows. We briefly review spectral moments and propose the use of m_2 as a network robustness measure in Section II. In Section III, we show the relationship between the second spectral moment and other robustness measures. We use the second spectral moment to assess robustness of real-world networks in Section IV, and discuss ways to design networks with controllable robustness in Section V. Section VI details our observations on the evolution of robustness under cascading failures in a power grid. After reviewing further related work in Section VII, we conclude in Section VIII.

II. Spectral Moments as a Robustness Measure

As we have mentioned, we propose using the second spectral moments m_2 of random walk transition matrix as a network robustness measure.

A. Spectral Moments

We firstly briefly review the spectral moments of the random walk transition matrix. For an undirected graph $G = (V, E)$ with vertices $V = \{v_1, v_2, \ldots, v_n\}$ and edges $E \subseteq V \times V$, its adjacency matrix $A \in \mathbb{R}^{n \times n}$ has $A_{ij} = 1$ if $(i, j) \in E$ and otherwise, $A_{ij} = 0$. The degree matrix $D \in \mathbb{R}^{n \times n}$ is a diagonal matrix with node degrees on its diagonal, i.e., $D_{ii} = \sum_{j=1}^{n} A_{ij}$. The transition matrix of the random walk on G is matrix $P = AD^{-1}$. As P is a stochastic matrix, its spectrum is also bounded: $1 = \lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_{n-1} \geq \lambda_n \geq -1$, where λ_i's are the eigenvalues of P. Here, we denote the ℓ-th spectral moment m_ℓ of a graph G using the spectrum of its random walk transition matrix P, $m_\ell = \mathbb{E}(\lambda^\ell) = \frac{1}{n}\sum_{i=1}^{n} {\lambda_i}^\ell$. Research has shown that spectral moments are connected to basic subgraphs such as edges, triangles, and squares [6]. Moreover, spectral moments have been used for applications such as network visualization, network identification [7], [8] and capturing the relationship between subgraphs and the whole network [9].

Here, we specifically focus on the second spectral moment m_2. In [6], the following theorem is proved, which will be used to prove some of the results here.

Theorem II.1 (Second Spectral Moment m_2)**.** *For graph G, the second spectral moment m_2 is*

$$m_2 = \mathbb{E}(d_i)\,\mathbb{E}(\frac{1}{d_i d_j}),$$

where $\mathbb{E}(d_i)$ is the average degree and $\mathbb{E}(\frac{1}{d_i d_j})$ is the expected value of $\frac{1}{d_i d_j}$ over edges, where d_i and d_j are the degrees of nodes i and j linked by some edge (i, j).

B. Time Complexity

For large graphs, we can compute accurate estimates of the low-order moments with the ApproxSpectralMoment algorithm [10]. The algorithm estimates the moments by simulating many random walks and computes the proportion of closed walks. To compute the ℓ-th spectral moment by simulating r random walks, it takes $O(r\ell)$ time. To compute m_2, we set $\ell \leq 2$ and $r = 10,000$ following the empirical results of [10]. As the random walks can be taken in parallel, it only takes less than a few seconds to compute the second spectral moment even for large networks [6], [10].

C. Second spectral moment m_2 and the Estrada Index

As mentioned above, m_2 is the expected return probability of a 2-step random walk. Naturally, one may have a valid concern that it does not directly capture robustness in terms of higher-order information, i.e., the return probability of longer walks. Here, we show that, on the contrary, m_2 actually provides tight upper and lower bounds on the expected return probability of a random walk of any length, discounting longer walks. For that, we first introduce the normalized Estrada index of the random-walk transition matrix $EE_{P-norm}(G)$.

The Estrada index of a graph G is defined as $EE(G) = \sum_{j=1}^{n} e^{\mu_j}$, where μ_j's are the eigenvalues of the adjacency matrix A [11]. The Estrada index counts the number of closed walks, discounting longer walks, as $EE(G) = \mathrm{trace}(e^A) = \sum_{k=0}^{\infty} \frac{\mathrm{trace}(A^k)}{k!}$. Therefore, Estrada index is sometimes used to measure the global connectivity of a graph. In [6], a variation of the Estrada index using the random walk transition matrix P is denoted as $EE_P(G) = \sum_{j=1}^{n} e^{\lambda_j} = \sum_{j=1}^{n} \mathrm{trace}(e^P) = \sum_{k=0}^{\infty} \frac{\mathrm{trace}(P^k)}{k!} = n\sum_{k=0}^{\infty} \frac{m_k}{k!}$. Unlike the Estrada index, $EE_P(G)$ computes the expected return probability of a random walk of any length, discounting longer walks. Intuitively, if a walk can travel far away from its starting node, it is an indication that the graph is well-connected. Generally, the smaller the $EE_P(G)$ value, the more well-connected the graph G. Here, we normalize $EE_P(G)$ by the size of the graph and get $EE_{P-norm}(G) = \frac{1}{n}EE_P(G) = \sum_{k=0}^{\infty} \frac{m_k}{k!}$, to cancel the effect of the size of the graph.

In Theorem II.2, we prove that the second moment m_2 provides both tight upper and lower bounds on $EE_{P-norm}(G)$. In

other words, the expected return probability of longer random walks can be bounded by functions of m_2.

Theorem II.2 (Bounds on $EE_{P-norm}(G)$ by m_2)**.** *For an undirected graph G without self-loops, its normalized Estrada Index $EE_{P-norm}(G)$ is bounded by the second moment m_2:*

$$1 + \frac{m_2}{2} \leq EE_{P-norm}(G) \leq 1 + m_2$$

Proof. We first prove $1 + \frac{m_2}{2} \leq EE_{P-norm}(G)$. For an undirected graph without self-loops, it is clear that $m_0 = 1$ and $m_1 = 0$. By definition, $EE_{P-norm}(G) = \sum_{k=0}^{\infty} \frac{m_k}{k!} \geq \sum_{k=0}^{2} \frac{m_k}{k!} = m_0 + m_1 + \frac{m_2}{2} = 1 + \frac{m_2}{2}$, as $m_k \geq 0$.

Next, we prove $EE_{P-norm}(G) \leq 1 + m_2$. As $e^x \leq 1 + x + x^2$, $EE_{P-norm}(G) = \frac{1}{n} EE_P(G) = \frac{1}{n} \sum_{j=1}^{n} e^{\lambda_j} \leq \frac{1}{n} \sum_{j=1}^{n} (1 + \lambda_j + \lambda_j^2) = 1 + m_1 + m_2 = 1 + m_2$.

The bounds are tight; consider an empty graph. Then, $m_k = 0$ for $k \geq 1$. Hence, $m_2 = 0$ and $EE_{P-norm}(G) = 1$. □

III. Connection to Existing Robustness Measures

Next, we connect m_2 with four well-known robustness measures: diameter, average distance, spectral radius, and giant component. Particularly, we show that spectral moments are connected to the robustness of graphs generated by two network models: Chung-Lu and Configuration Model.

Consider a random graph with an expected degree sequence (also known as the *Chung-Lu model* [12], [13]). Chung-Lu model is a general model $G(\mathbf{w})$ for random graphs with a given expected degree sequence $\mathbf{w} = (w_1, w_2, \ldots, w_n)$. For a random graph $G \in G(\mathbf{w})$, the edge between nodes v_i and v_j is chosen independently with probability $p_{ij} = \frac{w_i w_j}{\sum_i w_i}$, which is proportional to the product $w_i w_j$. Denote $\tilde{d} = \frac{\sum w_i^2}{\sum w_i}$ as the second-order average degree. Chung et al. have shown that $\tilde{d}$ is closely related to various graph properties [12]–[14]. In the rest of the paper, a random graph G with degree sequence $(d_1, d_2, \ldots, d_n)$ refers to one realization of those generated by the Chung-Lu model, i.e., $G \in G(\mathbf{w})$ where $\mathbf{w} = (d_1, d_2, \ldots, d_n)$. We show that the spectral moments of the graphs generated by the Chung-Lu model capture various robustness measures in them.

Similarly, we consider random graphs generated by the configuration model (Molloy-Reed model), where the graph has a fixed degree sequence. We show that spectral moments also capture robustness, in terms of the existence of the giant component, in such graphs.

We start with the Chung-Lu model and in Lemma III.1, we demonstrate that second-order average degree $\tilde{d}$ is lower bounded by the inverse of second spectral moment m_2 of a Chung-Lu random graph.

Lemma III.1. *For a random graph G with given expected degrees, the second-order average degree $\tilde{d}$ satisfies*

$$\tilde{d} \geq \sqrt{\frac{\mathbb{E}(d_i)}{m_2}},$$

where m_2 is the second spectral moment of G and $\mathbb{E}(d_i)$ is the average node degree in G.

Proof. By definition, $\tilde{d} = \frac{\sum w_i^2}{\sum w_i} = \frac{\sum d_i^2}{\sum d_i} = \frac{\mathbb{E}(d_i^2)}{\mathbb{E}(d_i)}$. From Theorem 4.1 of [6], for any graph $\mathbb{E}(\frac{1}{d_i d_j}) \geq \frac{\mathbb{E}^2(d_i)}{\mathbb{E}^2(d_i^2)}$, so $\mathbb{E}(\frac{1}{d_i d_j}) \geq \frac{1}{\tilde{d}^2}$, implying $\tilde{d}^2 \geq \frac{1}{\mathbb{E}(\frac{1}{d_i d_j})}$ and $\tilde{d} \geq \sqrt{\frac{1}{\mathbb{E}(\frac{1}{d_i d_j})}}$. By Thm. II.1, $m_2 = \mathbb{E}(d_i)\,\mathbb{E}(\frac{1}{d_i d_j})$, so $\tilde{d} \geq \sqrt{\frac{\mathbb{E}(d_i)}{m_2}}$. □

Next, we will show the connection between spectral moments with the following robustness measures: (1) average distance, (2) diameter, and (3) spectral radius of a graph with a given expected degree distribution.

I. Average Distance. In a graph G, denote distance $d(u, v)$ as the length of the shortest path between u and v. Average distance of a graph G, denoted by $\overline{d_{uv}}$, is the average distance over all pairs of vertices (u, v) in G. A smaller $\overline{d_{uv}}$ shows that nodes are closer to each other and the network is well-connected and more robust [2].

Theorem III.2. *For a random graph G with given expected degree sequence, if $\mathbf{w} = (d_1, d_2, \ldots, d_n)$ is admissible, for the average distance $\overline{d_{uv}}$, we have*

$$\overline{d_{uv}} \leq (1 + o(1)) \frac{2 \log n}{\log \mathbb{E}(d_i) - \log m_2}.$$

Proof. From [14], the average distance $\overline{d_{uv}}$ is almost surely $(1 + o(1)) \frac{\log n}{\log \tilde{d}}$, when the degree sequence is *admissible* (see definition in [14]). Specifically, $\overline{d_{uv}}$ is upper bounded by $(1 + o(1)) \frac{\log n}{\log \tilde{d}}$. By Lemma III.1, $\tilde{d} \geq \sqrt{\frac{\mathbb{E}(d_i)}{m_2}}$. Moreover, in our settings, d_i's are the degree of the nodes, so $d_i \geq 1$ or $d_i = 0$, and $\tilde{d} = \frac{\sum d_i^2}{\sum d_i} \geq 1$, and $\frac{\mathbb{E}(d_i)}{m_2} = \frac{1}{\mathbb{E}(\frac{1}{d_i d_j})} \geq 1$. Therefore, $\frac{1}{\log \tilde{d}} \leq \frac{1}{\log \sqrt{\frac{\mathbb{E}(d_i)}{m_2}}}$. Hence, $\overline{d_{uv}} \leq (1 + o(1)) \frac{\log n}{\log \sqrt{\frac{\mathbb{E}(d_i)}{m_2}}} = (1 + o(1)) \frac{2 \log n}{\log \mathbb{E}(d_i) - \log m_2}$. □

From Theorem III.2, for a random graph with a given expected degree distribution (naturally, n and $\mathbb{E}(d_i)$ is fixed), the average distance of the graph is upper bounded by a term that depends on m_2. Specifically, when m_2 is smaller, the upper bound is smaller. Hence, in terms of the average distance, a smaller m_2 indicates a more robust network.

II. Diameter. The diameter of graph G, denoted by $D(G)$, is the maximum distance over all pairs of nodes in G. The diameter is closely connected to robustness, as it is a tight upper bound on the distance between any two nodes in the network. Thus, a smaller diameter shows more robustness [2].

Theorem III.3. *For a random graph G with given expected degree sequence, if $\mathbf{w} = (d_1, d_2, \ldots, d_n)$ is specially admissible, the diameter $D(G)$ is almost surely $\mathcal{O}(\frac{2 \log n}{\log \mathbb{E}(d_i) - \log m_2})$.*

Proof. From [14], $D(G)$ is almost surely $\Theta(\frac{\log n}{\log \tilde{d}})$, when the degree sequence is *specially admissible* (see definition in [14]). As $\frac{1}{\log \tilde{d}}$ is upper bounded by $\frac{1}{\log \sqrt{\frac{\mathbb{E}(d_i)}{m_2}}}$, we have $D(G)$ is almost surely $\mathcal{O}(\frac{2 \log n}{\log \mathbb{E}(d_i) - \log m_2})$. □

Similar to the average distance, Theorem III.3 shows that the diameter of a random graph G with a given de-

gree sequence is upper bounded by a term that depends on m_2. Specifically, when m_2 is smaller, the upper bound on the diameter is smaller. Hence, in terms of the diameter, a smaller m_2 indicates a more robust network.

III. Spectral Radius. The largest eigenvalue of the adjacency matrix A is called its spectral radius ρ. The spectral radius is closely related to the *path capacity* or *loop capacity* of the graph. A larger ρ implies that the graph has many loops and paths, so the graph is well-connected [15], [16]. In general, a larger ρ indicates a more robust network.

Theorem III.4. *For a random graph with given expected degree sequence, if* $\tilde{d} > \sqrt{d_{\max}(G)}\log n$, *then* $\rho \geq (1 + o(1))\sqrt{\frac{\mathbb{E}(d_i)}{m_2}}$, *where* $d_{\max}(G)$ *is the maximum degree.*

Proof. Chung et. al [13] proved that when $\tilde{d} > \sqrt{d_{\max}(G)}\log n$, ρ is roughly equal to the the second order average degree $\tilde{d}$, i.e., ρ is almost surely $(1 + o(1))\tilde{d}$, and especially ρ is lower bounded by $(1 + o(1))\tilde{d}$ [13], [17]. By Lemma III.1, we get $\rho \geq (1 + o(1))\sqrt{\frac{\mathbb{E}(d_i)}{m_2}}$. □

Theorem III.4 indicates that if m_2 is smaller, then ρ has a greater lower bound. Hence, in terms of the spectral radius, a smaller m_2 indicates a more robust network.

Finally, we show that even when in the random graph the degree sequence is fixed, the spectral moments are related to network robustness. For that, we consider the graphs generated by the configuration model (Molloy-Reed model) and show that spectral moments capture the existence of the giant component.

IV. Giant Component. For a graph $G = (V, E)$, a giant component of G is a connected component having at least $\mathcal{O}(|V|)$ nodes [18], [19]. A component is called c-giant if it has at least $c \cdot |V|$ nodes (or $c \cdot |E|$ edges) [12]. In studies of network robustness, c is often defined as the fraction of nodes contained in the largest connected component, to measure network availability i.e., what percentage of the nodes can be reached [2]. Though the existence of a giant component does not mean that the network is robust (as in some cases the component can be split into small components by losing a few edges due to *bridges* in the network), it shows that the network keeps most nodes and maintains "functionality." In Theorem III.5, we show that m_2 can capture the existence of the giant component for Molloy-Reed random graphs.

Theorem III.5. *For a random graph* G *with an exact degree sequence generated by the Molloy-Reed model, when* $m_2 < \frac{1}{4}\mathbb{E}(d_i)$, *a giant component exists.*

Proof. Molloy-Reed Criterion states that for a random graph G generated by the Molloy-Reed model, when $\kappa = \frac{\mathbb{E}(d_i^2)}{\mathbb{E}(d_i)} > 2$, a giant component exists [20], [21]. Similar to Lemma III.1, we can show that $\kappa \geq \sqrt{\frac{1}{\mathbb{E}(\frac{1}{d_i d_j})}}$. Thus, if $\mathbb{E}(\frac{1}{d_i d_j}) < \frac{1}{4}$, we can ensure $\kappa > 2$ and a giant component exists. Further, the condition $\mathbb{E}(\frac{1}{d_i d_j}) < \frac{1}{4}$ is equivalent to $m_2 < \frac{1}{4}\mathbb{E}(d_i)$, proving the theorem. □

For a random graph G with an exact degree sequence, the average degree $\mathbb{E}(d_i)$ is fixed. Hence, from Theorem III.5, we find that for such a graph when m_2 is smaller, it is more likely to have a giant component.

A. Experiments on Synthetic Networks

We have shown the theoretical connection between m_2 and existing robustness measures. Here, we explore this connection empirically as well. To that end, we generate synthetic networks using the random graph model $G(n, p)$. For random graphs generated by $G(n, p)$, the behaviour of the size of the largest component is well-studied for p near $\frac{1}{n}$. For $p < \frac{1}{n}$, the size of the largest component is almost surely $O(\log n)$; for $p = \frac{1}{n}$, the size of the largest component is almost surely $\Theta(n^{2/3})$; and for $p > \frac{1}{n}$ the size of the largest component is almost surely $\Theta(n)$ [18], [19], [22]. For $p > \frac{1}{n}$, this largest component is commonly referred to as the *giant component* of $G(n, p)$, and the point $p = \frac{1}{n}$ is referred to as the *critical point* (for the *phase transition*). Here, we study the behavior of the second spectral moment m_2 and other network robustness measures near this critical point.

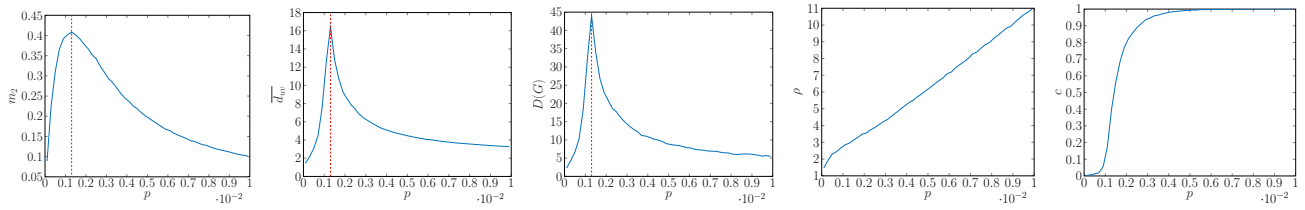
In our experiments, we set $n = 1,000$ nodes and vary p from 0.0001 to 0.01 with step size 0.0002. For each variation, we generate 20 random graphs, and in Figure 1, we plot the average value of m_2, $\overline{d_{uv}}$ (the average distance), $D(G)$ (the diameter), ρ (the spectral radius) and c (the fraction of nodes in the largest connected component). When the graph is not connected, we use $\overline{d_{uv}}$ and $D(G)$ of its largest connected component. We find that (1) with the increase of p, m_2 has a similar changing pattern to $\overline{d_{uv}}$ and $D(G)$: they all increase first and then decrease; (2) all of the turning points are at $p = 0.0013$, which is slightly greater than the critical point $p = 0.001$. In essence, the average distance and diameter increase with p when there is no giant component in the graph. However, when the giant component emerges, they keep increasing until a certain point and start to decrease. Our results show that m_2 captures this behavior well. Note that the time complexity to compute the average distance and diameter both requires $O(n^3/2^{\Omega(\log n)^{1/2}})$ [23] which is not feasible for large networks, but m_2 can be computed in a few seconds. Next, we look into using the second spectral moment m_2 to assess robustness in real-world networks.

IV. Assess Robustness in Real-World Networks

In this section, we aim to investigate spectral moment m_2 as a network robustness measure in real-world networks and to answer the question: [**Q1**] how to assess the robustness of networks with m_2? Therefore, we need to understand the connection between the robustness of a real-world network and its second spectral moment m_2. In other words, should a robust network have a larger or smaller m_2 value? Before presenting experiments, we review experimental setup.

A. Experimental Setup

We study 20 real-world networks from four general network categories: social networks, collaboration networks, road



(a) m_2 v.s. p (b) Average Distance v.s. p (c) Diameter v.s. p (d) Spectral Radius ρ v.s. p (e) Fraction of Nodes in Largest Connected Component c v.s. p

Figure 1: Robustness Measures v.s. p in $G(n,p)$; $n = 1,000$ and dashed line shows the turning point at $p = 0.0013$.

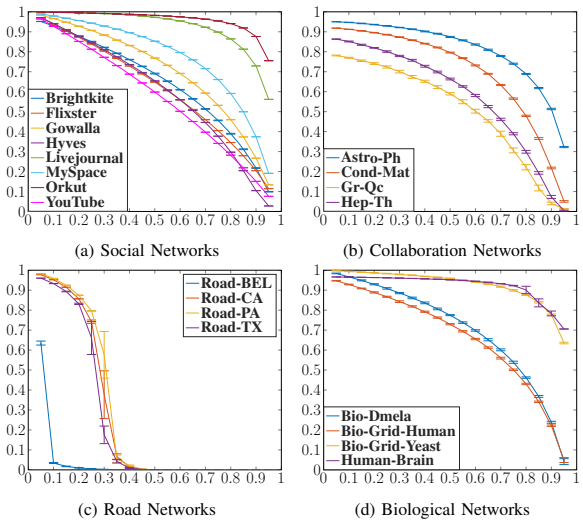
Table I: Dataset Statistics

Type	Network	$\|V\| = n$	$\|E\| = m$	Average Degree	Density ($\times 10^{-4}$)	m_2
Social Networks	Brightkite	58,228	214,078	7.353	1.263	0.1799
	Flixster	2,523,386	7,918,801	6.276	0.025	0.0261
	Gowalla	196,591	950,327	9.668	0.246	0.1403
	Hyves	1,402,673	2,777,419	3.960	0.028	0.0610
	Livejournal	3,017,286	85,654,976	56.78	0.188	0.0174
	MySpace	854,498	5,635,296	13.19	0.154	0.0923
	Orkut	3,072,441	117,185,083	76.28	0.248	0.0187
	YouTube	1,134,890	2,987,624	5.265	0.046	0.1574
Collaboration Networks	Astro-Ph	18,772	198,050	21.10	11.24	0.1007
	Cond-Mat	23,133	93,439	8.078	3.492	0.1672
	Gr-Qc	5,242	14,484	5.526	10.54	0.2831
	Hep-Th	9,877	25,973	5.259	5.324	0.2488
Road Networks	Road-BEL	1,441,295	1,549,970	2.143	0.014	0.4646
	Road-CA	1,965,206	2,766,607	2.816	0.014	0.3545
	Road-PA	1,088,092	1,541,898	2.834	0.026	0.3557
	Road-TX	1,379,917	1,921,660	2.785	0.020	0.3577
Biological Networks	Bio-Dmela	7,393	25,569	6.917	9.356	0.1278
	Bio-Grid-Human	9,527	62,364	13.09	13.74	0.1787
	Bio-Grid-Yeast	5,870	313,890	106.9	177.2	0.0198
	Human-Brain	177,600	15,669,036	176.4	9.910	0.0236

networks, and biological networks. We include eight social networks: *Brightkite* [24], *Flixster* [25], *Gowalla* [24], *Hyves* [25], *Livejournal* [26], *MySpace* [26], *Orkut* [24], and *YouTube* [24]; four collaboration networks: *Astro-Ph* [24], *Cond-Mat* [24], *Gr-Qc* [24], and *Hep-Th* [24]; four road networks: *Road-BEL* [24], *Road-CA* [24], *Road-PA* [24], and *Road-TX* [24]; four biological networks: *Bio-Dmela* [27], *Bio-Grid-Human* [27], *Bio-Grid-Yeast* [27], and *Human-Brain* [27]. The data statistics, including the m_2 value for each network, are in Table I.

B. Assess Network Robustness with Spectral Moments

To evaluate m_2 as a network robustness measure, we first define robustness of a real-world network. In its most abstract form, *robustness is the ability of a network to continue to perform well under failures or attacks* [1]. To quantify such a definition in our experiments, we consider the robustness of a network by looking at how c – the fraction of nodes in its largest connected component – changes under random edge failures. In other words, when losing the same number (or proportion) of edges, a more robust network exhibits a smaller drop in c value as most nodes within the "core" of the network are kept intact. Hence, for each network, we randomly remove $x\%$ of the edges of the graph by varying $x\%$ from 5% to 95% with step size 5%. For each $x\%$, we run the experiments 20 times and report the average c and its standard deviation in Figure 2. From the figure, we find that (1) road networks are much more vulnerable under random failures. For each road network, the size of its largest component drops sharply when losing edges randomly. Especially, by losing 35% of the edges, c becomes less than 10%. We notice that m_2 values of road networks are much larger than those of networks



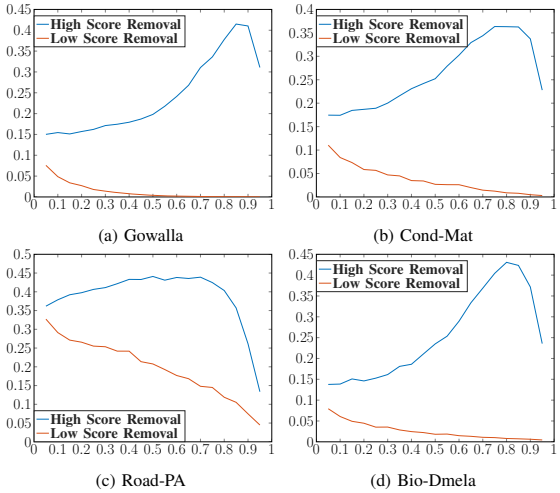
(a) Social Networks (b) Collaboration Networks (c) Road Networks (d) Biological Networks

Figure 2: Networks under Random Edge Failures. x value: fraction of edges removed; y value: fraction of nodes in the largest connected component c.

from other categories. Among road networks, Road-BEL is more vulnerable than others and has the largest m_2; (2) for networks from other three categories, c decreases smoothly as more edges are removed. Furthermore, if a network has a larger m_2, the fraction of nodes in its largest component shrinks faster. For networks with smaller m_2 values, such as Orkut and Human-Brain, they maintain more than 70% of the nodes in their largest component even after losing 90% of their edges. In general, these observations provide an answer to **Q1**: a real-world network with a smaller second spectral moment m_2 is more robust under random failures. Hence, we can compare the robustness of two networks by comparing their m_2 values, even if the networks vary in size.

V. Design Networks with Controllable Robustness

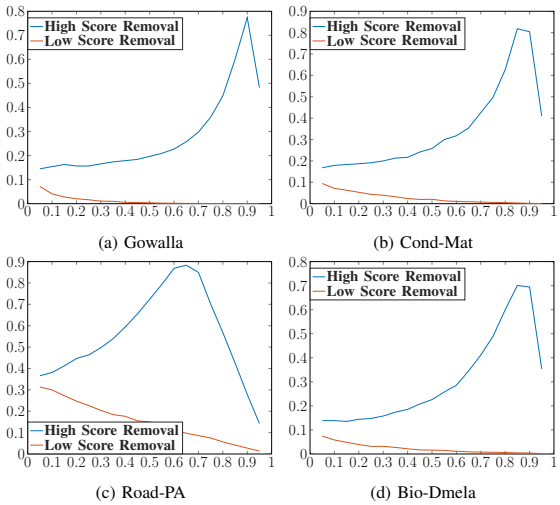
Next, we want to answer the question: [**Q2**] how to design networks with controlled robustness? In other words, can we design strategies to control (increase or decrease) robustness in a real-world network? From Section IV, we know that a robust network has a smaller m_2 value. Naturally, if we can control the network robustness by manipulating its m_2 value, we can "design" a network that is more robust under failures; or equivalently, develop more efficient attack models to harm the robustness of a network. Thus, we will design various



(a) Gowalla (b) Cond-Mat

(c) Road-PA (d) Bio-Dmela

Figure 3: Second spectral moment m_2 value with Batch Edge Removal. x: proportion of edges removed; y: m_2.



(a) Gowalla (b) Cond-Mat

(c) Road-PA (d) Bio-Dmela

Figure 4: Second Spectral Moment m_2 with Sequential Edge Removal. x: fraction of removed edges; y: m_2.

edge removal strategies here and assess their impact on the m_2 value of a network.

Theorem II.1 shows that $m_2 = \mathbb{E}(d_i)\,\mathbb{E}(\frac{1}{d_i d_j})$. Assume we remove a fixed number of edges from some graph G to get a new graph G'. The average degree of G' will only rely on the number of edges removed and is independent of which edges were removed from graph G. Hence, when a fixed number of edges are removed, what can make m_2 different is how these removed edges change the value of $\mathbb{E}(\frac{1}{d_i d_j})$. Intuitively, by removing edges (i, j) corresponding to higher $d_i d_j$ values (d_i and d_j are the degress of i and j), we should get a larger value of $\mathbb{E}(\frac{1}{d_i d_j})$ in G'. Hence, we design edge removal strategies that rely on the $d_i d_j$ values of edges. Here, we detail the developed edge removal strategies.

We define $d_i d_j$ value as the edge score for an edge (i, j) between nodes i and j with degrees d_i and d_j. We propose two strategies to remove edges based on the edge score: (1) *High Score Removal*, removing the edges with the highest scores from the graph; and (2) *Low Score Removal*, which removes the edges with the lowest scores. When an edge is removed from the graph, the scores of edges incident to the endpoints of the removed edge will change, which may impact the current ranking of edges based on this edge score. Hence, for the removal process, we propose two methods: (1) *Batch Removal*, where we pick top $x\%$ of edges in the graph based on each strategy (high score or low score removal) and remove them in one batch; (2) *Sequential Removal*, where each time we remove only the top-1 edge based on each strategy and after each removal, we update the ranks. In total, we remove $x\%$ of edges of the graph. For both methods, we vary $x\%$ from 5% to 95% with the step size 5%, and we report the changes in m_2 for one network from each category in Figure 3 and 4. For all other plots, please refer to the supplementary material.[1]

Table II: Phase Transition of m_2

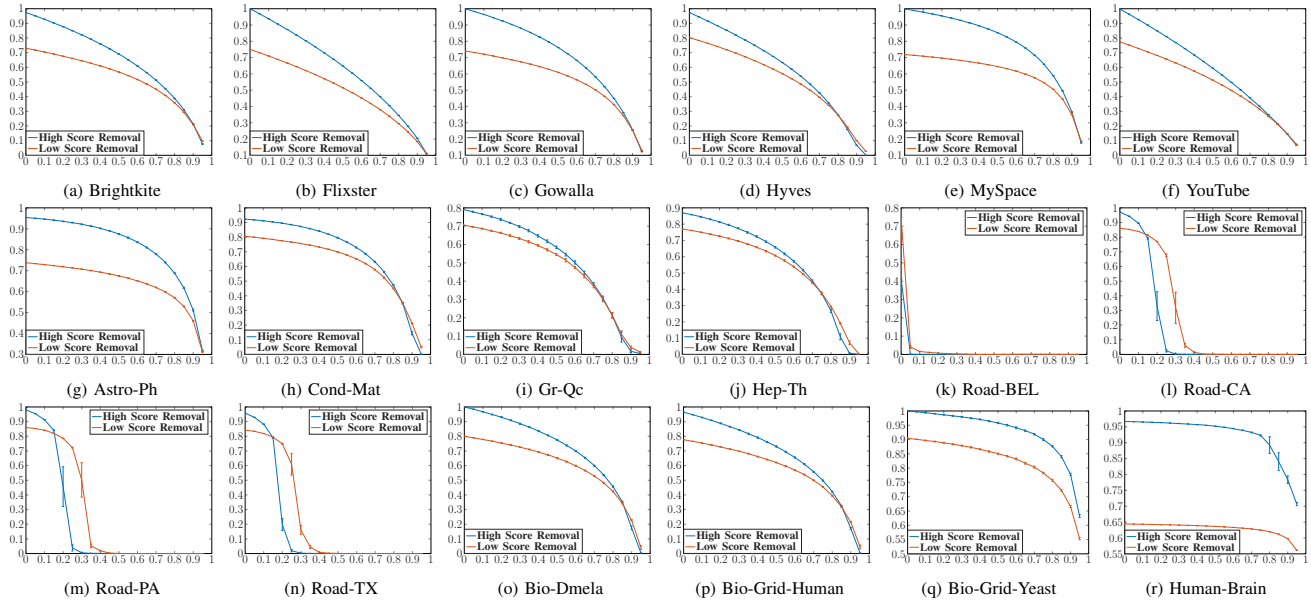
Network	Proportion of Edges Removed (Turning Point)	Average Degree of the Remaining Graph
Brightkite	0.85	7.353×0.15 = 1.10
Flixster	0.85	6.276×0.15 = 0.94
Gowalla	0.90	9.668×0.10 = 0.97
Hyves	0.85	3.960×0.15 = 0.59
YouTube	0.85	5.265×0.15 = 0.79
Astro-Ph	0.90	21.10×0.10 = 2.11
Cond-Mat	0.85	8.078×0.15 = 1.21
Gr-Qc	0.75	5.526×0.25 = 1.38
Hep-Th	0.70	5.259×0.30 = 1.66
Road-BEL	0.40	2.143×0.60 = 1.29
Road-CA	0.65	2.816×0.35 = 0.99
Road-PA	0.65	2.834×0.35 = 0.99
Road-TX	0.55	2.785×0.45 = 1.25
Bio-Dmela	0.85	6.917×0.15 = 1.04
Bio-Grid-Human	0.85	13.09 × 0.15 = 1.96

We observe that for both batch and sequential removal: (1) for *High Score Removal*, with more edges removed, m_2 of most networks increases first and after a certain point, m_2 drops sharply. Further, if we look at the turning point of the curve, it always happens when the average degree of the remaining graph is around 1.0 (see Table II), indicating a *phase transition* for m_2. However, if a network has a very high average degree (such as Bio-Grid-Yeast or Orkut), by removing 95% of its edges, the average degree of the remaining graph can be much greater than 1.0. For such networks, the phase transition will not appear in the figures; (2) for *Low Score Removal*, m_2 decreases monotonously as more edges are removed. So, generally, in response to **Q2**, removing edges (i, j) corresponding to highest $d_i d_j$ values decreases network robustness (increases m_2), and removing edges corresponding to lowest $d_i d_j$ values increases network robustness (decreases m_2).

A. Evaluation

We evaluate whether the proposed manipulations on m_2 can change network robustness. For a network G, we first remove 10% of its edges with *High Score Removal* (and *Low Score Removal*) in batch to get G_{High} (and G_{Low}); then we let G_{High} (and G_{Low}) experience the same random edge failures as detailed in Section IV-B. The results are shown in Figure 5. From the figure, we find that (1) we initially observe in G_{Low} a smaller largest connected component, as low degree nodes

[1]Other plots are available at https://bit.ly/3SqDPSP



(a) Brightkite (b) Flixster (c) Gowalla (d) Hyves (e) MySpace (f) YouTube

(g) Astro-Ph (h) Cond-Mat (i) Gr-Qc (j) Hep-Th (k) Road-BEL (l) Road-CA

(m) Road-PA (n) Road-TX (o) Bio-Dmela (p) Bio-Grid-Human (q) Bio-Grid-Yeast (r) Human-Brain

Figure 5: Network Robustness after m_2 Manipulation (Note: Due to the large size, Livejournal and Orkut are not included in this experiment.)

are removed from the component. However, this observation does not mean that G_{Low} is vulnerable as the remaining nodes in the component can be well-connected; (2) In terms of the robustness, G_{High} is more vulnerable under random failures. By looking at the slope of the curve, we observe that when under the same random failures (randomly losing the same number of edges), the size of the largest connected component of G_{High} shrinks faster than that of G_{Low}. Hence, *High Score Removal* increases m_2 of a network, making it less robust.

VI. Evolution of Network Robustness under Cascading Failures

Next, we are going to answer the question: [**Q3**] how to study the behavior of a complex system by observing the evolution of its network robustness? We specifically consider the evolution of network robustness under cascading failures. In reality, in a network-based system the activity of an edge (or a node) often depends on the activity of its neighboring edges (or nodes) [28]. Hence, the failure of an edge can trigger the failure of the edges incident to it, and such sequences of failures are called *cascading failures*. For example, a power grid network is composed of busses (nodes) and transmission lines (edges). If one (or multiple) transmission lines are disconnected (e.g., due to natural disasters or operator mistakes), it can cause some other transmission lines to fail by exceeding their power flow limit and trigger more failures. Different from random failures or failures caused by attacks, cascading failures are closely related to the governing laws of the underlying networked system, e.g., power flow equations. Hence, during cascading failures, how a network evolves in terms of its robustness can indeed shed light on the governing laws of the underlying system.

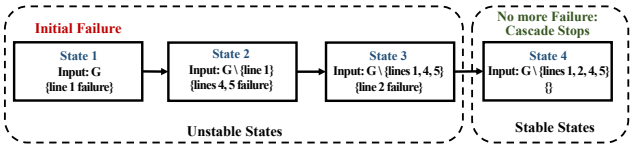


Figure 6: A cascade example

A. Data Collection

We study the cascading failures in a well-studied power grid network (see [29] for details). We generate the cascading failures with the methods provided by Ma et al. [30]. We sample 100,000 different initial loading conditions on this power grid. For each initial loading condition, we choose all single-line failures as the initial failures. Then, we use the AC-based power flow to obtain the cascading failures. As this power grid has 41 transmission lines, we have $41 \times 100,000 = 4,100,000$ initial failure events in total. Among these initial failures, 1,644,135 of them trigger a cascading failure sequence. Figure 6 provides an example. In this example, we define state 4 as the *stable state* of the cascade, and other states as *unstable states* as they trigger subsequent failures of power lines.

B. Analysis

In a cascade, at each state, the system can be viewed as a subgraph of the previous states as we are losing power lines (edges). Thus, we can view each cascade as a sequence of subgraphs. We represent each cascade using the m_2 values of its subgraphs, and we study the changing patterns of m_2

m_2	Number of Patterns	Proportions
$\nearrow$	2,466,379	46.4%
$\searrow$	2,836,207	53.4%
$\rightarrow$	10,583	0.2%

Table III: Changing Pattern of m_2 in Cascading Failures. $\nearrow$: m_2 increases; $\searrow$: m_2 decreases; $\rightarrow$: m_2 does not change.

m_2	Number of Cases	Proportions
$m_2^{\text{Initial}} > m_2^{\text{Final}}$	1,261,201	76.7%
$m_2^{\text{Initial}} < m_2^{\text{Final}}$	382,934	23.2%
$m_2^{\text{Initial}} = m_2^{\text{Final}}$	0	0.0%

Table IV: Comparison of m_2 of the initial failure state and the final state. m_2^{Initial}: m_2 of the initial state; m_2^{Final}: m_2 of the final state.

between consecutive states. For example, if a cascade has four states and m_2 values of the sequence of subgraphs are: $[0.3632, 0.3893, 0.3726, 0.3514]$, then the changing patterns are $\nearrow\searrow\searrow$ which is composed of one increase and two decrease of m_2. Across all the cascades, we report the total number of changing patterns in Table III. We find that in general, decreasing patterns (53.4%) are slightly more than the increasing patterns (46.4%). Next, for each cascade, we compare the m_2 of the initial failure state and that of the final (stable) state. Table IV demonstrates that for 76.7% of the cascades, the m_2 value of the final state is smaller than that of the initial state, compared to 23.2% on the other direction. The difference is much more significant than that of the consecutive changing patterns. Notice that a smaller m_2 indicates the network is more robust. Hence, in general, an initial failure happens at a vulnerable state, and after the cascading failures change system robustness, the system stabilizes (converges to a more robust network).

VII. Additional Related Work

Additionally, our work has links to the following areas:

I. Edge Modification. Studies have shown that edge modification, such as adding, rewiring [3], or protecting some edges, can enhance network robustness. Our work theoretically connects edge removal with spectral moments.

II. Spectral Robustness. Wu and his colleagues propose natural connectivity, which can be regarded as the "average eigenvalue" of the adjacency matrix [31]. In our work, we look at the eigenvalue distribution of the random walk transition matrix via its spectral moments (equivalently, the spectral moments of the normalized Laplacian matrix).

VIII. Conclusion

We propose a spectral measure for network robustness: the second spectral moment m_2 of the random walk transition matrix. We theoretically and empirically demonstrate that m_2 can capture network robustness: *a graph with a smaller second spectral moment m_2 is more robust*. We show the relationship between m_2 and edge properties so that one can control the network robustness by manipulating its m_2 value.

Acknowledgements. This research was supported in part by the National Science Foundation under awards CAREER IIS-1942929 and CAREER ECCS-2144918.

References

[1] W. Ellens and R. E. Kooij, "Graph measures and network robustness," *arXiv:1311.5064*, 2013.

[2] S. Freitas, D. Yang, S. Kumar, H. Tong, and D. H. Chau, "Graph vulnerability and robustness: A survey," *arXiv preprint arXiv:2105.00419*, 2021.

[3] A. Beygelzimer, G. Grinstein, R. Linsker, and I. Rish, "Improving network robustness by edge modification," *Physica A*, vol. 357, no. 3-4, pp. 593–612, 2005.

[4] A. Y. Ng, M. I. Jordan, and Y. Weiss, "On spectral clustering: Analysis and an algorithm," in *NIPS*, 2002, pp. 849–856.

[5] K. Dong, A. Benson, and D. Bindel, "Network density of states," in *KDD*, 2019, pp. 1152–1161.

[6] S. Jin and R. Zafarani, "The spectral zoo of networks: Embedding and visualizing networks with spectral moments," in *KDD*, 2020, pp. 1426–1434.

[7] S. Jin, V. Phoha, and R. Zafarani, "Network identification and authentication," in *ICDM*. IEEE, 2019, pp. 1144–1149.

[8] S. Jin, V. V. Phoha, and R. Zafarani, "Graph-based identification and authentication: A stochastic kronecker approach," *IEEE Transactions on Knowledge & Data Engineering*, vol. 34, no. 07, pp. 3282–3294, 2022.

[9] S. Jin, H. Tian, J. Li, and R. Zafarani, "A spectral representation of networks: The path of subgraphs," in *KDD*, 2022, pp. 698–708.

[10] D. Cohen-Steiner, W. Kong, C. Sohler, and G. Valiant, "Approximating the spectrum of a graph," in *KDD*. ACM, 2018, pp. 1263–1271.

[11] E. Estrada, "Characterization of the folding degree of proteins," *Bioinformatics*, vol. 18, no. 5, pp. 697–704, 2002.

[12] F. Chung and L. Lu, "Connected components in random graphs with given expected degree sequences," *Annals of combinatorics*, vol. 6, no. 2, pp. 125–145, 2002.

[13] F. Chung, L. Lu, and V. Vu, "The spectra of random graphs with given expected degrees," *Internet Mathematics*, vol. 1, no. 3, pp. 257–275, 2004.

[14] F. Chung and L. Lu, "The average distances in random graphs with given expected degrees," *PNAS*, vol. 99, no. 25, pp. 15 879–15 882, 2002.

[15] H. Tong, B. A. Prakash, C. Tsourakakis, T. Eliassi-Rad, C. Faloutsos, and D. H. Chau, "On the vulnerability of large graphs," in *ICDM*. IEEE, 2010, pp. 1091–1096.

[16] P. Van Mieghem, D. Stevanović, F. Kuipers, C. Li, R. Van De Bovenkamp, D. Liu, and H. Wang, "Decreasing the spectral radius of a graph by link removals," *Physical Rev. E*, vol. 84, no. 1, p. 016101, 2011.

[17] F. Chung, L. Lu, and V. Vu, "Eigenvalues of random power law graphs," *Annals of Combinatorics*, vol. 7, no. 1, pp. 21–33, 2003.

[18] P. Erdos, A. Rényi *et al.*, "On the evolution of random graphs," *Hung. Acad. Sci*, vol. 5, no. 1, pp. 17–60, 1960.

[19] S. Janson, D. E. Knuth, T. Łuczak, and B. Pittel, "The birth of the giant component," *Random Structures & Algorithms*, vol. 4, no. 3, pp. 233–358, 1993.

[20] M. Molloy and B. Reed, "A critical point for random graphs with a given degree sequence," *Random structures & algorithms*, vol. 6, no. 2-3, pp. 161–180, 1995.

[21] ——, "The size of the giant component of a random graph with a given degree sequence," *Combinatorics probability and computing*, vol. 7, no. 3, pp. 295–305, 1998.

[22] B. Bollobás, "The evolution of random graphs," *Trans. of the AMS*, vol. 286, no. 1, pp. 257–274, 1984.

[23] R. R. Williams, "Faster all-pairs shortest paths via circuit complexity," *SIAM Journal on Computing*, vol. 47, no. 5, pp. 1965–1985, 2018.

[24] J. Leskovec and A. Krevl, "SNAP Datasets: Stanford large network dataset collection," http://snap.stanford.edu/data, Jun. 2014.

[25] R. Zafarani and H. Liu, "Social computing data repository at ASU," 2009. [Online]. Available: http://socialcomputing.asu.edu

[26] Y. Zhang, J. Tang, Z. Yang, J. Pei, and P. S. Yu, "Cosnet: Connecting heterogeneous social networks with local and global consistency," in *Proceedings of the 21th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*. ACM, 2015, pp. 1485–1494.

[27] R. Rossi and N. Ahmed, "The network data repository with interactive graph analytics and visualization." in *AAAI*, vol. 15, 2015, pp. 4292–4293.

[28] A.-L. Barabási, "Network science," *Philosophical Trans. of the Royal Soc. A*, vol. 371, no. 1987, p. 20120375, 2013.

[29] R. Christie and I. Dabbagchi, "30 bus power flow test case," 1993.

[30] R. Ma, S. Jin, S. Eftekharnejad, R. Zafarani, and W. P. J. Philippe, "A probabilistic cascading failure model for dynamic operating conditions," *IEEE Access*, vol. 8, pp. 61 741–61 753, 2020.

[31] J. Wu, M. Barahona, Y.-J. Tan, and H.-Z. Deng, "Spectral measure of structural robustness in complex networks," *IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans*, vol. 41, no. 6, pp. 1244–1252, 2011.