Electronic Preprint for Journal of Information Processing Vol.28

Regular Paper

Predictability of Network Robustness from Spectral Measures

Kazuyuki Yamashita[1,a)] Yuichi Yasuda[1,b)] Ryo Nakamura[2,c)] Hiroyuki Ohsaki[1,d)]

Received: November 9, 2019, Accepted: June 1, 2020

Abstract: Robustness against failure and attack is one of the essential properties of large-scale dynamical system such as power grids, transportation system, communication systems, and computer networks. Despite its popularity and intuitiveness, a major drawback of descriptive robustness metrics such as the size of the largest connected component and the network diameter is computational complexity. Spectral measures such as the spectral radius, the natural connectivity, and the algebraic connectivity are much easier to obtain than descriptive metrics, but the *predictability* of those measures against different levels and types of failures has not been well understood. In this paper, we therefore investigate how effectively spectral measures can estimate the robustness of a network against random and adversary node removal. Our finding includes that, among five types of spectral measures, the effective resistance is most suitable for predicting the largest cluster component size under low node removal ratio, and that the predictability of the effective resistance is stable among different types of networks.

Keywords: network robustness, spectral measures, largest cluster component, random node removal, adversary node removal, scale-free network

1. Introduction

Robustness against failure and attack is one of the essential properties of large-scale dynamical system such as power grids, transportation system, communication systems, and computer networks [2]. The robustness of the network is a property that describes how much the entire network is functioning under circumstances where a part of the network has been removed by failure or attack [3]. In the literature, for constructing a robust system against failure and attack, many types of research have been performed to understand the robustness and also to improve the robustness by, for example, node/link protection and rewiring [4], [5].

Since the robustness is a multifaceted property of a network, several different metrics for network robustness — those from geometrical viewpoints (e.g., the size of the largest connected component, the average path length, and the efficiency) [3], [6], [7], [8], [9], [10] as well as spectral viewpoints (e.g., spectral radius, natural connectivity, and algebraic connectivity) [11], [12], [13], [14] — have been proposed in the literature.

Intuitive metrics for network robustness are geometrical ones; for instance, the *size* of the properly working subnetwork after failure or attack (e.g., the size of the largest connected component (i.e., the largest cluster [3])) and the *diameter* of the properly working subnetwork (e.g., the average path length [3], [9]). Generally, to measure one of those geometrical metrics, it is necessary to perform many simulations since failures are generally random processes. Through simulations, the robustness of a network can be estimated by, for example, measuring the largest cluster component size in synthetically degenerated networks.

Several spectral measures such as the spectral radius, the natural connectivity, and the algebraic connectivity quantify robustness-related properties of a graph such as the radius, connectivity, and redundancy. For instance, the spectral radius indicates the diffusion speed of information (e.g., virus and rumor) throughout the network, and the algebraic connectivity indicates the difficulty of network fragmentation [11], [14]. These spectral measures are obtained from the eigenvalues of the adjacency matrix or the Laplacian matrix given by the adjacency matrix and the degree matrix of a graph.

Robustness metrics can be classified into two categories: descriptive and predictive. Descriptive metrics measure how the network is functioning properly *after* failure or attack whereas predictive metrics estimate how the network is likely to function properly against *forthcoming* failure or attack.

Despite its popularity and intuitiveness, a major drawback of descriptive robustness metrics such as the size of the largest connected component and the diameter is the computational complexity; to evaluate the robustness of a network with a descriptive metric, the metric has to be measured *after* the occurrence of failure or attack, which generally requires, for instance, a large number of simulations.

Spectral measures such as the spectral radius, the natural con-

[1] Department of Informatics, Graduate School of Science and Technology, Kwansei Gakuin University, Sanda, Hyogo 669–1337, Japan
[2] Department of Electronics Engineering and Computer Science, Faculty of Engineering, Fukuoka University, Fukuoka 814–0180, Japan
[a)] kazuyuki@kwansei.ac.jp
[b)] yuichi@kwansei.ac.jp
[c)] r-nakamura@fukuoka-u.ac.jp
[d)] ohsaki@kwansei.ac.jp

This paper is an extension of Ref. [1].

nectivity, and the algebraic connectivity are much easier to obtain than descriptive metrics, but the *predictability* of those measures against different levels of failure or attack has not been well understood.

If we can predict the robustness of a network only from spectral measures without relying on measuring a descriptive metric, a more sophisticated understanding, designing, and redesigning of a network could be realized.

In this paper, we therefore investigate how effectively spectral measures can estimate the robustness of a network against random and adversary node removal. More specifically, we address the following research questions.

Q1. Among five spectral measures (the spectral radius, the spectral gap, the natural connectivity, the algebraic connectivity, and the effective resistance), which spectral measure does predict the geometrical metric (i.e., the size of the largest connected component) after random node removal most accurately?
It has been pointed out that several spectral measures (e.g., the natural connectivity and the algebraic connectivity) are related to the robustness against node and link removals [12], [14]. However, it is not sufficiently clarified whether spectral measures can be used as a substitute index for the size of the largest connected component and descriptive metrics.

Q2. How is the predictability of those spectral measures affected by the network (i.e., the topology, the network size, and the density)?
Depending on a system evaluated for robustness in question, the network topology, the number of nodes, and the number of links are diverse. As it is widely known that scale-free networks and denser networks are robust against random node removal [3], the robustness should depend on the features of networks.

Q3. Similarly, how is the predictability of those spectral measures affected by the degree of random node removal (e.g., under 1%, 5%, and 10% node loss)?
In our previous works, we have revealed that non-scale-free networks are robust when the node removal ratio is low, whereas scale-free networks are robust when the node removal ratio is high [8]. Also depending on the node removal ratio, the superiority of a network in terms of robustness is different. Therefore, similarly to Q2, it is necessary to clarify what extent the predictability of the spectral metric depends on the node removal ratio.

Q4. How are our observations regarding the above questions Q1–Q3 affected if nodes are removed *adversary* rather than randomly?
It is equivalently important to understand the robustness of a network not only against random node removal, which is generally caused by the failure of devices, but also against adversary node removal, which is caused by malicious attack. In the literature, it has been known that the robustness of a network against random node removal and adversary node removal significantly differs [3], [15], [16]. Therefore, answers to research questions Q1–Q3 might be quite different if the node removal pattern is changed.

To answer the above research questions, we investigate the predictability of the network robustness against random and adversary node removal from five spectral measures (the spectral radius, the spectral gap, the natural connectivity, the algebraic connectivity, and the effective resistance) through experiments.

Specifically, we generate a number of networks with different network sizes and densities using multiple synthetic network generation models, and measure the correlation between every spectral measure for a given network and its largest cluster component size after random and adversary node removal.

This paper is organized as follows. First, Section 2 summarizes previous works on the robustness of networks. Section 3 briefly explains the spectral measures used in this paper. Section 4 explains our experimental methodology. Section 5 presents experiment results and discusses the predictability of the network robustness from spectral measures. Section 6 investigates how the predictability of the network robustness is affected by the type of node removal. Finally, Section 7 provides a summary of this paper and addresses future works.

2. Related Works

In the literature, the robustness of a graph (or equivalently, a network) has been extensively studied in several research areas such as graph theory, network theory [17], network science [3], [9], [10], and network operations and management [7], [18].

In graph theory, classical measures called *vertex connectivity*, which is defined as the minimal vertex cut that separates a connected graph into multiple connected components, and *edge-connectivity*, which is defined as the smallest edge cut resulting in multiple connected components, have been extensively studied (see, for example, [17] and references therein). Graph connectivity is not identical to network robustness, but both are closely related.

In network science, the scale-free property of a complex network, which is generally characterized by the power-law distribution of node degrees, has been studied by many researchers [3], [9], [10]. One of major interesting findings in network science is that, in terms of the largest cluster component size and the diameter, scale-free networks are robust against random node removals whereas scale-free networks are fragile against adversary node removal. However, contrary to the common understanding, the authors of Ref. [19] reported that when the node removal ratio is not so high, non-scale-free networks are more robust against random node removal than scale-free networks in terms of the largest cluster component size.

On the other hand, the recent advancement in spectral graph theory enables spectral analysis of network robustness based on the distribution of eigenvalues of an adjacency matrix or a Laplacian matrix, each of which is constructed from the topology of a network [11], [12], [13], [14]. A variety of spectral measures for quantifying the network robustness such as the spectral radius [11], the natural connectivity [14] and the algebraic connectivity [12], have been proposed. In Ref. [12], the authors investigated the relationship between the node/link connectivity and the algebraic connectivity in various networks with different structures and scales. As a result, the authors show that the

algebraic connectivity increases as the node/link connectivity increases. Since the node/link connectivity correlates with the algebraic connectivity, it is expected that the algebraic connectivity could be regarded as an index for measuring the network robustness. On the other hand, in Ref. [14], the network robustness against edge removal is examined using the natural connectivity. Consequently, the authors show that as the number of link removals increases, the algebraic connectivity becomes zero when the network is disconnected. In contrast, it is shown that as the number of link removal increases, the natural connectivity smoothly decreases. This indicates that the natural connectivity might be suitable as an index for the network robustness against node/link removal.

To the best of our knowledge, the relationship between the graph metrics of a network and its robustness has been partly understood. In Ref. [20], Spearman's rank correlation coefficient between among every graph metric and flow robustness (e.g., the ratio of the number of reliable flows to the total number of flows in the network [21]) has been investigated. The authors show that the path diversity metric, the node-betweenness centrality and the effective resistance are suitable for quantifying the network robustness. However, the predictability of the network robustness from spectral metrics has not been clarified since their simulation experiments only use small graphs with 20 nodes.

Spectral-measure-based network redesign (e.g., rewiring links in a network so that a spectral measure for robustness is maximized) is one of the active research areas in the network robustness [4], [5]. For example, in Ref. [4], the authors proposed a method to improve the algebraic connectivity by sequentially rewiring links in the network.

3. Spectral Measures

In what follows, we briefly explain the definitions of five spectral measures used in this paper. Please refer to Ref. [5] for the details.

For a given graph $G = (V, E)$, let A and $D(= diag(d_v))$ denote adjacency matrix and degree matrix, respectively. Here, d_v represents the degree of node $v \in V$. From the adjacency and degree matrices, Laplacian matrix L of graph G is defined as $L = D - A$. Let $\lambda_N \leq \lambda_{N-1} \leq \cdots \leq \lambda_2 \leq \lambda_1$ denote a set of eigenvalues of adjacency matrix A, where $N(= |V|)$ represents the number of nodes. Also, let $\mu_1 \leq \mu_2 \leq \cdots \leq \mu_{N-1} \leq \mu_N$ denote a set of eigenvalues of Laplacian matrix L.

From the eigenvalues of adjacency and Laplacian matrices, five spectral measures are defined as follows.

- Spectral radius
  The spectral radius is defined as the largest eigenvalue λ_1 of adjacency matrix A. Spectral radius is one of important metrics of dynamical processes on a graph (e.g., propagation of virus and rumor). It is known that the graph with small spectral radius is robust against the propagation of information such as virus [11].
- Spectral gap
  The spectral gap is defined as the difference $\lambda_1 - \lambda_2$ in the largest eigenvalue λ_1 and the second largest eigenvalue λ_2 of adjacency matrix A. The spectral gap is known to be related to expansion properties of a graph (i.e., how the graph is sparse and highly-connected) [5].
- Natural connectivity
  From a set of eigenvalues of adjacency matrix A, the natural connectivity is defined as

$$\log\left(\frac{1}{N}\sum_{i=1}^{N} e^{\lambda_i}\right). \tag{1}$$

  Natural connectivity indicates the redundancy of a graph, and its characteristics is that it changes monotonically with the increase/decrease in the number of edges in the graph [14].
- Algebraic connectivity
  The algebraic connectivity is defined as the second smallest eigenvalue μ_2 of Laplacian matrix L. Algebraic connectivity indicates how easily/hardly a graph is disconnected. A graph with large algebraic connectivity indicates that it is difficult to divide the graph to subgraphs [12].
- Effective resistance
  From a set of eigenvalues of Laplacian matrix L, the effective resistance is defined as

$$N\sum_{i=2}^{N}\frac{1}{\mu_i}. \tag{2}$$

  Effective resistance is calculated from the sum of inverses of eigenvalues obtained from a Laplacian matrix. Effective resistance implies the robustness of a graph [5].

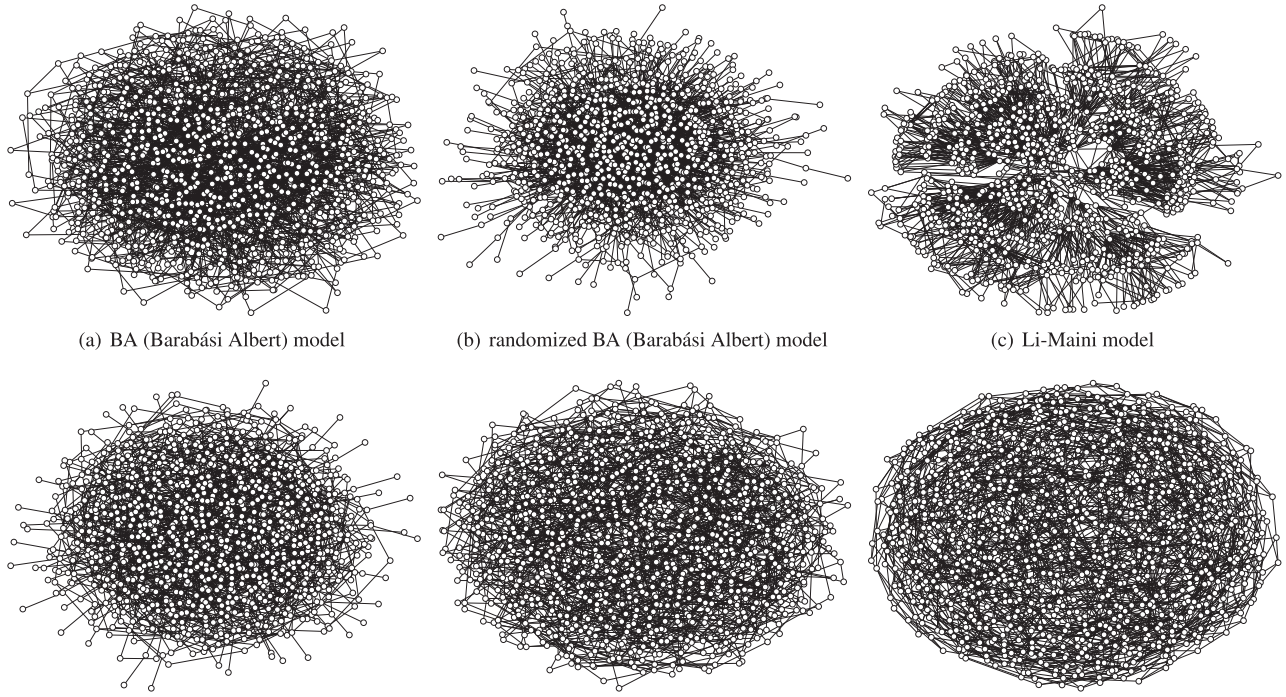
4. Method

Through experiments, we investigated the predictability of the network robustness against random node removal from five spectral measures (the spectral radius, the spectral gap, the natural connectivity, the algebraic connectivity, and the effective resistance). Specifically, we generated multiple networks for different network sizes and densities using synthetic network generation models, and measured the correlation between every spectral measure for a given original network and the largest cluster component size for the network after random node removals. **Figure 2** illustrates the overview of our experiments. In our experiments, we calculated the correlation of the spectral measures of original networks and the largest cluster component sizes of networks after random node removal.

We generated a large number of networks using six network generation models (BA (Barabási Albert) model [22], randomized BA model, Li-Maini model [23], ER (Erdős-Rényi) model [24], DB (Degree-Bounded) model [19], and random regular graph) with different network sizes and densities.

The DB model generates a network with N nodes and the average degree of $\bar{k}$. The DB model generates a degree-bounded random network as follows; (1) N nodes are initiated; and (2) for every node, $\bar{k}/2$ links are added between the node and another randomly-chosen node.

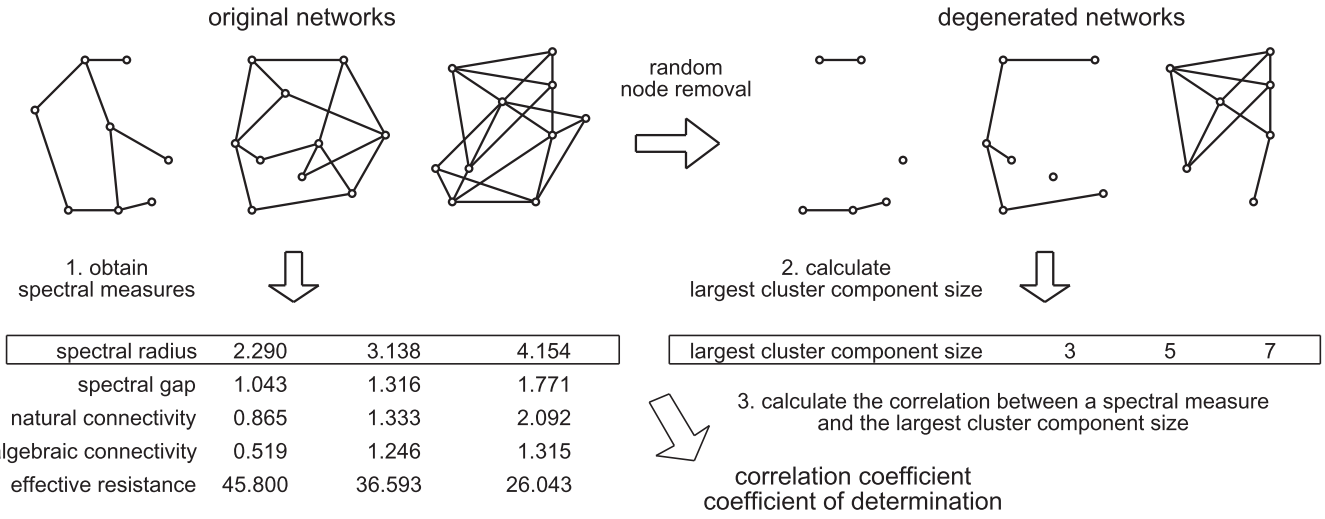
Since the BA model generates a network by repeatedly adding vertices with a fixed number m of edges, it can only generate networks with specific average degrees. The randomized BA model



(a) BA (Barabási Albert) model (b) randomized BA (Barabási Albert) model (c) Li-Maini model

(d) ER (Erdõs-Rényi) model (e) DB (Degree-Bounded) model (f) random regular graph

Fig. 1 Example networks generated with six types of network generation models (N = 1,000 and $\bar{k}$ = 4).



spectral radius	2.290	3.138	4.154
spectral gap	1.043	1.316	1.771
natural connectivity	0.865	1.333	2.092
algebraic connectivity	0.519	1.246	1.315
effective resistance	45.800	36.593	26.043

largest cluster component size	3	5	7

Fig. 2 An overview of our experiments.

relaxes this limitation; i.e., it can generate a scale-free network with an arbitrary average degree.

The difference between the BA model and the randomized BA model is in their preferential attachment stages. At the k-th cycle, the randomized BA model adds a node with a random number X_k of edges whereas the BA model with the fixed number m of edges. More specifically, in the randomized BA model, the number X_k of edges added at the k-th cycle is determined by the Bernoulli process with the probability of $1/m$.

The Li-Maini model [23] is one of network generation models for creating networks with cluster (i.e., community) structure. It has been designed to recreate the community structure observed in many social and biological networks. The Li-Maini model is an evolving network model based on inner-community and inter-community preferential attachment.

In our experiments, the network size N was varied between 100 and 1,000. Also, the average degree $\bar{k}$ (i.e., the network density) was varied between 4 and 8. We generated 100 network instances with each network generation model for given conditions (i.e., the network size N and the average degree $\bar{k}$).

Example networks generated with those network generation models are illustrated in **Fig. 1**. This figure visualizes the differences in generated networks; for instance, the network generated with Li-Maini model has a cluster structure.

For given network model M and node removal ratio p, we investigate the correlation between one of spectral measures for the *original* network and a descriptive metric (i.e., the largest cluster component size) for the *degenerated* network. In our experiments, we calculated five spectral measures from the adjacency and the Laplacian matrices of the original network. We then ob-

tained a degenerated network by randomly removing nodes from the original network, and the largest cluster component size in the degenerated network.

The correlation is measured by the correlation coefficient and the coefficient of determination. More specifically, for network model M, node removal ratio p, and spectral measure m, we measure the correlation coefficient $C^m_{M,p}$ and the determination of correlation $R^m_{M,p}$. The correlation is calculated as follows; (1) 100 network instances with N nodes and average degree $\overline{k}$ are generated using network generation model M; and (2) for these 100 network instances, the mean $\overline{m}$ of spectral measure m is calculated; and (3) degenerated networks are obtained by randomly removing p% of nodes from these network instances, and the mean $\overline{L(p)}$ of largest cluster component sizes of these degenerated networks is calculated; and (4) by repeating (1) to (3) while changing network size N and average degree $\overline{k}$, multiple samples of ($\overline{m}$, $\overline{L(p)}$) are obtained; and (5) from samples of ($\overline{m}$, $\overline{L(p)}$) obtained in (4), the correlation coefficient $C^m_{M,p}$ is calculated by the following equation, and the determination of correlation $R^m_{M,p}$ is obtained.

$$C^m_{M,p} = \frac{cov(\overline{m}, \overline{L(p)})}{\sigma_{\overline{m}} \sigma_{\overline{L(p)}}} \tag{3}$$

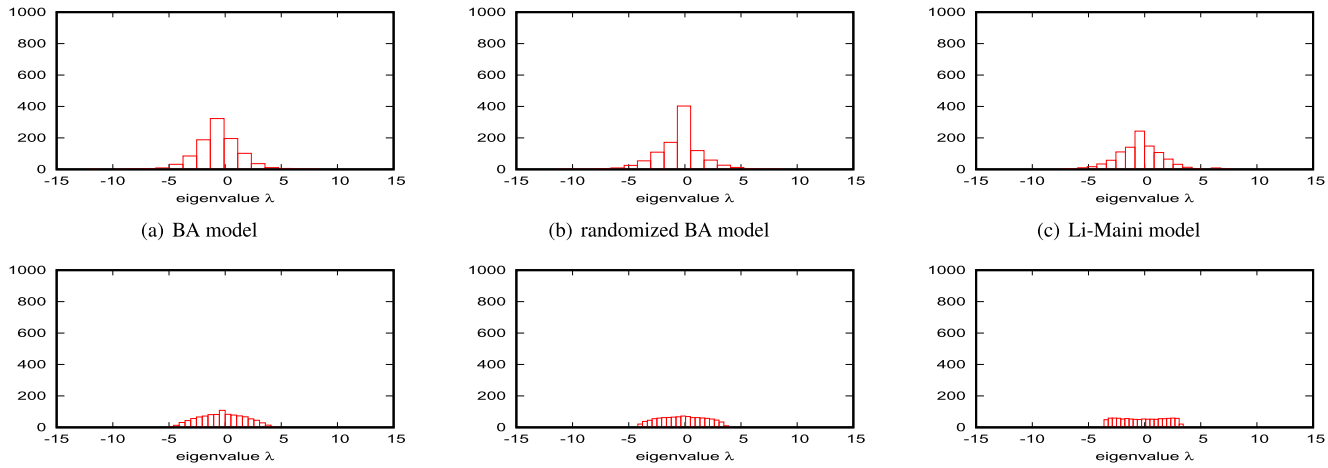
Here, $cov(\overline{m}, \overline{L(p)})$ is the covariance of $\overline{m}$ and $\overline{L(p)}$, $\sigma_{\overline{m}}$ and $\sigma_{\overline{L(p)}}$ are standard deviations of $\overline{m}$ and $\overline{L(p)}$, respectively.

5. Results and Discussion

Before investigating the correlation between spectral measures and a descriptive robustness metrics, we examine the spectral properties of six types of networks as well as their robustness against random node removal.

The spectrum of six types of networks (i.e., the histogram of eigenvalues of an adjacency matrix and a Laplacian matrix) are plotted in **Figs. 3** and **4**, respectively. In those figures, results for six network generation models are plotted. From these results, it is found that the distribution of eigenvalues highly depends on the network generation model. Specifically, in the case of scale-free networks whose degree distribution is highly skewed (BA, randomized BA, and Li-Maini), the distribution of eigenvalues for those networks are also highly skewed.

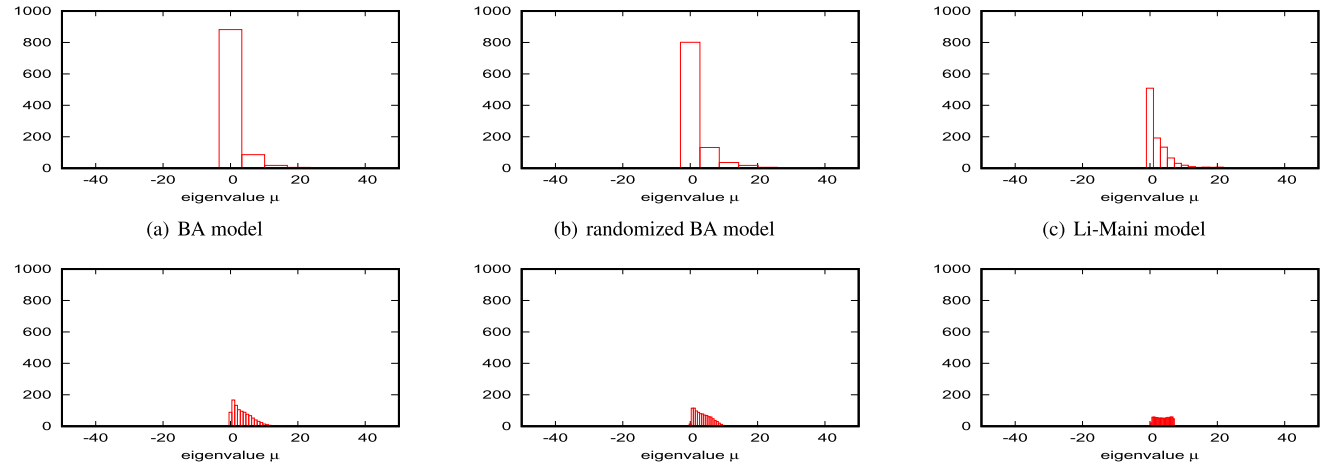
Spectral measures summarized in Section 3 are directly defined from those eigenvalues — eigenvalues λ_i of an adjacency matrix and eigenvalues μ_i of a Laplacian matrix; e.g., the spectral radius is the maximum of λ_i, the algebraic connectivity is the second minimum of μ_i, and the effective resistance is proportional to the



(a) BA model (b) randomized BA model (c) Li-Maini model

(d) ER model (e) DB model (f) random regular graph

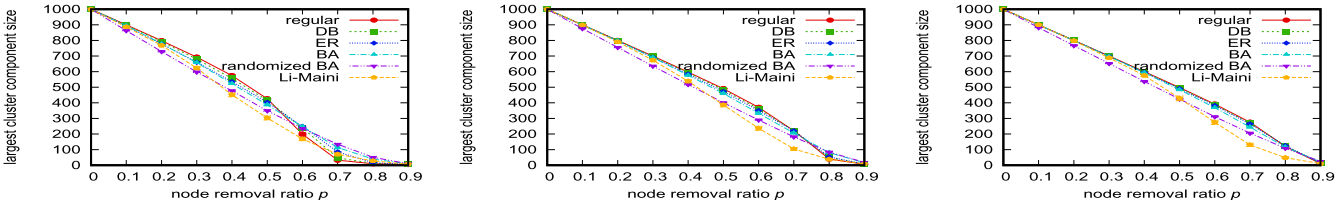
Fig. 3 Histogram of eigenvalues λ of an adjacency matrix for a network instance (N = 1,000 and $\overline{k}$ = 4).



(a) BA model (b) randomized BA model (c) Li-Maini model

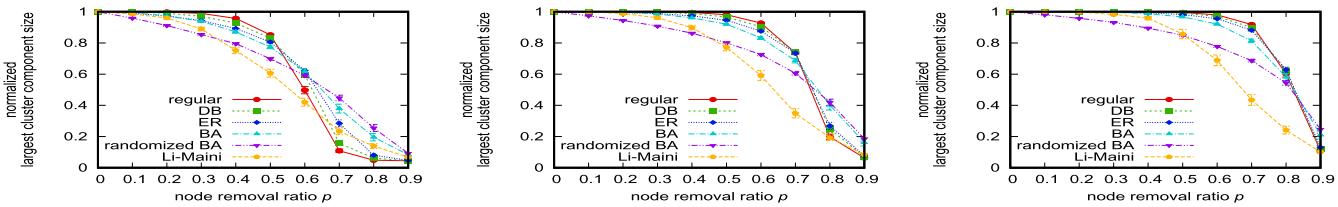
(d) ER model (e) DB model (f) random regular graph

Fig. 4 Histogram of eigenvalues μ of a Laplacian matrix for a network instance (N = 1,000 and $\overline{k}$ = 4).



(a) $\overline{k} = 4$ (b) $\overline{k} = 6$ (c) $\overline{k} = 8$

Fig. 5 Relation between the node removal ratio and the largest cluster component size after random node removal for networks with different densities (N = 1,000).



(a) $\overline{k} = 4$ (b) $\overline{k} = 6$ (c) $\overline{k} = 8$

Fig. 6 Relation between the node removal ratio and the normalized largest cluster component size after random node removal for networks with different densities (N = 1,000).

average of $1/\mu_i$.

Figures 3 and 4 illustrate that every type of network has different spectral properties, indicating that every type of network should have a different robustness against node removal.

The robustness of six types of networks is shown in **Figs. 5** and **11**, which illustrate how the largest cluster component is shrunk as the number of randomly-removed node increases. To clarify the difference of the largest cluster component sizes among six types of networks, the *normalized* largest cluster component size, which is defined as the ratio of the largest cluster component size to the network size (i.e., the number of remaining nodes excluding removed nodes), is plotted in **Fig. 6**. From these results, it can be found that the largest cluster component sizes vary according to the network generation model and the node removal ratio. Namely, when the node removal ratio is low (i.e., $p \leq 0.5$), the largest cluster component size of non-scale-free networks (e.g., DB and random regular graph) is larger than that of non-scale-free networks. On the contrary, when the node removal ratio is extremely high (i.e., $p \geq 0.7$), the largest cluster component size of scale-free networks (e.g., BA and randomized BA) is larger than that of non-scale-free networks.

These simulation results indicate that the robustness against random node removal is quite different in six types of networks and that such difference is noticeable in rather sparse networks (e.g., $\overline{k} = 4$). However, for denser networks (e.g., $\overline{k} = 8$), the difference in the largest cluster component size of network generation models except for the randomized BA model is marginal when the node removal ratio is not so high (i.e., $p \leq 0.5$).

The predictability of the network robustness against random node removal is shown in **Figs. 7** and **8**, which depict the correlation coefficient between every spectral measure and the largest cluster component size for different node removal ratios p. In Fig. 7, for a given network model, results for spectral measures are shown. Also, in Fig. 8, for a given spectral measure, results for different network generation models are shown.

One can find from Figs. 7 and 8 that the effective resistance has a much stronger correlation with the largest cluster component size than the other spectral measures unless the node removal ratio is very high, which suggests high predictability of the network robustness from the effective resistance. Also, one can find that the spectral radius seems to be the best metric to predict the network robustness under extremely-high node removal ratios. Similar to the spectral radius, the natural connectivity might be usable to predict the network robustness. However, the spectral gap and the algebraic connectivity are not suitable for predicting the network robustness since those two spectral measures are unstable (i.e., the strength of the correlation highly depends on the type of networks).

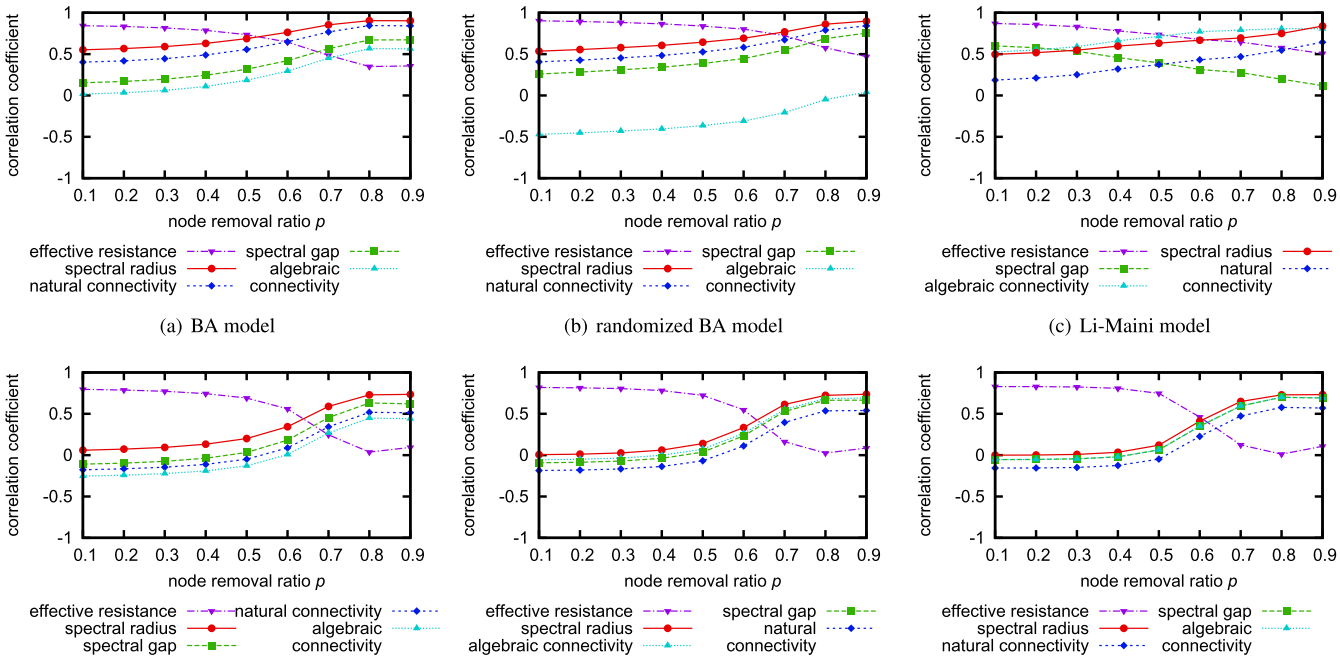
Stability of the predictability is also the favorable property of the effective resistance as shown in Fig. 8, which illustrates how the correlation coefficient between a spectral measure and the largest cluster comment size after random node removal are affected by the network topology.

In **Figs. 9** and **10**, the predictability of the network robustness from the effective resistance is also examined by the coefficient of determination, which is defined as the fraction of the variation that can be explained by the regression equation. These figures indicate that the coefficient of determination of the effective resistance is much higher than those of the other spectral measures.

Finally, based on our observations, we answer the research questions presented in Section 1.

Q1. Among five spectral measures (spectral radius, spectral gap, natural connectivity, algebraic connectivity, and effective resistance), which spectral measure predicts the geometrical metric (i.e., the largest cluster component) after random node failure most accurately?

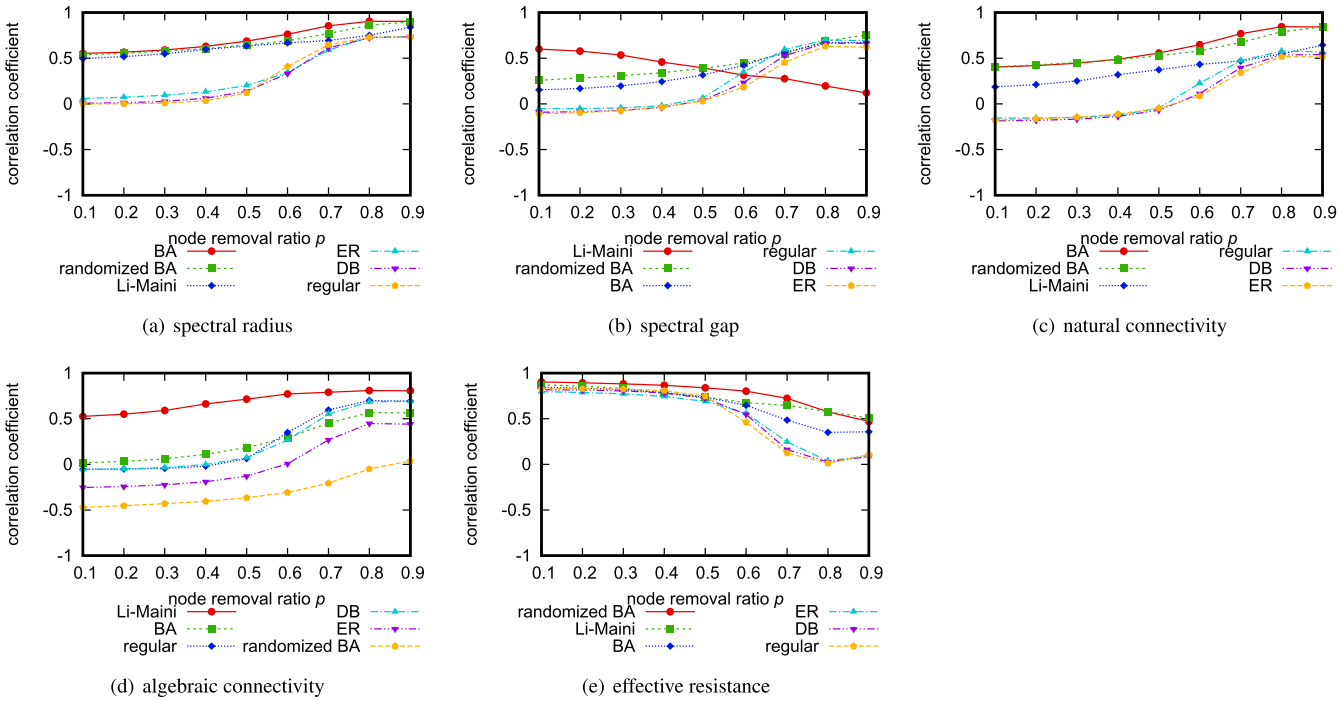
Among the five types of spectral measures focused in this paper, the effective resistance is most suitable for predicting the largest cluster component size under low node removal ratio (i.e., $p \leq 0.5$). However, the spectral radius and the natural connectivity are usable under the extremely-high node removal ratio (i.e., $p \geq 0.7$).



(a) BA model (b) randomized BA model (c) Li-Maini model

(d) ER model (e) DB model (f) random regular graph

Fig. 7 Correlation coefficient between every spectral measure and the largest cluster component size after random node removal.



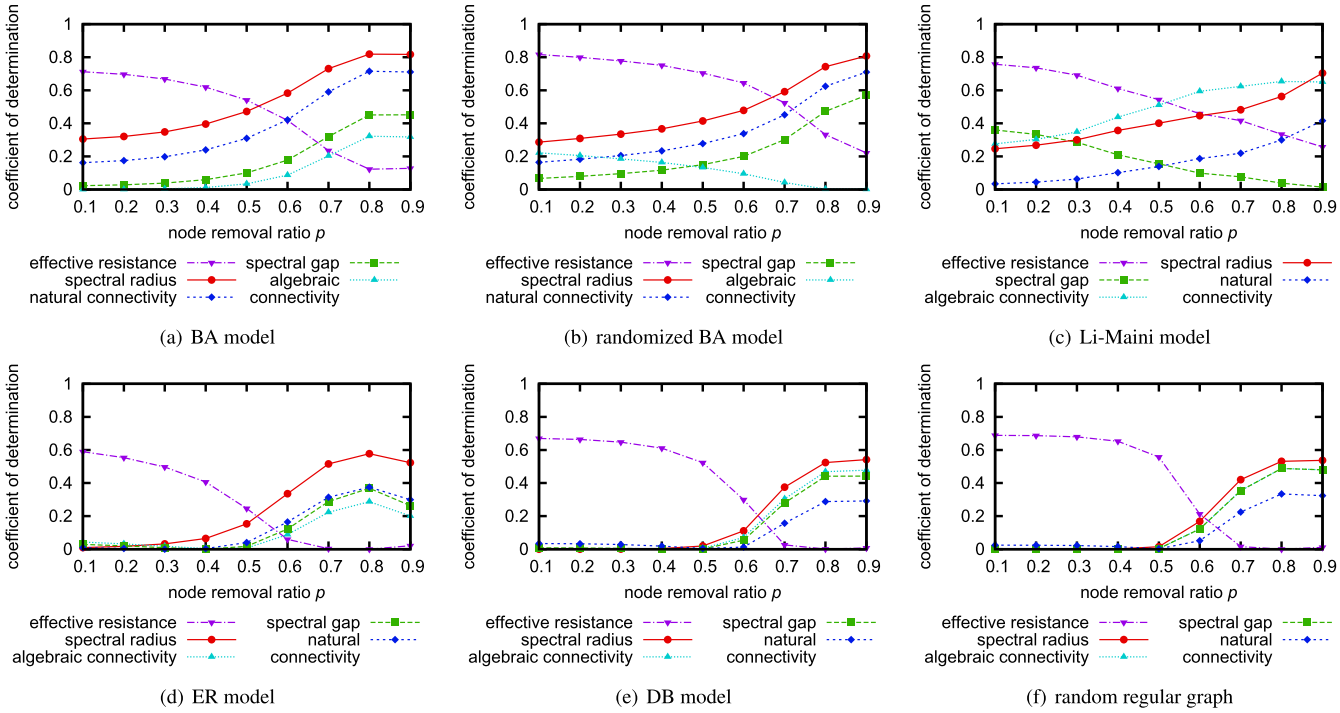
(a) spectral radius (b) spectral gap (c) natural connectivity

(d) algebraic connectivity (e) effective resistance

Fig. 8 Correlation coefficient between every spectral measure and the largest cluster component size after random node removal for different network generation models.

Q2. How is the predictability of those spectral measures affected by the network (i.e., topology, network size, and density)?
As Figs. 8 and 10 imply, the effective resistance is *stable* for networks generated with six types of generation models. In particular, the correlation between the effective resistance and the largest cluster component size are stronger for scale-free networks rather than non-scale-free networks.

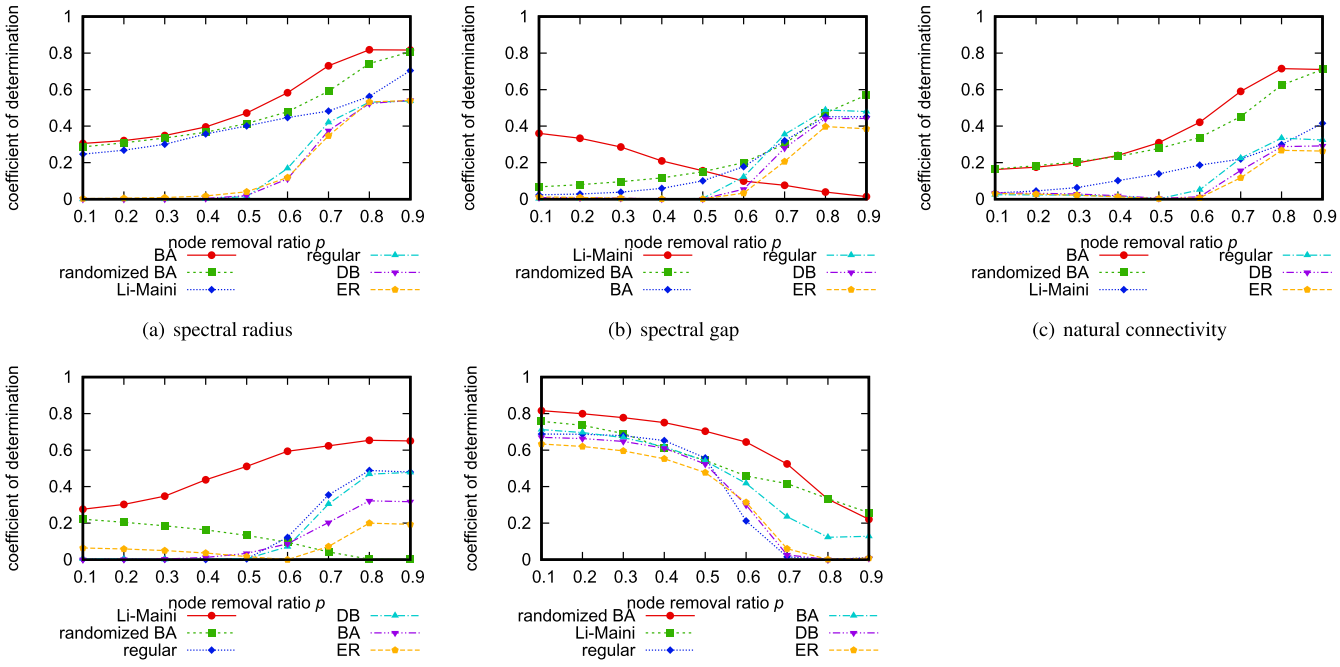
Q3. Similarly, how is the predictability of those spectral measures affected by the degree of random node failure (e.g., under 1%, 5%, and 10% node loss)?
As described in answer to Q1, the predictability of spectral measures is highly affected by the node removal ratio. Namely, under a low node removal ratio, the effective resistance is usable, whereas, under a high node removal ratio, the spectral radius and the natural connectivity are usable. For this reason, it is required to choose the spectral measure according to the evaluated system appropriately. For instance, in the context of evaluating the robustness of computer net-



(a) BA model (b) randomized BA model (c) Li-Maini model

(d) ER model (e) DB model (f) random regular graph

Fig. 9 Coefficient of determination between every spectral measure and the largest cluster component size after random node removal.



(a) spectral radius (b) spectral gap (c) natural connectivity

(d) algebraic connectivity (e) effective resistance

Fig. 10 Coefficient of determination between every spectral measure and the largest cluster component size after random node removal for different network generation models.

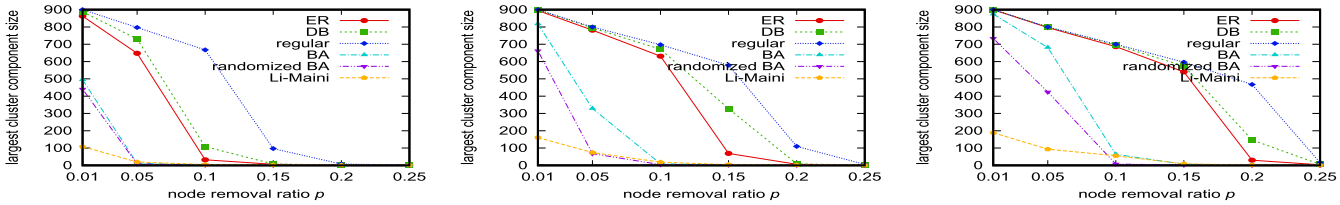
works, the node removal ratio is not so high, which suggests using the effective resistance for predicting the network robustness.

6. Case of Adversary Node Removal

In this section, we investigate the predictability of the network robustness from spectral measures under adversary node removal rather than random node removal.

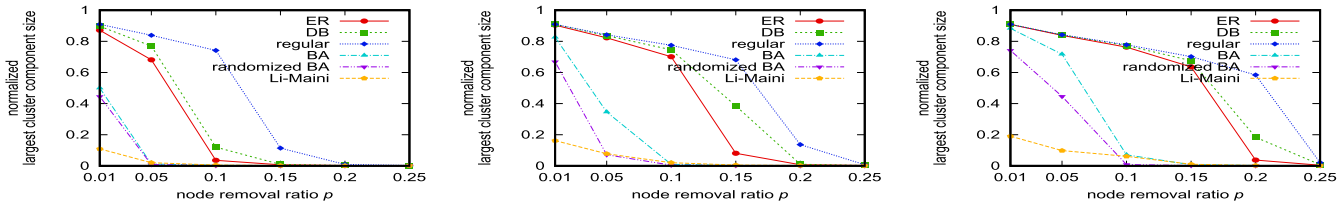
We use the same methodology with that in Section 4 except that, for a given node removal ratio p, a fraction p of high-degree nodes are *deterministically* removed from the network; i.e., nodes are removed from the network in the descending order of their degrees. In adversary node removal, the largest hub node with the largest number of links with other nodes is always removed from the network at first. The second largest hub node is removed next. Such a process is repeated until a fraction p of nodes are removed from the network.

The (normalized) largest component sizes of six types of net-



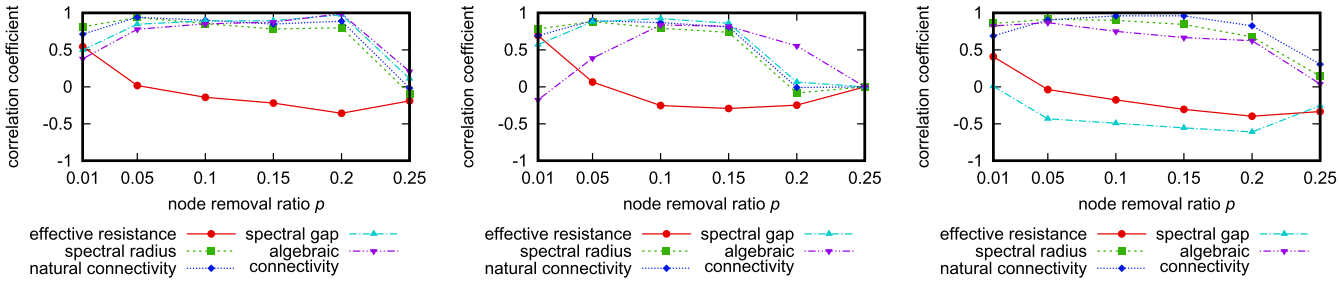
(a) $\overline{k} = 4$ (b) $\overline{k} = 6$ (c) $\overline{k} = 8$

Fig. 11 Relation between the node removal ratio and the largest cluster component size after adversary node removal for networks with different densities (N = 1,000).

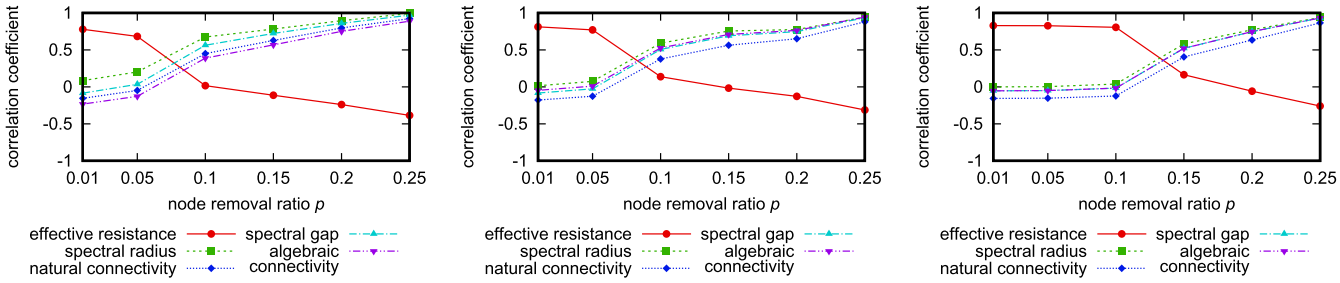


(a) $\overline{k} = 4$ (b) $\overline{k} = 6$ (c) $\overline{k} = 8$

Fig. 12 Relation between the node removal ratio and the normalized largest cluster component size after adversary node removal for networks with different densities (N = 1,000).



(a) BA model (b) randomized BA model (c) Li-Maini model

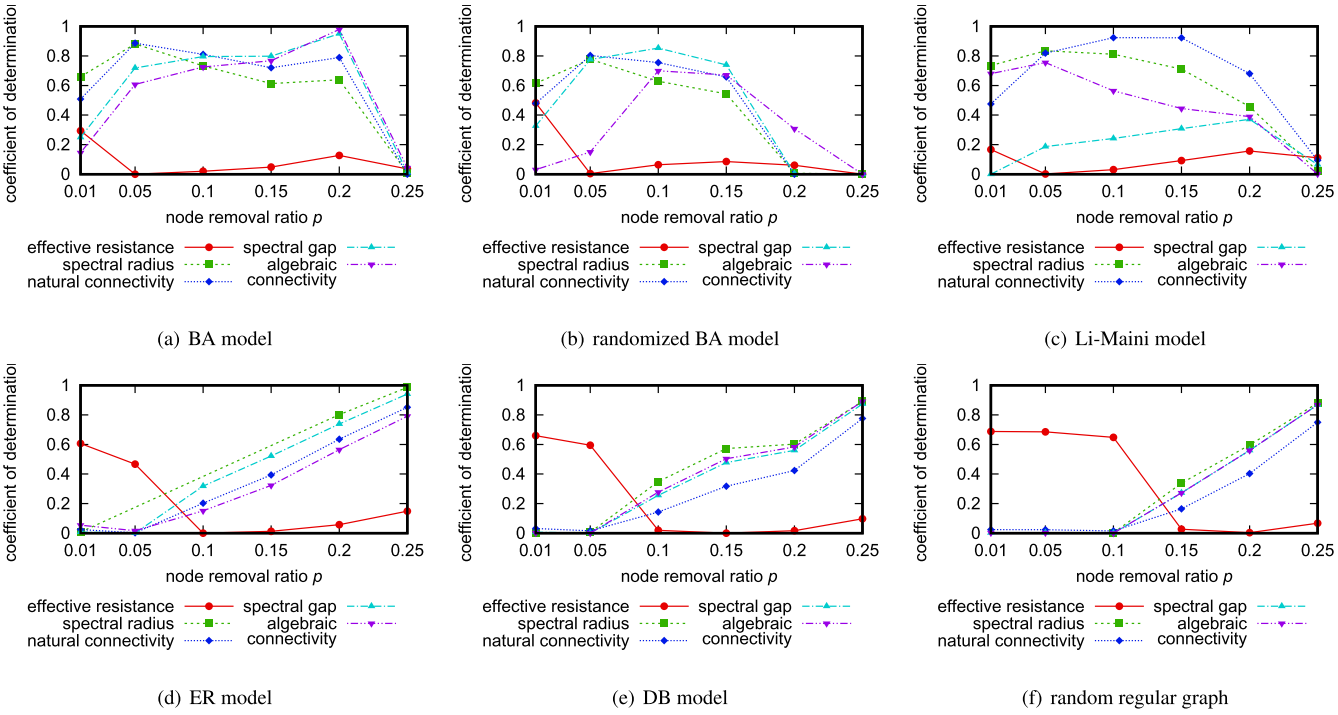


(d) ER model (e) DB model (f) random regular graph

Fig. 13 Correlation coefficient between every spectral measure and the largest cluster component size after adversary node removal.

works for different node removal ratios p are shown in **Figs. 11** and **12**, which clearly illustrate the vulnerability of scale-free networks (i.e., BA, randomized BA and Li-Maini) compared with non-scale-free networks (i.e., ER, DB and random regular graph). From those results, it can be found that similar to the case of random node removal, the largest cluster component sizes vary according to the network generation model and the node removal ratio. Namely, non-scale-free networks are more robust than scale-free networks and the random regular graph shows the best robustness among others. Moreover, it can be found that networks generated with all network generation models are isolated when the node removal ratio exceeds approximately 0.3.

The predictability of the network robustness against adversary node removal is illustrated in **Figs. 13** and **14**. One can find from Fig. 13 that the predictability of the spectral measures is highly affected by the network generation models and the node removal ratio. In non-scale-free networks, it can be found that the effective resistance has a much stronger correlation with the largest cluster component size than other spectral measures until giant cluster collapse ($p \leq 0.1$). On the other hand, one can find that the spectral radius seems to be the best metric to predict the network robustness in a scale-free network or any network for $p \geq 0.1$. The weak correlation between the effective resistance and the largest cluster component size in scale-free networks is probably due to the collapse of the giant cluster in those networks. Note that Fig. 11 illsutrates that the giant cluster diminishes in all scale-free



(a) BA model (b) randomized BA model (c) Li-Maini model

(d) ER model (e) DB model (f) random regular graph

Fig. 14 Coefficient of determination between every spectral measure and the largest cluster component size after adversary node removal.

networks even when the node removal ratio is small.

Finally, based on our observations, we answer the last research question presented in Section 1.

Q4. How are our observations regarding the above questions Q1–Q3 affected if nodes are removed *adversary* rather than *randomly*?

In the case of adversary node removal, the same conclusion as in the case of random node removal can be obtained. The predictability of the spectral measures is highly affected by the node removal ratio. The effective resistance is still suitable for predicting the largest cluster component size until the giant cluster collapses. Also, the spectral radius is usable when the node removal ratio is not small.

7. Conclusion

In this paper, we have investigated how effectively spectral measures can estimate the robustness of a network against random node failure. Through experiments, we have investigated the predictability of the network robustness against random node removal from five spectral measures (the spectral radius, the spectral gap, the natural connectivity, the algebraic connectivity, and the effective resistance). Specifically, we have generated multiple networks for different network sizes and densities using synthetic network generation models, and measured the correlation between every spectral measure for a given original network and the largest cluster component size for the network after random node removals. Consequently, we have shown that that, among five types of spectral measures, the effective resistance is most suitable for predicting the largest cluster component size under low a node removal ratio, and that the predictability of the effective resistance is stable for various networks generated with different network generation models. Furthermore, we have investigated the predictability of the network robustness from spectral measures under adversary node removal and revealed observations in the predictability of spectral measures for random node removal are still valid for adversary node removal.

As future work, we are planning to investigate the predictability of other descriptive metrics from spectral measures, and examine whether the descriptive metric (e.g., the largest cluster component size) can be estimated from spectral measures.

Acknowledgments This work was partly supported by JSPS KAKENHI Grant Number 19H04104 and 18J10278.

References

[1] Yamashita, K., Yasuda, Y., Nakamura, R. and Ohsaki, H.: On the Predictability of Network Robustness from Spectral Measures, *Proc. 7th IEEE International Workshop on Architecture, Design, Deployment and Management of Networks and Applications* (*ADMNET 2019*), pp.24–29 (2019).

[2] Albert, R. and Barabási, A.-L.: Statistical mechanics of complex networks, *Reviews of Moder Physics*, Vol.74, No.1, pp.47–97 (2002).

[3] Albert, R., Jeong, H. and Barabási, A.-L.: Error and attack tolerance of complex networks, *Nature*, Vol.406, pp.378–382 (2000).

[4] Sydney, A., Scoglio, C. and Gruenbacher, D.: Optimizing algebraic connectivity by edge rewiring, *Applied Mathematics and Computation*, Vol.219, pp.5465–5479 (2013).

[5] Chan, H. and Akoglu, L.: Optimizing network robustness by edge rewiring: a general framework, *Data Mining and Knowledge Discovery*, Vol.30, No.5, pp.1395–1425 (2016).

[6] Latora, V. and Marchiori, M.: Efficient Behavior of Small-World Networks, *Physical Review Letters*, Vol.87, No.19, pp.198701-1–198701-4 (2001).

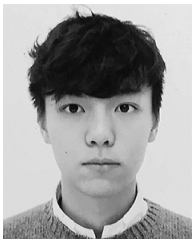
[7] Schneider, C.M., André A. Moreira, J.S.A.J., Havlin, S. and Herrmann, H.J.: Mitigation of malicious attacks on networks, *PNAS*, Vol.108, No.10, pp.3838–3841 (2011).

[8] Yamashita, K., Yasuda, Y., Nakamura, R. and Ohsaki, H.: Revisiting the Robustness of Complex Networks against Random Node Removal, *Journal of Information Processing*, Vol.27, pp.643–649 (2019).

[9] Holme, P., Kim, B.J., Yoon, C.N. and Han, S.K.: Attack vulnerability of complex networks, *Physical Review E*, Vol.65, pp.056109-1–056109-14 (2002).

[10] Crucitti, P., Latora, V., Marchiori, M. and Rapisarda, A.: Error and at-

tack tolerance of complex networks, *Physica A: Statistical Mechanics and its Applications*, Vol.340, pp.388–394 (2002).
[11] Jamakovic, A., Kooij, R., Mieghem, P.V. and van Dam, E.: Robustness of networks against viruses: the role of the spectral radius, *Proc. 13th IEEE Symposium on Communications and Vehicular Technology* (*SCVT 2006*), pp.35–38 (2006).
[12] Jamakovic, A. and Mieghem, P.V.: On the Robustness of Complex Networks by Using the Algebraic Connectivity, *Proc. 7th International IFIP-TC6 Networking Conference* (*NETWORKING 2008*), pp.183–194 (2008).
[13] Baras, J.S. and Hovareshti, P.: Efficient and robust communication topologies for distributed decision making in networked systems, *Proc. Joint 48th IEEE Conference on Decision and Control* (*CDC 2009*) *and 28th Chinese Control Conference*, pp.3751–3756 (2009).
[14] Jun, W., Barahona, M., Yue-Jin, T. and Hong-Zhong, D.: Natural Connectivity of Complex Networks, *Chinese Physic Letters*, Vol.27, No.7, pp.078902-1–078902-4 (2010).
[15] Cohen, R., Havlin, S. and Ben-Avraham, D.: Structural properties of scale free networks, *Handbook of Graphs and Networks*, Vol.4 (2003).
[16] Iyer, S., Killingback, T., Sundaram, B. and Wang, Z.: Attack robustness and centrality of complex networks, *PloS One*, Vol.8, No.4 (2013).
[17] Dekker, A.H. and Colbert, B.D.: Network Robustness and Graph Topology, *Proc. 27th Australasian Conference on Computer Science*, pp.359–368 (2004).
[18] Alderson, D., Li, L., Willinger, W. and Doyle, J.C.: Understanding Internet topology: principles, models, and validation, *IEEE/ACM Trans. Networking*, Vol.13, No.6, pp.1205–1218 (2005).
[19] Yamashita, K., Nakamura, R. and Ohsaki, H.: A Study on Robustness of Complex Networks against Random Node Removals, *Proc. 42nd IEEE Signature Conference on Computers, Software, and Applications* (*Student Research Symposium*) (*COMPSAC 2018*), pp.966–969 (2018).
[20] Alenazi, M.J.F. and Sterbenz, J.P.G.: Comprehensive comparison and accuracy of graph metrics in predicting network resilience, *2015 11th International Conference on the Design of Reliable Communication Networks* (*DRCN*), pp.157–164 (2015).
[21] Rohrer, J.P., Jabbar, A. and Sterbenz, J.P.: Path diversification: A multipath resilience mechanism, *2009 7th International Workshop on Design of Reliable Communication Networks*, pp.343–351, IEEE (2009).
[22] Barabási, A.-L. and Albert, R.: Emergence of Scaling in Random Networks, *Science*, Vol.286, No.5439, pp.509–512 (1999).
[23] Li, C. and Maini, P.K.: An evolving network model with community structure, *Journal of Physics A: Mathematical and General*, Vol.38, No.45, pp.9741–9749 (2005).
[24] Erdös, P. and Rényi, A.: On random graphs I., *Mathematicae*, Vol.6, No.26, pp.290–297 (1959).



Kazuyuki Yamashita received his B.E. degree in the Informatics from Kwansei Gakuin University, Japan, in 2019. His research work is in the area of evaluation of complex networks in terms of robustness. He is a student member of IEEE and Institute of Electronics, Information, and Communication Engineers of Japan (IEICE) and Information Processing Society of Japan (IPSJ).

Yuichi Yasuda received his B.E. and M.E. degrees in the Informatics from Kwansei Gakuin University, Japan, in 2018 and 2020, respectively. His research work is in the area of design and evaluation of Information-Centric Networking.

Ryo Nakamura received his M.E. and Ph.D. degrees from Kwansei Gakuin University, Japan, in 2017 and 2020, respectively. He is currently an assistant professor at Department of Electronics Engineering and Computer Science, Faculty of Engineering, Fukuoka University, Japan. His research work is in the area of performance analysis and evaluation of Information-Centric Networking. He is a member of IEEE, Institute of Electronics, Information and Communication Engineers of Japan (IEICE), and Information Processing Society of Japan (IPSJ).

Hiroyuki Ohsaki received his M.E. degree in the Information and Computer Sciences from Osaka University, Osaka, Japan, in 1995. He also received his Ph.D. degree from Osaka University, Osaka, Japan, in 1997. He is currently a professor at Department of Informatics, School of Science and Technology, Kwansei Gakuin University, Japan. His research work is in the area of design, modeling, and control of large-scale communication networks. He is a member of IEEE and Institute of Electronics, Information and Communication Engineers of Japan (IEICE).